Workbook

SANS

THE MOST TRUSTED SOURCE FOR INFORMATION SECURITY TRAINING, CERTIFICATION, AND RESEARCH | sans.org

https://t.me/learningnets

Copyright © 2021 Robert M. Lee and SANS Institute. All rights reserved to Robert M. Lee and/or SANS Institute.

PLEASE READ THE TERMS AND CONDITIONS OF THIS COURSEWARE LICENSE AGREEMENT ("CLA") CAREFULLY BEFORE USING ANY OF THE COURSEWARE ASSOCIATED WITH THE SANS COURSE. THIS IS A LEGAL AND ENFORCEABLE CONTRACT BETWEEN YOU (THE “USER”) AND SANS INSTITUTE FOR THE COURSEWARE. YOU AGREE THAT THIS AGREEMENT IS ENFORCEABLE LIKE ANY WRITTEN NEGOTIATED AGREEMENT SIGNED BY YOU.

With the CLA, SANS Institute hereby grants User a personal, non-exclusive license to use the Courseware subject to the terms of this agreement. Courseware includes all printed materials, including course books and lab workbooks, as well as any digital or other media, virtual machines, and/or data sets distributed by SANS Institute to User for use in the SANS class associated with the Courseware. User agrees that the CLA is the complete and exclusive statement of agreement between SANS Institute and you and that this CLA supersedes any oral or written proposal, agreement or other communication relating to the subject matter of this CLA.

BY ACCEPTING THIS COURSEWARE, YOU AGREE TO BE BOUND BY THE TERMS OF THIS CLA. BY ACCEPTING THIS SOFTWARE, YOU AGREE THAT ANY BREACH OF THE TERMS OF THIS CLA MAY CAUSE IRREPARABLE HARM AND SIGNIFICANT INJURY TO SANS INSTITUTE, AND THAT SANS INSTITUTE MAY ENFORCE THESE PROVISIONS BY INJUNCTION (WITHOUT THE NECESSITY OF POSTING BOND) SPECIFIC PERFORMANCE, OR OTHER EQUITABLE RELIEF.

If you do not agree, you may return the Courseware to SANS Institute for a full refund, if applicable.

User may not copy, reproduce, re-publish, distribute, display, modify or create derivative works based upon all or any portion of the Courseware, in any medium whether printed, electronic or otherwise, for any purpose, without the express prior written consent of SANS Institute. Additionally, User may not sell, rent, lease, trade, or otherwise transfer the Courseware in any way, shape, or form without the express written consent of SANS Institute.

If any provision of this CLA is declared unenforceable in any jurisdiction, then such provision shall be deemed to be severable from this CLA and shall not affect the remainder thereof. An amendment or addendum to this CLA may accompany this Courseware.

SANS acknowledges that any and all software and/or tools, graphics, images, tables, charts or graphs presented in this Courseware are the sole property of their respective trademark/registered/copyright owners, including:

AirDrop, AirPort, AirPort Time Capsule, Apple, Apple Remote Desktop, Apple TV, App Nap, Back to My Mac, Boot Camp, Cocoa, FaceTime, FileVault, Finder, FireWire, FireWire logo, iCal, iChat, iLife, iMac, iMessage, iPad, iPad Air, iPad Mini, iPhone, iPhoto, iPod, iPod classic, iPod shuffle, iPod nano, iPod touch, iTunes, iTunes logo, iWork, Keychain, Keynote, Mac, Mac Logo, MacBook, MacBook Air, MacBook Pro, Macintosh, Mac OS, Mac Pro, Numbers, OS X, Pages, Passbook, Retina, Safari, Siri, Spaces, Spotlight, There’s an app for that, Time Capsule, Time Machine, Touch ID, Xcode, Xserve, App Store, and iCloud are registered trademarks of Apple Inc.

PMP and PMBOK are registered marks of PMI.

SOF-ELK® is a registered trademark of Lewes Technology Consulting, LLC. Used with permission.

SIFT® is a registered trademark of Harbingers, LLC. Used with permission.

Governing Law: This Agreement shall be governed by the laws of the State of Maryland, USA.

https://t.me/learningnets

Exercise 0: FOR578 Lab Prep

Objectives

- Register your accounts, set up your VM, and prepare for class

Exercise: Setting Up your Lab—Registering Student Accounts

1. On your host system, navigate to Recorded Future at the following link:
`http://for578.com/recordedfuture`

NOTE for Online Training OnDemand Students: If you are an OnDemand student, you'll want to wait to set this up until you are close to starting lab 3.4 as the account is only valid for 30 days.

1. Enter the password provided. Live students will receive the password from their instructor. For OnDemand students, the password will be located in the My Labs section of your SANS portal. You can get there directly by going to connect.labs.sans.org.
2. Fill in the form—only fields with asterisks are required.
3. Your account will be activated in the next day or two by the Recorded Future staff.
4. The Recorded Future lab is on **Day 3**. Tell your instructor by the afternoon break on **Day 2** if you have not received an email.

2. On your host system, navigate to DomainTools at the following link:
`http://for578.com/domaintools`

1. Fill in the form—only things with asterisks next to them are required.
2. Your instructor will give you the registration code at the beginning of class on Day 1.
    i. For OnDemand students, the password will be located in the My Labs section of your SANS portal. You can get there directly by going to connect.labs.sans.org.
3. Follow any additional instructions from DomainTools and verify you can log in.
4. If you have any issues, please let your instructor know before Day 3.

3. On your host system, navigate to VirusTotal at the following link:
`https://www.virustotal.com/gui/join-us`

1. Fill in the form and register an account.

4. Microsoft Excel is a requirement for this course. Ensure you have a copy.

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets

Installing the FOR578 Linux VM – WINDOWS HOST

Exercise Preparation

1. Have access to BIOS password on Host machine (if applicable) to change h/w virtualization settings (if necessary)

2. Install VMware Workstation or VMware Player
   - A copy of VMware Player is provided in the **Installers** folder on your ISO or USB.
   - You can download a copy of free 30-day evaluation copy of VMware Workstation from https://www.vmware.com/products/workstation-pro/workstation-pro-evaluation.html

3. Install Zip program to unzip your VM. Other tools, like the built-in unzip utility in Windows, has proven to be unreliable on very large files.
   - A copy of the 7zip Installer can be found in the **Installer** folder on your ISO or USB.

Unzipping the FOR578 SIFT Virtual Machine on Windows Host

This section is for people using a Windows computer as their host. If you are using an Apple Mac as your host, please skip ahead to the section on Installing the FOR578 SIFT on a Mac Host.

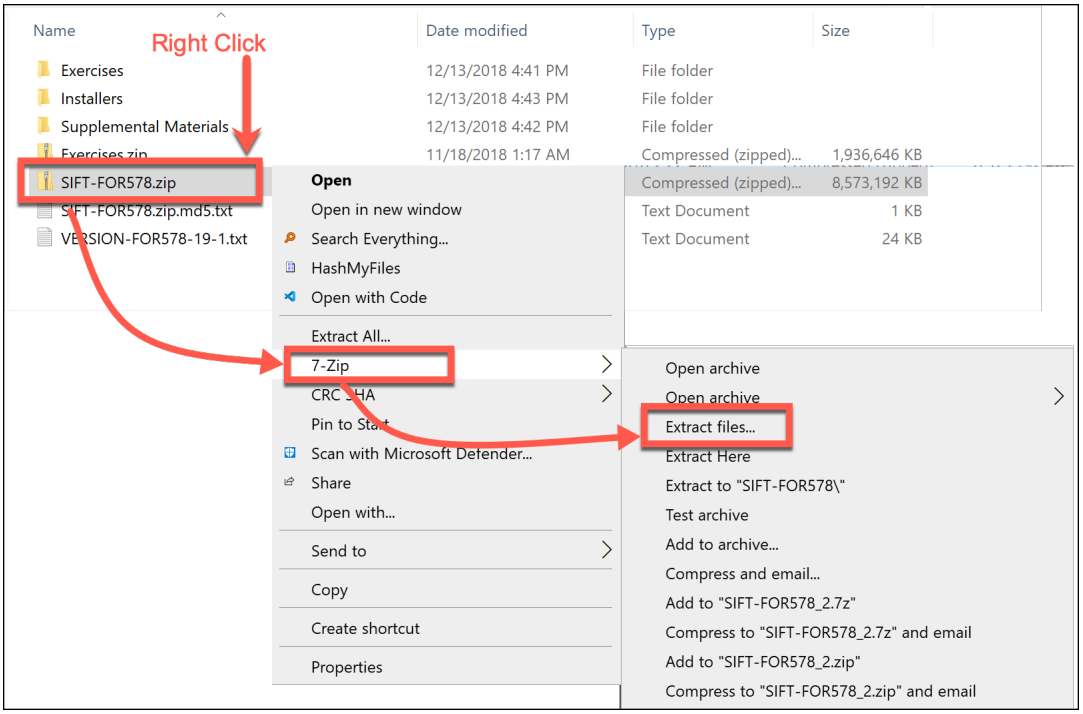
1. Mount the FOR578 ISO or insert the FOR578 USB A into your host system.
2. On the mounted ISO or USB, browse to the root directory.

© 2021 Robert M. Lee and SANS Institute

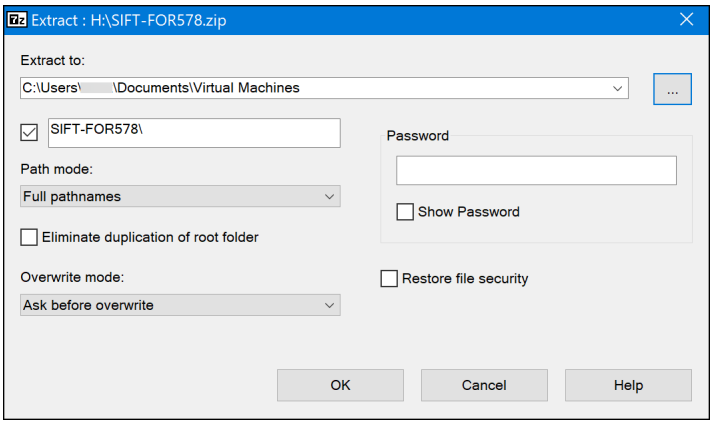
https://t.me/learningnets

3. Unzip the FOR578-SIFT.7z file to a Virtual Machines folder you have created on your host, as shown below:

- Right-click the FOR578-SIFT.7z file to get the 7-Zip options and select **Extract files** as shown below.



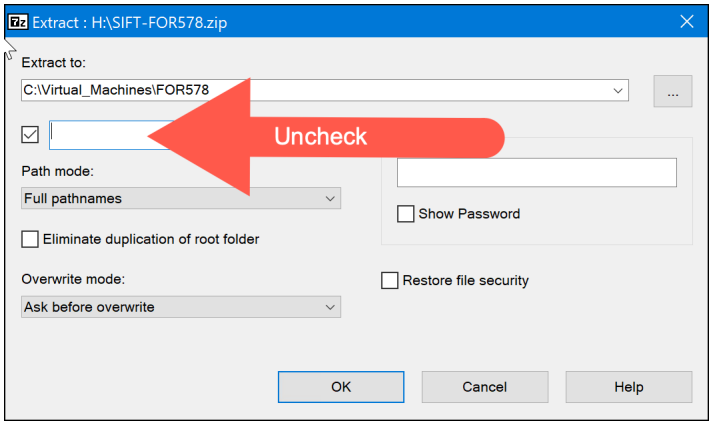
- Select a Folder on your system to "Extract to: " Generally, we recommend a folder where you keep your virtual machines such as **C:\Users\<Username>\Documents\Virtual Machines**. Do not extract to the ISO or the USB drive. It will fail.



© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets

- **Uncheck** the check-box below the "Extract to:" path and click OK.



- After a long extraction process (maybe 20–45 min), you should see a new folder in your selected export folder called **FOR578-SIFT**.

Exercise: Setting Up your Lab—Installing SIFT Workstation on a Windows Host

1. Extract **FOR578-SIFT.7z** to your computer:
    1. Download the course media file from your portal account, or if a USB was received, insert the course USB into your system.
    2. Copy the **FOR578-SIFT.7z** file to a location of your choice on the system.
    3. Extract the **FOR578-SIFT.7z** file to a location of your choice on the system.

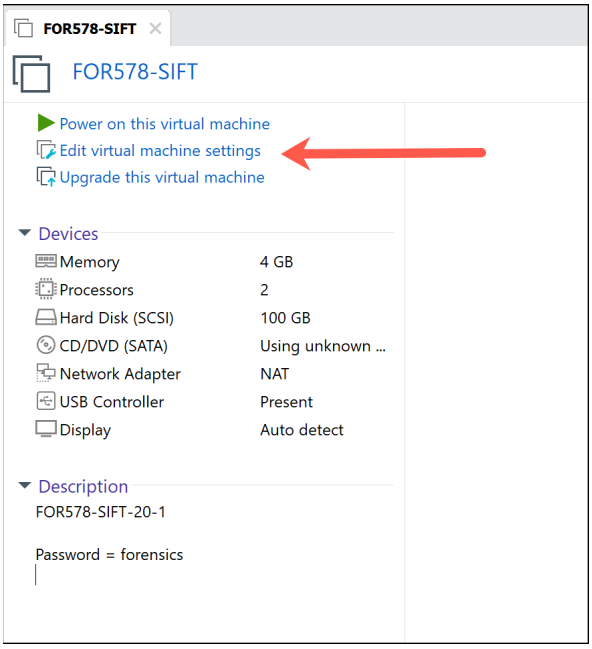
2. Launch VMWare Player or Workstation (if you use a Mac, you will need to use Fusion that is discussed in the next section):
    1. Choose **File -> Open**.
    2. Then navigate to **\Path-To\Virtual Machines\FOR578-SIFT\FOR578-SIFT.vmx** and select and open the file.

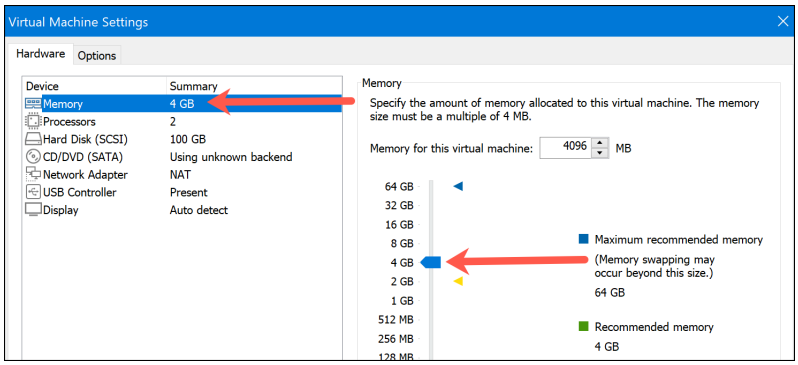
3. Next, adjust the memory by selecting **Edit virtual machine settings**. You can adjust the memory setting up or down. One of the most important settings is the VM's memory (RAM) setting. You will want to provide the FOR578 SIFT at least 3 GB of RAM if your host can support that. It is not recommended to provide your VM(s) more than one half (1/2) of the total amount of memory that your host has. If you are running more than one VM at a time, you will need to allocate that 1/2 of your host's memory across all the VMs. The FOR578-SIFT doesn't need a huge amount of memory to run well. In most situations, 4 GB memory is more than adequate.

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets

4. Adjust the memory by selecting **Edit virtual machine settings**. You can adjust the memory setting up or down. You can type in the amount of memory that you want to allocate to the FOR578 SIFT or use the "slider" to make those adjustment. The values are entered in MB. 4096 MB = 4 GB (4 x 1024).

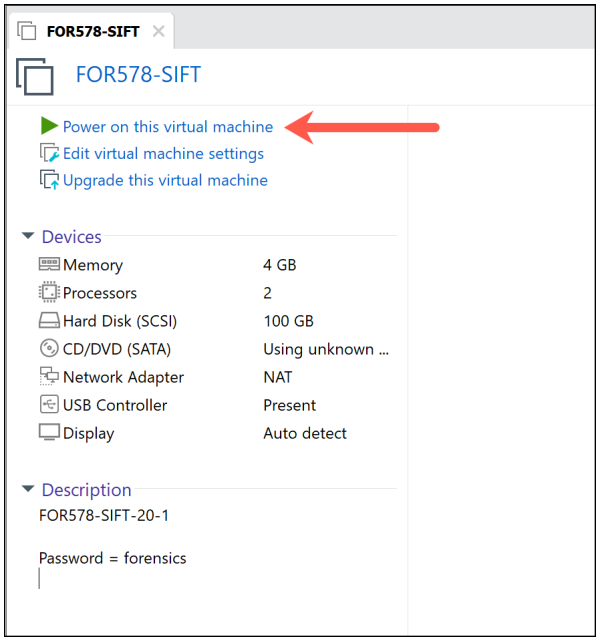




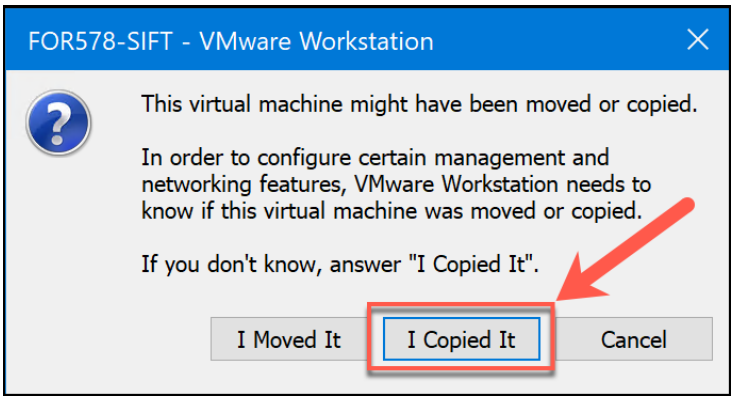
5. Start your SIFT VMware VM in VMware by selecting **Power on this virtual machine**.

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets



6. Select **I copied it** if prompted with the option.

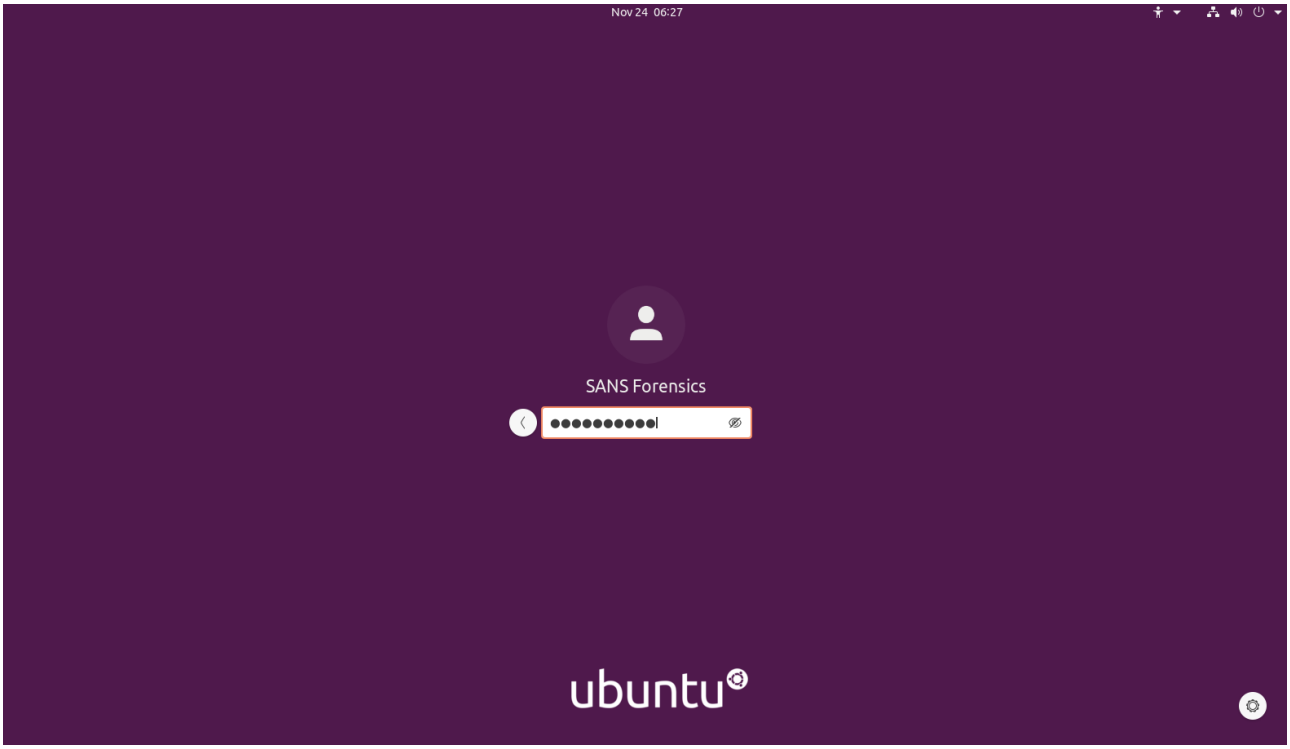


7. Log in to the VMWare machine with the following credentials:

- Login: **`SANS Forensics`**
- Password: **`forensics`**

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets



8. You have successfully prepared for the FOR578: Cyber Threat Intelligence course!

Installing the FOR578 Linux VM – MAC HOST

This section is for people using an Apple Mac computer as their host. If you are using an Windows computer as your host, please go back to the setup section above for Windows Hosts.

1. Mount the FOR578 ISO or insert the FOR578 USB A into your host system.
2. On the mounted ISO or USB, browse to the root directory.

Exercise Preparation

1. Have access to BIOS password on Host machine (if applicable) to change h/w virtualization settings (if necessary)

2. Install Fusion or Fusion Player
   - A copy of Fusion Player in provided in the **Installers** folder on your ISO or USB. You will need to register to get a free license key for Fusion Player.
   - Go to https://my.vmware.com/web/vmware/evalcenter?p=fusion-player-personal to register.

3. Install Keka to unzip your VM. Keka is a zip program for the Mac and handles 7zip archives.
   - A copy of the Keka Installer can be found in the **Installers** folder on your ISO or USB.

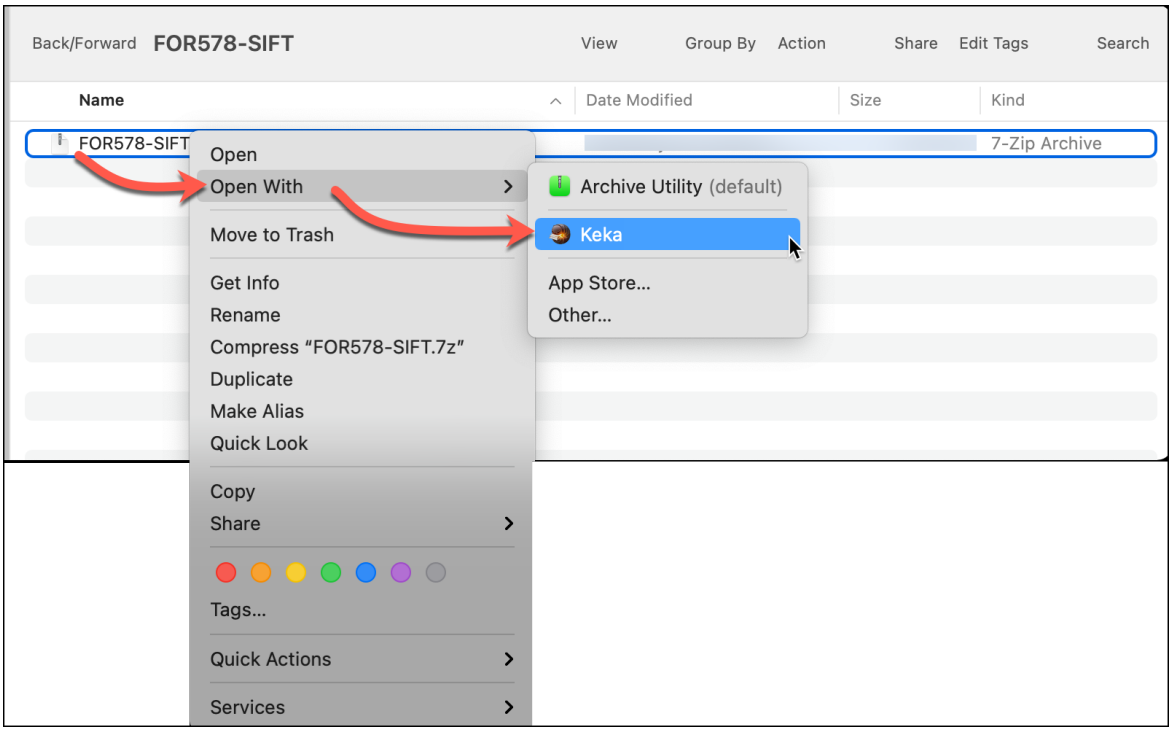
© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets

Unzipping the FOR578 SIFT Virtual Machine on Apple Mac Host

This section is for people using a Mac computer as their host. If you are using an Windows, please go back to the previous section for Windows hosts.

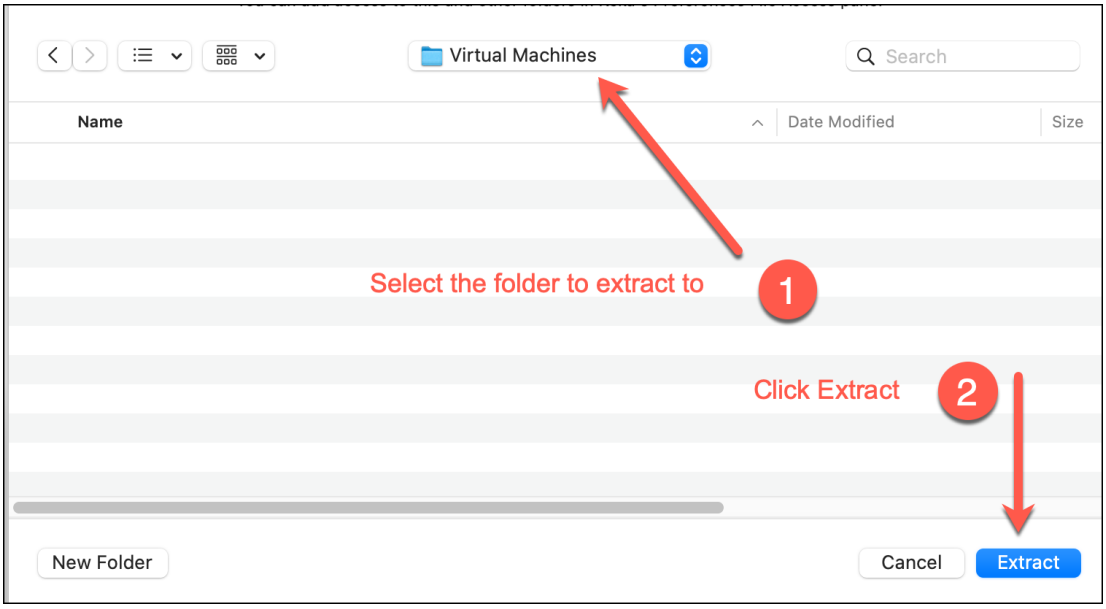
1. Mount the FOR578 ISO or insert the FOR578 USB A into your host system. (you may have already completed this step and step 2 below)
2. On the mounted ISO or USB, browse to the root directory.
3. Unzip the FOR578-SIFT.7z file using **Keka** to a Virtual Machines folder you have created on your Mac.
4. Right-click the FOR578-SIFT.7z file to get the **Open With** option and then select **Keka** as shown below.



5. Select the folder to which you wish to extract the VM and then click **Extract**.

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets



- Keka will display a progress bar showing the status on the unzipping process. After a long extraction process (maybe 20–45 min.), you should see a new folder in your selected export folder called **FOR578-SIFT**.



Configuring and Starting the FOR578 SIFT Virtual Machine on Apple Mac Host

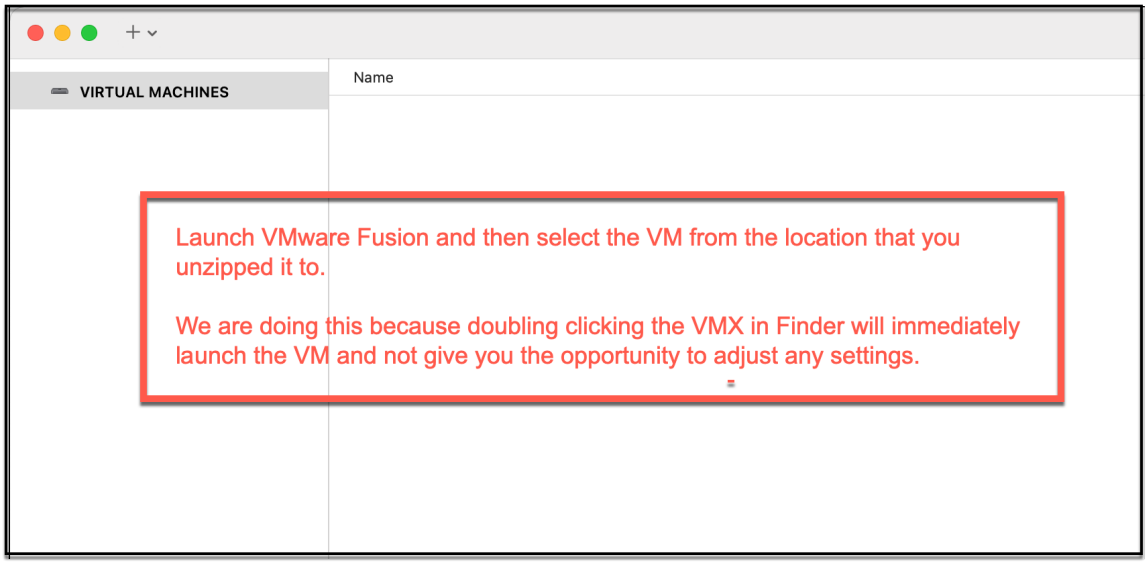
VMware Fusion behaves differently than the Workstation or Player on Windows hosts when the VM's VMX files are double-clicked. Because of this, we suggest a different first-time startup method.

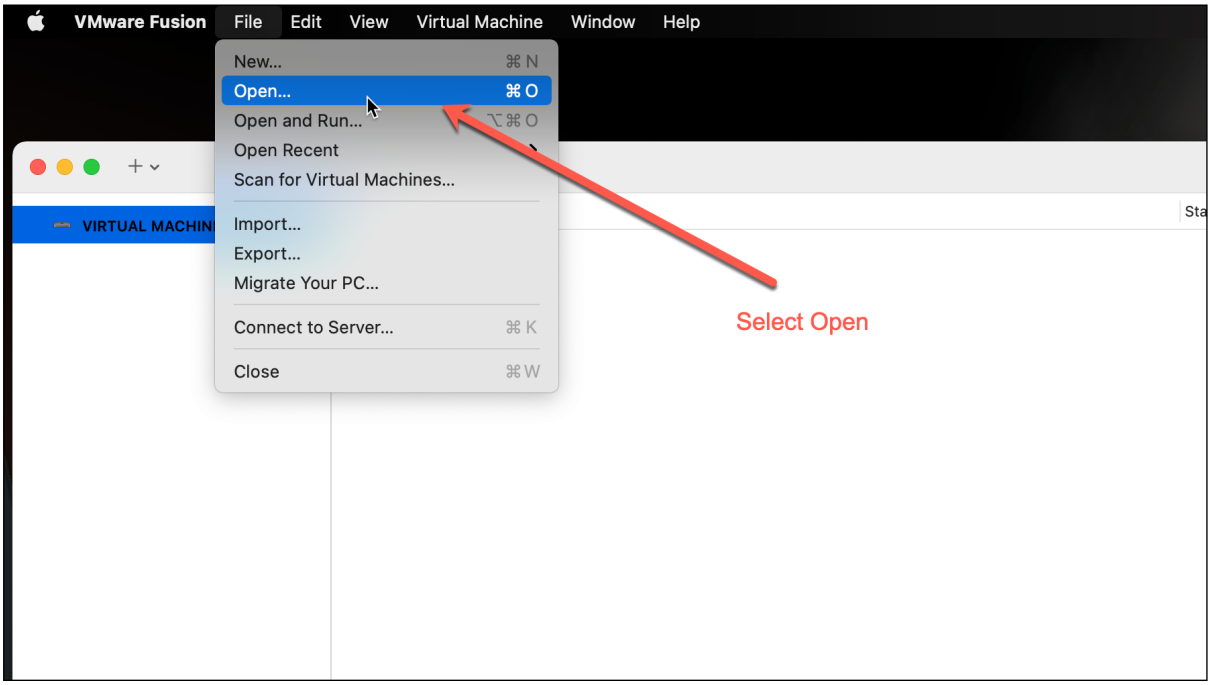
The first time that you start the FOR578 SIFT, you will want to start VMware Fusion first and then launch the FOR578 SIFT from within Fusion rather than double-clicking the VM file in Finder. We suggest this because double-clicking the VM in Finder will immediately launch the VM and not give you an opportunity to adjust any VM settings. After this first time, you might find that double-clicking the VM file is a faster way to launch the VM.

1. Launch VMware Fusion. You can select it from the Applications folder in Finder. You may have a different way to launch applications on your Mac, which is perfectly acceptable.
2. From the VMware Fusion menu at the top of the screen, select **File** and then **Open** as shown below.

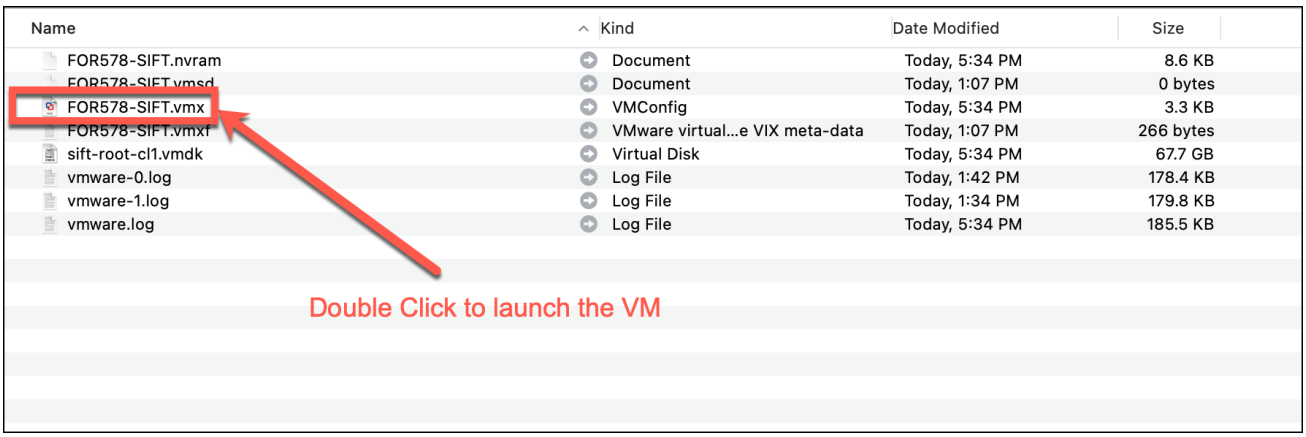
© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets





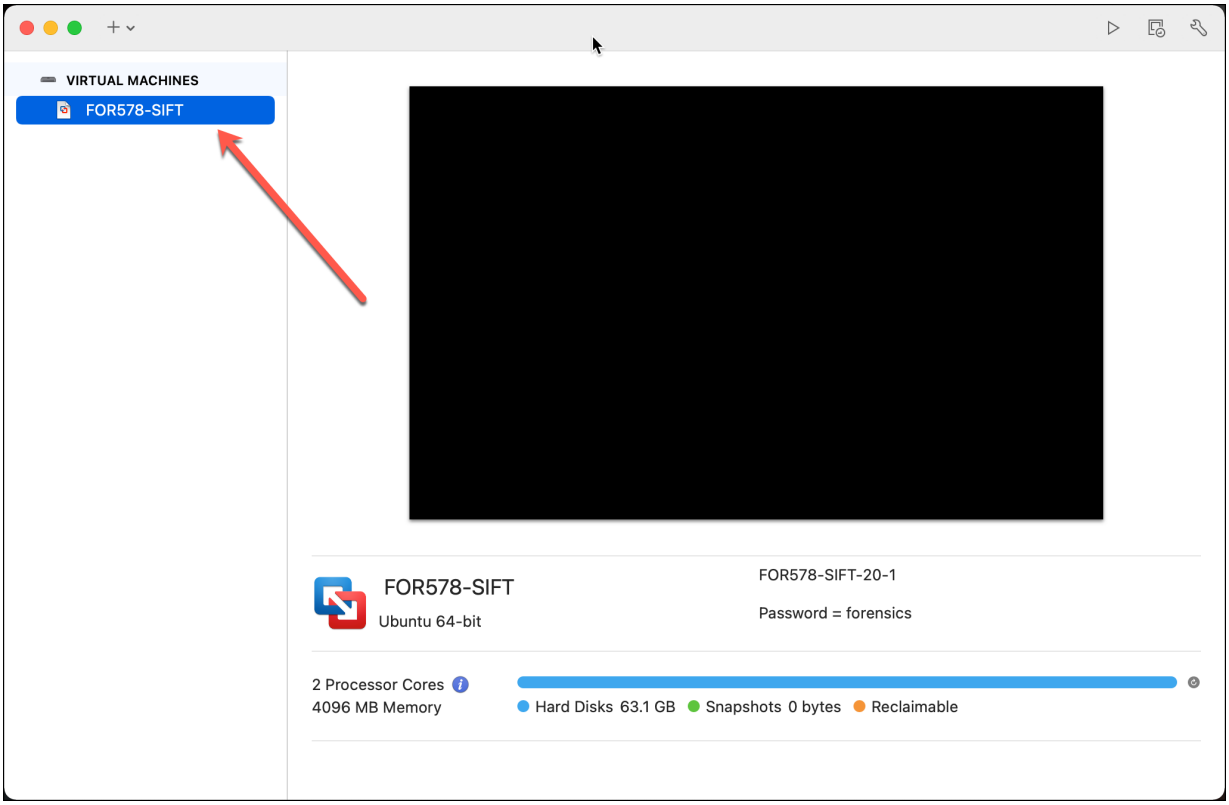
3. From the folder that you unzipped the FOR578 SIFT into, double-click the **FOR578-SIFT.vmx** file.



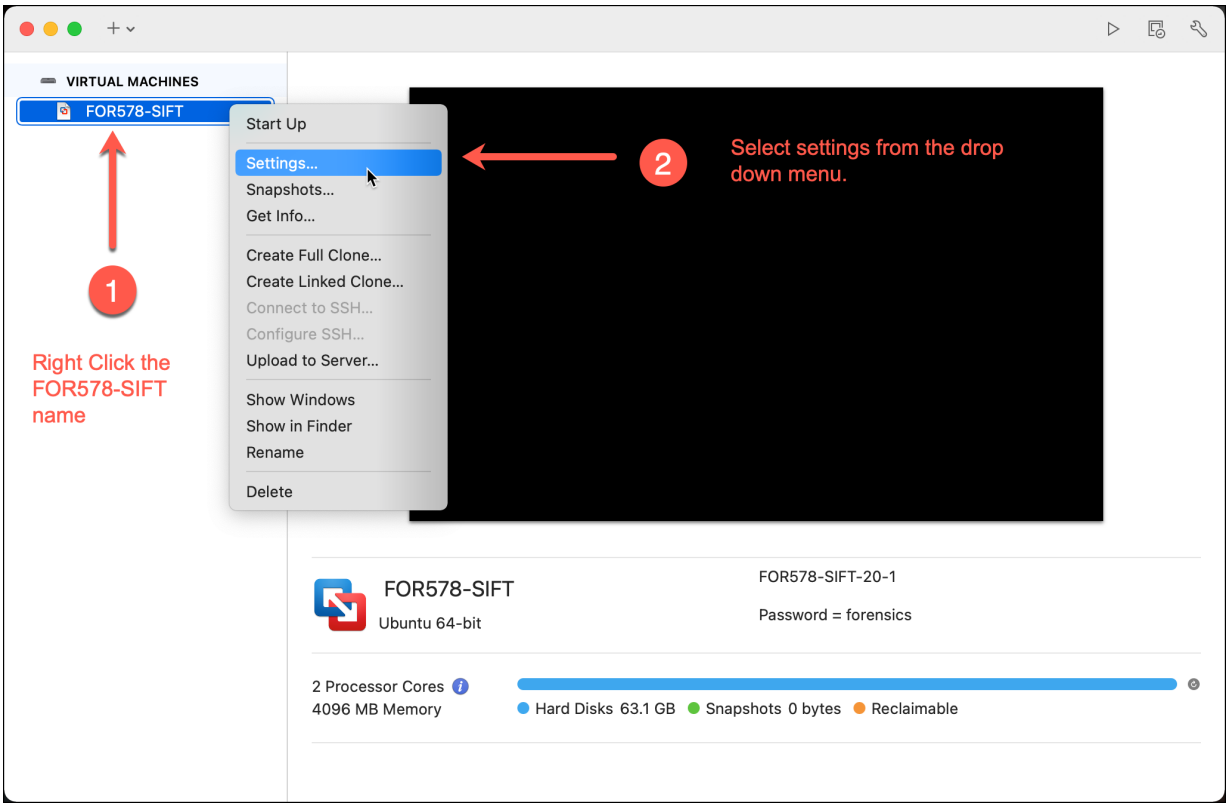
© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets

4. The VM will then be displayed in the left-hand column as shown below.



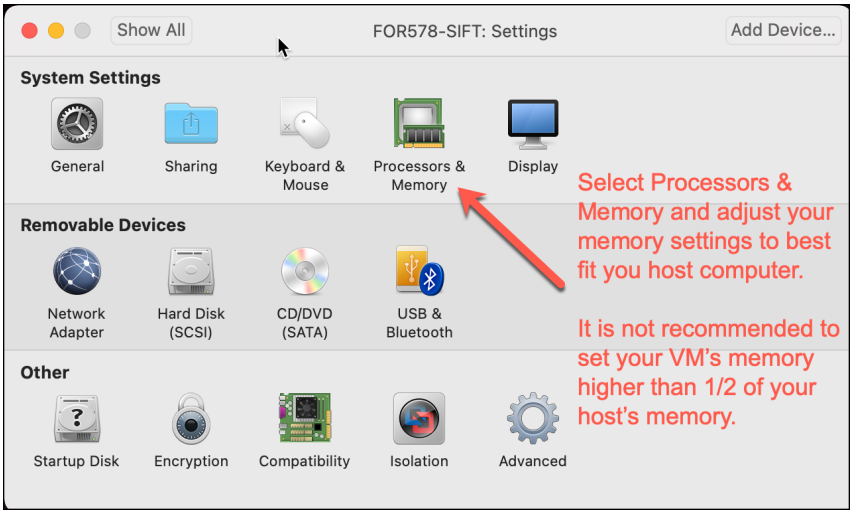
5. Right-click the FOR578-SIFT name in the left column and select **Settings**.



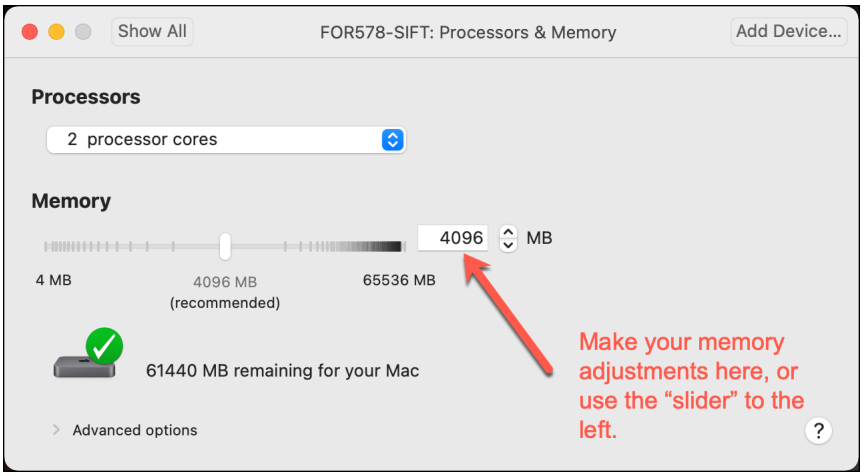
© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets

6. The VM Setting Screen will be displayed. The most important setting is the VM's memory (RAM) setting. You will want to provide the FOR578 SIFT at least 3 GB of RAM if your host can support that. It is not recommended to provide your VM(s) more than one half (1/2) of the total amount of memory that you host has. If you are running more than one VM at a time, you will need to allocate that 1/2 of your host's memory across all the VMs. The FOR578-SIFT doesn't need a huge amount of memory to run well. In most situations, 4 GB memory is more than adequate.



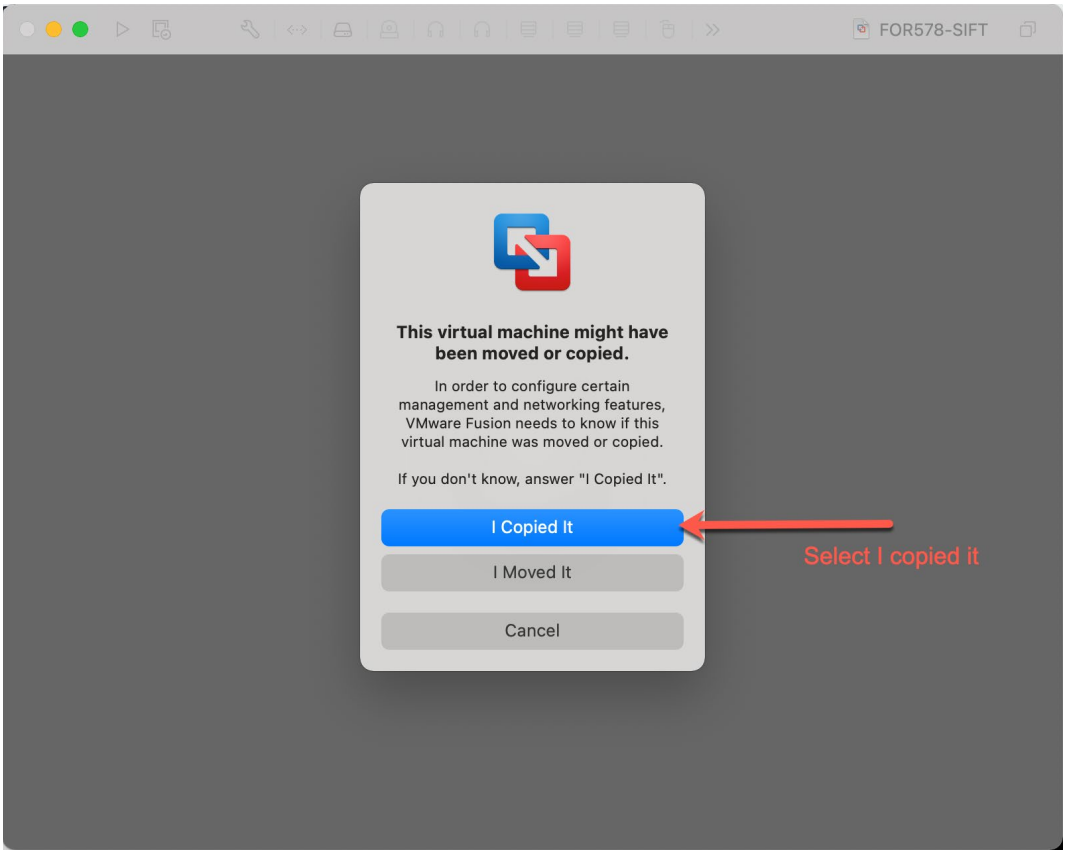
7. Adjust the memory by selecting **Edit virtual machine settings**. You can adjust the memory setting up or down. You can type in the amount of memory that you want to allocate to the FOR578 SIFT or use the "slider" to make those adjustments. The values are entered in MB. 4096 MB = 4 GB (4 x 1024).



8. You can now launch the VM by double-clicking the FOR578-SIFT name on the left side of the screen. The first time that you launch the VM, you will be asked if you copied or moved the VM. **Select I copied it**.

© 2021 Robert M. Lee and SANS Institute

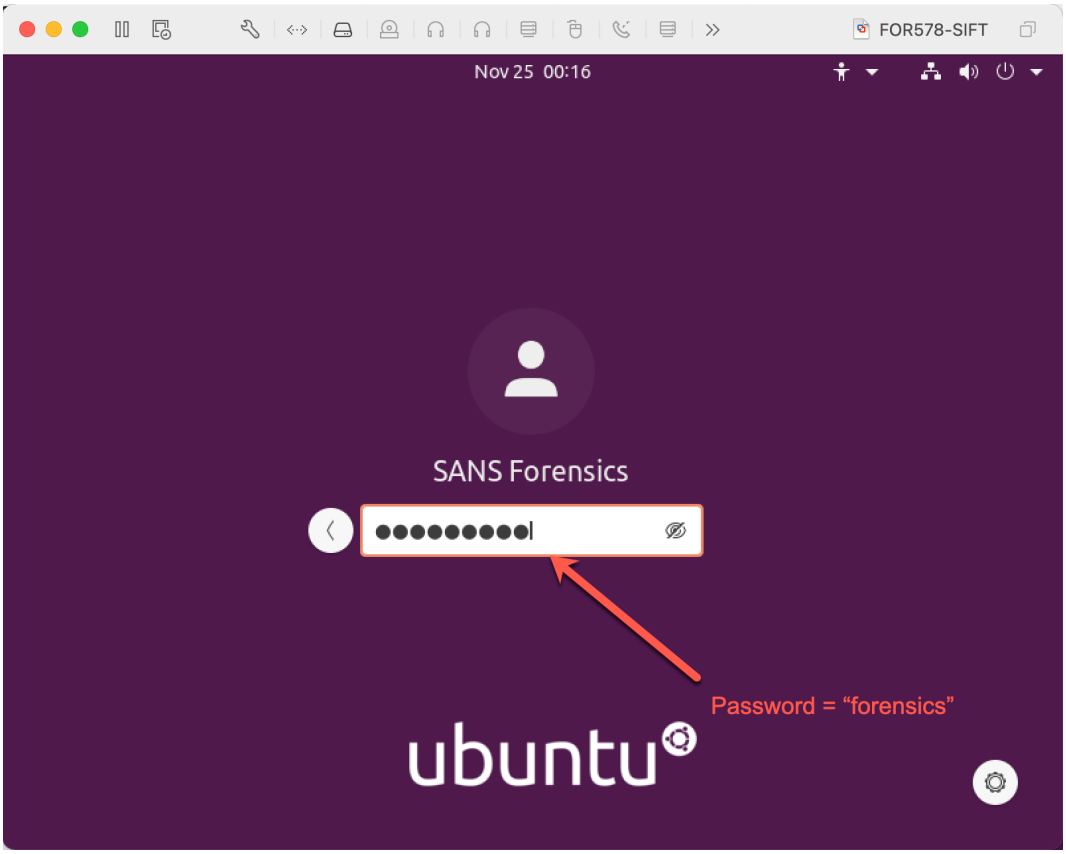
https://t.me/learningnets



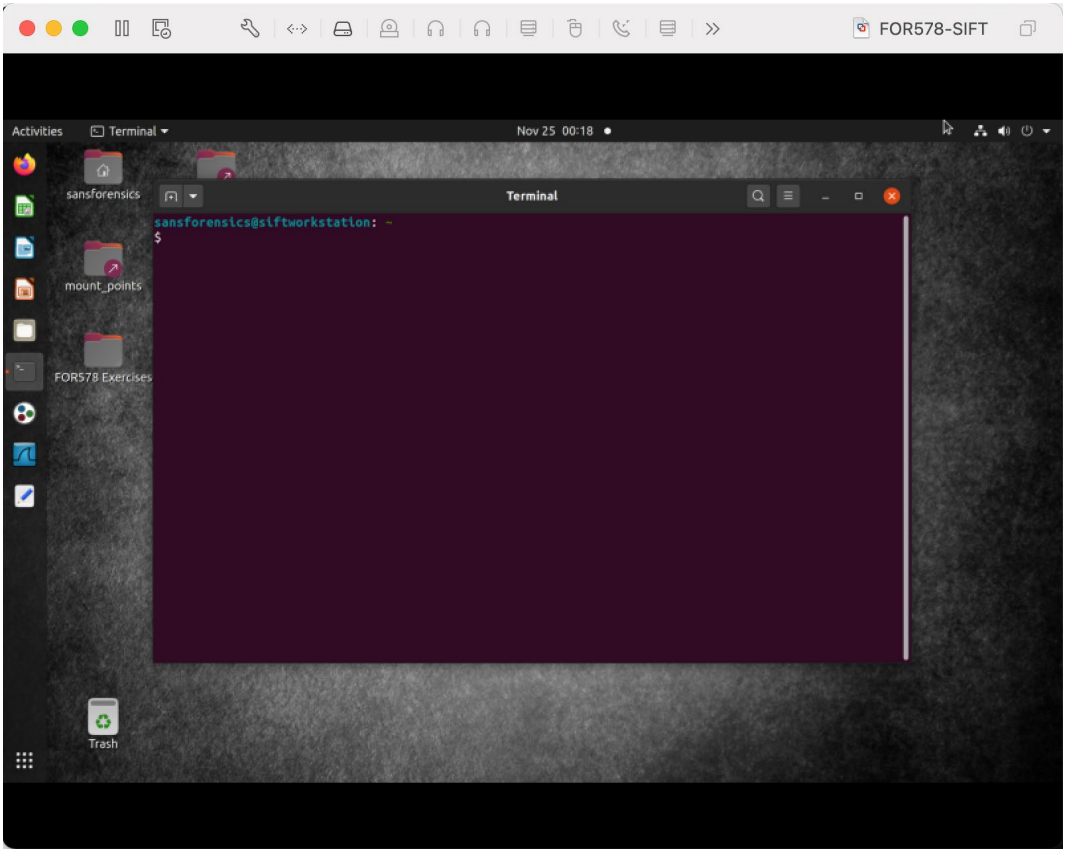
9. The FOR578 SIFT will begin to start up. Once it has launched, you will be presented with a login screen. Click the SANS Forensics user name and then enter "**forensics"** as the password.

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets



10. After entering the correct password, you will see the FOR578 SIFT Desktop and you are ready to work on your exercises. Congrats!



© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets

Exercise 1.1: Structured Analytic Techniques

Objectives

- Learn and leverage structured analytic techniques to facilitate decision-making

Structured Analytic Techniques Overview

In this lab, you will use two different types of structured analytic techniques (SATs). SATs are designed to help analysts perform analysis while abstracting themselves as much as possible from other influences such as bias. SATs can be leveraged for different types of analysis, including data organization, hypothesis generation, decision support, and conflict management. The SATs in this lab you will utilize are focused on data organization: They are Simple Brainstorming and Sorting.

***Simple Brainstorming** is most often used at the beginning of a project to identify a list of relevant variables, key drivers, sources of information, possible outcomes or solutions, and other information that can get an analyst started thinking critically about a topic. The goal of brainstorming is to generate as many ideas as possible without beginning to apply analytic judgment during the process to avoid biases such as anchoring bias.*

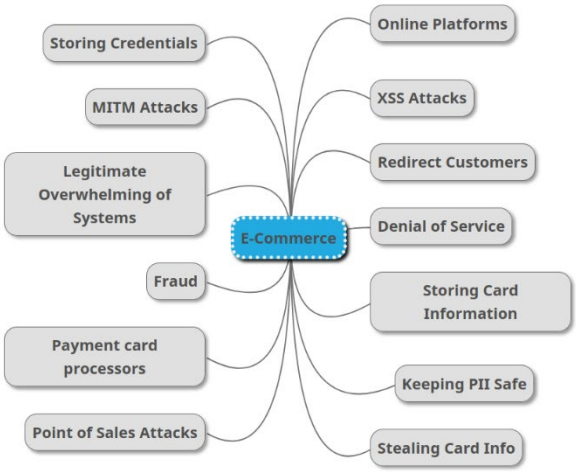
Example: Sarah has been asked by her management to assess how a move into a new market sector (e-commerce) would impact the company's security posture. Sarah is relatively familiar with threats to e-commerce but wants to compile an expanded list of keywords and variables so that she can do more research into specific threats that have faced that sector recently. She decides to use simple brainstorming to find out where she should direct her research.

Sarah starts by taking three minutes to write (or type) every word she can think of related to e-commerce and its related security considerations. To do this, Sarah draws from her own experience of e-commerce-specific security considerations and what she has learned previously about this sector by reviewing threat reports on tactics, techniques, and procedures commonly used to target e-commerce.

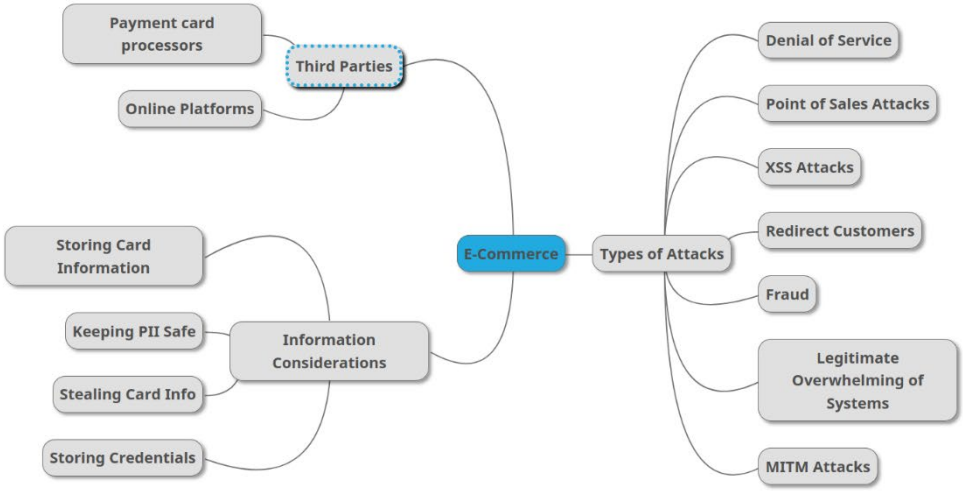
In this example, Sarah uses the free online mind mapping tool, MindMup.

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets



She then looks at the words she has written down and begins to cluster them by topic. She notices that she has identified classes of attacks, information that can be targeted by attackers, and third-party services that support e-commerce (which could also be targeted). She reorganizes her notes to associate the topics with the key variables. These will be the key variables (aka categories) Sarah will use as she moves into the research phase of her analysis.



Sarah also identifies that while she was able to think of several different types or classes of attacks, she was not as familiar with aspects of e-commerce, such as how third-party providers support e-commerce. She will need to focus on understanding that area more before she provides her assessment. This is also one of the reasons that group brainstorming is so effective—it brings in many different views, perspectives, and experiences to identify the most complete list of variables and group them appropriately.

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets

Sorting *is a way to structure and visualize variables of the topic you are looking into. It is a good technique for organizing large bodies of data to generate insights. Sorting is most often done with a spreadsheet or database program so that data can be sorted or organized in different ways. Sorting follows the general steps listed below:*

Step 1: Identify the variables or categories of a topic using a brainstorming method.
Step 2: Make these categories column headers in a spreadsheet.
Step 3: List facts, pieces of information, or hypotheses related to the categories in the appropriate column.
Step 4: Review the sorted data for trends or anomalies and list them out as either findings or areas to look into more.
Step 5: Review the findings, trends, and anomalies with others in your group; list and explain any variables you excluded or trends you discounted.

After the sorting process, you may either have found what you were looking for in the data, or you may have identified additional analysis that is needed. Either way, it is helpful to have a structured method for handling data and explaining your findings.

Example: Sarah has done additional research on threats related to e-commerce and has decided to sort her data to help her pull out trends that may be valuable to her CISO. She uses her favorite analytic tool, Excel. She uses the categories she identified during her brainstorming—type of attack, information impacted, and platform or third-party tool—and lists out these variables from attacks against e-commerce for the past several years. Since she is working with data across an extended time period, she adds the additional variable "year".

	A	B	C	D
1	**Attack Type**	**Platform/Third-Party**	**Information Targeted**	**Year**
2	XSS	e-Commerce website	Credit Card Information	2015
3	XSS	popular payment plugins	Credit Card Information	2016
4	SQL Injection	e-Commerce website	Credit Card Information	2019
5	SQL Injection	e-Commerce website	PayPal Informaiton	2019
6	SQL Injection	e-Commerce website	Customer Personal Information	2019
7	Unk	e-Commerce website	Customer Personal Information	2019
8	Unk	e-Commerce Mobile App	Customer Personal Information	2019
9	Phishing	Customers	Financial Information	2016
10	Phishing	Customers	Financial Information	2019
11	Phishing	Customers	Financial Information	2018
12	Phishing	e-Commerce Support Team	Database Access	2018
13	Phishing	e-Commerce Support Team	Database Access	2020

Sarah then sorts the data by platform or third-party tool, and observes the fact that in the majority of reported attacks, the business's website, mobile app, or even the support team was the target, although there are instances of third-party tools targeted as well, and the majority of those attacks occur in recent years. This is an insight that can help Sarah make recommendations about the need for robust security of all e-commerce

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets

related assets, along with specific user awareness training for support personnel once the company decides to expand into this new area.

Attack Type	Platform/Third-Party	Information Targeted	Year
Phishing	Customers	Financial Information	2016
Phishing	Customers	Financial Information	2018
Phishing	Customers	Financial Information	2019
Unk	e-Commerce Mobile App	Customer Personal Information	2019
Phishing	e-Commerce Support Team	Database Access	2018
Phishing	e-Commerce Support Team	Database Access	2020
XSS	e-Commerce website	Credit Card Information	2015
SQL Injection	e-Commerce website	Credit Card Information	2019
SQL Injection	e-Commerce website	PayPal Informaiton	2019
SQL Injection	e-Commerce website	Customer Personal Information	2019
Unk	e-Commerce website	Customer Personal Information	2019
XSS	popular payment plugins	Credit Card Information	2016

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets

Exercise Prep

You can use the online mind-mapping tool MindMup (https://www.mindmup.com/), or another tool or method of your choice for brainstorming, and Excel or another spreadsheet tool for sorting.

Supplementary information on Ransomware attacks can be found in the Ex1.1 Folder on your SIFT VM.

Exercise: Questions

Scenario 1: You are a threat intelligence analyst at a healthcare organization and your Chief Information Security Officer is concerned about Ransomware. They specifically want to know how serious of a threat it is to your organization and what should be done to prevent and prepare to respond to a ransomware attack.

Use Simple Brainstorming to identify relevant variables for research into ransomware attacks on the healthcare sector.

1. List the variables that will be useful to future research.

_____

Scenario 2: The CISO would also like to evaluate the success of anti-phishing efforts, including upgrading email filtering and conducting phishing-awareness training for staff. The SOC has put together a sample of phishing incidents, where Success means the email resulted in an incident, Reported means the email was reported to the SOC, and Blocked means the phishing email was quarantined by the new filter.

Use Sorting to identify relevant trends in phishing emails sent to the company.

2. Which department receives the most phishing emails?

_____

3. What day of the week and time are the most phishing emails sent?

_____

4. Do any departments likely need additional training on phishing awareness?

_____

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets

Exercise: Questions with Step-by-Step

Please note: The solutions in the Step-by-Step guide are examples. Your solutions will vary and that is to be expected. The goal of the lab is to have you think through the situations presented and use two structured approaches to weigh decisions and likely outcomes for addressing those situations.

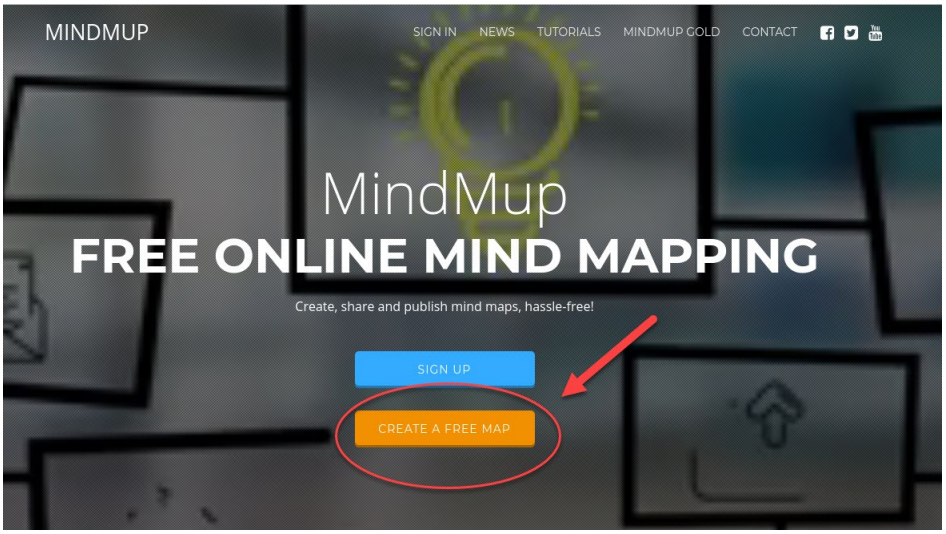
Use Simple Brainstorming to identify relevant variables for research.

1. List the variables that will be useful to future research (*these are just examples; your variables may be different).*

Initial Access Vectors, Preventions and Mitigation, Actions after compromise, Targets, Ransomware as a Service.

Read through the Ransomware reports in the Ex1.1 Folder.

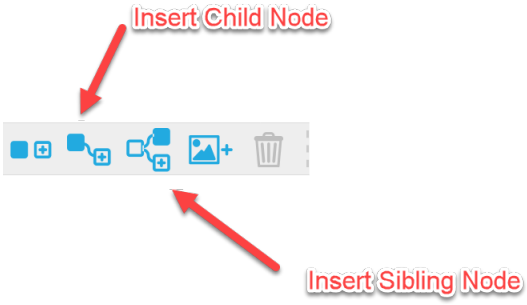
If you would like to use the online mind-mapping tool from the examples, go to https://www.mindmup.com/ and select "Create a free map".



Once you have the mind map open, double-click the primary node and change the default text to say "Ransomware". To add a new node, select the "insert child node" icon from the menu on the top. To add additional nodes without going back to the parent node, select the "insert sibling node" icon.

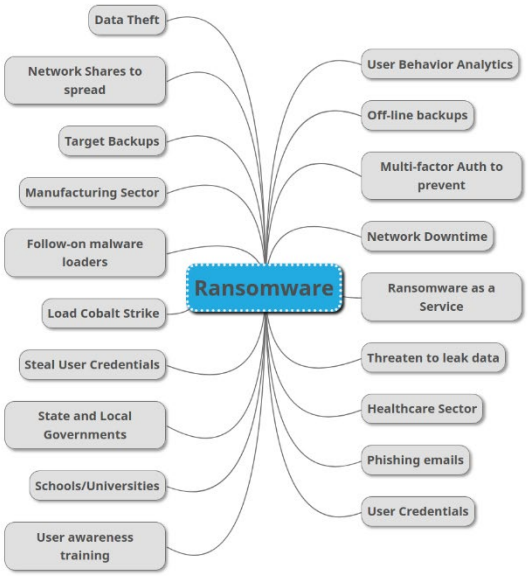
© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets



Take two or three minutes to brainstorm all the topics that would be relevant to your organization preparing for and responding to ransomware. If you need more background information before undertaking this step, make sure to read through the Ransomware articles in the Ex1.1 Folder.

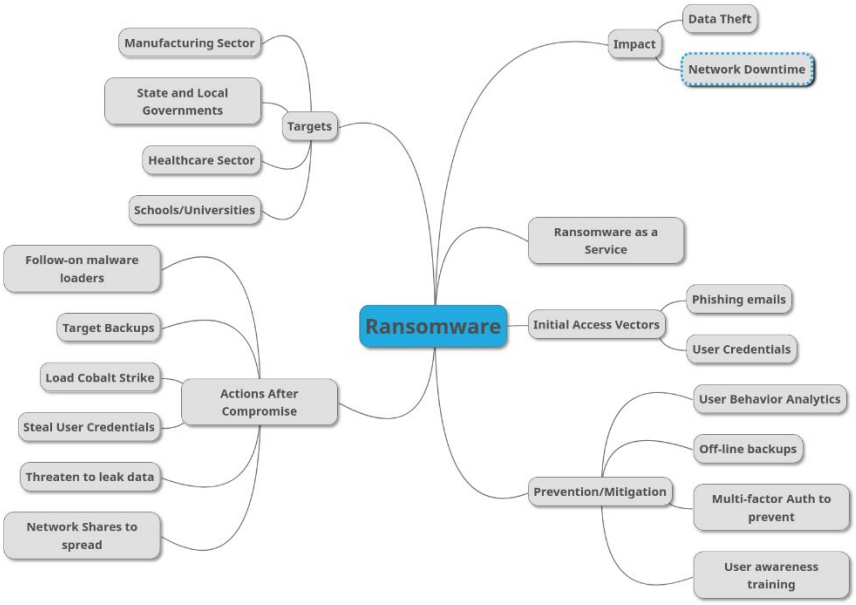
After the first round of brainstorming, you should have a map that looks something like this:



Review the nodes on the map and look for patterns. In the example above, the nodes can be clustered into initial access vectors, actions taken after compromise, targets, impact, and mitigation/remediation steps. One of the nodes, Ransomware as a Service, does not fit into any of the categories; however, it is fine to leave it as a standalone node, as it may be significant in future research or as a prompt to address trends in the ransomware industry. The revised map will look something like this:

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets



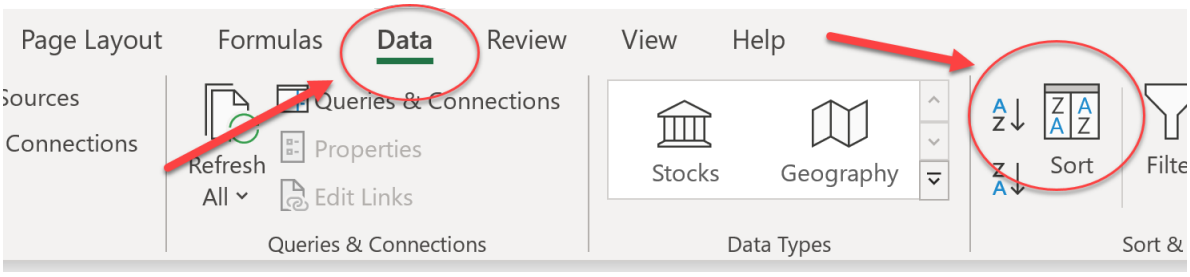
Use Sorting to identify relevant trends in phishing emails sent to the company.

Using Excel or another spreadsheet tool, open the file "phishingreport.csv" in the Ex1.1 folder.

2. Which department receives the most phishing emails?

Patient Accounts

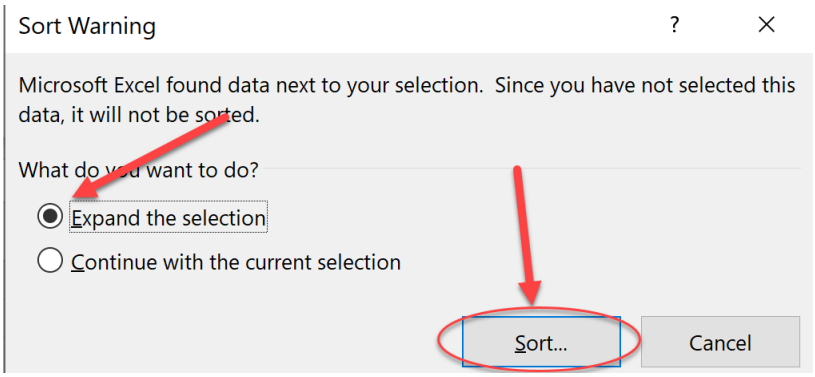
Select "Data" from the bar at the top, and then select "Sort"



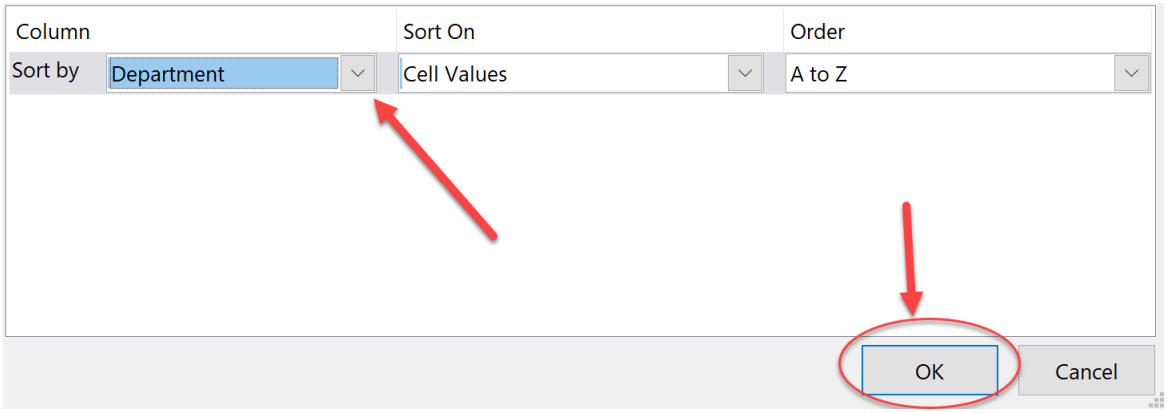
Excel will prompt you to expand the selection, so that data will stay aligned to its row after the columns are sorted. Select "Expand the Selection" and click "Sort".

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets



You will then be prompted to select which column to sort. Since we are trying to identify the department with the most phishing activity, select Sort by: "Department" and then select "Okay".



This will list the departments in alphabetical order. After reviewing the results, you will see that Patient Accounts had the most activity with 15 phishing emails received.

© 2021 Robert M. Lee and SANS Institute

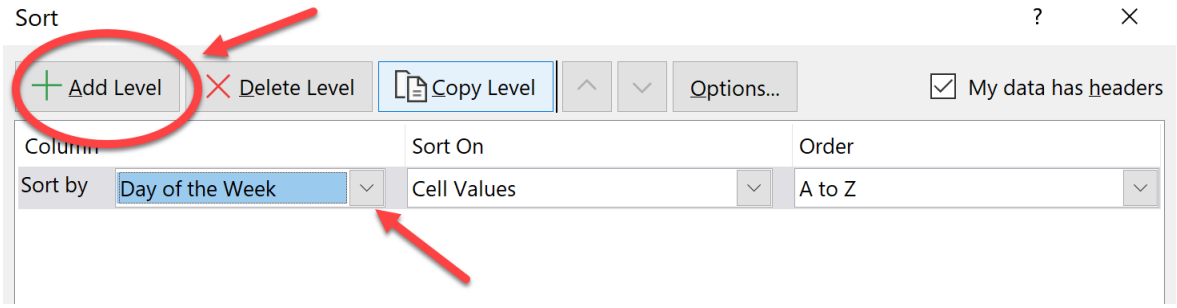
https://t.me/learningnets

monday	3:59	Occupational Therapy	Reported
monday	2:36	Occupational Therapy	Reported
saturday	16:42	Occupational Therapy	Reported
monday	3:33	Occupational Therapy	Reported
saturday	4:36	Occupational Therapy	Reported
thursday	16:57	Patient Accounts	Blocked
thursday	16:5	Patient Accounts	Blocked
thursday	5:07	Patient Accounts	Success
thursday	5:07	Patient Accounts	Success
monday	16:57	Patient Accounts	Success
tuesday	16:37	Patient Accounts	Success
tuesday	16:33	Patient Accounts	Success
sunday	7:52	Patient Accounts	Reported
sunday	8:02	Patient Accounts	Reported
monday	1:13	Patient Accounts	Success
monday	1:11	Patient Accounts	Success
monday	15:59	Patient Accounts	Success
tuesday	16:40	Patient Accounts	Success
tuesday	16:33	Patient Accounts	Success
tuesday	16:3	Patient Accounts	Success

3. What day of the week are the most phishing emails received?

Mondays, with clusters of activity around lunch on Fridays, and at the end of the business day on Tuesdays and Thursday

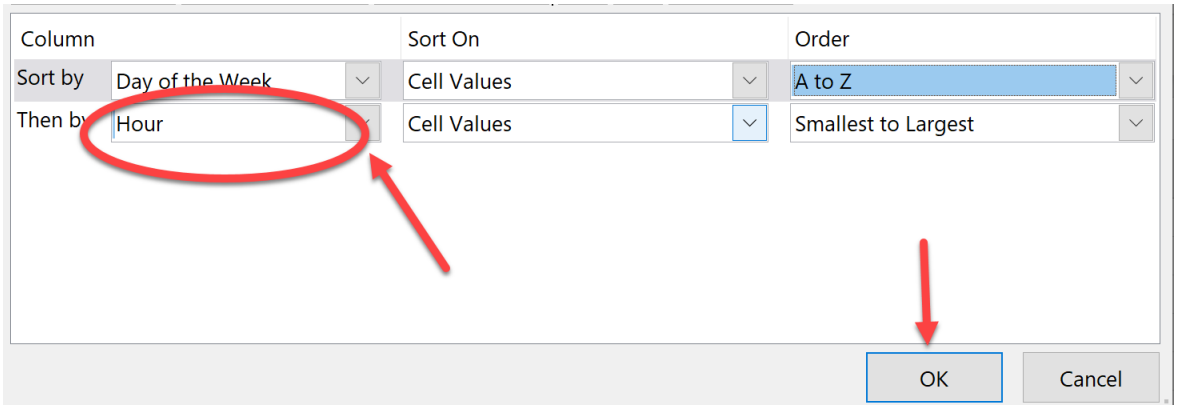
Hit sort again and this time sort by Day of the Week. To also sort the time of day within each day, select "Add Level".



In the second sort by drop-down select "Time" and hit "Sort"

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets



Now that the data is sorted by Day and then Time, look for patterns. Monday has the most phishing activity total, and it is divided into two groups—early morning and late afternoon. Friday has a cluster of phishing emails received around lunchtime. If you continue down and review the data, you will also see clusters of activity at the end of the day on Tuesday and Thursday.

Day of the Week	Hour	Department	Delivery Status
friday	1:31	Medical Records	Success
friday	1:40	Medical Records	Success
friday	12:25	Medical Records	Blocked
friday	12:28	Medical Records	Blocked
friday	12:31	Medical Records	Reported
friday	12:40	Medical Records	Blocked
friday	12:40	Medical Records	Blocked
friday	12:40	Medical Records	Blocked
monday	1:11	Health & Safety	Success
monday	1:11	Patient Accounts	Success
monday	1:13	Patient Accounts	Success
monday	2:36	Occupational Therapy	Reported
monday	2:37	Occupational Therapy	Reported
monday	3:33	Occupational Therapy	Reported
monday	3:37	Admissions	Success
monday	3:59	Occupational Therapy	Reported
monday	15:59	Patient Accounts	Success
monday	16:54	Health & Safety	Success
monday	16:54	Health & Safety	Success
monday	16:54	Health & Safety	Success
monday	16:57	Patient Accounts	Success
saturday	4:30	Health & Safety	Success

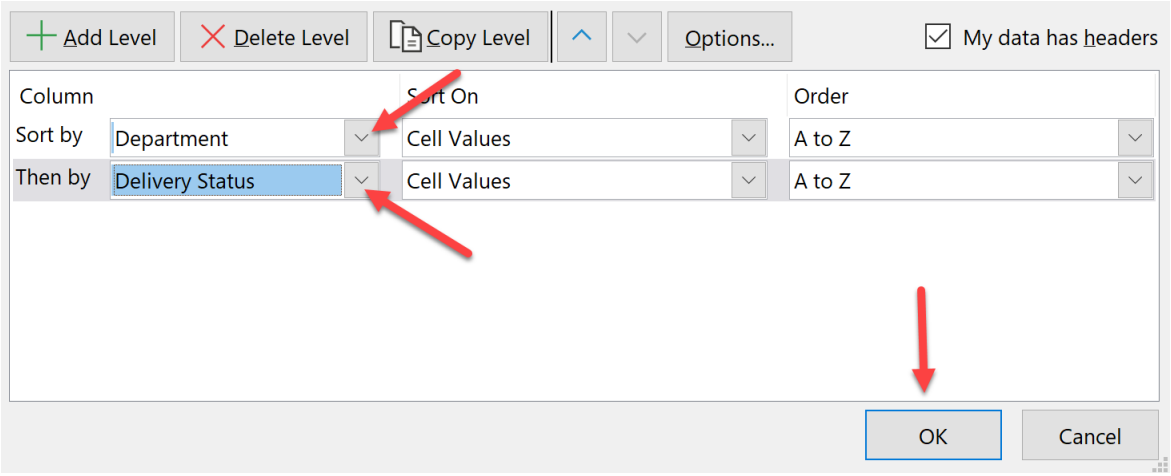
4. Do any departments likely need additional training on phishing awareness?

Health & Safety

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets

We will sort one more time in this exercise. Select Sort and then from the dropdown menus sort first by Department and then by Delivery Status.



From the results, we can see that the Health & Safety department—which receives quite a lot of phishing emails—has not reported a single phishing email. They would be a good candidate for review training.

sunday	8:03	Admissions	Success
thursday	16:57	Health & Safety	Blocked
monday	1:11	Health & Safety	Success
monday	16:54	Health & Safety	Success
monday	16:54	Health & Safety	Success
monday	16:54	Health & Safety	Success
saturday	4:30	Health & Safety	Success
saturday	4:36	Health & Safety	Success
sunday	7:52	Health & Safety	Success
sunday	17:00	Health & Safety	Success
sunday	17:00	Health & Safety	Success
thursday	16:56	Health & Safety	Success
thursday	16:56	Health & Safety	Success
thursday	16:56	Health & Safety	Success
friday	12:25	Medical Records	Blocked

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets

Exercise Key Takeaways

- **We learned two new Structured Analytical Techniques: Simple Brainstorming and Sorting**
- **We used these approaches in various scenarios to methodically think through real-world scenarios**
- **Structured Analytic Techniques allow analysts to better evaluate available information and identify trends, gaps, and areas where more research is needed, while also reducing the impact of bias**

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets

This page intentionally left blank.

https://t.me/learningnets

Technet24

Exercise 1.2: Consuming Along the Sliding Scale

Objectives

- Consume Intelligence to Generate Outputs for Active Defenders, Passive Defenses, and Architecture

Scenario: As a result of your initial research into ransomware threats to the healthcare sector, your CISO decided to reach out to other CISOs of organizations in your sector asking for information on any ransomware attacks they have experienced recently. He tells you that a hospital in an adjacent state reported a TrickBot infection in the past three months which took their systems offline temporarily. The attack aligned with reporting from CISA on ransomware threats to the healthcare sector.

You have been tasked with researching the previous attacks and converting what is known into a useable format for the security personnel operating across the Architecture, Passive Defense, and Active Defense categories of the Sliding Scale of Cyber Security.

Received Intelligence:

Reference Model: The Sliding Scale of Cyber Security



A recap to help facilitate the lab of the three applicable phases of the sliding scale:

- Architecture
  - Relates to the systems themselves, including a system of systems (such as networks) and their security. Design, supply chain, building, maintaining, etc., of the systems all fall into this category. An example would be including port mirroring on network switches to capture data, patching vulnerabilities, and generating new log types off systems for insight.
- Passive Defense
  - Relates to the systems placed on top of or in conjunction with other systems such as security tools. Anti-malware systems, endpoint protection, intrusion detection systems, log aggregators and analysis systems, and any other type of system or input into them that helps give visibility or performs automatic actions against adversaries and their capabilities.
- Active Defense
  - Relates to the human aspect of security against adversaries. Incident response, security operations, threat hunting, and other forms of reactive or proactive security where the human analyst is making decisions against the adversary or their capabilities.

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets

Exercise Prep

Read the Report in the Ex 1.2 folder on your SIFT VM or USB.

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets
Technet24

Exercise: Questions

1. What would a good network-based IOC be to identify the TrickBot infection identified in the report? (Give a specific data point and detail how it would be used; you do not need to create the rule.)

   - _____

2. What would a good host-based IOC be to identify TrickBot?

   - _____

3. Identify one of the Tactics, Techniques, and Procedures (TTPs) leveraged by the actors associated with TrickBot.

   - _____

4. Utilize an identified adversary TTP to generate a hypothesis that active defenders could use for initiating a threat hunt for this adversary.

   - _____

5. What would be an appropriate passive defense recommendation to disrupt the adversary's ability to compromise the network?

   - _____

6. What would an appropriate architecture recommendation be to hinder the adversary's ability to conduct this attack?

   - _____

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets

Exercise: Questions with Step-by-Step

1. What would a good network-based IOC be to identify the TrickBot infection identified in the report? (Give a specific data point and detail how it would be used; you do not need to create the rule.)

- **Block DNS requests to the identified domains: kostunivo[.]com, chishir[.]com, mangoclone[.]com, and onixcellent[.]com. Indications of DNS tunneling activity.**

  Malicious domains can be a simple and effective IOC. However, domains can also be brittle indicators in the sense that they are subject to change regularly. A better indicator would be a signature that alerts on the patterns or structure the malicious domains exhibit. In the case of TrickBot, the report states that TrickBot has been known to use DNS tunneling to hide command-and-control traffic. A signature that looks for indications of DNS tunneling activity, potentially based on the size of request and response, would remain effective even after the specific C2 domains were changed.

2. What would a good host-based IOC be to identify TrickBot?

- **Filename "AnchorDiag.txt". 12-character file names in the following directories: C:\Windows\, C:\Windows\SysWOW64\, C:\Users\[Username]\AppData\Roaming.**

  There are a few items we could alert from based on the CISA report, including the file named "AnchorDiag.txt" that is commonly dropped by the malware. The file is not present in *every* instance however, and the filename may change. Therefore, a better indicator is generally one based on general characteristics of the malware. In the report it mentions that after the malware executes on the compromised system, "TrickBot copies itself as an executable file with a 12-character randomly generated file name (e.g. mfjdieks.exe), which is then dropped into one of three directories. A rule that looks for filenames of that size in those directories could make for a solid host-based indicator of compromise.

3. Identify one of the Tactics, Techniques, and Procedures (TTPs) leveraged by the actors associated with TrickBot.

- **C2 over DNS using a single-byte XOR cipher to encrypt its communications**

  There are many TTPs exhibited by the adversary. The important thing is to not include any specific things such as the tool names, in this case anchor_dns. The TTPs would be how the adversary conducted their operation at a more abstracted level. Another example would be to note that the actor typically uses phishing emails delivered by commercial mass email delivery services, often with references to a failure to load a preview of the document, or the use of a loader and a backdoor in tandem, connecting to the same C2 infrastructure.

4. Utilize an identified adversary TTP to generate a hypothesis that active defenders could use for initiating a threat hunt for this adversary.

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets
Technet24

- **Hypothesis: The actors had previously repurposed existing protocols, such as tunneling C2 traffic through DNS, as a way to hide traffic. Looking for network activity that deviates from exiting protocol baselines in order to identify other hidden activities.**

The important thing here is to identify a testable idea and give some reference point to test it (such as what you might observe). Hypothesis generation does not need to have a specific recommendation for testing it, but a completed hypothesis must be testable.

5. What would be an appropriate passive defense recommendation to disrupt the actor's ability to compromise the network?

- **Email filtering that looks for and tests links included in the email text before delivering to the user.**

The actors associated with TrickBot and Bazar commonly use phishing email as an initial attack vector, and regardless of the campaign, often rely on users clicking links within the emails to begin the compromise. These campaigns are designed specifically to trick users into believing that they are legitimate, and therefore the best answer is a technical solution such as email filtering rather than relying exclusively on user awareness training.

6. What would an appropriate architecture recommendation be to hinder the adversary's ability to conduct this attack?

- **Network segmentation, have a plan to regularly back up data, which is stored offsite in an encrypted state**

Some architectural changes, such as ensuring proper network segmentation, will help prevent or reduce the spread of malware in the network. With ransomware in particular, it is critical to have a good backup process, and to test the process of restoring from backups to ensure limited downtime and full recoverability if needed.

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets

Exercise: Key Takeaways

- Consumer intelligence can be very useful in generating actionable information and indicators for use in passive defenses, architectural defenses, and by active defenders.
- We used some of the available consumer intelligence on TrickBot and Bazar to create network and host-based IOCs.
- We considered other TTPs that could be alerted upon, as well as architectural changes to make it more difficult for attackers to successfully utilize their preferred TTPs.

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets
Technet24

Exercise 1.3: Enriching and Understanding Limitations

Objectives

- Search for the indicators in Open-Source reporting
- Gather key details that will be useful to enrich understanding

Scenario: Your security operations and incident response team for Edison International was passed an indicator from a third-party source. There was no additional context for the indicator. Using the SHA1 hash and only Open-Source Intelligence (OSINT), it is your intelligence team's task to identify the context around this indicator, if it represents risk to Edison Power, a subsidiary of Edison International, and if it immediately impacts other industries. Specifically, the decision-makers are concerned about the manufacturing lines and the Industrial Control Systems (ICS) that are producing some of the final products developed from research and development at other sections of the holdings company.

Indicator Identified (this hash value is also in a text file on the USB in the Exercises directory):
SHA1 hash: 94488f214b165512d2fc0438a581f5c9e3bd4d4c

Exercise Prep

You will need internet access for this lab and will use a browser of your choice. Chrome was used when writing this lab.

The lab can be completed using the following websites:

Threatminer.org
(Utilize ThreatMiner and APTNotes)

Google.com (or your preferred search engine)

Because this is an internet-based lab, things are bound to change. Your view may not match the screenshots in the lab book.

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets

Exercise: Questions

1. What malware is associated with the indicator? You may search with Google, but also search via https://www.threatminer.org

   - _____

2. According to the ESET report on the malware, what type of systems does the malware target?

   - _____

3. From the ESET report identified in ThreatMiner, can the malware target all industries that use the type of systems identified in question 2?

   - _____

4. According to the Dragos report identified in ThreatMiner, what is the name of the threat group that created the malware?

   - _____

5. What other adversary campaign is linked to this threat group?

   - _____

6. According to the Dragos report, can this malware target all types of industries that leverage the systems identified in question 2?

   - _____

7. Can the malware impact Edison Power, and can it immediately impact the manufacturing lines?

   - _____

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets

Technet24

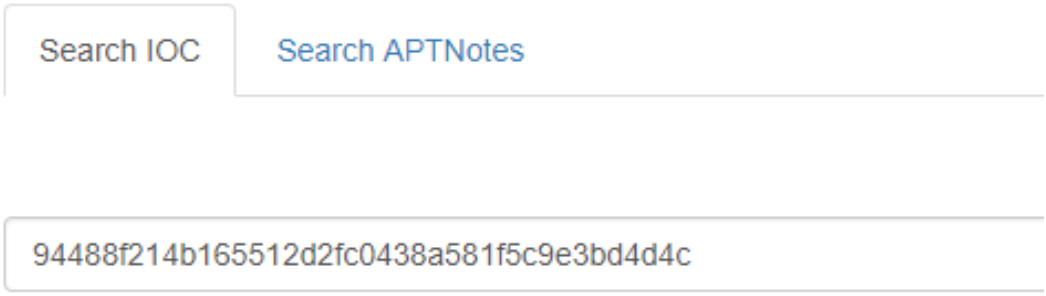
Exercise: Questions with Step-by-Step

1. What malware is associated with the indicator? You may search with Google, but also search via https://www.threatminer.org

   - **Industroyer/CrashOverride**

Many people may start with a Google search. A Google search for the hash will likely show CrashOverride in the first few hits.

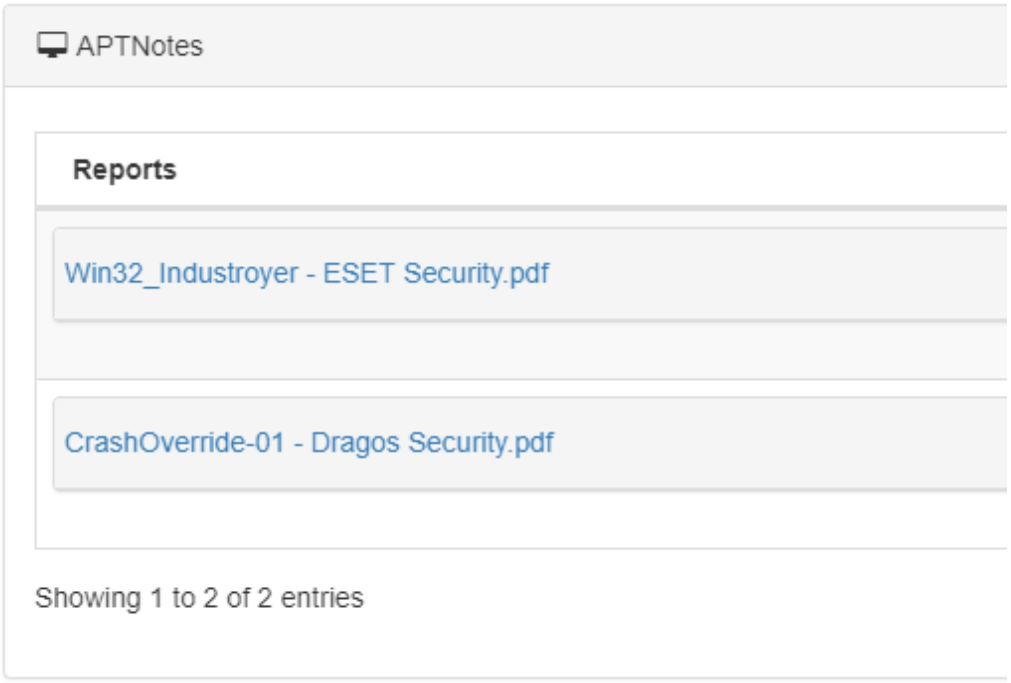
Alternatively, ThreatMiner is an excellent open-source portal designed specifically for threat research. It allows you to search for domains, IPs, digital hashes, email addresses, user agents, malware names, and more. To search this portal, we will navigate to https://www.threatminer.org in our browser. Then we can enter in the SHA1 hash given at the beginning of the lab and select the search button.



The search returns information but also has two reports under APTNotes, about halfway down the page. These reports reference the two different names associated with this hash value.

© 2021 Robert M. Lee and SANS Institute

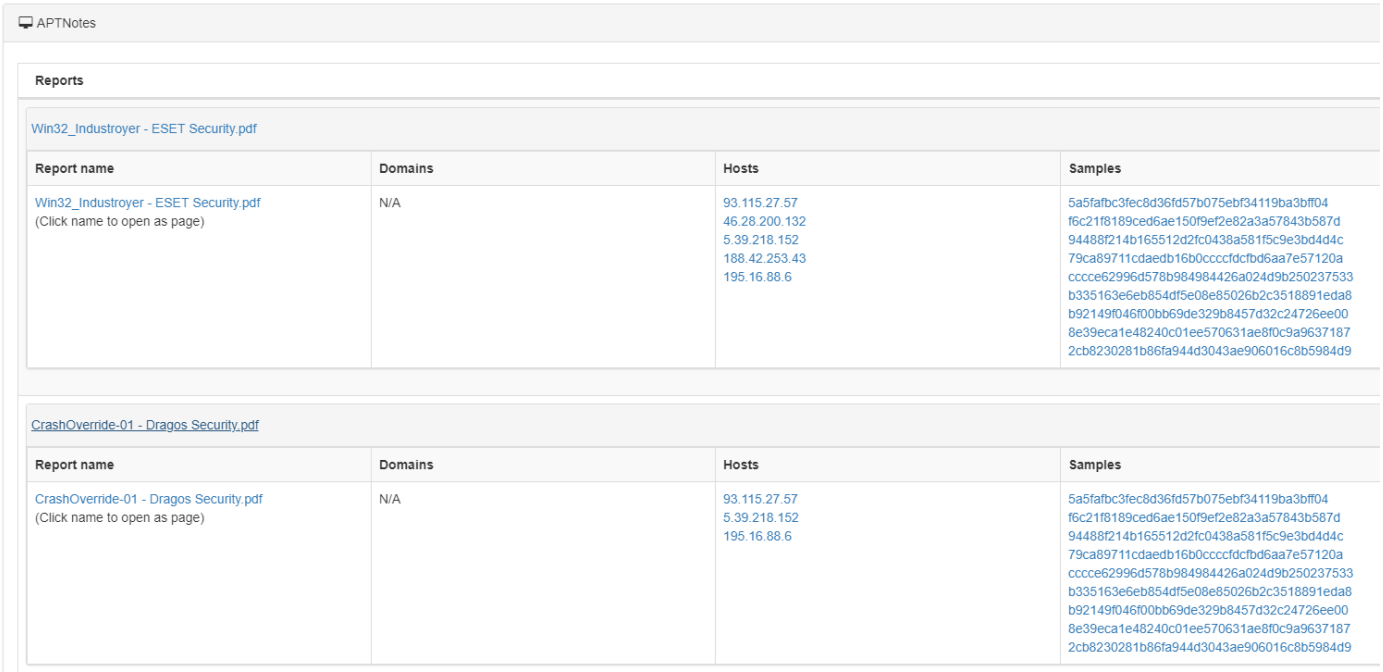
https://t.me/learningnets



2. According to the ESET report on the malware, what type of systems does the malware target?

- **Industrial Control Systems (ICS)**

By clicking on each report, we will see domains, IP addresses, and malware samples that have automatically been pulled out of the reports. We still have to validate any findings, though, as the extraction is automatic. Click on the report name to open the report and get some initial information.



APTNotes

Reports

Win32_Industroyer - ESET Security.pdf

Report name	Domains	Hosts	Samples
Win32_Industroyer - ESET Security.pdf (Click name to open as page)	N/A	93.115.27.57 46.28.200.132 5.39.218.152 188.42.253.43 195.16.88.6	5a5fafbc3fec8d36fd57b075ebf34119ba3bff04 f6c21f8189ced6ae150f9ef2e82a3a57843b587d 94488f214b165512d2fc0438a581f5c9e3bd4d4c 79ca89711cdaedb16b0ccccfdcfbd6aa7e57120a cccce62996d578b984984426a024d9b250237533 b335163e6eb854df5e08e85026b2c3518891eda8 b92149f046f00bb69de329b8457d32c24726ee00 8e39eca1e48240c01ee570631ae8f0c9a9637187 2cb8230281b86fa944d3043ae906016c8b5984d9

CrashOverride-01 - Dragos Security.pdf

Report name	Domains	Hosts	Samples
CrashOverride-01 - Dragos Security.pdf (Click name to open as page)	N/A	93.115.27.57 5.39.218.152 195.16.88.6	5a5fafbc3fec8d36fd57b075ebf34119ba3bff04 f6c21f8189ced6ae150f9ef2e82a3a57843b587d 94488f214b165512d2fc0438a581f5c9e3bd4d4c 79ca89711cdaedb16b0ccccfdcfbd6aa7e57120a cccce62996d578b984984426a024d9b250237533 b335163e6eb854df5e08e85026b2c3518891eda8 b92149f046f00bb69de329b8457d32c24726ee00 8e39eca1e48240c01ee570631ae8f0c9a9637187 2cb8230281b86fa944d3043ae906016c8b5984d9

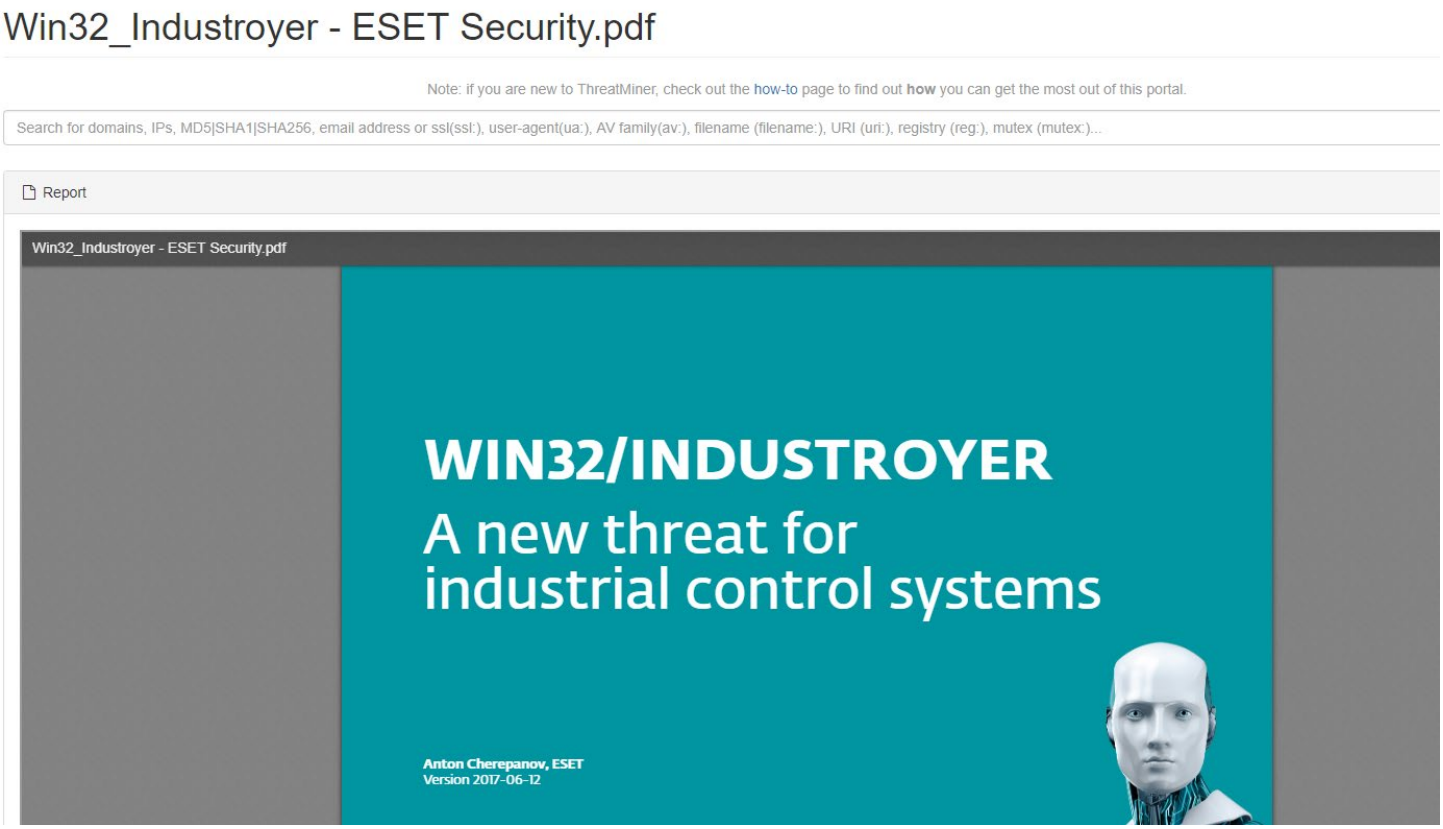
© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets
Technet24

The ESET report identifies Industroyer as targeting industrial control systems (ICSs). Industrial sites such as Edison Power, as well as the manufacturing lines of our sister company, employ ICSs so they are relevant to us.

3. From the ESET report identified in ThreatMiner, can the malware target all industries that use the type of systems identified in question 2?

- **Yes**



Digging into the report, we find that ESET claims that Industroyer can target every type of ICS, which would be very concerning and a serious claim. The malware analysis is done very well, but we might want to further validate these claims against other vendors before basing our analysis on one report.

4. According to the Dragos report identified in ThreatMiner, what is the name of the threat group that created the malware?

- **ELECTRUM**

There are some differences in assessments made by Dragos versus the ESET report. The most important note is that Dragos is also tracking the adversary group who developed the malware as ELECTRUM.

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets

5. What other adversary campaign is linked to this threat group?

- **SANDWORM**

According to the report, Dragos assesses with high confidence a direct link between ELECTRUM and SANDWORM. The SANDWORM team targeted U.S. and European infrastructure in 2014, which makes this threat immediately more relevant to those outside of Ukraine. A blog posted with the release of the report also emphasizes this point:

CRASHOVERRIDE

by Robert M. Lee - June 12, 2017

Today the Dragos, Inc. team is releasing a report titled CRASHOVERRIDE: Analyzing the Malware that Attacks Power Grids. CRASHOVERRIDE is a malware framework that has not been disclosed before today but is the capability used in the cyber-attack on the Ukraine electric grid in 2016 (not the 2015 attack). Dragos can also confirm that we are tracking the adversary group behind the attack as ELECTRUM and can assess with high confidence the group has direct ties to the Sandworm Team which targeted infrastructure companies in the United States and Europe in 2014 and Ukraine electric utilities in 2015. The report we are releasing today serves as an industry report to accompany the intelligence report our customers have received on the threat. The intelligence report goes into more technical exploration and ties together sensitive details, but the industry report contains everything that defenders need to analyze the threat, defend their systems, and understand the potential impact. The report will also educate on grid operations and try to illuminate the threat scenarios while reducing any hype and confusion on the impact.

6. According to the Dragos report, can this malware target all types of industries that leverage the systems identified in question 2?

- **No, only electric grid systems**

Following the link to get the full report reveals a few key up-front assessments, one of which is that the claim that "Industroyer" or "CRASHOVERRIDE" can easily be adapted to target other ICS is discredited. This was a key point in the ESET report and thus the name "Industroyer." The Dragos team (who specializes in ICS) has noted that it's not about a protocol change in the malware but, specifically, industrial knowledge must be codified into the malware to be used against other industries, and, so far, that has not been exhibited as a capability or the hostile intent of the adversary. This is important nuance, especially for our decision-makers to understand what industries are immediately impacted, especially if we have an ICS company but are not in the electric grid sector.

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets
Technet24

> CRASHOVERRIDE could be extended to other industries with additional protocol modules, but the adversaries have not demonstrated the knowledge of other physical industrial processes to be able to make that assessment anything other than a hypothetical at this point and protocol changes alone would be insufficient.

7. Can the malware impact Edison Power, and can it immediately impact the manufacturing lines?

- **Yes to Edison Power, not immediately for the manufacturing lines**

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets

Exercise: Key Takeaways

- **We learned to use open-source intelligence to effectively search for and report on acquired indicators.**

- **Deeper analysis of the acquired indicator allowed the intelligence team to identify exactly which parts of the business were at greatest risk. This is important information to convey to our decision-makers.**

- **We noted that having actual insight to the systems, operations, business requirements, etc., is imperative to being able to produce intelligence.**

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets
Technet24

Exercise 1.4: Strategic Threat Modeling

Objectives

- Develop a threat model for Edison International's newest acquisition, SpaderTech, identifying the primary information and resources that may be targeted
- Identify TTPs associated with potential activity groups in the threat model
- Identify priority intelligence requirements (PIRs)
- Identify intelligence gaps

Scenario: Edison International has just acquired a new technology company with an energy-focus: Spader Technology. Edison's CEO is eager to connect the networks as part of a new joint campus initiative; however, the CISO has some concerns about the security of the network. You have been asked to assess how the integration will change Edison's threat model and determine what changes, if any, should be made to existing security controls. Spader does not have a threat intelligence team, and therefore you will also need to assess whether Edison has the correct collection to understand and detect threats facing a company in this sector.

Exercise Prep

You will need to select a tool or series of tools to conduct brainstorming, sorting, or other SATs, as well as documenting your findings. In addition to answering the questions in the lab, you will be creating a visual representation of a threat model to present to the CEO. The MindMup tool from previous labs, Excel, Notepad, PowerPoint, or paper and pen are all acceptable tools.

Additionally, the following documentation and resources are available in the FOR578 Exercise Folder:

Resources: (in the **Ex. 1.4** folder)

- *Edison International's company newsletter*
- *Assessment of information and Resources prepared by SpaderTech Business Units*
- *VERIS spreadsheet with previous incident information from Spader*
- *Dragos' CRASHOVERRIDE Report*
- *Symantec's DRAGONFLY Report*
- *SANS Defense Use Case (DUC) 5 on Ukraine 2015 power grid attack*

The Final Model: *There is no single way to make a threat model, so the walkthrough will not match your answers and is simply an example to assist you. Your model will look different and will be based on different inputs such as CRASHOVERRIDE.*

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets

Exercise: Questions

1. After reading through the Edison Company Newsletter, what areas are likely PIRs that need to be taken into consideration as a part of the threat model?

- _____
- _____
- _____

2. After reading through the Information and Resources Assessment, what information do you think belongs in the threat model? Add these to the threat model worksheet.

- _____
- _____
- _____
- _____
- _____

3. According to the Incident Tracking spreadsheet, what systems or information have previously been impacted at SpaderTech?

- _____
- _____
- _____
- _____

4. What types of threats were the previous incidents associated with?

- _____
- _____
- _____

5. According to the Dragos, Symantec, and SANS reports, which adversaries target the energy sector?

- _____
- _____

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets

Technet24

- _____

6. From what we know from the previous exercises and case studies (and/or the reports), what are some of the tactics, techniques, and procedures (TTPs) of the adversaries and their capabilities?

- _____
- _____

7. What intelligence gaps are in the threat model currently? Do they align with any of the PIRs?

- _____
- _____
- _____
- _____

8. What additional security recommendations would you give based on this analysis?

- _____
- _____
- _____

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets

Exercise: Questions with Step-by-Step

1. After reading through the Edison Company Newsletter, what areas are likely priority intelligence requirements (PIRs) that need to be taken into consideration as a part of the threat model?

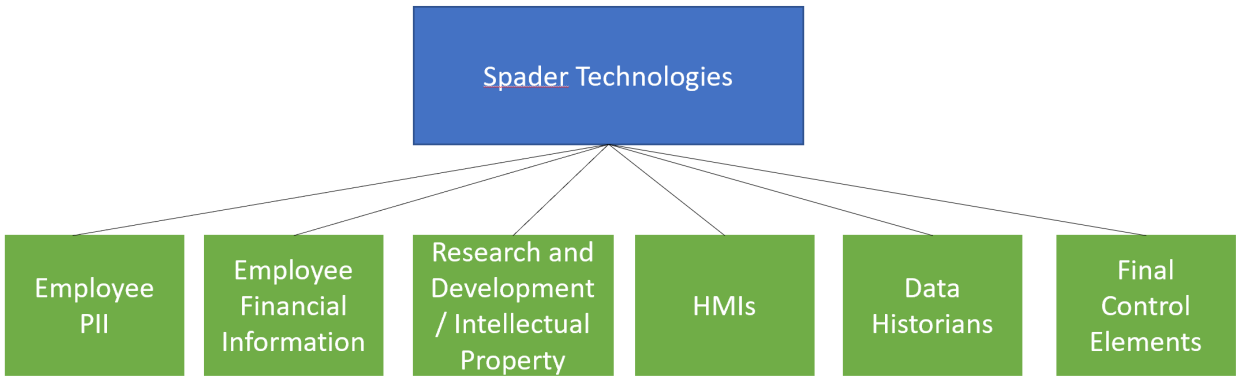
   - **Protecting Edison's new infrared handheld technologies**
   - **The new joint-campus venture and securing the Spader Test Network**
   - **Protecting the Intellectual Property associated with Spader's infrared nanotechnology**

2. After reading through the Information and Resources Assessment, what information do you believe belongs in the threat model? Add these to the threat model worksheet.

   - **Employee PII**
   - **Employee financial information**
   - **R&D information/Intellectual Property**
   - **Human Machine Interfaces (HMIs)**
   - **Final Control Elements (FCEs)**
   - **Data Historians**

   Open and review the file "Spader_Tech_Information and Resources.docx" in the exercise folder. The internal memo identifies these as sensitive information or mission-critical systems for Spader Technologies.

   Start the threat model representation by adding Spader Technologies to the top of the worksheet, as well as the six different data sources identified in the memo.



© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets
Technet24

3. According to the Incident Tracking spreadsheet, what systems or information have previously been targeted at Spader Technologies?
   - **Employees in Payroll**
   - **Employees in R&D**
   - **SpaderTech's Web Server**
   - **Scientists working on nanotechnology**

   Open and review the spreadsheet "Spader_Technologies_VERIS_Incident Tracking.xlsx" in the Exercise Folder. This spreadsheet contains details of previously investigated incidents at SpaderTech using the VERIS format. The spreadsheet identifies previous incidents, including several notable threats to SpaderTech. A spear phishing email directed at an employee in payroll indicates that employee PII and financial information were targeted. An incident where three laptops of R&D employees were infected with the Havex Trojans by an unidentified actor shows an interest in R&D information and potentially the Industrial Control Systems as well. A denial-of-service attack against the web server was carried out by a hacktivist group protesting the environmental impact of the energy sector. Scientists working on nanotechnologies were targeted by a phishing email with a malicious URL, which was inadvertently spread to other employees over chat.

4. What types of threats were the previous incidents associated with? Add these to the threat model representation.

   - **The payroll phishing attacked was linked to a criminal campaign and was likely financially motivated.**
   - **The Havex Incident was not attributed, but targeted operations employees in the SCADA networks. The Symantec report identifies Havex as a tool that targets ICS systems and attempts to enumerate connected systems, particularly looking for connected control systems.**
   - **The denial-of-service attack was conducted by an environmental activist group and targeted Spader Tech because it is part of the energy sector.**
   - **The targeting of the scientists working on nanotechnology was not attributed to any threat or activity group.**

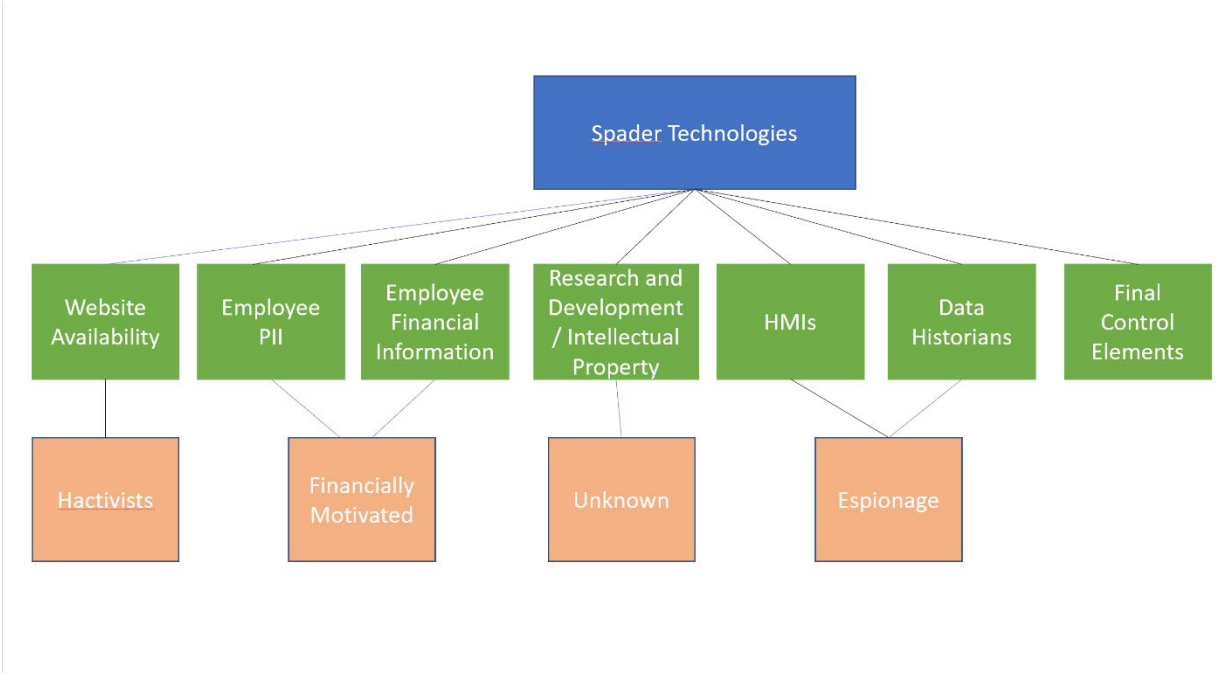
   Information from the spreadsheet that captured the results of the investigations provides information on the nature of the threats, including the fact that the payroll attack was linked to organized crime and that an attack on the company's website was carried out by an environmental hacktivist group. The website availability had not previously been identified as a potentially targeted system, so that field will need to be added to the threat model worksheet.

   The attackers behind the Havex intrusion were not identified; however, Symantec provides additional information on Havex, including the fact that it specifically targets Industrial Control Systems. SCADA networks, such as the ones in Spader Technologies, are a subset of Industrial Control Systems and are potentially targeted by this malware. The phishing of the nanotechnology scientists was also unattributed; however, given its targeted nature and the potential that it had not been fully remediated after initially infecting five workstations, this incident should likely continue to be investigated.

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets

Add the website availability as a target, and then add the nature of the threats to the threat model worksheet and link them to the resources they targeted.



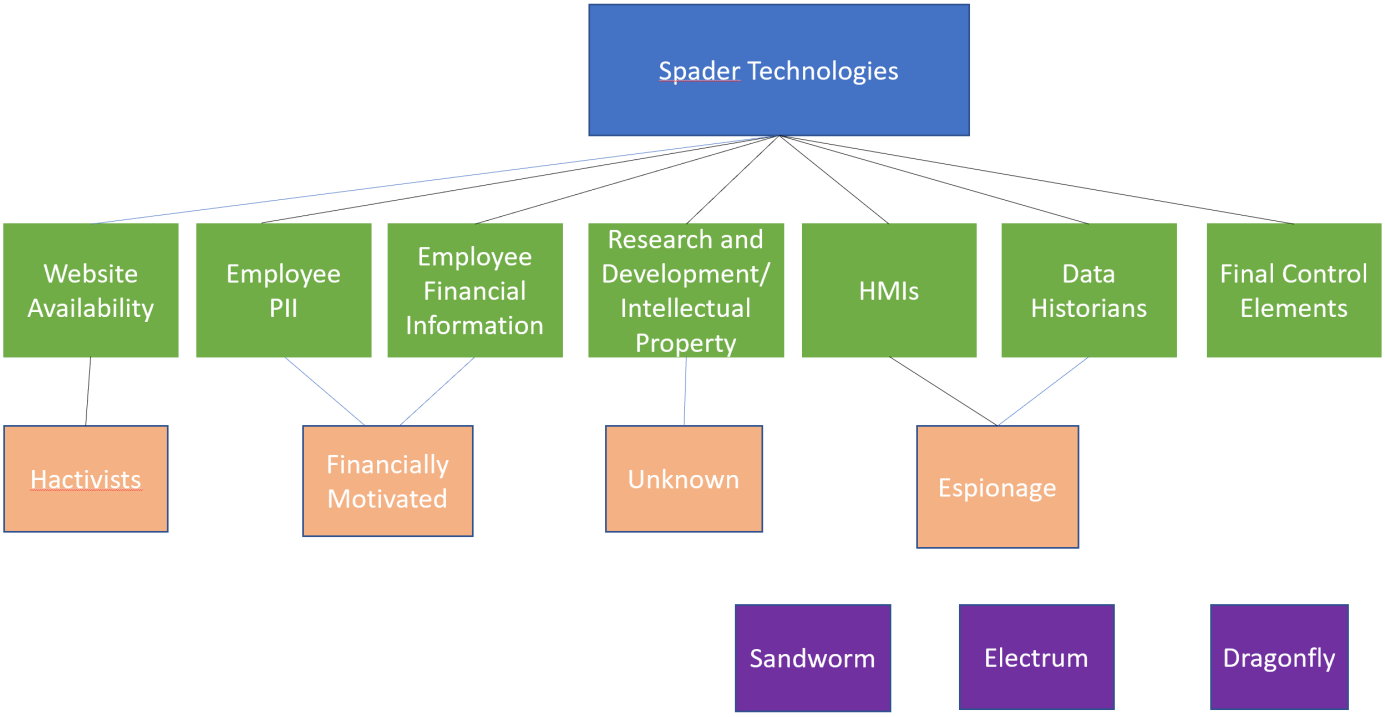
5. According to the Dragos, Symantec, and SANS reports, which adversaries target the energy sector? Add these to the threat model worksheet.

- **ELECTRUM**
- **SANDWORM**
- **DRAGONFLY**

Understanding more about the threats facing a new sector is critical to developing a threat model and identifying collection gaps. Threats such as financially motivated criminals and industrial espionage targeting R&D are not new to Edison; however, the threats facing the operational energy networks are. Open and review the three reports in the Ex. 1.4 folder. The energy sector includes companies involved in the exploration and development of oil or gas reserves, oil and gas drilling, renewable energy, electric grids, power stations, and more. According to the reports, there have been three adversary groups identified, including SANDWORM, ELECTRUM, and DRAGONFLY.

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets
Technet24



6. From what we know from the previous exercises and case studies (and/or the reports), what are some of the tools and tactics, techniques, and procedures (TTPs) of the adversaries?

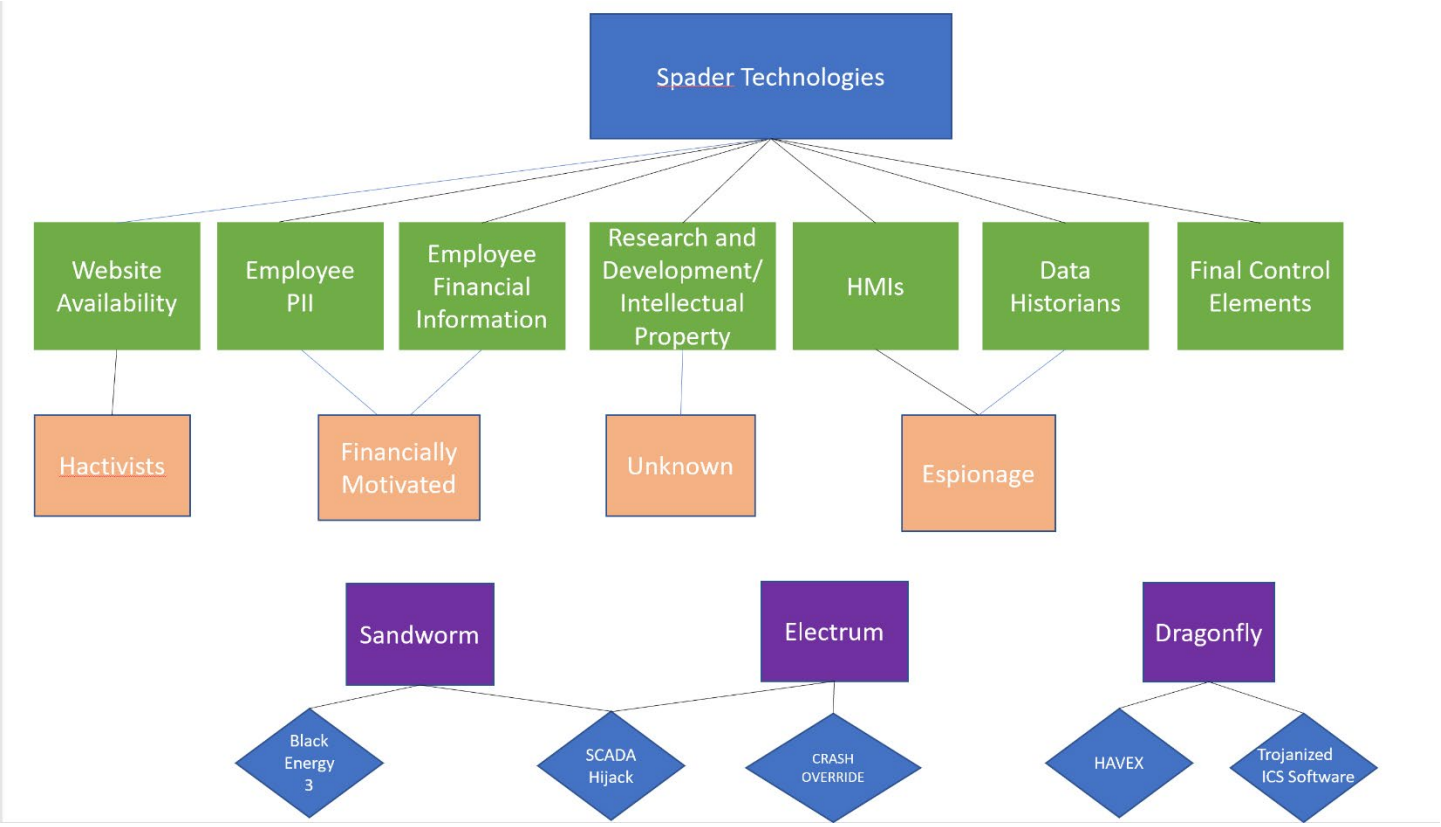
- **Watering Hole Attacks**
- **Trojanized ICS Installers**
- **HAVEX**
- **BlackEnergy 3**
- **CRASHOVERRIDE**

According to the Symantec report, Dragonfly typically uses watering hole attacks and malicious PDF files or trojanized ICS installers embedded with the HAVEX malware. SANDWORM leveraged the BlackEnergy 3 malware in the 2015 Ukraine attack as well as leveraging the ICS systems against themselves (SCADA hijack). ELECTRUM leveraged CRASHOVERRIDE, which took advantage of legitimate functionality in the ICS electric grid systems.

Add the TTPs and tools to your threat model worksheet.

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets



7. What intelligence gaps are in the threat model currently?

- **What was the nature of the phishing attack targeting the nanotechnology scientists (PIR)?**
- **Was the nanotechnology incident properly remediated (PIR)?**
- **What information was taken in the Espionage case (PIR)?**
- **Were other systems accessed?**

After reviewing the current threat model, it is apparent that there needs to be more research to understand the adversaries behind the incidents that were identified, including how they were originally detected, exactly what information was stolen in the espionage cases, and if there are any indications that SANDWORM or ELECTRUM have tried to target our company before. The first three gaps all tie back to PIRs on protecting new technologies and Research and Development initiatives. If there are indications that the threats spread to the test network, that would become a PIR as well.

8. What additional security recommendations would you give based on this analysis?

- **Ensure that protections are in place for the company chat system**
- **User Awareness Training for Phishing**

There are several potential recommendations that could be made based off the analysis of Spader Technologies' past incidents and threat models. The fact that an infection was spread through Spader's company chat is concerning, considering how much Edison International relies on chat for communications, especially around security issues and the fact that the chat systems do seem to be connected now. In addition, many of the past incidents at the company, and incidents related to the

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets
Technet24

energy sector in general, involve phishing. User awareness training, especially of energy-specific threats, will be helpful for Edison employees as well as Spader Employees.

Exercise: Key Takeaways

- **Understanding what threats may potentially impact your organization, including what type of data or systems they may target, can help prepare for or even prevent attacks, and can help to identify where additional resources are needed.**

- **Internal resources, including previous incidents and investigations and internal risk assessments, are critical to developing a threat model.**

- **Threat models need to be periodically updated based on new threat information or changes to the organization.**

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets

This page intentionally left blank.

https://t.me/learningnets

Technet24

Exercise 2.1: Collecting Reconnaissance and Delivery Data

Objectives

- Gain familiarity on intrusions that will serve as a foundation in the course scenario
- Identify and Categorize Indicators using the Kill Chain and Diamond Model
- Identify and Categorize MITRE ATT&CK® Tactics and Techniques

Scenario: As a cyber threat intelligence analyst working for Edison International (supporting your new subsidiary, Spader Technologies) you are constantly on the hunt for new intrusions that could identify a past, current, or future compromise of your organization. Your goal is to be able to identify sparse and seemingly disconnected pieces of data and events to identify if there are connections that tell a larger, more important story. To achieve this, you will map data to the Kill Chain, Diamond Model, and MITRE ATT&CK, which will allow you to better track intrusions as you complete additional analysis.

Exercise Prep

Students will utilize either the Excel document "Ex 2.1 Intrusion Template.xlsx" in the **Ex 2.1** folder on the USB in the **Exercises** folder or take notes however they would like, including a scratch pad.

They will also utilize MITRE ATT&CK—they may use the current version of ATT&CK at https://attack.mitre.org/. The exercise walkthrough uses ATT&CK version 8 located at https://attack.mitre.org/versions/v8/matrices/enterprise/. No other tools are necessary and the data required for the lab is provided below.

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets

Potentially Relevant Edison International Scans of External Gateway Server

Timestamp	IP Address	Ports Scanned	Ports Open
2020-08-13 13:23 UTC	89.34.237.11	80, 443, 22, 23	443
2020-08-14 02:02 UTC	51.11.247.89	443, 3389, 80	443, 3389
2020-08-15 13:23 UTC	21.50.50.23	3389	3389
2020-08-16 01:32 UTC	104.224.166.148	3389	3389

Received Emails

Sender: help@topenergysupport.com
Recipient: t.johnson@spadertech.com
Date: August 14, 2020
Attachment: None
Contents:
"Dear Timothy Johnson,

Our company specializes in supporting the energy sector. We have many tools to make remote support better. We have an updated tool of our VNC viewer which we wish you to try. You can get it from our Downloads page at http://downloads.topenergysupport.com. It will be much faster than current VNC tools. We hope you enjoy!

Kind regards,
Top Energy Support Team"

Sender: alayos@supplydenn.com
Recipient: t.johnson@spadertech.com
Date: August 14, 2020
Contents:
"Timothy Johnson,

Please find attached your invoice for the control equipment you purchased.

Supply Denn"

Attachment: "Invoice.docx"

Sandbox Results:
Malicious: Yes
Known Malware: Poison Ivy
Configuration Data: 38.72.115.9
Files Dropped: Document2.pdf

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets
Technet24

Exercise: Questions

Capture the indicators by Kill Chain and Diamond Model phases. Additionally, note any MITRE ATT&CK Technique and Tactics that you observe by indicator. You may complete this exercise using whatever tools you would like, ranging from scratch paper to the "Ex 2.1 Intrusion Template.xlsx" Excel file provided on the USB in the Ex 2.1 folder.

1. How many different intrusions are represented in the data?

   - _____

2. Capture relevant information from each intrusion. You may use the provided "Intrusion Indicators.xls" template or another method of your choice to capture this information.

3. Which Kill Chain phase (or phases) are represented in each intrusion?

   - **Intrusions 1-4:**_____
   - **Intrusion 5:**_____
   - **Intrusion 6:**_____

4. Map information from each intrusion to the four Diamond Model features.

5. Map information from each intrusion map to MITRE ATT&CK Tactics and Techniques/Sub-techniques.

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets

Exercise: Questions with Step-by-Step

Capture the indicators by Kill Chain and Diamond Model phases. Additionally, note any MITRE ATT&CK Technique and Tactics that you observe by indicator. You may complete this exercise using whatever tools you would like, ranging from scratch paper to the "Ex 2.1 Intrusion Template.xlsx" Excel file provided on the USB in the Ex 2.1 folder.

1. How many different intrusions are represented in the data?

- **Six**

We define an intrusion as any successful or failed activity, so even the scans would qualify as intrusions. At this point in our analysis, we do not have any reason to associate the external scanning indicators with any of the phishing emails or attachments. Therefore, you will have six unique intrusions at this point.

2. Capture relevant information from each intrusion. You may use the provided "Intrusion Indicators.xls" template or another method of your choice to capture this information.

We have determined that we should track six different intrusions at this point. One way to get started is to analyze logs and artifacts, and then start to identify relevant indicators and details on each intrusion. Collecting information about the intrusion in one place, especially as we analyze more complex intrusions, will help us be organized before we map to frameworks and models. You may use the provided "Intrusion Indicators.xls" file as a template or capture your notes however it makes sense for you. We choose to capture details in separate sheets in the provided Excel template. The notes below are just one way you could go about capturing relevant information.

Intrusion 1

Indicator	Comment
89.34.237.11	Scanned external gateway for ports 80, 443, 22, 23 (only port 443 open)

Intrusion 2

Indicator	Comment
51.11.247.89	Scanned external gateway for ports 443, 3389, 80 (ports 443, 3389 open)

Intrusion 3

Indicator	Comment
21.50.50.23	Scanned external gateway for port 3389 (port 3389 open)

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets
Technet24

Intrusion 4

Indicator	Comment
104.224.166.148	Scanned external gateway for port 3389 (port 3389 open)

Intrusion 5

Indicator	Comment
help(at)topenergysuport.com	Sender email for phish to T Johnson
t.johnson(at)spadertech.com	Victim of phish
“Top Energy Support Team”	"Signature" of phish to T Johnson
downloads.topenergysupport(dot)com	Malicious link in phish to T Johnson

Intrusion 6

Indicator	Comment
alayos(at)supplydenn.com	Sender email for phish to T Johnson
t.johnson(at)spadertech.com	Victim of phish
“Supply Denn”	"Signature" of phish to T Johnson
Invoice.docx	Attachment for phish to T Johnson
Poison Ivy	Malware family of Invoice.docx attachment in phish to T Johnson
Document2.pdf	File dropped by Invoice.docx attachment in phish to T Johnson
38.72.115.9	Config data from Invoice.docx attachment in phish to T Johnson

3. Which Kill Chain phase (or phases) are represented in each intrusion?

- **Intrusions 1-4: Reconnaissance**
- **Intrusion 5: Delivery**
- **Intrusion 6: Delivery and Weaponization**

Now that our intrusion information is organized, we will start by mapping each intrusion to one or more phases of the Kill Chain. Intrusions 1 through 4 are fairly straightforward—scanning of our external gateway falls under the Reconnaissance phase. We can add this information to our existing spreadsheets or however you chose to track your notes. Once updated, our spreadsheets may look something like below. We use “KC” to abbreviate “Kill Chain.”

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets

Intrusion 1

Indicator	Comment	KC Phase
89.34.237.11	Scanned external gateway for ports 80, 443, 22, 23 (only port 443 open)	Reconnaissance

Intrusion 2

Indicator	Comment	KC Phase
51.11.247.89	Scanned external gateway for ports 443, 3389, 80 (ports 443, 3389 open)	Reconnaissance

Intrusion 3

Indicator	Comment	KC Phase
21.50.50.23	Scanned external gateway for port 3389 (port 3389 open)	Reconnaissance

Intrusion 4

Indicator	Comment	KC Phase
104.224.166.148	Scanned external gateway for port 3389 (port 3389 open)	Reconnaissance

For Intrusion 5, since this is a phishing email, we determine it falls under the Delivery phase of the Kill Chain, so we mark all our indicators with that.

Intrusion 5

Indicator	Comment	KC Phase
help(at)topenergysuport.com	Sender email for phish to T Johnson	Delivery
t.johnson(at)spadertech.com	Victim of phish	Delivery
“Top Energy Support Team”	"Signature" of phish to T Johnson	Delivery
downloads.topenergysupport(dot)com	Malicious link in phish to T Johnson	Delivery

Intrusion 6 is a little trickier. We map the phishing email components to Delivery. We determine that as our malware analysts conducted analysis of the contents of the phishing email attachment, we were really looking at how the adversary weaponized that payload, so we map the malware analysis components to Weaponization. This is the concept of “phasal distortion”—the idea that sometimes,

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets
Technet24

when we get information about one phase, we can also cover another Kill Chain phase at the same time. We identify different indicators as Delivery and Weaponization depending on the phase we determine they represent.

Intrusion 6

Indicator	Comment	KC Phase
alayos(at)supplydenn.com	Sender email for phish to T Johnson	Delivery
t.johnson(at)spadertech.com	Victim of phish	Delivery
“Supply Denn”	"Signature" of phish to T Johnson	Delivery
Invoice.docx	Attachment for phish to T Johnson	Delivery
Poison Ivy	Malware family of Invoice.docx attachment in phish to T Johnson	Weaponization
Document2.pdf	File dropped by Invoice.docx attachment in phish to T Johnson	Weaponization
38.72.115.9	Config data from Invoice.docx attachment in phish to T Johnson	Weaponization

4. Map information from each intrusion to the four Diamond Model features.

Next, we want to map each intrusion to the Diamond Model so that we can identify any gaps we have as well as create activity groups later. Starting with Intrusions 1-4, which are all very similar, we decide that scanning falls under Capability (since we could consider it a technique), the source IP address doing the scanning falls under Infrastructure (since it delivers the Capability of scanning), and the victim is our External Gateway server. We can’t think of anything that falls under Adversary right now, which is okay —you won’t always have all four features of the Diamond Model for every intrusion. Updating our spreadsheet, it may look something like the below. We use “DM” to abbreviate “Diamond Model” and choose to capture this information on the same row as our indicators, but you could choose a different approach.

Intrusion 1

DM: Adversary	DM: Capability	DM: Infrastructure	DM: Victim
N/A	Scanning	89.34.237.11	External Gateway

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets

Intrusion 2

DM: Adversary	DM: Capability	DM: Infrastructure	DM: Victim
N/A	Scanning	51.11.247.89	External Gateway

Intrusion 3

DM: Adversary	DM: Capability	DM: Infrastructure	DM: Victim
N/A	Scanning	21.50.50.23	External Gateway

Intrusion 4

DM: Adversary	DM: Capability	DM: Infrastructure	DM: Victim
N/A	Scanning	104.224.166.148	External Gateway

For Intrusion 5, as we examine our existing indicators, we realize that some of these directly fall under different Diamond Model features, so we decide to reorganize our spreadsheet a little. Since the email signature of "Top Energy Support Team" represents a persona, we decide to place that under the Adversary feature. The Capability for this intrusion is phishing, and the Infrastructure (how that Capability is delivered) would be the sender email address of help(at)topenergysupport.com. Our Victim is t.johnson(at)spadertech.com. We decide to organize our information like the below, though of course, you could choose to organize it differently. (We move our other columns for the Kill Chain and with our Comments to the side, though we still keep them.)

Intrusion 5

Indicator	DM: Adversary	DM: Capability	DM: Infrastructure	DM: Victim
help(at)topenergysuport.com	"Top Energy Support Team"	Phishing	help(at)topenergysuport.com	t.johnson(at)spadertech.com
downloads.topenergysupport(dot)com	"Top Energy Support Team"	Phishing	help(at)topenergysuport.com	t.johnson(at)spadertech.com

As we map Intrusion 6 to the Diamond Model, we need to be sure to be consistent with what we mapped in earlier intrusions. (Perhaps we start keeping documentation of how we map these intrusions that we could later add to our style guide.) Since the email comes from an email address starting with "Alayos" and is signed with "Supply Denn", we could capture both of these under Adversary. We decide that depending on the data point, the Capability will be a little different, so we choose Phishing, Trojanized Document, and Poison Ivy for different indicators (we don't know the Capability for the IP address found in the malware config data yet). Our Infrastructure also differs a little, based on each indicator. For our phishing email, we choose the sender email address, alayos(at)supplydenn.com. For

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets
Technet24

the attachment Invoice.docx, however, we decide that the Phishing Email itself is what delivered the attachment, so we identify the overall Phishing Email as Infrastructure. For the malware analysis details of the contents of the malicious attachment, we consider Invoice.docx as the delivery vehicle for the malicious code itself, so we identify Invoice.docx as Infrastructure. Of course, you could choose to map these indicators differently. The Victim is more straightforward—for all indicators, we identify t.johnson(at)spadertech.com as the Victim. Our spreadsheet looks something like this, though yours may look differently.

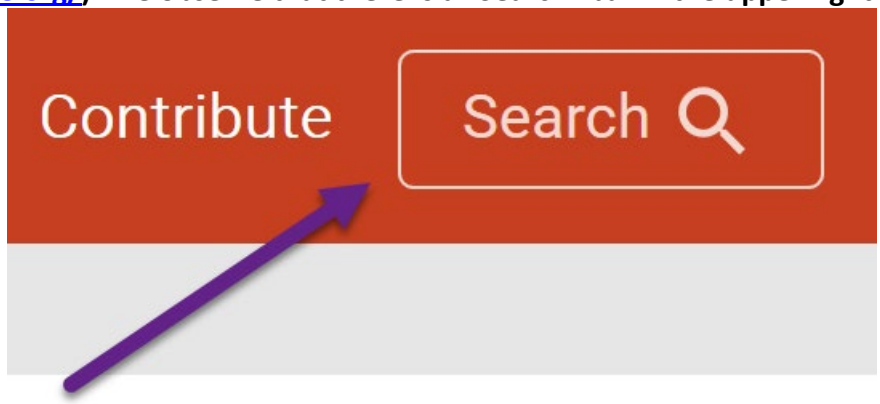
Intrusion 6

Indicator	DM: Adversary	DM: Capability	DM: Infrastructure	DM: Victim
alayos(at)supplydenn.com	Alayos/Supply Denn	Phishing	alayos(at)supplydenn.com	t.johnson(at)spadertech.com
Invoice.docx	Alayos/Supply Denn	Trojanized Document	Phishing Email	t.johnson(at)spadertech.com
Poison Ivy	Alayos/Supply Denn	Poison Ivy	Invoice.docx	t.johnson(at)spadertech.com
Document2.pdf	Alayos/Supply Denn	N/A	Invoice.docx	t.johnson(at)spadertech.com
38.72.115.9	Alayos/Supply Denn	Trojanized Document	Invoice.docx	t.johnson(at)spadertech.com

6. Map information from each intrusion map to MITRE ATT&CK Tactics and Techniques/Sub-techniques.

Now, we want to map to our third framework: ATT&CK. While a deep-dive into ATT&CK is beyond the scope of our course, you can identify additional training on ATT&CK (which was used in the development of this section) here: https://attack.mitre.org/resources/training/. Trying to map to ATT&CK can be overwhelming, so we recommend two key ways to make it easier.

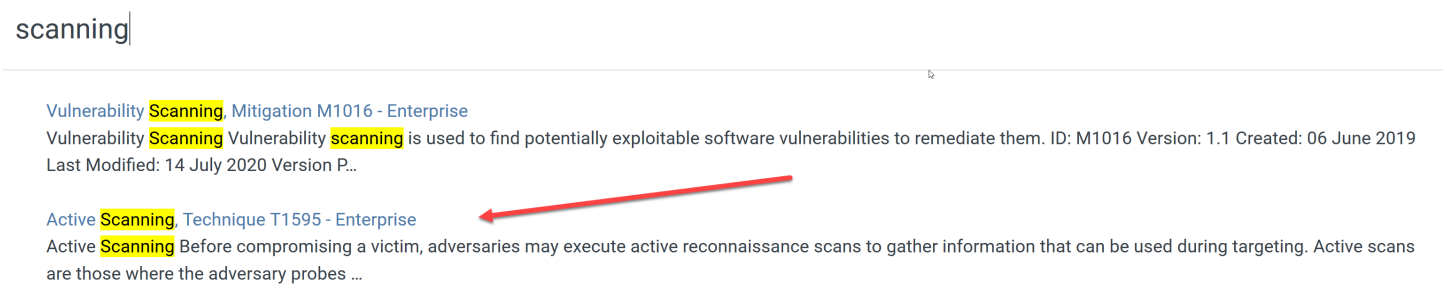
First, we can try searching the ATT&CK website for key words of the technique you are looking for. We try this approach for Intrusion 1, which involves scanning. Navigate to the ATT&CK website (for this walkthrough, we used https://attack.mitre.org/versions/v8/; the current version is available at https://attack.mitre.org/). We observe that there is a "Search" bar in the upper right of the website.



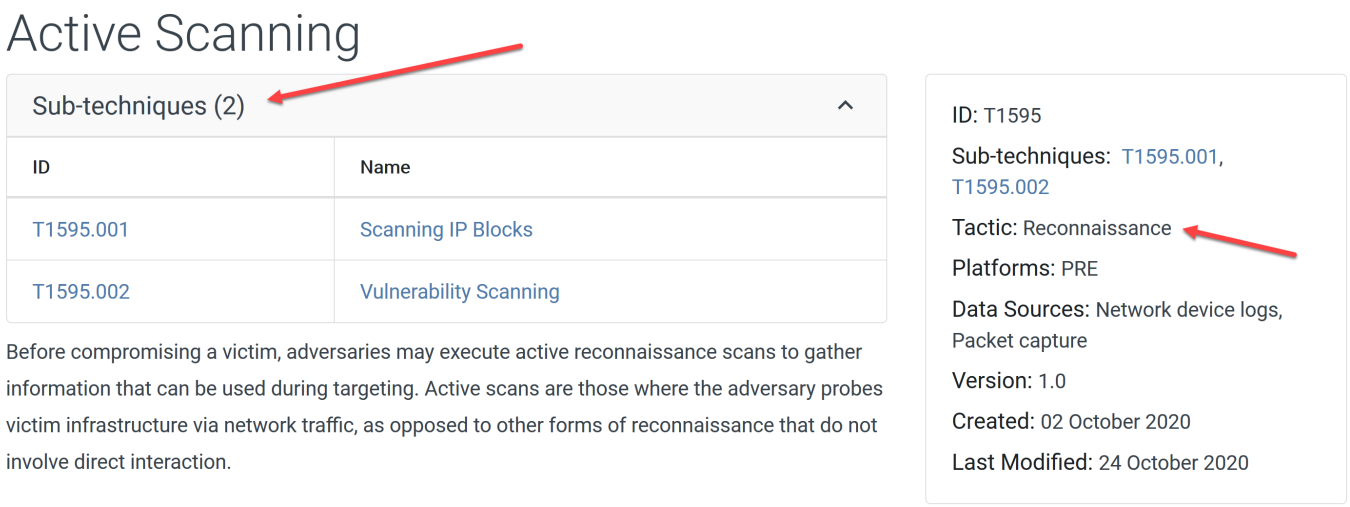
We click on this and try entering a keyword of "scanning." We see that "scanning" appears in several different techniques, but as we read the descriptions, we think the second technique, Active Scanning (T1595), sounds like what we're looking for.

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets



Clicking on that link, the website takes us to a page with more details on the technique. As we read the description, we see that Active Scanning has two more granular sub-techniques. We decide our behavior best maps to the parent Active Scanning technique. We also observe that in ATT&CK, this technique falls under the tactic of Reconnaissance—which happens to be the same name as the Kill Chain phase, though that will not always be the case.



(https://attack.mitre.org/versions/v8/techniques/T1595/)

Since Intrusions 1 through 4 are very similar, we decide to apply the same tactic and technique to all of them. Updating our spreadsheets, they may look something like the one below. We choose to capture the version of ATT&CK we mapped to since it changes.

Intrusions 1-4

ATT&CK Tactic v8	ATT&CK Technique v8
Reconnaissance	T1595 Active Scanning

For Intrusion 5, since we have a few indicators, we likely have more than one tactic and technique that may apply. We can start with a search of the website for "phishing," and via the method above, we determine that one technique is Spearphishing Link (T1566.002), which ATT&CK places under the Initial Access tactic. (You could also choose to map to the parent technique of Phishing instead.)

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets
Technet24

Phishing: Spearphishing Attachment

Other sub-techniques of Phishing (3)

Adversaries may send spearphishing emails with a malicious attachment in an attempt to gain access to victim systems. Spearphishing attachment is a specific variant of spearphishing. Spearphishing attachment is different from other forms of spearphishing in that it employs the use of malware attached to an email. All forms of spearphishing are electronically delivered social engineering targeted at a specific individual, company, or industry. In this scenario, adversaries attach a file to the spearphishing email and usually rely upon User Execution to gain execution.

ID: T1566.001

Sub-technique of: T1566

Tactic: Initial Access

Platforms: Linux, Windows, macOS

Data Sources: Detonation chamber, Email gateway, File monitoring, Mail server, Network intrusion detection system, Packet capture

(https://attack.mitre.org/versions/v8/tactics/enterprise/)

We aren't done yet, though. One important aspect of mapping to ATT&CK to remember is that multiple techniques could apply at once. Though Spearphishing Link covers the email itself, it still has to be executed somehow. Looking at the ATT&CK tactics, we observe that Execution is a distinct tactic from Initial Access.

Enterprise tactics

Enterprise Tactics: 14

ID	Name	Description
TA0043	Reconnaissance	The adversary is trying to gather information they can use to plan future operations.
TA0042	Resource Development	The adversary is trying to establish resources they can use to support operations.
TA0001	Initial Access	The adversary is trying to get into your network.
TA0002	Execution	The adversary is trying to run malicious code.

(https://attack.mitre.org/versions/v8/tactics/enterprise/)

Other than searching for keywords, a second method we can use to identify ATT&CK techniques is to start with the applicable tactic, and then skim the available techniques to try to determine the correct one. This is a good strategy if a keyword search doesn't work. We aren't sure what the method of Execution might be for phishing, so we can click on the link to the Execution tactic, which brings up all of the available techniques under that tactic. As we scroll through the available techniques, the User Execution technique (T1204) catches our eye. We observe that there is even a sub-technique that maps to Malicious Link (T1204.001), so we decide to use that technique for Intrusion 5 as well.

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets

T1204		User Execution	An adversary may rely upon specific actions by a user in order to gain execution. Users may be subjected to social engineering to get them to execute malicious code by, for example, opening a malicious document file or link. These user actions will typically be observed as follow-on behavior from forms of Phishing.
	.001	Malicious Link	An adversary may rely upon a user clicking a malicious link in order to gain execution. Users may be subjected to social engineering to get them to click on a link that will lead to code execution. This user action will typically be observed as follow-on behavior from Spearphishing Link. Clicking on a link may also lead to other execution techniques such as exploitation of a browser or application vulnerability via Exploitation for Client Execution. Links may also lead users to download files that require execution via Malicious File.
	.002	Malicious File	An adversary may rely upon a user opening a malicious file in order to gain execution. Users may be subjected to social engineering to get them to open a file that will lead to code execution. This user action will typically be observed as follow-on behavior from Spearphishing Attachment. Adversaries may use several types of files that require a user to execute them, including .doc, .pdf, .xls, .rtf, .scr, .exe, .lnk, .pif, and .cpl.

(https://attack.mitre.org/versions/v8/tactics/TA0002/)

Adding these techniques to our spreadsheet, our mapping looks something like the one below.

Intrusion 5

Indicator	Comment	ATT&CK Tactic v8	ATT&CK Technique v8
help(at)topenergysuport.com	Sender email for phish to T Johnson. "Signature" was "Top Energy Support Team."	Initial Access	T1566.002 Spearphishing Link
downloads.topenergysupport(dot)com	Malicious link in phish to T Johnson	Execution	T1204.001 Malicious Link

After mapping Intrusion 5 to ATT&CK, it's much easier to map Intrusion 6—we just need to be consistent. Using the keyword search and tactic-to-technique skimming methods, we determine the applicable techniques for Intrusion 6 include T1566.001 Spearphishing Attachment and T1204.002 Malicious File. It's important to remember that not every indicator or behavior will have an ATT&CK tactic and technique. Additionally, we see that there are techniques covering protocols in ATT&CK, but we don't yet know the protocol the IP address from the Poison Ivy malware config data uses, so we can identify that as a gap for now.

Intrusion 6

Indicator	ATT&CK Tactic v8	ATT&CK Technique v8
alayos(at)supplydenn.com	Initial Access	T1566.001 Spearphishing Attachment
Invoice.docx	Execution	T1204.002 Malicious File
Poison Ivy	N/A	N/A
Document2.pdf	N/A	N/A
38.72.115.9	N/A	Intelligence gap, not sure what protocol this IP uses

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets
Technet24

We have now successfully mapped all six intrusions to the Kill Chain, the Diamond Model, and ATT&CK. An example of a completed spreadsheet called "Ex 2.1 Intrusion Analysis – Completed" is available in your Ex 2.1 folder. This is just one example of how you could complete this analysis. Please note you will revisit these indicators and build upon this view throughout Section 2's exercises.

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets

Exercise: Key Takeaways

- **By mapping to the Kill Chain, Diamond Model, and MITRE ATT&CK, we organized information about six intrusions. We also identified gaps that may be useful for future analysis. We learned that mapping to these frameworks isn't always an easy task and requires an analyst to carefully consider how information applies. We also learned that there is flexibility in how to apply these frameworks and models.**

  We successfully analyzed information about the six intrusions that will serve as the foundation for future analysis throughout Section 2.

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets
Technet24

Exercise 2.2: Pivoting to Network Data with Indicators

Objectives

- Pivot from one data source to another leveraging indicators
- Identify and categorize any new indicators
- Determine where to pivot next to follow the intrusion

Scenario: You have several indicators to work with from your previous analysis of external scans and received emails, and now you need to determine if any of them have been found inside the network. Pivoting to the indicator(s) will ideally yield a path forward to investigating if SpaderTech has been compromised.

SpaderTech is currently working on a number of high-profile research efforts, including development of new nanotechnologies and the development of new control system equipment for a few power companies.

Exercise Prep

Students will utilize the SIFT VM. The file needed for this exercise is the packet capture in the **Ex 2.2** folder inside the **FOR578 Exercises** folder that was placed on the SIFT VM Desktop.

The following indicators from your Exercise 2.1 analysis will be useful to you, as you want to determine if they are in your network packet capture:

- 89.34.237.11
- 51.11.247.89
- 21.50.50.23
- 104.224.166.148
- 38.72.115.9

Additionally, there is a network map available in the **Ex 2.2** folder that can be used in any of the Section 2 labs.

Please note: For students new to Wireshark, please follow the Step-by-Step guide to optimize your time in class. This will allow you to learn new tools while also performing analysis pertinent to our investigation.

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets

Exercise: Questions

1. Which indicator(s) are present in the packet capture?

- _____

2. What is the victim system(s)?

- _____

3. What appears to be occurring between the indicator(s) and the target system(s)?

- _____

4. Is there any other malicious or suspicious activity occurring and if so between what systems?

- _____

5. Document any new indicators.

- _____

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets

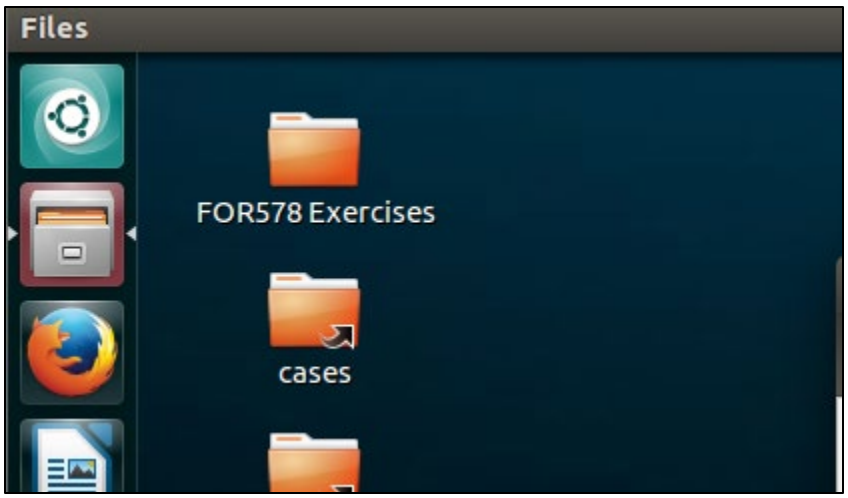
Technet24

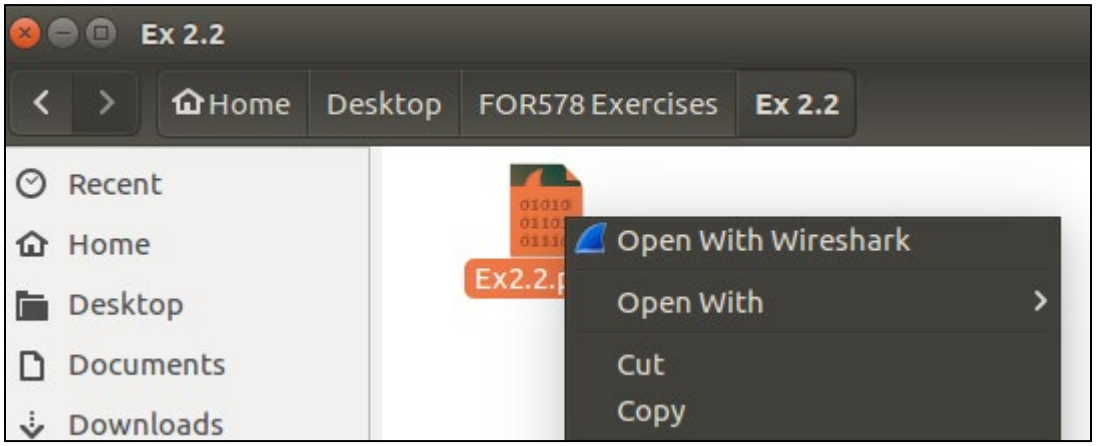
Exercise: Questions with Step-by-Step

1. Which indicator(s) are present in the packet capture?

- **51.11.247.89, which is being tracked as Intrusion 2**

In the **SIFT VM,** open the **FOR578 Exercises** folder on the Desktop and then open the **Ex2.2.pcap** in Wireshark by right-clicking the file and choosing **Open With Wireshark.**

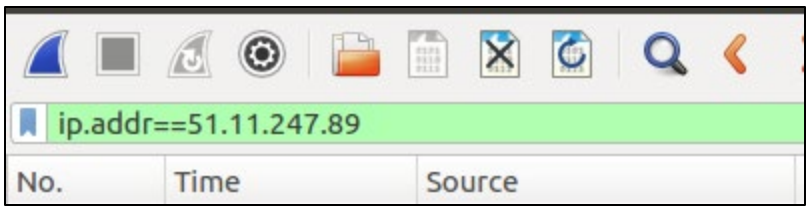




In the packet capture filter bar, enter **ip.addr==** followed by the IP address you want to search for and hit **Enter**. Search individually for each of the IP addresses from Exercise 2.1 (listed above). Note that the filter bar turns green when Wireshark recognizes the search as well-formed. Eventually, you will try out **ip.addr==51.11.247.89** which is present. You will not find the IP addresses 89.34.237.11, 21.50.50.23, 104.224.166.148, or 38.72.115.9 in the packet capture.

© 2021 Robert M. Lee and SANS Institute

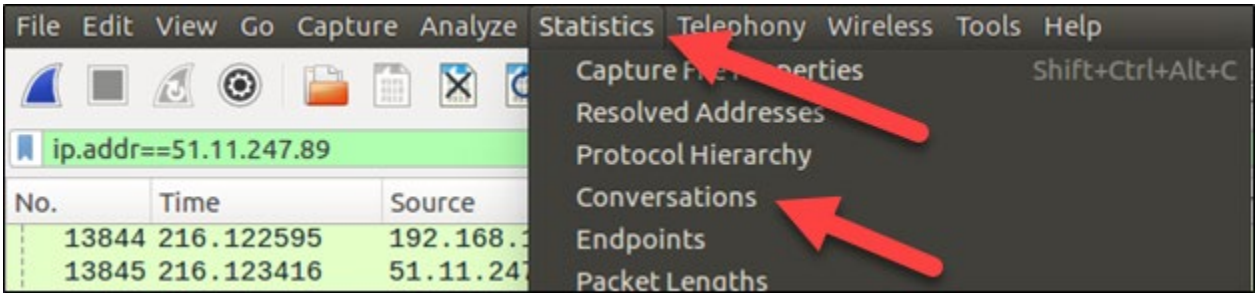
https://t.me/learningnets

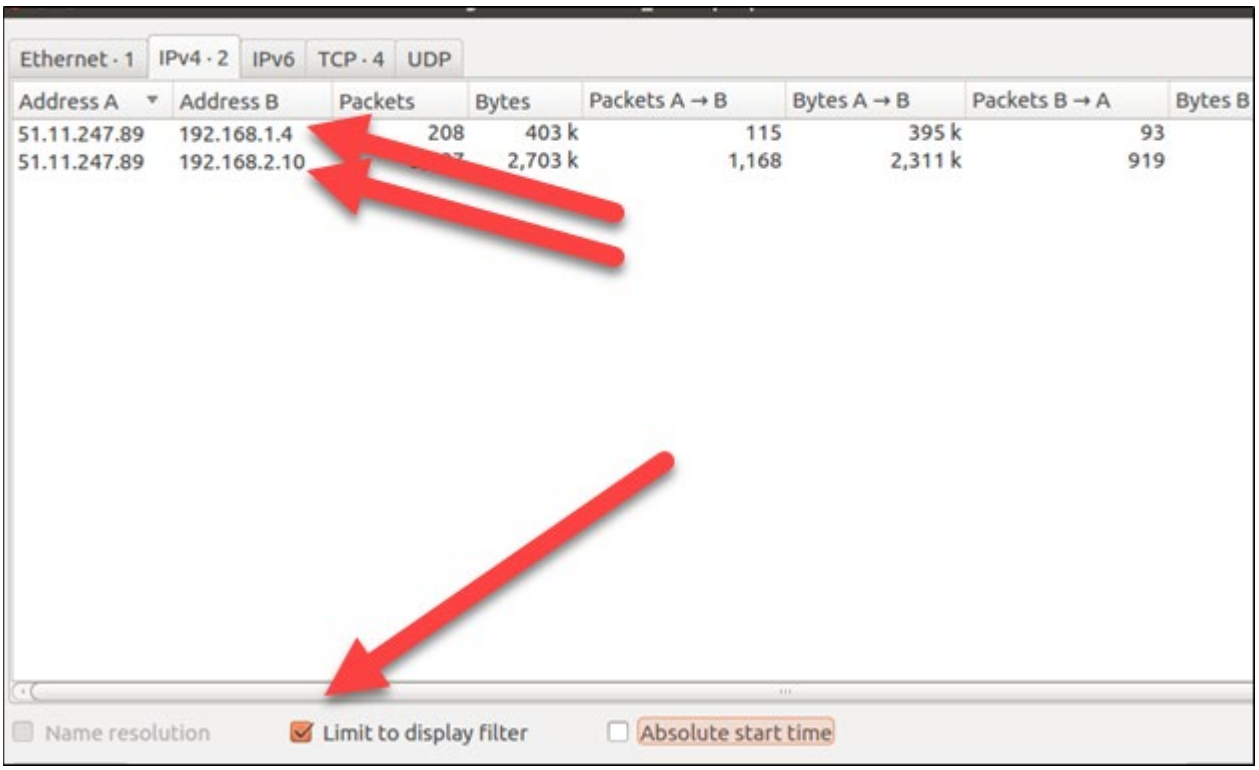


2. What is the victim system(s)?

- **192.168.2.10**

There are two IP addresses communicating to 51.11.247.89 that are viewable with results from the **ip.addr ==** filter from the last question. The first is 192.168.1.4 and the second is 192.168.2.10, which you could see from scrolling through the packet results, but that would take a while. You could more easily view that those two are the only IP addresses communicating by navigating to **Statistics** in the top menu, then selecting **Conversations** and applying the **Limit to display filter** at the bottom of the window. This quickly filters which IP addresses are present in the packet capture that are communicating to 51.11.247.89.

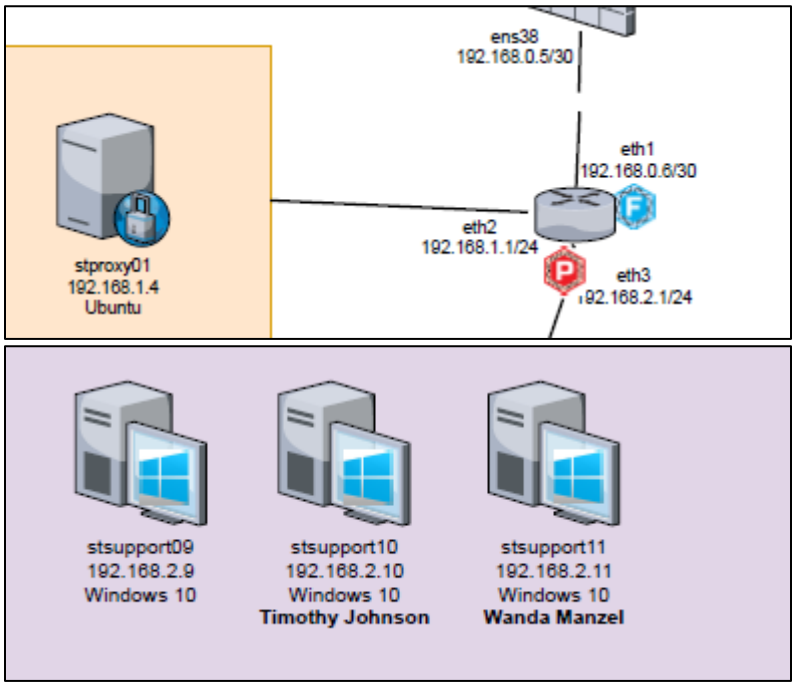




© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets
Technet24

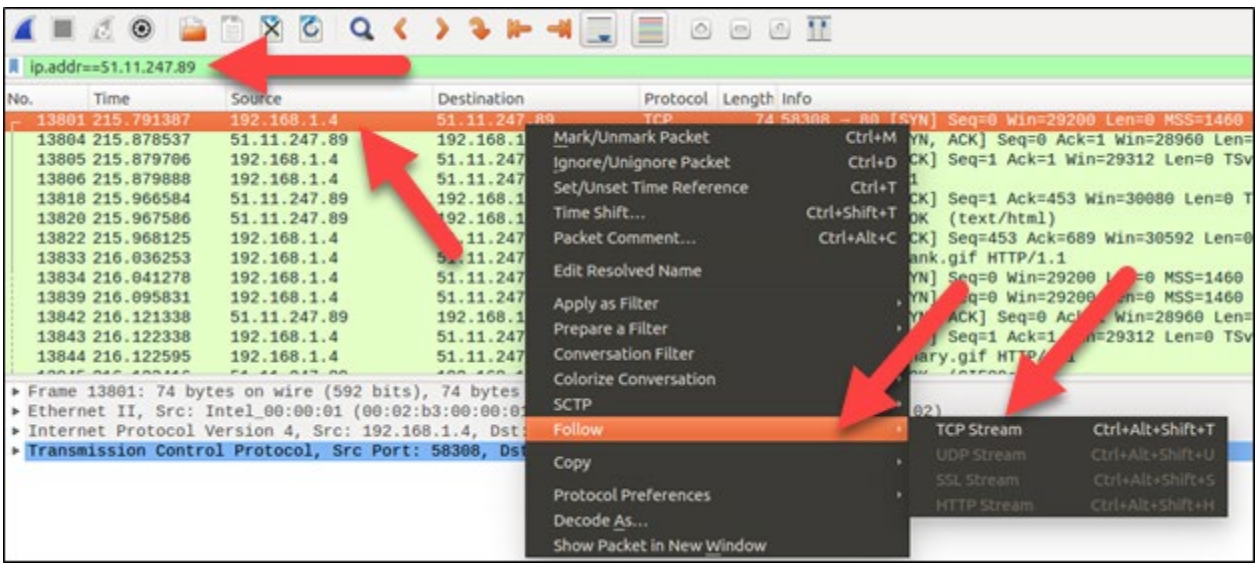
With a quick review of the network map, we can determine that 192.168.1.4 is a proxy and not a victim system. 192.168.2.10 is Timothy Johnson's computer, which is interesting as he also received phishing emails (as we know from Exercise 2.1).



3. What appears to be occurring between the indicator(s) and the target system(s)?

- **It appears the user clicked on the malicious link in the phishing email, which established a connection with 51.11.247.89.**

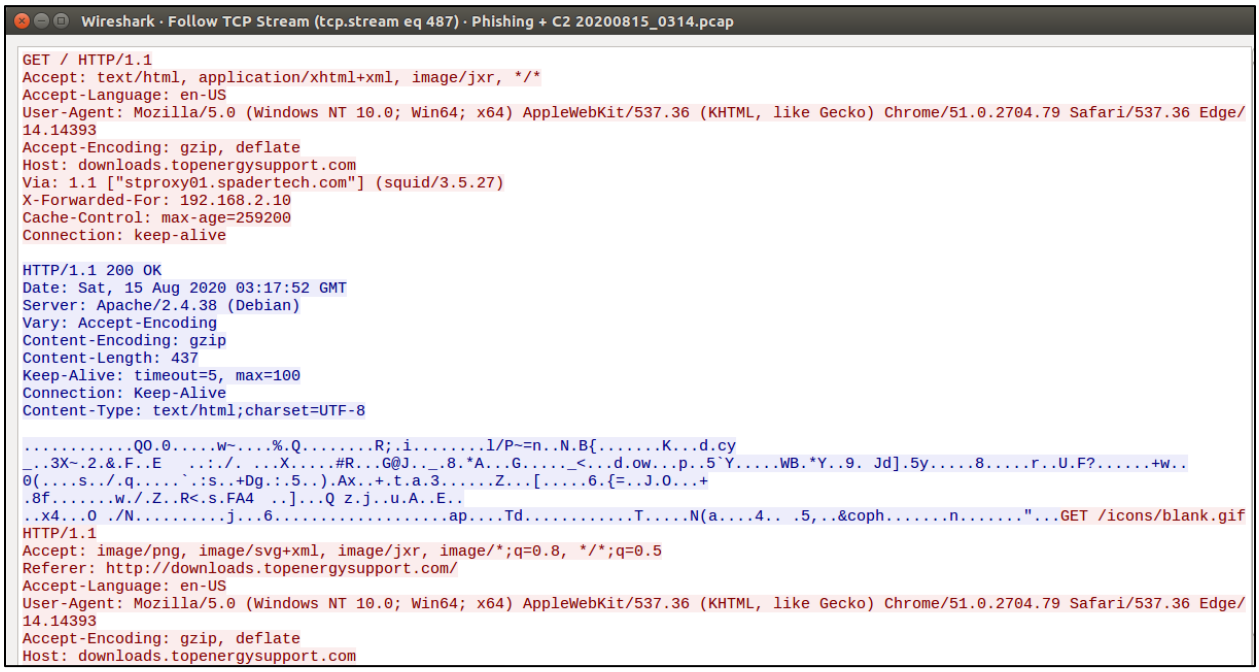
There are several different ways to analyze the data to determine what is occurring. One approach is to close the conversations statistics window, return to the 51.11.247.89 IP address filter, and right-click the first packet in the communication and choose **Follow** and **TCP Stream**.



© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets

This will display the contents of the stream.



Here, we can see that the IP address 51.11.247.89, the destination of this packet, is associated with the domain downloads.topenergysupport(dot)com, which we previously saw in one of the phishing emails. This presents a connection between the 51.11.247.89 that was scanning with the phishing email linking the intrusion stages we've observed together.

Our analysis of this stream is that it appears that the user probably clicked on the phishing email's link and established a connection with it through the proxy.

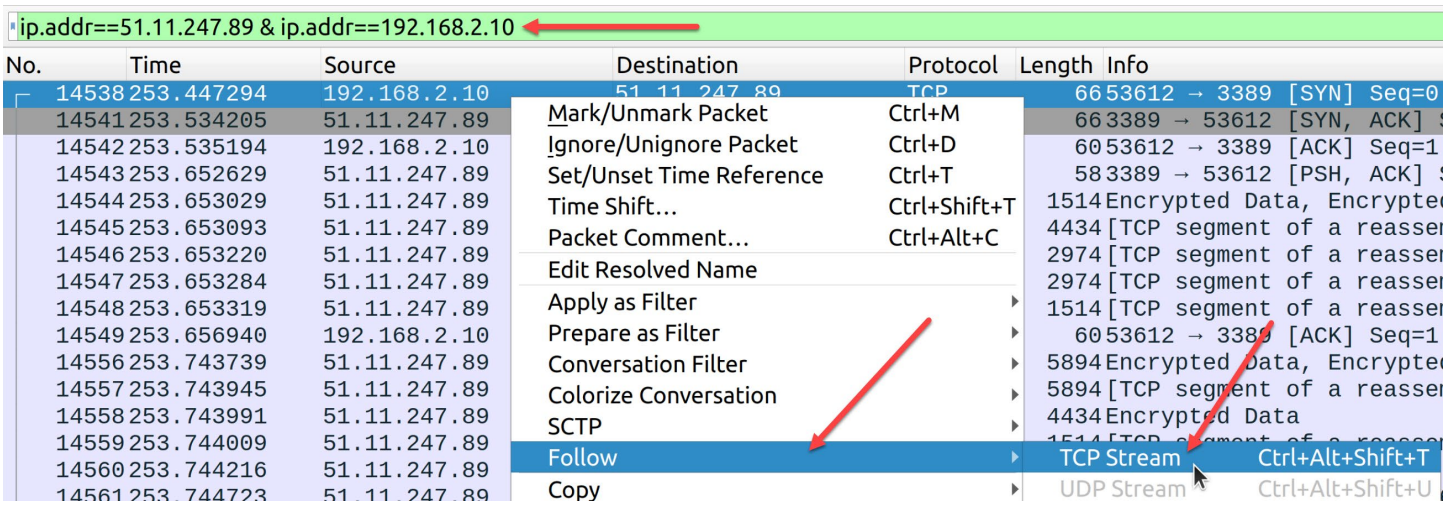
4. Is there any other malicious or suspicious activity occurring and if so between what systems?

- **The user installed an executable themed to be a VNCViewer application, which established a remote connection to the adversary's server 51.11.247.89.**

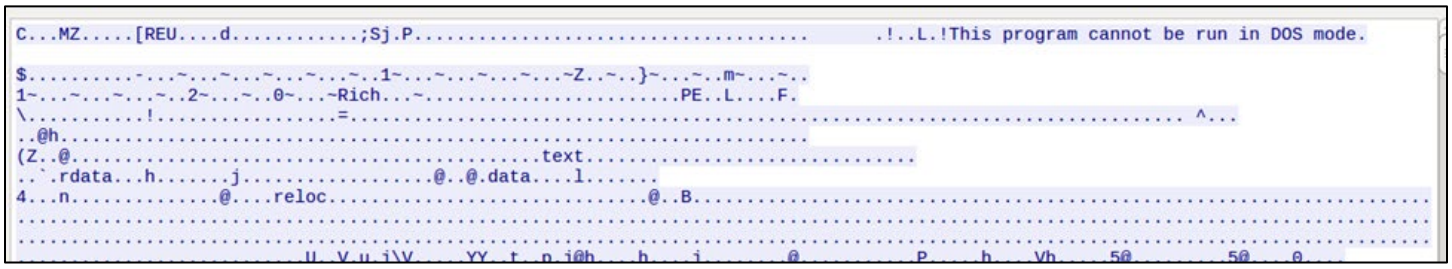
Again, there are a number of different ways to view the data. Since we want to look for activity to the suspicious IP from the second system, 192.168.2.10, we can filter on only packets to and from that IP address and the suspicious 51.11.247.89 IP. Filter on both IP addresses by filtering for **ip.addr==51.11.247.89 & ip.addr==192.168.2.10** and then choose a packet for further analysis. Right-click and select **Follow** and **TCP Stream** like we did before.

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets
Technet24



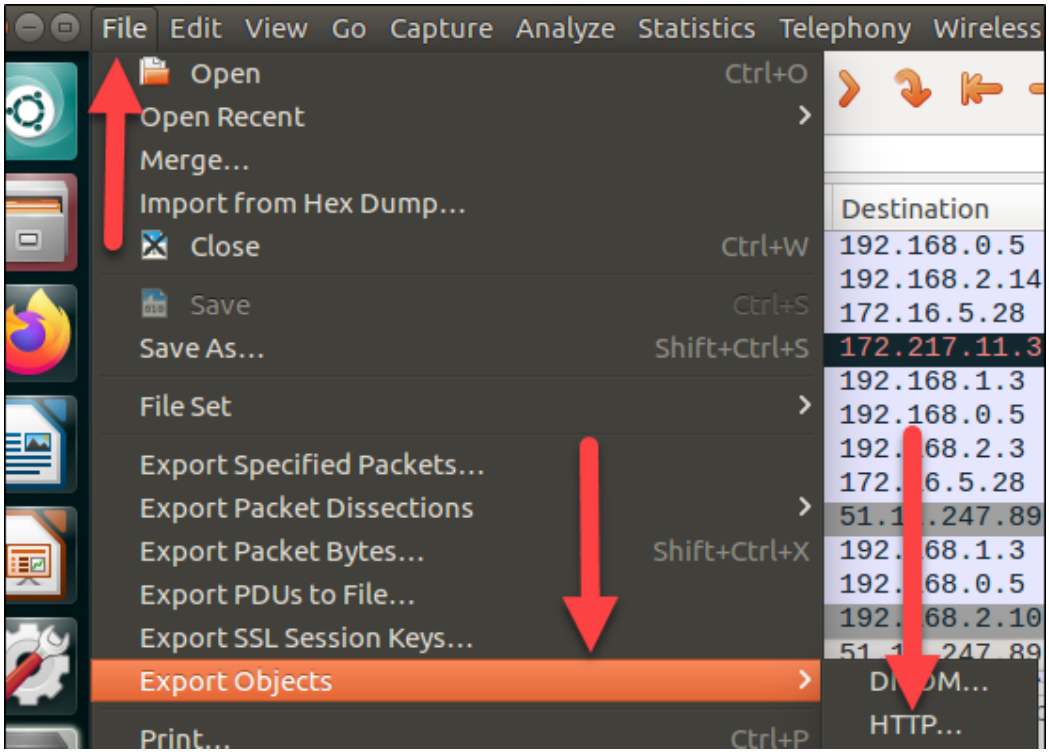
We are presented with the contents of the session, which clearly show an MZ header with "!This program cannot be run in DOS mode" which means that an executable was transferred to the victim system.



© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets

We can then go to **File** and **Export Objects** and choose **HTTP** to see if there are any files that we can pull out of the packet capture.



In reviewing the files, we see that downloads.topenergysupport(dot)com has downloaded a few files. The one that stands out the most is “vncviewer_v3.38.9_tcp.exe”.

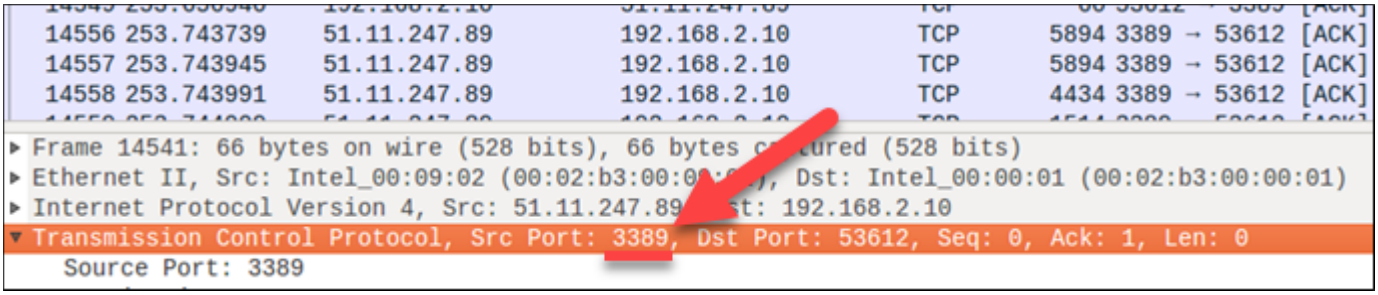


We can pass these to our internal reverse engineering team to determine what all the files do. Based on the network traffic we’ve observed so far, though, it is a fair assessment that the phishing email was delivered to Timothy Johnson, who clicked on the email’s malicious link which reached out through the proxy to the adversary’s website. After downloading the VNC Viewer file and installing it, a connection was established directly to the adversary’s server from Timothy Johnson’s computer.

Close out the **Follow TCP Stream** window. By clicking on any of the packets in the session between the two IP addresses, we can see that the TCP port used is 3389, which is the standard RDP port and was known to be open on the system from information presented in the last exercise.

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets
Technet24



5. Document any new indicators

- **vncviewer_v3.38.9_tcp.exe**

The only new indicator is the vncviewer_v3.38.9_tcp.exe file, which we will record because it may be a useful pivot point to further analyze this intrusion. In addition to identifying this new indicator, in this exercise we were able to link up the 51.11.247.89 Reconnaissance data with the phishing email from Top Energy Support and reasonably determine that the user of Timothy Johnson's system clicked on the link, downloaded the VNC Viewer application, which connected back to 51.11.247.89 for command and control and opened what appears to be an interactive session with Timothy Johnson's system.

If you are still using the Intrusion Indicators spreadsheet, you can collapse Intrusion 2 (or whatever Intrusion your 51.11.247.89 intrusion was) and Intrusion 5 (or whatever your Top Energy Support phishing email was). Further, you can note that the indicators are seen at multiple phases and multiple components of the Diamond Model and map to ATT&CK, similar to how you did in the previous exercise (since we want to be consistent with how we record information). Below is one example, though your analysis may look different.

	A	B	C
1	**Indicator**	**Comment**	**KC Phase**
2	51.11.247.89	Scanned external gateway for ports 443, 3389, 80 (ports 443, 3389 open)	Reconnaissance
3	help(at)topenergysuport.com	Sender email for phish to T Johnson. "Signature" was "Top Energy Support Team."	Delivery
4	downloads.topenergysupport(dot)com	Malicious link in phish to T Johnson	Delivery
5	vncviewer_v3.38.9_tcp.exe	Trojanized application downloaded from downloads.topenergysupport(dot)com	Installation

	D	E	F	G
1	**DM: Adversary**	**DM: Capability**	**DM: Infrastructure**	**DM: Victim**
2	N/A	Scanning	51.11.247.89	External Gateway
3	"Top Energy Support Team"	Phishing	help(at)topenergysuport.com	t.johnson(at)spadertech.com
4	"Top Energy Support Team"	Phishing	help(at)topenergysuport.com	t.johnson(at)spadertech.com
5	"Top Energy Support Team"	Trojanized Application	downloads.topenergysupport(dot)com	192.168.2.10

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets

	H	I
1	**ATT&CK Tactic v8**	**ATT&CK Technique v8**
2	Reconnaissance	T1595 Active Scanning
3	Initial Access	T1566.002 Spearphishing Link
4	Execution	T1204.001 Malicious Link
5	Defense Evasion	T1036.005 Match Legitimate Name or Location

Exercise: Key Takeaways

- **We analyzed packet capture to determine one of the IP addresses we were previously tracking was involved in network connections from a victim. We then determined that IP address was involved in two intrusions we previously tracked, so we combined those into one intrusion.**

- **We tracked new indicators and updated our analysis to reflect our updated understanding of the intrusions.**

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets
Technet24

Exercise 2.3: Pivoting to Memory with Indicators

Objectives

- Pivot from network data into a memory image using indicators
- Assist the forensics team with the investigation by pointing them in the right direction
- Determine the timeframe for the scope of the investigation

Scenario: At this point, you know Timothy Johnson's computer was likely compromised; the forensics team analyzed the vncviewer_v3.39.9_tcp.exe that you found in network traffic and found that it was trojanized to include Meterpreter, a common tool used by pen testers as well as adversaries.

The security team confirmed that there is no ongoing pen test right now, meaning this is likely an active intrusion, but you do not know much more than that. You now need to validate what you saw in the network traffic in the memory image and use that knowledge to identify anything more that could be used to help the forensics team. Many times, people go to forensics teams with a "forensicate this" mindset instead of laying out actual requirements. Your job here is to understand what more is needed and to get it to the forensics team.

SpaderTech executives want to know not only that a system was compromised but when the breach took place and what actions were taken by the adversary, including whether data was manipulated or stolen. This lab won't finalize all the pieces, but will start to pull the story together.

Exercise Prep

Students will utilize the SIFT VM. The file needed for this exercise is a memory image located in the **Ex 2.3** folder inside the **FOR578 Exercises** folder that was placed on the SIFT VM Desktop. The memory image is named "stsupport10-memory.dd4.001" and can be analyzed with Volatility.

Please note: For students new to the tool Volatility, please follow the Step-by-Step guide to optimize your time in class. This will allow you to learn new tools while also performing analysis pertinent to our investigation. You may also find this SANS Memory Forensics Cheat Sheet, which includes Volatility commands, to be useful: https://digital-forensics.sans.org/media/volatility-memory-forensics-cheat-sheet.pdf

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets

Exercise: Questions

1. Can you validate that vncviewer_v3.38 .9_tcp.exe successfully ran on the system? How is it communicating with the adversary?

   - _____

2. What suspect processes are running on the system and are there any relevant timestamps?

   - _____
   - _____
   - _____
   - _____

3. Where can we point forensic analysts to dig deeper to find more adversary activity?

   - _____

4. Document any new indicators and TTPs.

   - _____
   - _____
   - _____
   - _____
   - _____

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets

Technet24

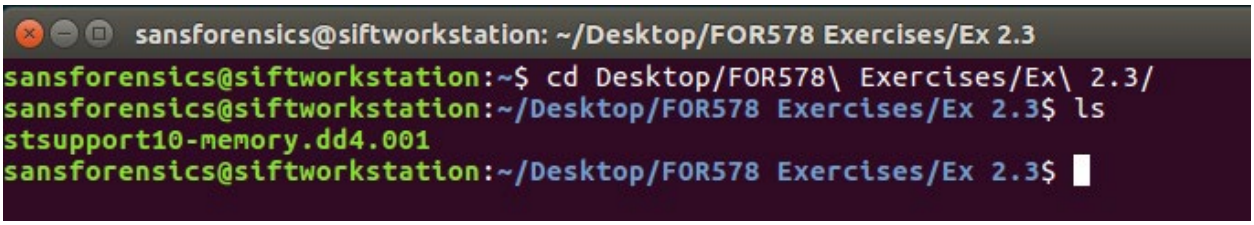
1. Can you validate that vncviewer_v3.38 .9_tcp.exe successfully ran on the system? How is it communicating with the adversary?

- **Yes, the process is running and communicating to 51.11.247.89 over port 3389**

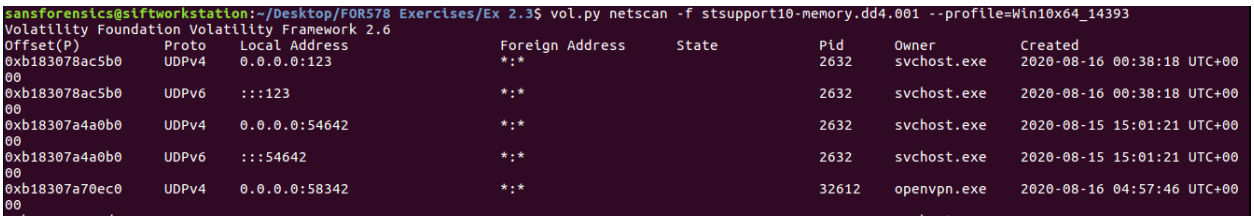
Normally when utilizing Volatility, one of the first commands that will be run is **imageinfo** to get the profile of the system which will allow the other plugins to correctly analyze the memory image. However, **imageinfo** is incredibly slow on this memory image, so to speed you along, please use the profile **Win10x64_14393**. Note that the profile command must be preceded by two dashes.

There are many ways to approach memory images to gather data. Since we know vncviewer_v3.38.9_tcp.exe was being utilized for network communications, we can start with the **netscan** plugin in Volatility.

In the SIFT VM, open up a terminal window (command line) and navigate to the Exercise 2.3 folder by typing the command (you can also use tab complete to navigate to the folder):
`cd Desktop/FOR578\ Exercises/Ex\ 2.3/`



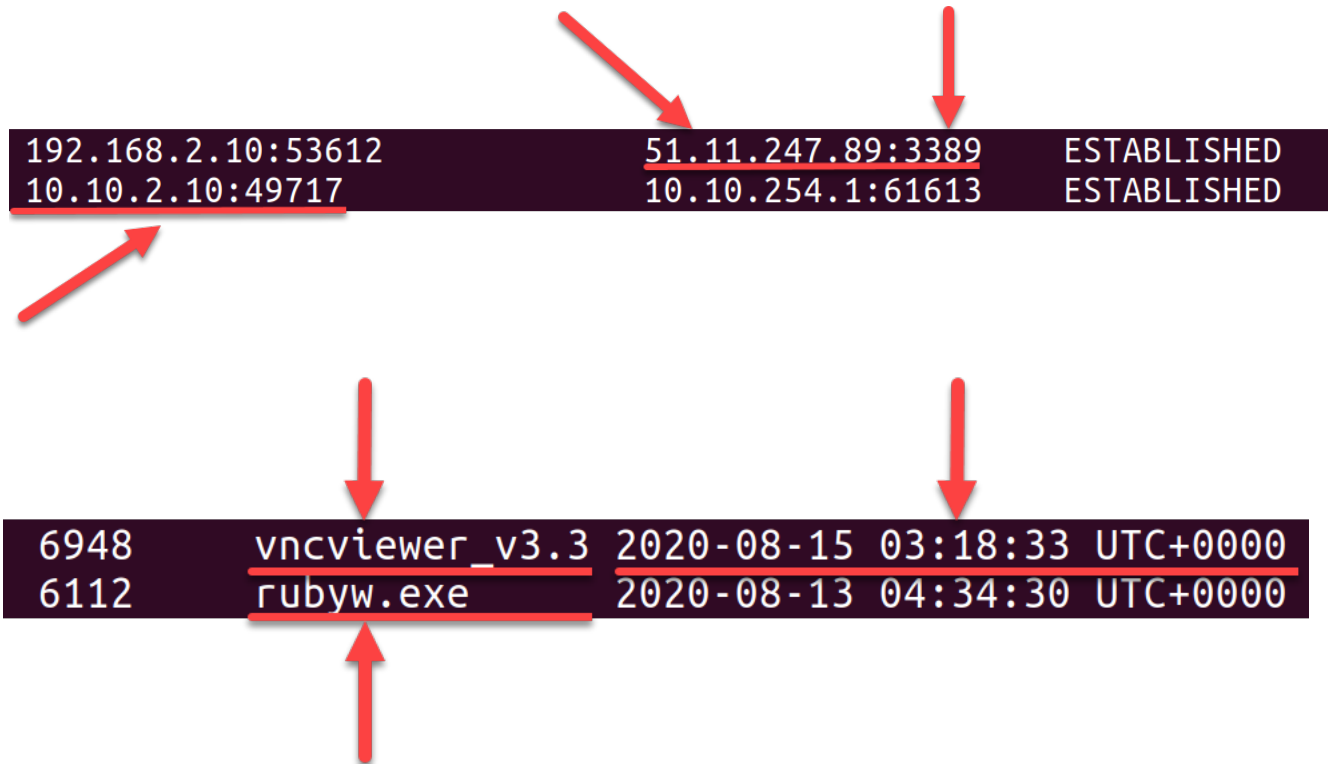
Next, run the **netscan** plugin on our memory image by typing the following command and pressing enter (the results will begin to return quickly, but it may take several moments to complete:
`vol.py netscan -f stsupport10-memory.dd4.001 --profile=Win10x64_14393`



In reviewing the results, we're trying to use the indicators we saw from the network data to find the relevant processes and information in the current data, the memory image. This output can be overwhelming, so to help us narrow down relevant network connections, we can look for process names or adversary IP addresses we already know about, including 51.11.247.89 and vncviewer_v3.3.89_tcp.exe. In our output, we see both (you should see the below commands on the same line; they are separated here for visibility):

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets



We see that the vncviewer_v3.3 process established its external connection to 51.11.247.89 over TCP port 3389, which matches up with what we saw in the network traffic. We also see that it was created at 2020-08-15 at 3:18:33 UTC. This can help us time scope the beginning of the investigation on the system. Interestingly, we also see a "rubyw.exe" that is communicating to 10.10.2.10 as an internal network. At this time, we're not going to dig deeper there, but we could flag that optionally for the forensics team to take a deeper look at.

2. What suspect processes are running on the system and are there any relevant timestamps?

- **vncviewer_v3.3 which was created at 2020-08-15 03:18:33 UTC and exited at 2020-08-15 04:26:64_UTC**
- **cmd.exe which was created at 2020-08-16 04:53:28 UTC and_exited at 2020-08-16 05:27:17_UTC**
- **cmd.exe which was created at 2020-08-16 05:27:43 UTC and exited at 2020-08-16 5:51:49 UTC**
- **Two different ipconfig.exe processes with the latest being created at 2020-08-16 04:46:59 UTC and exiting at 2020-08-16 04:46:59 UTC**

There are a variety of plugins in Volatility that will help you find the running processes. There is a **timeliner** plugin that can create a timeline if we want to be very accurate; however, for the purpose of quickly triaging the memory image, we'll utilize the **pslist** plugin and see if there's any obvious thing there.

Run the command:

```
vol.py pslist -f stsupport10-memory.dd4.001 --profile=Win10x64_14393
```

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets
Technet24

```
sansforensics@siftworkstation: ~/Desktop/FOR578 Exercises/Ex 2.3
sansforensics@siftworkstation:~/Desktop/FOR578 Exercises/Ex 2.3$ vol.py pslist -f stsupport10-memory.dd4.001 --profile=Win10x64_14393
Volatility Foundation Volatility Framework 2.6
Offset(V)          Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Start                          Exit
------------------ -------------------- ------ ------ ------ -------- ------ ------ ------------------------------ ------------------------------
0xffffb183076b0040 System                     4      0    109        0 ------      0 2020-08-13 04:33:54 UTC+0000
0xffffb1830846a040 smss.exe                 352      4      2        0 ------      0 2020-08-13 04:33:54 UTC+0000
0xffffb1830adfd080 csrss.exe                652    636     10        0      0      0 2020-08-13 04:34:10 UTC+0000
0xffffb1830abff080 smss.exe                 772    352      0 --------      1      0 2020-08-13 04:34:11 UTC+0000   2020-08-13 04:34:11 UTC+0000
0xffffb1830adc6080 wininit.exe              780    636      1        0      0      0 2020-08-13 04:34:11 UTC+0000
0xffffb1830b12e080 csrss.exe                792    772     13        0      1      0 2020-08-13 04:34:11 UTC+0000
0xffffb1830b171080 winlogon.exe             976    772      2        0      1      0 2020-08-13 04:34:11 UTC+0000
0xffffb1830b1c2080 services.exe             392    780      5        0      0      0 2020-08-13 04:34:11 UTC+0000
0xffffb1830b1dc740 lsass.exe                796    780     10        0      0      0 2020-08-13 04:34:11 UTC+0000
0xffffb1830b1b6800 svchost.exe             1416    392     17        0      0      0 2020-08-13 04:34:11 UTC+0000
0xffffb1830b1ac800 svchost.exe             1632    392     10        0      0      0 2020-08-13 04:34:12 UTC+0000
0xffffb1830ba13080 dwm.exe                 2024    976     11        0      1      0 2020-08-13 04:34:12 UTC+0000
0xffffb1830b1a6800 svchost.exe             2312    392     41        0      0      0 2020-08-13 04:34:13 UTC+0000
0xffffb1830b1a2800 svchost.exe             2320    392     62        0      0      0 2020-08-13 04:34:13 UTC+0000
0xffffb1830baeb800 svchost.exe             2488    392     26        0      0      0 2020-08-13 04:34:13 UTC+0000
0xffffb1830bae5800 svchost.exe             2500    392     16        0      0      0 2020-08-13 04:34:13 UTC+0000
0xffffb1830bacf800 svchost.exe             2632    392     30        0      0      0 2020-08-13 04:34:13 UTC+0000
0xffffb1830bacb800 svchost.exe             2732    392     19        0      0      0 2020-08-13 04:34:13 UTC+0000
0xffffb1830bce9580 svchost.exe             4856    392      4        0      0      0 2020-08-13 04:34:14 UTC+0000
0xffffb1830b04c800 svchost.exe             5144    392      9        0      0      0 2020-08-13 04:34:15 UTC+0000
0xffffb1830ae0b280 spoolsv.exe             5552    392     11        0      0      0 2020-08-13 04:34:15 UTC+0000
0xffffb1830af05580 rubyw.exe               6112    392     10        0      0      0 2020-08-13 04:34:17 UTC+0000
```

Then, look through the process list for anything that stands out as particularly interesting. First, we see that there are some OpenVPN processes running but those don't seem immediately suspicious; we would expect there to be VPN software on the system and it doesn't overlap with what the adversary was doing. For now, we will flag them as an item to ask our administrators about, but based on the timestamp, it doesn't seem like they are relevant. When doing investigations, sometimes we have to triage what is *most likely* to be suspicious since it would be difficult to validate every single one of these processes.

```
SearchUI.exe          21304   1416     36        0      1      0 2020-08-13 04:44:30 UTC+0000
vmtoolsd.exe          22240  19276      5        0      1      0 2020-08-13 04:44:44 UTC+0000
OneDrive.exe          22972  19276     15        0      1      1 2020-08-13 04:44:45 UTC+0000
openvpnserv.ex        23536    392      3        0      0      0 2020-08-13 04:45:41 UTC+0000
openvpn-gui.ex        18880  19276      3        0      1      0 2020-08-13 04:48:38 UTC+0000
mstsc.exe             15076  19276     13        0      1      0 2020-08-13 04:52:15 UTC+0000
dllhost.exe           19932   1416      2        0      1      0 2020-08-13 04:54:38 UTC+0000
```

A good strategy is to search for previous indicators and TTPs we know about, as well as looking for activity in the time frame of our malicious activity. As we try this strategy, we then see the vncviewer_v3.3 process running and can identify that it was created on 2020-08-15 at 3:18:33 UTC and exited the same day at 04:26:04. This gives us a really useful window of time of a little over an hour that the adversary was likely using that process. However, that's not very long and past experience working intrusions would tell any reasonable analyst that unless the adversary was caught or antivirus or similar exited the process, it's not likely the adversary would complete their objective in an hour and exit their process. We'd keep looking through the processes anyway, but this makes our search more likely to yield something useful.

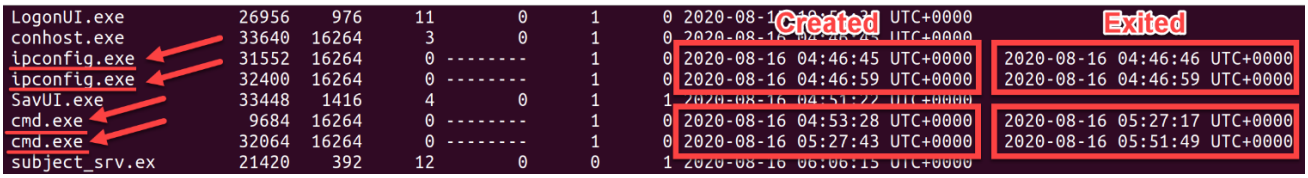
```
Taskmgr.exe           32248  19276     16        0      1      0 2020-08-15 03:13:09 UTC+0000
MicrosoftEdgeC        28584  19236     20        0      1      0 2020-08-15 03:17:55 UTC+0000
vncviewer_v3.3         6948  18716      0 --------      1      1 2020-08-15 03:18:33 UTC+0000   2020-08-15 04:26:04 UTC+0000
MicrosoftEdgeC        29884  19236      0 --------      1      0 2020-08-15 14:33:16 UTC+0000   2020-08-15 14:50:05 UTC+0000
MicrosoftEdgeC        26856  19236     23        0      1      0 2020-08-15 14:49:03 UTC+0000
MicrosoftEdgeC        30620  19236     31        0      1      0 2020-08-15 14:52:51 UTC+0000
```

Since we believe that vncviewer_v3.3 process is suspicious, it's a good idea to look for any other suspicious-looking processes that occur after it based on timestamp. We see cmd.exe running as well as ipconfig.exe. Unless the user was running the command line themselves and checking their ipconfig data themselves, this is something that is likely adversary related, so we will note it as suspicious, but we should check with our administrators later to make sure they didn't perform this activity. It's important to remember that cmd.exe and ipconfig.exe won't always be malicious, but this time, they stand out as particularly relevant. Also, cmd.exe and ipconfig.exe have the parent process ID (PPID) of

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets

16264 as does conhost.exe (which we could document, but we already have enough information at this time).



ipconfig.exe and cmd.exe were both created on the 16th, the day after the vncviewer_v3.3 process was created. The first cmd.exe was created at 04:53:28 UTC and exited at 05:27:17 UTC, the ipconfig.exe processes were run at 04:46:59 and exited immediately, and another cmd.exe was created at 05:27:43 and exited the same day at 05:51:49. This is all suspicious activity worth further investigation and can help the forensic analysts as they look deeper into the memory or disk image. Our initial analysis creates a scoped time window of investigation.

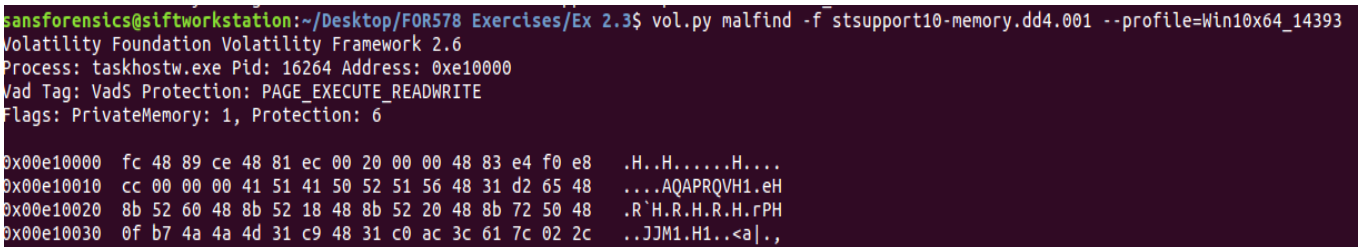
The obvious answer, though, is to look at the PID of 16264 and determine what that is. We could take that approach, but instead we will try a different tactic in the next question.

3. Where can we point forensic analysts to dig deeper to find more adversary activity?

- Users\t.johnson\AppData\Local\Temp\Low

One plugin we can use is **malfind**, which looks for suspicious activity such as code that looks like executables such as DLLs or shellcode inside of running processes. Because we feel comfortable that the adversary had a running process on the system, and that it exited but that the adversary likely remained, we can assess that there is potentially another persistence mechanism for the adversary.

Run the command:
`vol.py malfind -f stsupport10-memory.dd4.001 --profile=Win10x64_14393`



The first process that is identified by **malfind**, and is flagged multiple times (as we can observe as we scroll down the output), is taskhostw.exe. The normal process by the same name, taskhostw.exe, is common in Windows environments to manage the Task Host, which is used in a number of places including the execution of DLLs and making sure that programs are closed properly when the system is shut down. However, there is something odd going on with taskhostw.exe.

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets
Technet24

```
Process: taskhostw.exe Pid: 16264 Address: 0x2d52ad70000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: PrivateMemory: 1, Protection: 6

0x000002d52ad70000  4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00   MZ..............
0x000002d52ad70010  b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00   ........@.......
0x000002d52ad70020  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0x000002d52ad70030  00 00 00 00 00 00 00 00 00 00 00 00 e8 00 00 00   ................

0x000000002ad70000 4d               DEC EBP
0x000000002ad70001 5a               POP EDX
0x000000002ad70002 90               NOP
```

Continuing to review the malfind output, we can clearly see that taskhostw.exe, with the process ID (PID) 16264, has an executable (denoted by the MZ header) embedded inside of it. We will pass this to the forensics team so that the malware reverse engineers can look at it and see if there's anything important about that executable.

It looks like this process, PID 16264, is our other malicious process running on the system and could be connected to the initial intrusion. Timestamps and other forensic analysis would be required to really validate this is connected and not a remnant of a previous intrusion, but in the scenario it is safe to proceed with the assumption that it is connected.

To really find out what's going on, though, we could either carve out the executable to see what it is or to see if there are any relevant handles in the process. A simplistic way to look at handles in this context is that they will allow us to see if there are actions being taken by this process that can help us piece together the context on what is occurring. We will use the **handles** plugin in Volatility and focus it on the PID 16264 with the -p flag.

Run the command:

```
vol.py handles -p 16264 -f stssupport10-memory.dd4.001 --
profile=Win10x64_14393
```

```
sansforensics@siftworkstation:~/Desktop/FOR578 Exercises/Ex 2.3$ vol.py handles -p 16264 -f stsupport10-memory.dd4.001 --profile=Win10x64_14393
Volatility Foundation Volatility Framework 2.6
Offset(V)          Pid      Handle              Access Type            Details
------------------ ------ ---------- ---------------------------- -------
0xffffb1830a876140  16264        0x4          0x1f0003 Event
0xffffb1830a86f170  16264        0x8               0x1 WaitCom...Packet
0xffffb1830a82e940  16264        0xc          0x1f0003 IoCompletion
```

```
16264  0xe00   0x20019 Key     MACHINE\SOFTWARE\MICROSOFT\POWERSHELL\1\SHELLIDS
16264  0xe04   0x1f0003 Event
16264  0xe08   0x1f0003 Event
16264  0xe0c   0x1f0003 Event
16264  0xe10   0x1f0003 Event
16264  0xe14   0x1fffff Thread  TID 15068 PID 16264
16264  0xe4c   0x1f0001 ALPC
16264  0xe54   0x1fffff Process cmd.exe(32064)
16264  0xe58    0xf01ff Token
16264  0xe68   0x1fffff Thread  TID 32440 PID 16264
16264  0xe6c   0x1fffff Process cmd.exe(9684)
16264  0xe74   0x100020 File    \Device\HarddiskVolume2\Users\t.johnson\AppData\Local\Temp\Low
```

Reviewing the output, we will see a lot of details. The first thing that stands out is the use of PowerShell, a common Windows utility that is also commonly taken advantage of by adversaries. Seeing it in this suspicious process helps confirm that the adversary is attempting to use PowerShell at least in some part of their intrusion. Additionally, we see the two different cmd.exe processes from earlier with the exact same PIDs as we saw in the **pslist** output (32064 and 9684); further confirming their connection to PID 16264. Lastly, we see a file created for user **t.johnson** at the filepath

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets

Users\t.johnson\AppData\Local\Temp\Low. The **Temp** folder is a common place for adversaries to take advantage of given that it has write privileges. This is exactly the type of information we can leverage to point our forensic analysts to and ask them to recover the contents of that file through disk forensics.

We can now ask our forensic experts to really hone in on vncviewer and taskhostw at PID 16264 to determine if they can confidently link them together, which will link the intrusion together for us and determine what activity the adversary is doing especially as it relates the **Temp** folder.

4. Document any new indicators and TTPs.

- **cmd.exe, ipconfig.exe, and taskhostw.exe**
- **Users\t.johnson\AppData\Local\Temp\Low**
- **T1059 Command and Scripting Interpreter**
- **T1016 System Network Configuration Discovery**
- **T1055 Process Injection**

As with most things indicator and TTP related, this is very much up to the analyst view on what they choose to abstract out of the intrusion for collection and documentation. Also, how you interpret the TTPs displayed can vary from analyst to analyst.

For one approach, the documentation of the four different (three unique names) processes make the most sense with the adversary file in the Temp folder. Using MITRE ATT&CK, we can capture the seemingly most relevant tactics and techniques. Since we want to quickly document information, we're not going to map to ATT&CK sub-techniques right now, though you could choose to capture the information differently. Our view on these could change over time depending on the context of the newly discovered information in the intrusion. It is important as an analyst to take notes and document what matters to you and not obsess about everything being perfect before you've concluded your investigation. (You could choose to place the Kill Chain, Diamond Model, and ATT&CK mappings in the same row; we have divided it below for easy of viewing.)

Indicator	KC Phase
cmd.exe	Actions on Objectives
cmd.exe	Actions on Objectives
ipconfig.exe	Actions on Objectives
taskhostw.exe	Actions on Objectives
Users\t.johnson\AppData\Local\Temp\Low	Actions on Objectives

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets
Technet24

Indicator	DM: Adversary	DM: Capability	DM: Infrastructure	DM: Victim
cmd.exe	Unknown	Process Creation	T.Johnson's Account	192.168.2.10
cmd.exe	Unknown	Process Creation	T.Johnson's Account	192.168.2.10
ipconfig.exe	Unknown	Process Creation	T.Johnson's Account	192.168.2.10
taskhostw.exe	Unknown	Evasion	T.Johnson's Account	192.168.2.10
Users\t.johnson\AppData\Local\Temp\Low	Unknown	Unknown	T.Johnson's Account	192.168.2.10

Indicator	ATT&CK Tactic	ATT&CK Technique
cmd.exe	Execution	T1059 Command and Scripting Interpreter
cmd.exe	Execution	T1059 Command and Scripting Interpreter
ipconfig.exe	Discovery	T1016 System Network Config Discovery
taskhostw.exe	Defense Evasion	T1055 Process Injection
Users\t.johnson\AppData\Local\Temp\Low	Unknown	Unknown

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets

Exercise: Key Takeaways

- **Pivoting from network data into a memory image using Volatility allowed us to scope our intrusion and identify new indicators and TTPs.**

- **Our initial analysis identified multiple items of interest, including a folder as well as a timeframe, which will point our forensics team in the right direction as they conduct further analysis.**

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets
Technet24

Exercise 2.4: Understanding the Actions on Objective in an Intrusion

Objectives

- Wrap up the investigation into the intrusion by analyzing the adversary's actions on objective
- Document what the impact of the adversary was
- Record key indicators and TTPs

Scenario: The forensic team came back with some additional information after you were able to direct them to the right locations in the system memory and disk. They determined that the adversary initially compromised T.Johnson's system utilizing Meterpreter and then proceeded to use it, PowerShell, and native Windows tools to perform system and network reconnaissance. They were also able to positively identify that the adversary migrated the vncviewer process to the taskhostw.exe process (performing process injection), which was the malicious process we previously viewed. They were able to amplify this conclusion by noting that the executable we found in taskhostw.exe was also Meterpreter, which the vncviewer_3.38.9_tcp.exe also used.

They were able to find one more unique indicator. The Temp file we found contained T.Johnson's credentials that were dumped from lsass.exe and there is an file named out.rar that they were able to recover. However, they do not know the contents and it is password protected.

The forensic analysts would like to know if there are any keywords that could be used for trying to crack the password on out.rar or if we can determine what data might be in the rar file. This overlaps with the request of the executives to know the impact of the breach.

Exercise Prep

Students will utilize the SIFT VM to analyze a packet capture and memory image. The packet capture is a new file whereas the memory image is the same one we previously analyzed. Both are located in the **Ex 2.3** folder inside the **FOR578 Exercises** folder that was placed on the SIFT VM Desktop.

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets

Exercise: Questions

1. Are there any other potentially compromised systems on the network?

- _____

2. Are there any files of interest that the adversary likely accessed?

- _____

3. What is the password for out.rar?

- _____

4. Document any new indicators and TTPs.

- _____
- _____
- _____
- _____
- _____

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets

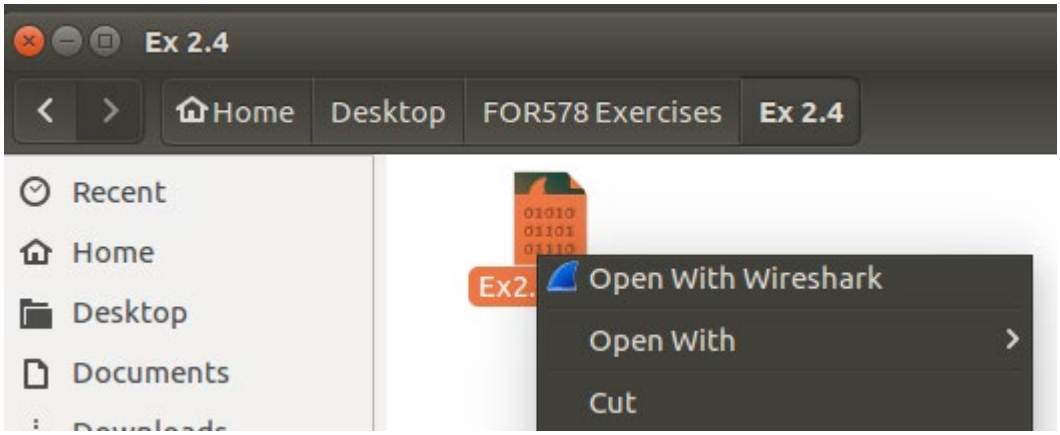
Technet24

Exercise: Questions with Step-by-Step

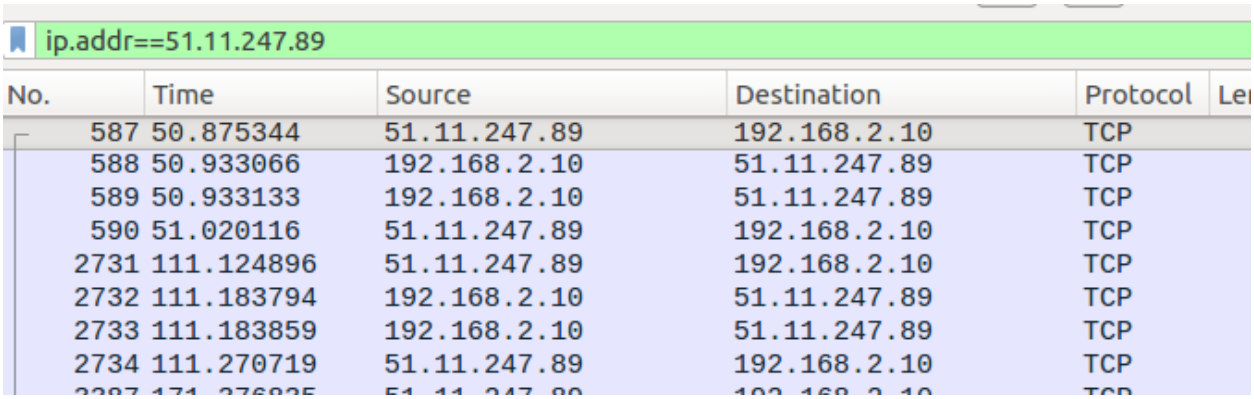
1. Are there any other potentially compromised systems on the network?

- **10.0.1.13 and 10.0.1.12**

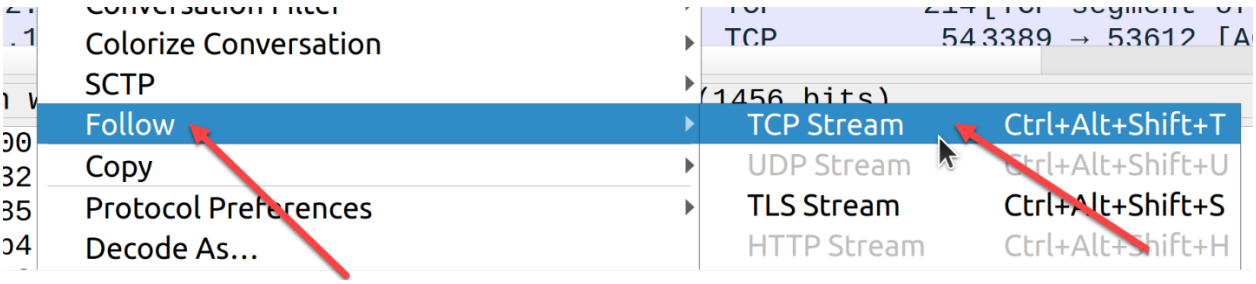
Navigate to the **FOR578 Exercises** folder, open the **Ex 2.4** folder, and then right-click on **Ex2.4.pcap** and select **Open With Wireshark.**



In the packet capture filter bar, enter **ip.addr==51.11.247.89** and hit **Enter**. Note that the filter bar turns green when Wireshark recognizes the search as well-formed.

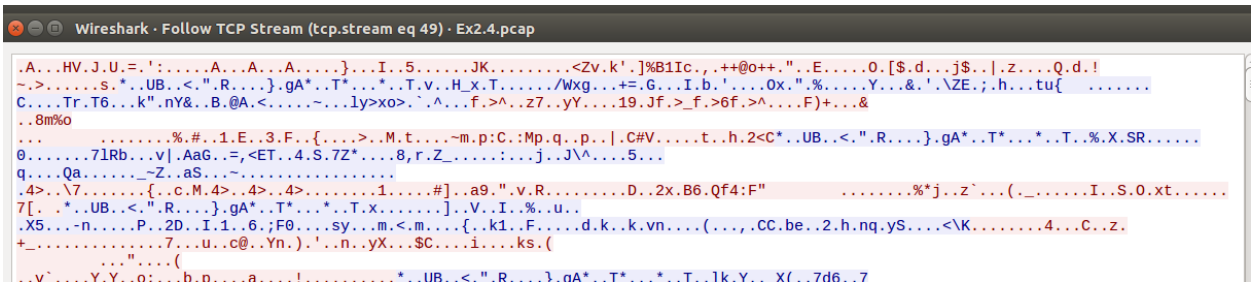


Follow one of the streams by right-clicking a packet (represented in individual rows) and then choosing **Follow** and **TCP Stream**.



© 2021 Robert M. Lee and SANS Institute

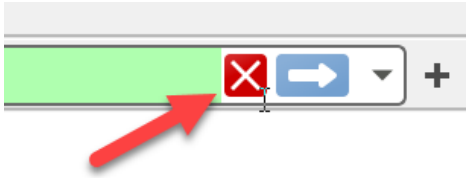
https://t.me/learningnets



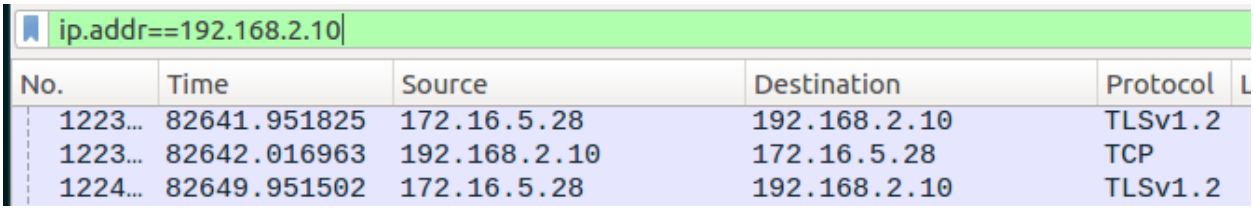
As we could reasonably expect, the packet capture looks encrypted or at least obfuscated.

Following streams is not going be as effective this time around. What matters most is what systems are being targeted. So instead of pivoting off the adversary infrastructure, we can pivot off of the victim infrastructure.

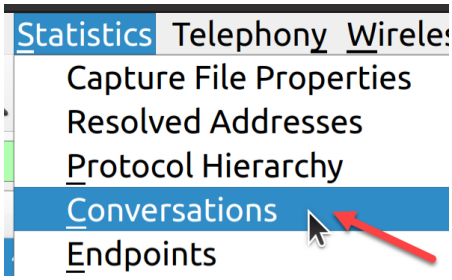
Exit out of the **Follow TCP Stream** window and clear your current selection by clicking the **Clear display filter** icon at the right of the filter bar.

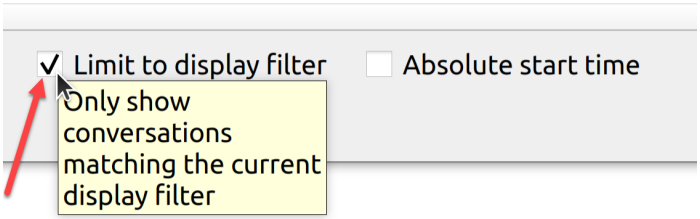


Next, filter on one of your victim IP addresses by entering the following into the filter:
`ip.addr==192.168.2.10`



Go to **Statistics** and choose **Conversations** and then check the **Limit to Display** filter at the bottom of the screen that pops up.

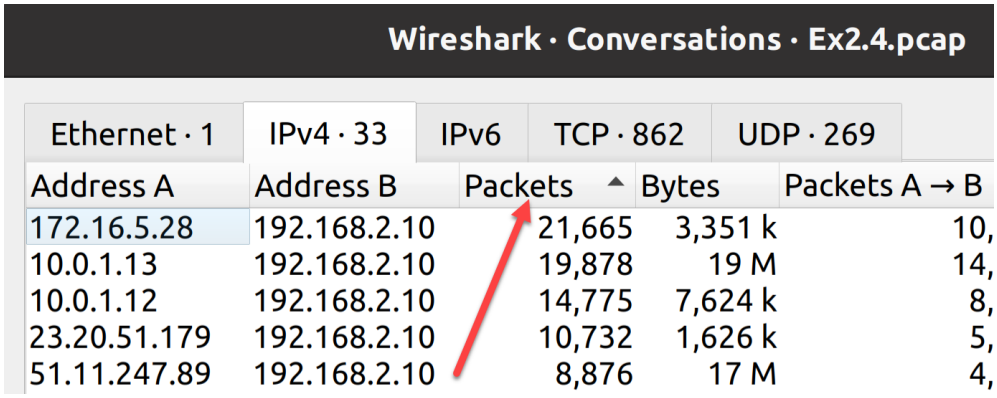




© 2021 Robert M. Lee and SANS Institute

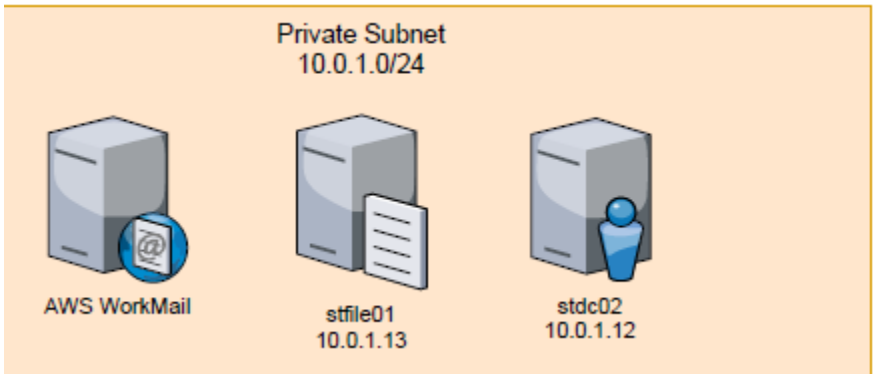
https://t.me/learningnets
Technet24

Click on the **IPv4** tab and then sort by the number of Packets (largest to smallest) by clicking on the **Packets** column twice.

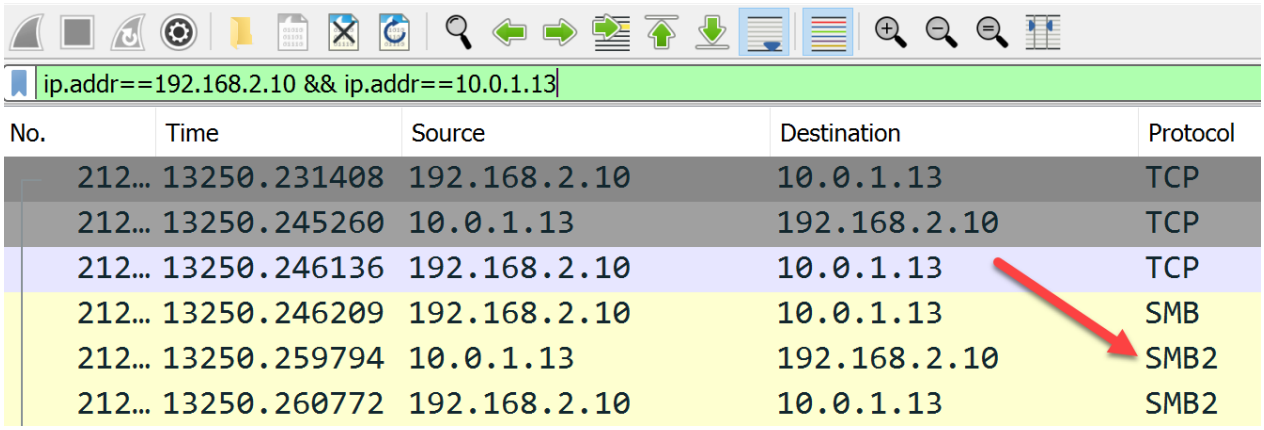


There are plenty of IP addresses that 192.16.2.10 is communicating with, but there is a lot of traffic going to 10.0.1.13 and 10.0.1.12 with a lot of Bytes being transferred as well.

In referencing our network diagram, we can determine that 10.0.1.13 and 10.0.1.12 are internal systems. 10.0.1.13 seems to be the most important as it is our file server where we host sensitive research and client data.



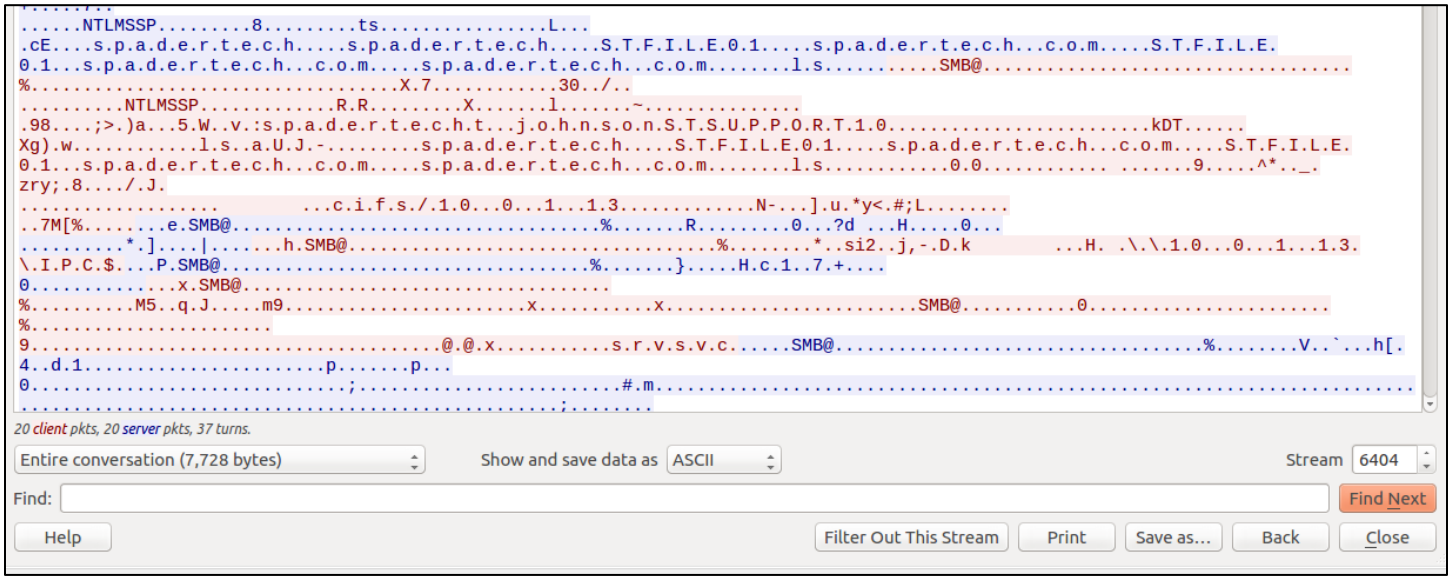
We will want to see what kind of communications are occurring here. Close the **Conversations** window and go back to the filter bar and filter for:
`ip.addr==192.168.2.10 && ip.addr==10.0.1.13`



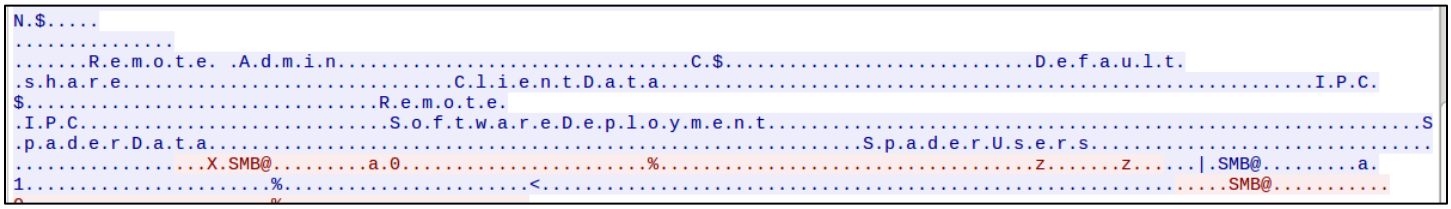
© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets

Examining the Protocol column for these packets, it looks like this is mostly SMB traffic. Click on one of the packets with the SMB2 protocol and right-click, then select **Follow** and **TCP Stream**.



Based on the strings we see in this packet, including **tjohnson**, **Remote Admin**, **ClientData**, and **C$**. If you weren't sure what these strings were telling you, you might do research on them, including by referencing the MITRE ATT&CK page on SMB/Windows Admin Shares. (https://attack.mitre.org/techniques/T1021/002/) It appears that the adversary is moving laterally from 192.18.2.10 into 10.0.1.13 over SMB and using Timothy Johnson's account to access ClientData.



2. Are there any files of interest that the adversary likely accessed?

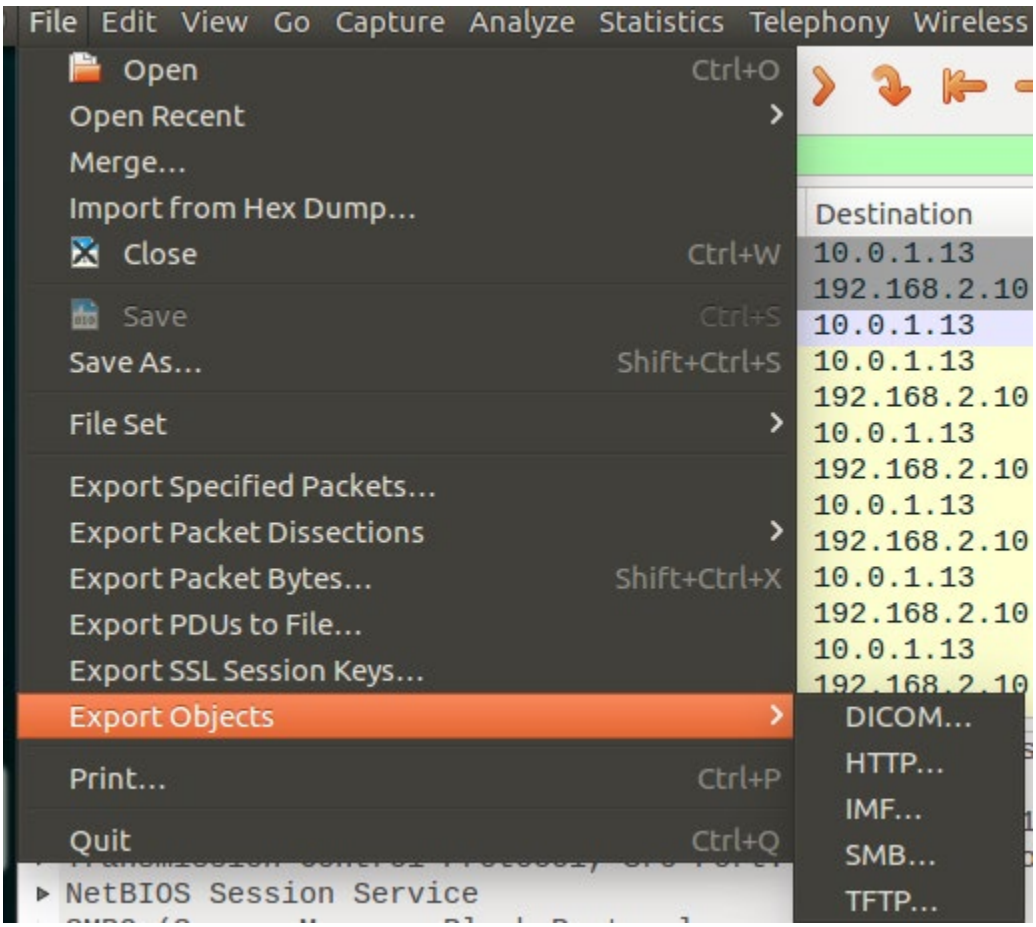
- **Hydro One related project files to the customer Alset**

We could continue to follow the streams, but since this is SMB data, we can also just use Wireshark's native ability to carve out files and see if we find anything of interest.

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets
Technet24

Click **File** and **Export Objects** and choose **SMB**.

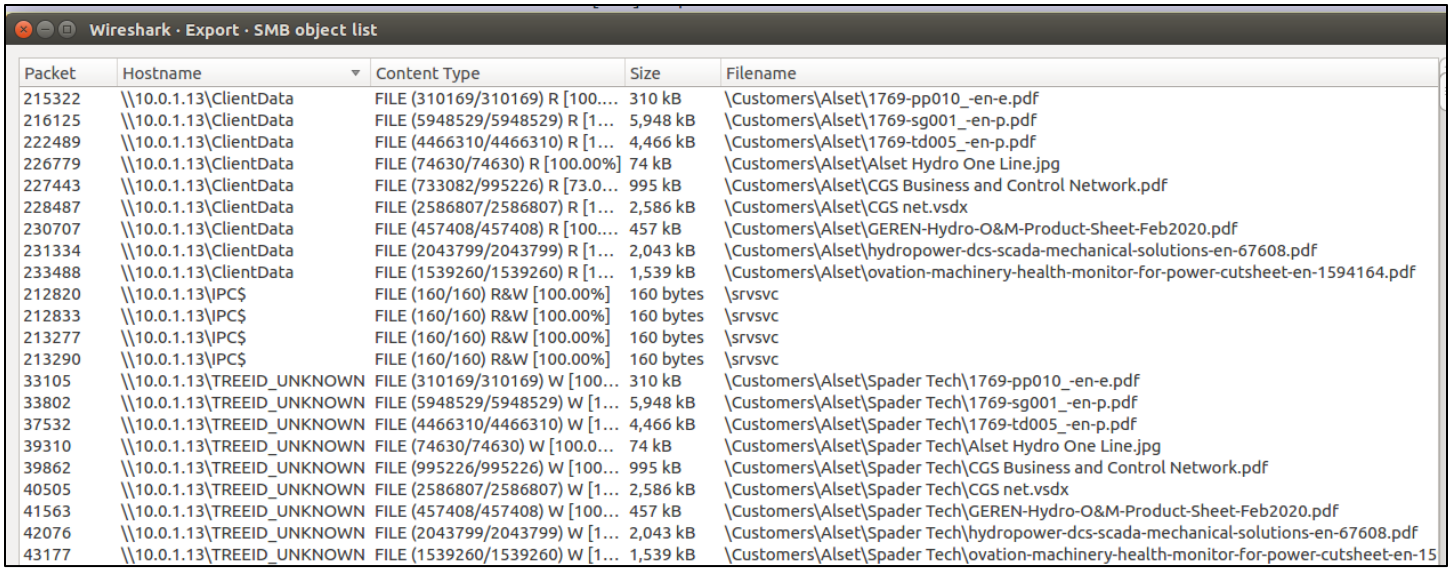


There's a lot here to go through manually, but we know we're mostly interested in 10.0.1.13 so click the **Hostname** column, which will cause the data to sort by the unique hosts.

We see that 10.0.1.13 has data transferred to 192.168.2.10 from a number of different directories including "ClientData" which includes PDFs, images, and Visio Diagrams associated with the Customer "Alset". These documents are all control system related with references to Hydro One, SCADA solutions, and Ovation equipment (a type of industrial control system software and hardware).

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets



Packet	Hostname	Content Type	Size	Filename
215322	\\10.0.1.13\ClientData	FILE (310169/310169) R [100....	310 kB	\Customers\Alset\1769-pp010_-en-e.pdf
216125	\\10.0.1.13\ClientData	FILE (5948529/5948529) R [1...	5,948 kB	\Customers\Alset\1769-sg001_-en-p.pdf
222489	\\10.0.1.13\ClientData	FILE (4466310/4466310) R [1...	4,466 kB	\Customers\Alset\1769-td005_-en-p.pdf
226779	\\10.0.1.13\ClientData	FILE (74630/74630) R [100.00%]	74 kB	\Customers\Alset\Alset Hydro One Line.jpg
227443	\\10.0.1.13\ClientData	FILE (733082/995226) R [73.0...	995 kB	\Customers\Alset\CGS Business and Control Network.pdf
228487	\\10.0.1.13\ClientData	FILE (2586807/2586807) R [1...	2,586 kB	\Customers\Alset\CGS net.vsdx
230707	\\10.0.1.13\ClientData	FILE (457408/457408) R [100....	457 kB	\Customers\Alset\GEREN-Hydro-O&M-Product-Sheet-Feb2020.pdf
231334	\\10.0.1.13\ClientData	FILE (2043799/2043799) R [1...	2,043 kB	\Customers\Alset\hydropower-dcs-scada-mechanical-solutions-en-67608.pdf
233488	\\10.0.1.13\ClientData	FILE (1539260/1539260) R [1...	1,539 kB	\Customers\Alset\ovation-machinery-health-monitor-for-power-cutsheet-en-1594164.pdf
212820	\\10.0.1.13\IPC$	FILE (160/160) R&W [100.00%]	160 bytes	\srvsvc
212833	\\10.0.1.13\IPC$	FILE (160/160) R&W [100.00%]	160 bytes	\srvsvc
213277	\\10.0.1.13\IPC$	FILE (160/160) R&W [100.00%]	160 bytes	\srvsvc
213290	\\10.0.1.13\IPC$	FILE (160/160) R&W [100.00%]	160 bytes	\srvsvc
33105	\\10.0.1.13\TREEID_UNKNOWN	FILE (310169/310169) W [100...	310 kB	\Customers\Alset\Spader Tech\1769-pp010_-en-e.pdf
33802	\\10.0.1.13\TREEID_UNKNOWN	FILE (5948529/5948529) W [1...	5,948 kB	\Customers\Alset\Spader Tech\1769-sg001_-en-p.pdf
37532	\\10.0.1.13\TREEID_UNKNOWN	FILE (4466310/4466310) W [1...	4,466 kB	\Customers\Alset\Spader Tech\1769-td005_-en-p.pdf
39310	\\10.0.1.13\TREEID_UNKNOWN	FILE (74630/74630) W [100.0...	74 kB	\Customers\Alset\Spader Tech\Alset Hydro One Line.jpg
39862	\\10.0.1.13\TREEID_UNKNOWN	FILE (995226/995226) W [100...	995 kB	\Customers\Alset\Spader Tech\CGS Business and Control Network.pdf
40505	\\10.0.1.13\TREEID_UNKNOWN	FILE (2586807/2586807) W [1...	2,586 kB	\Customers\Alset\Spader Tech\CGS net.vsdx
41563	\\10.0.1.13\TREEID_UNKNOWN	FILE (457408/457408) W [100...	457 kB	\Customers\Alset\Spader Tech\GEREN-Hydro-O&M-Product-Sheet-Feb2020.pdf
42076	\\10.0.1.13\TREEID_UNKNOWN	FILE (2043799/2043799) W [1...	2,043 kB	\Customers\Alset\Spader Tech\hydropower-dcs-scada-mechanical-solutions-en-67608.pdf
43177	\\10.0.1.13\TREEID_UNKNOWN	FILE (1539260/1539260) W [1...	1,539 kB	\Customers\Alset\Spader Tech\ovation-machinery-health-monitor-for-power-cutsheet-en-15

We could extract all these files for the forensic analysts, but at this point, we will continue on as it's clear the adversary was targeting at least the customer Alset's data and has likely exfiltrated out sensitive client information. It would be good to verify this, though, by understanding the contents of the out.rar file our forensic analysts were able to recover. If the files are a match, then it is reasonable to assess that the adversary leveraged 192.168.2.10 as the internal staging server, moved the sensitive files to that system, archived them up, and then exfiltrated them out.

3. What is the password for out.rar?

- **Alset**

The forensic analysts would like a set of keywords as their requirement is to understand some terms to make a password cracking list out of to try to crack open out.rar.

There are many ways to approach this, including just using the keywords of the adversary persona information (e.g. Top Energy Support) as well as any of the files associated with what the adversary was searching for.

However, before we compile a list, we can assess that the adversary was searching for files associated with Alset (since we see that those files were transferred) and we also know from our forensic analysts that there was a file named **out.rar**. So, we can return to the memory image and see if there's anything else that stands out now that we have a new keyword to search.

In the SIFT VM, open up a terminal and navigate to the Ex 2.3 folder (if you are not already there from the last exercise) with the following command:

```
cd Desktop/FOR578\ Exercises/Ex\ 2.3
```

Next, run the following command to search for **out.rar** in the memory image:

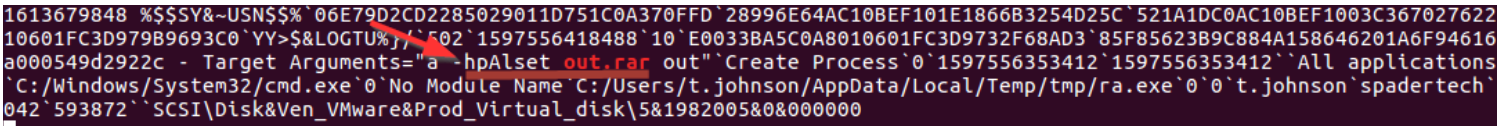
```
strings -td -a stsupport10-memory.dd4.001 | grep "out.rar"
```

```
sansforensics@siftworkstation:~/Desktop/FOR578 Exercises/Ex 2.3$ strings -td -a stsupport10-memory.dd4.001 | grep "out.rar"
582109216 out.rar
582109392 out.rar
```

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets
Technet24

Normally, you'd likely output this to a text file, but go ahead and pay attention as the information displays across your screen. We can clearly see the **out.rar** file get highlighted, and of great interest is a **Target Argument** which shows the **-hp** command options followed by "Alset". If you weren't sure what these options were, a quick Google search would reveal that the **-hp** options are used to encrypt files with a password that follows—so "Alset" is our password!



You've just saved the team a lot of time. They don't need to create a password cracker. The password for the out.rar file is "Alset".

4. Document any new indicators and TTPs.

- **out.rar**
- **Alset**
- **10.0.1.13 and 10.0.1.12**
- **Collection – T1560 Archive Collected Data**
- **Lateral Movement – T1021.002 Remote Services: SMB/Windows Admin Shares**
- **Exfiltration – T1041 Exfiltration over C2 Channel**

What you choose to document is up to you, but some of the more interesting indicators include the victim IP addresses (10.0.1.13 and 10.0.1.12), the targeted customer "Alset", the out.rar file, and the password "Alset".

The adversary pivoted through 192.16.2.10 to perform lateral movement using SMB and network shares to access the target system and then exfiltrate out the documents over an existing C2 channel after staging the files on 192.16.2.10 and archiving them up. There are many ways to document this information, and the spreadsheet below is just one example.

Indicator	KC Phase	DM: Adversary	DM: Capability	DM: Infrastructure	DM: Victim
Alset (password)	Actions on Objectives	"Top Energy Support"	Archived Folders	192.168.2.10	10.0.1.13
out.rar	Actions on Objectives	"Top Energy Support"	Archived Folders	192.168.2.10	10.0.1.13
10.0.1.13	Actions on Objectives	"Top Energy Support"	Internal Network Shares	192.168.2.10	10.0.1.13
10.0.1.12	Actions on Objectives	"Top Energy Support"	Internal Network Shares	192.168.2.10	10.0.1.12

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets

Indicator	ATT&CK Tactic	ATT&CK Technique
Alset (password)	Collection	T1560.001 Archive Collected Data
out.rar	Collection and Exfiltration	T1560.001 Archive Collected Data and T1041 Exfiltration Over C2 Channel
10.0.1.13	Lateral Movement	T1021.002 Remote Services: SMB/Windows Admin Shares
10.0.1.12	Lateral Movement	T1021.002 Remote Services: SMB/Windows Admin Shares

Exercise: Key Takeaways

- **By examining packet capture and memory, we were able to analyze the adversary's actions on objective.**

- **We determined the adversary likely accessed files related to a customer, Alset, and conducted lateral movement via internal network shares over SMB.**

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets
Technet24

Exercise 2.5: Satisfying Priority Intelligence Requirements

Objectives

- Document and analyze the key findings of the intrusions
- Satisfy priority intelligence requirements using intrusion analysis
- Ready key findings for future intrusion analysis

Scenario: Your cyber threat intelligence team has been able to gather a lot of important details and information by analyzing the intrusion into Timothy Johnson's computer and broader SpaderTech network. At this time, it's important to document the key findings and finalize the Priority Intelligence Requirements necessary for cleaning up this compromise and preparing for future intrusions. You have been working hand in hand with the incident responders already, but the final analysis and documentation will ensure everyone is on the same page about what needs to happen next.

The Priority Intelligence Requirements:

- *1. Out of the six intrusions, are any successful compromises?*
- *2. What are the key indicators associated with the successful compromise(s)?*
- *3. What are the most useful TTPs out of the successful compromise(s)?*
- *4. What was the impact of the adversary's successful compromise(s)?*
- *5. What key indicators/TTPs could be used to track future intrusions?*

Exercise Prep

Students will not need to use their VMs or technical tools for this lab.

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets

Exercise: Questions

1. Using the information gathered through Exercises 2.1-2.4, aggregate the core timeline details, key indicators, and TTPs leveraged by the adversary if not already done. In addition to the Kill Chain, Diamond Model, and ATT&CK, also map details to the Kill Chain Courses of Action. You may start from the "Ex 2.1 Intrusion Analysis – Completed.xls" file from the Ex 2.1 folder or whatever other method you used to track intrusion analysis.

2. Analyze the intrusion and finalize the output for the Priority Intelligence Requirements.

- *1. Out of the six intrusions, are any successful compromises?*

  _____

- *2. What are the key indicators associated with the successful compromise(s)?*

  _____

- *3. What are the most useful TTPs out of the successful compromise(s)?*

  _____

- *4. What was the impact of the adversary's successful compromise(s)?*

  _____

- *5. What key indicators/TTPs could be used to track future intrusions?*

  _____

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets
Technet24

Exercise: Questions with Step-by-Step

1. Using the information gathered through Exercises 2.1-2.4, aggregate the core timeline details, key indicators, and TTPs leveraged by the adversary if not already done. In addition to the Kill Chain, Diamond Model, and ATT&CK, also map details to the Kill Chain Courses of Action. You may start from the "Ex 2.5 Intrusion Analysis – Starting Point.xlsx" file from the Ex 2.5 folder or whatever other method you used to track intrusion analysis.

This is a highly subjective lab in which you should compile everything you have done through the Exercise 2.1-2.4 labs and satisfy the Priority Intelligence Requirements. Consumers all consume intelligence differently, and in the real world, you'd work with them to determine what format and structure they can use your information in. For this exercise, just compile the information in a way that's useful to you. This walkthrough will begin with and add to the "Ex 2.5 Intrusion Analysis – Starting Point.xlsx" file from the Ex 2.5 folder, though you can start with whatever other method you used to track intrusion analysis.

We will begin by reviewing information from Exercises 2.2 through 2.4, and ensuring it is added to our spreadsheet.

- **In Exercise 2.2, by analyzing packet capture, we identified the new indicator of vncviewer_v3.38.9_tcp.exe. We also observed that the packet capture showed a user connecting to the domain downloads.topenergysupport(dot)com, which established a connection to IP address 51.11.247.89. Since that same IP address, 51.11.247.89, was used in scanning identified in our previous Intrusion 2, we decided to "collapse" Intrusion 5, the Top Energy phishing email, into Intrusion 2, the scanning from 51.11.257.89 – those now represent our new Intrusion 2. After completing that analysis in Exercise 2.2, our new Intrusion 2 sheet might look something like the below. (See the appropriate sheets in the "Ex 2.5 Intrusion Analysis – Starting Point.xlsx" file from the Ex 2.5 folder for full visibility into each of the below partial screenshots.)**

Indicator	Comment	KC Phase
51.11.247.89	Scanned external gateway for ports 443, 3389, 80 (ports 443, 3389 open)	Reconnaissance
help(at)topenergysuport.com	Sender email for phish to T Johnson. "Signature" was "Top Energy Support Team."	Delivery
downloads.topenergysupport(dot)com	Malicious link in phish to T Johnson	Delivery
vncviewer_v3.38.9_tcp.exe	Trojanized application downloaded from downloads.topenergysupport(dot)com	Installation

- **In Exercise 2.3, we conducted memory analysis with Volatility and identified multiple different indicators and TTPs associated with Intrusion 2, the compromise of T. Johnson's machine via a phishing email. We added several indicators, including cmd.exe, ipconfig.exe, taskhostw.exe, and a suspicious Temp directory to our analysis spreadsheet.**

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets

Indicator	Comment	KC Phase
51.11.247.89	Scanned external gateway for ports 443, 3389, 80 (ports 443, 3389 open)	Reconnaissance
help(at)topenergysuport.com	Sender email for phish to T Johnson. "Signature" was "Top Energy Support Team."	Delivery
downloads.topenergysupport(dot)com	Malicious link in phish to T Johnson	Delivery
vncviewer_v3.38.9_tcp.exe	Trojanized application downloaded from downloads.topenergysupport(dot)com	Installation
cmd.exe	Unsure what it did, intelligence gap (parent process PID 16264, injected taskhostw process)	Actions on Objectives
cmd.exe	Unsure what it did, intelligence gap (parent process PID 16264, injected taskhostw process)	Actions on Objectives
ipconfig.exe	Likely used for discovery (parent process PID 16264, injected taskhostw process)	Actions on Objectives
taskhostw.exe	Process injection of vncviewer process into taskhostw.exe	Actions on Objectives
Users\t.johnson\AppData\Local\Temp\Low	Folder used for data staging	Actions on Objectives

- **In Exercise 2.4, we analyzed packet capture and memory to identify more information about the adversary's Actions on Objectives in Intrusion 2. We previously added several new indicators and TTPs to our analysis spreadsheet, including out.rar, Alset, and the victim Ips of 10.0.1.13 and 10.0.1.12. We realized that we had other information from our forensic team (provided at the beginning of Exercise 2.4), so we will also add Meterpreter, PowerShell, and lsass.exe to our analysis spreadsheet, being sure to map to the Kill Chain, Diamond Model, and ATT&CK as we did before.**

Indicator	Comment	KC Phase
Meterpreter	Vncviewer was trojanized to include Meterpreter (unsure what techniques Meterpreter used, intelligence gap)	Actions on Objectives
powershell.exe	Unclear how it was used, intelligence gap	Actions on Objectives
lsass.exe	Used to dump T. Johnson's credentials	Actions on Objectives
Alset	Password used for archive out.rar	Actions on Objectives
out.rar	Name of archived files collected and exfiltrated over existing C2 channel	Actions on Objectives
10.0.1.13	File server compromised by lateral movement over SMB2 using T Johnson account	Actions on Objectives
10.0.1.12	File server compromised by lateral movement over SMB2 using T Johnson account	Actions on Objectives

It is becoming clear to us that Intrusion 2 has the most activity. To better make sense of the entire intrusion and identify any gaps, we decide to bring our Intrusion 2 analysis into a different view, make sure we didn't miss anything important, check to make sure we have all Kill Chain stages covered, and also determine what Courses of Action we have performed. This will help us more easily respond to our Priority Intelligence Requirements. We are using the "Diamond Model-KC Mapping" sheet of the provided Excel file, "Ex 2.5 Intrusion Analysis – Starting Point", but you may do this however you choose.

We choose to go methodically through each Kill Chain phase, and as we do so, map to the Courses of Action, Diamond Model, and ATT&CK within that phase.

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets
Technet24

We start by looking at Reconnaissance. This isn't too hard because we already have that in our spreadsheet for Intrusion 2. As we look at the information, though, we realize we've omitted something that may be important later—the timestamp of the initial scanning or our external gateway. We also see that we've duplicated information by mapping Scanning to both the Diamond Model and ATT&CK, and Reconnaissance to both the Kill Chain and ATT&CK, so we collapse those. In thinking about what Course of Action we've taken, we determine we've only done historic searches—the Discover Course of Action. This is important to capture because we may want to recommend other Courses of Action. We choose to fill in empty cells with gray to help emphasize our gaps.

For just the Reconnaissance phase, our spreadsheet looks like the one below, though yours may look different.

	Discover	Detect	Deny	Disrupt	Degrade	Deceive	Adversary	Infrastructure	Capability	Victim
Recon	51.11.247.89 (2020-08-14 02:02:02 UTC)							51.11.247.89	T1595 Active Scanning (ports 443, 3389 open)	SpaderTech External Gateway

As we move to the Weaponization phase, we realize our existing spreadsheet doesn't have anything for the Weaponization phase. The adversary certainly had to weaponize the email and register the malicious domain prior to delivery, so we fill in relevant information for the Weaponization phase due to the "phasal distortion" from the Delivery phase.

	Discover	Detect	Deny	Disrupt	Degrade	Deceive	Adversary	Infrastructure	Capability	Victim
Weaponization								hxxp://downloads.topenergysupport(dot)com (T1583.001 Acquire Infrastructure: Domains)	Link hosting malicious file themed as VNC software (T1036.005 Match Legitimate Name or Location)	t.johnson(at) spadertech(dot)com

Looking at the Delivery and Exploitation phases next, we realize we may have overlooked the Exploitation phase. We previously mapped the malicious link in the phishing email to Delivery, but thinking about it further, we realize the user clicking that link actually represents human exploitation. Another key takeaway we notice from this analysis, and discussing with our defenders, is that this is the only phase so far where we have a forward-looking detection implemented on the delivery email address. This is useful because we note that we may need to take the Detect Course of Action for other phases as well. We adjust our information accordingly, resulting in the following.

	Discover	Detect	Deny	Disrupt	Degrade	Deceive	Adversary	Infrastructure	Capability	Victim
Delivery		help(at)topenergysupport(dot)com					"Top Energy Support"	help(at)topenergysupport(dot)com	Phishing w/ malicious link (T1566.002 Spearphishing Link)	t.johnson(at) spadertech(dot)com
Exploit								hxxp://downloads.topenergysupport(dot)com	Social Engineering (T1204.001 User Execution: Malicious Link)	t.johnson(at) spadertech(dot)com

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets

The Installation phase is fairly straightforward since we already captured that information.

	Discover	Detect	Deny	Disrupt	Degrade	Deceive		Adversary	Infrastructure	Capability	Victim
Install	vncviewer_v3.38.9_tcp.exe							"Top Energy Support"	hxxp://downloads.topenergysupport(dot)com	Trojanized Application vncviewer_v3.38.9_tcp.exe (T1036.005 Match Legitimate Name or Location)	192.168.2.10

We then realize we don't have anything yet for the Command and Control phase. In discussing with our forensic analysts, they clarify that Meterpreter, which they briefly mentioned to us before, was actually used to send instructions to victims over RDP via IP address 51.11.247.89, so we decide that belongs in Command and Control rather than Actions on Objective as we previously assigned. It is completely normal and expected that as information changes, our analysis changes as well. This new finding emphasizes the importance of asking follow-up questions of forensic analysts and others we work with on intrusions. As we map this information to Command and Control, we add to our spreadsheet.

	Discover	Detect	Deny	Disrupt	Degrade	Deceive		Adversary	Infrastructure	Capability	Victim
C2	51.11.247.89								51.11.247.89 :3389	RDP/Meterpreter (T1021.001 Remote Desktop Protocol)	192.168.2.10

Our final phase, Actions on Objectives, has lots of information. For the purposes of this analysis, we chose to summarize all of those indicators and techniques. We realize we have a lot of ATT&CK techniques, so we decide to come back to those details later to enter everything into our Threat Intelligence Platform (TIP). As we do a closer analysis of timestamps to make sure we didn't miss anything, we spot a pattern. It appears the adversaries operate between consistent hours. This is an important detail mapping to the Adversary feature of the Diamond Model that we want to be sure to include.

	Discover	Detect	Deny	Disrupt	Degrade	Deceive		Adversary	Infrastructure	Capability	Victim
Actions	taskhostw.exe and Document Exfil (2020-08-16 03:18:34 UTC)							"Top Energy Support." Choice of "Alset" as a password, which was the target's company name. Operates consistently between 02:00:00 - 04:30:00 UTC	192.168.2.10	Meterpreter, PowerShell, SMB, taskhostw.exe injection, internal tools such as cmd.exe and ipconfig.exe, rar (T1059.001 PowerShell, T1059.003 Windows Command Shell, T1059.003 Windows Command Shell, T1016 System Network Configuration Discovery, T1055 Process Injection, T1074.001 Local Data Staging, T1003.001 LSASS Memory, T1560 Archive Collected Data, T1041 Exfiltration over C2 Channel, T1021.002 SMB/Windows Admin Shares, T1078.003 Local Accounts)	192.168.2.10, 10.0.1.13, 10.10.1.12, T. Johnson account, and Alset customer files

A key point to this exercise is that what each analyst chooses to abstract out of an intrusion is entirely up to them and their interpretation of the user's intelligence requirements. Later in the course, when we get to piecing together intrusions into larger clusters and groups, even later getting to attribution, it should stand out that the information we're operating off of isn't all of the details of the adversary but what the analysts were able to find of those intrusions and what they chose to highlight and collect. This will absolutely make small and sometimes large changes on the final analysis we produce as intelligence analysts.

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets
Technet24

2. Analyze the intrusion and finalize the output for the Priority Intelligence Requirements.

One possible set of answers are below. Your answers may differ, and this is completely fine.

- *1. Out of the six intrusions, are any successful compromises?*

Only the "Top Energy" intrusion was successful, which is why decided to do a deeper dive on it.

- *2. What are the key indicators associated with the successful compromise(s)?*

The IP address 51.11.247.89 was used in multiple phases of the kill chain and as such is a key indicator as was the usage of Meterpreter.

- *3. What are the most useful TTPs out of the successful compromise(s)?*

The phishing tactics and clicking on links were things we already have reasonably documented on the team but can choose to do so again to add extra weight to the importance of controls against these tactics. The most interesting tactics and techniques to call attention to were the T1560 Archive Collected Data, T1041 Exfiltration over C2 Channel, and T1021.001 Remote Services: Remote Desktop Protocol). We could work with defenders to ensure proper security controls and detections for these tactics and techniques.

- *4. What was the impact of the adversary's successful compromise(s)?*

The adversary was successfully able to exfiltrate documents associated with Hydro One and industrial engineering projects associated with the client Alset.

- *5. What key indicators/TTPs could be used to track future intrusions?*

The behaviors of the adversary theme phishing after the energy focused projects and then leverage internal tools such as PowerShell and open-source tools such as Meterpreter are the best TTPs to document. The "living on the land" style of behaviors in combination with energy and client-focused documents is interesting. The 51.11.247.89 IP address was used consistently enough that it should be looked at to see any overlaps with future intrusions. Additionally, the password being the victim company's name was an interesting observable worth documenting. In the future, if we see multiple of these behaviors and indicators together, it could represent an overlap worth clustering on.

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets

This page intentionally left blank.

https://t.me/learningnets

Technet24

Exercise 3.1: Aggregating and Pivoting in Excel

Objectives

- Understand how Excel can be used to work with large datasets
- Use filtering and pivot tables to summarize large amounts of data
- Apply heat maps to datasets as appropriate to quickly visualize data

Scenario: A recent tipper from a threat intelligence sharing group included a large amount of Poison Ivy configuration information. The company that shared the information revealed that they had experienced an intrusion around the same time as Edison analysts were responding to the intrusion at Spader Technologies. With overlaps in the timing and the malware used, you want to enhance your intelligence on the adversary's C2 infrastructure with an emphasis on both discovery of the potentially ongoing activity, as well as mitigation of future or follow-on intrusions. Analyze the provided data to determine if it contains any additional information that can help address these concerns.

Exercise: Prep

Familiarize yourself with the "Poison Ivy Config Dumps.csv" document in the **Ex 3.1** folder. This is the source data for this exercise. The adversary you have been recently tracking uses the C2 IP 38.72.115.9. Use this information and tools within Excel to answer the following questions.

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets

Exercise: Questions

1. What configuration parameters appear within the Poison Ivy Configuration Dumps data?

   - _____

2. What configuration values were present in the sample that used 38.72.115.9 as the C2 IP?

   - _____

3. What are the top five most frequently used passwords within the samples? List them in order here. How did you make this determination? (Hint: Use a pivot table.)

   - _____

4. Analysis of the intrusion attempts against your organization indicated that one Poison Ivy sample was configured to beacon to 38.72.115.9, which appears in this dataset. Can you find any other samples in this dataset that are related? What are their hash values? What fields did you use to find them?

   - _____

5. Create a heatmap showing a cross-comparison between mutexes and ports using pivot tables. Can you determine what the default values for Poison Ivy possibly are based on this data?

   - _____

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets
Technet24

6. What is the significance of the findings in sections 4 and 5? **Hint**: Articulate your response in terms of the Diamond Model, Kill Chain, and the properties of campaigns

- _____

  _____

  _____

  _____

7. What are the indicators we could leverage going forward?

- _____
- _____

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets

Exercise: Questions with Step-by-Step

1. What configuration parameters appear within the Poison Ivy Configuration Dumps data?

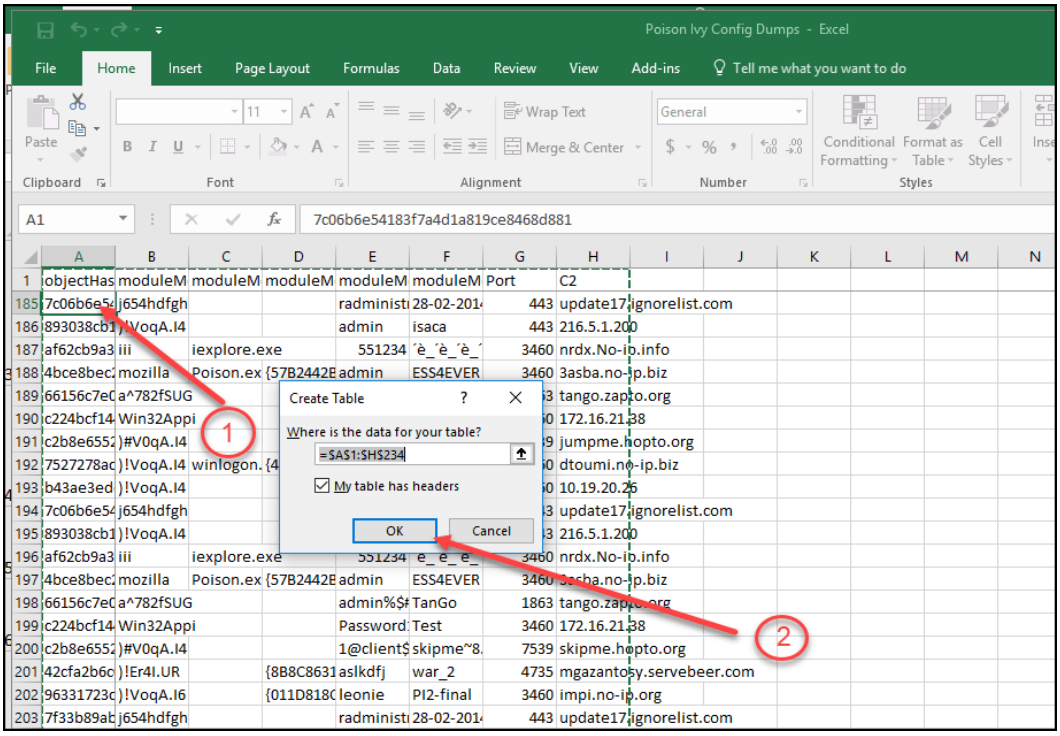
   - **Hash value, mutex, "inject into" process, active setup value, password, implant ID, C2 port, C2 location**

   These are the values that can be found in the headings within the Excel file. Each of these fields may have options set, but as we can see in the data, not all fields MUST include a value. While many of these are self-explanatory, we may ask the group who shared the information or our internal forensic analysts about any values we are unfamiliar with. If you have not heard of a mutex, think of that as a unique value that acts as a "bookmark" in memory so malware knows it is already running (it doesn't want to run again if it doesn't have to). "Active setup value" is a registry modification that causes the malware to be run automatically.

2. What configuration values were present in the sample that used 38.72.115.9 as the C2 IP?

   - **a8e9ce659a90207137bd6a712450c6ce,)#V0qA.I4, Emmental, ImplantCfg1, 4444, 38.72.115.9**

   We want to format the raw data from the "Poison Ivy Config Dumps.csv" file so that we can filter and sort on each of the values. First, click in the upper left-hand side of the spreadsheet (A1). Second, type "Ctrl-T". We will see the dialog box named "Create Table", then click "OK." We will now see a formatted, filterable table with small down arrows in the right-hand side of each column header. We now can filter on one or all of the columns.

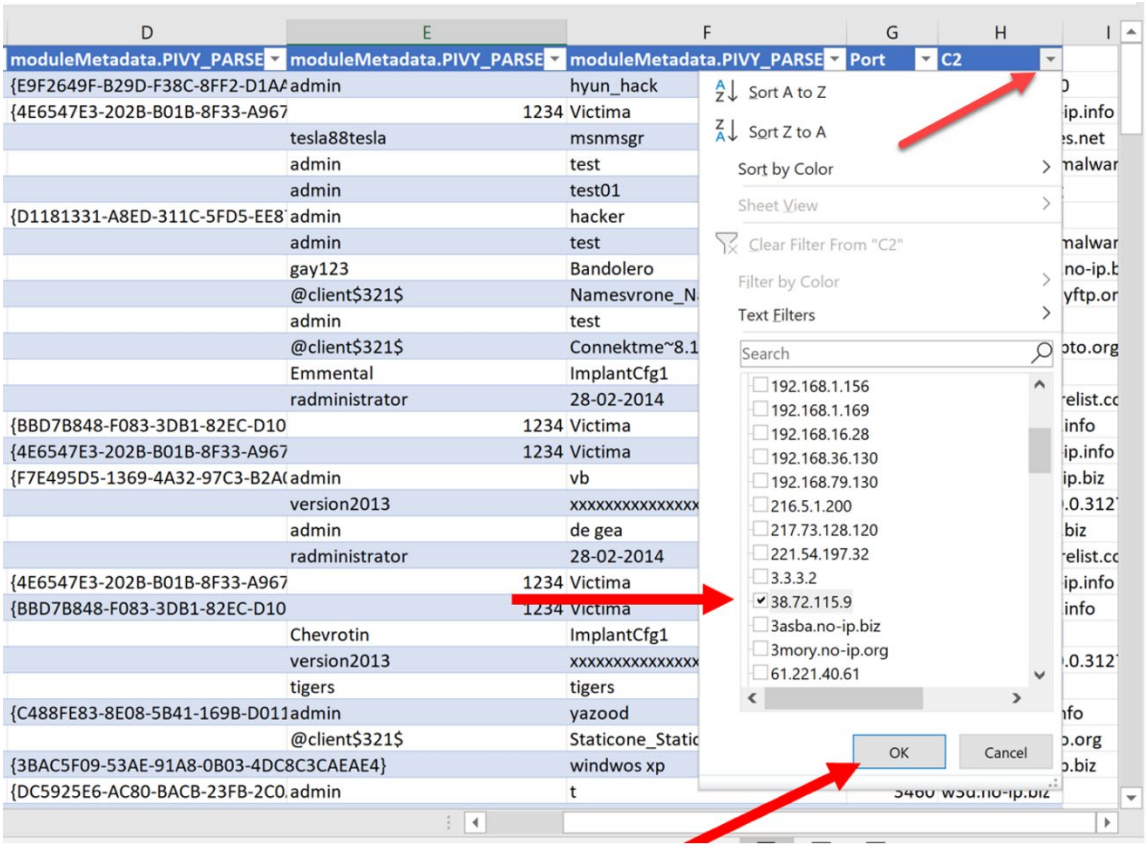


We can now filter the entire list to show only rows that have the value "38.72.115.9" in the C2 column. Pull down the arrow on the right side of the C2 Column (column H) and uncheck the top item named "(Select All)." This will unselect all values and then allow us to only check the ones

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets
Technet24

we are interested in. Next, find the IP "38.72.115.9" in the list (we can also enter it in the "Search" bar) and check it. Click the OK button. The list will now show only rows that have "38.72.115.9" in the C2 column, which is a single row in our dataset.



This reveals a single sample with the preceding values.

moduleMetadata.PIVY_PARSE	moduleMetadata.PIVY_PARSE	moduleMetadata.PIVY_PARSE	moduleMetadata.PIVY_PARSE	moduleMetadata.PIVY_PARSE	Port	C2
)#V0qA.I4			Emmental	ImplantCfg1	4444	38.72.115.9

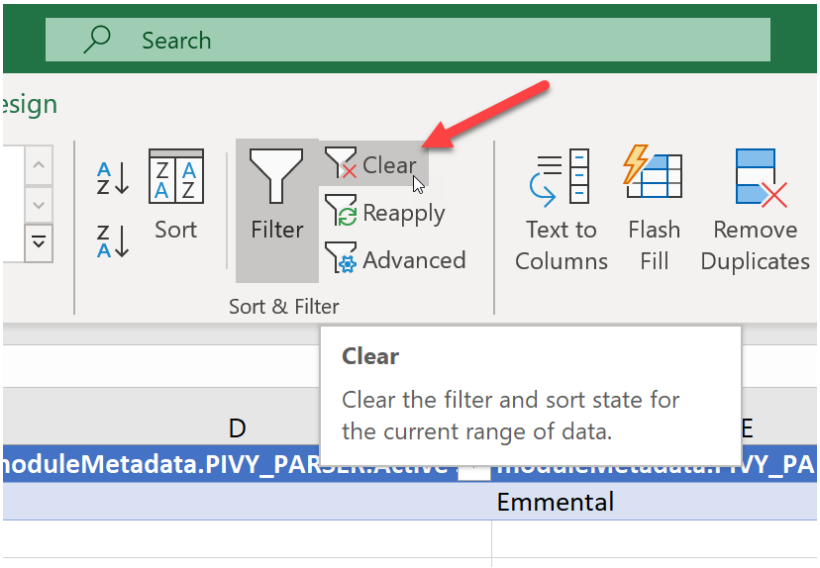
3. What are the top five most frequently used passwords within the samples? List them in order here. How did you make this determination? (Hint: Use a pivot table.)

- **admin, radminstrator, admin%$#@!, @client$321$, leonie**

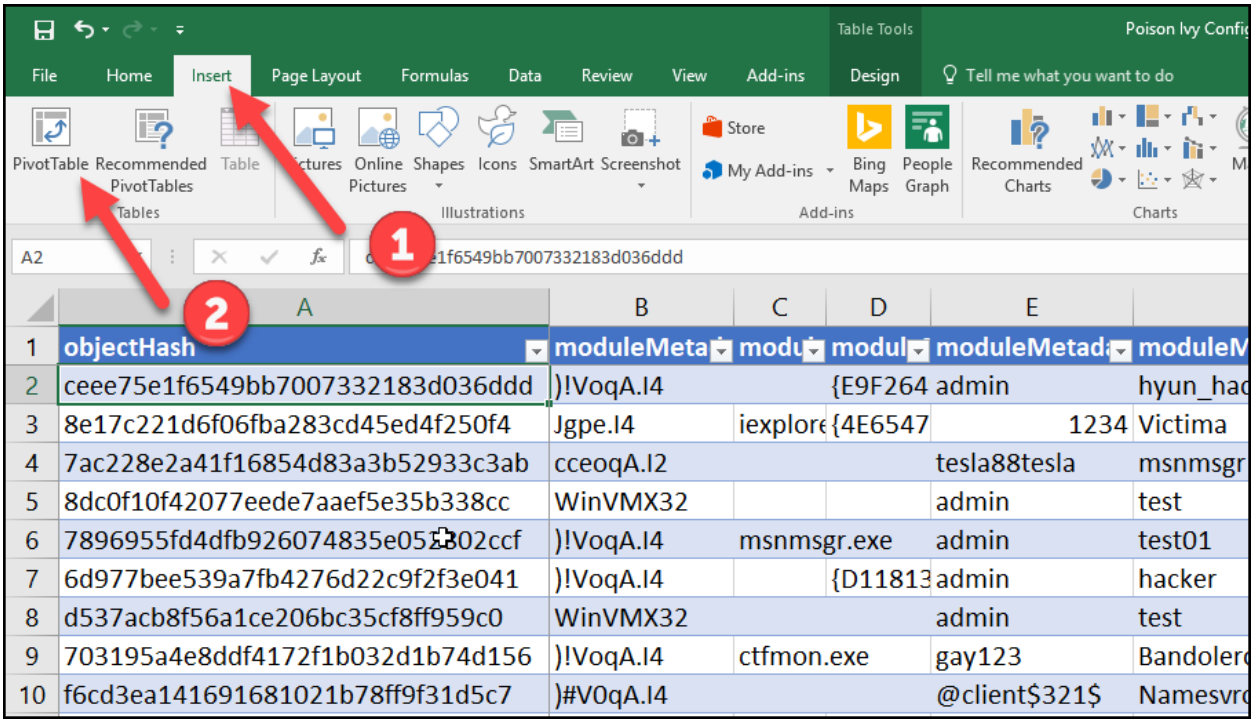
© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets

Make sure to clear our filter from the previous question by selecting "Clear" from the "Sort & Filter" section of the "Data" menu.



From the Insert tab, select PivotTable.

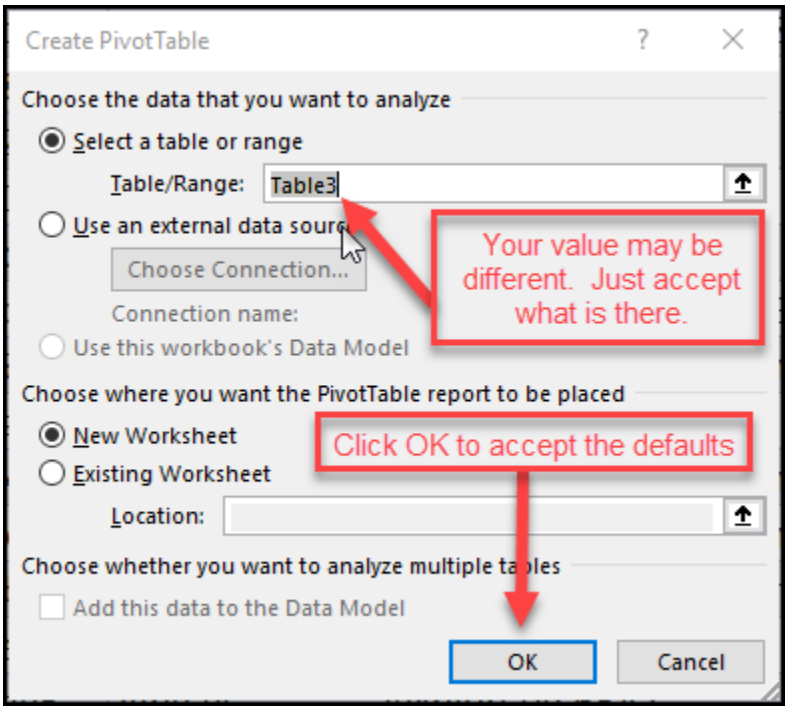


Accept the default values in the dialog box. An empty PivotTable in a new Sheet will appear.

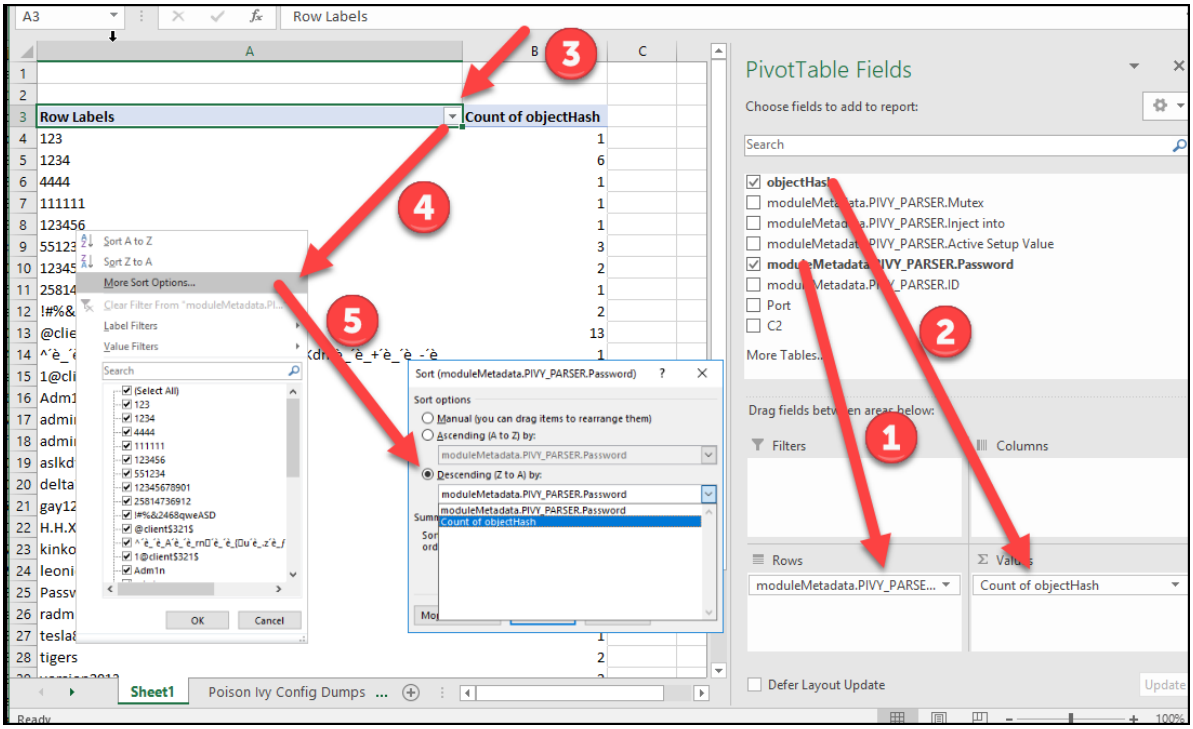
© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets

Technet24



Drag the "moduleMetadata.PIVY_PARSER.Password" field to Rows; and 2. "ObjectHash" to Values (ensuring it reads "Count of objectHash); 3. Click the down arrow next to "Row Labels" and select "More Sort Options"; and last, 5. Select arrange as "Descending" by "Count of ObjectHash" and click "OK."



The final pivot table should look as follows. This pivot table counts the number of unique hash values that use each of the passwords. There are other ways to count these passwords in Excel, but this is a simple way to count the top five most commonly used passwords.

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets

3	Row Labels	Count of objectHash
4	admin	121
5	radministrator	29
6	@client321	13
7	admin%$#@!	13
8	leonie	8
9	aslkdfj	7
10	1234	6
11	1@client321	6
12	Password123	3
13	551234	3
14	version2013	2

4. Analysis of the intrusion attempts against your organization indicated that one Poison Ivy sample was configured to beacon to 38.72.115.9, which appears in this dataset. Can you find any other samples in this dataset that are related? What are their hash values? What fields did you use to find them?

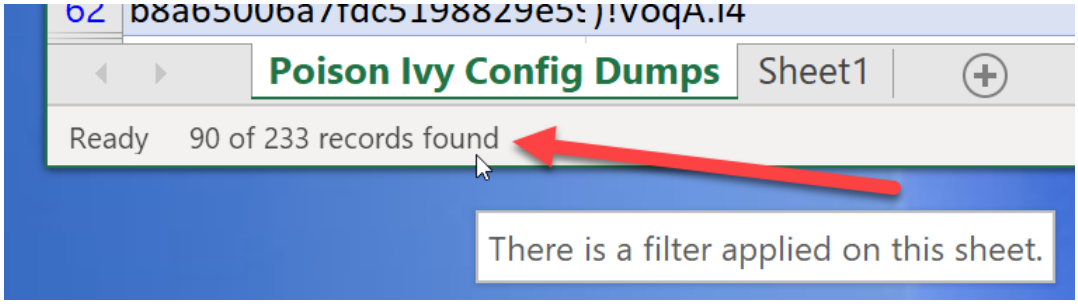
- **a8e9ce659a90207137bd6a712450c6ce**
- **840336231952dacf8fb7012a83b4e833**
- **0f24c0343385521867928417d63dc9b4**
- **b263c48036d25bed7f03d36535687fb6**
- **815a38c63e13c0a660467dbda5a74933**
- **a5ec4ad4aee9ef33c2be05119cead806**
- **7d00b43c19f4721e7156532552d656f9**
- **7527278acd2ccb56204d1d26fe2b414f**
- **7c06b6e54183f7a4d1a819ce8468d881**
- **036ec2e68385525d3c0dfc51357707b8**

To identify related samples, we can use Excel's filtering functionality to identify other samples that have values overlapping with the ones we previously identified in the sample that beacons to 38.72.115.9: the mutex ")#V0qA.I4", the password "Emmental", the ID "ImplantCfg1", and/or the port 4444. When trying to find related samples, generally, the fewer related samples there are with a certain value, the more unique pivot point is in our dataset, making those connections more meaningful.

If we filter on the mutex)#V0qA.I4 (using the same methodology we previously did), we will observe in the lower left of our sheet that 90 out of 233 samples have that same mutex. This seems like a large portion of our dataset, so we decide not to record those hashes.

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets
Technet24



Next, we try filtering on the same ID value "ImplantCfg1". (Make sure to clear our filter between searches.) When we do that filter, we can see 5 total samples (4 new ones) that are part of this campaign because this ID isn't a common or default value (unlike the 90 results returned for the mutex). There is actually a second pivot we can use, however. We notice that the majority of the ports associated with "ImplantCfg1" are port 4444, so we decide to use that as an additional pivot point.

B	C	D	E	F	G	H
moduleMetadata.PIVY_PARSE	moduleMetadata.PIVY_PARSE	moduleMetadata.PIVY_PARSE	moduleMetadata.PIVY_PARSE	moduleMetadata.PIVY_PARSE	Port	C2
)!V0qA.I4			Emmental	ImplantCfg1	4444	38.72.115.9
)!VoqA.I4			Chevrotin	ImplantCfg1	4444	61.221.40.61
)!VoqA.I4			Beaufort	ImplantCfg1	80	itservicesinc.net
)!VoqA.I4			Reblochon	ImplantCfg1	4444	76.29.149.73
)!VoqA.I4			Comte	ImplantCfg1	4444	76.29.149.78

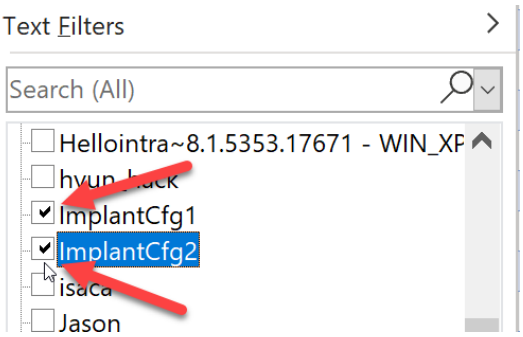
After doing the filter on port 4444, we actually have additional samples that weren't originally caught by the first filter, and are able to identify another ID value, "ImplantCfg2," that is very similar to the first.

moduleMetadata.PIVY_PARSE	moduleMetadata.PIVY_PARSE	moduleMetadata.PIVY_PARSE	moduleMetadata.PIVY_PARSE	moduleMetadata.PIVY_PARSE	Port	C2
)!V0qA.I4			Emmental	ImplantCfg1	4444	38.72.115.9
)!VoqA.I4			Chevrotin	ImplantCfg1	4444	61.221.40.61
)!VoqA.I4			Mimolette	ImplantCfg2	4444	helpdeskforu.net
)!VoqA.I4			Reblochon	ImplantCfg1	4444	76.29.149.73
)!VoqA.I4			Cancoillotte	ImplantCfg2	4444	itsupportnets.com
)!VoqA.I4			Comte	ImplantCfg1	4444	76.29.149.78
)!VoqA.I4			Livarot	ImplantCfg2	4444	76.29.149.133
)!VoqA.I4			Pelardon	ImplantCfg2	4444	68.72.115.39

If we do one final search based off of the Parser ID field, and include both ImplantCfg1 and ImplantCfg2 in our filter (by selecting both check boxes), we get a final list of samples that are potentially related to the previous intrusion. Some use port 80, but there are other values, such as the Mutex and passwords that also confirm these samples are likely related. We also notice that all of the passwords are a single word, and if we did some additional searching, we may be able to determine that these are all related somehow. (Hint: Google!) If you found all of them, and identified the password naming schema, great job! (Does anyone feel hungry after figuring that out?) We should now record these hashes, mutexes, and C2 domains and IPs for later use since they may be useful for Discover or Detect Courses of Action.

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets



moduleMetadata.PIVY_PARSE	moduleMetadata.PIVY_PARSE	moduleMetadata.PIVY_PARSE	moduleMetadata.PIVY_PARSE	moduleMetadata.PIVY_PARSE	Port	C2
)!V0qA.I4			Emmental	ImplantCfg1	4444	38.72.115.9
)!VoqA.I4			Chevrotin	ImplantCfg1	4444	61.221.40.61
)!VoqA.I4			Mimolette	ImplantCfg2	4444	helpdeskforu.net
)!VoqA.I4			Beaufort	ImplantCfg1	80	itservicesinc.net
)!VoqA.I4			Reblochon	ImplantCfg1	4444	76.29.149.73
)!VoqA.I4			Cancoillotte	ImplantCfg2	4444	itsupportnets.com
)!VoqA.I4			Comte	ImplantCfg1	4444	76.29.149.78
)!VoqA.I4			Livarot	ImplantCfg2	4444	76.29.149.133
)!VoqA.I4			Pelardon	ImplantCfg2	4444	68.72.115.39
)!VoqA.I4			Morbier	ImplantCfg2	80	supportdesk.biz

5. Create a heatmap showing a cross-comparison between mutexes and ports using pivot tables. Can you determine what the default values for Poison Ivy possibly are based on this data?

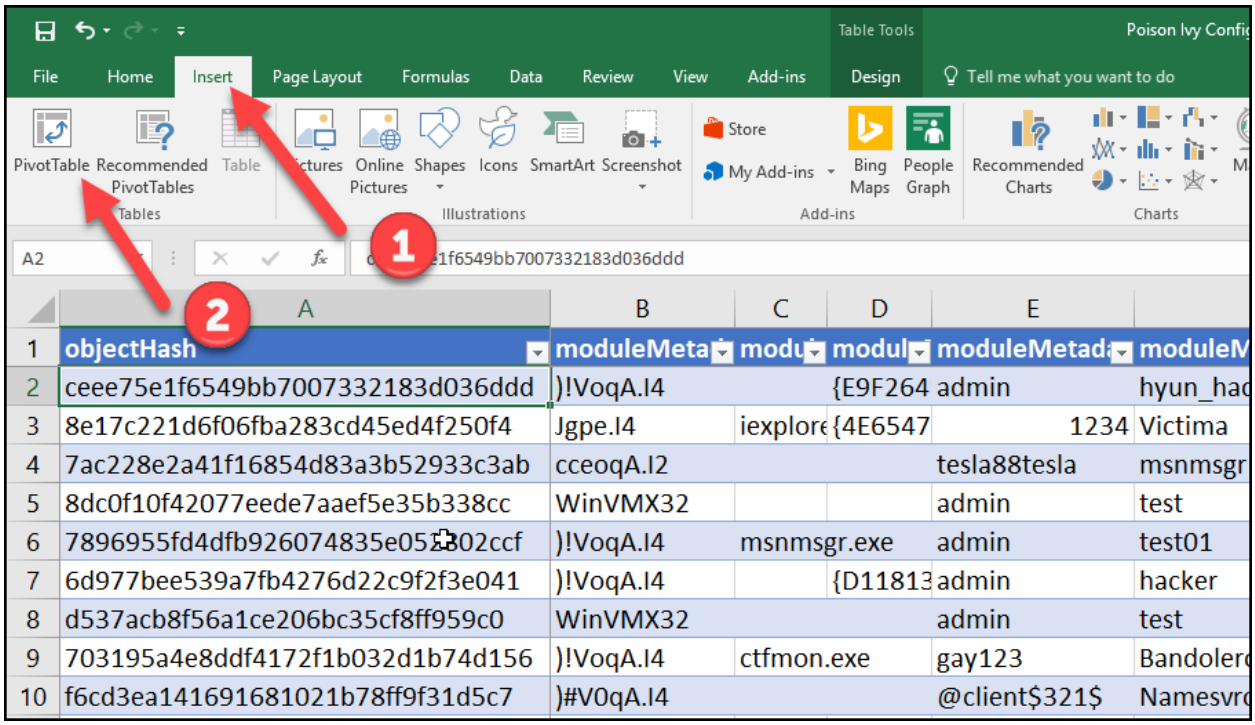
- **<u>The default values are likely port 3460 and)!VoqA.I4.</u>**

To use Excel to make this determination, use the pivot table feature again within Excel to identify the intersection counts for the mutex and port values (that is, for each mutex, how many samples with that mutex have a given port).

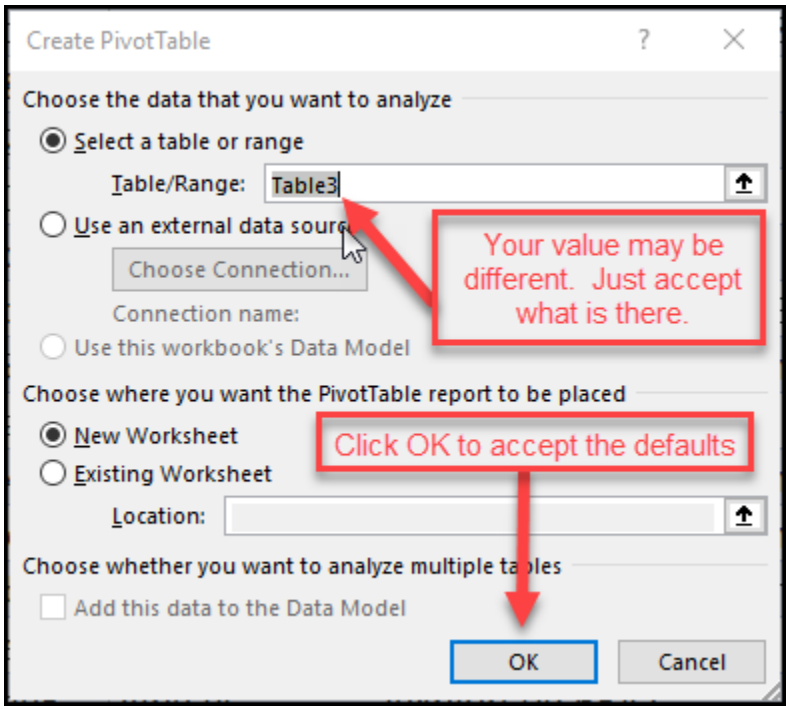
We will start by creating a pivot table from the "Poison Ivy Config Dumps.csv" file that we formatted with filterable columns earlier in this lab. That starting point looks like the screenshot below. We will then click the "Insert" tab and next click the "PivotTable" button similar to how we created the first Pivot Table.

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets
Technet24



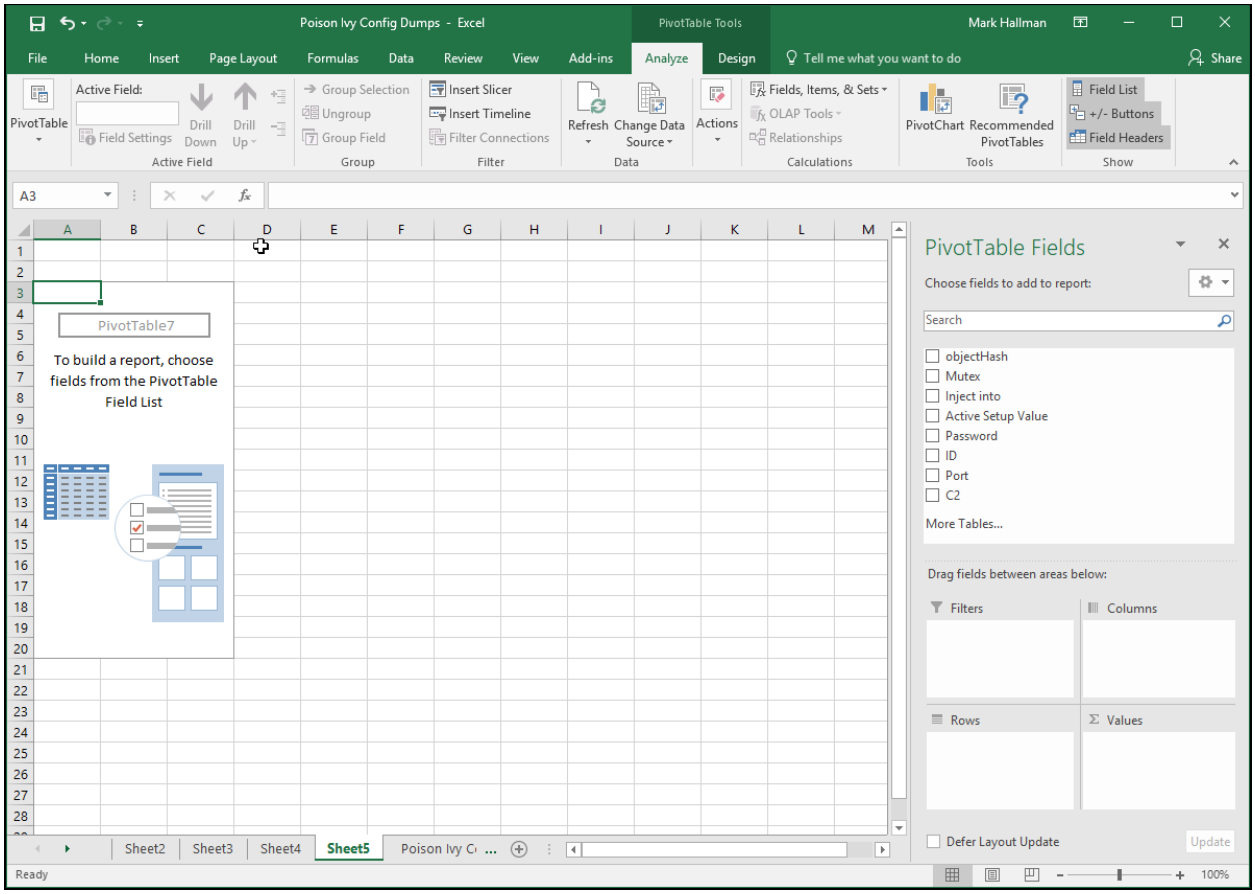
A dialog box, like the one shown below, will pop up. Accept the default values.



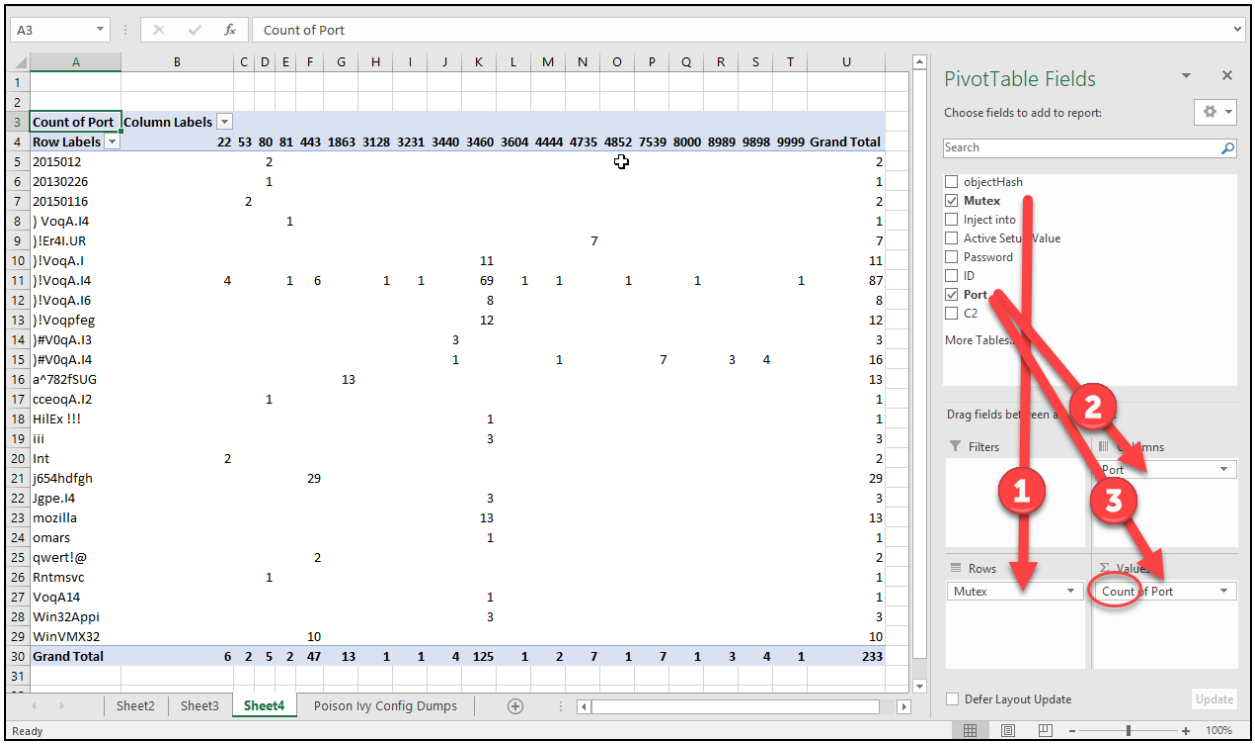
A blank pivot table will now appear in a new sheet within our workbook.

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets



Next, we will begin the creation of the pivot table by dragging columns to boxes that define the areas (like rows, columns, aggregation) of the pivot table. 1. Drag Mutex to the "Rows" box; 2. Drag Port to the "Columns" box; and 3. Drag Port to the "Values" box.

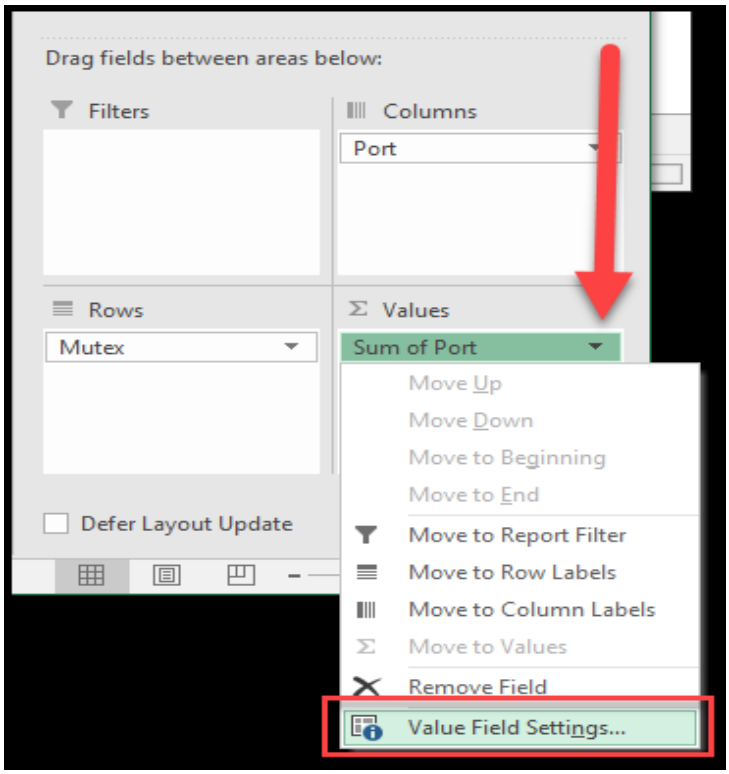


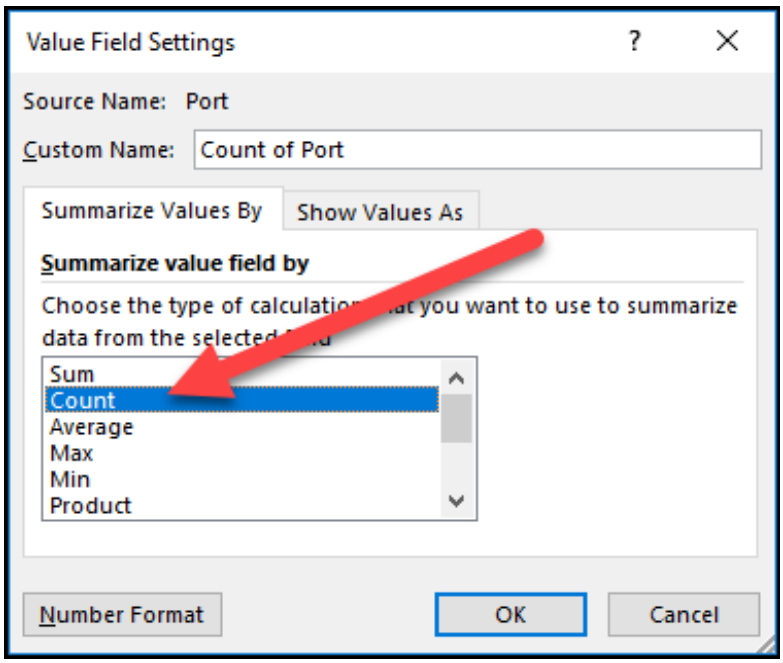
© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets

Technet24

Looking at our table, we might notice it looks odd—the values are too high. This is because Excel is adding together ports rather than counting them. We will need to change the default action of "Sum" on the "Values" field to "Count." We want the pivot table to count the number of ports, not find the sum of them. Click the arrow on the "Sum of Port" row in the Values box (bottom right-hand box). Select "Values Field Settings." Select "Count" from the Values Field Settings dialog box and click "OK."

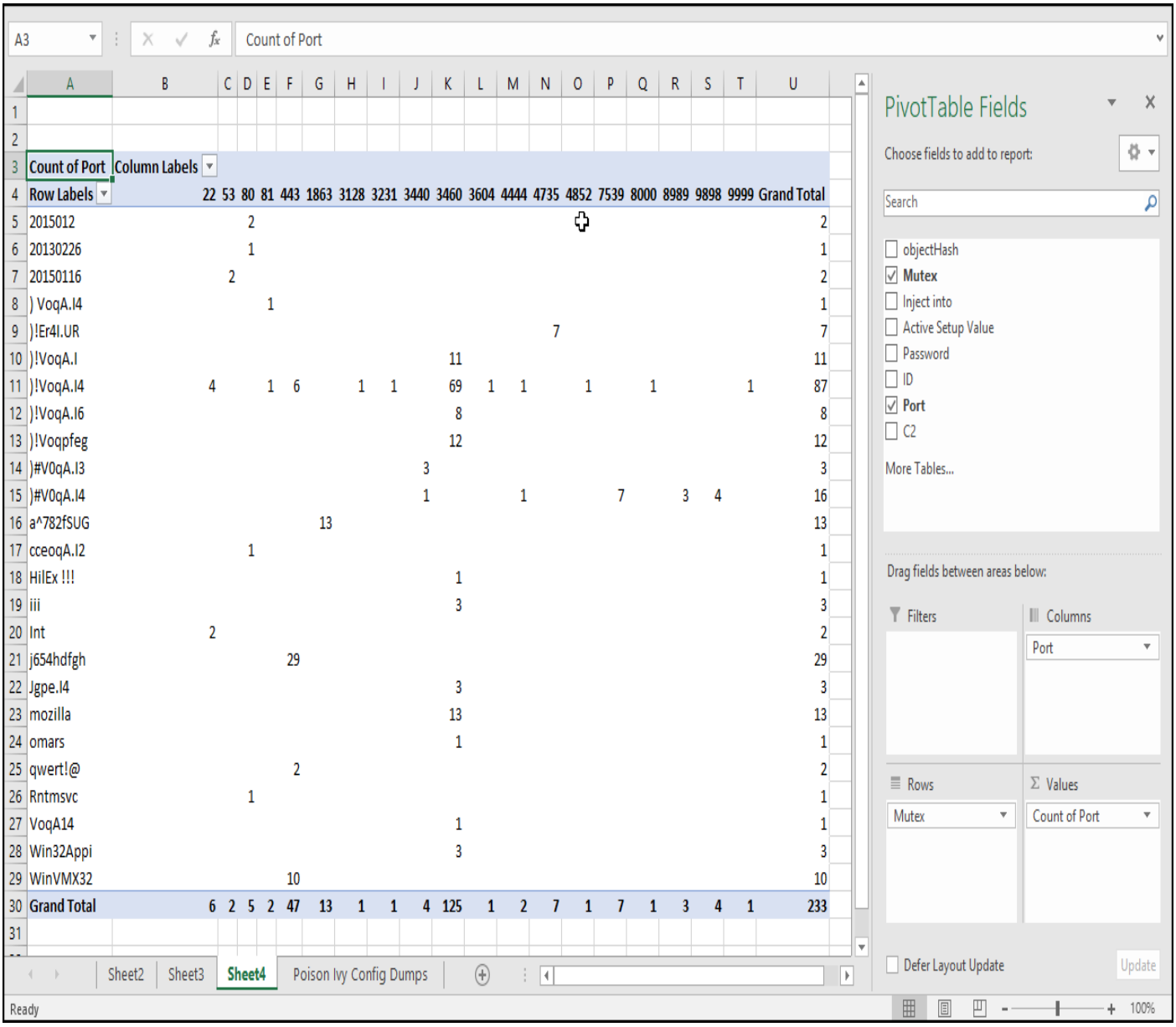




© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets

Our resulting pivot table should look like the screenshot below.



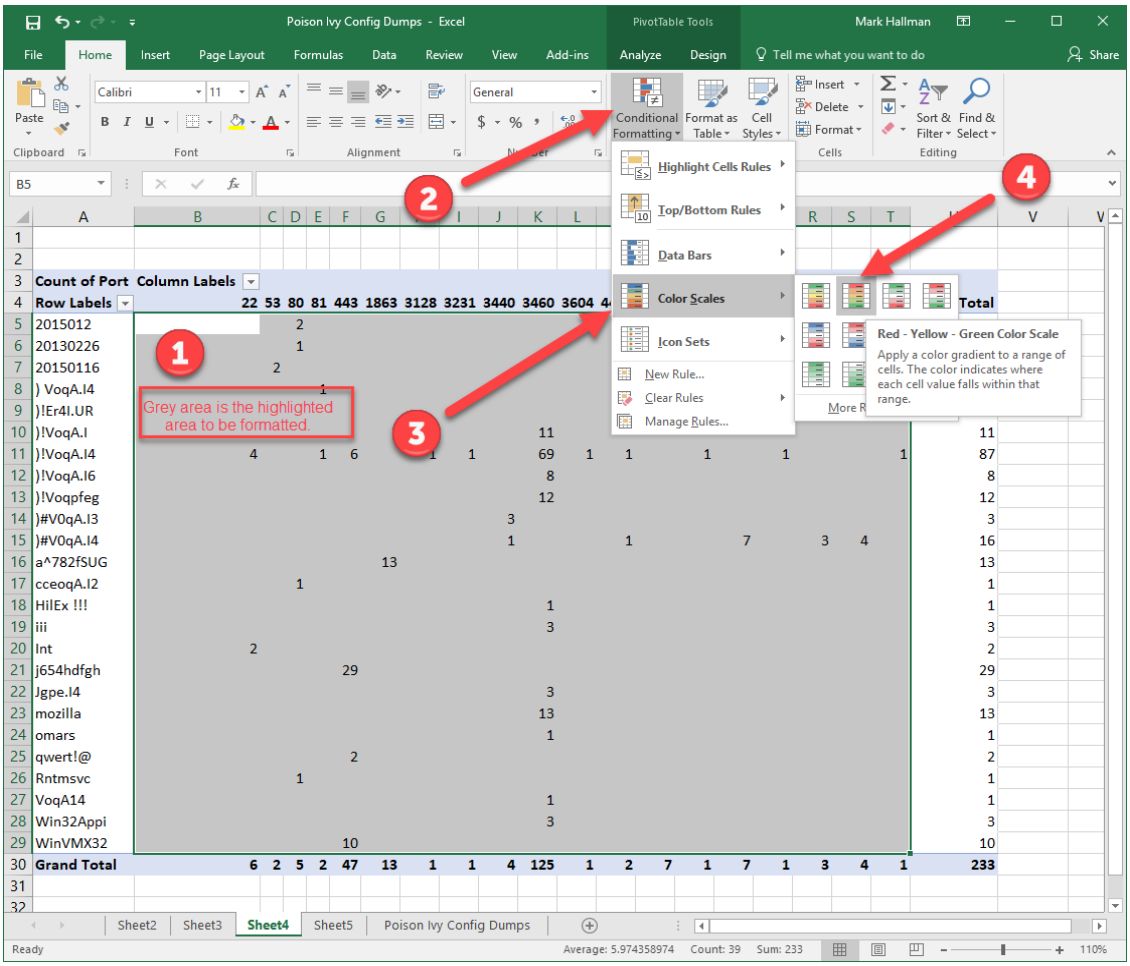
Count of Port	Column Labels																			
Row Labels	22	53	80	81	443	1863	3128	3231	3440	3460	3604	4444	4735	4852	7539	8000	8989	9898	9999	Grand Total
2015012			2																	2
20130226			1																	1
20150116		2																		2
) VoqA.I4				1																1
)!Er4I.UR													7							7
)!VoqA.I										11										11
)!VoqA.I4	4			1	6		1	1		69	1	1		1		1			1	87
)!VoqA.I6										8										8
)!Voqpfeg										12										12
)#V0qA.I3									3											3
)#V0qA.I4									1			1			7		3	4		16
a^782fSUG						13														13
cceoqA.I2			1																	1
HilEx !!!										1										1
iii										3										3
Int	2																			2
j654hdfgh					29															29
Jgpe.I4										3										3
mozilla										13										13
omars										1										1
qwert!@					2															2
Rntmsvc			1																	1
VoqA14										1										1
Win32Appi										3										3
WinVMX32					10															10
Grand Total	6	2	5	2	47	13	1	1	4	125	1	2	7	1	7	1	3	4	1	233

We will use "conditional formatting" to automatically create a heatmap of the data in the table with the highest values in red, middle values in yellow, and low values in green. (Excel automatically determines the range of our values.) To apply conditional formatting to an area, select the data to be formatted (1), followed by selecting the desired formatting style from the Conditional Formatting dropdown (2)—we will choose the "Red – Yellow – Green Color Scale" in this example, but you may choose whatever you'd like. Conditional formatting will colorize each cell according to its relative value among the set of cells highlighted, allowing for the easy creation of what are known as "heatmaps."

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets

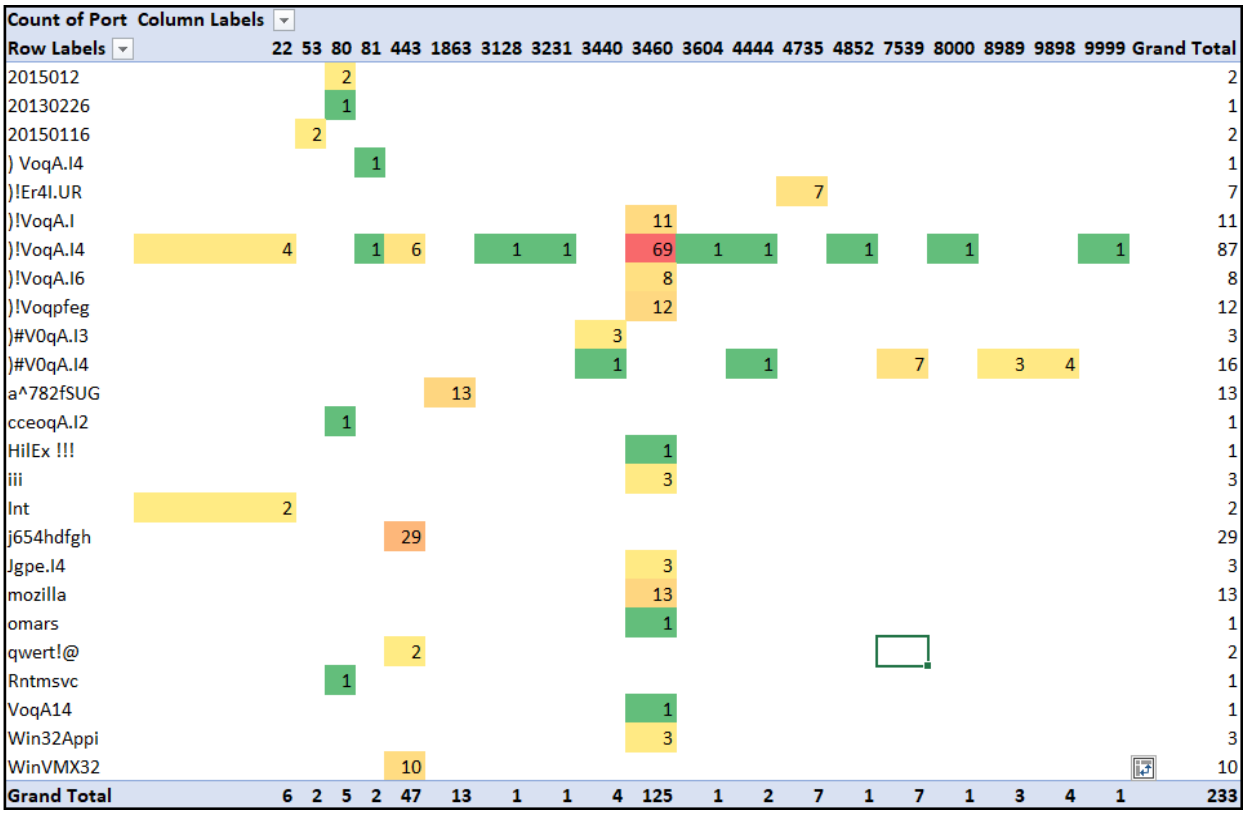
Technet24



After adding conditional formatting to the pivot table, it should look like the one below. By applying conditional formatting, we can clearly observe that the most frequent "Mutex-Port" combination is ")!VoqA.I4" and "3460." Often, the most frequently-used values in a dataset like this are the default, since some adversaries don't bother to change them. Therefore, we assess these are the default values for Poison Ivy.

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets



Count of Port	Column Labels																			
Row Labels	22	53	80	81	443	1863	3128	3231	3440	3460	3604	4444	4735	4852	7539	8000	8989	9898	9999	Grand Total
2015012			2																	2
20130226			1																	1
20150116		2																		2
) VoqA.I4				1																1
)!Er4I.UR													7							7
)!VoqA.I										11										11
)!VoqA.I4	4			1	6		1	1		69	1	1		1		1			1	87
)!VoqA.I6										8										8
)!Voqpfeg										12										12
)#V0qA.I3									3											3
)#V0qA.I4									1			1			7		3	4		16
a^782fSUG						13														13
cceoqA.I2			1																	1
HilEx !!!										1										1
iii										3										3
Int	2																			2
j654hdfgh					29															29
Jgpe.I4										3										3
mozilla										13										13
omars										1										1
qwert!@					2															2
Rntmsvc			1																	1
VoqA14										1										1
Win32Appi										3										3
WinVMX32					10															10
Grand Total	**6**	**2**	**5**	**2**	**47**	**13**	**1**	**1**	**4**	**125**	**1**	**2**	**7**	**1**	**7**	**1**	**3**	**4**	**1**	**233**

6. What is the significance of the findings in sections 4 and 5? **Hint**: Articulate your response in terms of the Diamond Model, the Kill Chain, and the properties of campaigns.

- **First, the team has identified additional indicators that represent more complete intelligence about the adversary's infrastructure in the C2 phase; this was the primary objective and fills intelligence gaps that were suspected to exist. We can now take Courses of Action on these indicators and try to identify additional activity. Second, additional TTPs were identified that reveal more about how the adversary prepares for and executes intrusions: There was no modification of the default Poison Ivy mutex, and there is a clear pattern in the user ID and passwords that are configured in Poison Ivy by this adversary.**

7. What are the indicators we could leverage going forward?

- **Mutex:)!VOqA.I4**
- **IPs: 61.221.40.61, 76.29.149.73, 76.29.149.78, 76.29.149.133, and 68.72.115.39**
- **Domains: helpdeskforu[.]net, itsupportnets[.]com, itservicesinc[.]net, and supportdesk[.]biz**

The indicators are all those that we could link back to the variants of Poison Ivy that could be tied to our original intrusion (Intrusion 6, the "Supply Denn" phishing email). You may choose different indicators based on those that resonate with you the most; the indicators chosen are those most likely useful to pivot off of and sweep our environment to reveal knowledge gaps that we previously had.

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets
Technet24

Exercise: Key Takeaways

- **CTI analysts can use Excel as an extremely powerful tool to help process, filter, and summarize large datasets.**

- **Analytical tools such as filtering, pivot tables, and conditional formatting can provide the analyst with a quick way to glean important information from large datasets. Imagine the power of using these tools with much larger datasets.**

- **Be sure to pivot/filter ("ask questions") through the data in all possible ways to accurately and completely analyze the subject data.**

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets

This page intentionally left blank.

https://t.me/learningnets

Technet24

Exercise 3.2: Domain Pivoting

Objectives

- Gain familiarity with online domain pivoting tools
- Pivot around data points to identify additional key intelligence

Scenario: You have been monitoring intelligence regarding the "Leet" adversary that has been targeting other companies operating in the same vertical business lines as Edison International with potential correlation to their recent incidents. We understand what the intrusion looks like in depth, but we have only pivoted on it internally or with shared information. Other tools and infrastructure ***might*** *have been used against you by the same adversary, which was not revealed in our Kill Chain completion.*

You shared back the new "Leet" set of intrusions to your peer who passed you the Poison Ivy samples we analyzed in Exercise 3.1, and it led them to find a new domain and IP address in their environment linked to the indicators you provided. They didn't note any overlaps, simply that as they were investigating these indicators, they found more.

Additionally, you just received an RFI from the Edison SOC analysts, who said a threat feed alert with the domain onixcellent.com just triggered on one of Edison International's devices that had been previously compromised (192.168.5.27), but they do not have any additional context.

Useful Indicators from your peer (linked to indicators you provided):
Domain: chishir.com
IP: 216.146.38.70

Indicator from SOC RFI on threat feed alert:
Domain: onixcellent.com

Please note: For students new to the tools presented in this lab, we recommend you follow the Step-by-Step guide to optimize your time in class. This will allow you to learn new tools while also performing analysis pertinent to our investigation.

Exercise: Prep

You will need your DomainTools account that you registered for in Lab 0

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets

Exercise: Questions

1. Is the domain that was passed by our peer (*chishir.com)* likely malicious?
   - _____
2. Is this domain likely adversary registered, dynamic DNS, or legitimate but compromised?
   - _____
3. Is the previously identified IP address (*216.146.38.70)* likely malicious?
   - _____
4. Is the domain flagged by our SOC analysts (*onixcellent.com)* likely malicious?
   - _____
5. What is the name of the Registrant that was used for the domain?
   - _____
6. What other domains have been registered by the same name as onixcellent.com?
   - _____
7. Is there any overlap between the indicators passed to the CISO and the domain reported by the SOC analysts?
   - _____
8. Is there any overlap between the indicators you found and the "Leet" set of intrusions?
   - _____

Because this is OSINT, your answers may differ from the lab; this is perfectly fine.

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets
Technet24

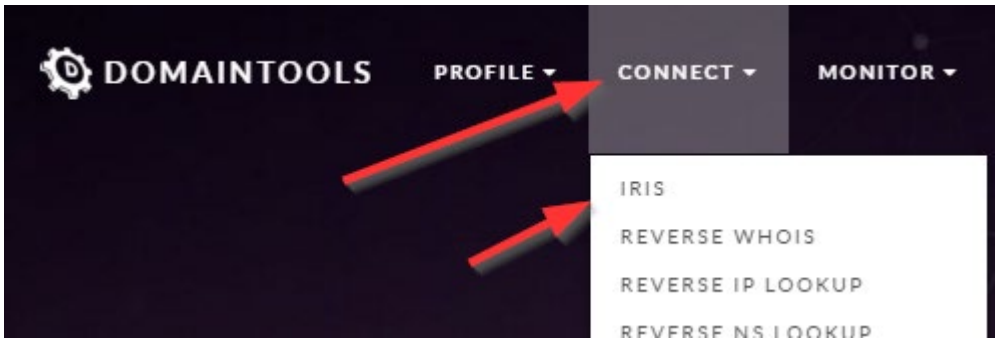
Exercise: Questions with Step-by-Step Guide

1. Is the domain passed by our peer (*chishir.com)* likely malicious?

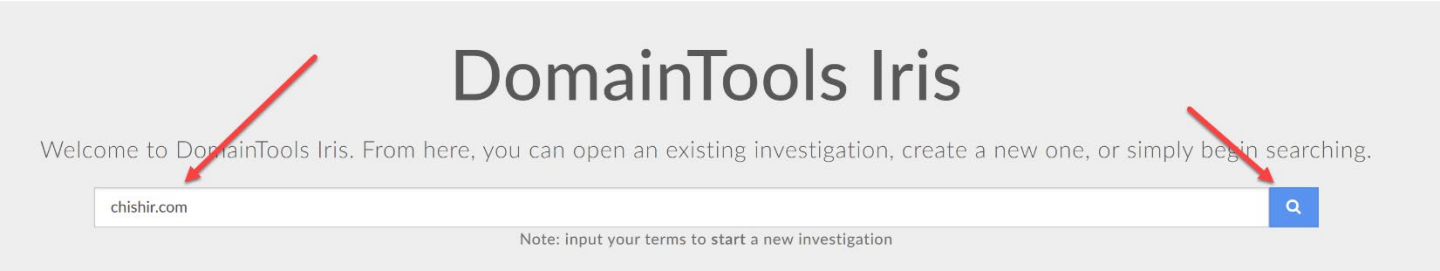
- **Yes**

In your browser, navigate to domaintools.com and log in with the account you registered during Lab 0.

On the DomainTools interface, navigate to Iris:



Type the domain (*chishir.com)* into the DomainTools Iris search bar and click the blue magnifying glass.

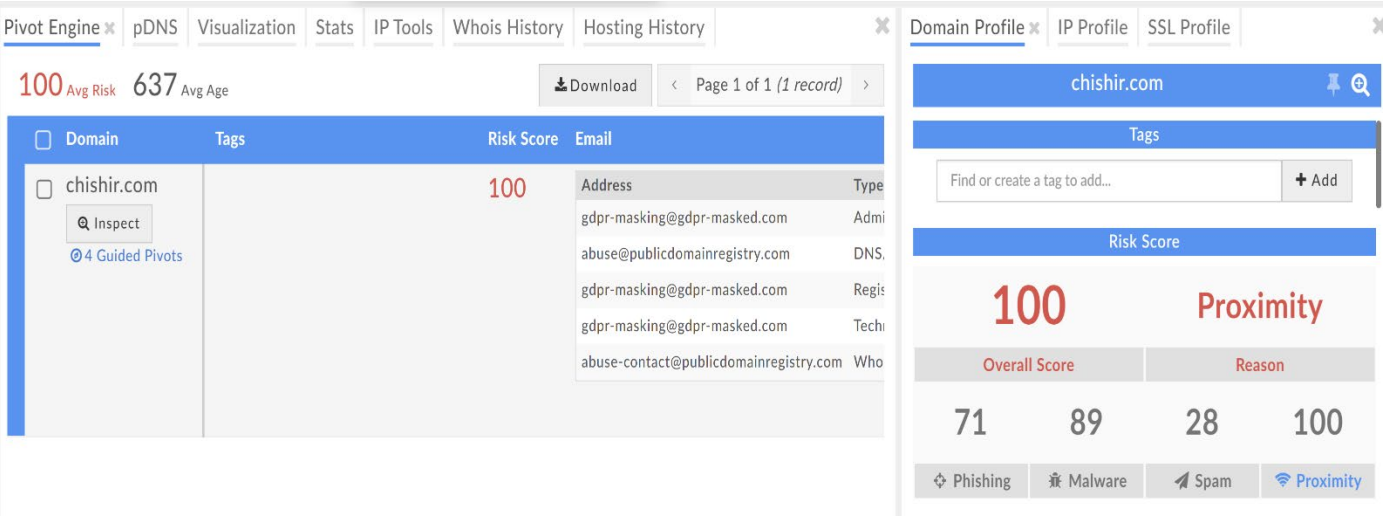


The default tab is the Pivot Engine, which shows a high-level view of different searches done, the available information, and any correlation with other information available. Here, we can right-click on an indicator and get a menu of additional query options for the new indicator or expand the current search by including the indicator as a search term in the query box above the results tabs. We can navigate different tabs simply by selecting them at the top or bottom of the browser in the respective toolbars.

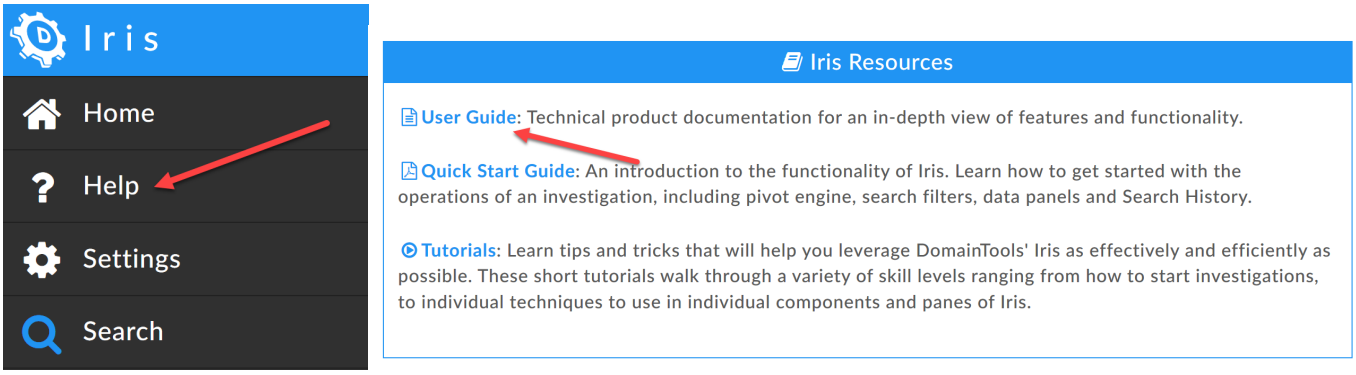
Here, we see the domain has a Risk Score of 100. Without further research, we do not know why DomainTools classifies this domain as a high risk, but this fits into the assumption that this is a malicious domain. This is not enough for us to fully validate that this is a malicious domain, but it is enough to go off of right now.

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets



If we want to get more information on what DomainTools means by "Risk Score," we can navigate to the Help menu and click on "User Guide," and by searching documentation, we come to the below page that explains "Risk Score." It is good for analysts to get in the habit of understanding how the tools they use define different values.



Question:

What is the Risk Score?

Answer:

Available as an optional Iris add-on, the DomainTools Risk score predicts how likely a domain is to be malicious. The score comes from two distinct algorithms: Proximity to Known Maliciousness examines how closely connected a domain is to other known-bad domains, while Threat Profile leverages machine learning to model how closely the domain resembles others used for spam, phishing or malware. The strongest signal from either of those algorithms becomes the overall Risk Score.

(https://www.domaintools.com/support/what-is-the-risk-score)

2. Is this domain likely adversary registered, dynamic DNS, or legitimate but compromised?

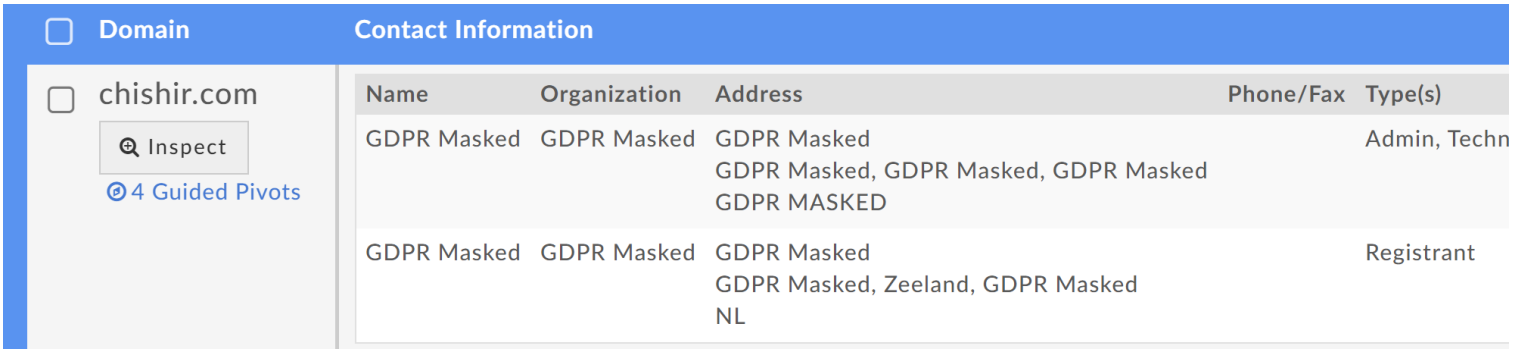
- **Adversary Registered**

In the Pivot Engine view, we see that the Contact Information for the domain is masked by the General Data Protection Regulation (GDPR) data privacy requirements (https://gdpr-info.eu/), so that does not give us much to go off of. There are several other indications of the nature of the domain, however.

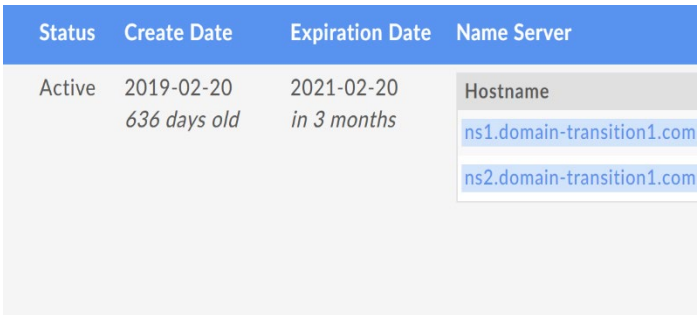
© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets

Technet24



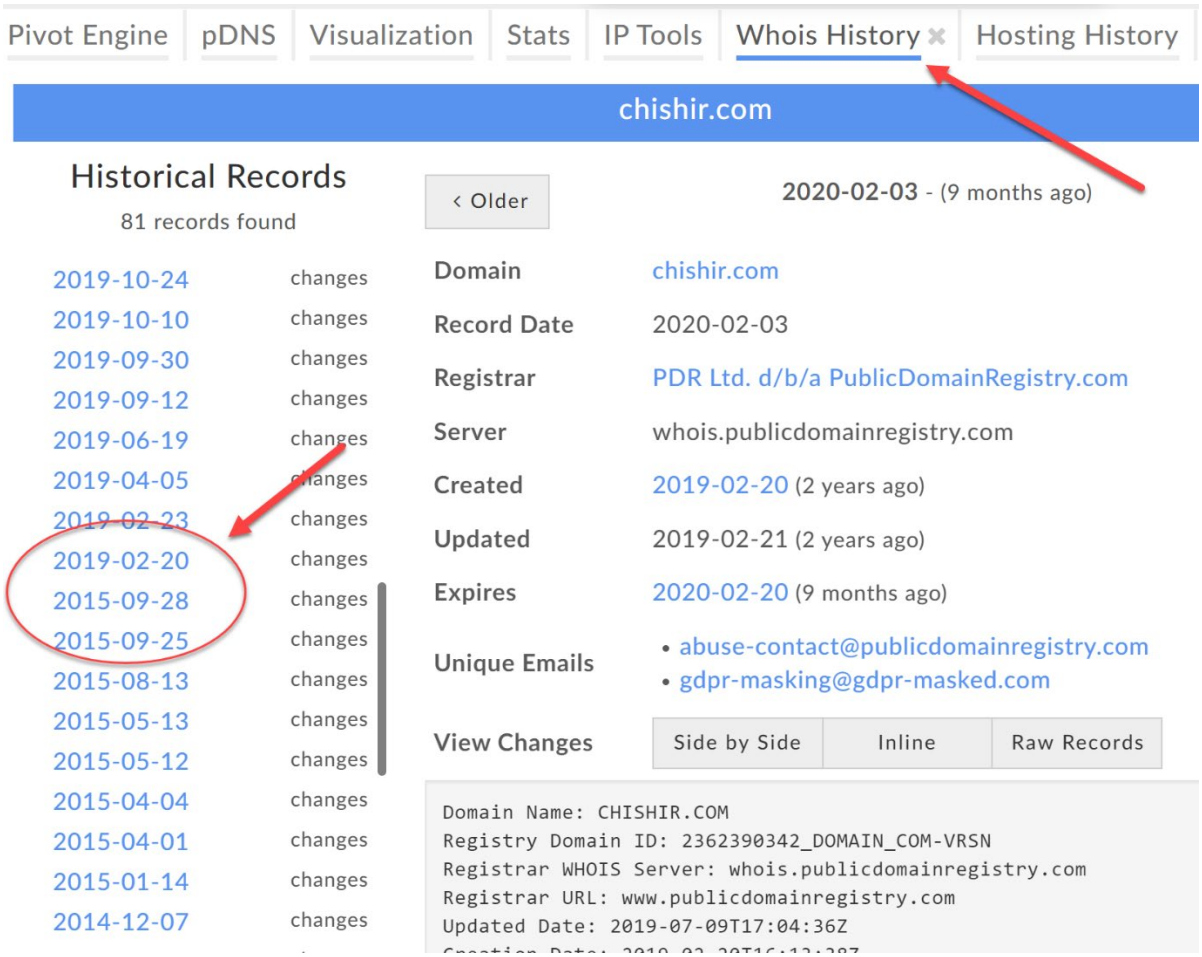
Registration information available as we scroll to the right of the Pivot Engine window shows the domain was registered on 2019-02-20.



By going to the Whois History tab, we can see that there are 81 historical records (at the time of this lab creation; your results will likely differ) that date back to 2010. However, there is a four-year gap between 2015 and 2019 where the domain was not active.

© 2021 Robert M. Lee and SANS Institute

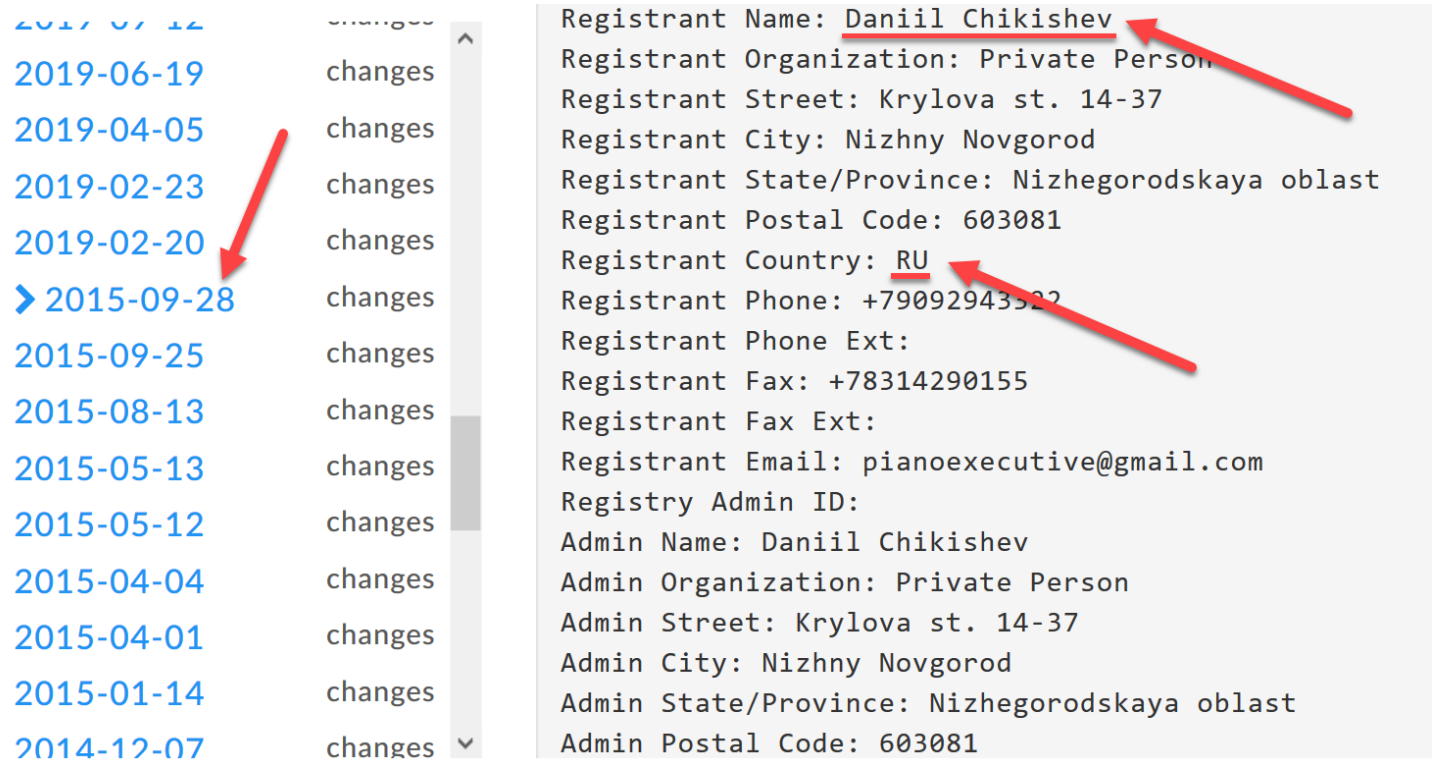
https://t.me/learningnets



Reviewing the Whois history shows that in 2015 and prior, the domain was registered to an individual named "Daniil Chikishev" who was reportedly in Russia (we need to remember that this information can be spoofed); however, that registrant let the domain expire and it sat dormant until it was re-registered in 2019.

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets
Technet24

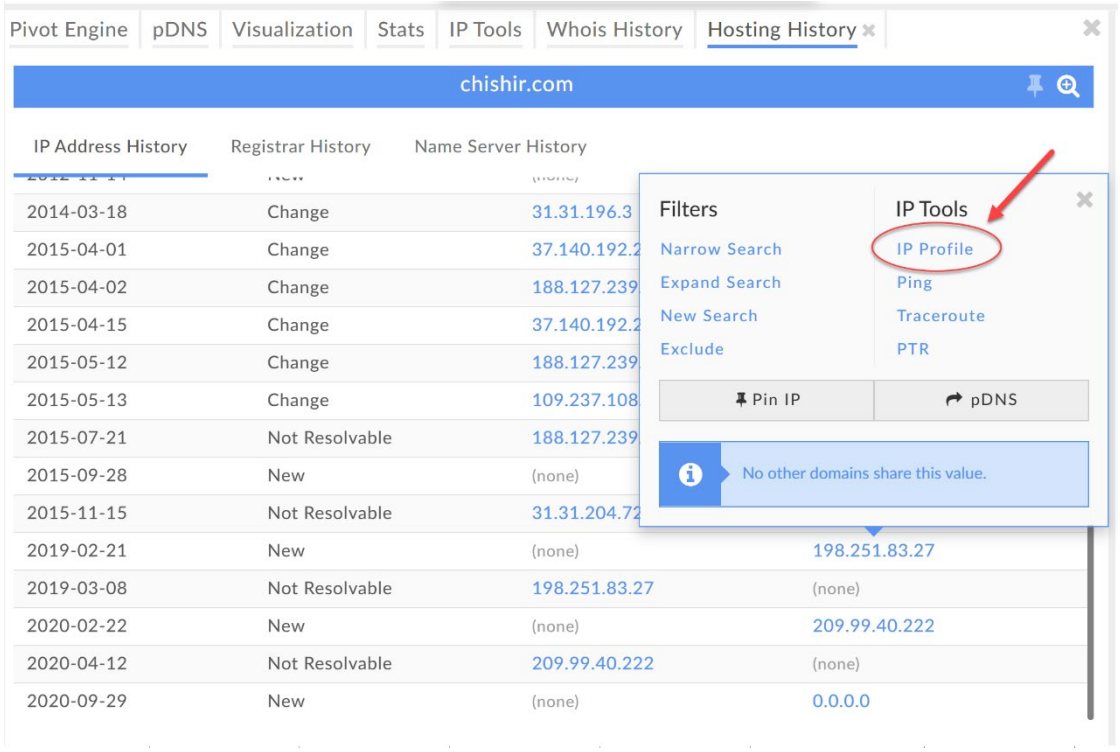




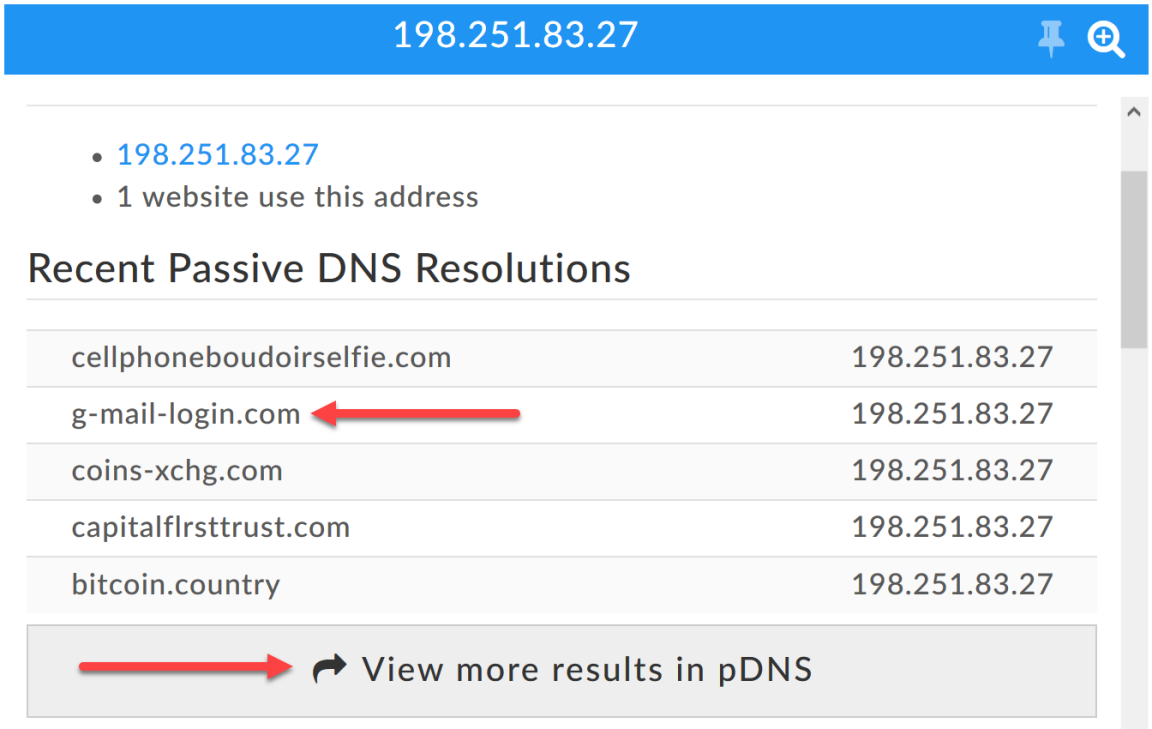
Go to the Hosting History tab and review the IP address history. Based on the Whois information, we assess that we can ignore the activity prior to the 2019 registration. We see that it has resolved to two IP addresses in between being parked (not resolving to anything). Right-click on the first IP address, 198.251.83.27, and select IP Profile to get a quick snapshot of that IP.

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets



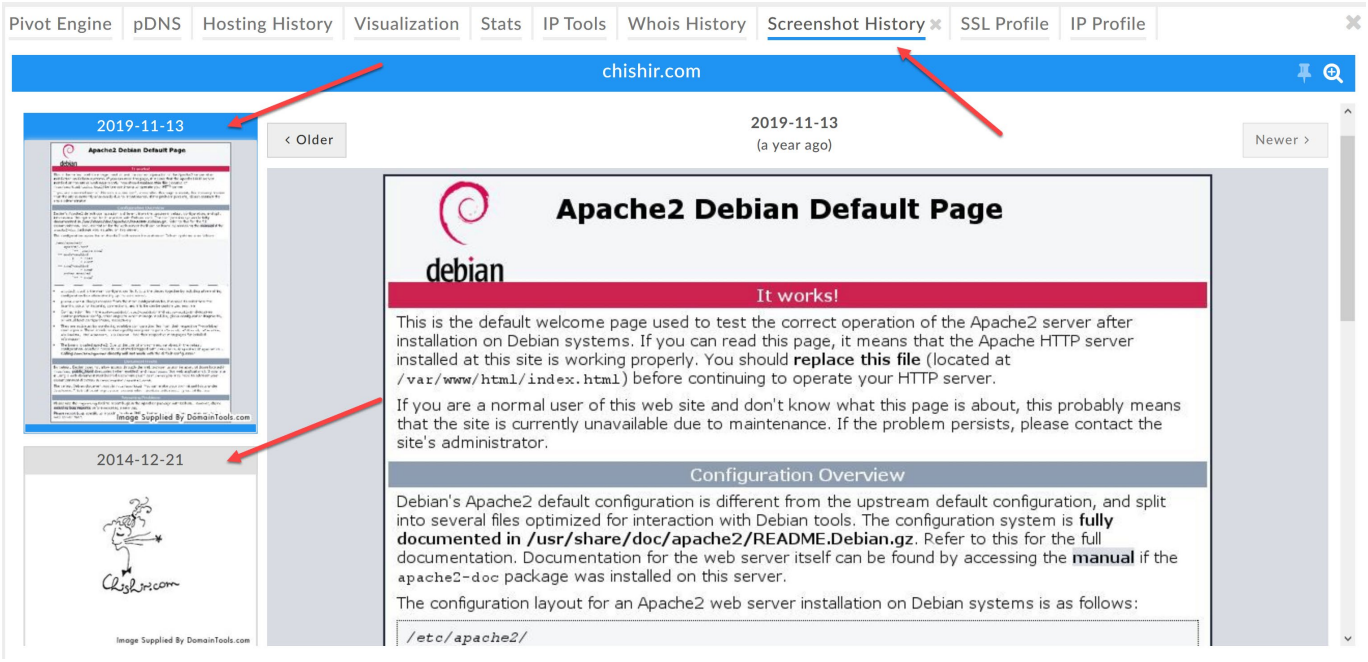
The IP Profile shows that the IP has a Risk Score of 71, which is relatively high, and Passive DNS shows resolutions to other suspicious looking domains, such as g-mail-login[.]com, which appears to be a typosquatting domain (when a domain attempts appear legitimate). DomainTools shows us the most recent Passive DNS resolutions, and by clicking on "View more results in pDNS," we can see the full results.



© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets
Technet24

Finally, we can check the Screenshot History navigating to the "Screenshot History" tab. As we analyze the screenshot history on the left, we can see that, while the domain appeared to have some sort of a website in 2014, it has had the Apache2 default page displayed since being re-registered, meaning that while the domain has been registered and is being hosted, there is not web content associated with it. While there are other possible explanations for this, this does suggest that it may not be a legitimate website.

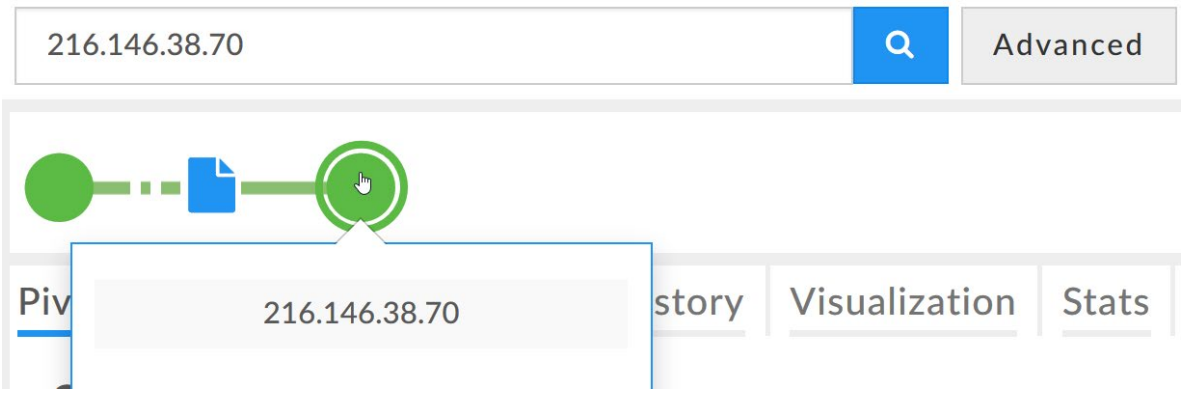


None of these details are conclusive; however, when combined, they do support the assessment that this malicious domain was likely registered by an adversary to support their operations.

3. Is the previously identified IP address (*216.146.38.70*) likely malicious?

- **No**

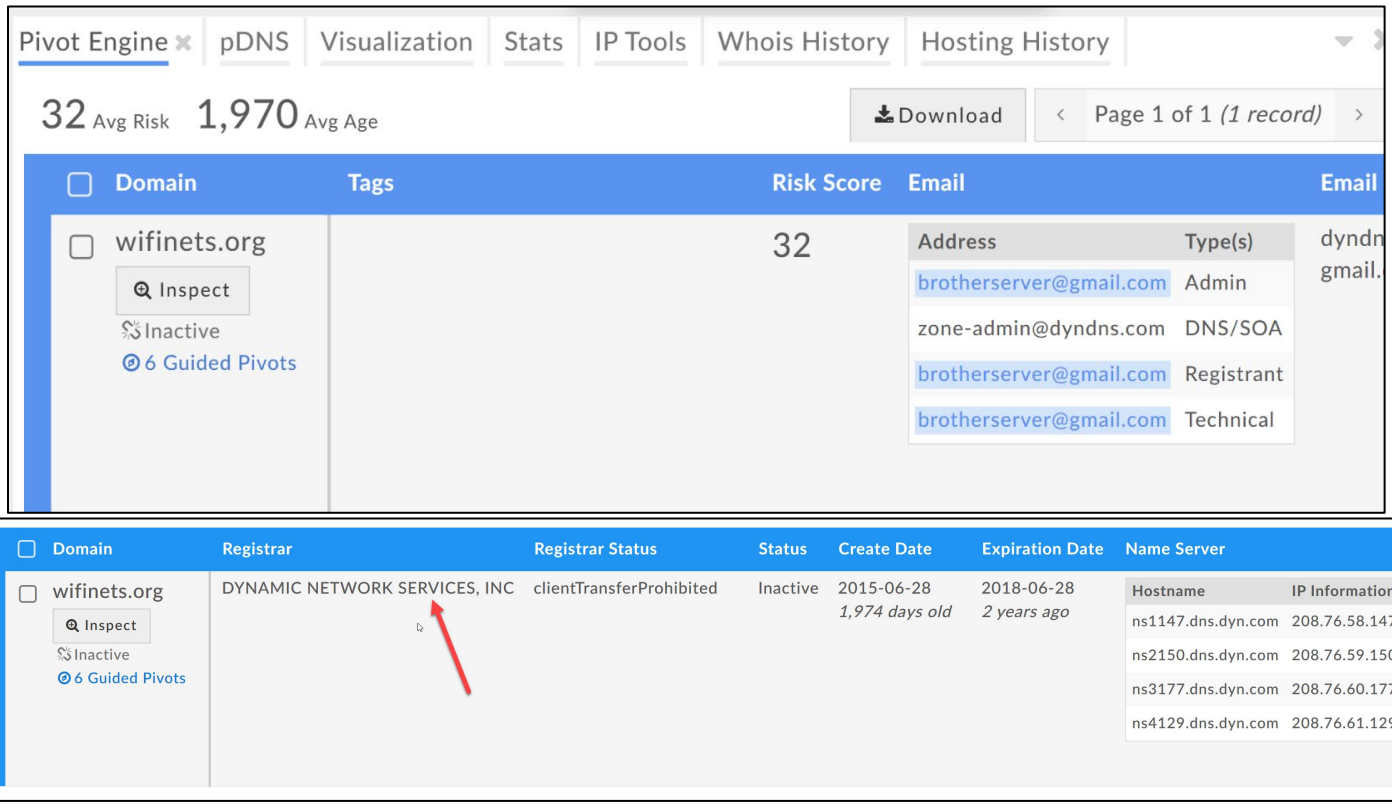
Navigate back to the Pivot Engine tab and start a new search by entering the IP address 216.146.38.70 in the top search bar, and then pushing enter or clicking the search icon. Note that DomainTools tracks your search history with circles along the top to help you track where you are.



© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets

There are multiple domains listed in the Pivot Engine with varying degrees of proximity to the IP address in question. If you scroll all the way to the right of the Pivot Engine page, you will see that the IP address is linked with Dynamic Network Services, or Dyn, a domain registration service. This signifies that this IP address is not a unique indicator, since domain registration service IPs generally host many different domains for different registrants, so this IP may not be useful in detecting malicious activity. However, it can still be useful for understanding the intrusion because there was a malware sample that called out to it.



Switch to the pDNS (Passive DNS) Tab and sort by "Last Seen" dates, with the most recent dates at the top, by clicking twice on the "Last Seen" column header. This allows us to view the most recent passive DNS resolutions for the IP address. At the time of this exercise creation, all of the most recent resolutions for the IP address have related to checkip.dyndns[.]com or similar domains (your view may look different, but as you scroll through the domains, you should see the domains in the below screenshot).

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets
Technet24

Pivot Engine | pDNS | Visualization | Stats | IP Tools | Whois History | Hosting History | Screenshot History

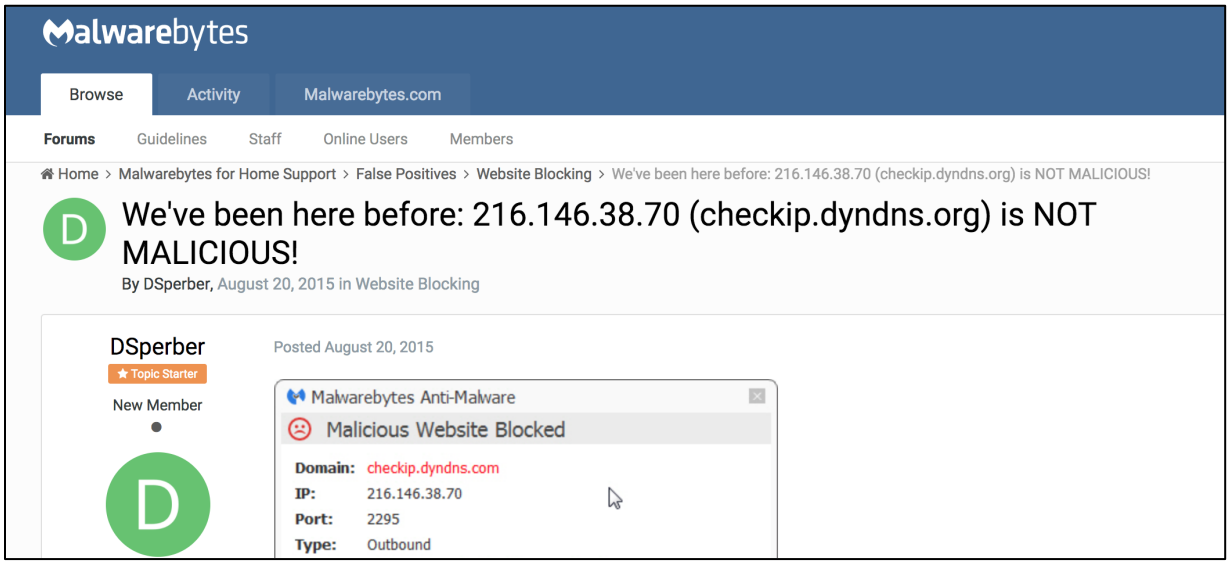
216.146.38.70

Note: wildcards (*) may be used for either hostname or tld.

Record Type:	Source:	Result Limit:	After Date:	Before Date:
A	All	500	YYYY-MM-DD	YYYY-MM-DD

Query	Type	Source	Count	Response	First Seen	Last Seen
checkip-iad.dyndns.com	A	D	55268	216.146.38.70	2011-05-18, 15:02	2020-11-18, 04:06
checkip-iad.dyndns.com	A	A	1	216.146.38.70	2014-09-04, 00:00	2020-11-17, 23:59
checkip-iad.dyndns.com	A	B	1	216.146.38.70	2020-10-22, 17:32	2020-10-22, 17:32
checkip.dyndns.org	A	A	1	216.146.38.70	2015-11-19, 00:00	2020-07-07, 23:59
checkip-iad.dyndns.com	A	C	19	216.146.38.70	2015-10-08, 10:53	2020-04-07, 10:52

While DomainTools gives us a good starting point, we should supplement our findings with other open-source searches to try to add information. At this point, we can do a quick Google search on the IP address, which will reveal that the website hosted at the IP address 216.146.38.70 tells users their external IP address. It is common for various types of malware to use a domain or service like this to determine the external IP address of victims after they gain initial access to the machine, and these domains and IPs will commonly show up as related to a malware sample. Some of the searches that return show just how common it is for this IP address, and other external IP address checks, to be flagged incorrectly as malicious. Based on a forum posting in Malwarebytes, it looks like other users have been confused by this IP as well, though we should treat forum postings like this carefully and evaluate other information as well.



(https://forums.malwarebytes.com/topic/164980-2161463870-checkipdyndnscom-is-legitimate/)

This IP is not likely malicious, but we may look to Discover or Detect its use in our network to reveal potentially infected systems if this activity is not normally seen in our network. If it is not a needed address, it could also be blocked. Many organizations block dynamic DNS services as a precaution.

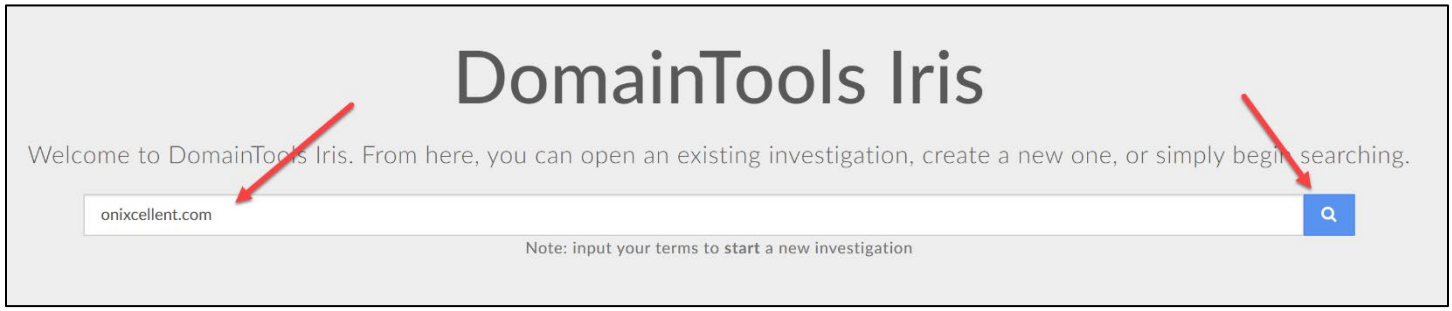
© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets

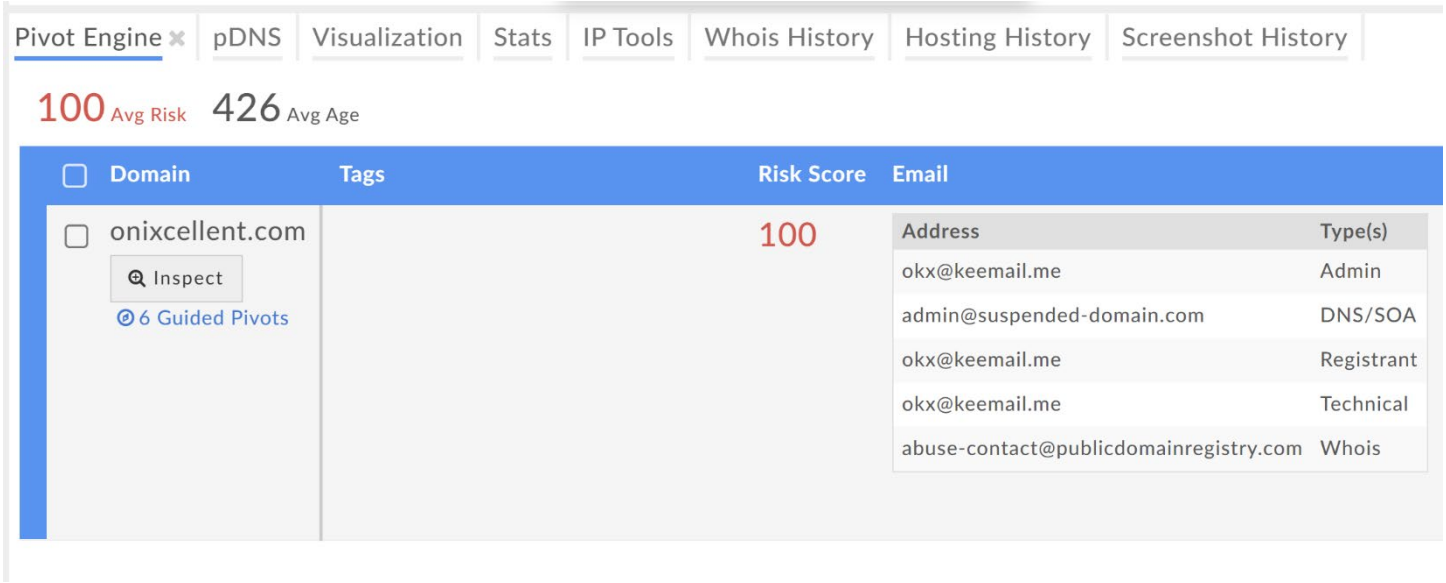
4. Is the domain flagged by our SOC analysts (*onixcellent.com)* likely malicious?

- **Yes**

Click the "Home" icon on the left to return to the search engine. Enter the domain and click the search icon.



DomainTools defaults to opening the tab you last used. If you are not already on the Pivot Engine, click on that tab. Similar to the previous domain we analyzed, this one also has a risk score of 100.



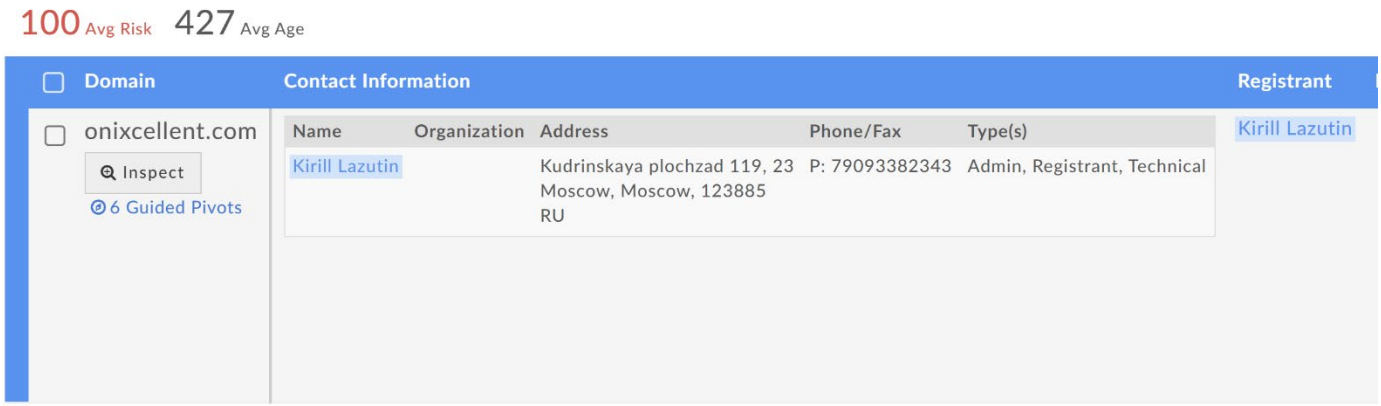
5. What is the name of the Registrant that was used for this domain?

- **Kirill Lazutin**

Registrant names can be interesting things to identify to correlate domains together. It is not definitive but sometimes can be a key indicator, especially when chosen by the adversary. From the Pivot Engine we can scroll over to "Contact Information", and we see that the contact information is not protected by a privacy services, which gives us additional information we can pivot from.

© 2021 Robert M. Lee and SANS Institute

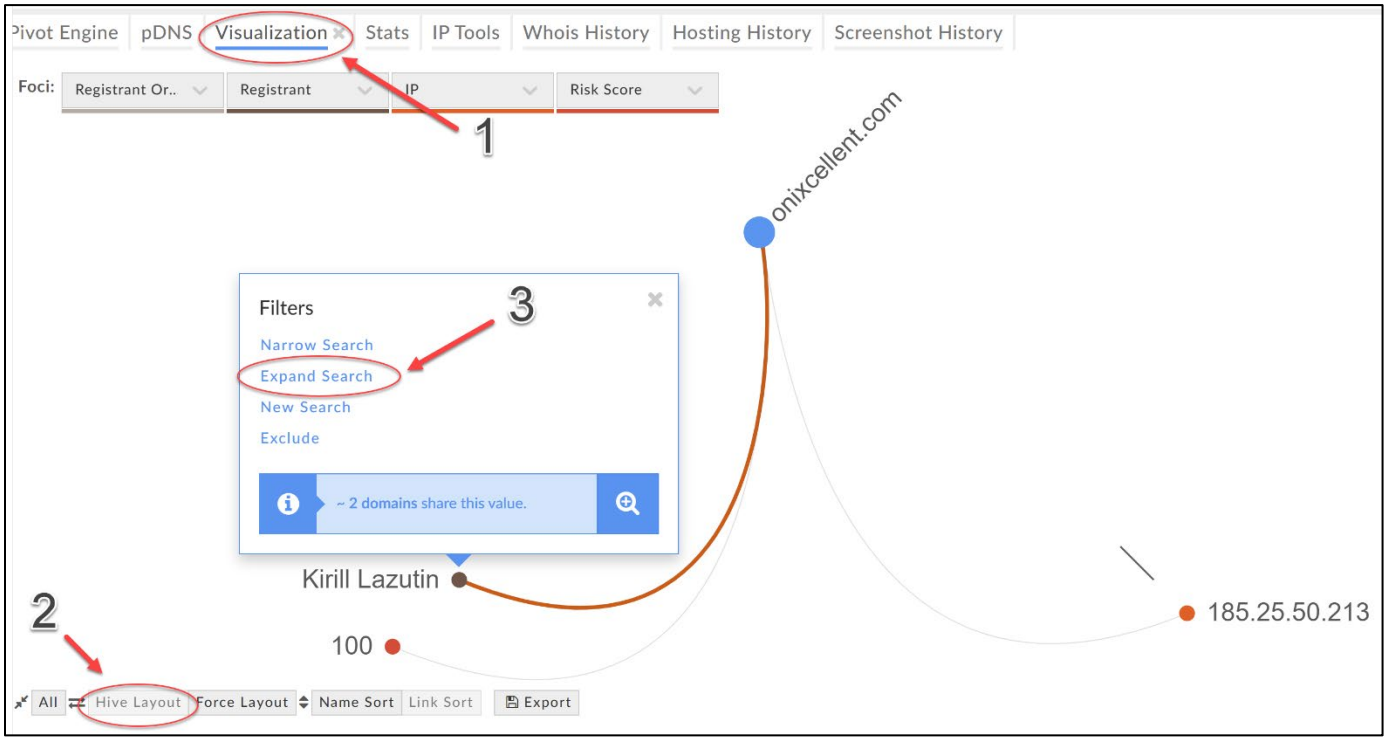
https://t.me/learningnets
Technet24



6. What other domains have been registered by the same name as onixcellent.com?

- **eng-academy.org, ladysasha.xyz, parmezan.pro, rabidpandashop.com, шефмегаполис.рус, шефшоп.рус**

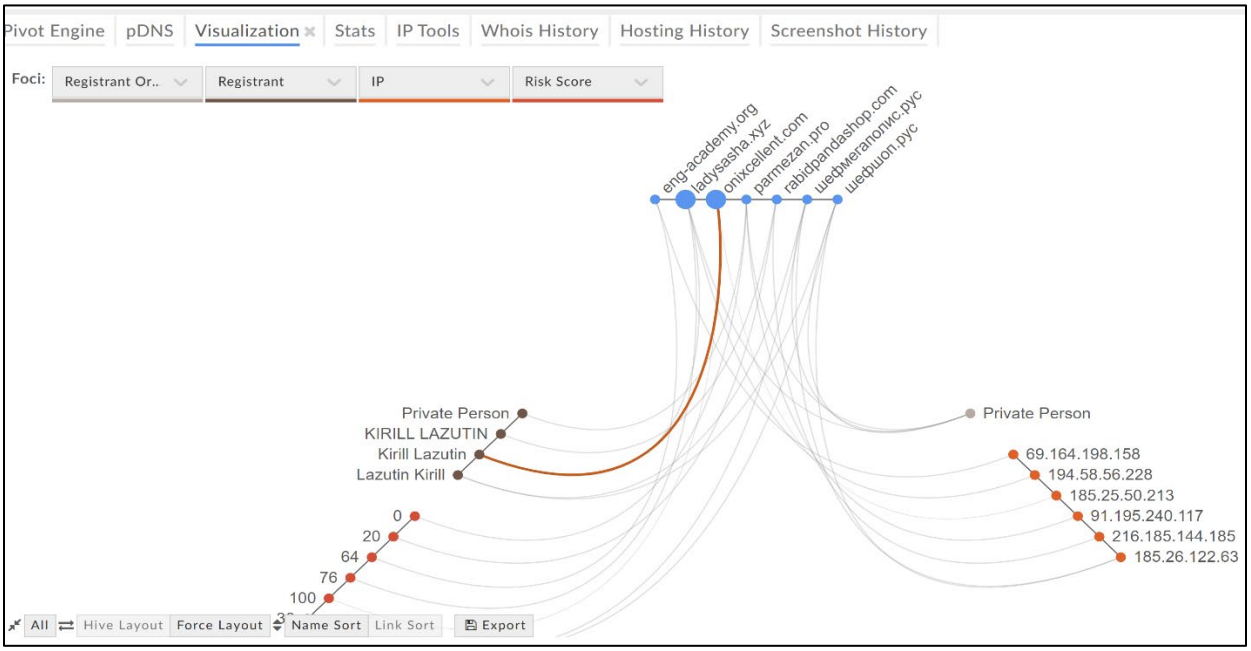
The easiest way to identify this information in DomainTools is to click on the Visualization tab in the top toolbar, which will show a visual representation of all the information linked together. Select "Hive Layout" on the bottom if it is not already selected. On the visualization, find the name we identified in the last question, "Kirill Lazutin," and right-click it (your node may appear in a slightly different location than the below screenshot). From the menu that pops up, select "Expand Search" to include other entities associated with the name.



© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets

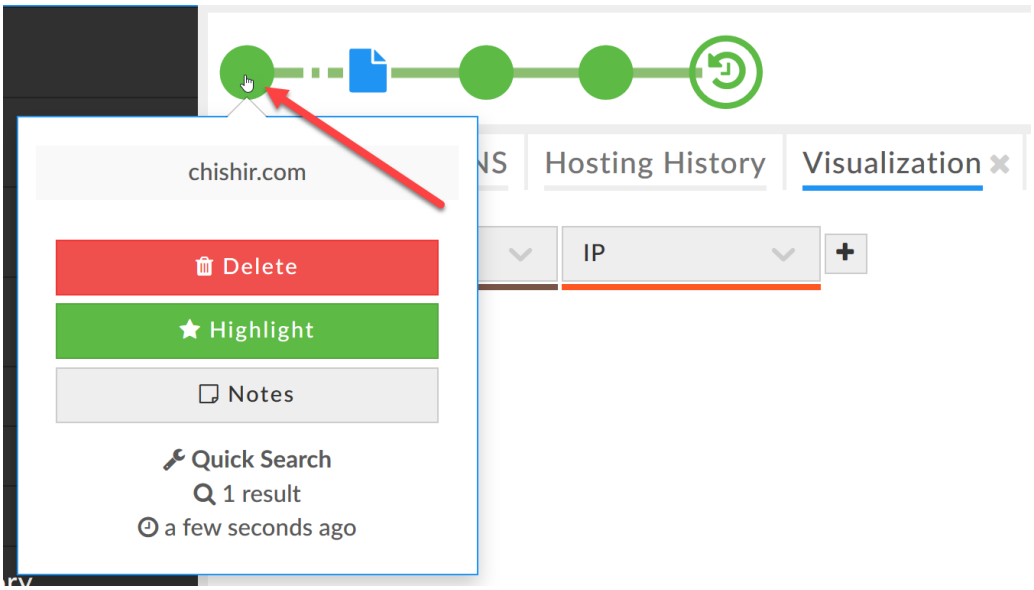
Now, we see that that the Registrant "Kirill Lazutin" is tied to several other domains and IP addresses. Furthermore, we see several variations of this name, including "KIRILL LAZUTIN" and "Lazutin Kirill" have been used with these domains. Depending on the "Foci" you have selected in the upper left, your visualization may look slightly different than the below. Click the "+" icon to add additional Foci if you choose, but as long as you have the Foci for Registrant and IP selected, you can identify the significant overlaps.



7. Is there any overlap between the indicators passed to the CISO and the domain reported by the SOC analysts?

- **<u>Yes, the name server</u>**

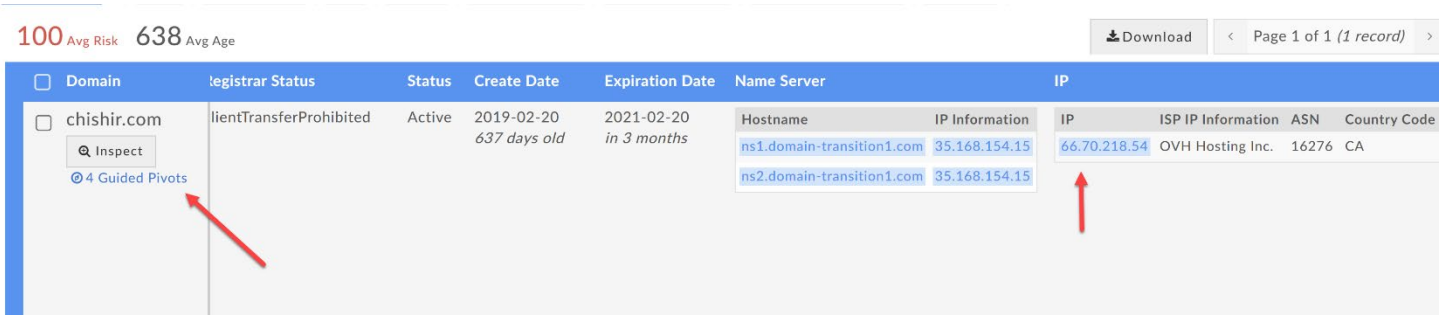
In the top navigation bar, click on the first green circle that was our search for "chishir.com" to return to that search.



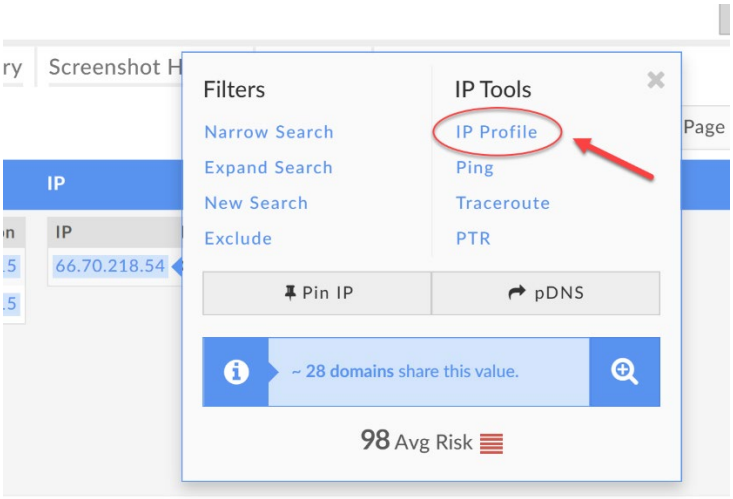
© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets
Technet24

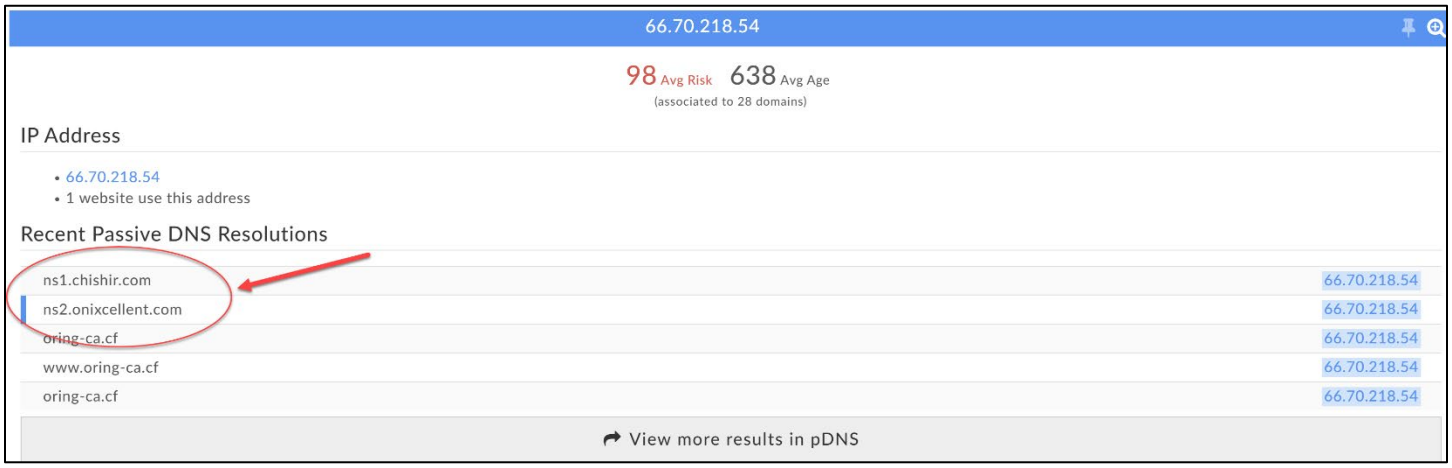
From the Pivot Engine, we see that there are 4 Guided Pivots off of this domain, including an IP address from OVH Hosting (we need to scroll over to the right to see this).



Right-click the IP address 66.70.218.54 and select "IP Profile"



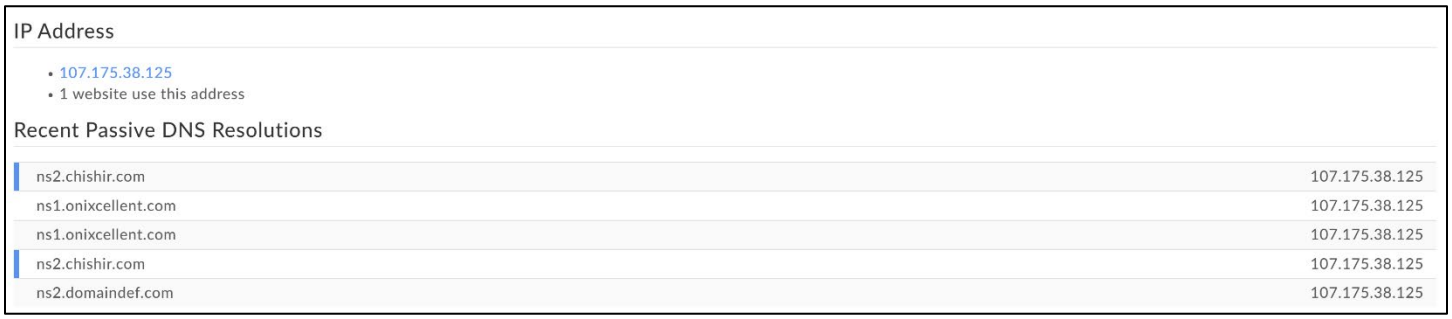
We see that the IP have a high Risk Score itself (98). Additionally, under recent Passive DNS resolutions we see name server domains (which we identify based on them starting with "ns1" and "ns2", a naming pattern used by name server domains) that are associated with both chichir.com, which was flagged to the CISO, and onixcellent.com, which was reported by the SOC. This suggests those two indicators, and therefore the two incidents, may be related.



© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets

Additional exploration into this IP address or these name servers could potentially reveal even more overlap. For example, reviewing the passive DNS resolutions of the name servers circled above reveals a second IP address overlap between the two domains of 107.175.38.125.


IP Address

- 107.175.38.125
- 1 website use this address

Recent Passive DNS Resolutions

ns2.chishir.com	107.175.38.125
ns1.onixcellent.com	107.175.38.125
ns1.onixcellent.com	107.175.38.125
ns2.chishir.com	107.175.38.125
ns2.domaindef.com	107.175.38.125

8. Is there any overlap between the indicators you found and the "Leet" set of intrusions?

- **No**

It's compelling to start linking these datasets together because we're making interesting finds. However, nothing here has shown any overlap with the "Leet" intrusions either in indicators or in behavioral overlaps. The only potential overlap is that the same victim system (192.168.5.27) that was once compromised by "Leet" was also apparently compromised by this new intrusion. But that is a very bad link without much stronger forensic evidence to tie it together.

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets
Technet24

Exercise: Key Takeaways

- **The ability to use starting points and build around each through the pivoting process is a critical skill for CTI analysts. You can see how to move from few data points to many through exploiting external data sources.**

- **External data sources can be just as critical as internal data sources in validating, understanding, and scoping the threats to your organization.**

- **Linking the events that were reported from external sources to information received from internal sources can start to build a pattern of activity. After confirming the malicious nature of the domain the SOC flagged, we can ask them to search for the additional indicators provided to the CISO and then share any additional information back to the reporting party.**

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets

This page intentionally left blank.

https://t.me/learningnets

Technet24

Exercise 3.3: Open-Source Intelligence

Objectives

- Identify additional information about the malicious IP address identified during the investigation
- Identify additional IOCs that are potentially related to your investigation
- Identify which IOCs require additional actions or investigation

Scenario: We previously gathered indicators related to the intrusions we faced in Day 2. We had not used OSINT to enrich those indicators, though. In Day 3's material, we've been able to find overlaps that are interesting with various intrusions, including now the larger "Leet" set. We had another configuration IP address we have not previously leveraged and we should determine if there's any new pivots or interesting information that can be revealed using it.

Previous Useful Indicator from Exercise 2.1
IP Addresses: 38.72.114.16
(IP in malware config data in "Invoice.docx" attachment from Supply Denn phishing email)

Exercise Prep

You will be using the web applications AlienVault OTX and VirusTotal as well as the command-line tool Automater, which will be run from the SIFT VM.

You will need internet access for this lab and will use a browser of your choice.

You will utilize the following sites in this lab:

www.virustotal.com
otx.alienvault.com

Note: This lab involves running live OSINT queries and, therefore, may return different or more information than the responses in the step-by-step walkthrough. The focus of this lab is to identify additional information, and as long as you follow the identified processes, you will be identifying valuable information about your target, even if it does not match the examples exactly.

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets

Exercise: Questions

1. Using the tool Automater, what potentially malicious domains are associated with the IP address 38.72.114.16?

   - _____

2. What malware sample(s) have communicated with this IP address?

   - _____

3. What type of threat is the malware associated with?

   - _____

4. From VirusTotal, what are the filenames associated with the hash(es) and when was the file created?

   - _____

5. From AlienVault's Open Threat Exchange, what threat(s) are associated with the domains linked to the IP?

   - _____

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets

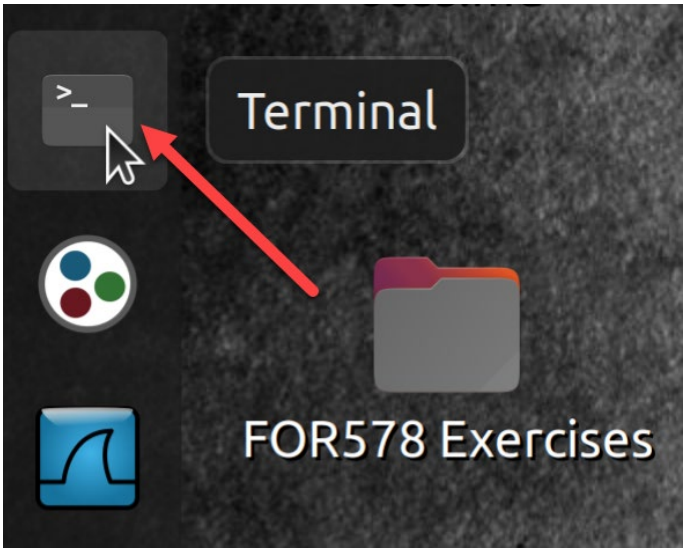
Technet24

Exercise: Questions with Step-by-Step Guide

1. Using the tool Automater, what potentially malicious domains are associated with the IP address 38.72.114.16?

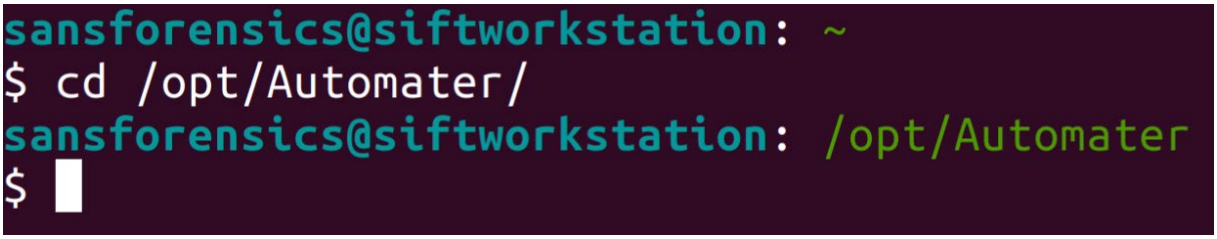
- **yo.acmetoys[.]com, ea.onmypc[.]info, mmy.ddns[.]us, nz.compress[.]to**

In the SIFT VM, open a terminal by clicking on the left menu.



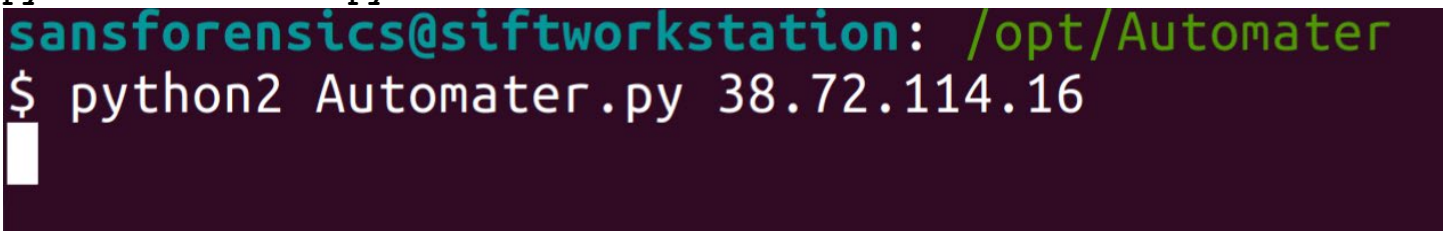
From our terminal, run the following command and press "Enter" to change directories to "/opt/Automater/", which is where the Automater tool is installed on our VM:

```
cd /opt/Automater/
```



Next, enter the following command to run the Python-based Automater tool on the IP address 38.72.114.16 (it may take a few moments for the tool to run; if it fails, make sure our SIFT VM has internet connectivity):

```
python2 Automater.py 38.72.114.16
```



© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets

Automater checks a series of repositories for information on IPs, domains, and hashes. In this case, we see both VT (VirusTotal), pDNS (passive DNS), and VT (VirusTotal) Malicious URLs. VirusTotal has listed a series of URLs that have been categorized as malicious, most commonly because a malware sample reached out to the URL. Passive DNS resolutions do not automatically qualify as malicious; however, the timing (overlap with resolutions of identified malicious domains) and naming of the two additional domains listed under passive DNS resolutions would qualify them as suspicious. (Because Automater pulls live data, your results may vary slightly from the one below.)

```
+] VT Country: US
+] VT AS Owner: No results found
+] VT pDNS: ('2014-11-06 00:00:00', 'de.onmypc.info')
+] VT pDNS: ('2014-10-21 00:00:00', 'ea.onmypc.info')
+] VT pDNS: ('2014-11-06 00:00:00', 'mmy.ddns.us')
+] VT pDNS: ('2014-11-06 00:00:00', 'nz.compress.to')
+] VT pDNS: ('2019-11-19 12:13:37', 'yo.acmetoy.com')
+] VT Malware: ('2014-10-22 11:36:04', '079b9a455bc2ed92ce045abc34342e4c7f8fa3d1ab6ab5420842ab392a35d480')
+] VT Mal URLs: ('hxxps://yo.acmetoy.com/', '2020-09-14 10:03:39')
+] VT Mal URLs: ('hxxp://yo.acmetoy.com/', '2020-07-16 19:31:57')
+] VT Mal URLs: ('hxxp://38.72.114.16/', '2019-06-11 01:52:25')
+] VT Mal URLs: ('hxxp://ea.onmypc.info:443/', '2014-11-04 15:53:58')
+] VT Mal URLs: ('hxxp://ea.onmypc.info/', '2014-11-04 15:37:17')
+] VT Mal URLs: ('hxxp://ea.onmypc.info:53/0D170A0456F787F525171D55', '2014-10-27 12:30:01')
+] VT Mal URLs: ('hxxp://ea.onmypc.info/E9D1AD2D535F608E057F46EF', '2014-10-22 11:36:00')
+] VT Mal URLs: ('hxxp://ea.onmypc.info:53/80525CD000A332442FE5D579', '2014-10-21 09:58:12')
+] Blacklist from IPVoid: No results found
+] ISP from IPvoid: No results found
+] Country from IPVoid: No results found
```

2. What malware sample(s) are associated with this IP address?

   - **079b9a455bc2ed92ce045abc34342e4c7f8fa3d1ab6ab5420842ab392a35d480**

Automater also queries VirusTotal for malware hashes associated with IPs and domains. In this case, we see that one hash was identified.

```
____________________     Results found for: 38.72.114.16     ____________________
No results found in the RTex DNS
No results found in the FNet URL
[+] VT ASN: No results found
[+] VT Country: US
[+] VT AS Owner: No results found
[+] VT pDNS: ('2014-11-06 00:00:00', 'de.onmypc.info')
[+] VT pDNS: ('2014-10-21 00:00:00', 'ea.onmypc.info')
[+] VT pDNS: ('2014-11-06 00:00:00', 'mmy.ddns.us')
[+] VT pDNS: ('2014-11-06 00:00:00', 'nz.compress.to')
[+] VT pDNS: ('2019-11-19 12:13:37', 'yo.acmetoy.com')
[+] VT Malware: ('2014-10-22 11:36:04', '079b9a455bc2ed92ce045abc34342e4c7f8fa3d1ab6ab5420842ab392a35d480')
[+] VT Mal URLs: ('hxxps://yo.acmetoy.com/', '2020-09-14 10:03:39')
[+] VT Mal URLs: ('hxxp://yo.acmetoy.com/', '2020-07-16 19:31:57')
[+] VT Mal URLs: ('hxxp://38.72.114.16/', '2019-06-11 01:52:25')
[+] VT Mal URLs: ('hxxp://ea.onmypc.info:443/', '2014-11-04 15:53:58')
[+] VT Mal URLs: ('hxxp://ea.onmypc.info/', '2014-11-04 15:37:17')
[+] VT Mal URLs: ('hxxp://ea.onmypc.info:53/0D170A0456F787F525171D55', '2014-10-27 12:30:01')
[+] VT Mal URLs: ('hxxp://ea.onmypc.info/E9D1AD2D535F608E057F46EF', '2014-10-22 11:36:00')
[+] VT Mal URLs: ('hxxp://ea.onmypc.info:53/80525CD000A332442FE5D579', '2014-10-21 09:58:12')
[+] Blacklist from IPVoid: No results found
[+] ISP from IPvoid: No results found
[+] Country from IPVoid: No results found
[+] Malc0de Date: No results found
[+] Malc0de IP: No results found
```

3. What type of threat is the malware associated with?

   - **Backdoor, Trojan, Snojan, Poison, Vundo**

Automater can also query by hash. Run the following query from the command line (you should copy and paste the hash value from your previous results rather than manually typing it):

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets
Technet24

```
python2 Automater.py 079b9a455bc2ed92ce045abc34342e4c7f8fa3d1ab6ab5420842ab392a35d480
```

```
sansforensics@siftworkstation: /opt/Automater
$ python2 Automater.py 079b9a455bc2ed92ce045abc34342e4c7f8fa3d1ab6ab5420842ab392a35d480
```

The results display information on the detections and categorization of the hash by many antivirus and threat intelligence vendors. In this case, we see that there are different detection names based on vendor; however, there are several overlaps in classification. We see the classifications Backdoor, Trojan, Snojan, Poison, and Vundo from multiple vendors, which increases our confidence that this sample is related to those terms. These classifications can help us understand the nature of the malware, which can help us make sure we are looking for the right things in our environment.

```
[+] MD5 found on VT: 1
[+] Scan date submitted: 2019-11-18 03:41:04
[+] Detected Engines: 40
[+] Total Engines: 71
[+] Vendor | Classification: ('FireEye', 'Generic.mg.f48506db289620fe')
[+] Vendor | Classification: ('Zillya', 'Trojan.Snojan.Win32.2722')
[+] Vendor | Classification: ('K7AntiVirus', 'Trojan ( 00511f191 )')
[+] Vendor | Classification: ('Alibaba', 'Backdoor:Win32/Snojan.40879c1d')
[+] Vendor | Classification: ('K7GW', 'Trojan ( 00511f191 )')
[+] Vendor | Classification: ('Invincea', 'heuristic')
[+] Vendor | Classification: ('BitDefenderTheta', 'Gen:NN.ZexaF.32250.di0@aaMQNici')
[+] Vendor | Classification: ('Symantec', 'Backdoor.Darkmoon')
[+] Vendor | Classification: ('APEX', 'Malicious')
[+] Vendor | Classification: ('Paloalto', 'generic.ml')
[+] Vendor | Classification: ('Kaspersky', 'Trojan.Win32.Snojan.bocs')
[+] Vendor | Classification: ('NANO-Antivirus', 'Trojan.Win32.Snojan.fmqvmf')
[+] Vendor | Classification: ('Avast', 'Win32:Trojan-gen')
[+] Vendor | Classification: ('F-Secure', 'Trojan.TR/Vundo.Gen2')
[+] Vendor | Classification: ('VIPRE', 'Trojan.Win32.Generic!BT')
[+] Vendor | Classification: ('TrendMicro', 'BKDR_POISON.WYX')
[+] Vendor | Classification: ('McAfee-GW-Edition', 'Generic Trojan.ga')
[+] Vendor | Classification: ('Trapmine', 'malicious.moderate.ml.score')
[+] Vendor | Classification: ('SentinelOne', 'DFI - Suspicious PE')
[+] Vendor | Classification: ('Avira', 'TR/Vundo.Gen2')
[+] Vendor | Classification: ('Fortinet', 'W32/POISON.WYX!tr.bdr')
[+] Vendor | Classification: ('Antiy-AVL', 'Trojan/Win32.TSGeneric')
[+] Vendor | Classification: ('Microsoft', 'Backdoor:Win32/Poison.K')
[+] Vendor | Classification: ('AegisLab', 'Trojan.Win32.Snojan.4!c')
[+] Vendor | Classification: ('ZoneAlarm', 'Trojan.Win32.Snojan.bocs')
[+] Vendor | Classification: ('TACHYON', 'Trojan/W32.Snojan.57344.B')
[+] Vendor | Classification: ('AhnLab-V3', 'Dropper/Win32.Injector.C1160793')
[+] Vendor | Classification: ('McAfee', 'Generic Trojan.ga')
[+] Vendor | Classification: ('MAX', 'malware (ai score=97)')
[+] Vendor | Classification: ('VBA32', 'Backdoor.Win32.Hupigon.dguz')
[+] Vendor | Classification: ('ESET-NOD32', 'a variant of Win32/Injector.DNSH')
[+] Vendor | Classification: ('TrendMicro-HouseCall', 'BKDR_POISON.WYX')
[+] Vendor | Classification: ('Rising', 'Malware.Undefined!8.C (TFE:5:Fb687Xzt7mT)')
[+] Vendor | Classification: ('Yandex', 'Trojan.Vundo!4IVpaMncg3M')
[+] Vendor | Classification: ('Ikarus', 'Trojan.Win32.Agent')
[+] Vendor | Classification: ('AVG', 'Win32:Trojan-gen')
[+] Vendor | Classification: ('Panda', 'Generic Suspicious')
```

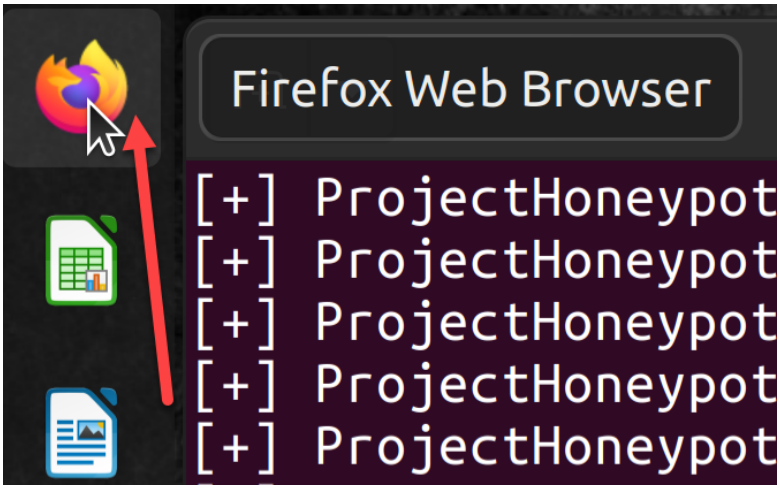
© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets

4. From VirusTotal, what are the filenames associated with the hash(es), and when was the file created?

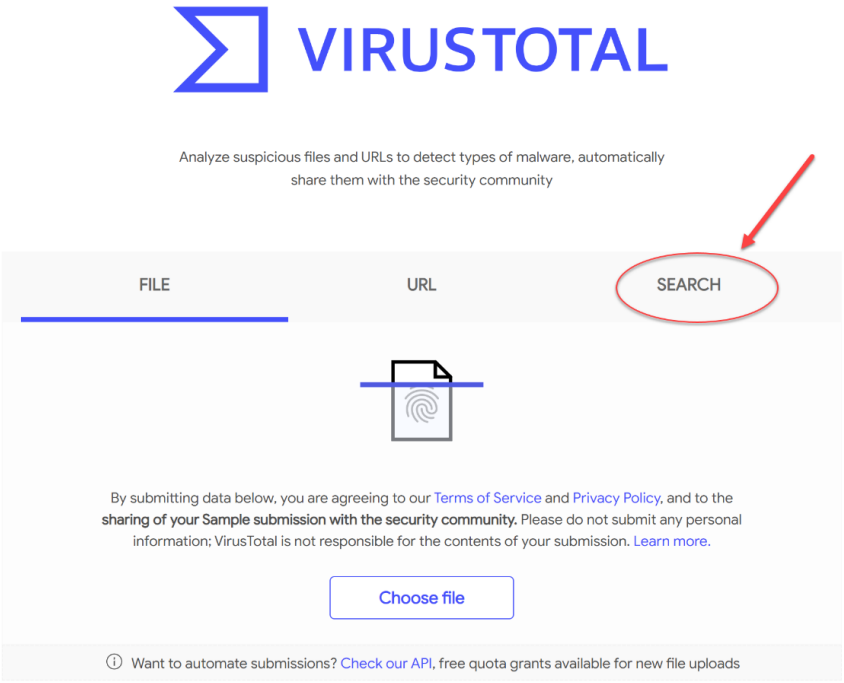
   - **THNCKREST.exe, created on October 9, 2012**

The VirusTotal antivirus vendor tags give us a good starting point. However, if we want to find detailed information such as filenames, we will have to leave Automater and search for the hashes directly in VirusTotal. Open up Firefox in our SIFT VM by clicking on the icon in the left menu.



We can copy and paste the hash values from our Automater command-line results into the VirusTotal Search box. We are viewing this information in a live environment, and VirusTotal updates with the most recent information it analyzes; it is possible that your results will not match the screenshots below.

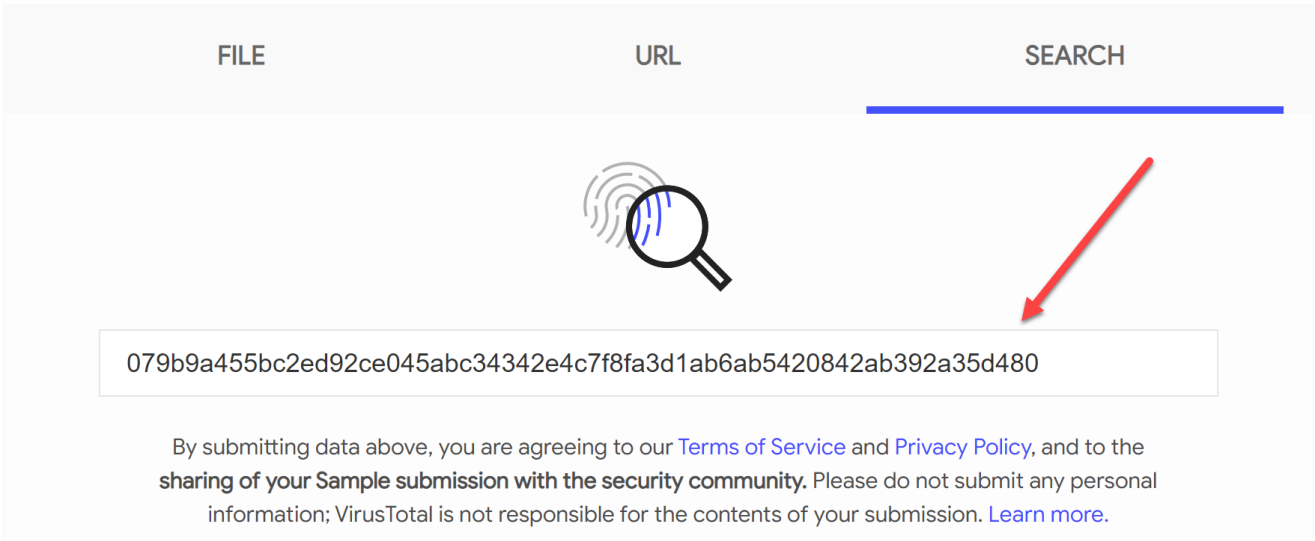
In Firefox on our VM, navigate to www.virustotal.com. Select "Search". We do not need to log in to conduct searches.



© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets
Technet24

Copy the hash we previously searched for (079b…) from the Automater command line into the VirusTotal search box and hit enter.



VirusTotal shows the detections that we saw in Automater; however, there are other details present. When searching for a hash, a filename typically shows up under the hash value at the top of the VirusTotal results page. (VirusTotal frequently changes the user interface, so your results may look different than the one below.) In this case, we see the file is named "THNCKREST". If we want to learn more, we can go to the "Details" tab to get more information about the file.

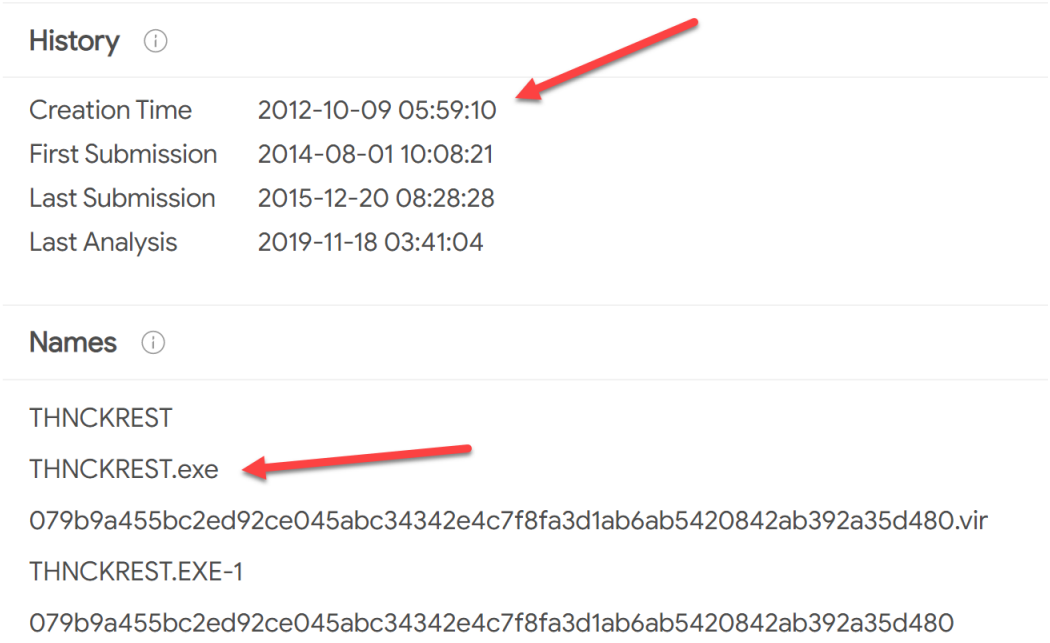


The details tab has a lot of information about the file that can be useful, including other hash values aside from the SHA-256 hash value provided by Automater. If we scroll down the page, we can see the File Creation Date, First and Last Submission date, and Last Analysis date. We are looking for the creation date, which is 2012-10-09. We also confirm the name from the main page, THNCKREST.exe. Understanding the creation date of a file can help us to understand how long a particular type of malware has been active, which can help us to scope how far back to look in the discovery phase for additional signs of an intrusion. For

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets

some malware samples, we may see multiple different names, which can be interesting to help us understand what filenames were used in files coming from various submitters. (For example, sometimes adversaries will name the same files differently to target different victims.)



5. From AlienVault's Open Threat Exchange, what threat(s) are associated with the domains linked to the IP?

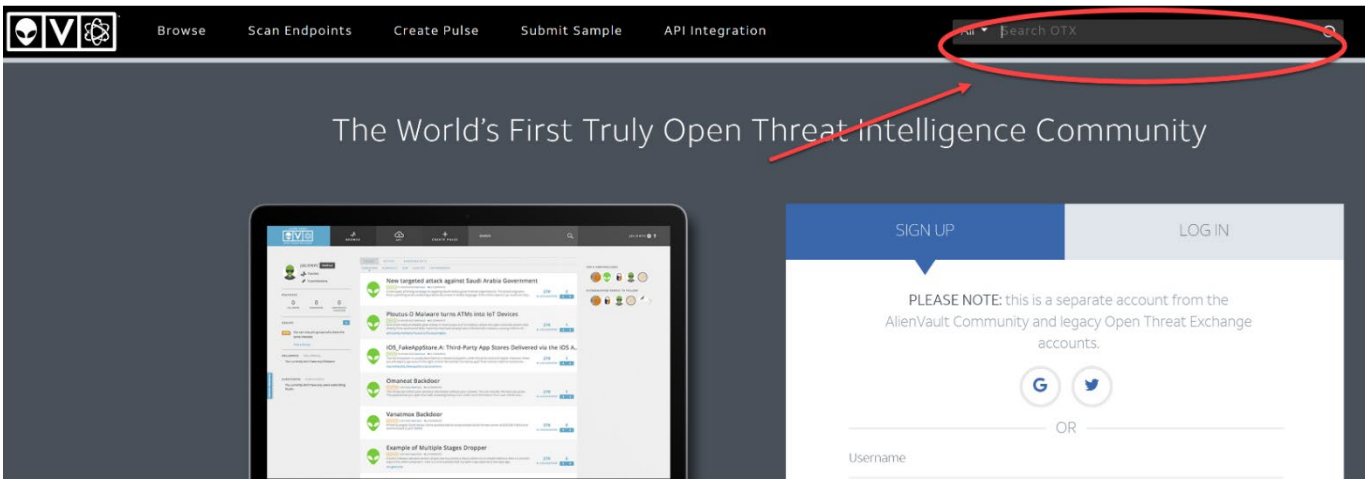
- **<u>Two of the domains linked to the IP are associated with the Cloud Hopper campaign</u>**

In a web browser on our VM, navigate to otx.alienvault.com. It is not necessary to create a login to access the threat exchange for searching purposes. Enter the first domain from our previous Automater results for "VT Mal URLs", which was "yo.acmetoy.com", into the search bar on the top right of the screen.

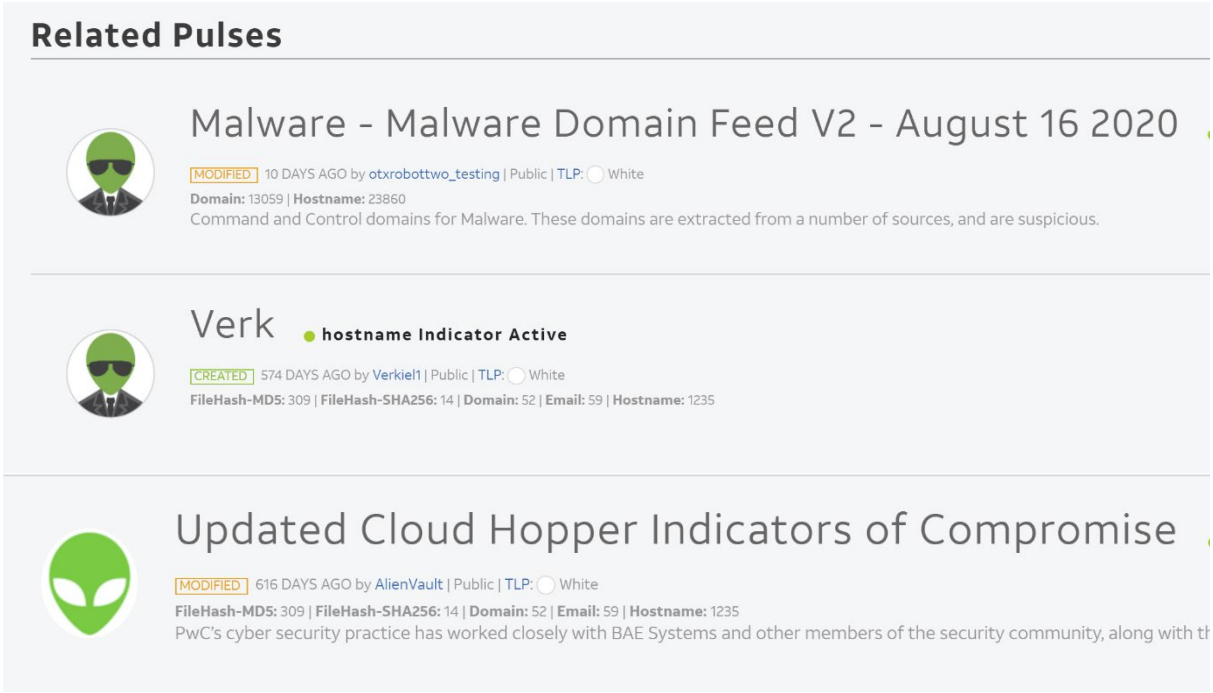
```
[+] VT Mal URLs: ('hxxps://yo.acmetoy.com/', '2020-09-14 10:03:39')
[+] VT Mal URLs: ('hxxp://yo.acmetoy.com/', '2020-07-16 19:31:57')
[+] VT Mal URLs: ('hxxp://38.72.114.16/', '2019-06-11 01:52:25')
[+] VT Mal URLs: ('hxxp://ea.onmypc.info:443/', '2014-11-04 15:53:58')
[+] VT Mal URLs: ('hxxp://ea.onmypc.info/', '2014-11-04 15:37:17')
[+] VT Mal URLs: ('hxxp://ea.onmypc.info:53/0D170A0456F787F525171D55', '2014-10-27 12:30:01')
[+] VT Mal URLs: ('hxxp://ea.onmypc.info/E9D1AD2D535F608E057F46EF', '2014-10-22 11:36:00')
[+] VT Mal URLs: ('hxxp://ea.onmypc.info:53/80525CD000A332442FE5D579', '2014-10-21 09:58:12')
```

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets
Technet24



OTX does not have any threat information on the domain "yo.acmetoys.com", so we try searching for the next domain, "ea.onmypc.info". OTX does have information on the next domain on the list, "ea.onmypc.info", as we can see in the "Related Pulses" section. As we investigate those Pulses, we observe this IP is listed as a malware command-and-control domain and is linked with Updated Cloud Hopper IOCs.



Reviewing the remaining domains show that one other domain, "nz.compress.to", is also associated with Cloud Hopper and shows up on several threat feeds tied to that activity. A search for the initial IP address will also return the Cloud Hopper IOC list.

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets



(https://otx.alienvault.com/pulse/58ebadf17c71a907e4d4b067)

Since OTX provides links to source materials, we can also browse to read the PWC report referenced to get additional details on Operation Cloud Hopper (https://www.pwc.co.uk/issues/cyber-security-services/insights/operation-cloud-hopper.html), including additional TTPs and IOCs that can be helpful to understanding the potential impact of this threat and ensuring that the intrusion has been properly remediated. We would need to conduct further analysis to determine if our incident is associated with Operation Cloud Hopper as defined by PWC, but at this point, we have a link between the two.

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets
Technet24

Exercise: Key Takeaways

- **Open Source Information can provide additional details and clarity around threats that have been identified in your network.**

- **Tools such as Automater can expedite the process of identifying whether or not there is any information available on a given indicator.**

- **Analysts will almost always need to pivot to the source of the information to get additional details and validate the findings prior to actioning them or making assessments based off of Open-Source Information.**

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets

This page intentionally left blank.

https://t.me/learningnets

Technet24

Exercise 3.4: Sifting Through Massive Amounts of OSINT

Objectives

- Utilize Recorded Future to satisfy the Priority Intelligence Requirement (PIR)
- Learn more about OSINT and searching large amounts of it to satisfy intelligence requirements

Scenario: Money Bin's contracted incident response team needs our help with a time-sensitive PIR: to identify any information we can about the C2 server they found to help them with the ransomware case they are actively working.

Received indicator:
85.25.3.13 as a C2 address identified in Money Bin's compromised networks

Exercise Prep

This exercise requires the use of an internet connection and a web browser of your choice. You should use your username and password for Recorded Future that you created in Exercise 0. This information should be used to log in to the website www.RecordedFuture.com.

It is important to note that this is a Software as a Service (SaaS) hosted product and is subject to change. In other words, changes in the tool may occur that make the images in this lab not 100% identical to what you see on the website. In addition, given that this subject is OSINT, the open-source material will change sometimes. The purpose of this lab is not to stress specifics but instead the power of open-source information, as well as the value added by professional tools. ***Do not feel you have to get all the same answers as the walkthrough. Instead, focus on the capabilities; the walkthrough is a sample approach to assist your efforts. The walkthrough's images will not be the same as yours because the OSINT is updated daily.***

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets

Exercise: Questions

1. What malware family is associated with the IP address (**85.25.3.13**)?

- _____

2. Is the malware related to ransomware and if so, how?

- _____

3. How would we use indicators from OSINT to help the incident responders?

- _____

4. Are there any specific families or ransomware that are associated with the malware?

- _____

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets

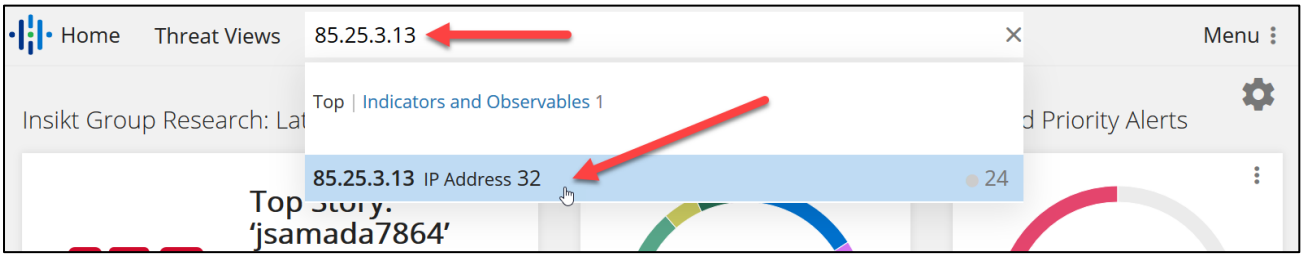
Technet24

1. What malware family is associated with the IP address (**85.25.3.13**)?

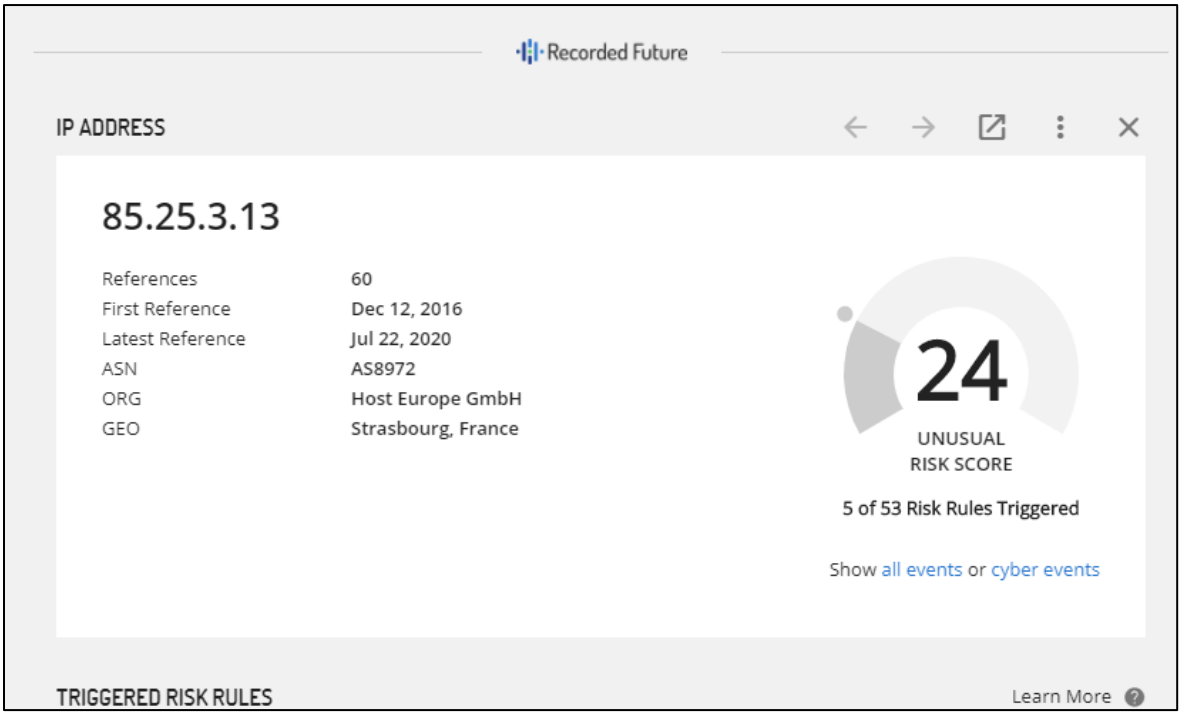
- **TrickBot**

First, log in to www.RecordedFuture.com with the account you created in Exercise 0.

We will be met with the home page; if we are not, simply click the Home button in the top left of the page. Enter the IP address 85.25.3.13 into the search bar and select the "IP address" result that returns.



We will get a pop-up that shows all the details that Recorded Future has easily accessible on this IP address. Scrolling on this page will reveal a wide variety of details. Realize all this comes from OSINT and thus can be inaccurate, so we must validate this information. However, Recorded Future's intel team, the Insikt Group, and machine learning do sift out a lot of trash that helps keep the information relatively accurate, especially for OSINT.

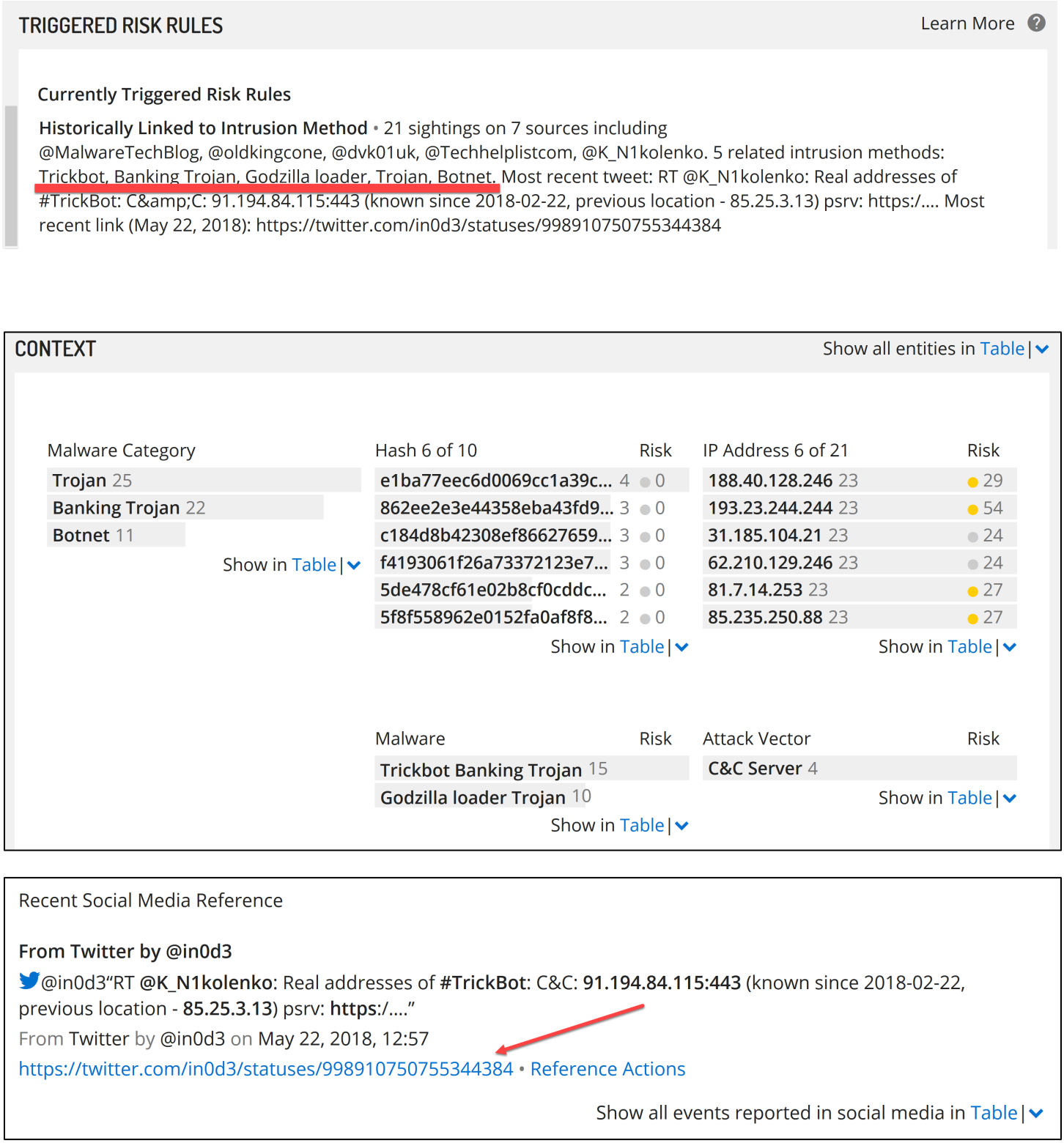


As you review the information, you will see multiple references not only to TrickBot malware but also Banking Trojan (a generic name), and Godzilla loader. Keep reviewing the material and you will

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets

find that all the information centers around the discussion of TrickBot, and there are social media references that we can click on (the screenshot is provided below so that you do not have to click) that link the C2 IP address explicitly to TrickBot.



TRIGGERED RISK RULES

Learn More

Currently Triggered Risk Rules

Historically Linked to Intrusion Method • 21 sightings on 7 sources including @MalwareTechBlog, @oldkingcone, @dvk01uk, @Techhelplistcom, @K_N1kolenko. 5 related intrusion methods: Trickbot, Banking Trojan, Godzilla loader, Trojan, Botnet. Most recent tweet: RT @K_N1kolenko: Real addresses of #TrickBot: C&C: 91.194.84.115:443 (known since 2018-02-22, previous location - 85.25.3.13) psrv: https:/.... Most recent link (May 22, 2018): https://twitter.com/in0d3/statuses/998910750755344384

CONTEXT

Show all entities in Table

Malware Category	
Trojan	25
Banking Trojan	22
Botnet	11

Show in Table

Hash 6 of 10		Risk
e1ba77eec6d0069cc1a39c...	4	0
862ee2e3e44358eba43fd9...	3	0
c184d8b42308ef86627659...	3	0
f4193061f26a73372123e7...	3	0
5de478cf61e02b8cf0cddc...	2	0
5f8f558962e0152fa0af8f8...	2	0

Show in Table

IP Address 6 of 21	Risk
188.40.128.246 23	29
193.23.244.244 23	54
31.185.104.21 23	24
62.210.129.246 23	24
81.7.14.253 23	27
85.235.250.88 23	27

Show in Table

Malware	Risk
Trickbot Banking Trojan	15
Godzilla loader Trojan	10

Show in Table

Attack Vector	Risk
C&C Server	4

Show in Table

Recent Social Media Reference

From Twitter by @in0d3

@in0d3"RT **@K_N1kolenko**: Real addresses of **#TrickBot**: C&C: **91.194.84.115:443** (known since 2018-02-22, previous location - **85.25.3.13**) psrv: **https**:/...."

From Twitter by @in0d3 on May 22, 2018, 12:57

https://twitter.com/in0d3/statuses/998910750755344384 • Reference Actions

Show all events reported in social media in Table

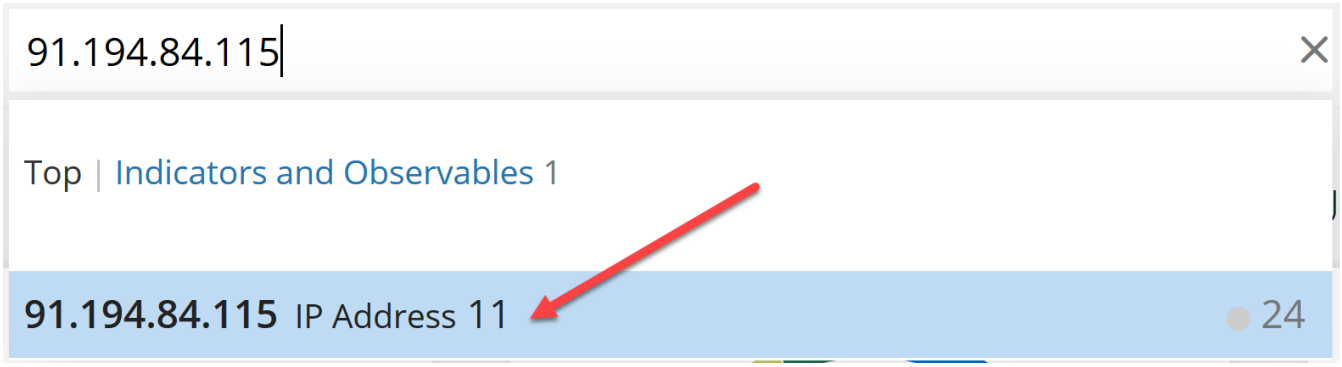
© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets

Technet24

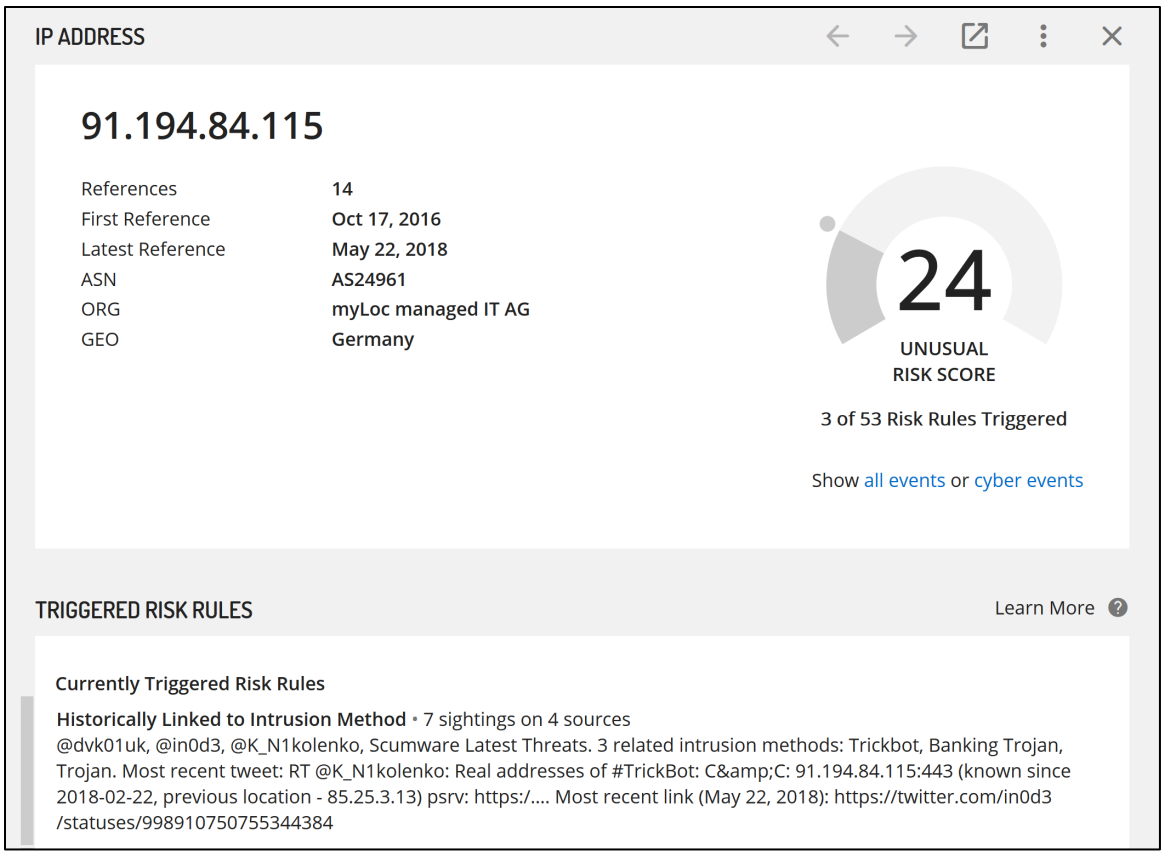


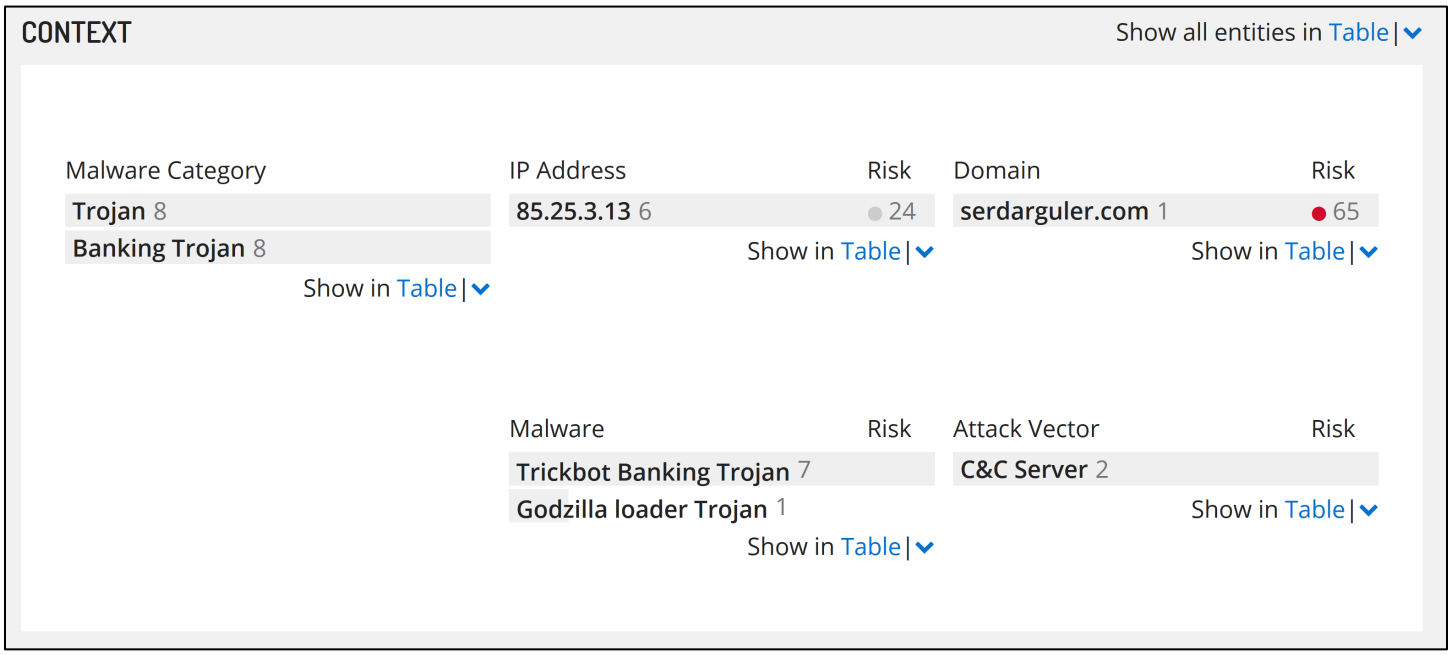
It's hard to verify social media posts and OSINT in general, but so far, there's a lot of details here that fit cleanly for us; at this point, it's safe to at least search on the 91.194.84.115 IP address from the tweet to see if there's any additional information we can find. Exit out of the "IP Address" window from our search on 85.25.3.13 and search for 91.194.84.115 in the Recorded Future search bar at the top of the page. Select the "IP Address" result for this IP as we did before.



© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets





The information helps us link the IP address further to TrickBot as the malware. Additionally, there's a domain that stands out as odd: serdarguler(dot)com. It has some level of risk associated to it and instead of the thousands of IP addresses and hashes, it is a singular item. For that reason, we'd want to record it for the incident responders, too.

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets

Technet24

2. Is the malware related to ransomware and if so, how?

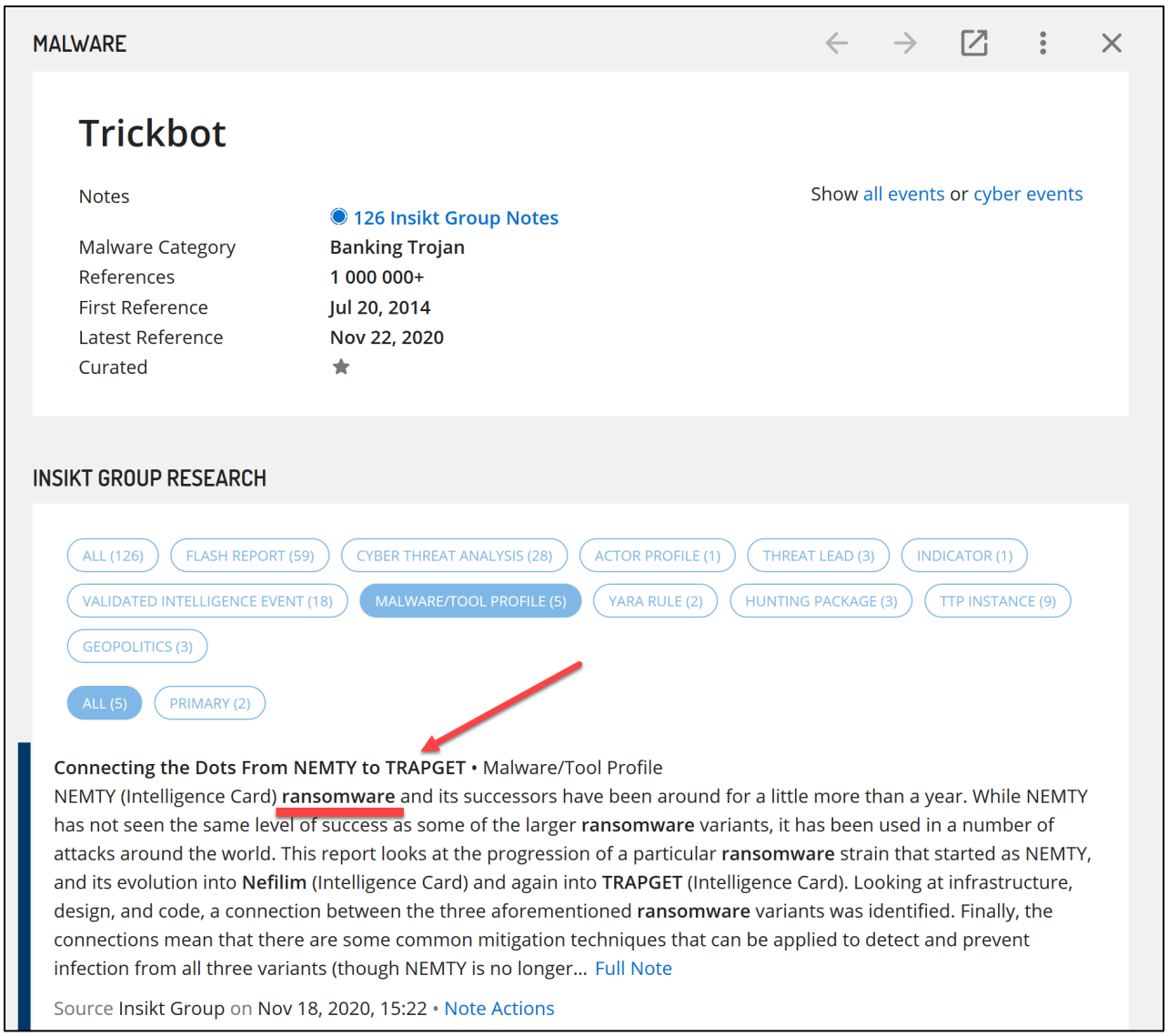
- **Yes, TrickBot is a first stage implant for ransomware**

At this point, we can search specifically for TrickBot and see what Recorded Future knows about it.



© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets



The page associated with TrickBot has a lot of information and references you can read. All of them point to the fact that TrickBot has been heavily leveraged as a first stage implant or malware leveraged by adversaries to then position ransomware in the organization. This overlaps with exactly what we expected to find based on the incident at Money Bin and increases our confidence that we are gathering good information related to the incident. You can continue to read up on TrickBot to learn more about it and record things like key indicators and TTPs for the incident responders.

3. How would we use indicators from OSINT to help the incident responders?

- **<u>As a pared-down dataset for cross-comparison to fill in knowledge gaps</u>**

So far in the class, we've used indicators as a pretty specific type of data for either pivoting on or creating insights to cluster intrusions as key indicators. But that's not the only use-case for indicators. In cases like this, it is completely reasonable to download the datasets we can find and tag them as low confidence indicators related to this incident. At this point, we wouldn't use the indicators we're finding to create some intrusion set or later an Activity Group, unless we find something particularly key that stands out, and instead we can just download them as a larger CSV file. The incident responders could very easily use this data to cross compare what they find in the

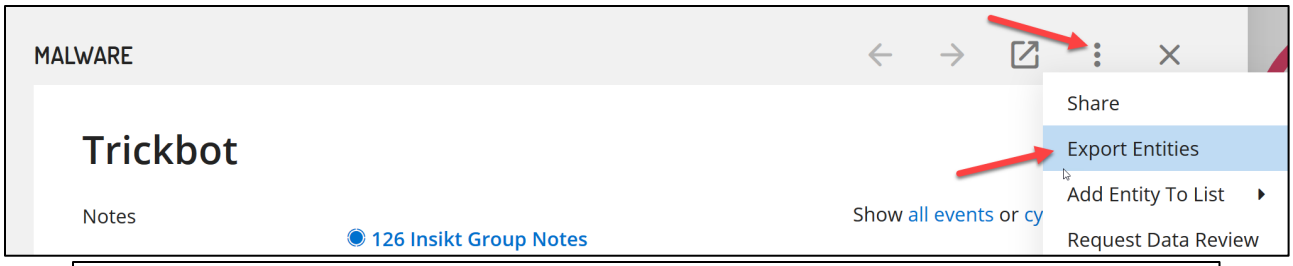
© 2021 Robert M. Lee and SANS Institute

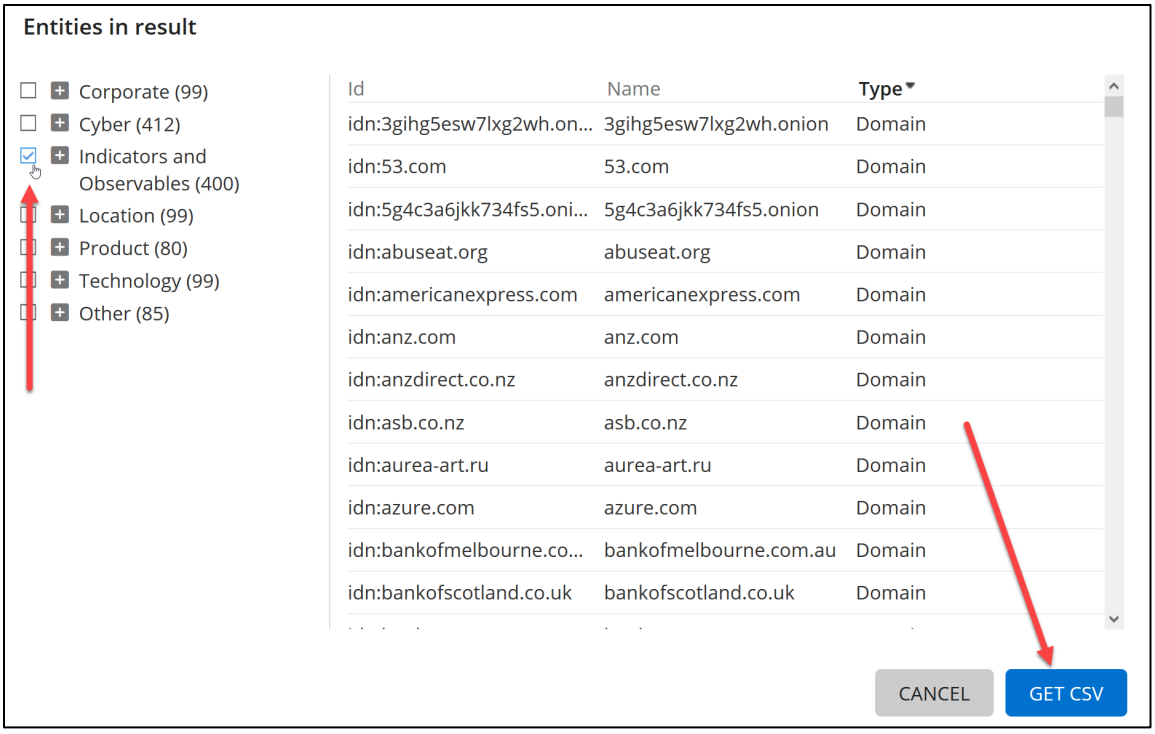
https://t.me/learningnets
Technet24

networks and see if there are any hits. That would then serve to call back to the CTI team and have them put in a request for information (RFI) to determine how the activity on the network relates to TrickBot (or not). Then, with the proper focus, we could go see what else we could find related to those specific indicators. Essentially, we are not pivoting on the information, but giving the incident responders enough data to compare against to see if they can create any links for us to then go pivot off of that newly revealed data to satisfy their knowledge gaps.

If we just try to pivot on everything, we will go down a rabbit hole and overwhelm ourselves and the incident responders.

In Recorded Future, we could download these datasets into your knowledge management system of choice or even as a CSV. We are not going to export anything, but if you wanted to do this later, you could click the three dots at the top of the "Trickbot" malware window, then select "Export Entities". From that menu, you could select the Entities you wanted to export, such as "Indicators and Observables", and then click "Get CSV" to download a .csv file.



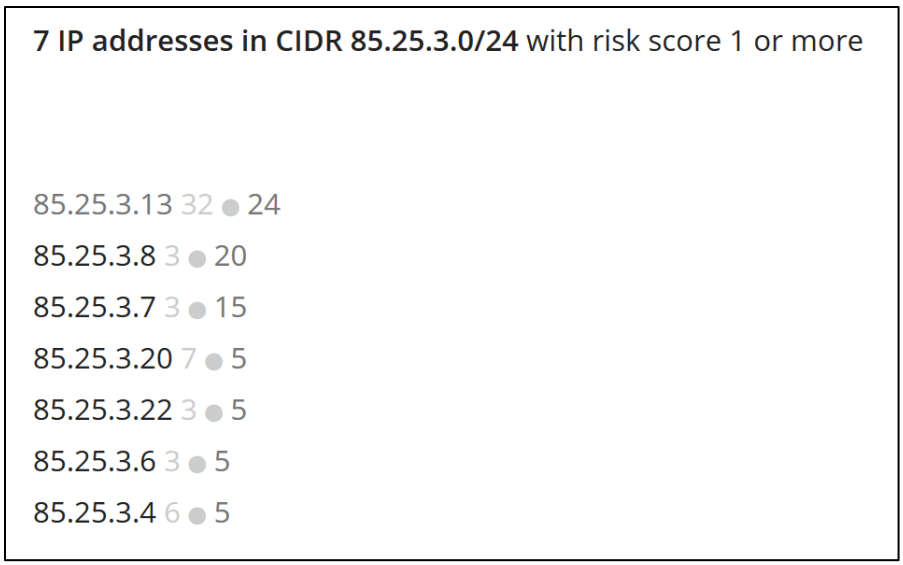


We are not going to export anything, but here's some examples of interesting datasets we would have seen in the context pages of your searches so far:

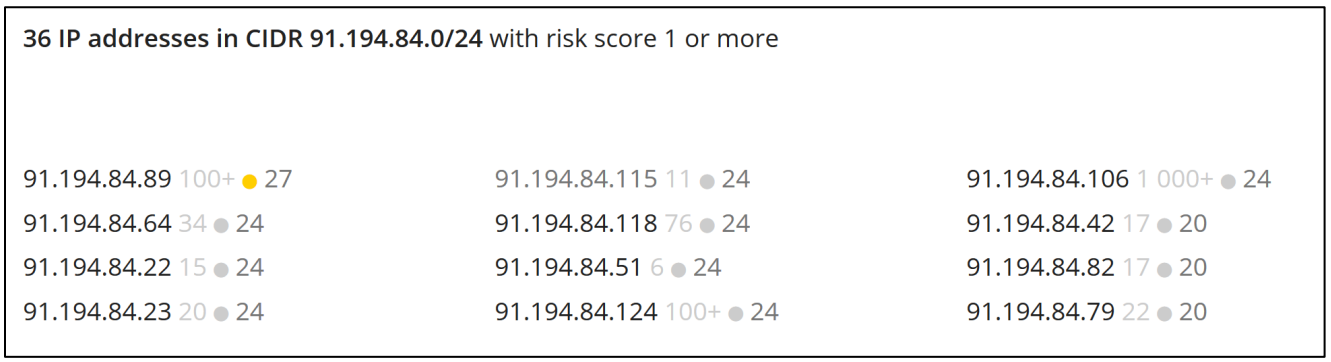
From our search on IP 85.25.3.13, this gives us additional IP addresses in the same range that may be "risky":

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets



From our search on IP 91.194.84.115, this gives us additional IP addresses in the same range that may be "risky":



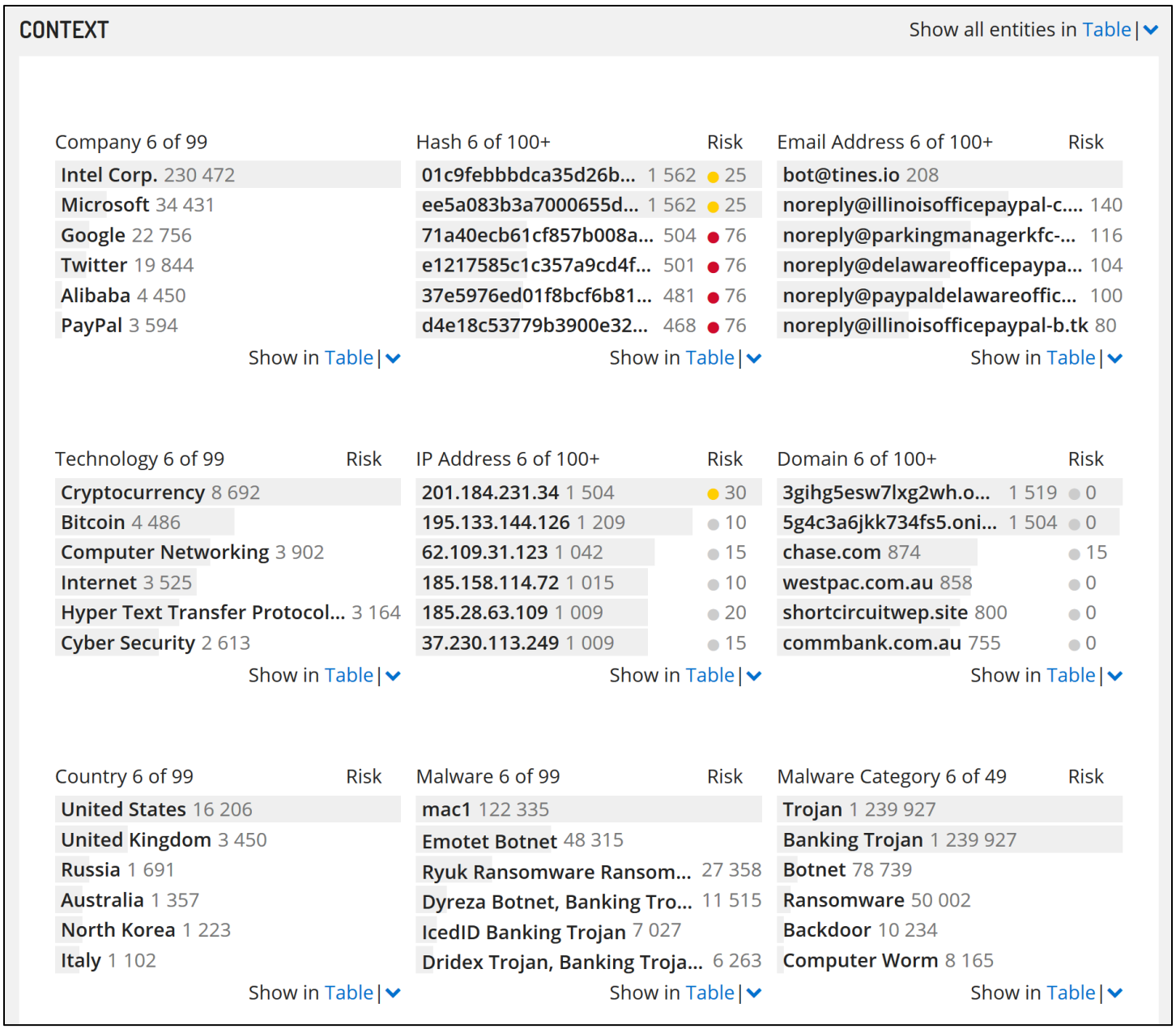
4. Are there any specific families or ransomware that are associated with the malware?

- **Ryuk**

Off of the TrickBot context page in Recorded Future, we can look at associated groups, malware families, and indicators.

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets
Technet24

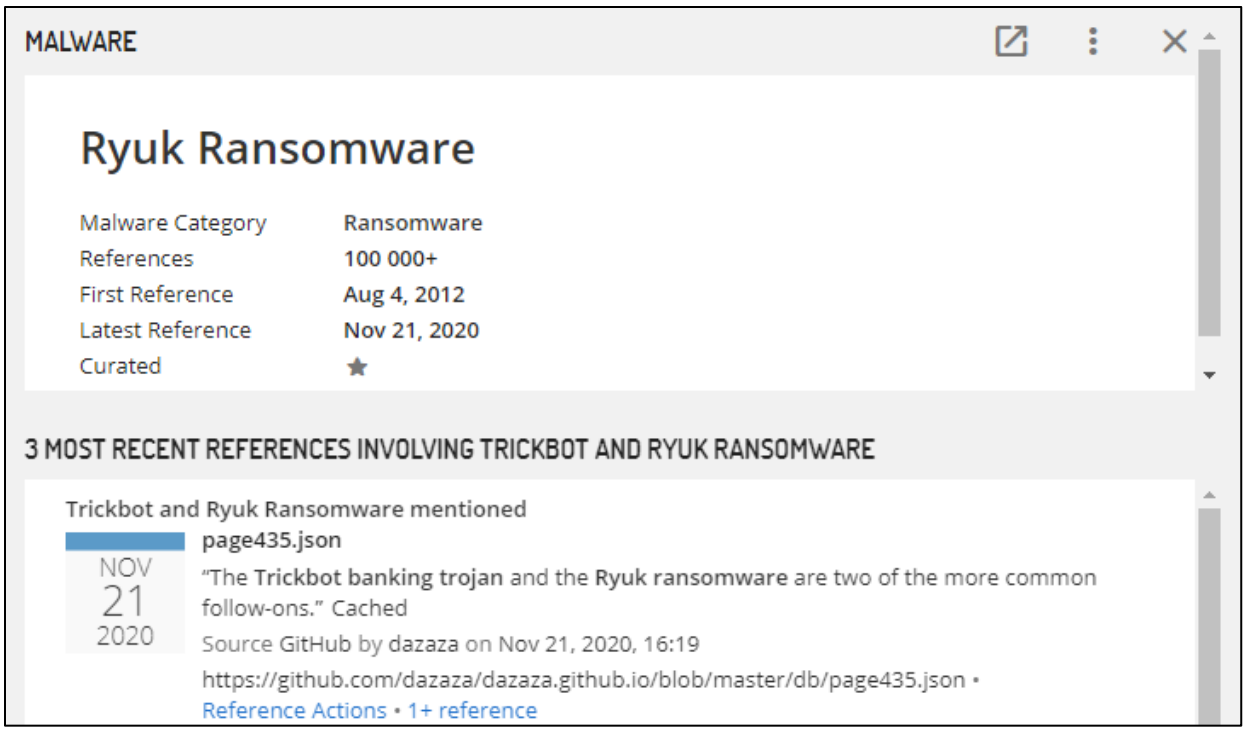


There's a lot of information we can go through but interestingly under the Malware section, we see references to IcedID, Emotet, and Dridex. These are all malware families with Trojan capabilities. None of them are actually ransomware. However, we also see "Ryuk Ransomware" in the list, marking the first reference to a specific family of ransomware.

We could then search for Ryuk in the Recorded Future search bar.

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets



The first reference to Ryuk shows a recent (at the time of this lab creation) GitHub page linking TrickBot to Ryuk. Depending on what Recorded Future displays when you run this search, you may have to do additional searching to identify the link between TrickBot and Ryuk.

You can continue to search and learn more, but at this point, any additional information gathering will inform our analysis that Ryuk is a common family of malware delivered through TrickBot to organizations. We can also find mention through any variety of sources on this page that the adversaries who leverage TrickBot and Ryuk also often use Cobalt Strike and other open-source tools and living on the land techniques to move around the compromised victims.

Before we gather far more information than might be useful to the incident responders, it would be appropriate at this time to send them the low confidence indicators in a CSV and tell them that the C2 address is linked to TrickBot and potentially the delivery of Ryuk. This is important context for them, because if they see an alert for TrickBot, response time is crucial since it could lead to Ryuk being delivered. Further, known TTPs of these types of breaches include the use of open-source tools seen in pen tests and native functionality in the environment associated with living on the land techniques. This would be more than enough for the incident responders to leverage for quick analysis and let us know if they find anything to confirm anything we've told them. If they can confirm anything at all, and provide any additional context or technical indicators, we as intel analysts could then follow those threads to find more information for them. As this is a Priority Intelligence Requirement, we can consider it satisfied while staying on standby to continue to support.

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets
Technet24

Exercise: Key Takeaways

- **By searching Recorded Future, we determined that the C2 IP address our incident responders previously identified was related to TrickBot. Further analysis determined TrickBot frequently delivers a ransomware family known as Ryuk. We were able to identify multiple indicators and TTPs to assist the incident responders.**

- **While OSINT tools like Recorded Future can assist with identifying information, analysts must validate findings and provide appropriate information to consumers to meet intelligence requirements.**

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets

This page intentionally left blank.

https://t.me/learningnets

Technet24

Exercise 3.5: TLS Certificate Pivoting

Objectives

- Ingest structured data into Maltego's CaseFile for visual analysis
- Use properties of entities and relationships to identify interesting data points

Scenario: A recent sample from a blocked email attachment to SpaderTech was flagged as malicious and was identified as TrickBot. There was configuration data in the TrickBot sample with the IP address 21.50.50.23. That IP address is not useful to this portion of the scenario; however, it is interesting as it was an IP address that we saw scanning SpaderTech in Exercise 2.1. Our email sandbox vendor provided some basic data around TrickBot. Additionally, some open-source searches and CSVs of TrickBot TLS certificate data from a trusted sharing group provided more context around the malware. You will analyze the shared TrickBot TLS certificate data using CaseFile to determine any new infrastructure beyond what your sandbox flagged and see if it provides any additional information for future tracking.

Exercise: Prep

Familiarize yourself with the "Trickbot certificates.csv" and "Trickbot IPs.csv" documents in the **Ex 3.5** folder in the SIFT VM. This is the source data for this exercise. Use this information and Maltego to answer the questions. Import the "Trickbot certificates.csv" first to answer questions 2–4, and then import the "Trickbot IPs.csv" to answer questions 5 and 6. **Please use the version of Maltego installed in your SIFT VM for this exercise, even if you have Maltego installed somewhere else.**

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets

Exercise: Questions

1. What entities and properties will you need to create within Maltego CaseFile to handle the import of the **Trickbot certificates.csv** file?

   - _____

2. When looking at the properties of the two TLS certificates, what similarities do you see?

   - _____

3. What differences do you see in the properties of the two TLS certificates?

   - _____

4. What entities and properties do you need to use when importing the **Trickbot Ips.csv** file?

   - _____

5. What relationships do you see between the two certificates after importing the **Trickbot Ips.csv** file?

   - _____

6. What does the certificate information tell us about IP 85.25.3.13?

   - _____

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets

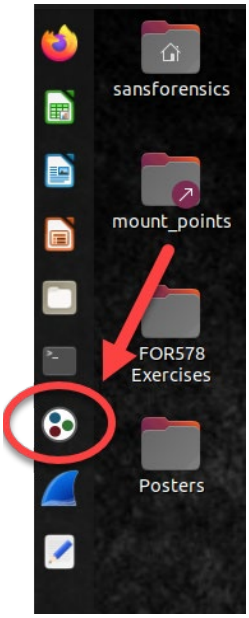
Technet24

Exercise: Questions with Step-by-Step

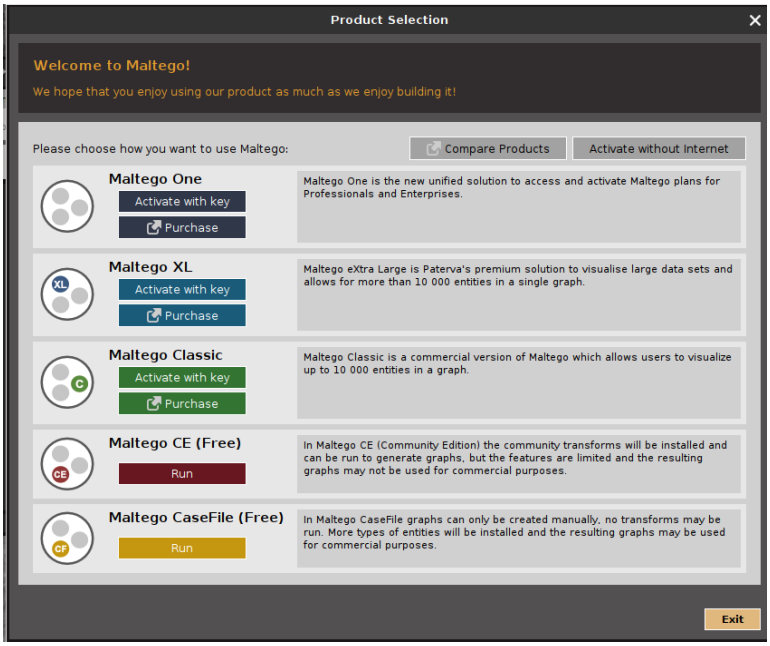
1. What entities and properties will you need to create within Maltego to handle the import of the **Trickbot certificates.csv** file?

- **Entity: TLS Certificate, Properties: SHA1, Subject, Issuer, Not Before, Not After**

From the SIFT VM, click the "Maltego" icon on the task bar.

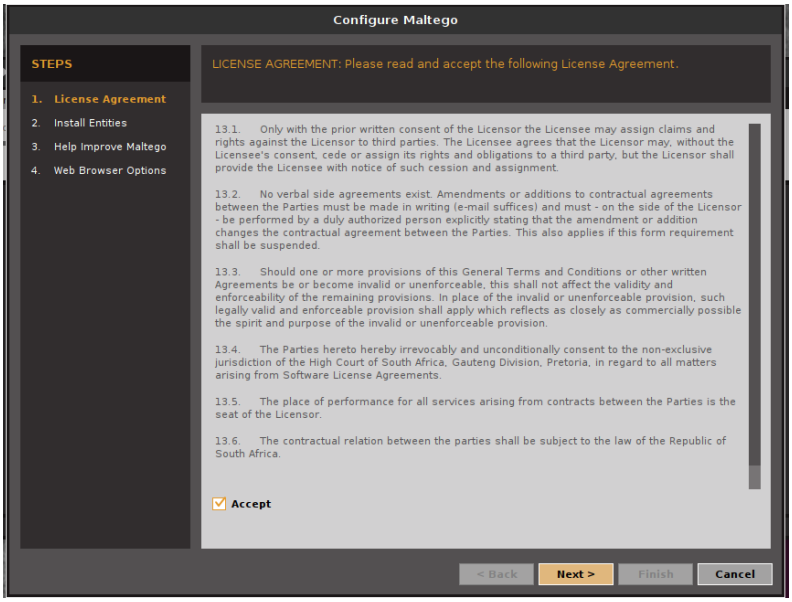


On the Product Selection page, select "Maltego CaseFile" and hit "Run".

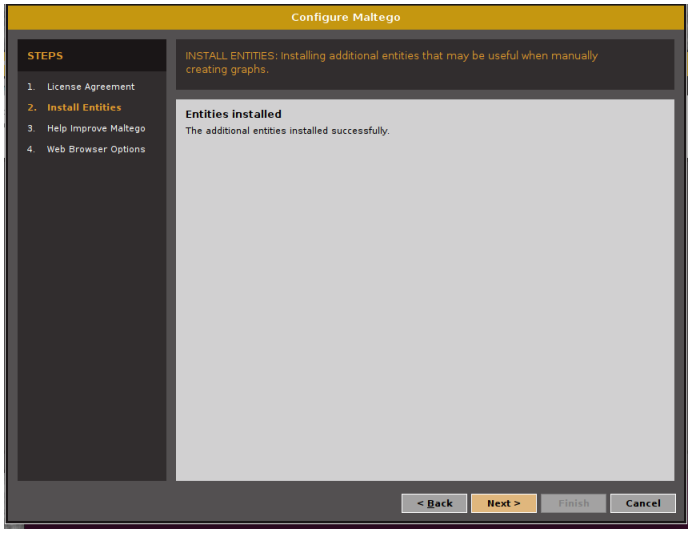


© 2021 Robert M. Lee and SANS Institute
https://t.me/learningnets

Read and accept the License Agreement and select “Next”.



Follow the prompts and select “Next” as Entities are installed.

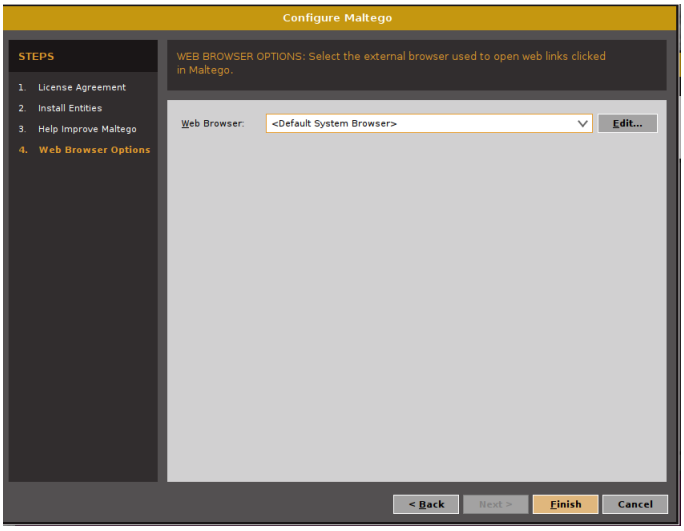


Keep the default sections for the next two windows, and then select “Finish”.

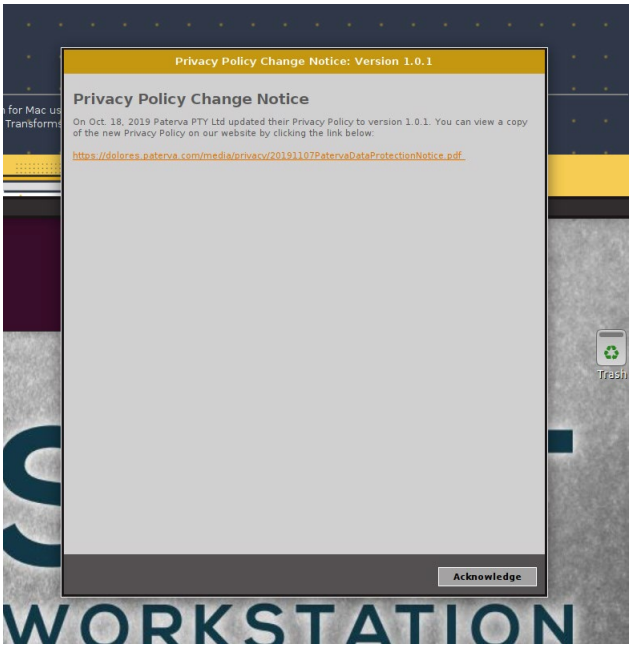
© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets

Technet24

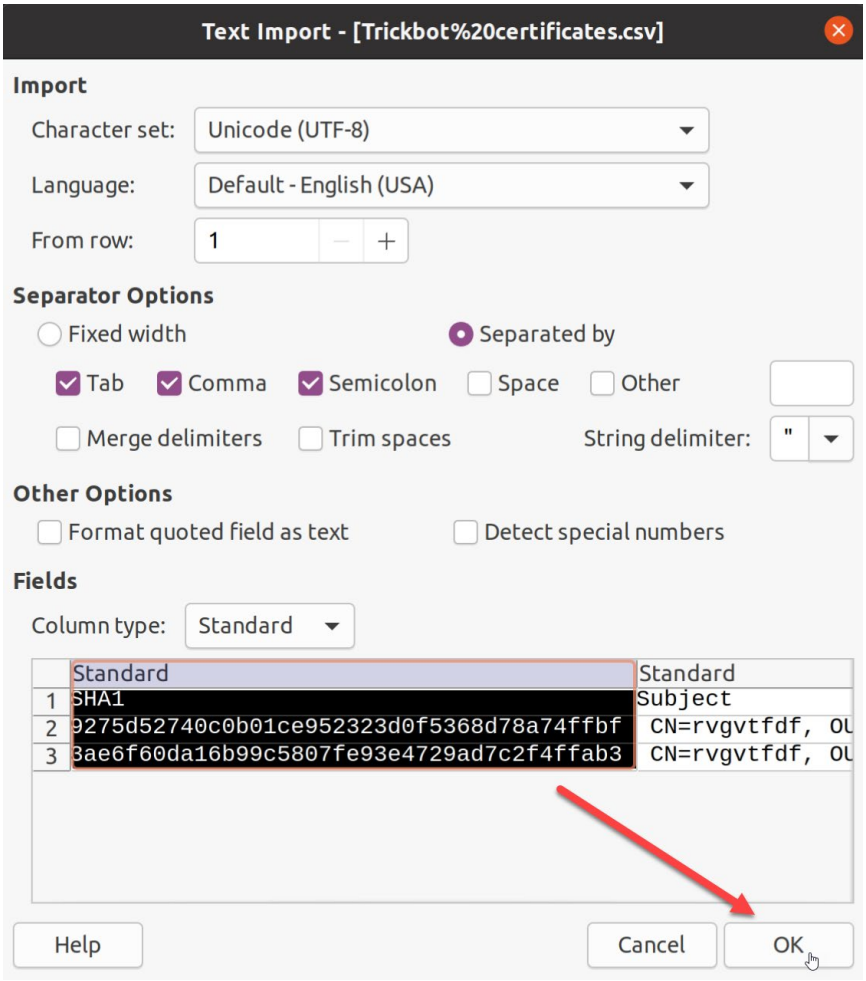


Acknowledge any Policy Change Notifications, if one appears. *You now have Maltego CaseFile up and running!*



Navigate to the Ex 3.5 folder and open the "Trickbot certificates.csv" file in your VM to view its contents. It will automatically open in a tool called LibreOffice, which is like Microsoft Excel. Select the default import options and click "OK".

© 2021 Robert M. Lee and SANS Institute
https://t.me/learningnets

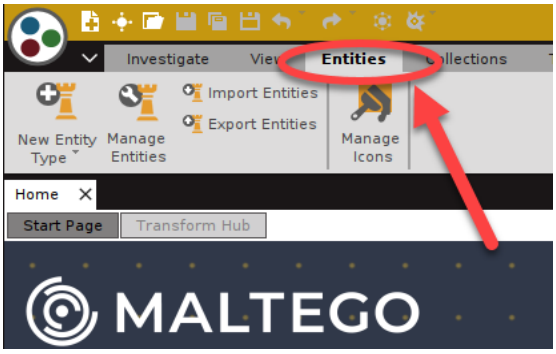


After opening the Trickbot certificates.csv file, we see that Row 1 has the names of the fields, specifically SHA1, Subject, Issuer, Not Before, and Not After. Therefore, those will be the properties we need, and this is dealing with TLS Certificates. Maltego comes with some entities by default, but TLS Certificate is not one of those, so we will need to create that entity ourselves.

	A	B	C	D	E
1	SHA1	Subject	Issuer	Not Before	Not After
2	9275d52740	CN=rvgvtfdf, OU	CN=rvgvtfdf, OU=rs	2019-06-08T17:51:56Z	2020-06-08T17:51:56Z
3	3ae6f60da1	CN=rvgvtfdf, OU	CN=rvgvtfdf, OU=rs	2020-06-07T18:54:19Z	2021-06-07T18:54:19Z

Navigate back to Maltego and select the Entities tab from the menu.

© 2021 Robert M. Lee and SANS Institute
https://t.me/learningnets
Technet24



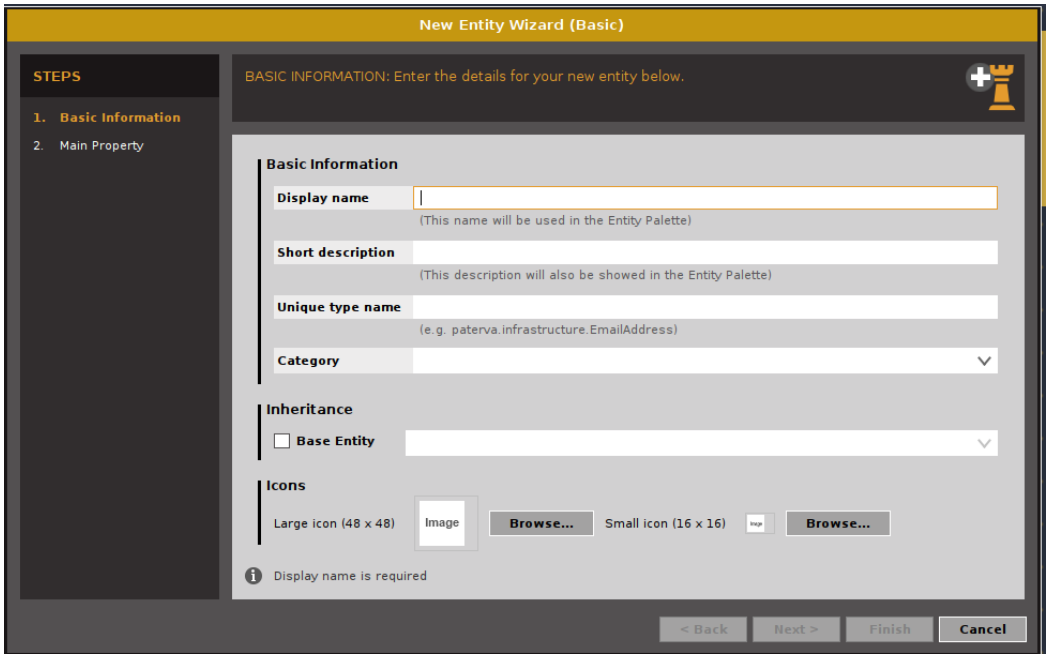
Create a new entity type from the Entities tab by selecting <u>New Entity Type</u>, and then selecting "New Entity Type" again from the dropdown menu.



The following pop-up dialog box displays.

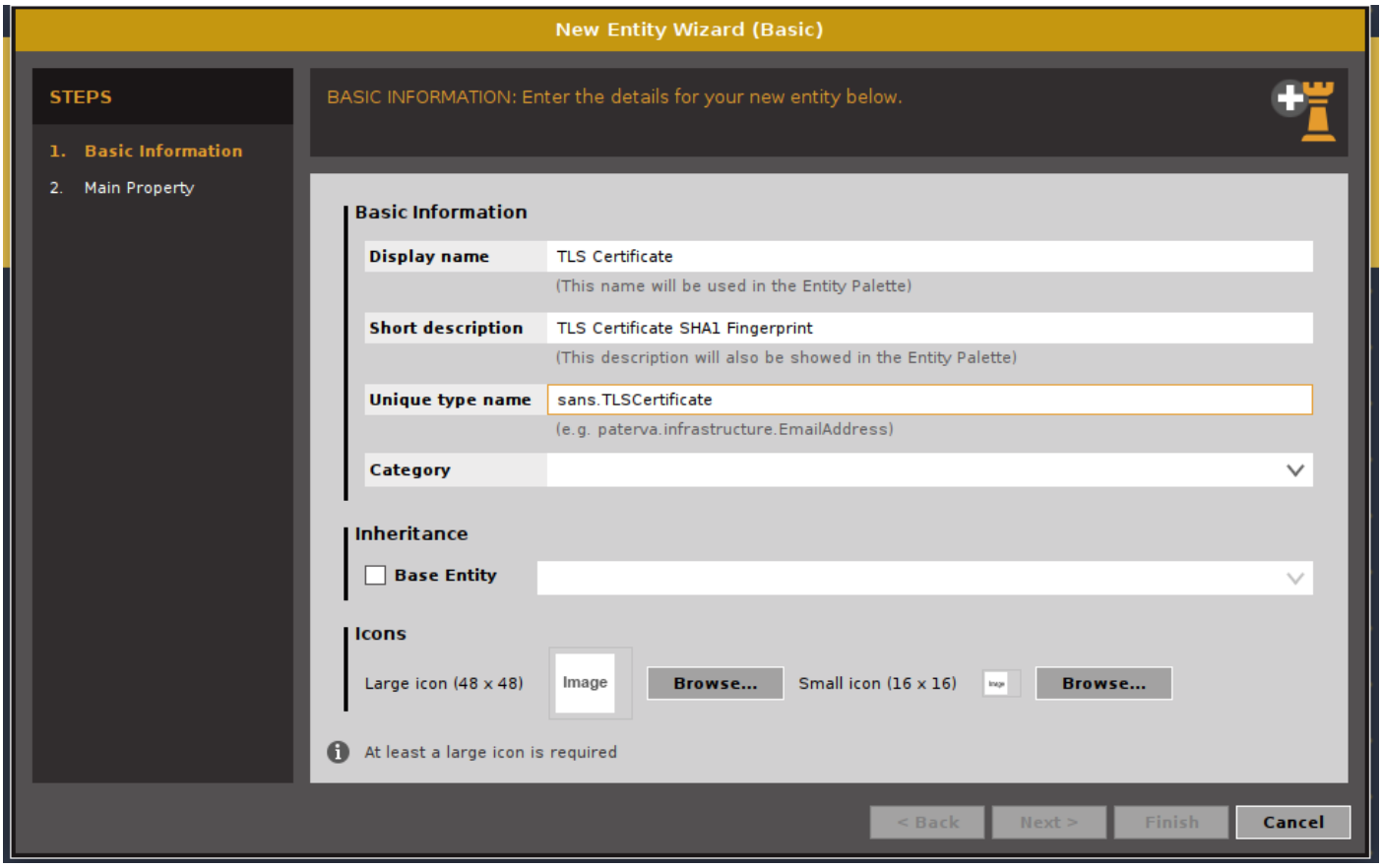
© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets



Fill in the appropriate values for the entry fields in the form. Fields include Display Name, which is the name of the type of information that you will be providing, and a Short Description, which will be associated with the Display Name and will provide additional information on the item. The Unique Type name ensures that there are no other entities with the exact same name to avoid duplications.

© 2021 Robert M. Lee and SANS Institute
https://t.me/learningnets
Technet24



The next step is to select an icon to associate with the entity you are creating. Maltego includes a built-in icon set for creating custom entities. Select Browse in the Icons section. The following dialog box will pop up. Select the Technology tab and select the SSLCertificate icon, then select OK.

© 2021 Robert M. Lee and SANS Institute

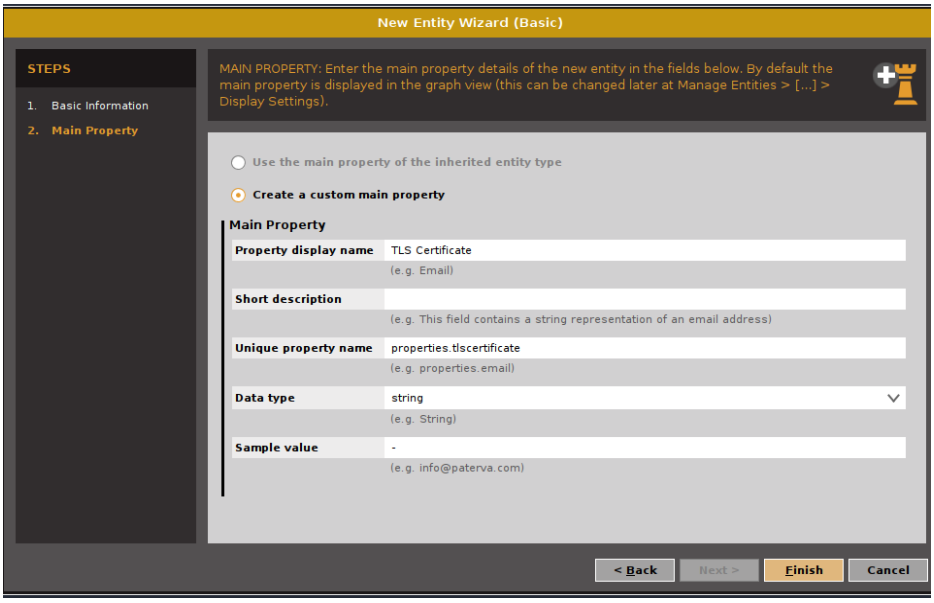
https://t.me/learningnets



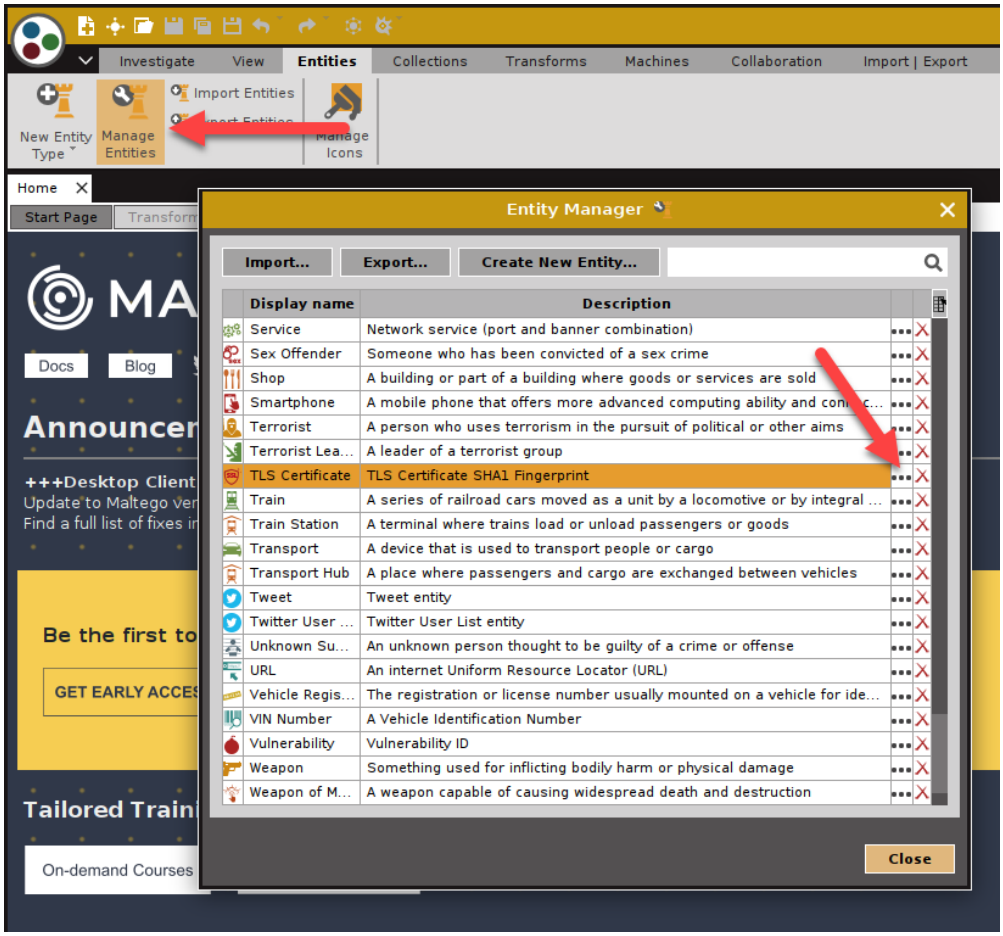
After entering the above information, selecting our icon, and clicking "Next," we are taken to another screen to add some additional information about the entity. Select "Create a custom main property", which should be selected by default. The "Property display name" is the same as the "Display Name" from the previous screen. This field is intended to help the creator and other users understand what the entity contains. The "Unique property name" is similar to the "Unique Display Name", as it must be a unique value to differentiate the entity's properties from those of other entities. Data type will almost always be a string, and the sample value is a sample of the string that will be associated with that entity. We will leave our data type as string for this entity.

Enter the required fields for the entity and select Finish.

© 2021 Robert M. Lee and SANS Institute
https://t.me/learningnets
Technet24

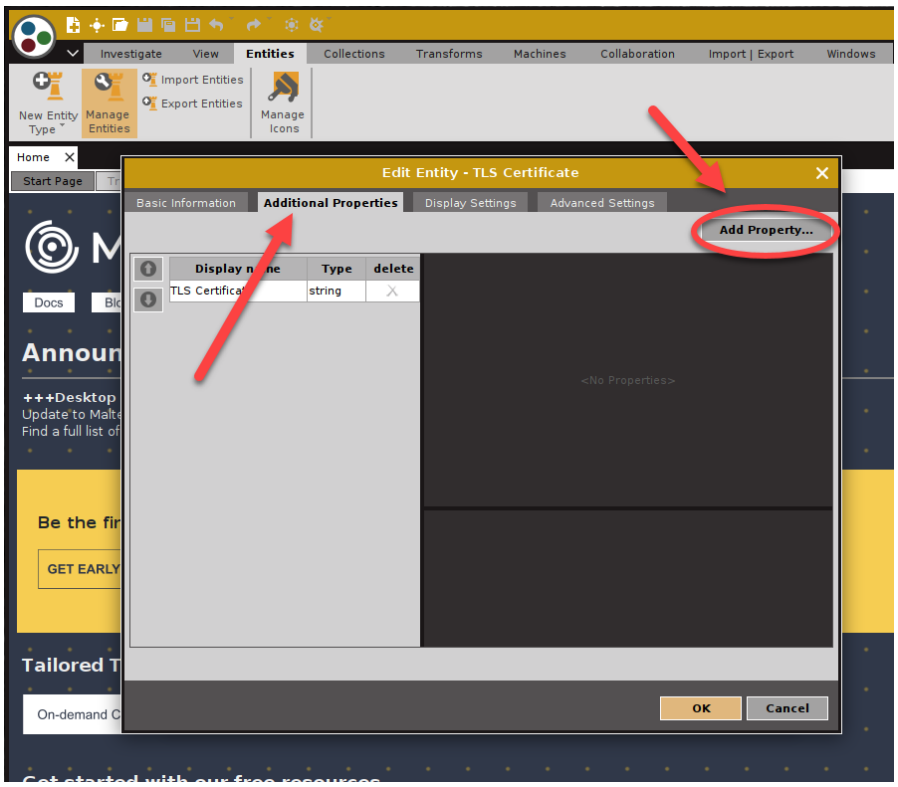


Now our TLS Certificate entity has been created, but we will need some additional properties for this entity to display some additional useful data. To do that, go back to the Entities tab and select "Manage Entities." The Entity Manager will pop up. Find the new TLS Certificate entity that was created and click the "…" to add additional properties.

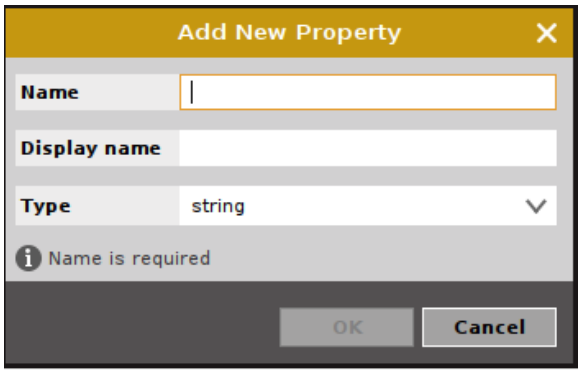


© 2021 Robert M. Lee and SANS Institute
https://t.me/learningnets

Next, select the "Additional Properties" Tab and click the "Add Property" button.



The "Add New Property" window should look like this.

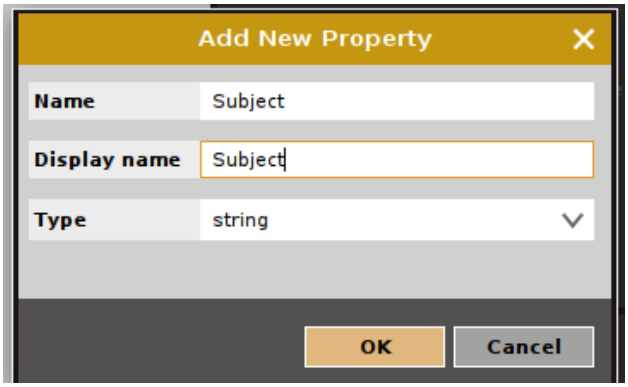


Enter "Subject" into the "Name" and "Display name" fields to create the Subject property, and then select OK.

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets

Technet24



Repeat this process for each of the properties that we determine we need to create. For this lab, we will create additional properties for Subject, Issuer, Not Before, and Not After. Examples of all the data fields needed for this exercise are shown below.

Issuer:



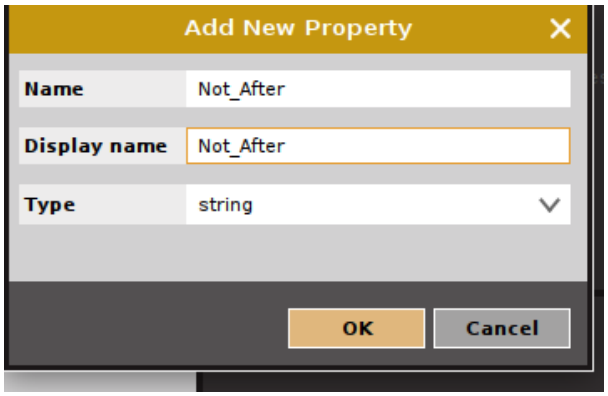
Not Before (naming with an underscore instead of a space is a best practice to follow, since sometimes spaces cause problems for operating systems):



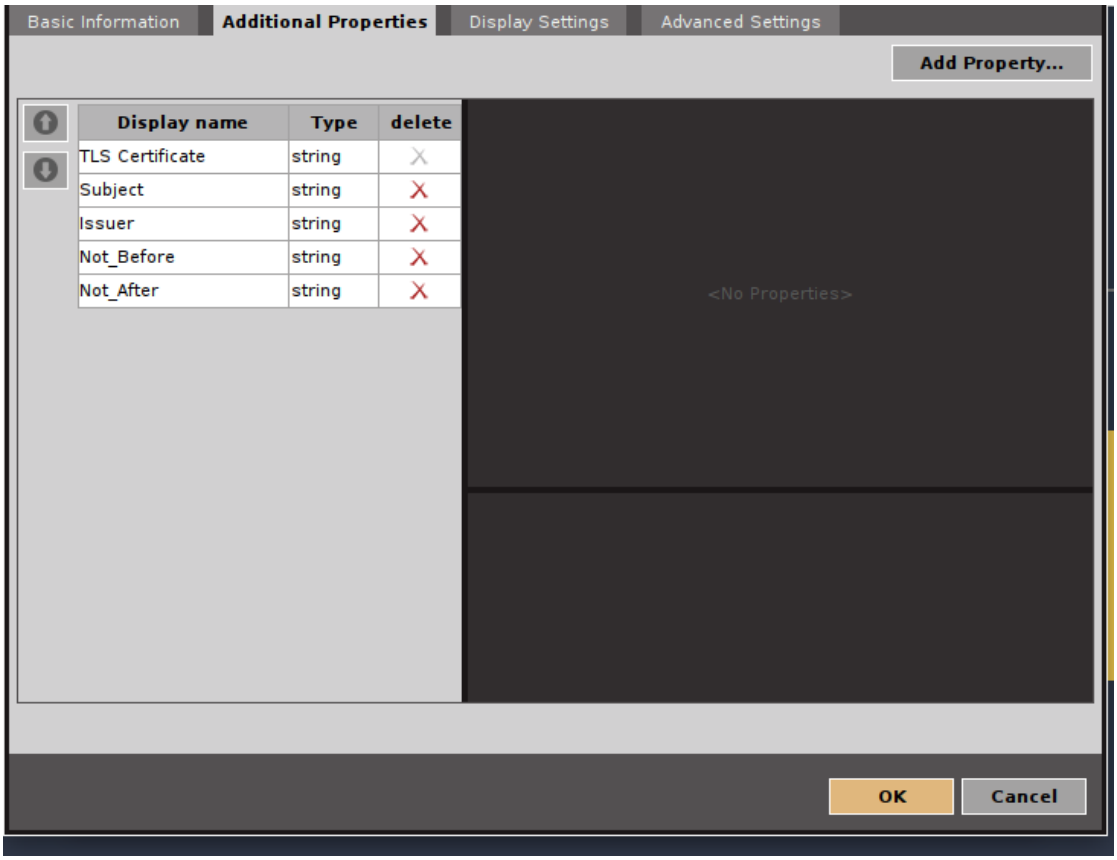
© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets

Not After:



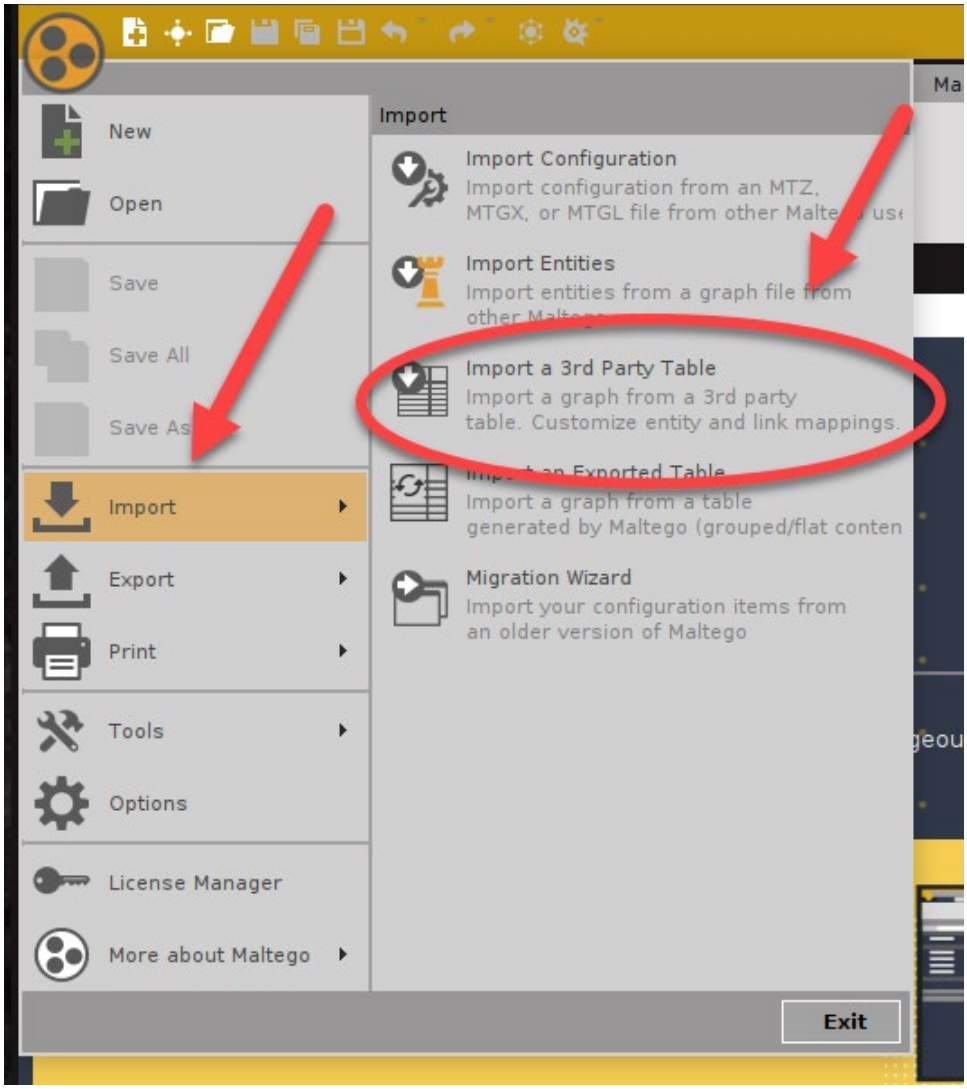
Once we have added all the properties, we should see something similar to this:



Select OK, then Close, and your TLS certificate has been updated.

Once the new TLS Certificate entity and its properties are created, import the data from our CSV file. To do that, click the large circle menu button at the top left, and then select Import -> Import a 3rd Party Table.

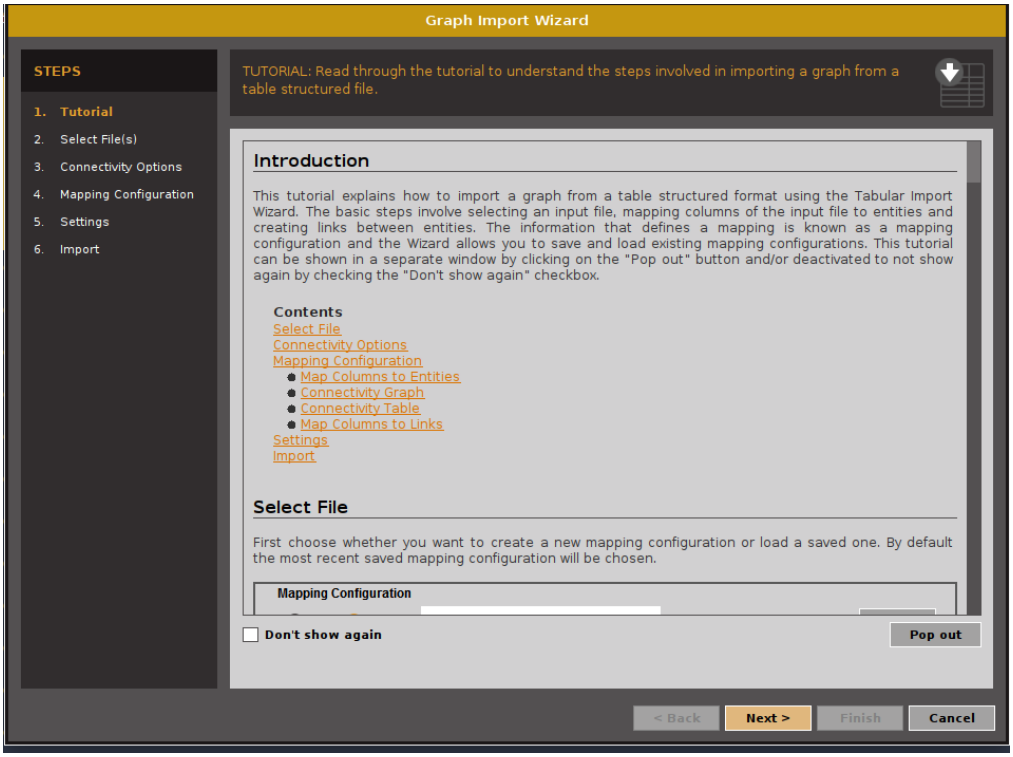
© 2021 Robert M. Lee and SANS Institute
https://t.me/learningnets
Technet24



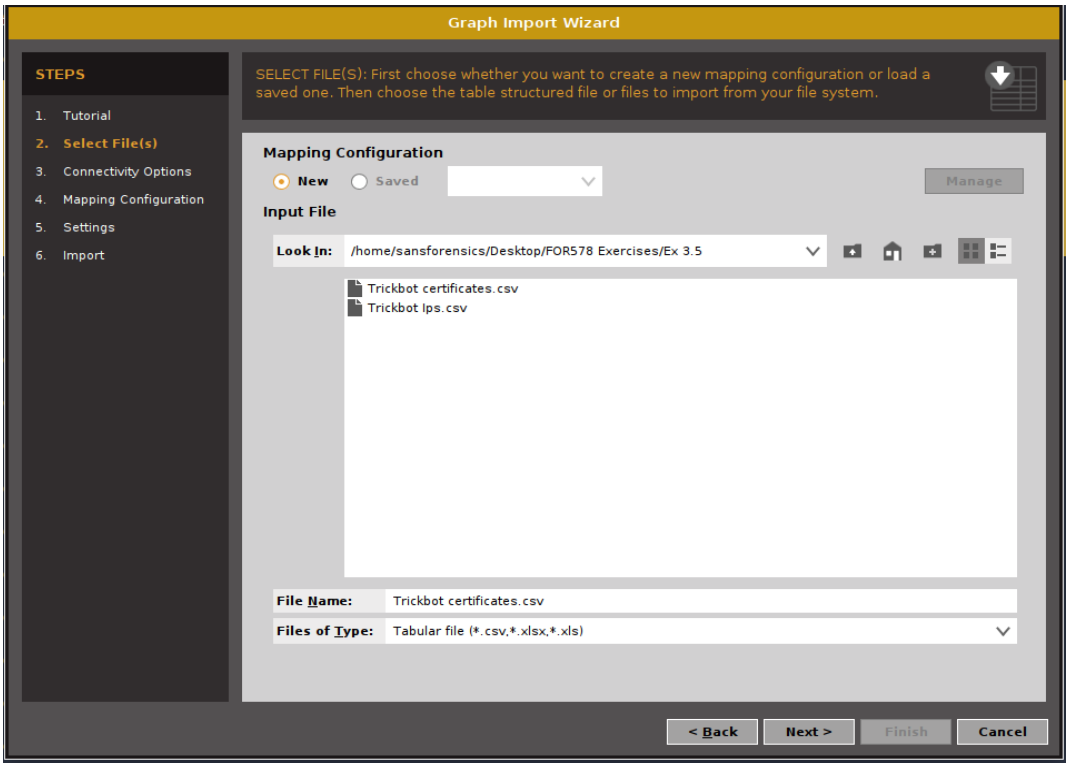
The following pop-up dialog box displays. Select Next.

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets

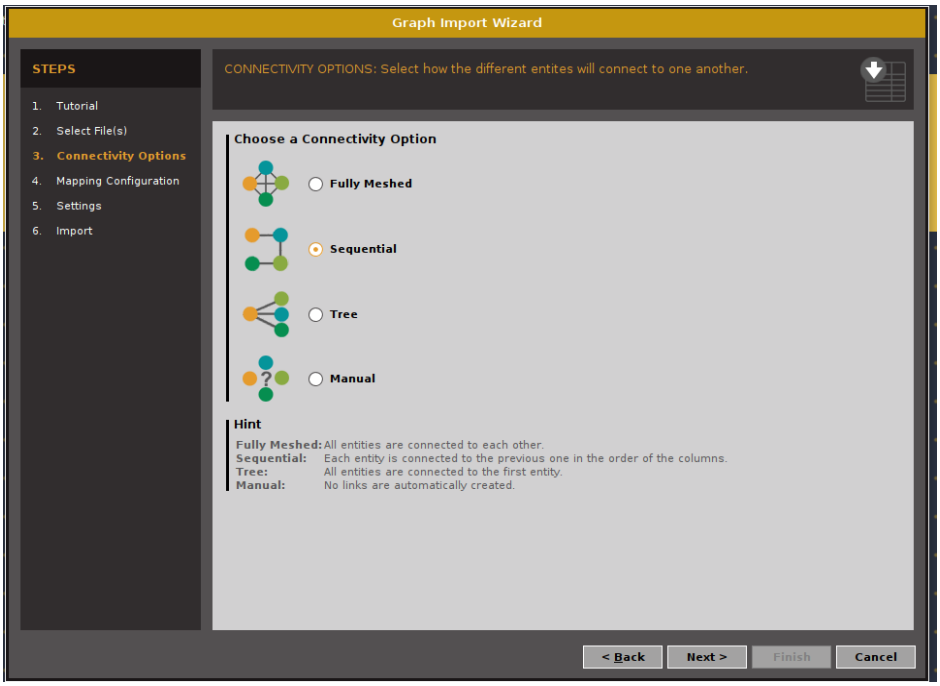


Choose the file "Trickbot certificates.csv" from Ex 3.5 folder as your import data and click Next. The full path is /home/sansforensics/Desktop/FOR578 Exercises/Ex 3.5.



Choose the default Connectivity Option (Sequential) and click Next.

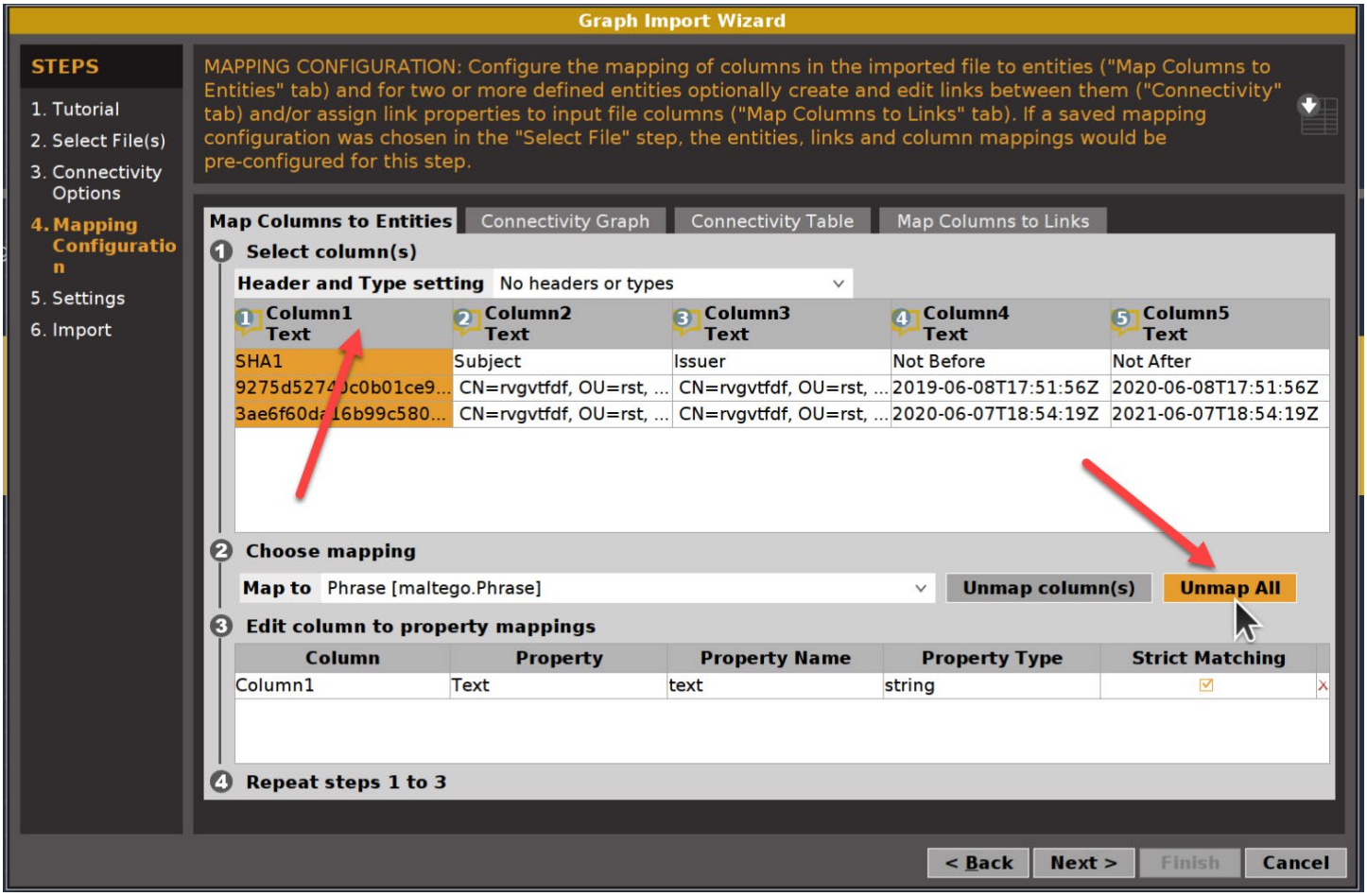
© 2021 Robert M. Lee and SANS Institute
https://t.me/learningnets
Technet24



The "Graph Import Wizard" can guide us through the process of importing each of the fields we want to graph into the specification. We observe that the import wizard tries to map some of the columns for us. In the below screenshot, it tried to map the columns to the "Text" entity. This isn't right, so we should click on any column and then click "Unmap All" to start fresh.

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets



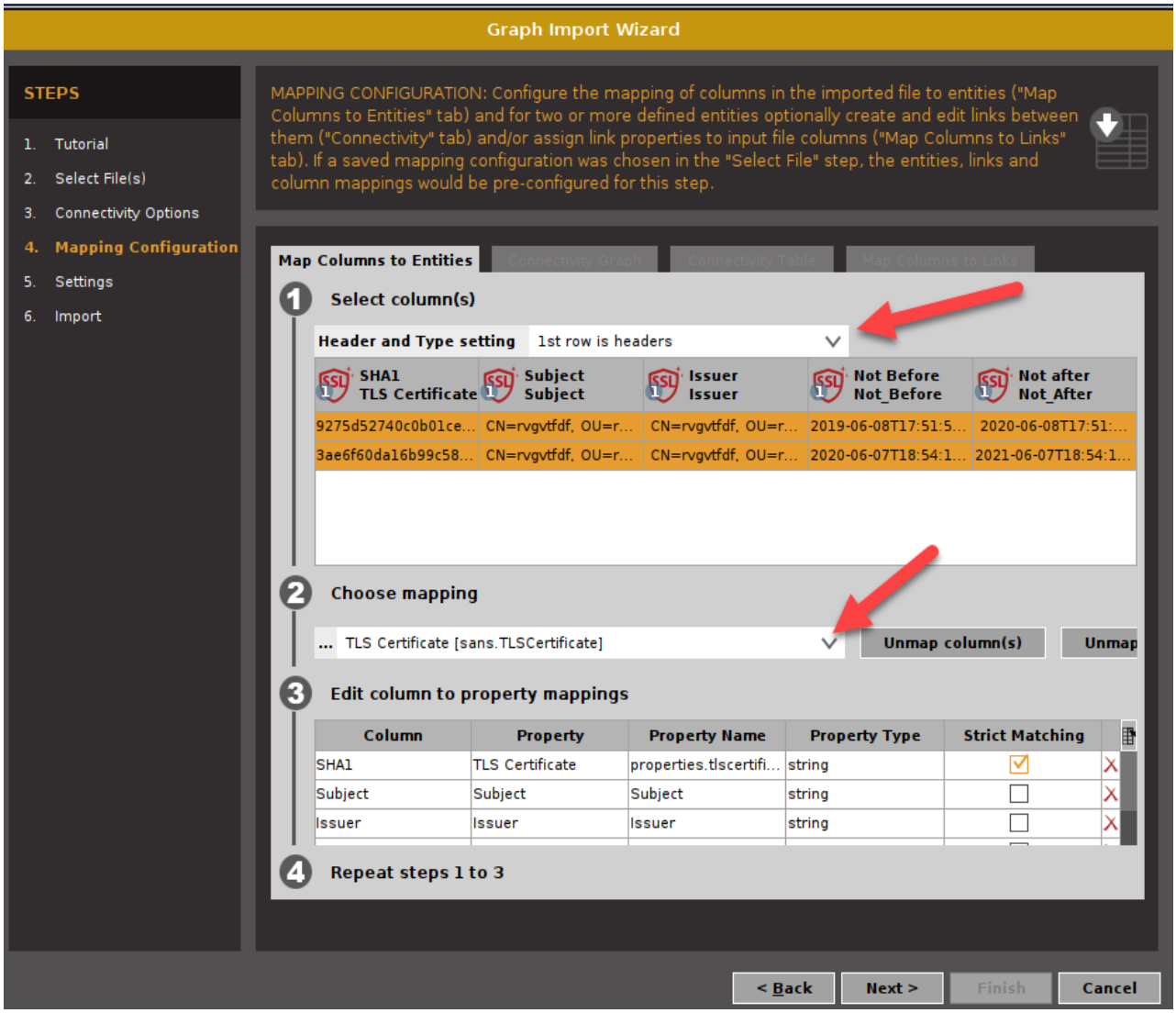
The purpose of this window is for us to tell Maltego how we want our CSV data to be mapped to entities and properties. Use the "Header and Type Setting" pull-down and choose "1st row is headers" because you have header information in your data file. Then select all the columns (use the Shift key to select all columns—they will highlight orange) and map it to the TLS Certificate entity you created. We select all the columns at once because we want to map them all as different properties on the same TLS Certificate entity.

Map the Subject column to the Subject property, the Issuer column to the Issuer property, the Not Before column to the Not Before property, and the Not After column to the Not After property. (It should line up correctly by default.)

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets

Technet24



After mapping your columns to the property entity, select Next twice (leave the defaults as is) and click Finish.

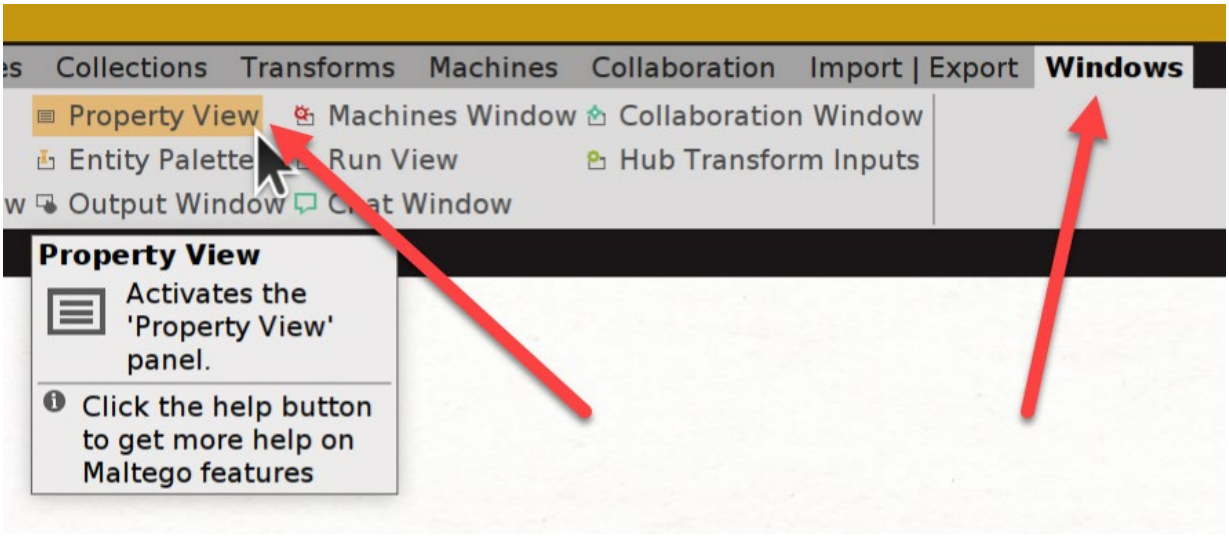
Last, you get a confirmation window that gives you statistics regarding how many rows were successfully extracted (in this case, 2 Rows), any errors, and how many entities were created (in this case, 2 Entities). Once you confirm that the import was successful, you will be able to view the two created entities on the graph and interact with them.

2. **When looking at the properties of the two TLS certificates, what similarities do you see?**

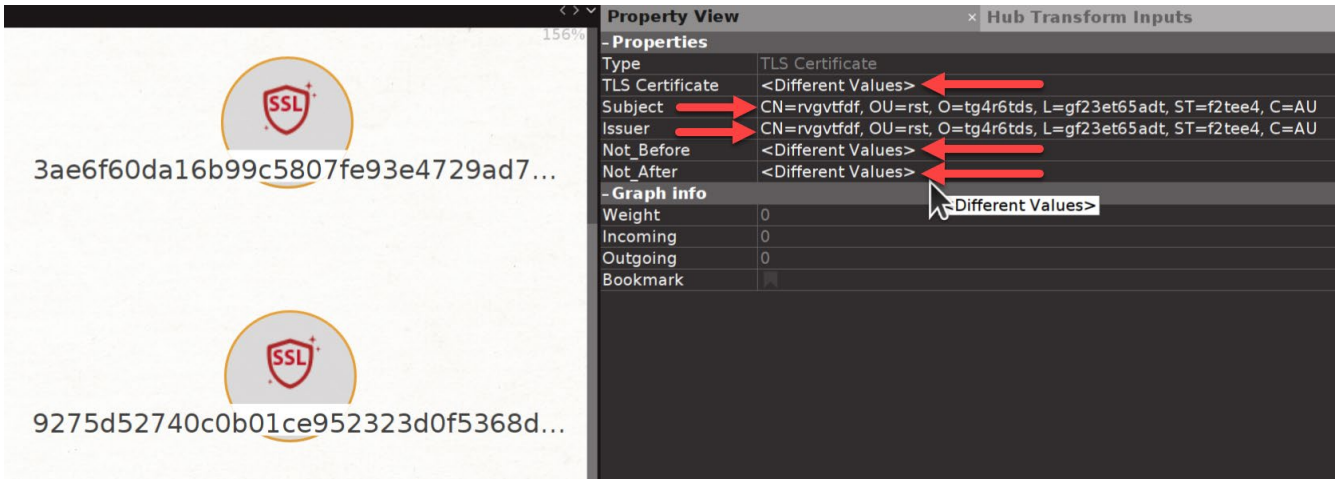
   - **Both certificates have the same subject and issuer**

One easy way to compare both TLS Certificates is by using the "Property View" window. Click the Windows menu, then click on Property View to bring up that window on the right side of our screen. (The "Windows" menu also lets us bring up other important windows such as the "Entity Palette" in case they are closed.)

© 2021 Robert M. Lee and SANS Institute
https://t.me/learningnets



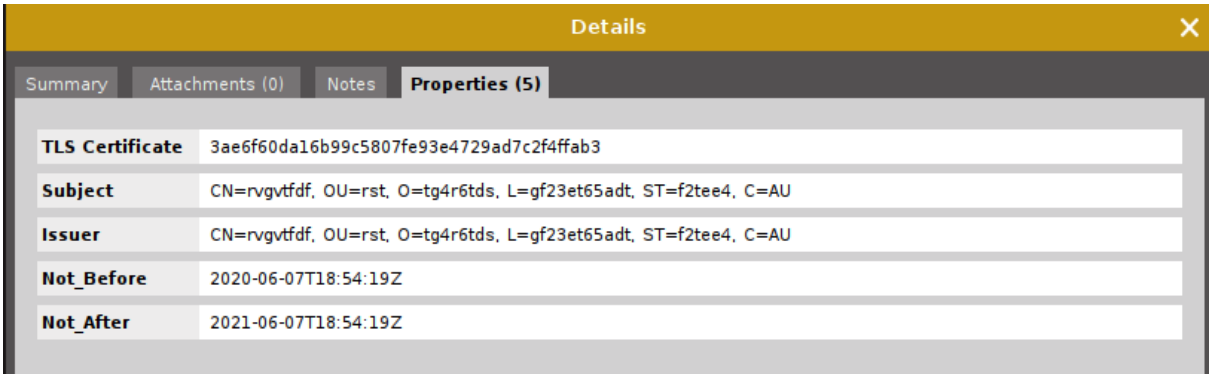
Now, select both TLS Certificates on our graph by clicking and dragging to highlight them both (we know they are selected when the orange circle appears around the entity icon). Observe that "Property View" tells us that the TLS Certificate, Not_Before, and Not_After properties are different between these two entities, while the Subject and Issuer properties are the same.

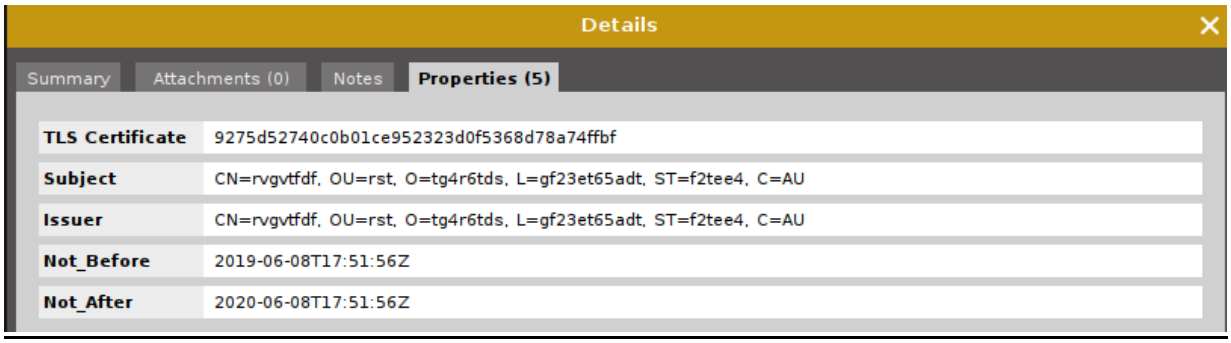


However, this only gives us a summary of how the properties compare. We want to look at the exact dates on the certificates. To do this, double-click each TLS Certificate entity, in turn, on the graph to view their details. Then check the Properties tab.



© 2021 Robert M. Lee and SANS Institute
https://t.me/learningnets
Technet24





3. **What differences do you see in the properties of the two TLS certificates?**

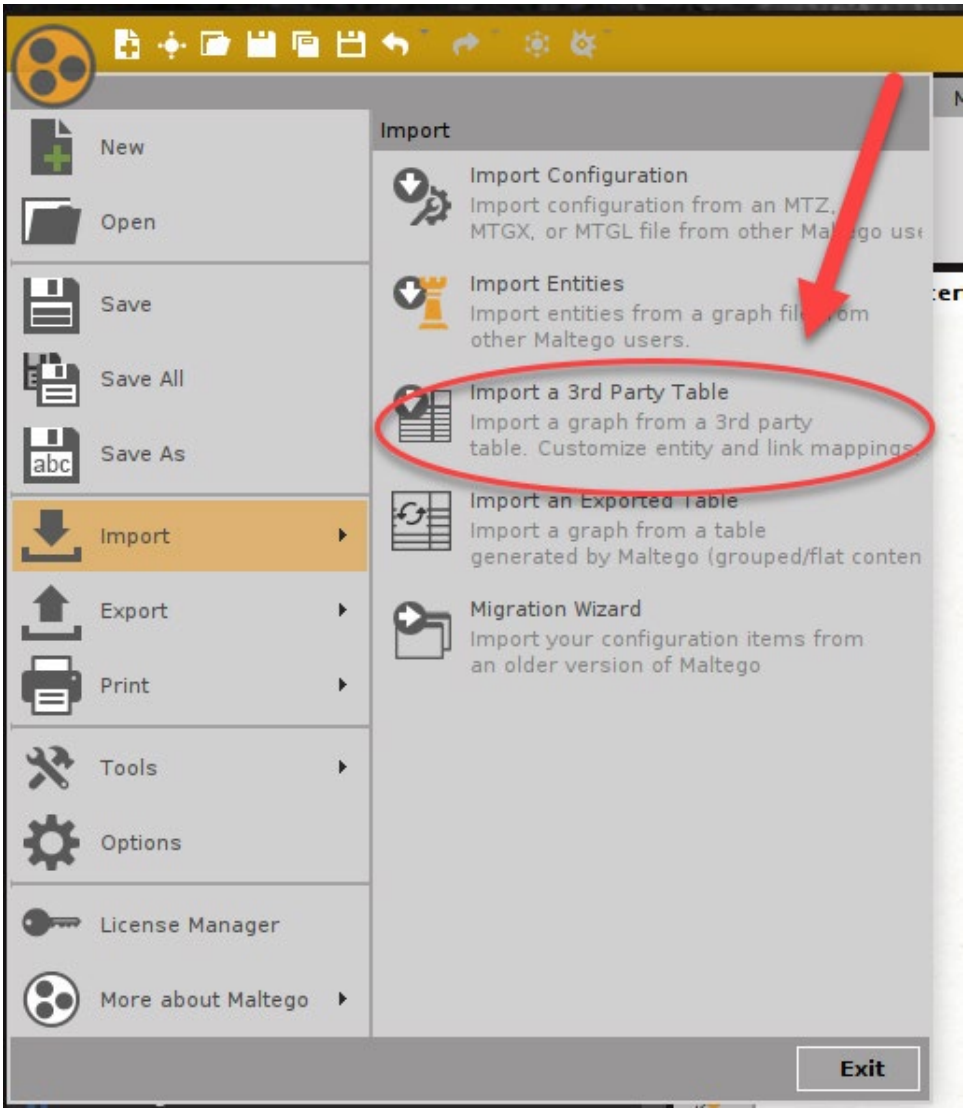
   - **The Not Before and Not After dates are different. The certificate beginning with 3ae… looks like it was created one day before the 927… certificate was going to expire. This is an interesting finding to note since it suggests a relationship between the certificates. This shows that pivoting on TLS certificates should also include pivoting on IP addresses.**

4. **What entities and properties do you need to use when importing the Trickbot Ips.csv file?**

   - **The IP addresses need to be mapped to the IP Address entity, and the TLS certificate will need to be mapped to the TLS certificate entity we created earlier. Additionally, the First Seen and Last Seen should be added as properties.**

From the same graph that was created in questions 1 and 2, perform the Import Graph from Table action again, this time using the Trickbot Ips.csv file.

© 2021 Robert M. Lee and SANS Institute
https://t.me/learningnets

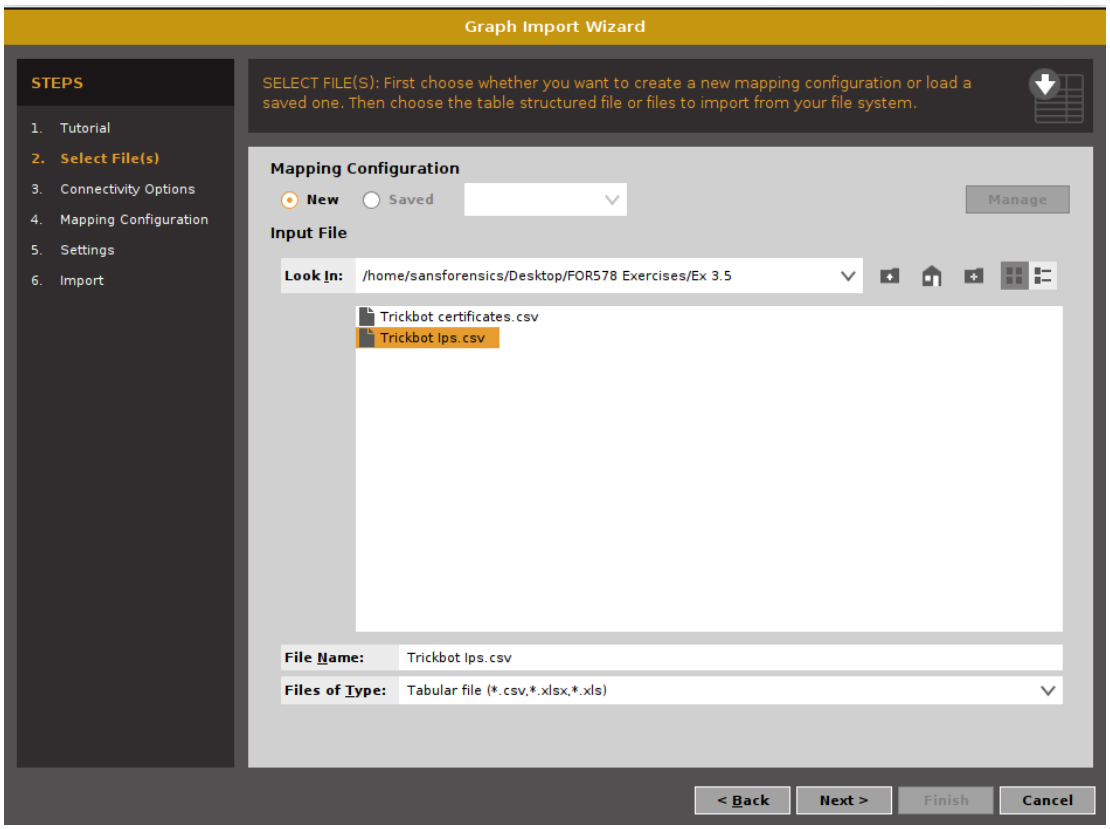


Just like the last import, select Next on the first screen. Then select the Trickbot Ips.csv from the Ex 3.5 folder.

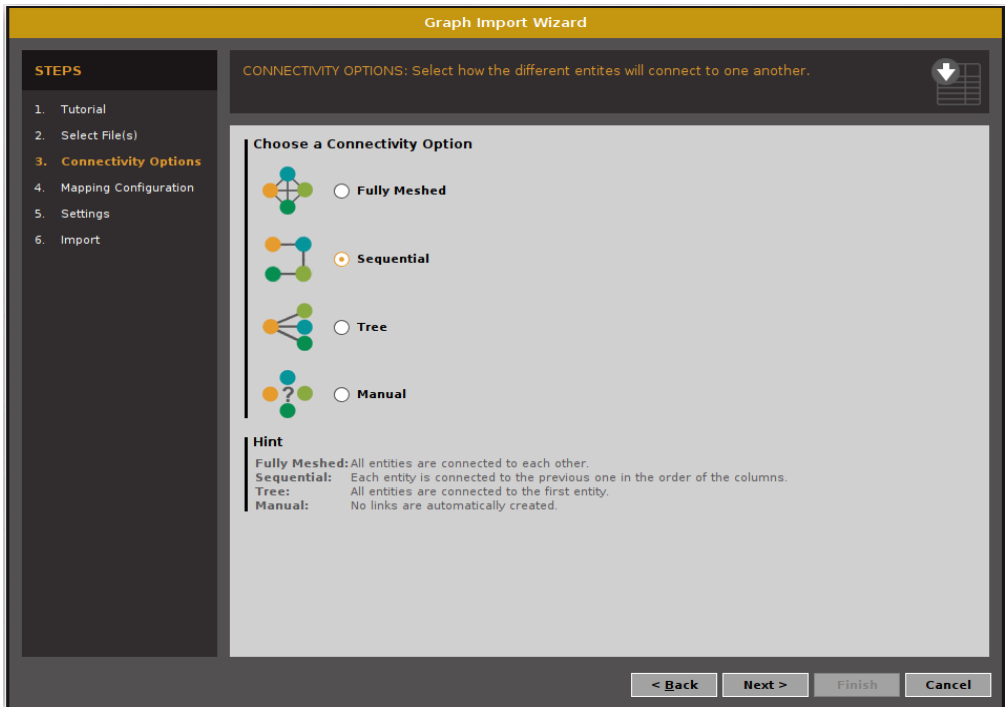
© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets

Technet24

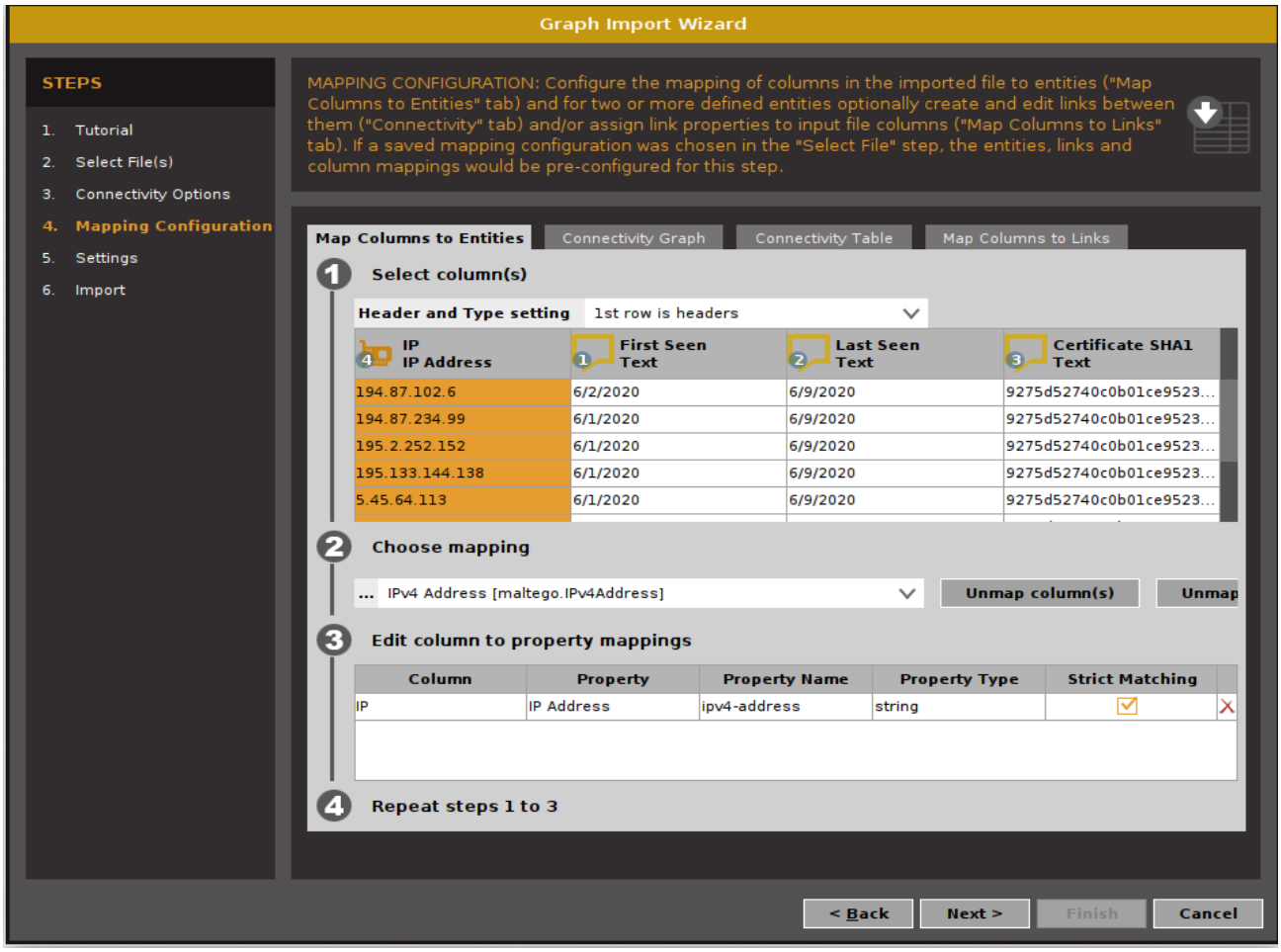


Choose the default Connectivity Option (Sequential).



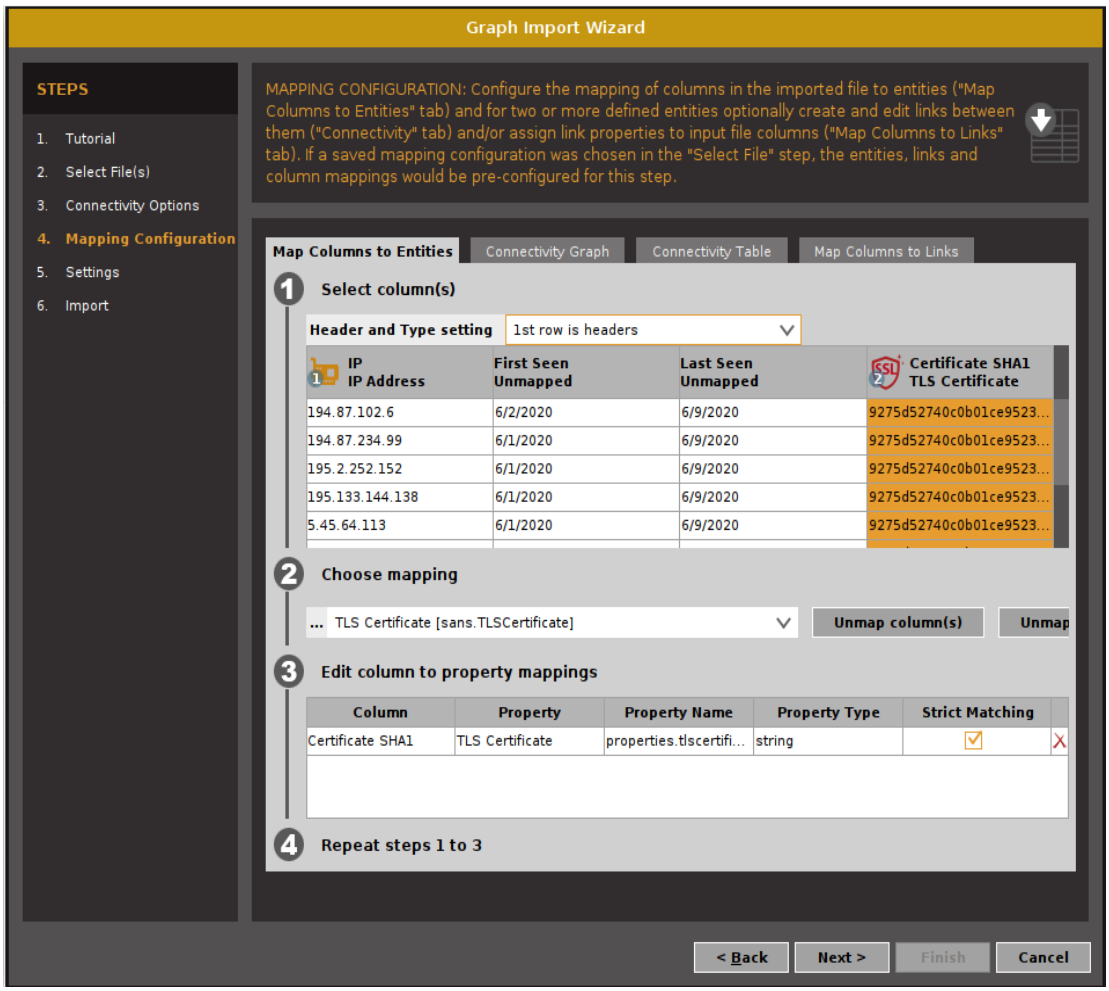
© 2021 Robert M. Lee and SANS Institute
https://t.me/learningnets

For the mapping, make sure to select "1st row is headers" from the dropdown. Then select *only the IP column* and map it to the to the IPv4 Address entity. We are only selecting one column because that is the only column we want mapped to the IPv4 Address entity.



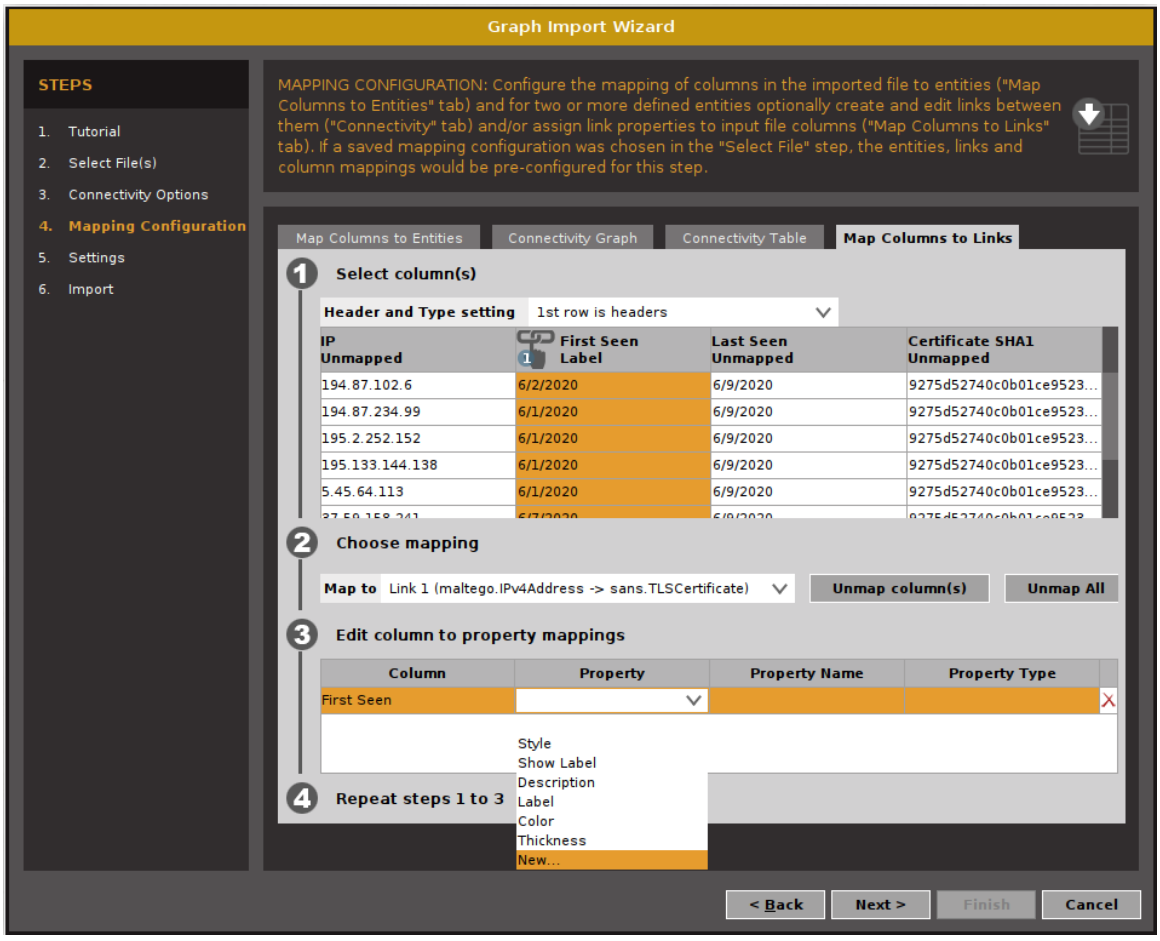
Then, select *only* the Certificate SHA1 column and map it to the TLS Certificate entity we previously created. Next, select shift to highlight *both* the "First Seen" and "Last Seen" columns at the same time and select "Unmap Column(s)". Your screen should now look like the below, with only the first and last columns mapped.

© 2021 Robert M. Lee and SANS Institute
https://t.me/learningnets
Technet24

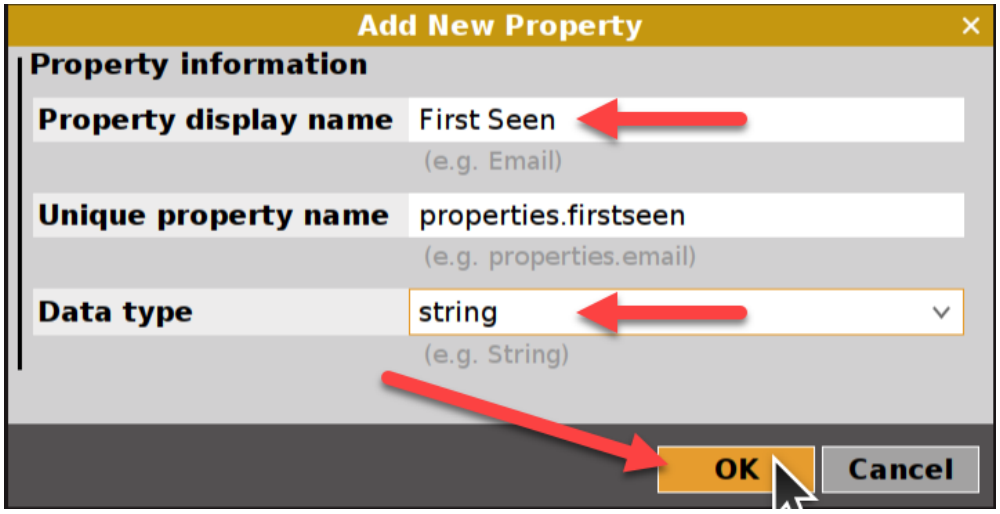


Whenever importing data, we need to think about how we want it mapped. IP Addresses are entities, and TLS Certificates are also entities. However, the "First Seen" and "Last Seen" dates describe the *link between* a TLS Certificate and an IP Address—the dates when that certificate was valid for that IP. Therefore, we want to map these two dates to the *link between* the two entities we just mapped. To do this, select the "Map Columns to Links" Tab. Select the "First Seen" column and then select "Link 1 (maltego.IPv4Address -> sans.TLSCertificate)" from the "Map to" dropdown menu. Next, in the "Edit column to property mappings" section, click the "Property" dropdown and select New. This allows us to assign the "First Seen" data to a new property name, since Maltego doesn't have one for this data yet.

© 2021 Robert M. Lee and SANS Institute
https://t.me/learningnets

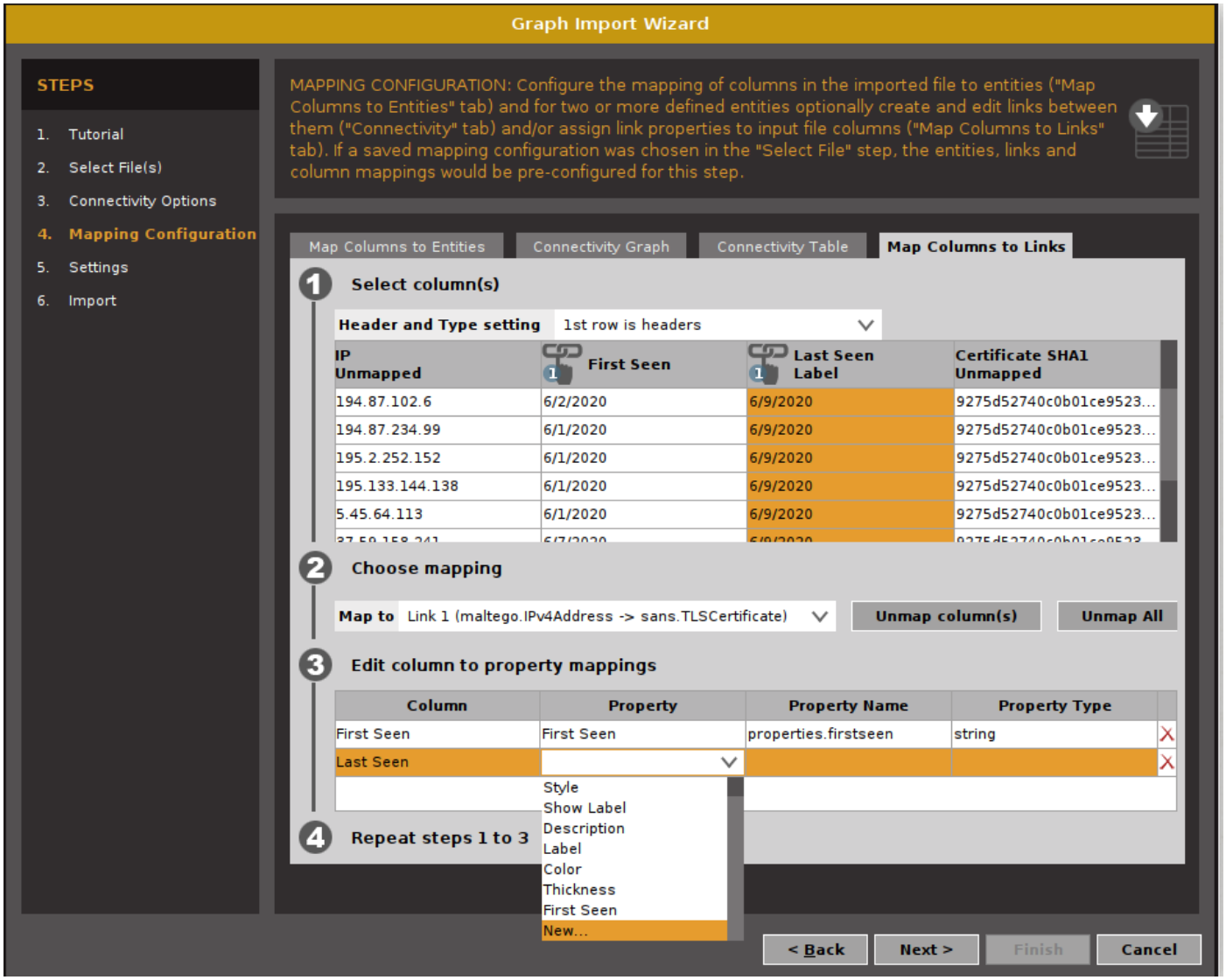


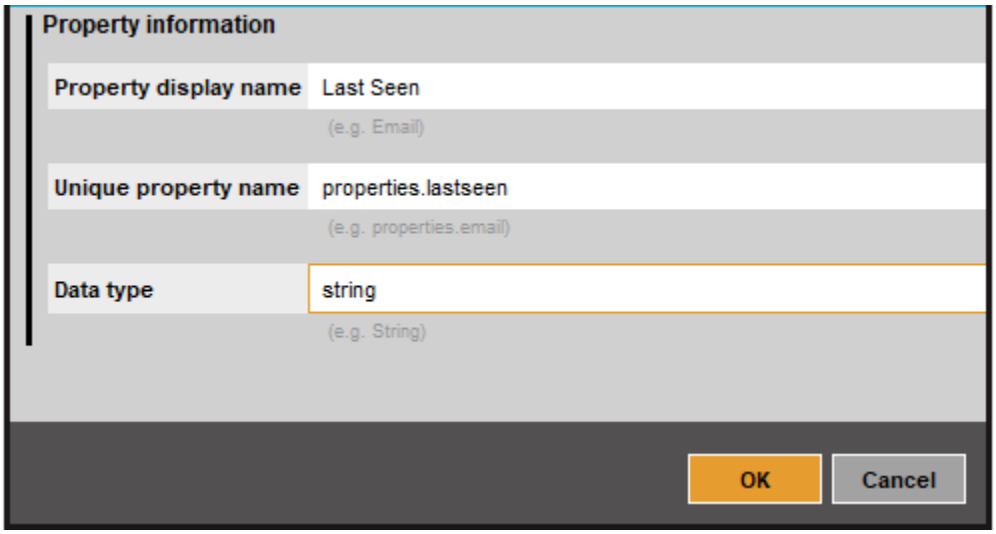
In the "Add New Property" window, set the "Property display name" to "First Seen". The Unique property name is set by Maltego but can be changed if needed. Make sure the Data Type is set to string, then click OK.



Repeat the same step for the "Last Seen" column as shown below.

© 2021 Robert M. Lee and SANS Institute
https://t.me/learningnets
Technet24



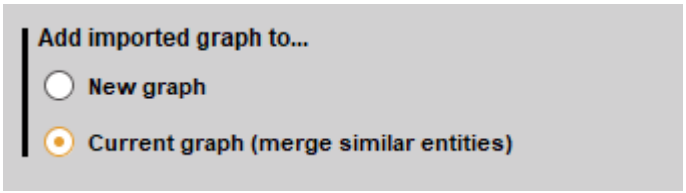


© 2021 Robert M. Lee and SANS Institute
https://t.me/learningnets

Make sure the "Header and Type setting" pull-down is still set to "1st row is headers."



Click Next, and before you click Next again, make sure you change the "Add imported graph to…" section to "Current Graph" instead of "New Graph". This will result in our second CSV entities being imported to the same graph we previously used. Maltego will merge similar entities, such as any TLS Certificates with the same SHA1 values.

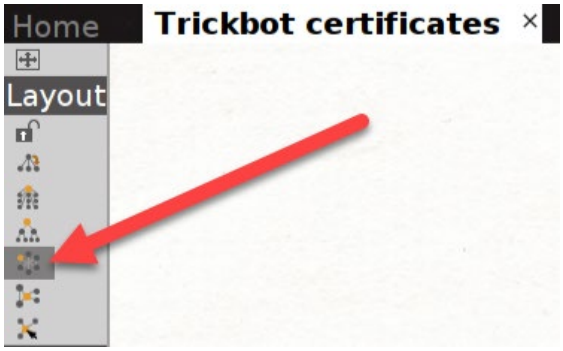


Then click Next, then Finish. We should have imported 38 rows, 32 entities, and 38 links. If you do not get those results, double-check the steps above to ensure you imported everything exactly as written. Now, review the new graph to answer questions 5 and 6.

5. **What relationships do you see between the two certificates after importing the Trickbot Ips.csv file?**

- **There are eight IP addresses that have direct links between both TLS certificates. This means that we have seen the certificates be updated on previously found IP addresses. This is a great indicator of command-and-control infrastructure.**

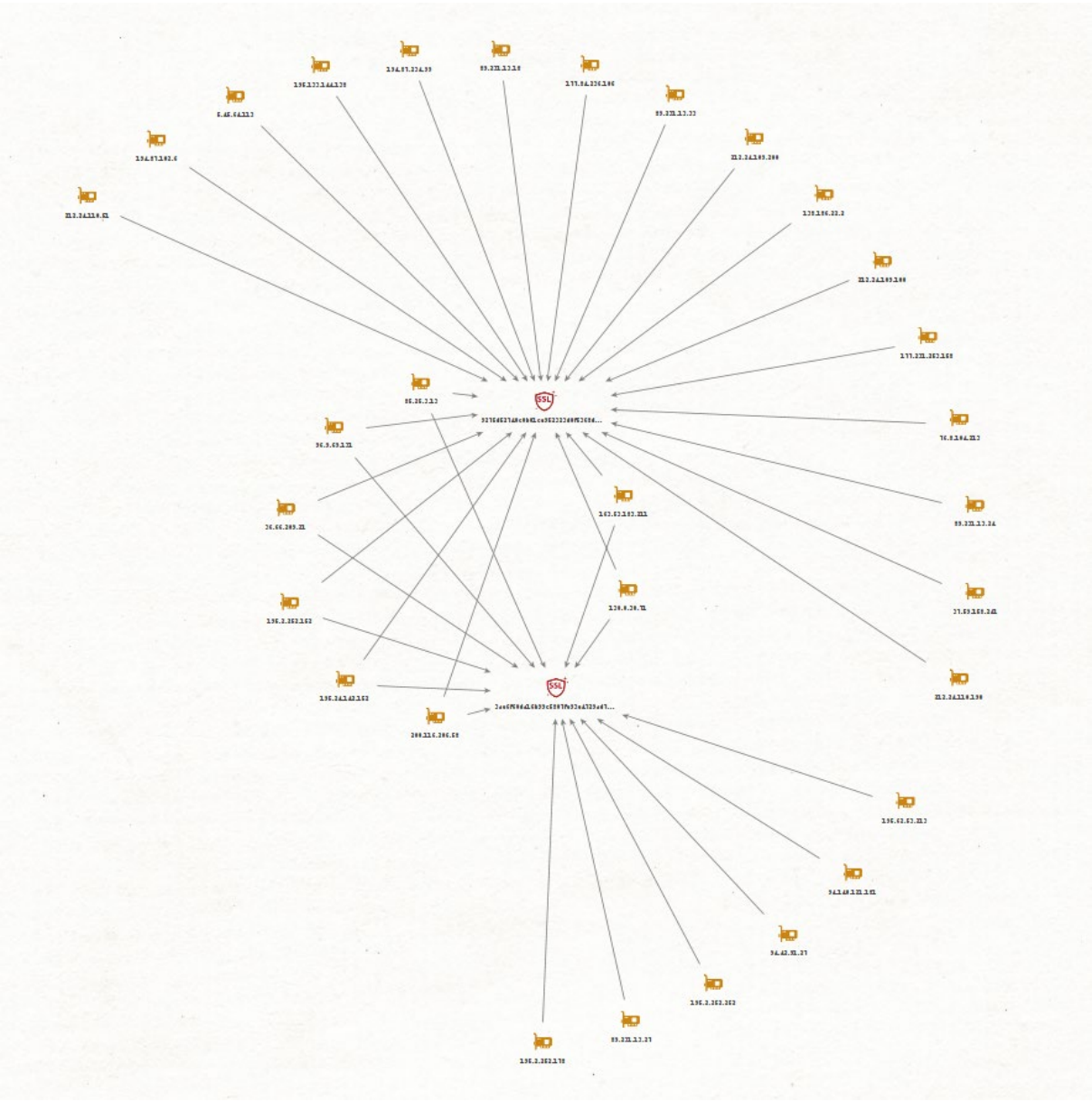
Your graph should look something like below. If it does not, entire "Set layout mode to Circular" is selected under the left-side "Layout" menu. You may also experiment with other layouts if you wish.



This Circular layout allows us to clearly observe that there are eight IP addresses that have been observed using both of these certificates. As we consider why that might be, we assess that it must mean those IP addresses are of concern to someone (like an adversary). If those IP addresses were

© 2021 Robert M. Lee and SANS Institute
https://t.me/learningnets
Technet24

not important, an adversary likely would not have bothered to register another TLS certificate on them. This leads us to make the assessment that those eight IP addresses may be command and control infrastructure.



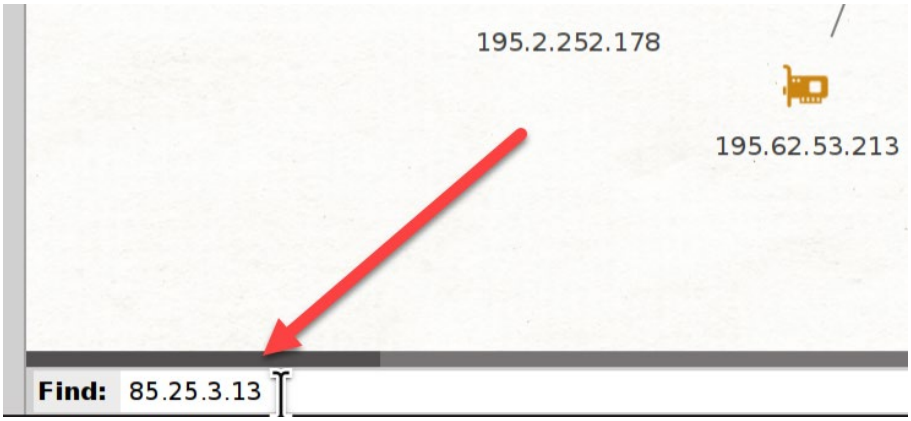
6. **What does the certificate information tell us about IP 85.25.3.13?**

- **<u>The IP is likely a long-term command-and-control server for this set of intrusions.</u>**

To further support our assessment that these IP addresses may be command-and-control infrastructure, we can take a closer look at the dates when the certificates were valid on certain IPs. Jump to the 85.25.3.13 IP address on your graph. One way to do this is by selecting CTRL+F to bring up the "Find" window at the bottom, and then typing in 85.25.3.13 and hitting enter.

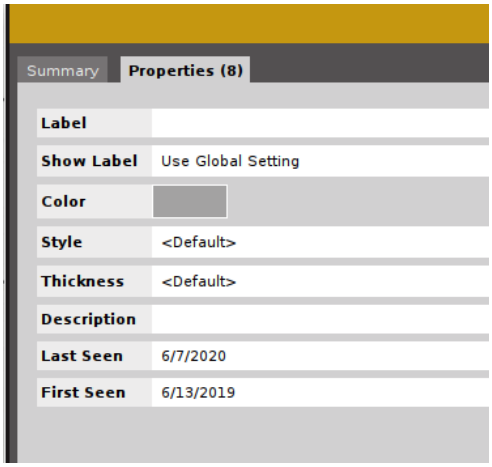
© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets



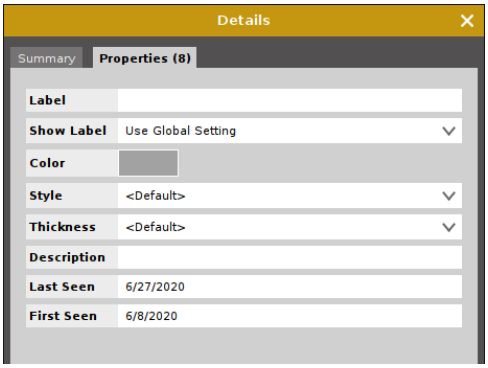
Now the IP address of interest is highlighted. The links between the IP address and the certificates are also highlighted in teal. Double-click on each link between the IP address and the certificates, in turn, to view the properties of the link between the two entities. (You may also hover over each link and view its properties in the "Property View" window we used before.)

We know that certificate 9275d52740c0b01ce952323d0f5368d78a74ffbf was created on 6/8/2019, as we saw the "Not Before" date on that certificate previously. The IP address 85.25.3.13 was last seen with the 9275d52740c0b01ce952323d0f5368d78a74ffbf certificate on 6/7/2020, which is the day before that certificate was set to expire.

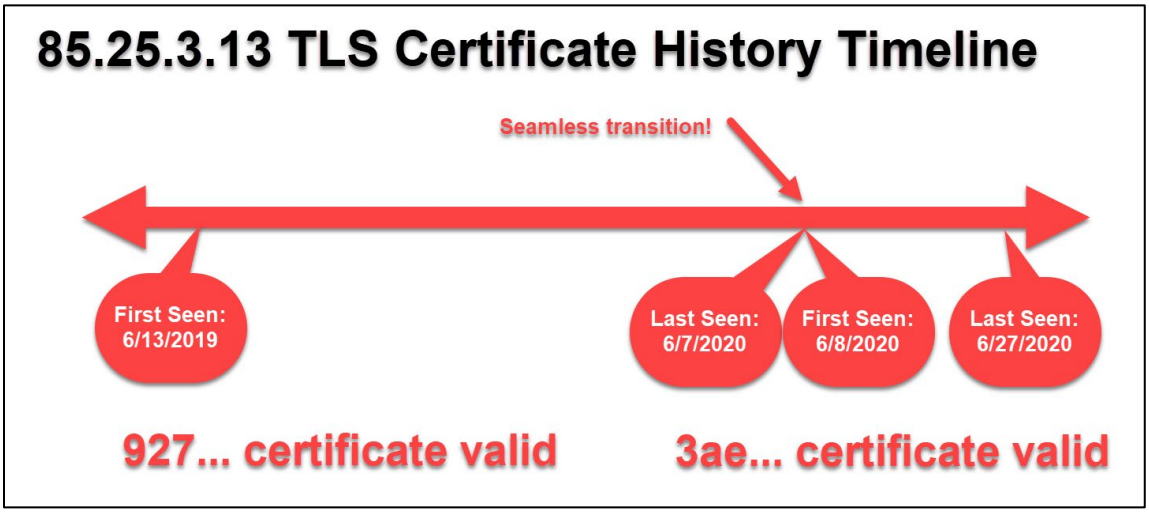


On 6/8/2020, the IP address 85.25.3.13 was seen with the newer 3ae6f60da16b99c5807fe93e4729ad7c2f4ffab3 certificate, and activity continued at least to 6/27/2020.

© 2021 Robert M. Lee and SANS Institute
https://t.me/learningnets
Technet24



It might help to think of this overlap like a timeline. Just as the 927... certificate expired, the 3ae… certificate was registered to take its place. The fact that the adversary cared enough to register a new certificate on this IP helps us support the assessment that this is an indicator of long-term command-and-control usage.



Exercise: Key Takeaways

- **Looking at the use of TLS certificates by malware and the IP addresses they are seen on is a great method for finding and tracking additional network infrastructure.**
- **Reviewing the Not Before and Not After dates of a certificate can give you a start to a timeline of when it was actively first being used.**
- **Having the ability to routinely check and store dates when TLS certificates were seen can also help identify long-term usage and possibly critical nodes in a command-and-control infrastructure.**

© 2021 Robert M. Lee and SANS Institute
https://t.me/learningnets

This page intentionally left blank.

https://t.me/learningnets

Technet24

Exercise 4.1: Storing Threat Data and Information

Objectives

- Leverage a storing platform to collect, structure, and store indicators and information
- Identify correlations between intrusion data and analyze common techniques

Scenario: We previously analyzed six intrusions against Edison and Spader Technologies (which you collapsed into five intrusions) and mapped details to the Kill Chain, Diamond Model, and MITRE ATT&CK. Though Excel was a good place to start, we now want to import this data into MISP so that we do not lose track of it. We also want to see if you can correlate it to other existing data. We have done additional analysis and divided your spreadsheet by indicators and ATT&CK techniques, which you will now enter into MISP. Our team has previously used MISP to track indicators from external reports, and we also want to use MISP to track ATT&CK techniques.

Exercise Prep

*You will use the SANS VM and the MISP application. The username for MISP is "**for578@for578.org**" and the password is "**SANSForensics!**" (minus the quotes). You will also use the **"Combined Intrusion Data"** spreadsheet in the **Ex 4.1** folder. If MISP does not load the first time, simply restart the VM and it should load.*

Your team has started taking notes about how you enter data into MISP, which is the start of a MISP Style Guide. The team has agreed upon the following procedures for entering MISP data:

- Remove all redactions of indicators such as (dot) or [.]
- Use the following Categories and Types for our Attributes:

Category	Type	What we use it for
Internal Reference	link	External URLs of original reports
Attribution	threat-actor	Anything in the Adversary vertice of the Diamond Model like passwords that doesn't have another type
Payload delivery	filename	Any filenames used during intrusions, including email attachments and Windows built-in files
Network activity	ip-dst or ip-src	Any IPs used during intrusions, ip-dst is for outbound traffic and ip-src is for inbound traffic
Network activity	domain	Any domains used during intrusions
Payload installation	malware-type	Any malware family names used during intrusions
Payload delivery	email-src	For sender email addresses of phishing emails
Artifacts dropped	pattern-in-file	Any unique folder names or paths
Artifacts dropped	mutex	Any mutexes identified from malware analysis/pivoting
Targeting data	target-machine	Any victim/target IP addresses

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets

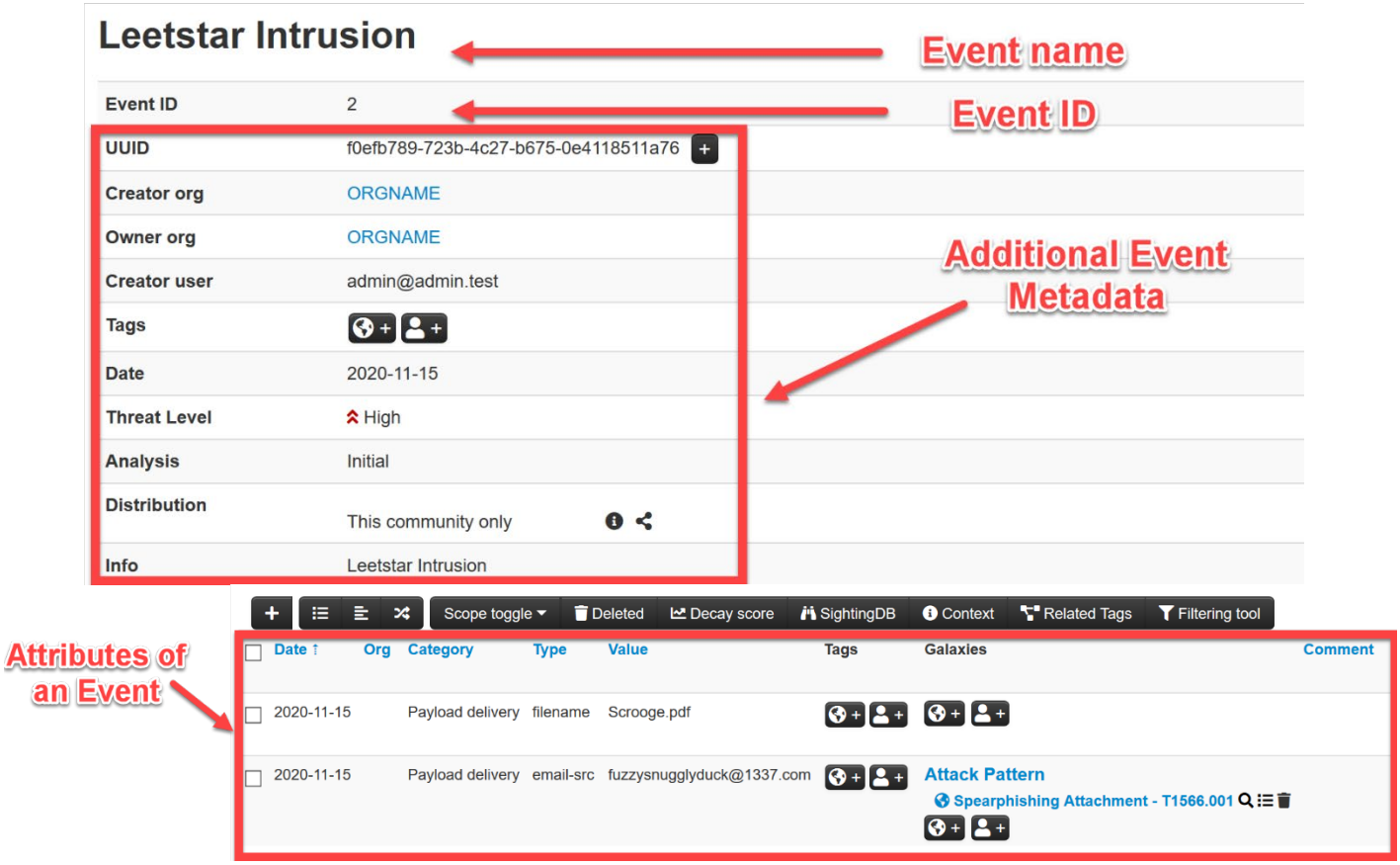
MISP Primer

If you haven't used MISP before, you may want to check out their Quick Start Guide and documentation here: https://www.circl.lu/doc/misp/quick-start/. Every threat intelligence platform has what is commonly referred to as an "ontology"—the characteristics of object types the platform uses. MISP has many features, and we'll just scratch the surface of them in this exercise, so refer to the documentation for additional details.

Here are some basic parts of the MISP "ontology" and what they mean in plain language (see the MISP documentation at https://www.circl.lu/doc/misp/ for full definitions):

- **Events**: This is a key object in MISP; for example, an intrusion may be an Event.
  - **Attributes**: Each Event can have one or more Attributes, which have a **Category**, **Type**, and **Value**.
    - **Tags**: Each attribute may have one or more Tags. For example, an IP address may have a Kill Chain Tag of "Reconnaissance".
- **Galaxies**: Events and Attributes can have attached Galaxies. For example, an Event may have an ATT&CK technique Tag added from the MITRE ATT&CK Galaxy**.**

Example MISP Event Ontology



© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets

Technet24

Exercise: Questions

Part 1: Indicators

1. *Our tier 1 SOC analysts have already input data from Intrusions 1, 2, 3, and 4 into MISP as events with attributes. Log in to MISP to review the data and compare it to the **Combined Intrusion Data** spreadsheet and your team's draft MISP Style Guide (above). Did you have to update any of the previous-entered events to match your team's Style Guide?*

   - _____

2. *Enter the data for Intrusion 6 from the **Combined Intrusion Data** spreadsheet into MISP, following your team's Style Guide and using the freetext import tool. Manually add any attributes you feel are relevant that the freetext import tool missed. What adjustments do you have to make after using the freetext import tool?*

   - _____

3. *For each intrusion event, look at Related Events and the Correlation Graph. Do any of our intrusions match previous data from external reports?*

   - _____

4. *What do these overlaps tell us (or not tell us)? What hypotheses can we form about why we observe these overlaps?*

   - _____

Part 2: ATT&CK Techniques

5. *Your SOC analysts have already added the ATT&CK techniques from the **Combined Intrusion Data** spreadsheet to Intrusions 1, 2, 3, and 4. Add the appropriate ATT&CK techniques from the **Combined Intrusion Data** spreadsheet to the Intrusion 6 event in MISP by adding the appropriate MITRE ATT&CK galaxy tag to each attribute.*

6. *Based on the techniques you have added, what is the most prevalent technique you have observed in your dataset for these intrusions? Use the Statistics feature in MISP to help you.*

   - _____

7. *Why is this technique prevalence information relevant? What recommendations could you make to your defenders based on it?*

   - _____

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets

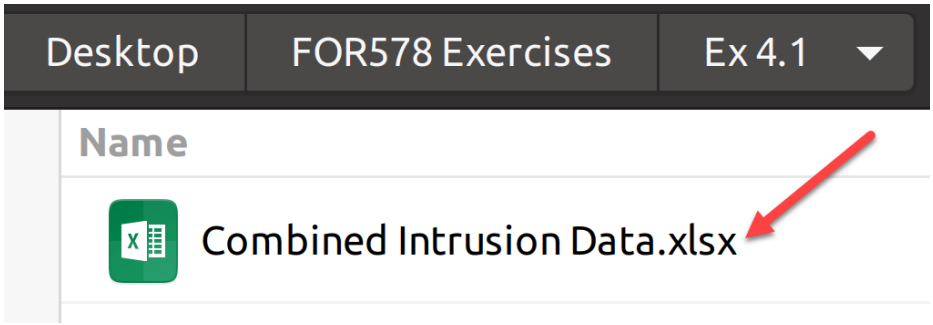
Exercise: Questions with Step-by-Step

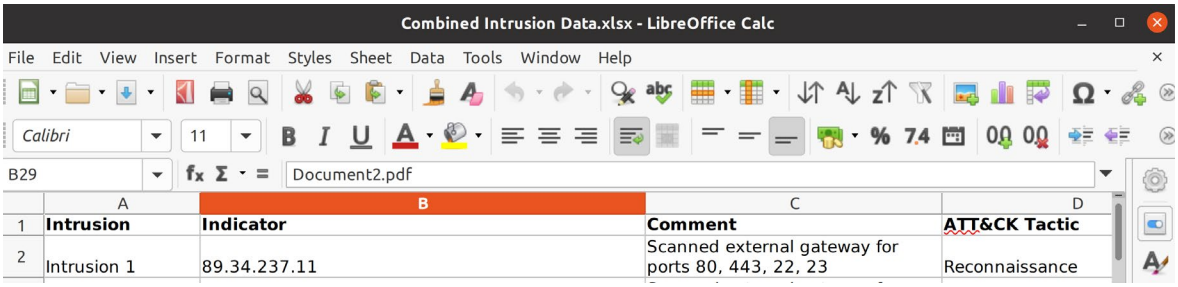
Part 1: Indicators

1. *Our tier 1 SOC analysts have already input data from Intrusions 1, 2, 3, and 4 into MISP as events with attributes. Log in to MISP to review the data and compare it to the* ***Combined Intrusion Data*** *spreadsheet and your team's draft MISP Style Guide (above). Did you have to update any of the previous-entered events to match your team's Style Guide?*

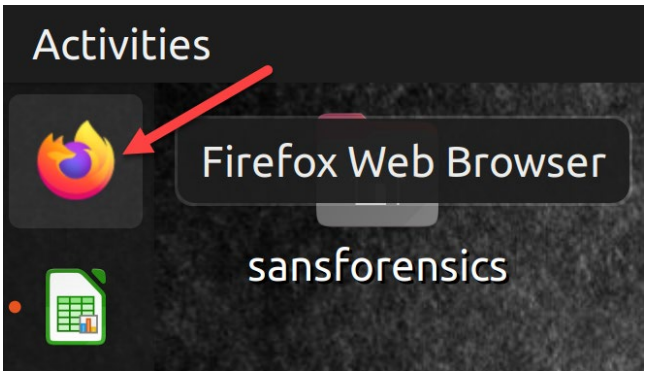
   - Yes, we had to update attributes on the events for Intrusions 1 and 2.

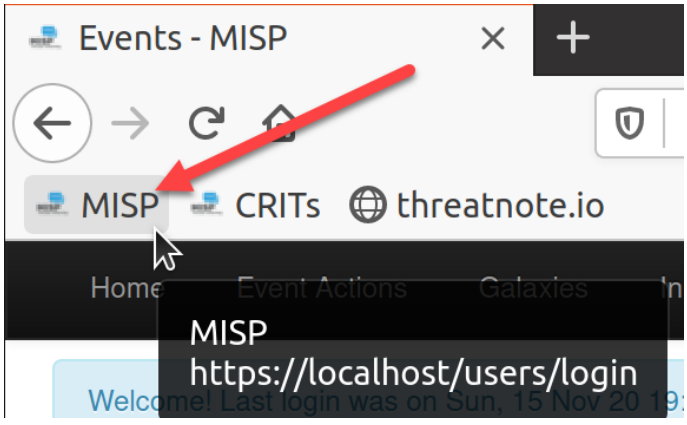
Open your Combined Intrusion Data spreadsheet from the Ex 4.1 folder on your VM. You can also open this spreadsheet on your host, which may be helpful particularly if you can view it on another screen. This file will automatically open in LibreOffice, an Excel-like application that comes with Ubuntu.





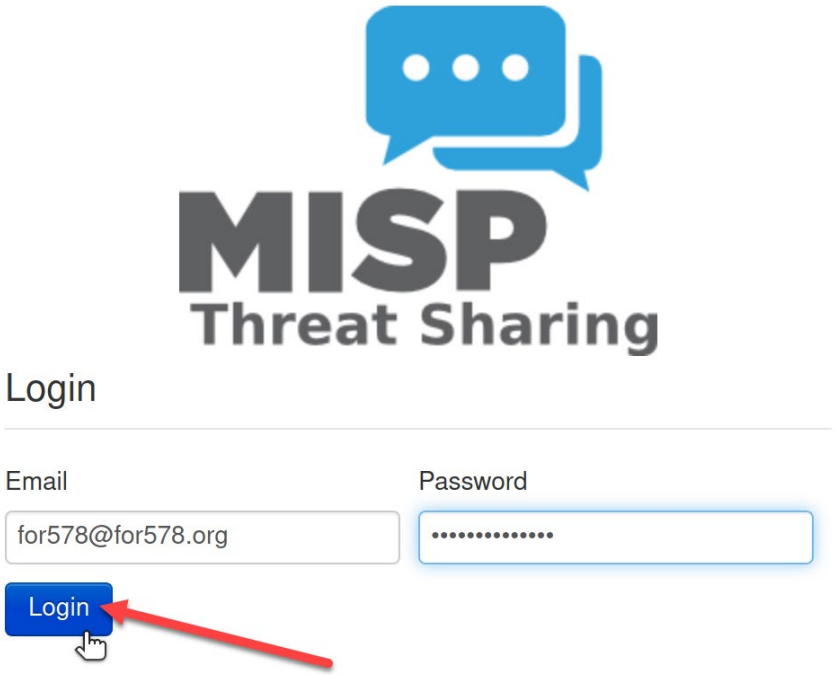
Launch the SANS SIFT VM and open MISP by opening Firefox from the left menu and clicking on the MISP bookmark.





© 2021 Robert M. Lee and SANS Institute
https://t.me/learningnets
Technet24

Log in to MISP using the user/pass: for578@for578.org / SANSForensics!

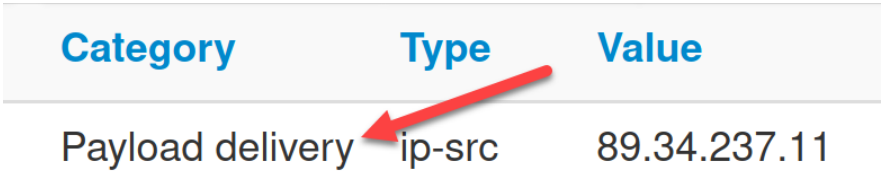


When we log in, we see events that already exist in MISP, including the events we need to review: Intrusions 1, 2, 3, and 4 (plus some external reporting). To view an event, click on the ID number associated with it.



4	1	for578@for578.org	2020-08-16	Intrusion 4
3	5	for578@for578.org	2020-08-15	Intrusion 3
2	15	for578@for578.org	2020-08-14	Intrusion 2
1	1	for578@for578.org	2020-08-13	Intrusion 1

Review the attributes for the Intrusion 1 event and compare them to the above style guide and your spreadsheet. We observe that the category is "Payload delivery", but our style guide dictates we should use the category "Network activity".

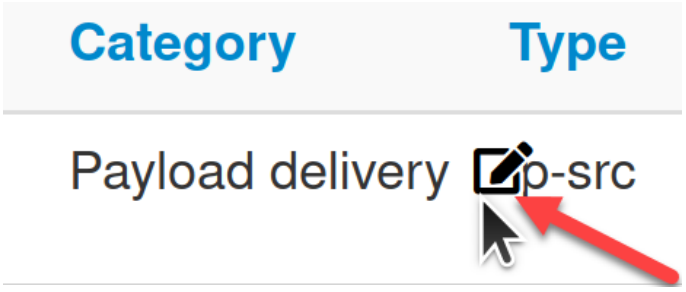


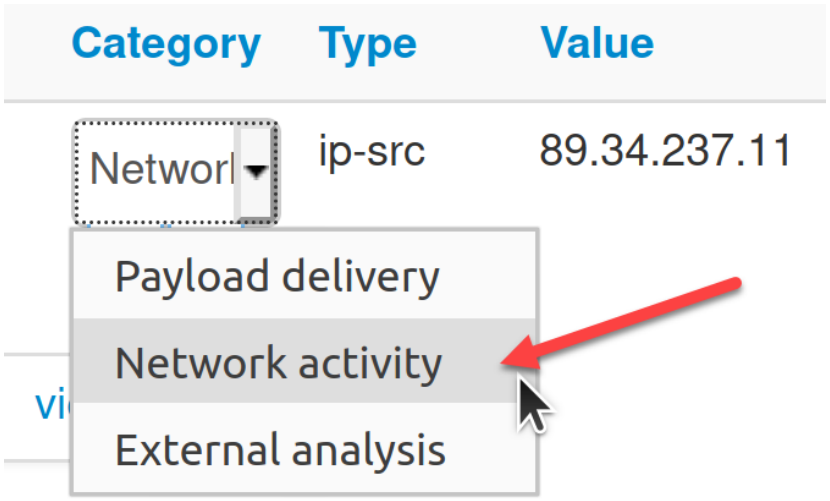
Category	Type	Value
Payload delivery	ip-src	89.34.237.11

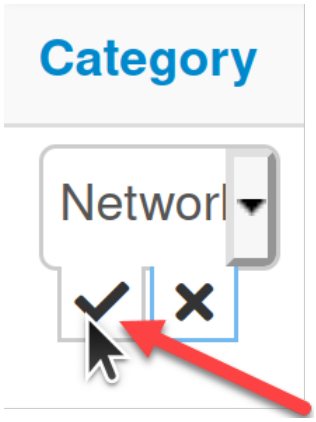
© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets

To change this, hover over "Payload delivery", click the edit icon, select "Network activity", and click the check mark to save the changes.





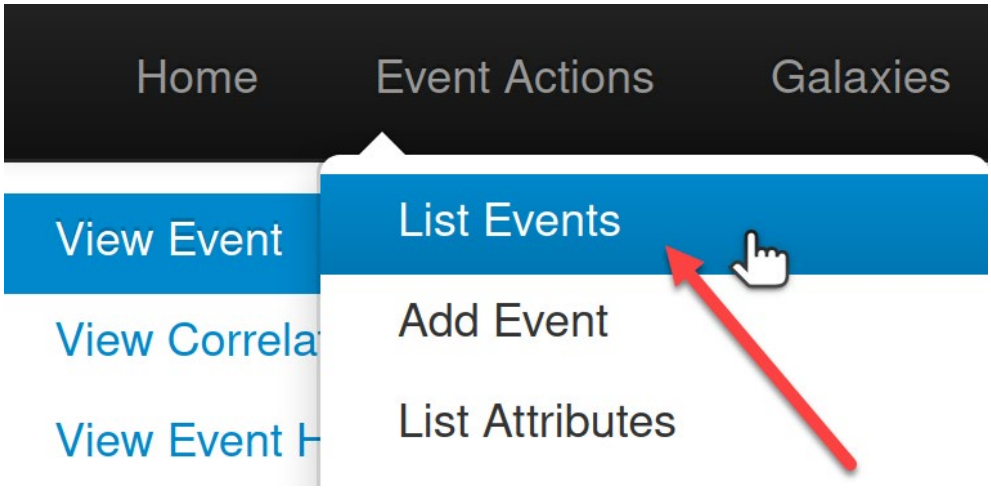


The corrected attribute should now look like this, which matches our style guide.

Category	Type	Value
Network activity	ip-src	89.34.237.11

© 2021 Robert M. Lee and SANS Institute
https://t.me/learningnets
Technet24

Now let's check the other events. To get back to the main event list, go to "Event Actions" and "List Events" in the top menu.

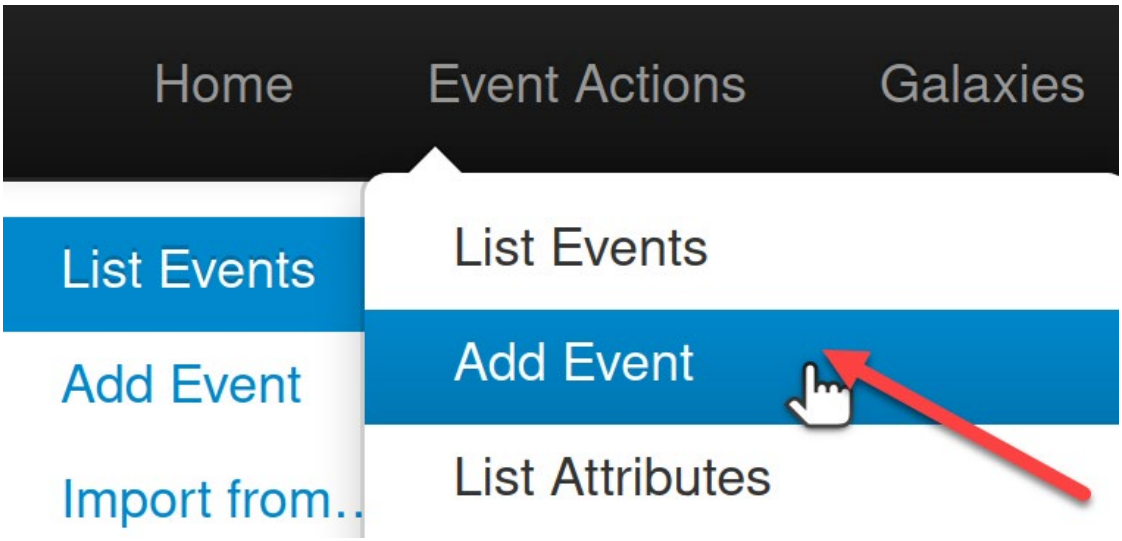


We review the events for Intrusion 2, 3, and Intrusion 4 as well, and they look good to us. If you identify other improvements or edits to be made, feel free to make them.

2. *Enter the data for Intrusion 6 from the **Combined Intrusion Data** spreadsheet into MISP, following your team's Style Guide and using the freetext import tool. Manually add any attributes you feel are relevant that the freetext import tool missed. What adjustments do you have to make after using the freetext import tool?*

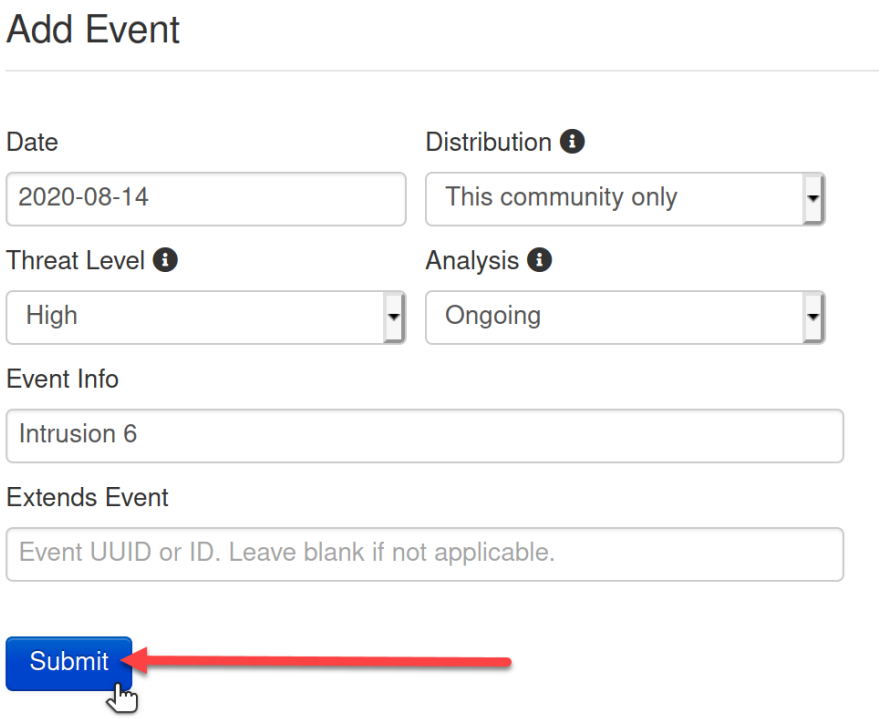
   - **We had to change the email address and mutex Types and manually add an attribute for Poison Ivy.**

To add a new event to MISP, go to the "Event Actions" menu and select "Add Event".

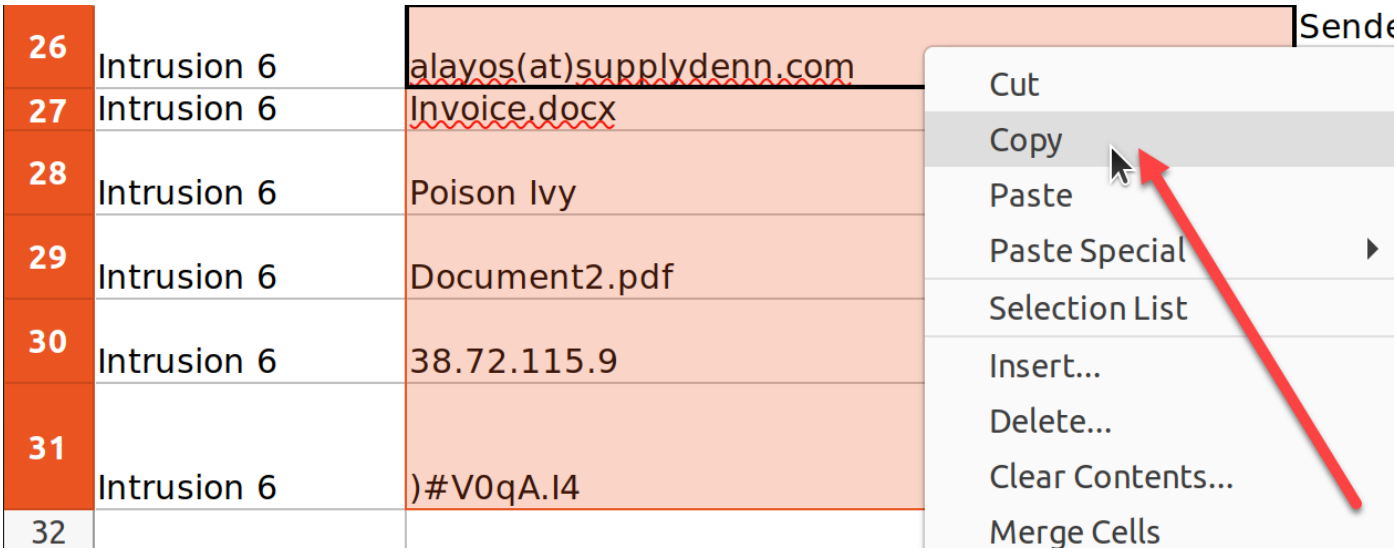


© 2021 Robert M. Lee and SANS Institute
https://t.me/learningnets

We will enter the date of the intrusion, 2020-08-14, which we know from Exercise 2.1. We will keep our distribution to "This community only" since we don't want to share this just yet. Our Threat Level is "High" and our analysis is "Ongoing". For Event Info, we just enter "Intrusion 6", and we can update it later if we need to. Click "Submit" to add the event.

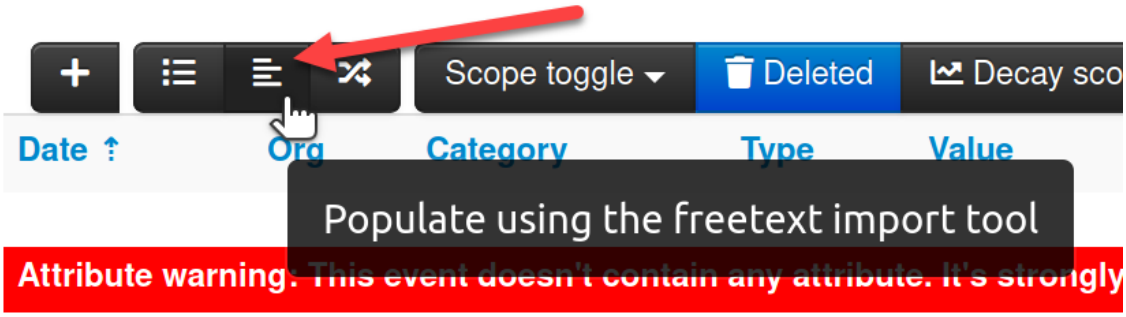


Now our event is created, but as MISP warns us, there are no attributes. We could manually add attributes, but we are going to see if MISP's freetext import feature helps save us time ingesting indicators. Navigate to your "Combined Intrusion Data" spreadsheet in LibreOffice and highlight just the six indicators for Intrusion 6. Right click and select "Copy".

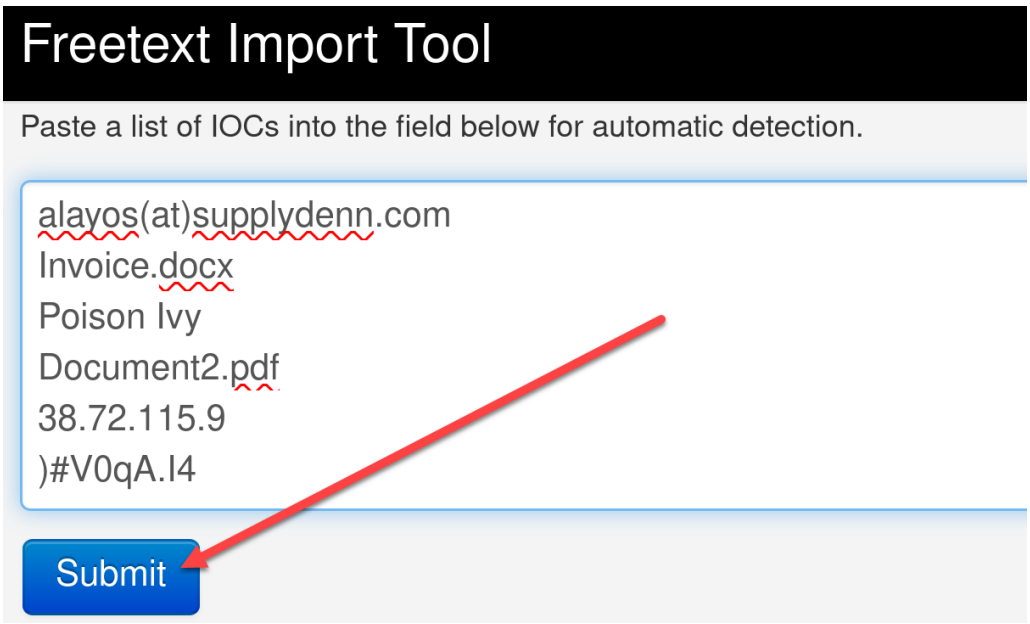


© 2021 Robert M. Lee and SANS Institute
https://t.me/learningnets
Technet24

Navigate back to MISP. In the attributes menu, select the icon for "Populate using the freetext import tool".



Right-click and paste your indicators into the field, then click "Submit".



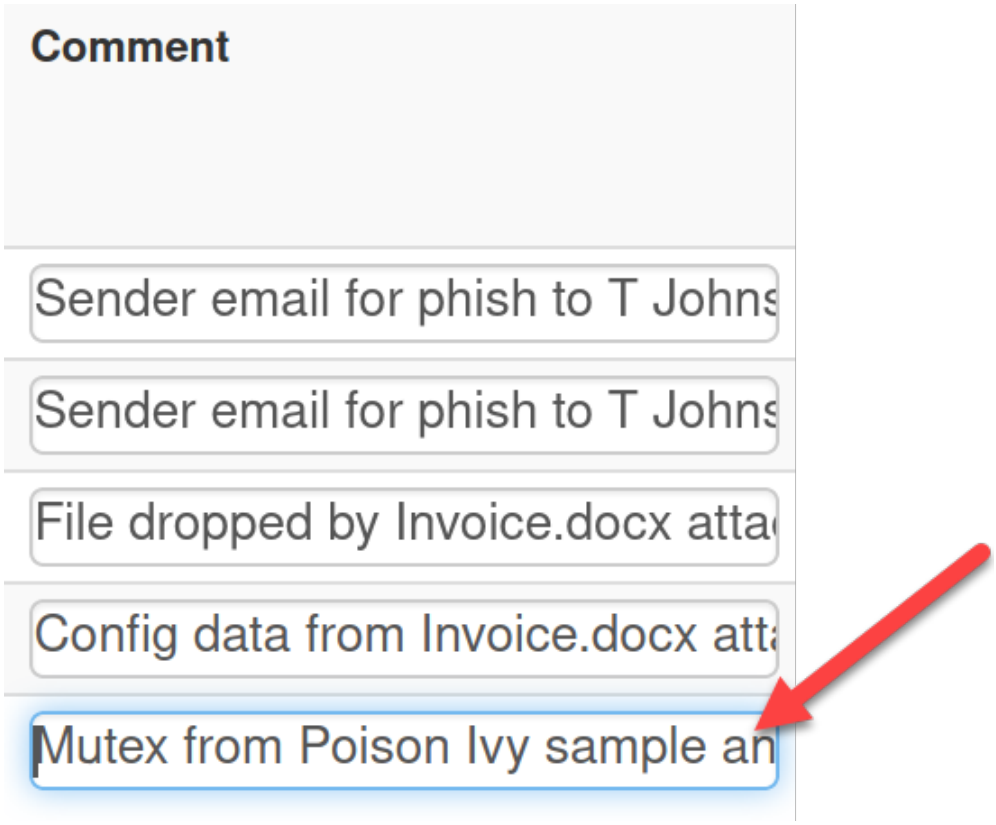
Your output should look like the below. MISP attempts to identify the correct Category and Type for each indicator, but sometimes it gets it wrong. You'll also note that MISP did not recognize "Poison Ivy" as a valid indicator.

Value	Similar Attributes	Category	Type
alayos(at)supplydenn.com		Payload delivery	filename
Invoice.docx		Payload delivery	filename
Document2.pdf		Payload delivery	filename
38.72.115.9	7	Network activity	ip-dst
#V0qA.I4		Payload delivery	filename

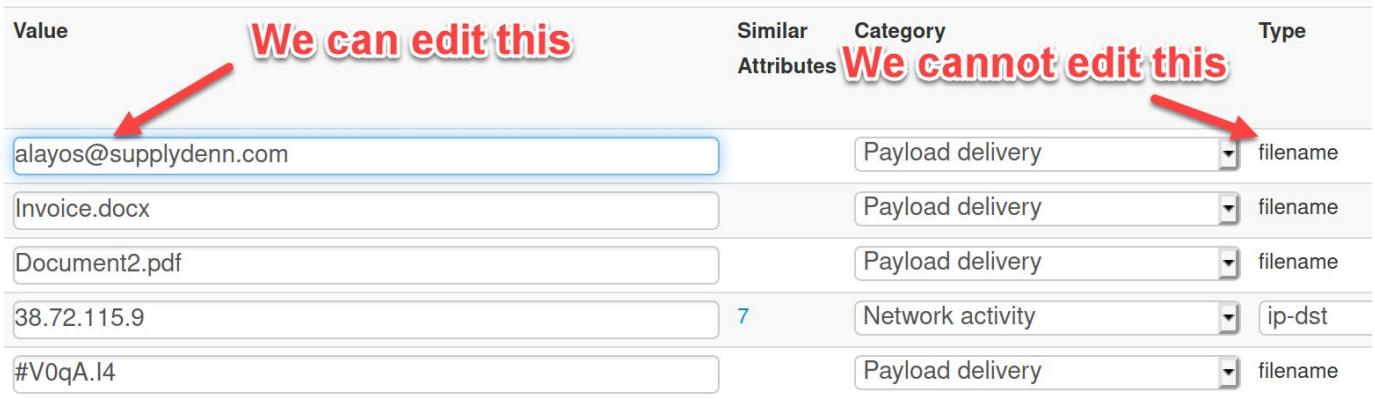
© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets

Copy and paste each "Comment" cell from your spreadsheet into the "Comment" field corresponding to each indicator in MISP. (Remember, we never want to import indicators without context!!!)



We also observe that there is an "(at)" in the first email address, and it has the wrong Category and Type, so we want to update that. We see that we can change the "(at)" by editing the value directly, but we can't change the Type from this view.

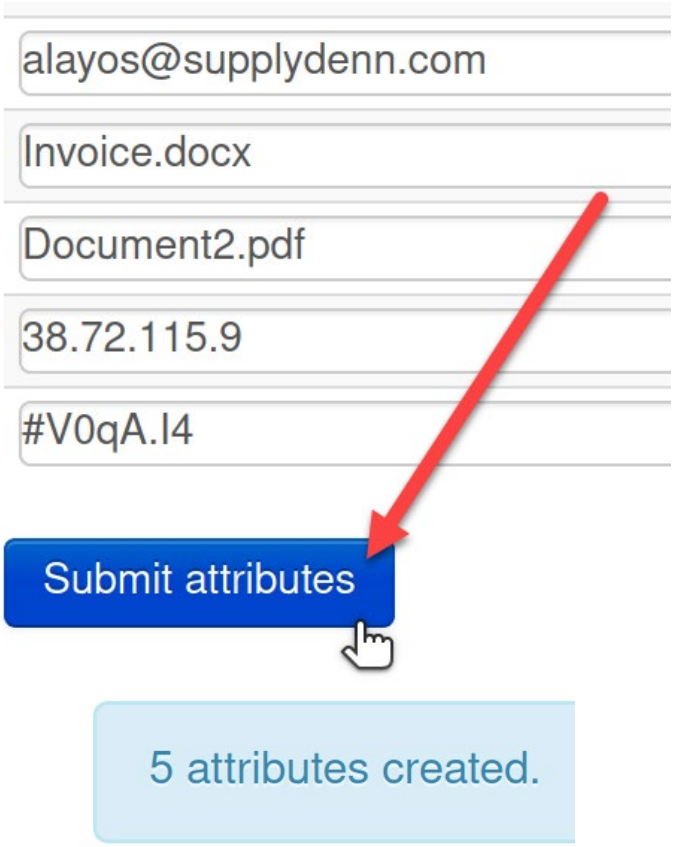


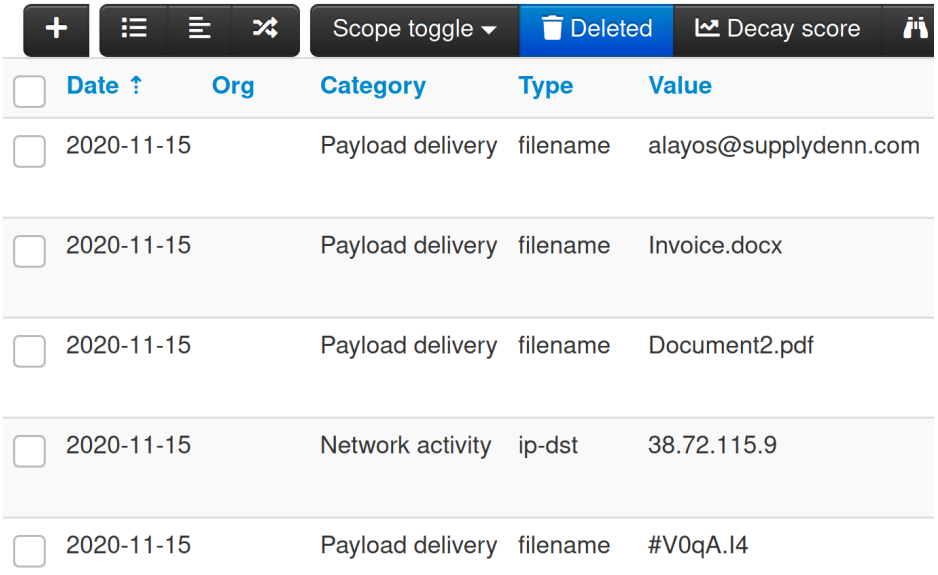
© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets

Technet24

No worries! Go ahead and click "Submit attributes". You should see the "5 attributes created" at the top, and then the created attributes farther below.



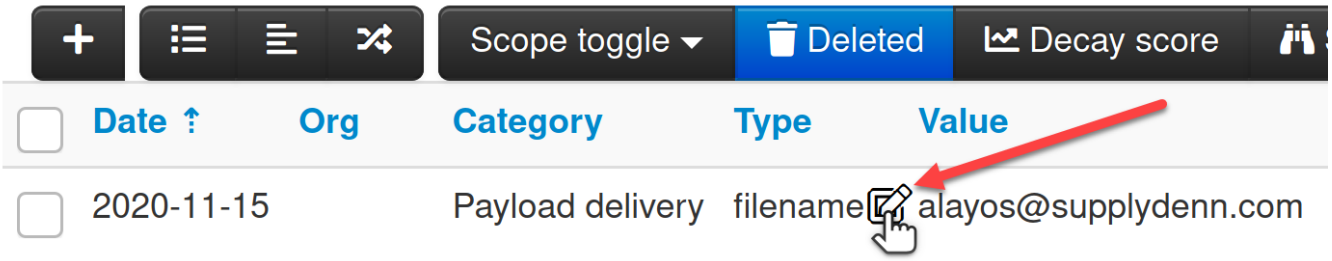


Date	Org	Category	Type	Value
2020-11-15		Payload delivery	filename	alayos@supplydenn.com
2020-11-15		Payload delivery	filename	Invoice.docx
2020-11-15		Payload delivery	filename	Document2.pdf
2020-11-15		Network activity	ip-dst	38.72.115.9
2020-11-15		Payload delivery	filename	#V0qA.I4

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets

From this view, we can adjust the email address to the correct Type (email-src) by clicking the edit, selecting "email-src" from the dropdown, and clicking the check mark to accept the edit, just like we did before.



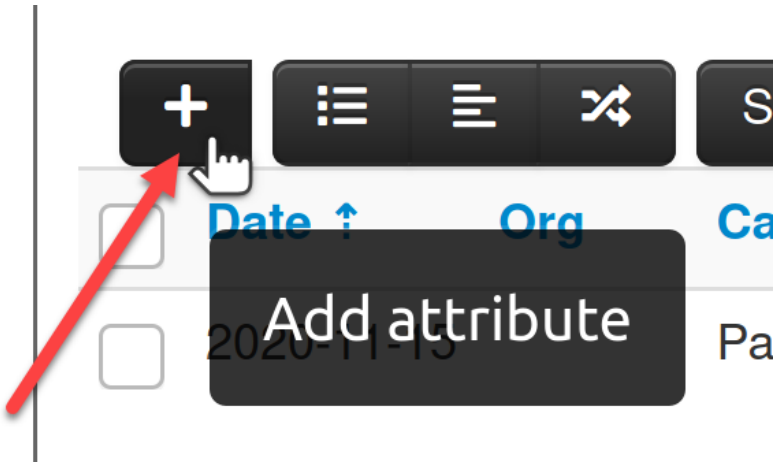
Once you fix it, your indicator should now look like this.

Payload delivery email-src alayos@supplydenn.com

We also need to update the mutex type since MISP did not correctly ingest that. Change the Category to "Artifacts dropped" and the Type to "mutex" (per your style guide) as you did before. Once you fix it, your new indicator should now look like this.

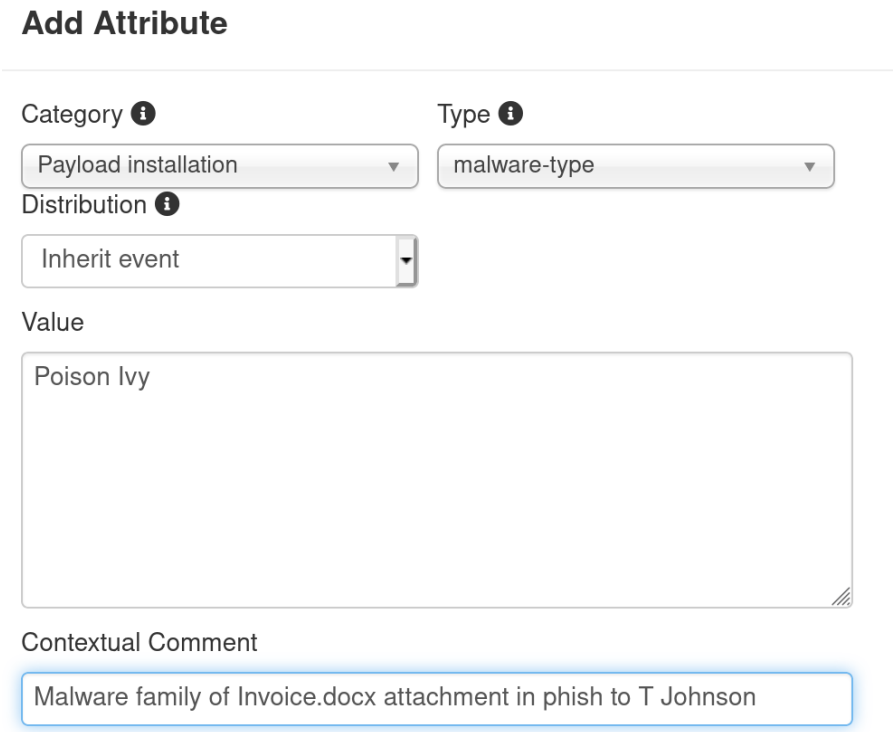
Artifacts dropped mutex #V0qA.I4

The last thing we need to do is manually add our "Poison Ivy" indicator since the freetext import tool didn't recognize that. Click the "+" icon in the attributes menu to add a new attribute.



© 2021 Robert M. Lee and SANS Institute
https://t.me/learningnets
Technet24

We'll be sure to follow our style guide (Category of "Payload installation" and Type of "malware-type") as well as add a comment for context.



Click "Submit", and you'll observe this attribute added to the event.

Category	Type	Value	Tags	Galaxies	Comment
Payload installation	malware-type	Poison Ivy			Malware family of Invoice.docx attachment in phish to T Johnson

We've now successfully added all the indicator data from our spreadsheet to MISP.

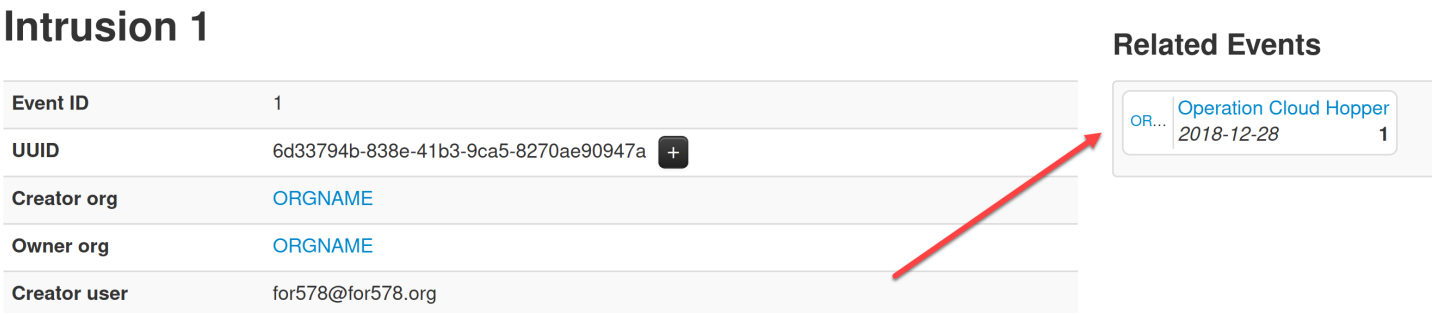
© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets

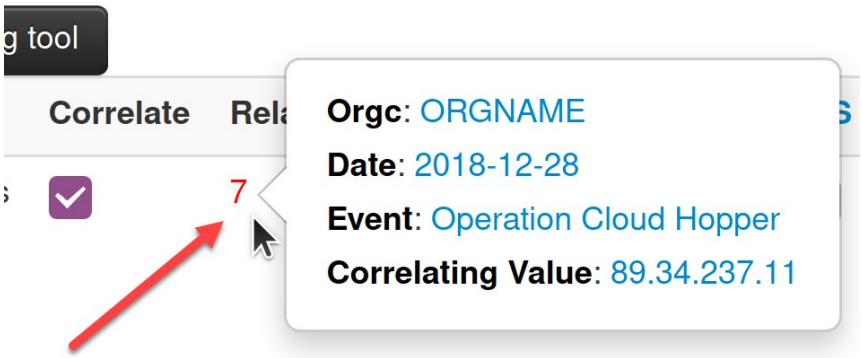
3. *For each intrusion event, look at Related Events and the Correlation Graph. Do any of our intrusions match previous data from external reports?*

- **Yes, Intrusions 1, 3, 4, and 6 all have indicators that correlate with previous events.**

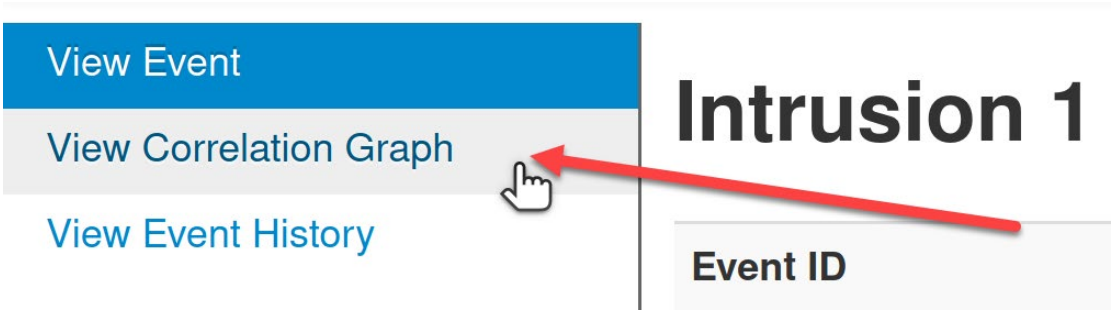
Now that our data is entered, we want to see if any indicators in our Intrusion events match previous indicators in MISP. Go to "Event Actions" > "List Events" and open Intrusion 1 as you did before. At each Intrusion event, we can see in the upper right if there are any "Related Events". We observe that Intrusion 1 matches the Related Event "Operation Cloud Hopper".



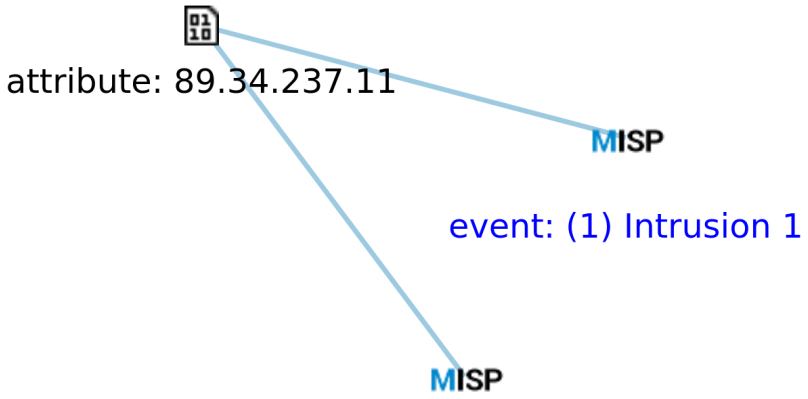
If we scroll down to the Attributes section, we can see that MISP tells us the attribute that matches the other event. Hover over the event ID in the "Related Events" column to observe the value that matches. In this event, we observe that the "Correlating Value" between the events is IP address 89.34.237.11.



We can also visualize this correlation using the "Correlation Graph". In the left menu from an event, click "View Correlation Graph", which allows us to visualize the correlation between the two events.



© 2021 Robert M. Lee and SANS Institute
https://t.me/learningnets
Technet24



After you look at Intrusion 1, proceed to look for correlations between the other Intrusion events we entered and previous data in MISP in the same manner as above. You should identify the following correlations:

- **Intrusion 1 correlates to "Operation Cloud Hopper" based on IP 89.34.237.11**
- **Intrusion 3 correlates to both "Cobalt Strike Beacon Tweet" and "Targeted ransomware: GoGaLocker and MegaCortex" based on IP 89.105.198.28**
- **Intrusion 4 correlates to "Operation Cloud Hopper" based on IP 104.224.166.148**
- **Intrusion 6 correlates to "Operation Cloud Hopper" based on IP 38.72.115.9**

4. *What do these overlaps tell us (or not tell us)? What hypotheses can we form about why we observe these overlaps?*

- **These overlaps simply tell us that the same indicators have been observed in our intrusions as in previous reporting. We need to be cautious and should not jump to conclusions that Intrusions 1, 4, and 6 "were definitely Operation Cloud Hopper" and Intrusion 3 "was definitely GoGaLocker or MegaCortex". Rather, these are overlaps that give us another piece of evidence and something we should look into further. There could be many hypotheses about why we identified these overlaps, including that different adversaries are using the same infrastructure – which commonly happens, especially in "ransomware as a service" intrusions. For Intrusion 3, a reasonable hypothesis was that our intrusion may have involved Cobalt Strike and the IP 89.105.198.28 is a C2 server that has been reused by multiple ransomware operators. These hypotheses give us points to conduct further investigation, gather additional evidence, and potentially evaluate competing hypotheses.**

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets

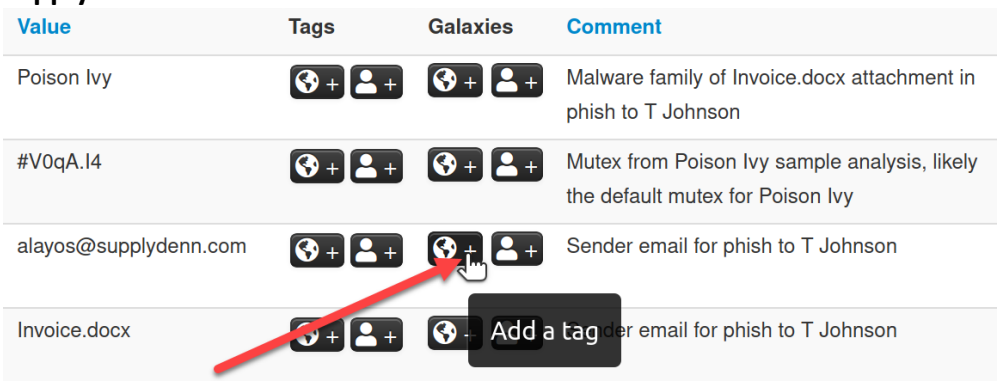
Part 2: ATT&CK Techniques

5. *Your SOC analysts have already added the ATT&CK techniques from the **Combined Intrusion Data** spreadsheet to Intrusions 1, 2, 3, and 4. Add the appropriate ATT&CK techniques from the **Combined Intrusion Data** spreadsheet to the Intrusion 6 event in MISP by adding the appropriate MITRE ATT&CK galaxy tag to each attribute.*

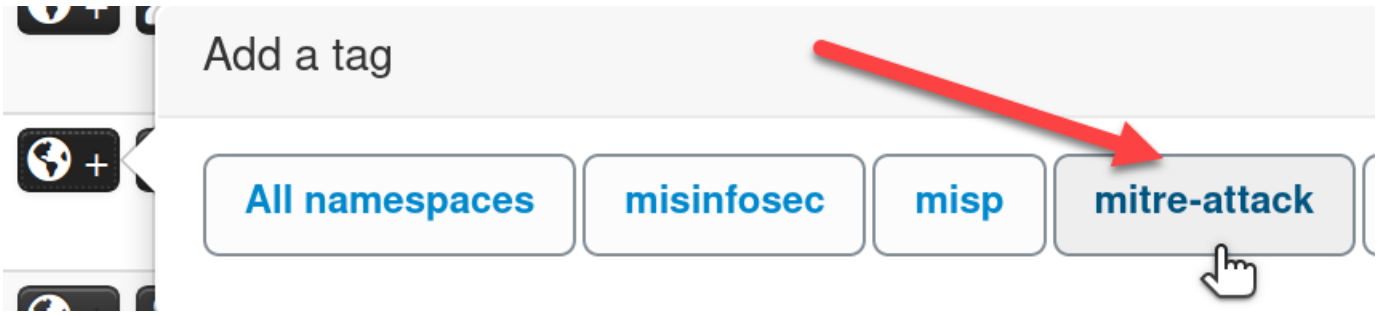
To add ATT&CK techniques to each of our events, we will use the MISP galaxy tag feature. We can relate ATT&CK techniques at the event or attribute level, but we want to relate them at the attribute level to give the most context possible. Referencing our Combined Intrusion Data spreadsheet, we observe that we only have two techniques to add for Intrusion 6: T1566.001 Spearphishing Attachment and T1204.002 Malicious File. It's important to remember that not every indicator or data point will have an ATT&CK technique, and that's okay.

Intrusion 6	alayos(at)supplydenn.com	Sender email for phish to T Johnson	Initial Access	T1566.001 Spearphishing Attachment
Intrusion 6	Invoice.docx	Attachment for phish to T Johnson	Execution	T1204.002 Malicious File
Intrusion 6	Poison Ivy	Malware family of Invoice.docx attachment in phish to T Johnson	N/A	N/A
Intrusion 6	Document2.pdf	File dropped by Invoice.docx attachment in phish to T Johnson	N/A	N/A
Intrusion 6	38.72.115.9	Config data from Invoice.docx attachment in phish to T Johnson	N/A	Intelligence gap, not sure what protocol this IP uses
Intrusion 6	)#V0qA.I4	Mutex from Poison Ivy sample analysis, likely the default mutex for Poison Ivy	N/A	N/A

We start by opening the event for Intrusion 6 and navigating to the attributes section. Under the "Galaxies" column, click the "+" icon next to the globe icon to add a galaxy tag to the "alayos@supplydenn.com" attribute.

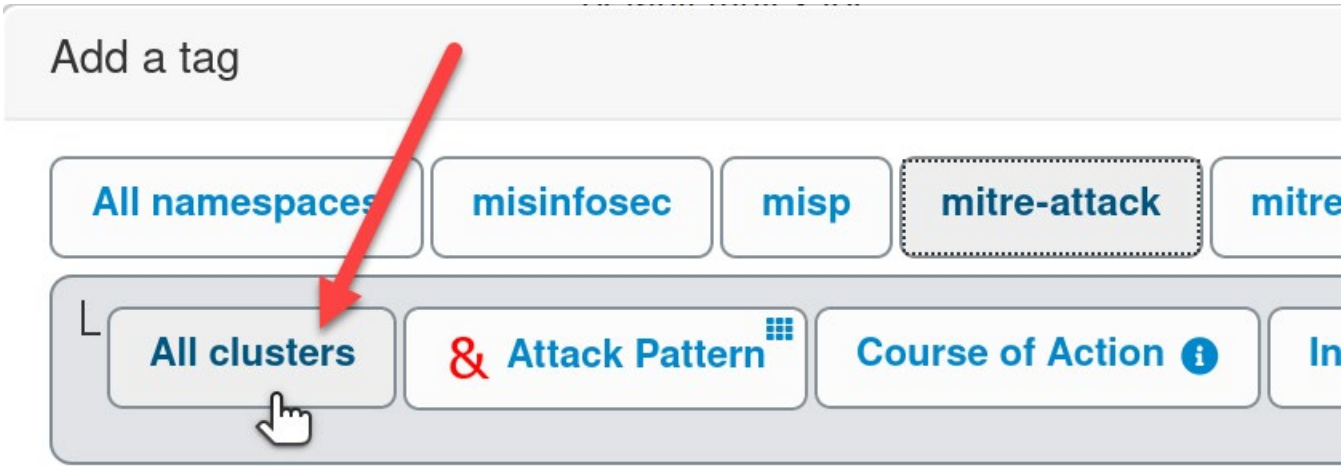


Click on the "mitre-attack" Galaxy button.

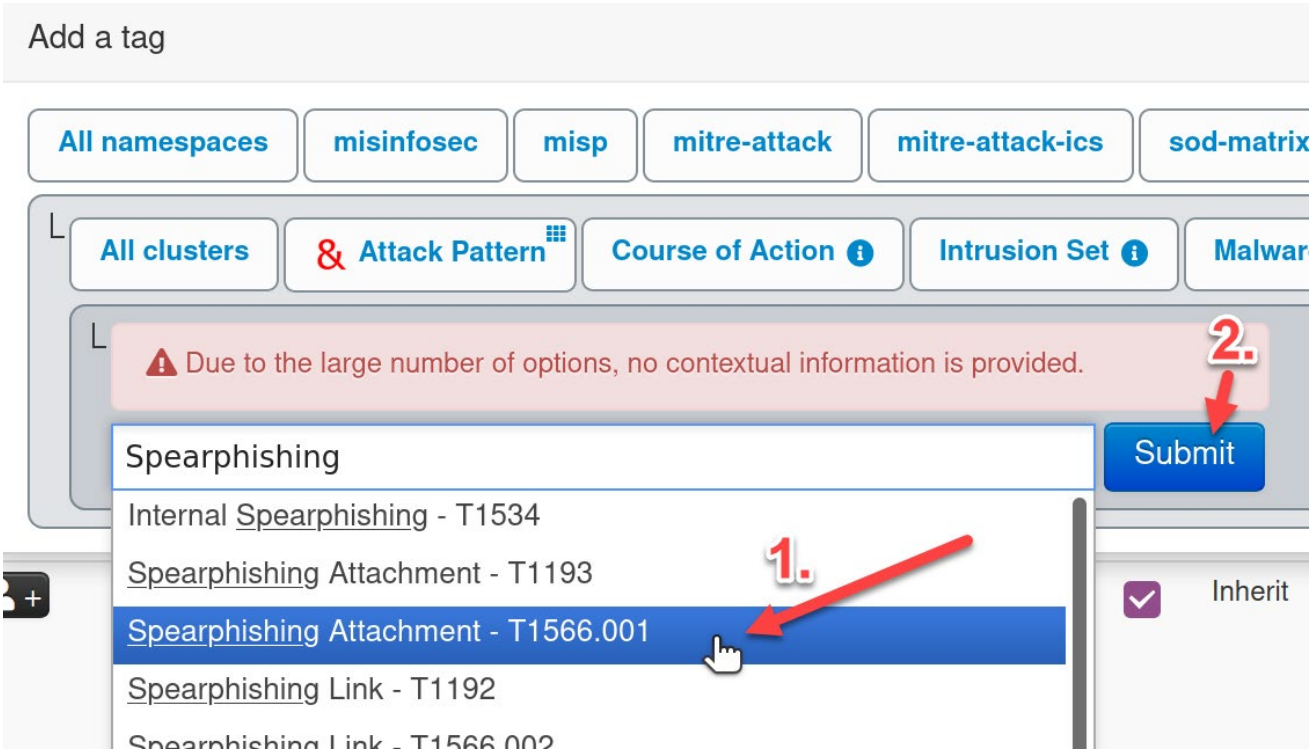


© 2021 Robert M. Lee and SANS Institute
https://t.me/learningnets
Technet24

Then click on "All clusters", which lets us search through all available clusters in the "mitre-attack" namespace.



Begin typing your sub-technique name, "Spearphishing…" into the field and observe that MISP will begin searching for the appropriate sub-technique. Click the correct sub-technique from the list, T1566.001, and then click "Submit."



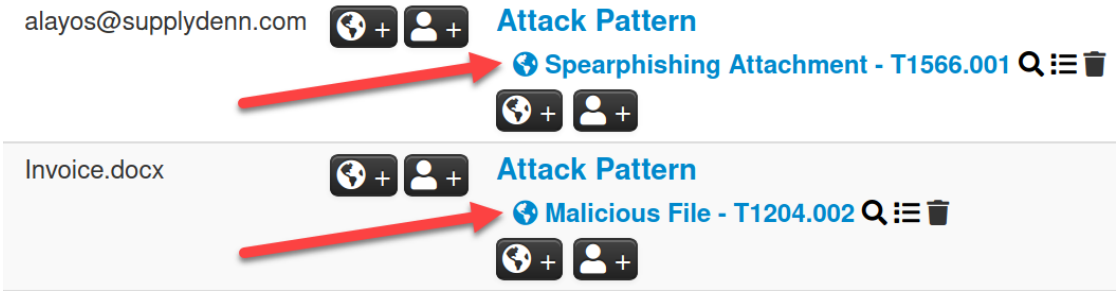
You will now see the "Spearphishing Attachment" sub-technique added to your "Galaxies" column as a tag on the attribute for "alayos@supplydenn.com".

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets



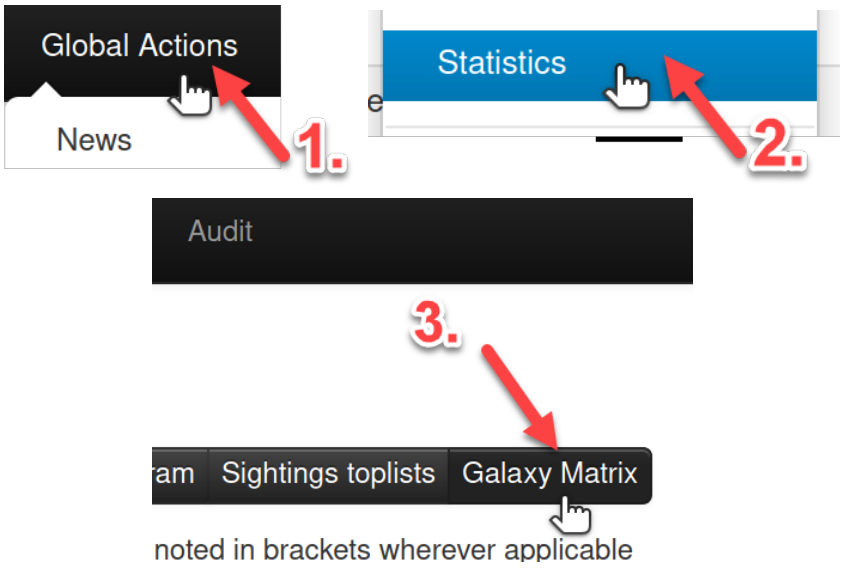
You have added the first technique to Intrusion 6. Now, add the second technique, T1204.002 Malicious File, to the "Invoice.docx" attribute in the same way you did above. When complete, your two attributes with ATT&CK techniques added should look like the one below.



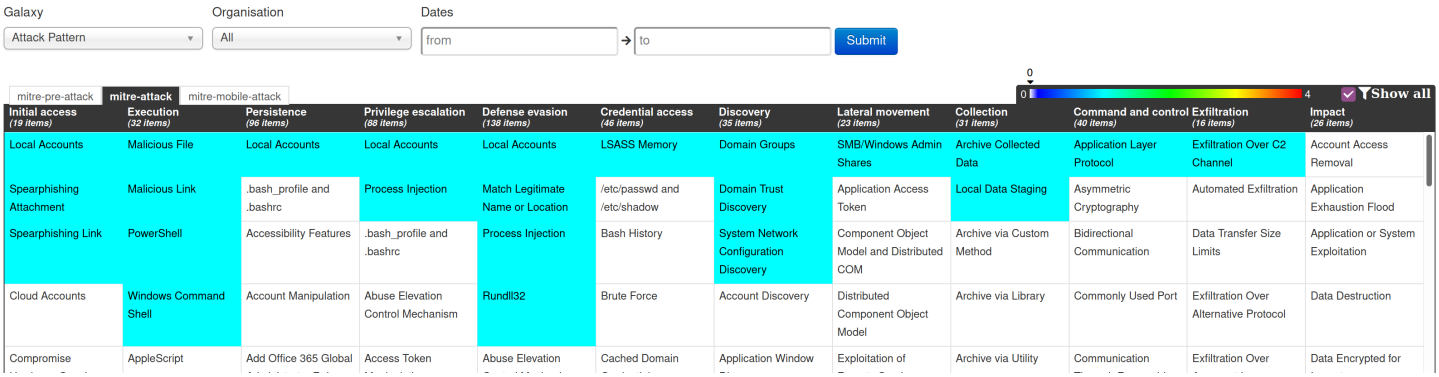
6. *Based on the techniques you have added, what is the most prevalent technique you have observed in your dataset for these intrusions? Use the Statistics feature in MISP to help you.*

- **<u>T1595 Active Scanning (ATT&CK v8) or T1254 Conduct active scanning (ATT&CK v7)</u>**

In MISP, we can observe a heat map of all of the ATT&CK techniques we have added to MISP events and attributes. To access this heat map, navigate to "Global Actions" > "Statistics" > "Galaxy Matrix".



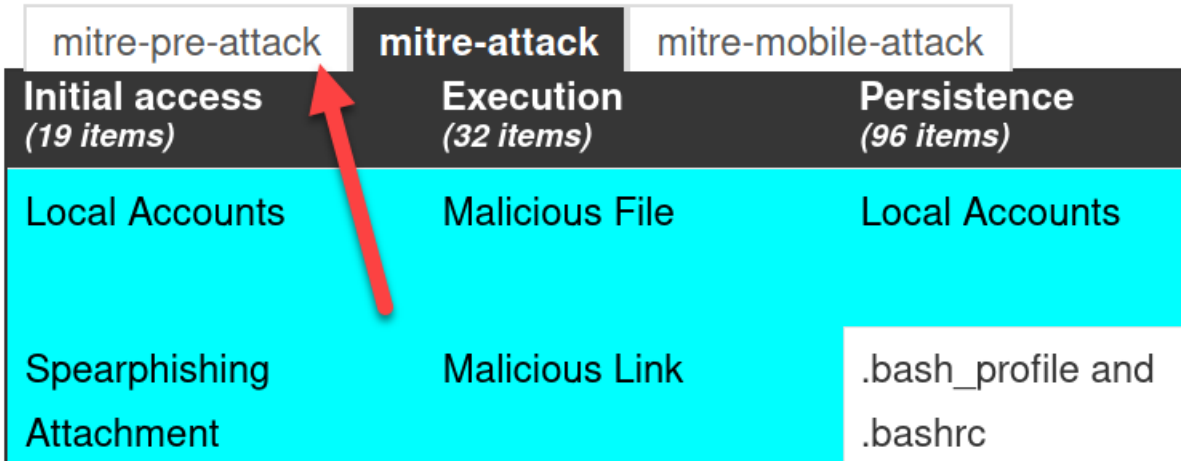
© 2021 Robert M. Lee and SANS Institute
https://t.me/learningnets
Technet24



Observe that MISP automatically assigns colors to cells based on the number of times the technique is present in MISP events and attributes. 0 is blue (low value) and 4 is red (high value).



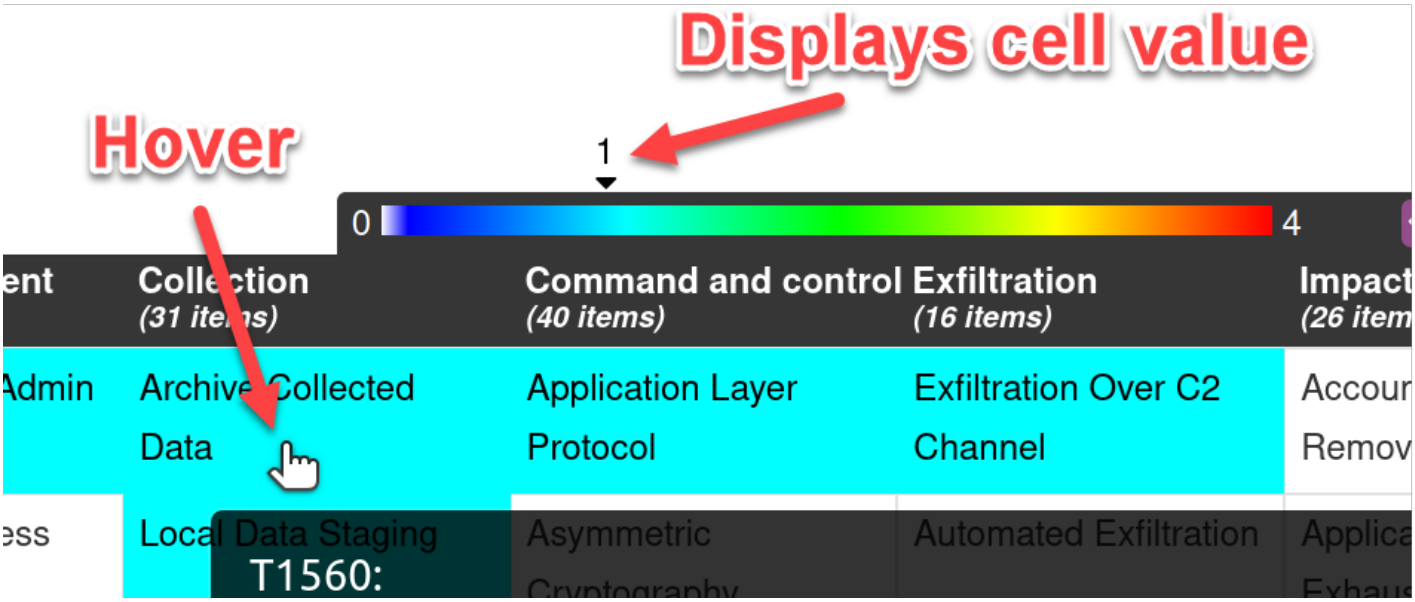
We observe something else important: We see that the version of ATT&CK in MISP has "mitre-pre-attack", so it appears MISP is using version 7 of MITRE ATT&CK (https://attack.mitre.org/versions/v7/) rather than a more recent version. This is one of the limitations of open-source software: Sometimes, it may not have the most up-to-date version of frameworks. This tells us we need to look at both the "mitre-pre-attack" and "mitre-attack" matrices.



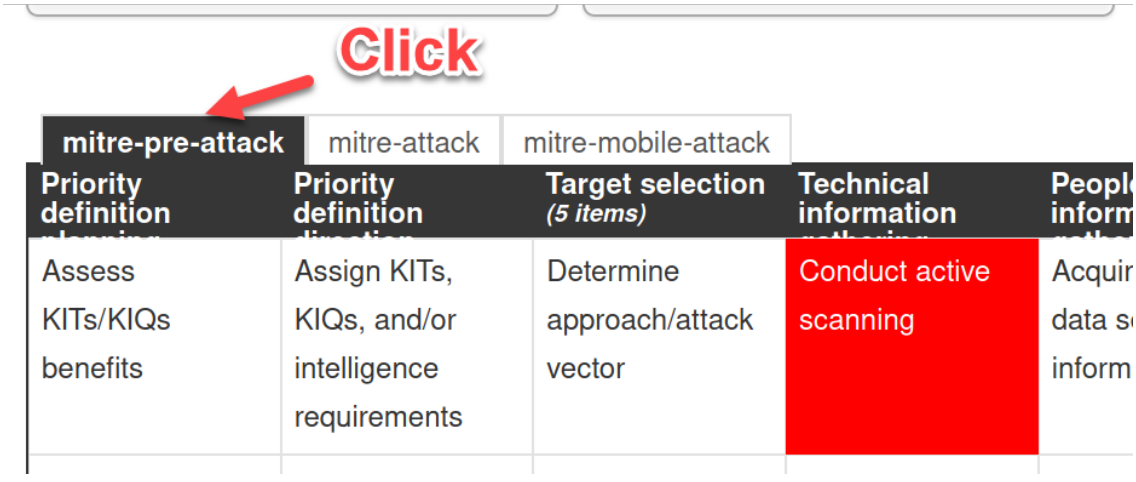
© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets

From viewing the "mitre-attack" matrix, we observe that all our techniques are the same color and value. As we hover over each technique, the gradient key displays the cell value, meaning that each of the techniques in the "mitre-attack" matrix have only one appearance in our instance of MISP.



However, we know from the gradient key that the highest value in our dataset is 4, so we also need to remember to view the "mitre-pre-attack" matrix. When we click on that matrix, we observe that the highest value of 4, shown in red, is the technique "Conduct active scanning." If we go to version 8 of MITRE ATT&CK version at https://attack.mitre.org/versions/v8/, we can observe that there is a newer, similar technique called T1595 Active Scanning. Because ATT&CK changes frequently, dealing with those changes needs to be part of our workflow as analysts as we work with the framework. Both techniques are similar, so we could record either one as the most prevalent technique in our dataset.



© 2021 Robert M. Lee and SANS Institute
https://t.me/learningnets
Technet24

7. *Why is this technique prevalence information relevant? What recommendations could you make to your defenders based on it?*

   - **It is relevant for us to know that T1595 Active Scanning (or T1254 Conduct active scanning) is the most common technique observed in our intrusions because it allows us to prioritize which techniques to focus on based on our own internal data. Our team was previously overwhelmed with which techniques to focus on in MITRE ATT&CK, and we can now recommend they focus on Active Scanning since we have observed that technique in four intrusions. We could make various recommendations to defenders based on this technique, including those from the MITRE page (below, https://attack.mitre.org/versions/v8/techniques/T1595/) such as analyzing referrers or user-agent strings. This is just one example—we make other recommendations to our defenders, too.**

> ## Detection
>
> Monitor for suspicious network traffic that could be indicative of scanning, such as large quantities originating from a single source (especially if the source is known to be associated with an adversary/botnet). Analyzing web metadata may also reveal artifacts that can be attributed to potentially malicious activity, such as referer or user-agent string HTTP/S fields.
>
> Much of this activity may have a very high occurrence and associated false positive rate, as well as potentially taking place outside the visibility of the target organization, making detection difficult for defenders.
>
> Detection efforts may be focused on related stages of the adversary lifecycle, such as during Initial Access.

BONUS: You don't need to do this as part of this exercise, but if you wanted to, you could write up a report about any or all of these intrusions; we can use the MISP Markdown feature. You can read more about this feature here: https://www.misp-project.org/2020/10/08/Event-Reports.html.

Exercise: Key Takeaways

- **We took advantage of both automated and manual data ingest features to ingest data into MISP. We observed that MISP can automate some data ingest, but we must validate and sometimes manually edit that data.**
- **We used MISP's correlation features to identify correlations to other data, but assessed these correlations may not mean the same malware or groups are behind our intrusions.**
- **We used MISP's galaxy features to visualize common ATT&CK techniques across our intrusions and make defender recommendations. We learned that when we use ATT&CK, we need to keep in mind that it is frequently updated.**

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets

This page intentionally left blank.

https://t.me/learningnets

Technet24

Exercise 4.2: Identifying Cognitive Biases

Objectives

- Identify multiple cognitive biases and logical fallacies in a news report

Scenario: *The combination of any technical field that folks misunderstand, as well as a concept such as cyber threat intelligence, generates a number of opportunities to identify cognitive biases. Industrial control systems (ICSs) present a perfect pairing with CTI for such mistakes to be made. In this exercise, you will look at a report that was put out by a media organization that made claims related to CTI and ICS.*

Exercise Preparation

In the **Ex 4.2** folder, you will find a PDF titled "A Decoy Computer Was Set Up Online." Read it in its entirety and identify at least two cognitive biases or logical fallacies. You may track these however you wish; highlighting and commenting directly in the PDF is one approach.

If you finish early, feel free to read the rebuttal articles (part 1 and part 2) published by CSO, which includes comments from the vendor.

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets

Exercise: Task

1. Identify at least two cognitive biases or logical fallacies. You may use biases and fallacies discussed in class or others that you know about.

- _____
- _____

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets

Technet24

Exercise: With a Sample Approach

1. Identify at least two cognitive biases or logical fallacies. You may use biases and fallacies discussed in class or others that you know about.

- **Anchoring**

- **Anecdotal Fallacy**

There are multiple examples of logical fallacies and cognitive biases in this article. The reason this article was chosen is that it is a very public view of what many are told about cyber threat intelligence. It also presents a technical concept that many are unfamiliar with, creating a scenario that is believable based on lack of understanding of two topics.

At the beginning of the report, the reporter states that he set out with the idea of showing the global nature of attacks against ICSs. This is the beginning indication of an Anchoring bias because the individual set out to prove something he thought to be a fact instead of asking a question and seeing if the data supported it. As an example, the reporter could have asked, "Are there global attacks against ICSs? Are they detectable, and how might we show that?" Because he did not approach the situation with an open mind, though, Congruence Bias is also a good choice because the reporter failed to consider other hypotheses and selectively sought to support the hypothesis he came up with.

It will also be appropriate to identify a Burden of Proof fallacy, albeit indirectly. The reporter made claims regarding ICS networks being under "daily assault by hackers, and that threat is only growing as more countries develop advanced cyber-war capabilities," yet offers no proof of this statement. Therefore, this leaves the reader in a position to have to prove the reporter incorrect.

Most significantly, the reporter and vendor prioritized data collected from their honeypots instead of the significant amount of data regarding ICS threats in the community. Looking at the data in the community would have revealed that there are very low numbers of "attacks" reported. The ICS-CERT generally reports around 200 incidents a year, and there are to date only a handful of incidents that qualify as an "attack." Yet, because the data was collected by them, the reporter prioritized this data as the most relevant and felt comfortable claiming 6,000 attacks from the U.S., followed by 3,500 from China, and 2,500 from Russia. This is a good example of the Anecdotal Fallacy. Without other data presented and with a priority placed on the data that was personally relevant and experienced by the individuals, they did not accurately look at the wider evidence available.

The reporter makes additional statements without any proof, which opens up an opportunity for you to research additional biases and fallacies not yet discussed in the class. For example, the vendor states that "the data largely reflect reconnaissance missions, in which hackers often use less obfuscation." This statement is based on assumptions and a lack of visibility into all the available data. Likewise, the reporter states, "More than anything, the experiment shows that the U.S. is the conduit for a lot of the world's attack traffic…"

Use your internet connection to research cognitive biases or logical fallacies that might represent these statements or others in the report.

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets

Exercise: Key Takeaways

- **Identifying cognitive biases and logical fallacies in reports by others is a good way to learn to recognize these. Ultimately, we want to recognize these biases and fallacies in our teams and ourselves to ensure we do not produce flawed intelligence analysis.**

- **Cognitive biases and logical fallacies are common in our everyday life, including in news reports. Learning to identify them not only makes us better intelligence analysts, but savvier consumers of news and information as well.**

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets
Technet24

Exercise 4.3: Analysis of Competing Hypotheses

Objectives

- Gain experience with the Analysis of the Competing Hypotheses (ACH) structured analytic technique
- Provide an assessment to leadership based on performing ACH

Scenario: *The Edison International CTI team is asked to review the conclusion of the Incident Response team from the Money Bin ransomware case.*

The relevant conclusion that the executives are concerned about is that the adversary was using the ransomware as a diversion and exfiltrated key account information from the bank of high net worth individuals. The exfiltration was confirmed, but if this were a diversion effort, it could impact how the bank communicates about the attack. Moreover, it will impact what they tell federal authorities and peers in the community, as well as influence their own preparation and re-analysis of existing ransomware cases to look for exfiltration.

Exercise Preparation

The walkthrough is only one example; there are many ways to do this exercise. The questions below are one way to record as you work through this exercise, but you may find it useful to use a separate spreadsheet or another method of recording notes. This exercise is designed to use the information below along with information from Exercise 3.4 on TrickBot and Ryuk. For students new to the ACH technique, scoping the exercise to this information may be helpful. However, you may bring in open-source information or other information you assess to be related.

What we know:

Money Bin was compromised with ransomware. We previously identified the 85.25.3.13 IP address as a C2 server. The incident responders were then able to find a sample of TrickBot on an Enterprise system after we informed them of our analysis of the IP address (from Exercise 3.4 when we searched Recorded Future). They did not have the data to show any human-operated movement inside the network such as lateral movement; the systems that housed that information were unrecoverable. However, based on the discovery of TrickBot and the proliferation of some ransomware family across the network, they correlated the two events together and deemed that the ransomware variant was “definitely” Ryuk.

In the process of investigating the incident through log and network flow analysis, the incident responders noticed large volumes of data leaving the network roughly 18 hours ahead of the ransomware outbreak but 10 hours after TrickBot was first seen in the network. They could not find any other indicators or observables to show that there were other intrusions.

However, the IP address that the exfiltration was going to was registered to a Brazilian IP address and there were numerous domains associated with that IP, including domains involving the persona “Robin” and various characters from “Robin Hood.” Analysis of the exfiltration included archived files of account information from high net worth individuals at the bank.

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets

Exercise: Questions

1. **The first step in the ACH process is to formulate hypotheses to meet the requirement levied.**

H1._____

H2._____

H3._____

H4._____

2. **Make a list of significant evidence and arguments for and against each hypothesis.**

The next step in the ACH process is to identify all the evidence supporting or refuting the hypotheses we've identified.

E1._____

E2._____

E3._____

E4._____

E5._____

E6._____

E7._____

E8._____

3. **Map the evidence to the hypotheses.**

	H1	H2	H3	H4
E1				
E2				
E3				
E4				
E5				
E6				
E7				
E8				

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets

Technet24

4. Refine the matrix.

At this point, it should be clear which evidence is not of diagnostic value (meaning the diagnostic is the same for all hypotheses, such as all pluses, minuses, or zero; this indicates the evidence does not help us prioritize one hypothesis over another).

- Identify the pieces of evidence that are not of diagnostic value:

_____

5. Prioritize the hypotheses.

Perform the hypothesis comparison. Prioritize the hypotheses, with those having the most refuting evidence at the bottom and building up to those with the least refuting evidence at the top. Consider this the vertical comparison, whereas Step 3 was the horizontal comparison.

- Prioritize the hypotheses
- Try to *disprove* each hypothesis now (by looking at refuting evidence) instead of proving it

Highest priority

_____

_____

Lowest priority

_____

_____

6. Evidentiary dependence.

Are there any pieces of evidence on which your assessment of the highest-likelihood hypothesis heavily depends? Are there only one or two pieces of evidence that, if omitted, would change your assessment?

- Identify the one or two most critical pieces of evidence to your assessment. Note their confidence, volatility, or underlying assumptions.

_____

_____

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets

7. Report conclusions.

You're ready to provide your finalized assessment. Write one paragraph describing your conclusion, capturing all the necessary elements to properly qualify your report (including estimative language and evidentiary dependency, as well as intelligence gaps) and make it complete (including alternative hypotheses and any rejected evidence of note).

- Provide your final report.

8. Identify milestones.

There are plenty of ways the situation could change, especially in the case of this report that would affect your conclusion.

- Identify at least one milestone that would impact your assessment and in what way.

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets

Technet24

Exercise: Questions with Walkthrough

This walkthrough provides one way of working through an ACH for this requirement. There are many ways to approach this analysis, and this should not be considered the "right" answer.

1. **The first step in the ACH process is to formulate hypotheses to meet the requirement levied.**

   H1. The ransomware was a diversion.

   H2. There were two separate intrusions and the ransomware was not a diversion.

   H3. There was no intrusion; it was a false positive.

   H4. The second intrusion was an insider.

   At this point, we do not want to throw out hypotheses; we try to come up with different hypotheses instead of thinking about their likelihood. You may have a different number of hypotheses than this walkthrough; this is perfectly fine, as different analysts approach analysis differently.

2. **Make a list of significant evidence and arguments for and against each hypothesis.**
   The next step in the ACH process is to identify all the evidence supporting or refuting the hypotheses we've identified.

   E1. The exfiltration took place before the ransomware.

   E2. No other intrusions were found in the network.

   E3. TrickBot was found in close temporal proximity to the exfiltration.

   E4. An outside firm handled and confirmed the ransomware case.

   E5. There are no public cases of TrickBot/Ryuk being used as a diversion.

   E6. "Robin Hood" and similar theming share no overlaps with the TrickBot intrusion.

   E7. Ryuk operations often take place quickly; the delay left a window for exfiltration.

   E8. Money Bin is a financial organization.

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets

3. **Map the evidence to the hypotheses.**

	H1	H2	H3	H4
E1. The exfiltration took place before the ransomware.	+	-	-	-
E2. No other intrusions were found in the network.	+	-	+	+
E3. TrickBot was found in close temporal proximity to the exfiltration.	+	-	-	-
E4. An outside firm handled and confirmed the ransomware case.	0	0	-	0
E5. There are no public cases of TrickBot/Ryuk being used as a diversion.	-	+	0	0
E6. "Robin Hood" and similar theming share no overlaps with the TrickBot intrusion.	-	+	0	0
E7. Ryuk operations often take place quickly; the delay left a window for exfiltration.	+	-	0	0
E8. Money Bin is a financial organization.	0	0	0	0

Now we place a + where evidence supports the hypothesis, - where it takes away from the hypothesis, 0 where it does not impact it, and ++ or -- for particularly important evidence or more appropriately combinations of multiple pieces of smaller evidence types (like multiple indicators firing). There are many ways to approach ACH, and you could choose to use numbers instead (such as 1, -1, 0, 2, and -2). This is a particularly useful approach if you are using a spreadsheet since it allows you to add each column later on.

4. **Refine the matrix.**

   At this point, it should be clear which evidence is not of diagnostic value.

   - Identify the pieces of evidence that are not of diagnostic value:

     E8 is not diagnostic since it has no impact on any of our hypotheses.

5. **Prioritize the hypotheses.**

   Perform the hypothesis comparison. Prioritize the hypotheses, starting with those having the most refuting evidence at the bottom and building up to those with the least refuting evidence. Consider this the vertical comparison, whereas Step 3 was the horizontal comparison.

   - Prioritize the hypotheses
   - Try to *disprove* each hypothesis now instead of proving it **(Heuer designed this technique specifically to hedge against confirmation bias, when we include only evidence that *supports* our hypothesis)**.

     Now we structure the hypotheses against highest and lowest likelihood based on the diagnostics performed.

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets
Technet24

When we analyze the number of pieces of evidence that are refuting (-), supporting (+), or irrelevant (0), and rank the hypotheses with the least refuting evidence at the top, we may produce an analysis like the below. Since there is a tie in the number of refuting pieces of evidence between Hypothesis 1 and Hypothesis 4 (two pieces of evidence), we decide to look at our supporting evidence to prioritize Hypothesis 1 over Hypothesis 4, though different analysts may approach this differently. With 2 refuting pieces of evidence and 4 supporting, Hypothesis 1 is our highest priority. With 4 refuting pieces of evidence and 2 supporting, Hypothesis 2 is our lowest priority. It is important to remember, however, that this doesn't mean Hypothesis 1 is the "right answer"—the purpose of ACH is not to give us the "right answer," it is to get us to structure our thinking and hedge against biases.

Hypothesis Number	Number of refuting pieces of evidence (-)	Number of supporting pieces of evidence (+)	Number of irrelevant pieces of evidence (0)
H1	2	4	2
H4	2	1	5
H3	3	1	4
H2	4	2	2

Highest priority

H1

Lowest priority

H2

6. Evidentiary dependence.

Are there any pieces of evidence on which your assessment of the highest-likelihood hypothesis heavily depends? Are there only one or two pieces of evidence that, if omitted, would change your assessment?

- Identify the one or two most critical pieces of evidence to your assessment. Note their confidence, volatility, or underlying assumptions.

E1 and E3 are similar and very useful in this analysis.

E2 was the one piece of evidence that, if refuted, could massively change things.

7. Report conclusions.

You're ready to provide your finalized assessment. Write one paragraph describing your conclusion, capturing all the necessary elements to properly qualify your report (including estimative language and evidentiary dependency, as well as intelligence gaps) and make it complete (including alternative hypotheses and any rejected evidence of note).

- Provide your final report.

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets

The cyber threat intelligence team has no reason to refute the assessment of the incident response team. The CTI team assesses with low confidence that the ransomware operation was a diversion to hide the exfiltration of data related to high net worth individuals. This low confidence assessment is based in part on the limited time provided to complete the analysis. Key evidence in this assessment was that no other intrusions were found in the network, and if this evidence changed, the CTI team would need to reassess this conclusion. Alternative hypotheses include that there were two separate intrusions and the ransomware was not a diversion, that there was no intrusion and it was a false positive, and that there was a second intrusion that was an insider threat. In this assessment, the CTI team found that the information that Money Bin is a financial organization did not help us prioritize the most likely hypothesis. A key intelligence gap for this assessment is that the team did identify public cases of TrickBot/Ryuk being used as a diversion; identifying any cases of this would help us reach higher confidence in our assessment.

---

8. Identify milestones.

There are plenty of ways the situation could change, especially in the case of this report that would affect your conclusion.

- Identify at least one milestone that would impact your assessment and in what way.

If forensics show that there were multiple intrusions at the time of the exfiltration, it would potentially change the analysis.

Exercise: Key Takeaways

- **The Analysis of Competing Hypotheses structured analytic technique helps us hedge against confirmation bias and other types of bias by forcing us to compare evidence against multiple hypotheses. While it doesn't give us the "right answer," it helps us slow down and structure our analysis.**

- **By using ACH, we were able to support the previous conclusion of the Incident Response team. While we agreed with their conclusion, we now have the analysis to back up why we made the assessment, which is important since this decision has significant implications for our company.**

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets
Technet24

Exercise 4.4: Visual Analysis in Maltego

Objectives

- Use import functionality to ingest new entities and structured data into Maltego CaseFile for visual analysis
- Use visualization features such as layout controls, bubble charts, and link strength to identify specific data subsets

Scenario: You will be leveraging the same intrusion data from Exercise 3.1 where you created pivot tables in Excel to analyze the Poison Ivy samples identified during the intrusion at SpaderTech. This time, though, you will be using Maltego CaseFile to explore visual analysis in comparison. Analysts need to be familiar with different types of analysis skills and determine which works best for them.

Exercise Prep

Familiarize yourself with the "Poison Ivy Config Dumps.csv" document in the Ex 4.4 folder. This is the source data for this exercise. The adversary you have been recently tracking commonly uses the C2 IP 38.72.115.9. Use this information and Maltego to answer the following questions.

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets

Exercise: Questions

1. What entities do you need to create within Maltego CaseFile to handle the import data?

   - _____

2. What trends about this dataset are more apparent in a visual representation than they were in a spreadsheet view?

   - _____

3. Can you determine what the most frequently used port, mutex, and password are?

   - _____

4. Does the Poison Ivy sample we are interested in, the one configured with 38.72.115.9, have any commonly used values?

   - _____

5. What other network-based indicators would be useful for further analysis?

   - _____

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets

Technet24

Exercise: Questions with Step-by-Step

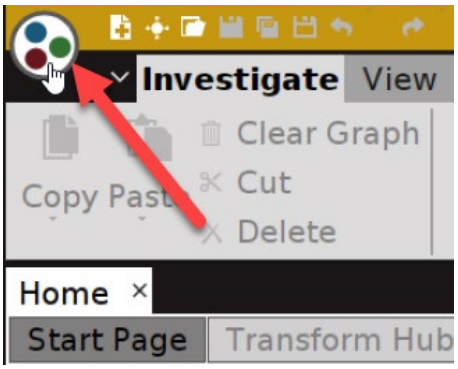
1. What entities do you need to create within Maltego CaseFile to handle the import data?

- **Hash, mutex, password, PIVY ID, port, C2node**

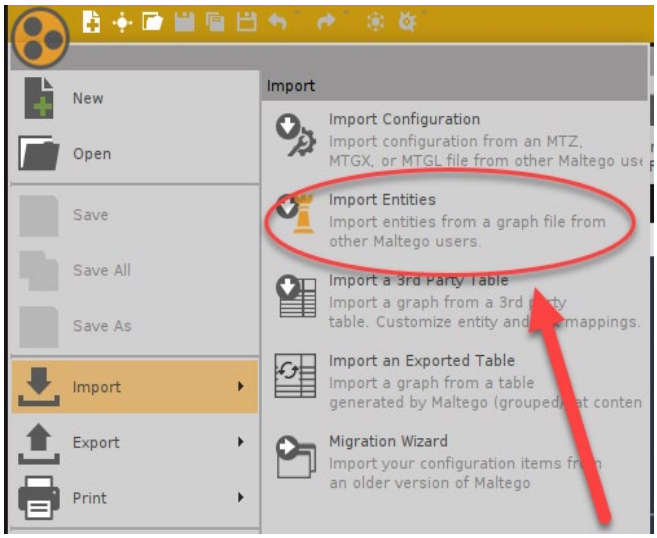
The configuration dump .csv contains information on Poison Ivy samples, as we know from working with this dataset in Exercise 3.1. For each sample, what is captured is a hash, mutex, password, poison ivy ID, port, and command-and-control node. There is additional information such as process injection information that has been captured for a few of the samples, but we will not include that in our analysis today.

In a previous exercise, we manually created entities, but we can also import entities that may be shared by others via a .mtz (Maltego archive) file. In order to import the entities, follow the steps below.

Select the Main Menu Icon.



Select Import and then Import Entities from the menu.

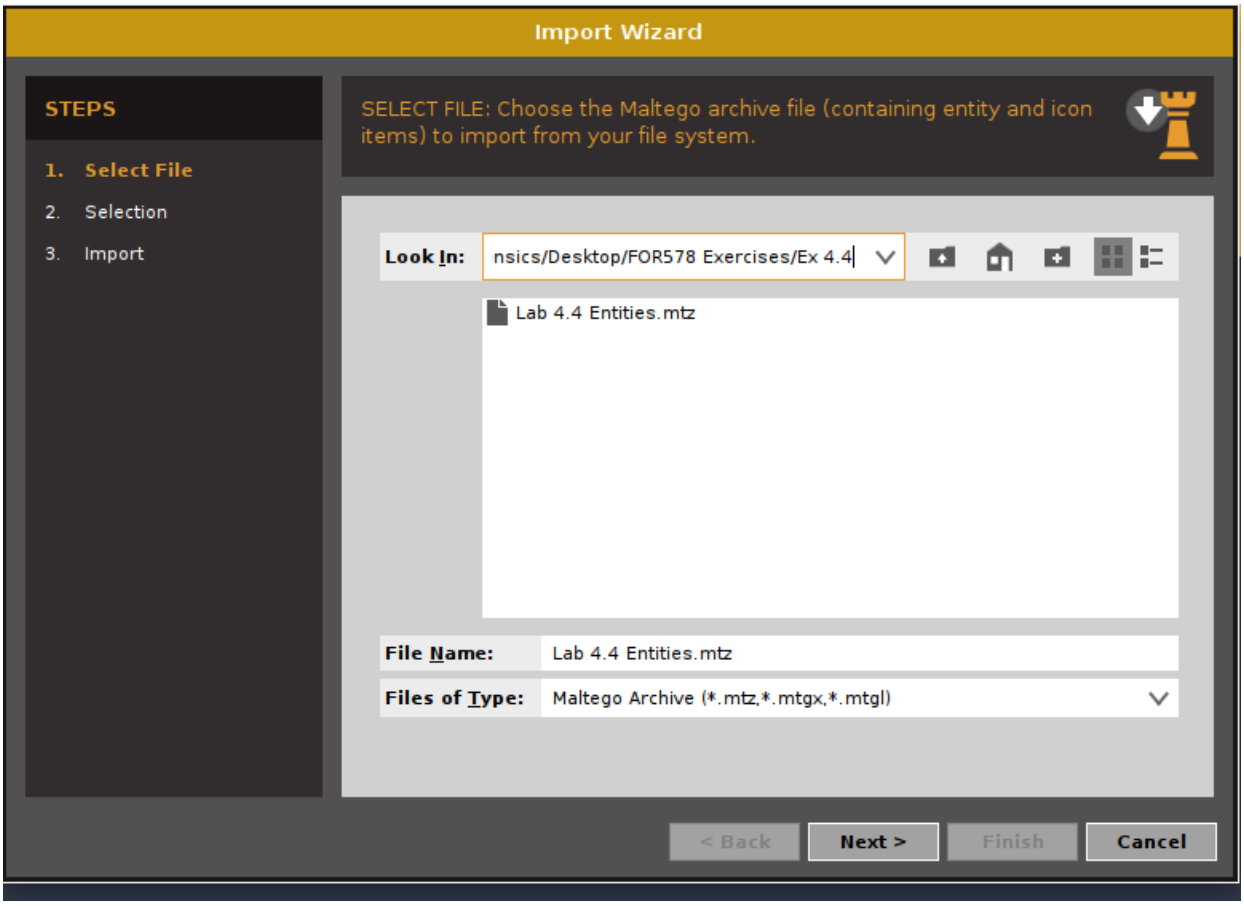


© 2021 Robert M. Lee and SANS Institute

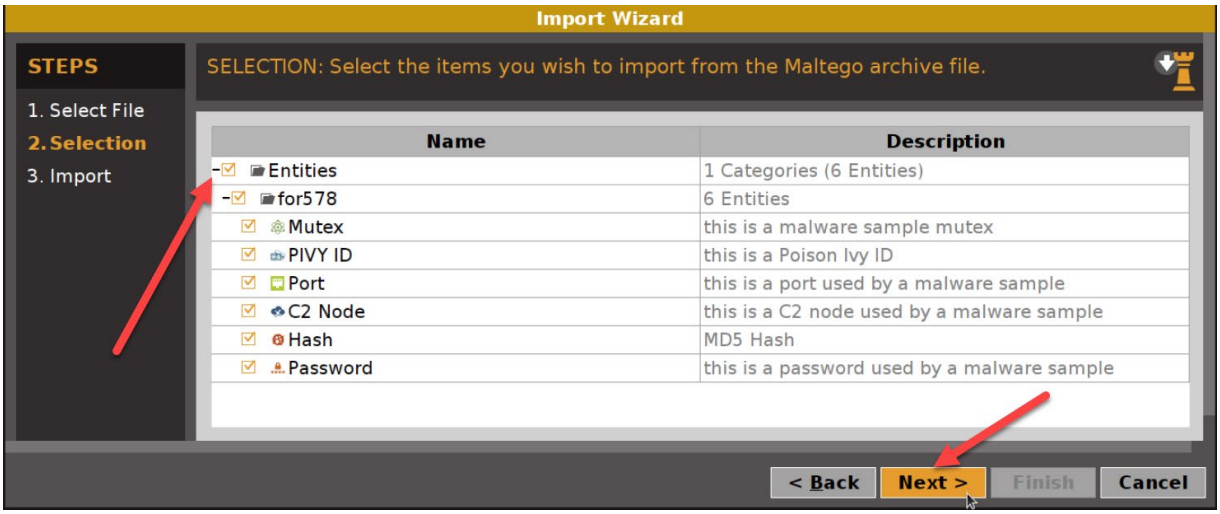
https://t.me/learningnets

The Import Wizard will ask for the .mtz file to upload. The specific location is /home/sansforensics/Desktop/FOR578 Exercises/Ex 4.4.

Select "Lab 4.4 Entities.mtz" and click Next.



In the next window, we can select the items you wish to import. All six entities should be selected by default. We can click the + icon to expand the entities to check and ensure these are the entities we need. Then, we will click Next.

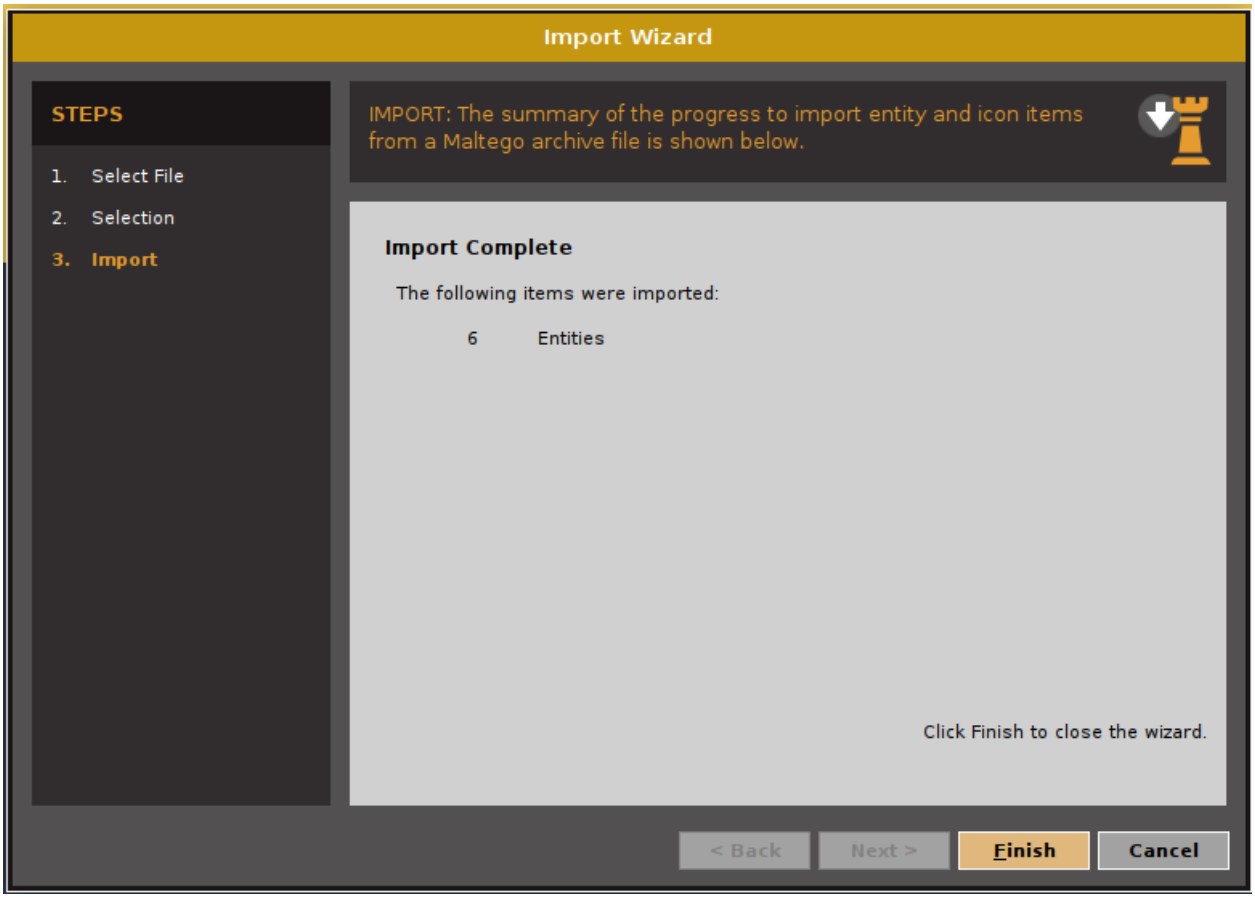


© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets

Technet24

The Import Wizard will finish the import and identify how many entities were added, which should be 6 Entities. Click Finish.



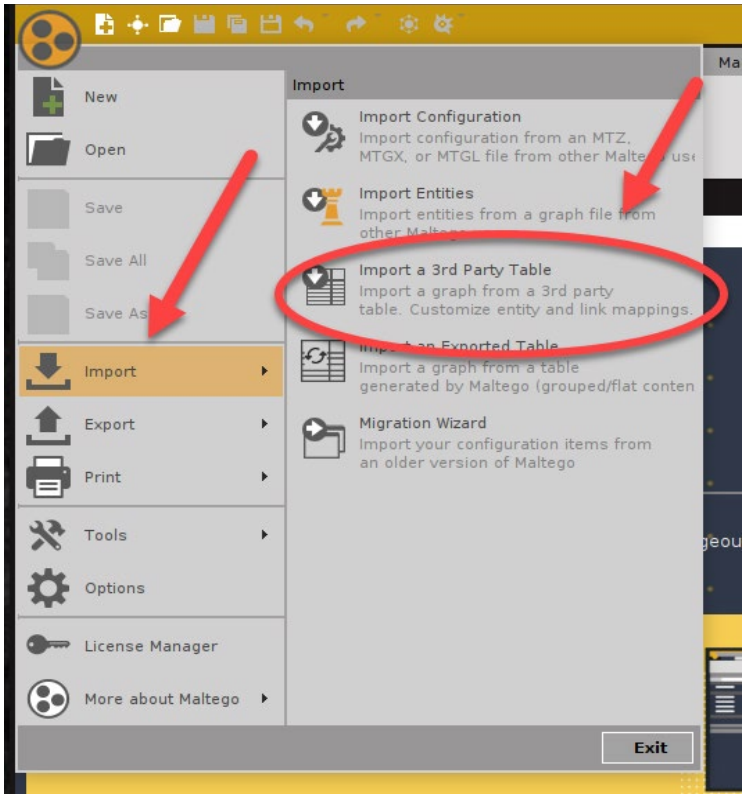
We have imported the six entities we identified in Question 1:

- **Hash**
- **Mutex**
- **Poison Ivy ID**
- **Password**
- **Port**
- **C2 Node**

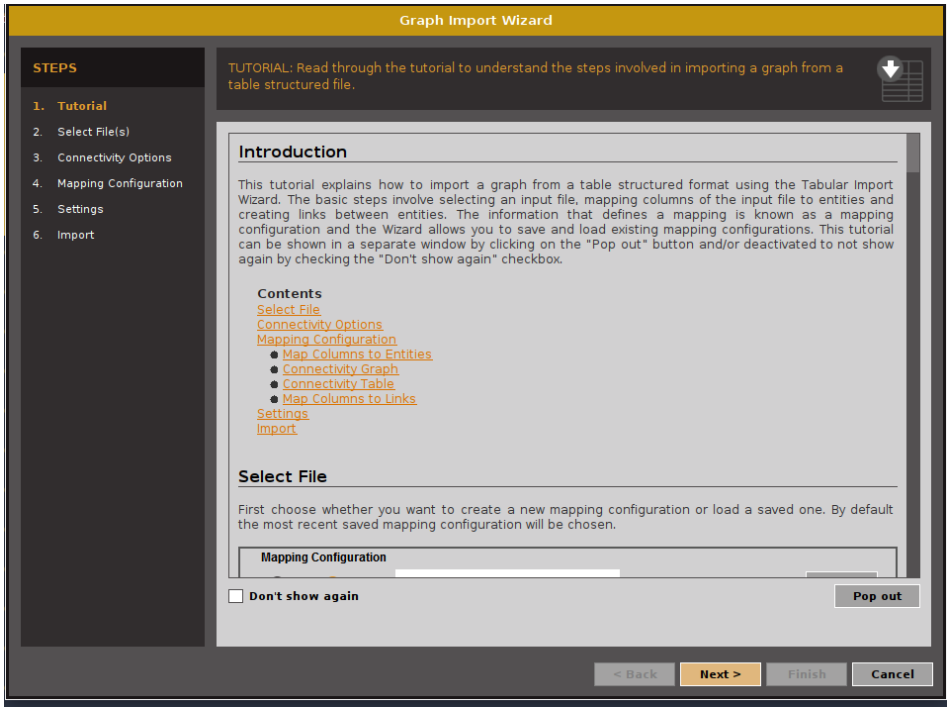
Once all of the entities are imported, next, import the data from our CSV file. To do that, click the large circle menu button at the top left, and then select Import -> Import a 3rd Party Table.

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets



The following pop-up dialog box displays. Select <u>Next</u>.

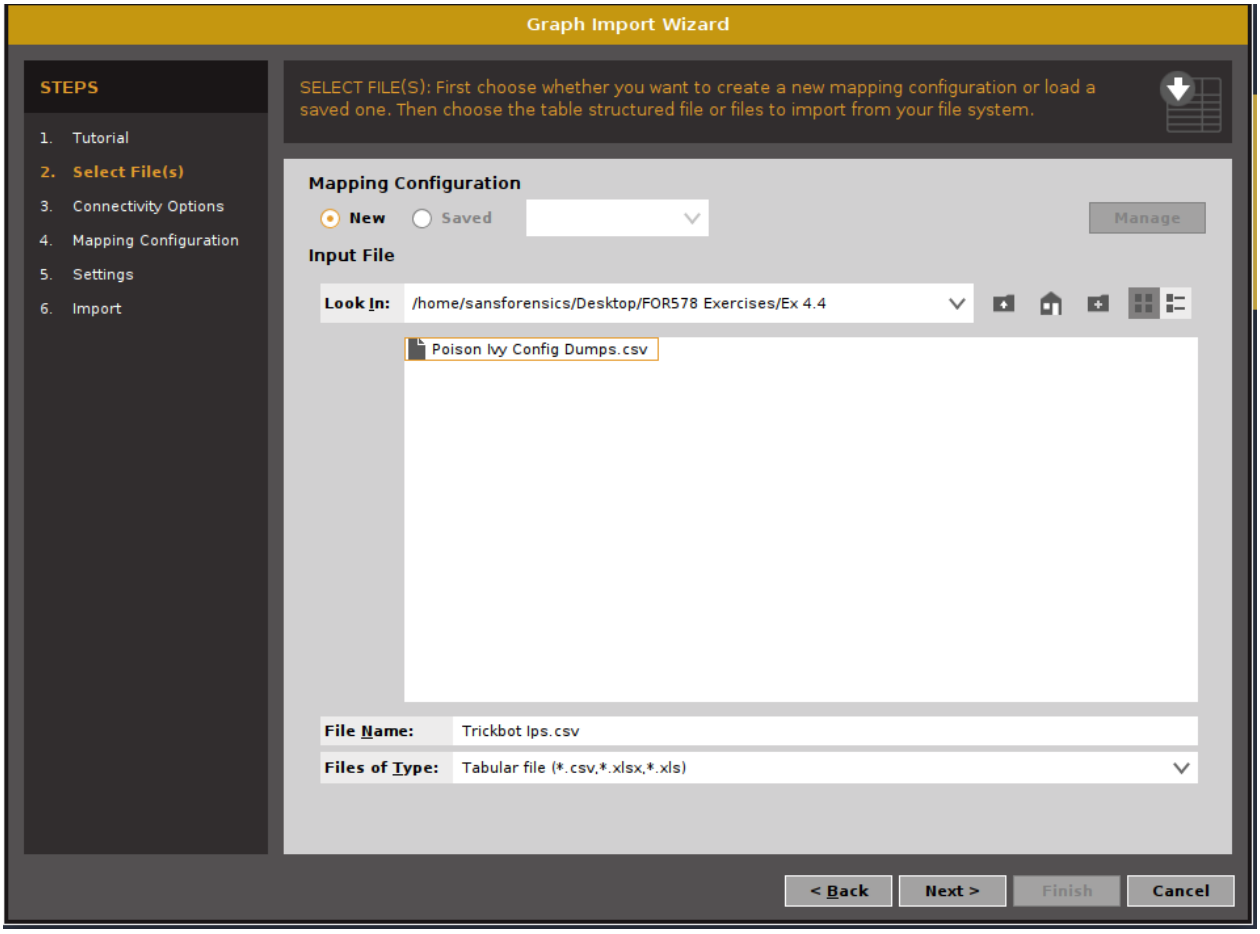


© 2021 Robert M. Lee and SANS Institute

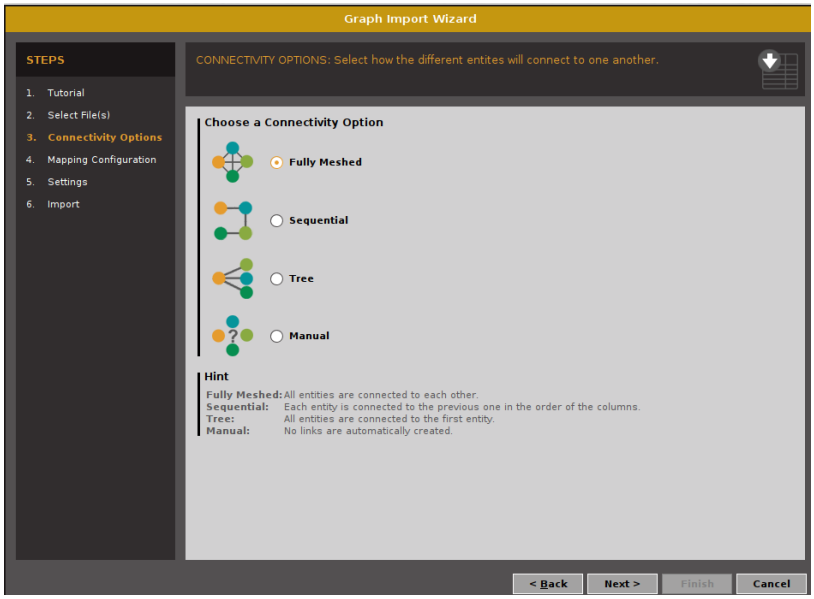
https://t.me/learningnets

Technet24

Choose your file from the Desktop as our import data. The specific location is /home/sansforensics/Desktop/FOR578 Exercises/Ex 4.4.



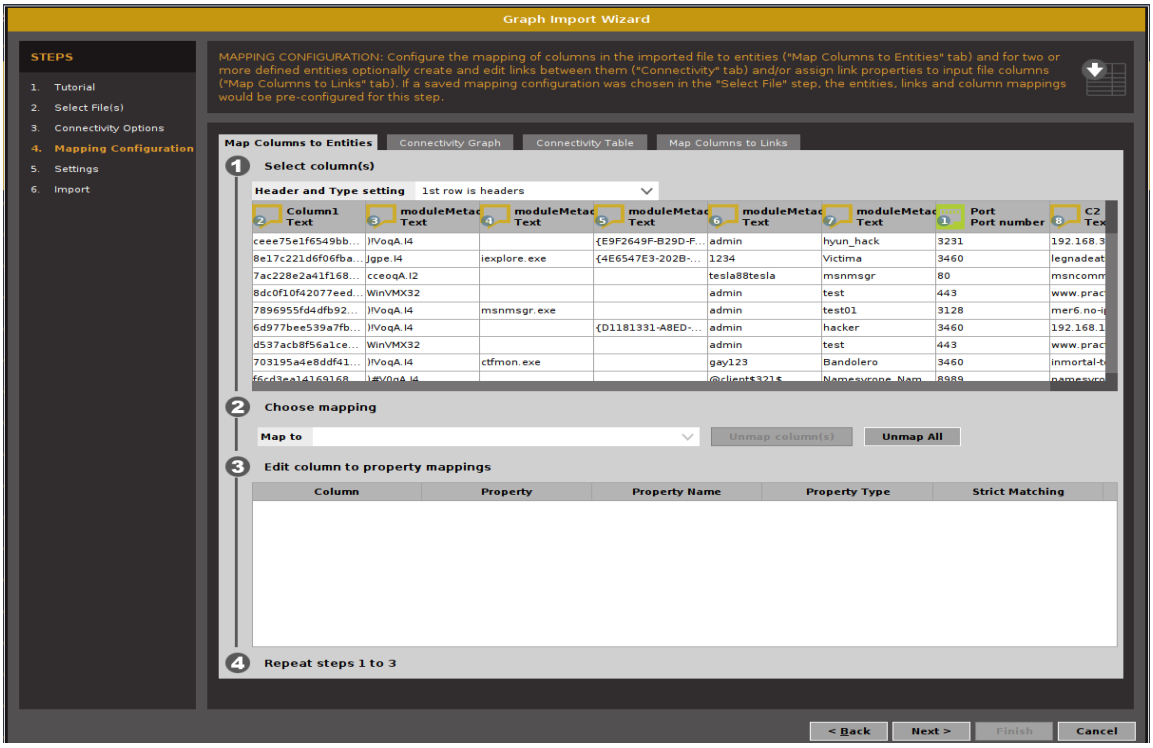
Select "Fully Meshed" on the Connectivity Options page so that all of the entities on each line will be associated with each other, and then select "Next".



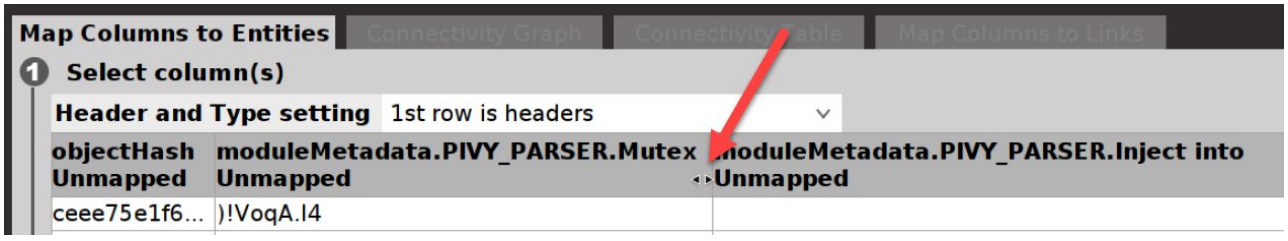
© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets

The Import Wizard can guide us through the process of importing each of the fields we want to graph into the specification. It will try to automatically identify fields, and in this case, we need to unmap several of the auto-mapped fields. Click on the columns that have been identified as "Text" (with the yellow icon) and then select "Unmap Column(s)."



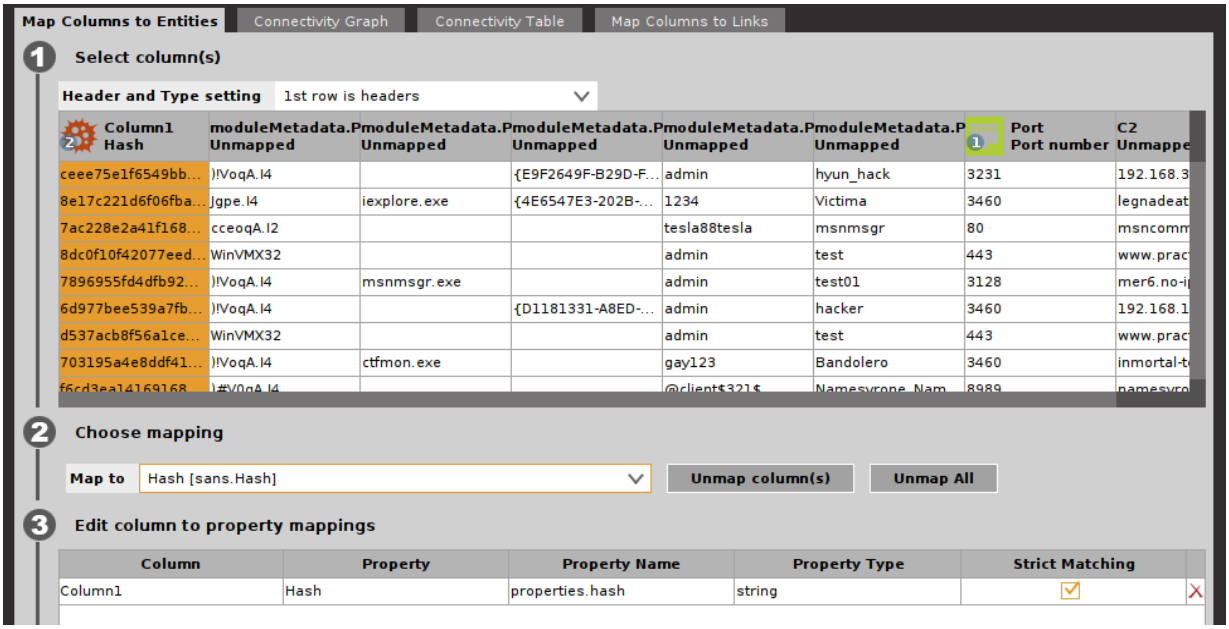
Click the "Header and Type setting" dropdown menu and choose "1st row is headers" because we have header information in your data file. Then select one column at a time and map each one to an entity type that we created. We need to map *six total columns to entities*: hash (column 1), mutex (column 2), password (column 5), Poison Ivy ID (column 6), port (column 7), and C2 (column 8). Since they are not prevalent in our dataset and we do not have entities for them, we will skip mapping "inject into" (column 3) and active setup value (column 4). If we need to better see the column headers, we can click on the lines between the columns and drag and drop to expand the header fields.



Map "objectHash" to the "Hash" entity you created by selecting the "objectHash" column in Section 1, and then select "Hash" from the dropdown menu in Section 2. Section 3 will auto-populate with the information you entered when you created the entity. Check to ensure that it is accurate, and then move onto the remaining columns.

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets
Technet24



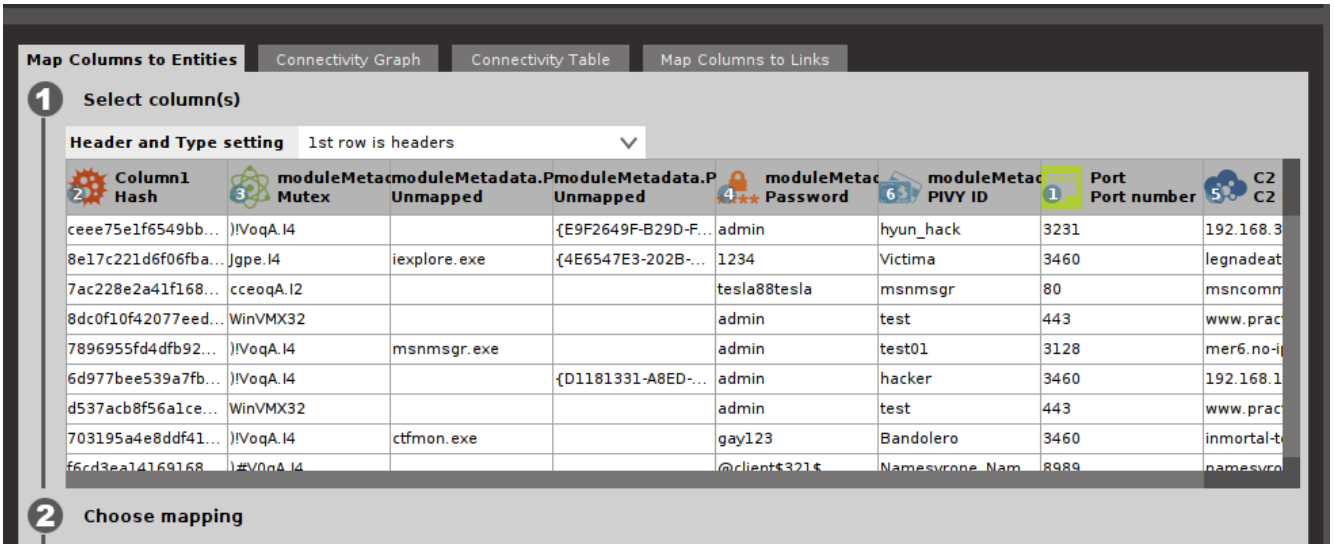
- **Map the "moduleMetadata.PIVY_PARSER.Mutex" in column 2 to the "Mutex" entity you imported by selecting the column in Section 1 and then select "Mutex" from the dropdown menu in Section 2.**

- **Map the "moduleMetadata.PIVY_PARSER.Password" in column 5 to the "Password" entity you imported by selecting the column in Section 1, and then select "Password" from the dropdown menu in Section 2.**

- **Map the "moduleMetadata.PIVY_PARSER.ID" in column 6 to the "PIVY ID" entity you imported by selecting the column in Section 1, and then select "PIVY ID" from the dropdown menu in Section 2.**

- **Map the "Port" in column 7 to the "Port" entity you imported by selecting the column in Section 1, and then select "Port" from the dropdown menu in Section 2. (If Maltego correctly auto-mapped this, we should just check to verify it was done correctly; we may not need to map the column.)**

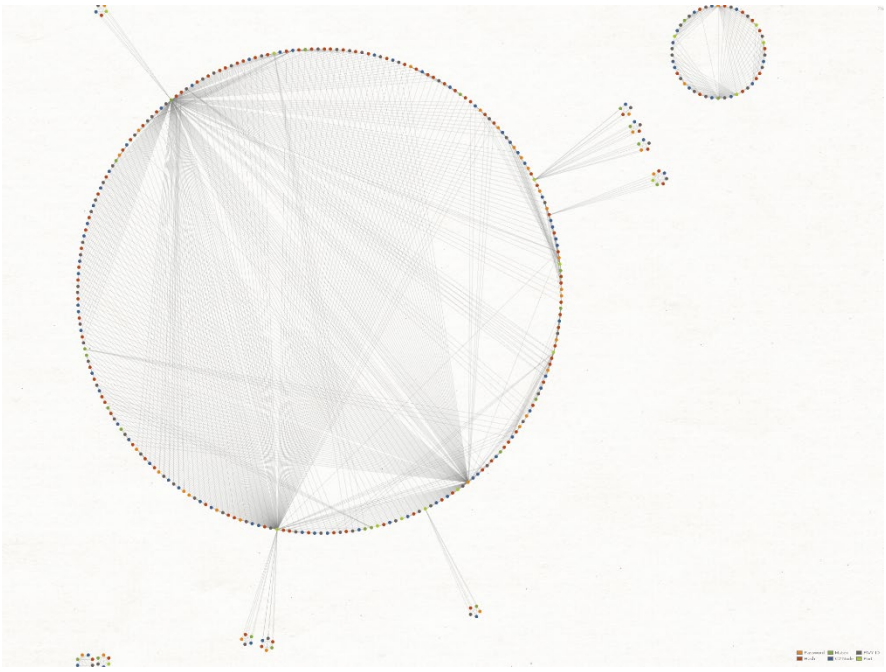
- **Map the "C2" in column 8 to the "C2 Node" entity you imported by selecting the column in Section 1, and then select "C2 Node" from the dropdown menu in Section 2.**



© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets

Select "Next." We will see a confirmation window that gives us statistics regarding how many rows were successfully extracted (233 Rows), any errors, and how many entities and links were created (330 Entities and 2576 Links). Once we confirm that the import was successful, we will be able to view and interact with the graph. Depending on your graph layout, your graph may look a little different from the below.



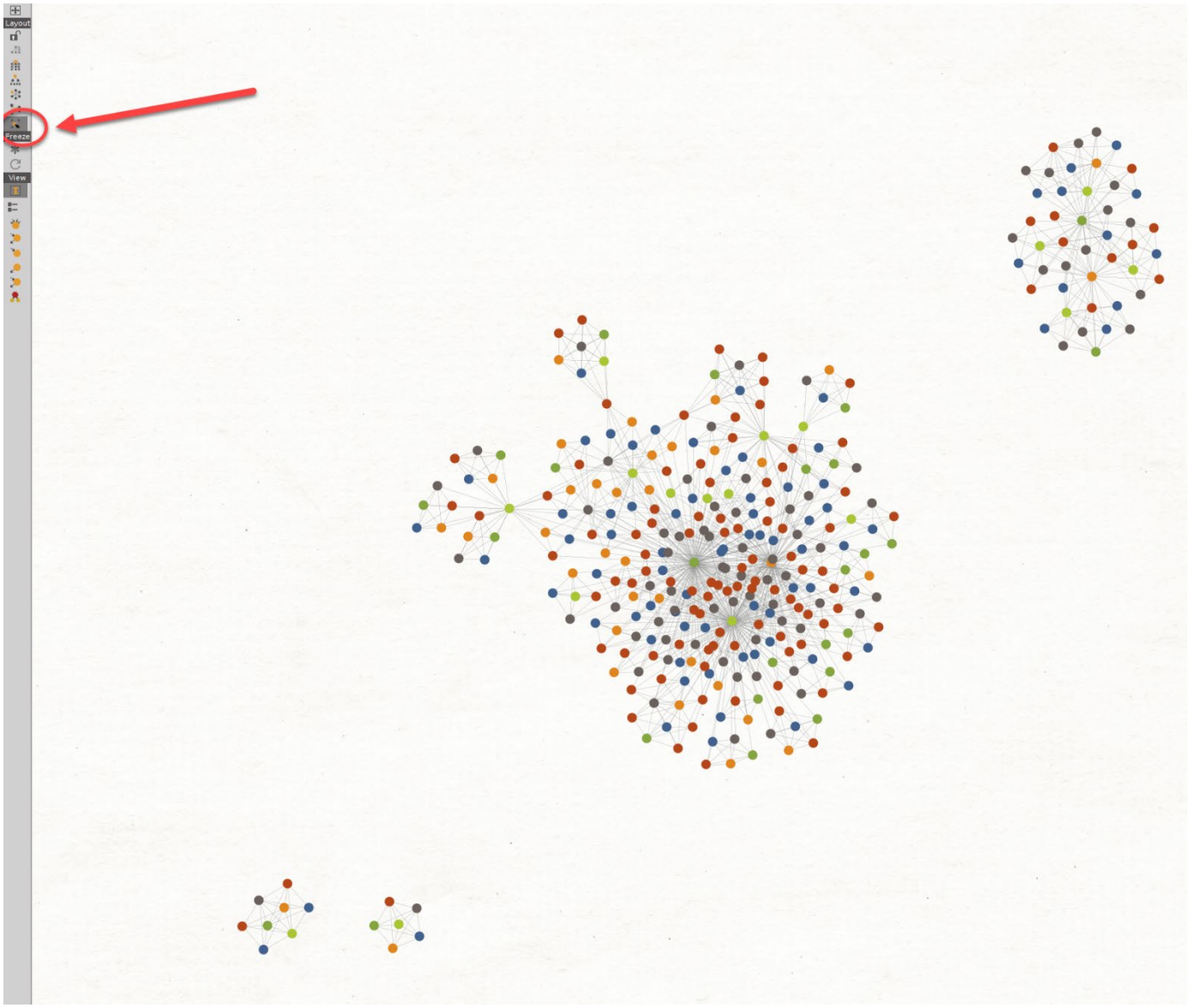
2. **What trends about this dataset are more apparent in a visual representation than they were in a spreadsheet view?**

- **The majority of the samples have at least one related link, with most having more than one. There are several clusters with only one link to the larger cluster, and three groupings that are completely isolated from the other samples.**

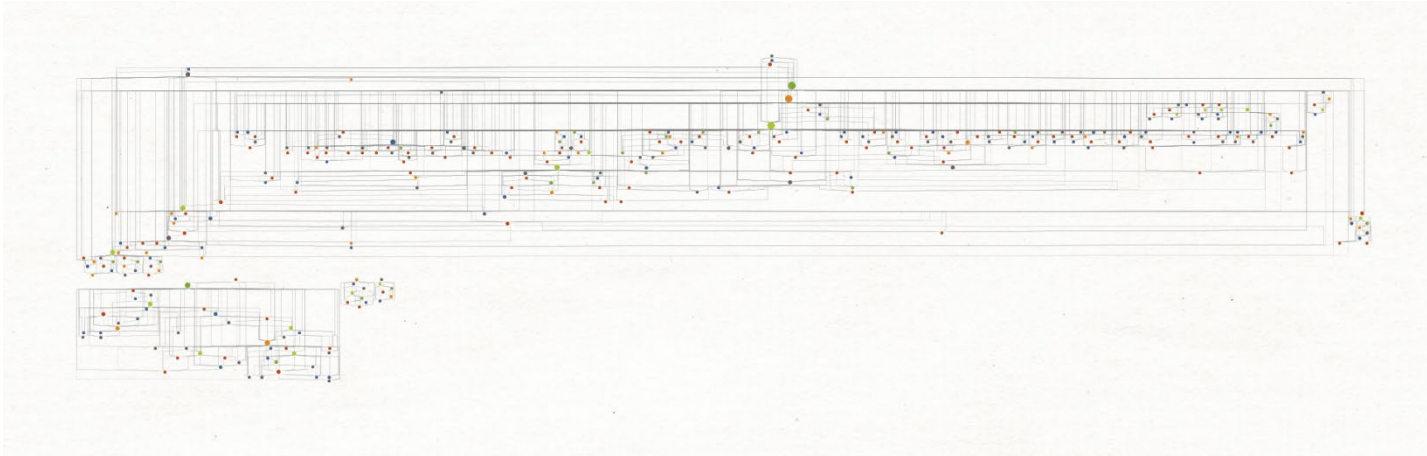
This pattern of most samples having at least one related link can be seen as soon as the graph loads in the default "Circular Layout." However, it can also be helpful to switch between the different Layouts on the pane on the left. Try switching between them to see which one makes the pattern most obvious. One example is the "Interactive Organic" mode, shown below, though your graph may look different. You can read more about how the different layouts work in Maltego documentation here: https://docs.maltego.com/support/solutions/articles/15000009615-graph-sidebar.

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets
Technet24



You can also try "Hierarchical" view. Which one shows the patterns most clearly from your perspective? There is no one right answer—different analysts find patterns in different ways.



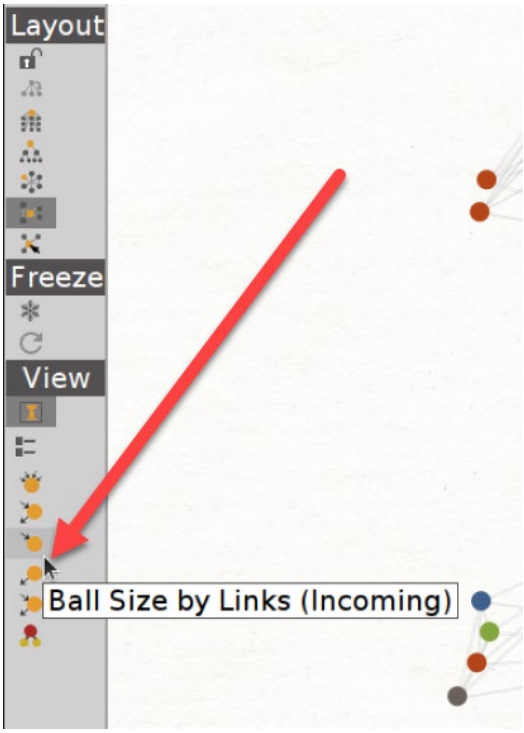
© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets

3. **Can you determine what the most frequently used port, mutex, and password are?**

- **Port: 3460, Mutex:)!VoqA.I4, Password: admin**

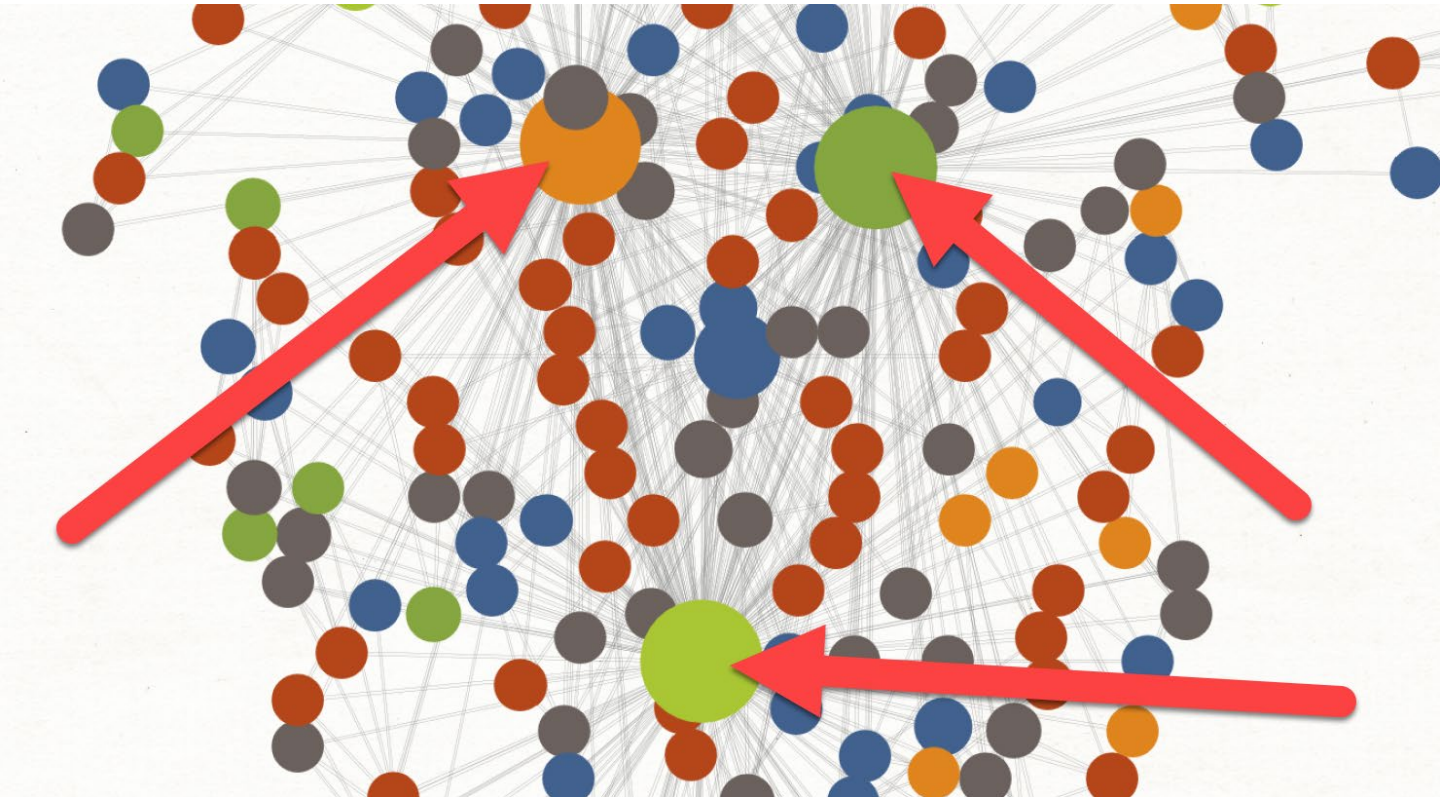
There are several different ways to view the graph that will allow analysts to view the different weightings and relationships between entities. These views are located on the left side under "View". Select the option for "Ball Size by Links (Incoming)", which will make the entities with the highest number of incoming links the largest. This allows us to view the most common entities from the import.



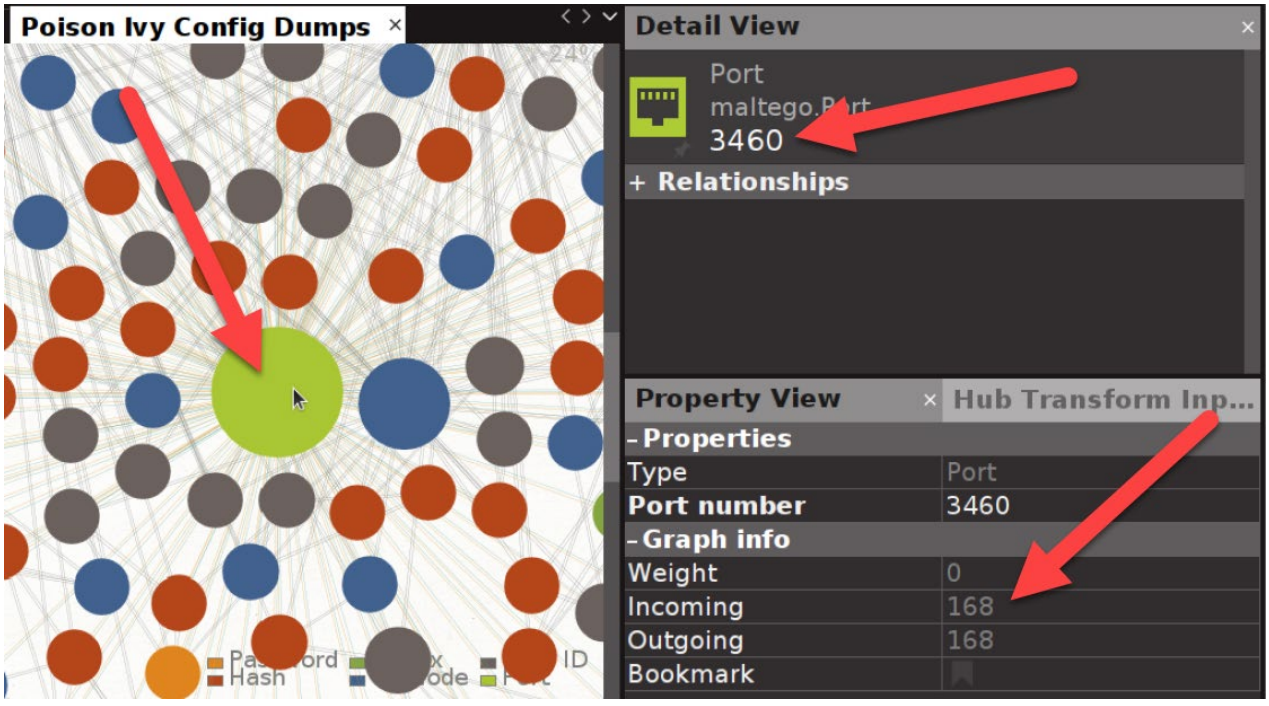
Visually examine the circles on the graph and select or zoom in on the largest entities to identify their values. Consult the color key in the bottom right of the graph to determine which colors represent which entities.

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets
Technet24



If we mouse over the larger nodes, the "Detail View" on the right side will show the value and the "Property View" will show the number of incoming and outgoing links. (If these views are not there, you can select them from the "Windows" menu.) This can help determine which values are the largest within this dataset. The below screenshot shows our analysis of the largest mutex circle, and therefore the most common port in our dataset: 3460. Conduct a similar analysis to determine that the most common mutex is)!VoqA.I4 and most common password is admin.



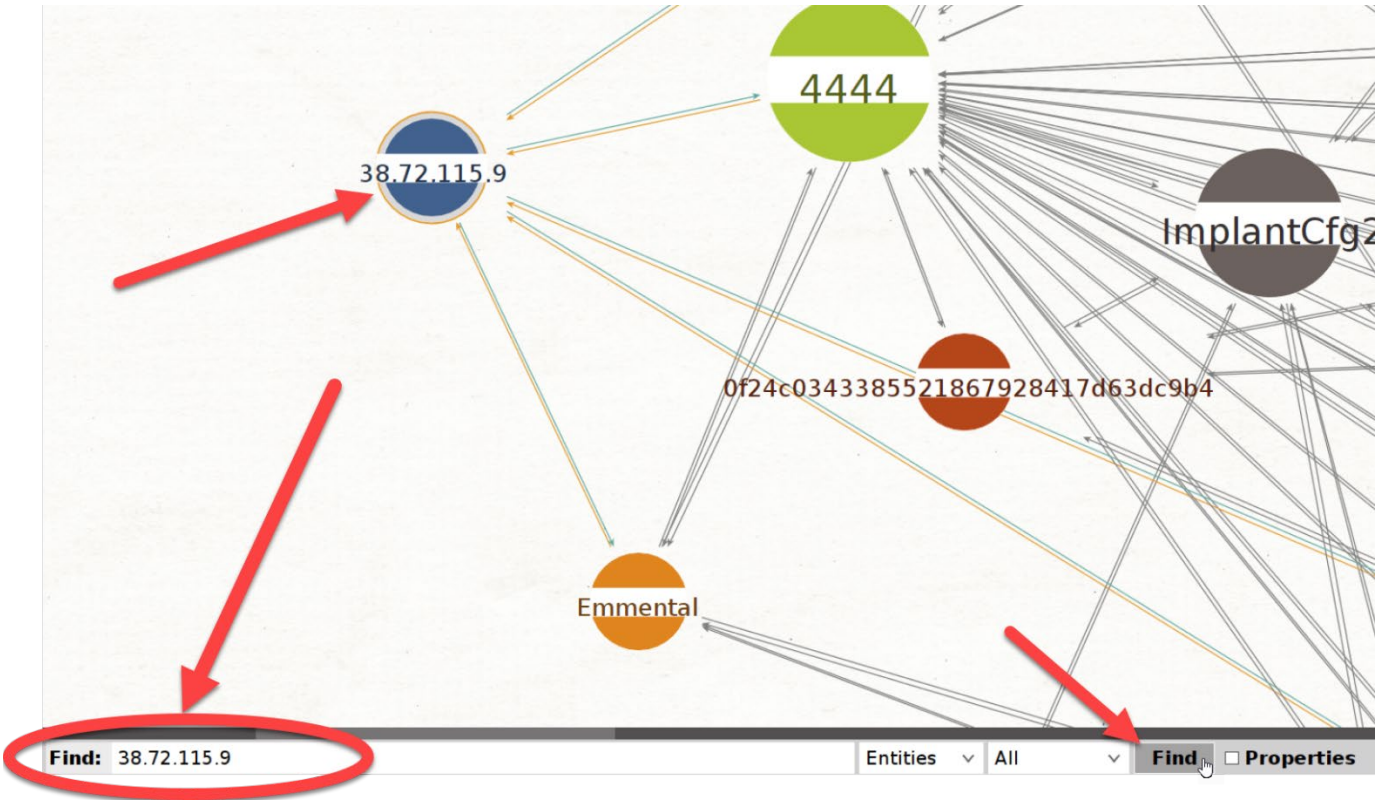
© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets

4. **Does the Poison Ivy sample we are interested in, the one configured with 38.72.115.9, have any commonly used values?**

- **<u>Yes, the mutex associated with 38.72.115.9, ")!VoqA.I4", is the most commonly used mutex identified in question 3.</u>**

Select CTRL-F to bring up the "find" window within Maltego and enter the value we are looking for, "38.72.115.9," and select "Find." The entity will be surrounded with an orange circle when it is selected.

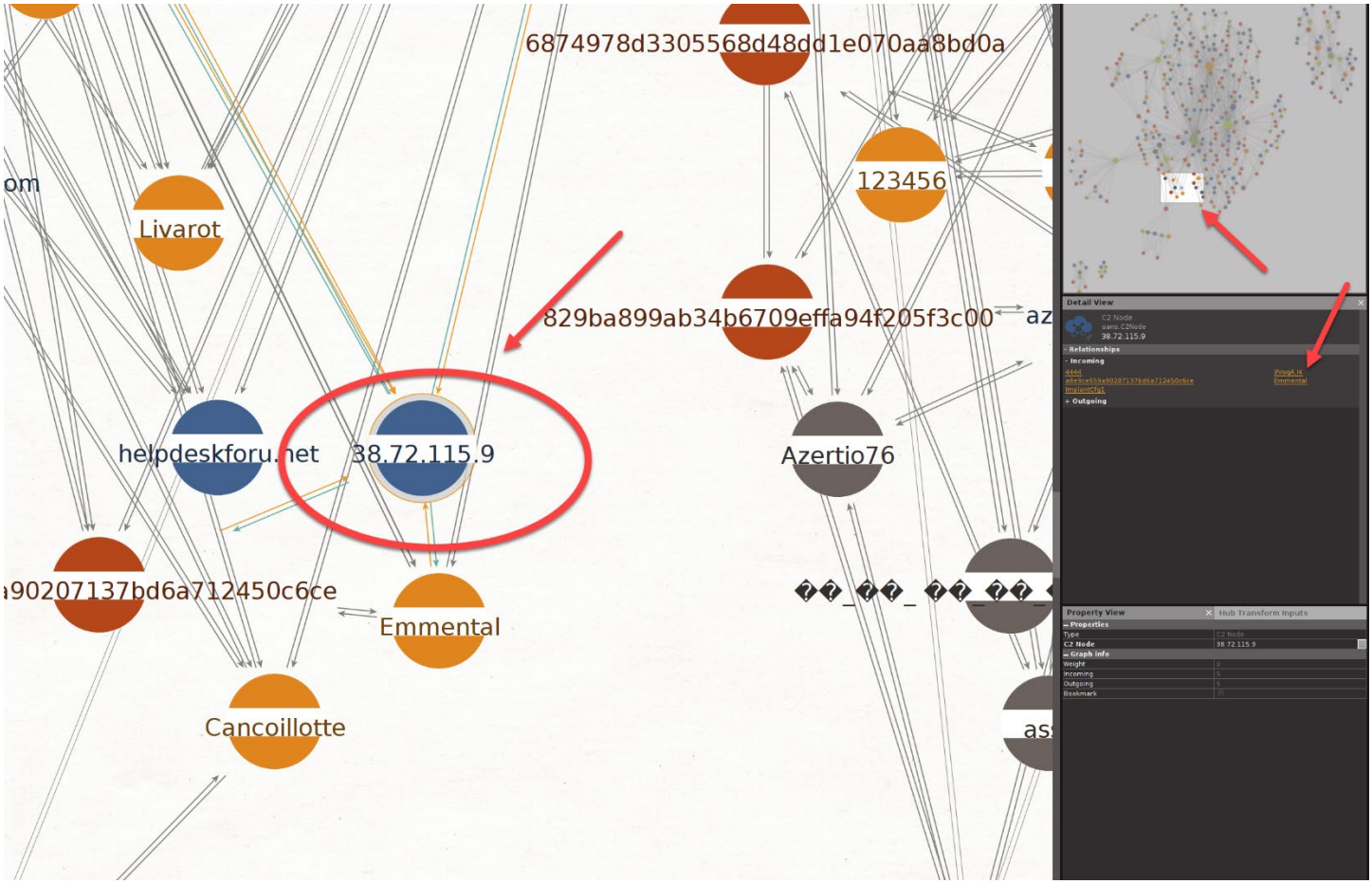


After locating the entity, look at the cluster of activity it is associated with. The port value is 4444, which is shared between several other C2 Nodes but is not the most common port identified previously. The implant ID is ImplantCfg1, which is also shared between several samples. The mutex, however, is)!VoqA.I4, which is shared across a large number of the samples.

In addition, if we look at the graph overview to see where the node sits on the larger graph, we can clearly see that it is part of the large cluster with at least some overlap to the majority of the samples and is not one of the three isolated clusters. You can try different layouts to see if others help you more clearly see the connections, and you can also manually move around entities if that helps your analysis.

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets
Technet24



5. **What other network-based indicators would be useful for further analysis?**

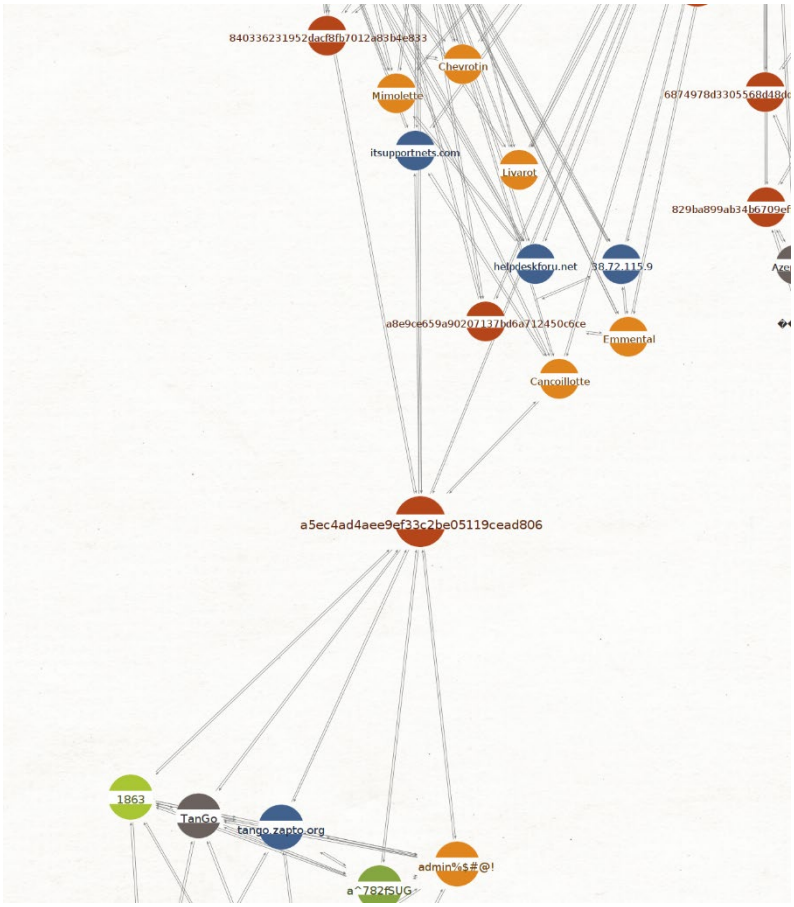
- **<u>Cluster 1: itservicesinc.net, itsupportnets.com, supportdesk.biz, 61.221.40.61, 76.29.149.73, 76.29.149.133, port 80. Cluster 2: tango.zapto.org, port 1863</u>**

Looking at the cluster of activity around 38.72.115.9, we can see that several other command and control nodes have been configured with the similar parameters, including implant name, port, and password. There is also another cluster that shares a hash with the 38.72.115.9 cluster, but does not have the same port, password schema, or implant name. This is an interesting find and could help understand more about the activity group behind this and how they operate.

Identifying these additional C2 nodes, along with other ports that have been used with the additional nodes, and discovering if they have been seen in our environment can help to ensure that there were no other compromises related to the one identified.

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets



Exercise: Key Takeaways

- **Visualization can empower an analyst to better understand large datasets without needing to know every piece of data within the dataset.**
- **By using different display layouts, you may more easily understand the structure within the data. You could see the automatic clustering within the Organic layout, but with using the block layout, you can see the direct lineage in a top-down format to show clustered, hierarchical relationships.**
- **Large graphs can be searched and then the connected nodes reviewed both by visual analysis (looking at the graph for links) and also by reviewing relationships in the detail pane in CaseFile. Having both of these analytic methods available can reveal insights that may be missed with non-visual analysis.**

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets
Technet24

Exercise 4.5: The Rule of 2

Objectives

- Given structured threat information, apply the Diamond Model to add intrusions to an existing activity group and build new activity groups

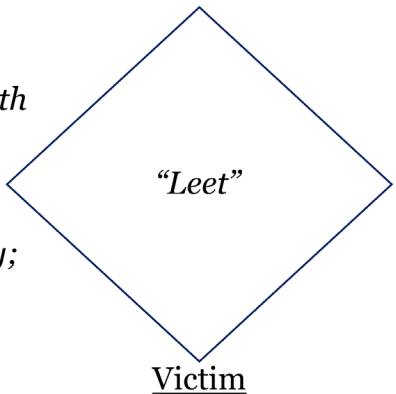
Scenario: As the CTI team for Edison International, you have tracked an intrusion set you have called "Leet". Now, you want to formally define an activity group for that intrusion so you can track related activity. You have existing information about the intrusion set from previous work to help you define that activity group. Additionally, you have been supplied with structured threat information from your security operations center and incident response team members from within Edison International about other intrusions that Edison has experienced. You have been asked to satisfy several intelligence requirements:

- *First, you need to define an Activity Group around the Leet intrusion set*
- *Next, you also have the requirement to determine if any existing intrusion sets match your new Activity Group.*
- *Last, you have the requirement to identify any other activity groups that you should be tracking with relation to the Edison International companies (microprocessor technologies, electric power, and point-of-sales/retail systems. Additionally, hospitality services such as hotels should be considered because of our numerous traveling employees).*

Exercise Prep

The Analytic Requirement we have for the Leet intrusion set is to understand and track the adversary that compromised Edison International. The Activity Group will be called DERPYHOOVES. Below is a summary of what our work thus far has revealed about the Leet intrusion set.

Recap of Leet Intrusion Set



© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets

Exercise Information

The following are quick summaries and structured threat information provided by the CTI team's previous efforts to get data into a structured format, as well as inputs from external teams such as incident response and the security operations center, but using our structured schema of the Kill Chain. Your task is to see if any of these intrusions match your newly-defined activity groups as well as identify new activity groups from these intrusions.

There are many ways to approach this analysis, and you can choose the method that works best for you. Your main work will be dividing these intrusions into the Diamond Model—you may choose whether you keep the Kill Chain mappings as you do that or not.

Intrusion 1
Victim: Government organization that is a big buyer of microprocessors
Structured Information:

Kill Chain Phases	Key Findings
KC 1: Reconnaissance	
KC 2: Weaponization	
KC 3: Delivery	
KC 4: Exploitation	
KC 5: Installation	COM scriptlet reaches out to images.chinabytes.info
KC 6: Command and Control	Hardcoded IPs no clear pattern
KC 7: Actions on Objectives	Meterpreter metsvc backdoor

Intrusion 2
Victim: Hotel chain in Europe
Structured Information:

Kill Chain Phases	Key Findings
KC 1: Reconnaissance	
KC 2: Weaponization	
KC 3: Delivery	
KC 4: Exploitation	
KC 5: Installation	Gamefish malware
KC 6: Command and Control	Legitimate but compromised domains local to the target
KC 7: Actions on Objectives	Stealing point-of-sale data and guest information

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets
Technet24

Intrusion 3
Victim: Research and development firm in Germany for computer chips
Structured Information:

Kill Chain Phases	Key Findings
KC 1: Reconnaissance	
KC 2: Weaponization	
KC 3: Delivery	
KC 4: Exploitation	CVE-2016-7255
KC 5: Installation	
KC 6: Command and Control	Meterpreter metsvc backdoor communicating on Port 31337
KC 7: Actions on Objectives	PowerShell for recon and lateral movement

Intrusion 4
Victim: Hotel chain
Structured Information:

Kill Chain Phases	Key Findings
KC 1: Reconnaissance	
KC 2: Weaponization	
KC 3: Delivery	Phishing emails with Word Documents
KC 4: Exploitation	Social Engineering (Vacation Themed) to enable Macros
KC 5: Installation	
KC 6: Command and Control	
KC 7: Actions on Objectives	

Intrusion 5
Victim: Electric power company's business networks
Structured Information:

Kill Chain Phases	Key Findings
KC 1: Reconnaissance	
KC 2: Weaponization	
KC 3: Delivery	Phishing Emails from George@elie7epower(dot)com
KC 4: Exploitation	CVE-2017-0199
KC 5: Installation	PlugX malware w/ mutex 1337
KC 6: Command and Control	Hardcoded IPs in Taiwan, China, and Vietnam
KC 7: Actions on Objectives	EternalBlue for lateral movement / stealing contracts

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets

Intrusion 6
Victim: Academics researching new microprocessor technology
Structured Information:

Kill Chain Phases	Key Findings
KC 1: Reconnaissance	
KC 2: Weaponization	Metasploit strings contained in Macros
KC 3: Delivery	Phishing emails from support-themed domains
KC 4: Exploitation	
KC 5: Installation	
KC 6: Command and Control	Meterpreter backdoor
KC 7: Actions on Objectives	Hashes dumped via “hashdump”, R&D documents exfiltrated to 76.29.149.132/fjerk

Intrusion 7
Victim: Critics of the Syrian government
Structured Information:

Kill Chain Phases	Key Findings
KC 1: Reconnaissance	
KC 2: Weaponization	
KC 3: Delivery	Phishing emails themed to military members
KC 4: Exploitation	MITM vulnerability in iTunes
KC 5: Installation	
KC 6: Command and Control	IP addresses in Venezuela
KC 7: Actions on Objectives	

Intrusion 8
Victim: Vendor of electric grid equipment
Structured Information:

Kill Chain Phases	Key Findings
KC 1: Reconnaissance	
KC 2: Weaponization	
KC 3: Delivery	Waterhole leveraging vendor websites
KC 4: Exploitation	Metasploit modules
KC 5: Installation	
KC 6: Command and Control	Porn- and Disney-themed domains
KC 7: Actions on Objectives	Stealing internal system network information

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets
Technet24

Intrusion 9
Victim: Leading microprocessor vendor
Structured Information:

Kill Chain Phases	Key Findings
KC 1: Reconnaissance	
KC 2: Weaponization	
KC 3: Delivery	Supply chain of Seagate Hard Drive
KC 4: Exploitation	Modification of source code in hard drive
KC 5: Installation	Create and use hidden disk area in HDD source code
KC 6: Command and Control	
KC 7: Actions on Objectives	Stealing IP and anti-forensics with Windows log manipulator

Intrusion 10
Victim: Embassies and government institutions
Structured Information:

Kill Chain Phases	Key Findings
KC 1: Reconnaissance	
KC 2: Weaponization	Natural language Spanish usage
KC 3: Delivery	Watering hole through Blogs
KC 4: Exploitation	Social Engineering Toolkit and run Java executable
KC 5: Installation	Java executable and RAR files
KC 6: Command and Control	Adversary registered blogs with Spanish usage
KC 7: Actions on Objectives	

Intrusion 11
Victim: Military hospitals
Structured Information:

Kill Chain Phases	Key Findings
KC 1: Reconnaissance	
KC 2: Weaponization	Single Factor Authentication VPNs
KC 3: Delivery	VPN
KC 4: Exploitation	Existing PowerShell Usage
KC 5: Installation	Nothing Additional Installed
KC 6: Command and Control	
KC 7: Actions on Objectives	Healthcare records

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets

Intrusion 12
Victim: Human rights activists in the Middle East
Structured Information:

Kill Chain Phases	Key Findings
KC 1: Reconnaissance	
KC 2: Weaponization	
KC 3: Delivery	Phishing emails themed toward activists
KC 4: Exploitation	MITM vulnerability in iTunes
KC 5: Installation	
KC 6: Command and Control	IP addresses in Brazil
KC 7: Actions on Objectives	

Intrusion 13
Victim: Hotel chain
Structured Information:

Kill Chain Phases	Key Findings
KC 1: Reconnaissance	
KC 2: Weaponization	
KC 3: Delivery	Phishing emails with Word Documents
KC 4: Exploitation	Social Engineering to use Macros
KC 5: Installation	Gamefish malware
KC 6: Command and Control	
KC 7: Actions on Objectives	EternalBlue for lateral movement

Intrusion 14
Victim: Office of Personnel Management
Structured Information:

Kill Chain Phases	Key Findings
KC 1: Reconnaissance	Chinese University IPs scanning external gateway
KC 2: Weaponization	
KC 3: Delivery	
KC 4: Exploitation	
KC 5: Installation	
KC 6: Command and Control	
KC 7: Actions on Objectives	

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets
Technet24

Exercise: Questions

1. Define the formal high-level definition of DERPYHOOVES to meet our analytical requirement.

- _____

2. Which intrusions match the newly-created DERPYHOOVES Activity Group?

- _____
- _____

3. How many other Activity Groups could you create using the Rule of 2?

- _____
- _____
- _____

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets

Exercise: Questions with Step-by-Step

1. Define the formal high-level definition of DERPYHOOVES to meet our analytical requirement.

- **Adversary: High, Victim: High, Infrastructure: N/A, Capability: N/A**

Our analytical requirement is to track the adversary that compromised Edison International and its companies. Because this adversary has shown not only the interest but has successfully compromised the organization, the CTI team wants to keep track on this specific adversary. It is not a requirement at this time to get to state or criminal group attribution, though that could be supported later if we needed that for an intelligence requirement. What matters, though, is given this group's compromising of our organization, we want to track their various evolutions and make sure we're prepared for them.

Therefore, we prioritize the Adversary and Victim features as high, and deprioritize Infrastructure and Capability.

2. Which intrusions match the newly-created DERPYHOOVES Activity Group?

- **Intrusion 5**
- **Intrusion 6**

There are multiple ways you could reach this answer. Regardless of how you choose to perform your analysis, some type of structured methodology would be helpful to allow you to compare the existing DERPYHOOVES features (Adversary, Victim, Infrastructure, and Capability) to the features of each of the new intrusions we are considering. One approach would simply be to review the Adversary features of DERPYHOOVES, skim the other intrusions for anything that looks "related", and then move on to each feature in turn.

Intrusion 5 has a "leet speak" reference potentially in the email "eli7e" and the use of PlugX specifically with the Mutext "1337" correlates to the choices and theming in DERPYHOOVES.

Intrusion 6's infrastructure wouldn't normally be enough, but the fact that the IT support-themed emails are consistent across numerous intrusions has us reconsider that as a human fingerprint, in the Adversary feature. The fjerk folder and very similar IP address to ones we've observed before further make the correlation.

In both the above intrusions, because we're relying on indicators, we wanted to see the indicator as a *key* indicator, i.e. seen in two or more kill chain steps. Therefore, Intrusion 3, which has the "31337" port but nothing else, wouldn't be enough; also, that port is pretty commonly used.

As always, your answers may differ from these, and that's perfectly fine.

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets
Technet24

3. How many other Activity Groups could you create using the Rule of 2?

- **Three**

Our next task is to look at the 14 intrusions to see if we can create any other activity groups by looking for meaningful overlaps in two or more features of the Diamond Model (the Rule of 2). Without some kind of methodology, this would be a difficult task. One approach you could take would be to use Excel to divide information from each intrusion into the four Diamond Model features, then use the filtering functionality we previously learned to identify overlaps. An example of how you could do this is shown below.

	A	B	C
1	**Intrusion Number**	**Diamond Feature**	**Unique Data Point**
2	Intrusion 1	Adversary	
3	Intrusion 1	Victim	Gov org that buys microprocessors
4	Intrusion 1	Capability	COM scriptlet, Meterpreter
5	Intrusion 1	Infrastructure	images.chinabytes[.]info, hardcoded IPs
6	Intrusion 2	Adversary	
7	Intrusion 2	Victim	Hotel chain in Europe (Stole POS data and guest info)
8	Intrusion 2	Capability	Gamefish malware
9	Intrusion 2	Infrastructure	Legit but compromised domains local to target

	A	B	C
1	**Intrusion Number**	**Diamond Feature**	**Unique Data Point**
3	Intrusion 1	Victim	Gov org that buys microprocessors
11	Intrusion 3	Victim	R&D firm in Germany for computer chips
23	Intrusion 6	Victim	Academics researching microprocessors

You do not have to take this approach—perhaps it works for you to use mind-mapping software or draw out diamonds and make connections. As we've learned, different analysts approach analysis differently.

Intrusion 1, 3, and 6 all have a shared "capability" and "victim" vertices using common hacking tools in the Metasploit framework or similar frameworks (Cobalt Strike) and targeting microprocessor-related victims.

Intrusion 2 and 13 both have "capability" and "victim" vertices overlaps as well, leveraging Gamefish malware and targeting hotel chains.

Intrusion 4 is targeting hotel chains, but we do not have enough information about the other intrusions to tie it to anything else at this time. Phishing emails and social engineering is too broad to link to anything else; the Vacation theme is interesting, but we'd want to dig into it to see if it's really tailored or simply random vacation theming.

Intrusion 5 uses the EternalBlue exploit and vulnerability like Intrusion 13, but there's nothing else linking them, and the exploit and vulnerability were made publicly available through ShadowBrokers leaks (not required to know for this exercise, but good knowledge to complement the understanding).

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets

Intrusion 7 and 12 both use a MITM in iTunes in the “capability” vertices and have an overlap in “victims” of targeting dissidents and human rights activists in Syria and the Middle East.

Intrusion 8 has shared “capability” with some intrusion sets and some shared “victims” but not together. This is a good misleading one but isn’t correlated with anything else at this time.

Intrusion 9 sounds particularly enticing to our intelligence requirement but does not correlate with anything else.

Intrusion 10, 11, and 14 are all interesting Intrusion Sets as well, but they do not share two vertices with any other intrusion sets.

Therefore, the unique activity groups are the combinations of Intrusion 1/3/6, 2/13, and 7/12.

Exercise: Key Takeaways

- **We used our analytical requirement to define a new activity group named DERPYHOOVES. We then identified two intrusions that should be added to that activity group.**
- **We created additional activity groups using the Rule of 2. By examining our original requirements, we were able to share three activity groups that were relevant to Edison International.**

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets
Technet24

Exercise 5.1: Developing IOCs in YARA

Objectives

- Gain familiarity with YARA
- Validate YARA-based IOC Against Victim Memory Image

Scenario: An understanding of the activity identified in the SpaderTech intrusion of multiple machines was gathered from both external threat intelligence and internally from various security personnel. It is now your job as a threat intelligence analyst to disseminate that data into a usable form by tactical level members. Sharing the data in a tactical form for malware analysts usually takes the form of a YARA rule.

Exercise Prep

This lab uses the SIFT VM and the same memory image from Exercise 2.3 in the **Ex 5.1** folder in the **FOR578 Exercises** folder on the SIFT VM Desktop.

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets

Exercise: Questions

1. Out of the following C2 indicators, which one(s) is(are) detected in the memory image? Create a YARA rule to determine this, then run the rule on the memory image **stsupport10-memory.dd4.001**.

Indicators:
51.11.247.89
downloads.topenergysupport.com

- _____
- _____

2. Out of the following indicators, which one(s) is(are) detected in the memory image? Create a YARA rule to determine this, then run the rule on the memory image **stsupport10-memory.dd4.001**.

Indicators:
vncviewer_v3.38.9_tcp.exe
rubyw.exe
ipconfig.exe
taskhostw.exe
out.rar
lsass.exe

- _____
- _____
- _____
- _____

3. Create a single YARA rule that alerts when at least one indicator from each set of indicators above is observed.

© 2021 Robert M. Lee and SANS Institute

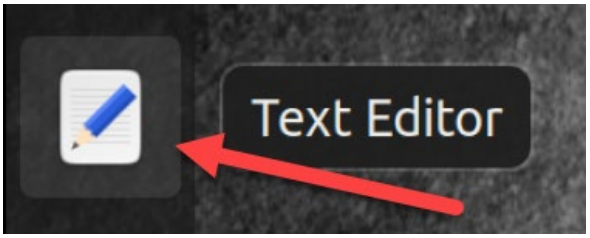
https://t.me/learningnets
Technet24

Exercise: Questions with Step-by-Step

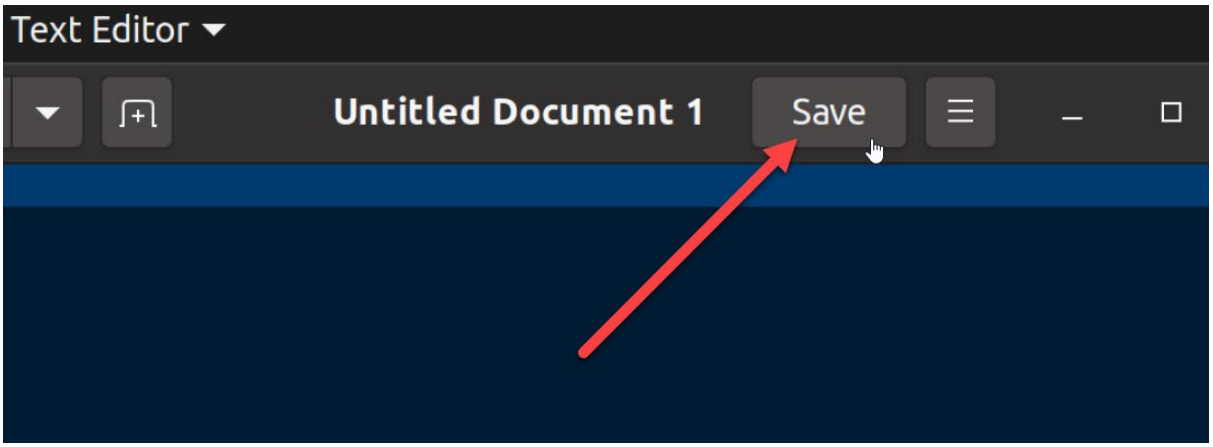
1. Out of the following C2 indicators, which one(s) is(are) detected in the memory image? Create a YARA rule to determine this, then run the rule on the memory image **stsupport10-memory.dd4.001**.

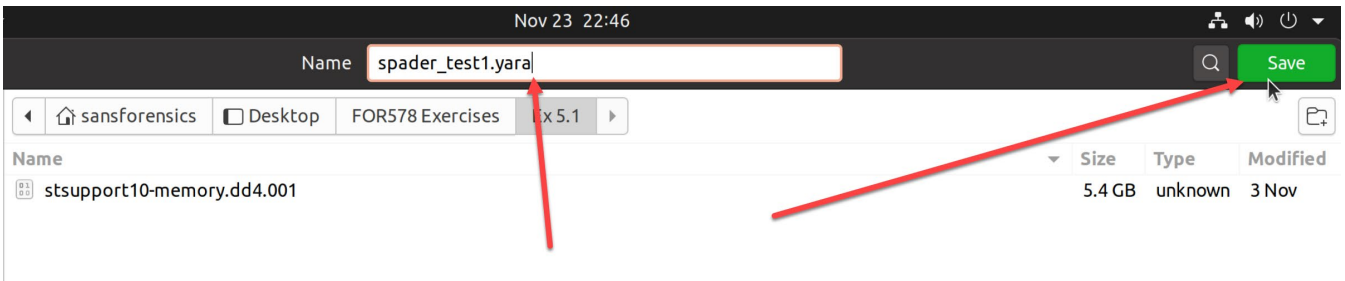
   Indicators:
   51.11.247.89
   downloads.topenergysupport.com

   Log in to the SIFT VM and open the Text Editor from the left menu. To write YARA rules, it can be helpful to create them in a text file.



   When making YARA rules, it can be good to distinguish between validated and test rules. Test rules are those we make initially, and validated rules are ones that are proven to work that we might also put in production. Click Save, and name the file "spader_test1.yara", saving it in our "Ex 5.1" folder. (We do not need to put a ".yara" after the file name for it to work, but it is helpful for identification purposes.) Next, click the green Save button.

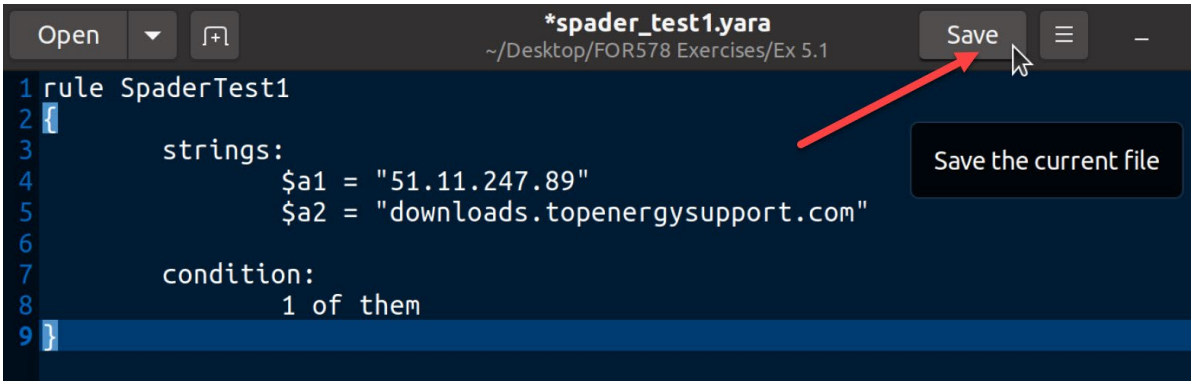




© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets

Write a YARA rule that looks for either of our two network indicators. We choose to use the condition "1 of them", but you could write this in different ways. Create the text file exactly as shown below and then click Save and exit the Text Editor.



Next, open a terminal from the left menu and navigate to the Ex 5.1 folder by entering the following command (remember, we can save time with tab-complete):

```
cd Desktop/FOR578\ Exercises/Ex\ 5.1/
```

Double check we saved our YARA rule in the right location by running the following command:

```
ls
```

We should see our YARA rule and the memory image, "stsupport10-memory.dd4.001". Recall that we can run YARA against any static dataset such as files or memory images.

```
sansforensics@siftworkstation: ~/Desktop/FOR578 Exercises/Ex 5.1
$ ls
spader_test1.yara  stsupport10-memory.dd4.001
```

To determine which of the strings matches the memory file, we need to pass yara the –s option for it to show which strings match.

Execute the following command:

```
yara –s spader_test1.yara stsupport10-memory.dd4.001
```

```
sansforensics@siftworkstation: ~/Desktop/FOR578 Exercises/Ex 5.1
$ yara -s spader_test1.yara stsupport10-memory.dd4.001
```

After a few moments, the terminal window should show which, if any, indicators match and their location in the file. When YARA outputs "SpaderTest1 stsupport10-memory.dd4.001", this tells us that the rule ran successfully against the memory file and had matches on our condition. In this case, both the 51.11.247.89 IP address and downloads.topenergysupport[.]com indicators have matches. We observe one match and one memory address location (starting with "0x…") for the IP, and many matches for the domain.

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets
Technet24

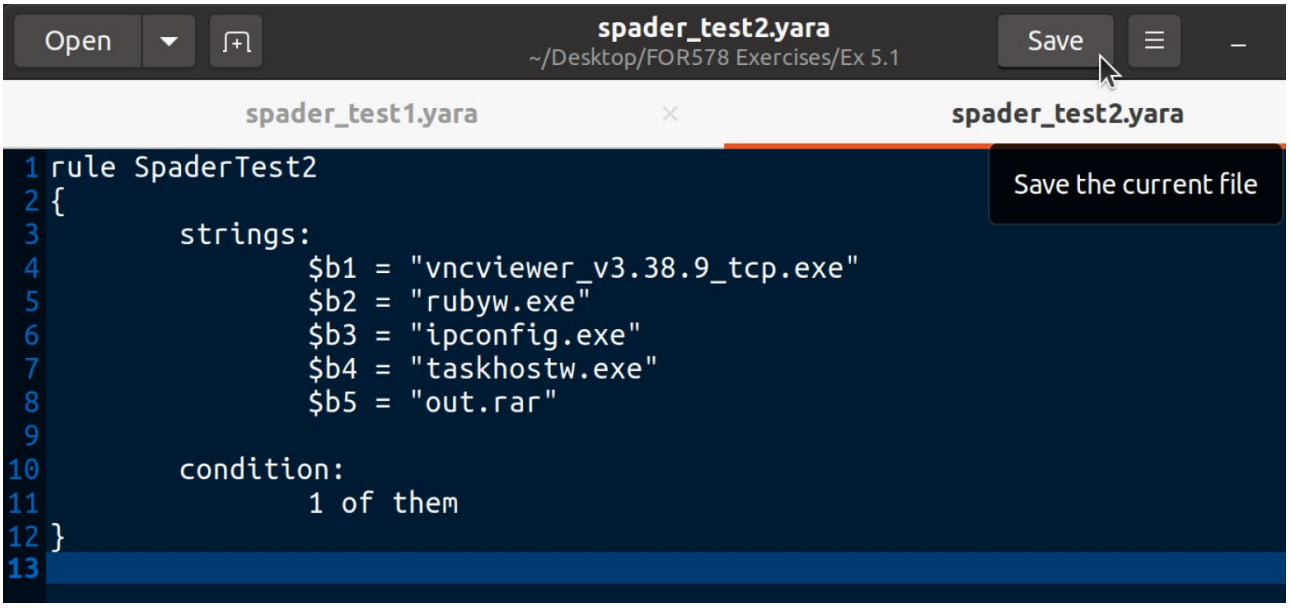
```
sansforensics@siftworkstation: ~/Desktop/FOR578 Exercises/Ex 5.1
$ yara -s spader_test1.yara stsupport10-memory.dd4.001
SpaderTest1 stsupport10-memory.dd4.001
0x5dd9f220:$a1: 51.11.247.89
0x534470b:$a2: downloads.topenergysupport.com
0x5344732:$a2: downloads.topenergysupport.com
0x1cc70f70:$a2: downloads.topenergysupport.com
0x2347a592:$a2: downloads.topenergysupport.com
0x2c92a7d4:$a2: downloads.topenergysupport.com
0x3bf6d8c7:$a2: downloads.topenergysupport.com
0x3ce8bd17:$a2: downloads.topenergysupport.com
0x41adf3c5:$a2: downloads.topenergysupport.com
0x41adf845:$a2: downloads.topenergysupport.com
0x41adf875:$a2: downloads.topenergysupport.com
0x41adf8d5:$a2: downloads.topenergysupport.com
0x41adf905:$a2: downloads.topenergysupport.com
```

2. Out of the following indicators, which one(s) is(are) detected in the memory image? Create a YARA rule to determine this, then run the rule on the memory image **stsupport10-memory.dd4.001**.

Indicators:

vncviewer_v3.38.9_tcp.exe
rubyw.exe
ipconfig.exe
taskhostw.exe
out.rar

Navigate back to Text Editor in our left menu. Click the small arrow in the top menu next to "Text Editor", then select New Document to create a new text file. Name it "spader_test2.yara," save it to the same Ex 5.1 folder that we previously used, and enter the indicators given as strings with the condition of "1 of them" as shown below. Next, click Save to ensure your changes are saved.



© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets

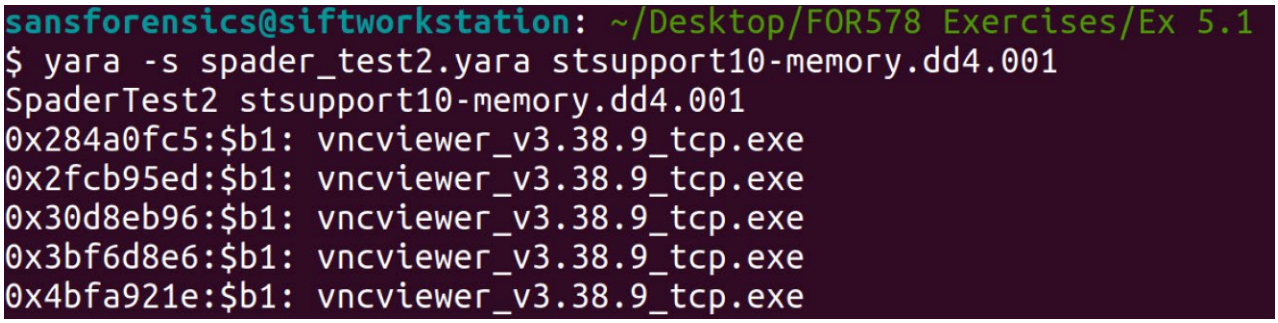
Save the file and make sure the file is in the Ex 5.1 folder. From the terminal, run the rule against the memory file.

Execute the following command:

```
yara –s spader_test2.yara stsupport10-memory.dd4.001
```



After a few moments, the terminal window should display multiple hits for all four of the strings we searched for.



BONUS: If you have extra time on this exercise, you can also add "nocase" and "wide" after each declared variable, such as

```
$b5 = "out.rar" nocase wide
```

This will have the string search for any combination of uppercase and lowercase lettering. Wide will allow it to search for the string's letters spread out across multiple bytes when stored in memory. Try running the same command you did earlier against a new rule with "nocase wide" added. What do you notice that is different? Can you spot the pattern and the oddity in how YARA is displaying the results?

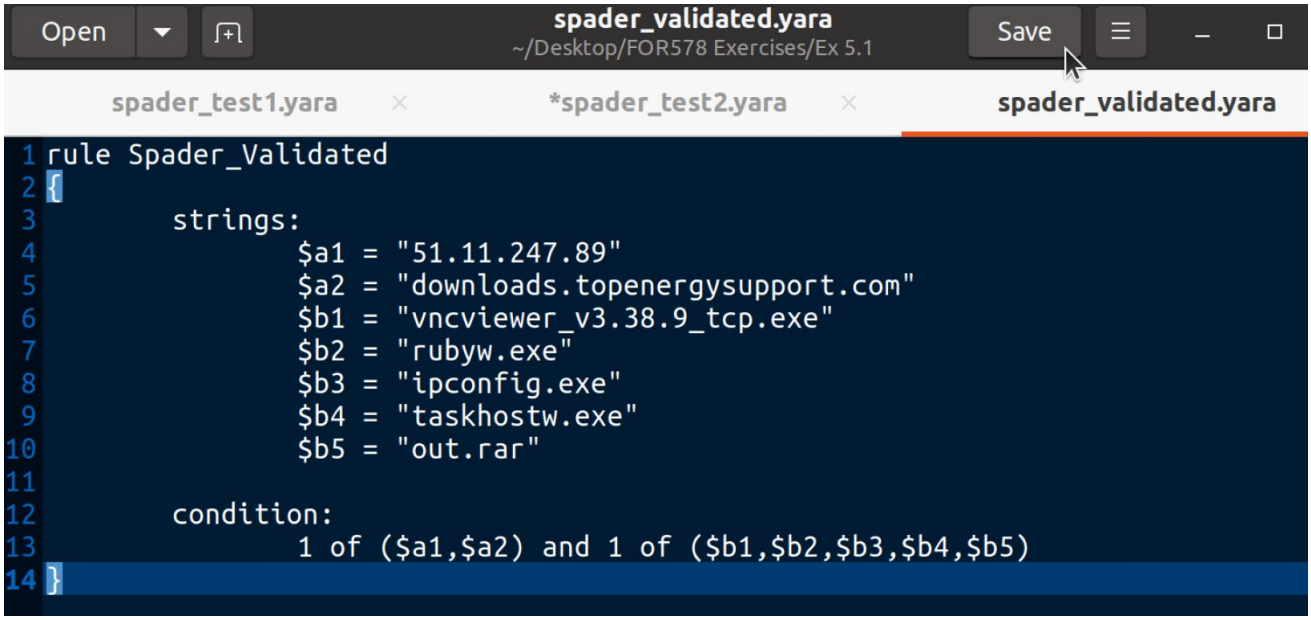
4. Create a single YARA rule that alerts when at least one indicator from each set of indicators above is observed.

Now that we know both rules work, we can create a single rule that alerts using 1 of each of the indicators from the two rules we created. You may have noticed that in the first rule, we used the $a variable for the strings, and in the second rule, we used the $b variable. You can choose any variables you like; however, this was done so that it is easy to identify which strings belong to which rule in our consolidated rule.

Navigate back to the Text Editor, create a new text file and name it "spader_validated.yara", and save it in the Ex 5.1 folder as we did before. In this file, put all the strings from the previous two files. (We can copy and paste the strings from the first two rules to save time.) To add a higher degree of confidence to the IOC, we will give it a condition of requiring one match from the $a variables and one match from the $b variables. Fill in the file as seen below:

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets
Technet24



Save the file, ensure it is in the Ex 5.1 folder, and run it against the memory image.

Execute the following command:

```
yara -s spader_validated.yara stsupport10-memory.dd4.001
```

```
sansforensics@siftworkstation: ~/Desktop/FOR578 Exercises/Ex 5.1
$ yara -s spader_validated.yara stsupport10-memory.dd4.001
```

After a few moments, matches should occur for all of our strings, as expected. Now you have a validated rule that contains known indicators, as well as additional ones that may be present in compromised files. We could action our findings in several ways. First, we should send our findings to our forensic analysts to ensure they identified all relevant information from this memory file. Additionally, we could pass these YARA rules (perhaps with additional editing to remove potentially noisy processes like ipconfig.exe and taskhostw.exe) to our defenders to deploy to our enterprise Endpoint Detection and Response (EDR) tool so we will be alerted if other machines are affected by these indicators. Of course, we would need to further test these rules before deploying to our entire enterprise to ensure no negative performance impacts.

```
sansforensics@siftworkstation: ~/Desktop/FOR578 Exercises/Ex 5.1
$ yara -s spader_validated.yara stsupport10-memory.dd4.001
Spader_Validated stsupport10-memory.dd4.001
0x5dd9f220:$a1: 51.11.247.89
0x534470b:$a2: downloads.topenergysupport.com
0x5344732:$a2: downloads.topenergysupport.com
0x1cc70f70:$a2: downloads.topenergysupport.com
0x2347a592:$a2: downloads.topenergysupport.com
0x2c92a7d4:$a2: downloads.topenergysupport.com
0x3bf6d8c7:$a2: downloads.topenergysupport.com
```

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets

Key Takeaways

- **The purpose of this lab was to help gain familiarity with YARA while also creating a validated IOC for the malware identified in the SpaderTech intrusion. Tailoring of the rules could be done to make them useful in various situations. For example, adding indicators, requiring more indicator matches, or removing indicators that weren't validated could make the rule more tailored for different environments.**

- **YARA rules represent one example of dissemination at the tactical level. While some CTI teams may write YARA rules themselves, others may simply provide information for forensic or malware analysts to write the rules. Either way, understanding how a YARA rule is created helps CTI analysts be better prepared to disseminate to tactical consumers.**

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets
Technet24

Exercise 5.2: Working with STIX and ATT&CK

Objectives

- Leverage scripts that can help us automatically pull STIX data from a TAXII server
- Identify STIX objects and custom properties
- Use identified data to produce a visualization

Scenario: We have identified multiple ATT&CK techniques used in the SpaderTech intrusion. By using a script from the ATT&CK repo that leverages STIX and TAXII, we can pull back the data sources used by various techniques. We can then create a visualization to help identify data sources that may be useful for us to collect on those techniques. Identifying techniques used by adversaries in intrusions against our network is a great input that CTI analysts can provide to our defenders. We can also help them understand the data sources they should monitor to detect those techniques.

Exercise Prep

You will use your SIFT VM for this exercise. Files for this exercise are in the **Ex 5.2** folder on your VM, though you can acquire all files needed for this exercise yourself from https://github.com/mitre-attack/attack-scripts.

This exercise is based on a blog by Andy Applebaum from the MITRE ATT&CK team (https://medium.com/mitre-attack/visualizing-attack-f5e1766b42a6)

You will also use the website: **rawgraphs.io**

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets

Exercise: Questions

1. What Python script from the MITRE ATT&CK scripts repo will help us pull ATT&CK techniques mapped to data sources?

   - _____

2. What does the following Python code do?

```
collection = Collection("https://cti-
taxii.mitre.org/stix/collections/95ecc380-afe9-11e4-9b6c-
751b66dd541e/")
```

   - _____

3. What custom property in STIX does MITRE ATT&CK use to track data sources?

   - _____

4. Run the python script "`techniques_data_sources_vis.py`" from the command line. What does it output?
   - **i.** To do this you must be in the virtual environment, to get there use the following:
     Close out of the Text Editor where we viewed the Python code. Open a new terminal and execute each of the following commands in sequence:
     1. **cd Desktop/FOR578\ Exercises/Ex\ 5.2**
     2. **cd attack-scripts/**
     3. **python3 -m venv env**
     4. **source env/bin/activate**
     5. **cd scripts**

   - _____

5. Which data sources from our dataset could help us cover the largest number of techniques? Determine this by creating a Circular Dendrogram mapping techniques to data sources using rawgraphs.io.

   - _____
   - _____

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets
Technet24

Exercise: Questions with Step-by-Step

Launch the SIFT VM, open a terminal, and change directories to the Ex 5.2 folder with the following command:

```
cd Desktop/FOR578\ Exercises/Ex\ 5.2
```

Execute the `ls` command and observe that there is a folder called "attack-scripts". This has been downloaded for you from https://github.com/mitre-attack/attack-scripts. If we change directories to that folder and execute another `ls` command, we observe several files and folders, as shown below.

```
sansforensics@siftworkstation: ~/Desktop/FOR578 Exercises/Ex 5.2
$ cd Desktop/FOR578\ Exercises/Ex\ 5.2
bash: cd: Desktop/FOR578 Exercises/Ex 5.2: No such file or directory
sansforensics@siftworkstation: ~/Desktop/FOR578 Exercises/Ex 5.2
$ ls
attack-scripts
sansforensics@siftworkstation: ~/Desktop/FOR578 Exercises/Ex 5.2
$ cd attack-scripts/
sansforensics@siftworkstation: ~/Desktop/FOR578 Exercises/Ex 5.2/attack-scripts
$ ls
CHANGELOG.md     env     LICENSE.txt  README.md         scripts
CONTRIBUTING.md  layers  NOTICE.txt   requirements.txt
sansforensics@siftworkstation: ~/Desktop/FOR578 Exercises/Ex 5.2/attack-scripts
$
```

Next, execute `cd scripts` to change directories again, then `ls` the contents of the "scripts" folder. We observe multiple Python scripts in this folder, including one named "techniques_from_data_source.py".

```
sansforensics@siftworkstation: ~/Desktop/FOR578 Exercises/Ex 5.2/attack-scripts
$ cd scripts
sansforensics@siftworkstation: ~/Desktop/FOR578 Exercises/Ex 5.2/attack-scripts/scripts
$ ls
diff_stix.py  README.md                    techniques_data_sources_vis.py
layers        technique_mappings_to_csv.py  techniques_from_data_source.py
sansforensics@siftworkstation: ~/Desktop/FOR578 Exercises/Ex 5.2/attack-scripts/scripts
$
```

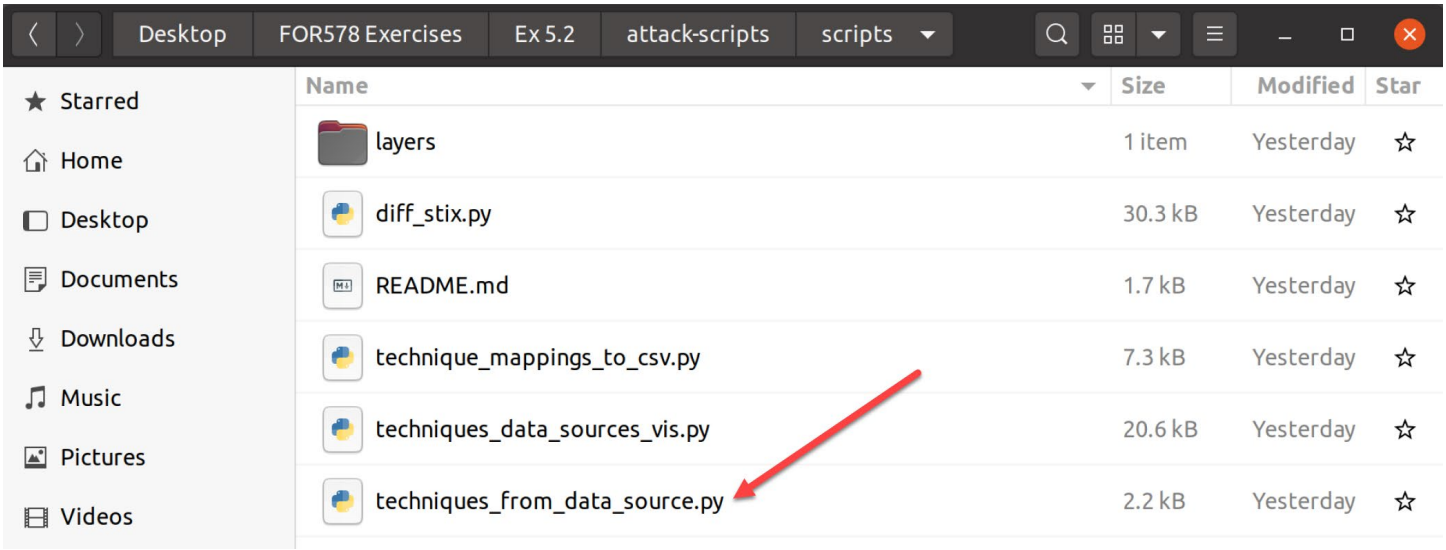
1. **What Python script from the MITRE ATT&CK scripts repo will help us pull ATT&CK techniques mapped to data sources?**

   - **techniques_from_data_source.py**

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets

In the Files explorer window, navigate to the "scripts" folder we just observed from the command line and observe that the "techniques_from_data_source.py" script is visible through the GUI as well as the command line.



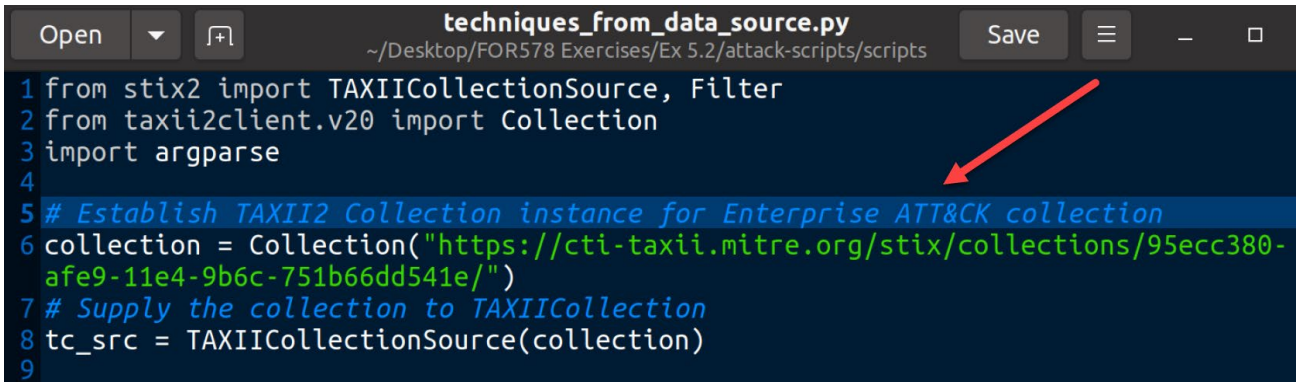
Double-click on the "techniques_from_data_source.py" file and it will automatically open in Text Editor. Here, we can see the Python script contents. Analyze this Python code to answer the following questions.

2. What does the following Python code do?

```
collection = Collection("https://cti-
taxii.mitre.org/stix/collections/95ecc380-afe9-11e4-9b6c-
751b66dd541e/")
```

- **<u>This Python code establishes a TAXII2 Collection instance for Enterprise ATT&CK collection.</u>**

This Python script is well-commented so it tells us exactly what this code is doing—it is connecting to the TAXII2 server hosted by MITRE if we run this code. This code is necessary to allow our VM to pull down the necessary STIX objects.



© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets
Technet24

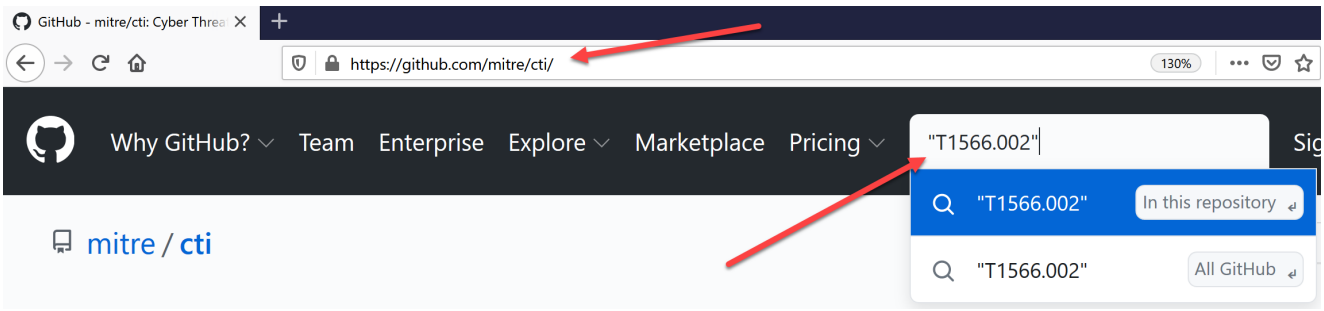
3. **What custom property in STIX does MITRE ATT&CK use to track data sources?**

- **x_mitre_data_sources**

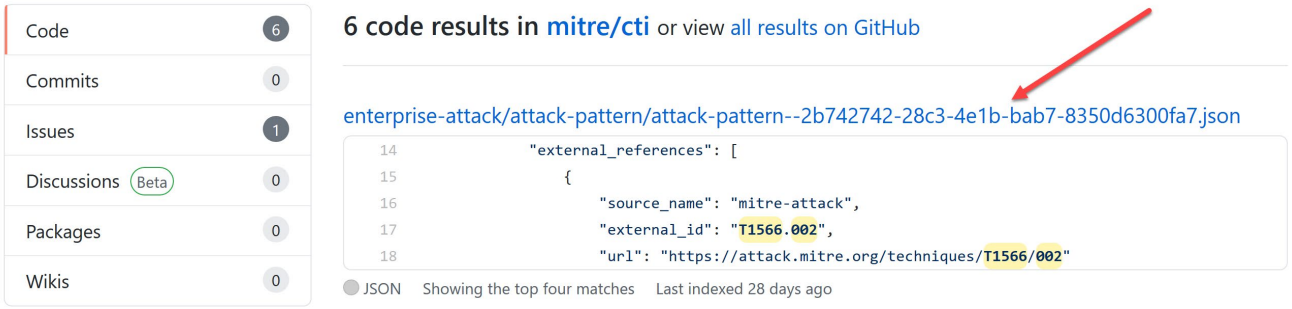
While STIX has many objects, sometimes organizations need custom properties to support their requirements. MITRE has created a STIX property named "x_mitre_data_sources" to track Data Sources that may be useful to help identify a technique or sub-technique. Any custom properties in STIX should begin with "x_", as we would learn by reviewing additional STIX documentation (https://stix2.readthedocs.io/en/latest/guide/custom.html#). We can directly observe this data source's property in the Python code on line 33.

```
28 def techniques(data_source):
29     """returns all techniques which contain the given data source."""
30
31     techs_with_data_src = tc_src.query([
32         Filter("type", "=", "attack-pattern"),
33         Filter("x_mitre_data_sources", "in", data_source)
34     ])
35
36     return techs_with_data_src
37
```

To investigate this property more, navigate to https://github.com/mitre/cti/, where we can directly view the STIX behind ATT&CK. For example, search on one of the sub-techniques we mapped in the SpaderTech intrusion, "T1566.002", which corresponds to Spearphishing Link. Select the option to search just "In this repository".



We should receive six results. Click on the first result.



© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets

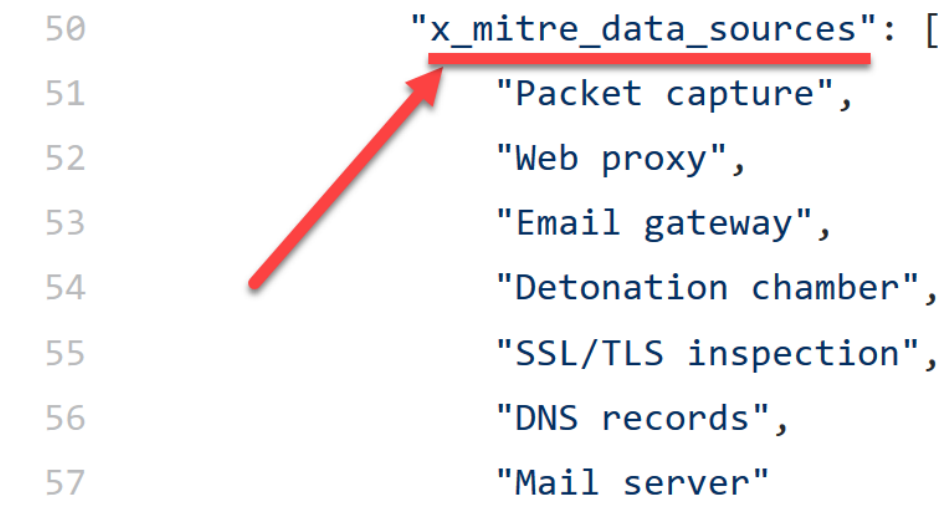
This should take us to the following URL—if it does not, you can navigate there directly: https://github.com/mitre/cti/blob/253622f36393e4aa012725f0ce428dcd275f5d20/enterprise-attack/attack-pattern/attack-pattern--2b742742-28c3-4e1b-bab7-8350d6300fa7.json

Observe that this is a STIX bundle that contains multiple objects, including "attack-pattern", which is used for ATT&CK technique and sub-techniques by MITRE.



```
{
    "type": "bundle",
    "id": "bundle--24bfb91a-84a1-46f7-bb38-0aa99cb34a95",
    "spec_version": "2.0",
    "objects": [
        {
            "id": "attack-pattern--2b742742-28c3-4e1b-bab7-8350d6300fa7",
            "description": "Adversaries may send spearphishing emails with a malicious
            "name": "Spearphishing Link",
            "created_by_ref": "identity--c78cb6e5-0c4b-4611-8297-d1b8b55e40b5",
            "object_marking_refs": [
                "marking-definition--fa42a846-8d90-4e51-bc29-71d5b4802168"
            ],
```

As we scroll down further to view additional STIX objects, observe the "x_mitre_data_sources" property, which has multiple values.



```
"x_mitre_data_sources": [
    "Packet capture",
    "Web proxy",
    "Email gateway",
    "Detonation chamber",
    "SSL/TLS inspection",
    "DNS records",
    "Mail server"
```

If we navigate to https://attack.mitre.org/techniques/T1566/002/, we observe those same values displayed under "Data Sources". This is because "behind the scenes", the ATT&CK website is using STIX. Many of the tools and websites we use, such as Threat Intelligence Platforms, may also be using STIX "in the background." As CTI analysts, it is helpful for us to understand the code behind what we use.

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets
Technet24

Phishing: Spearphishing Link

Other sub-techniques of Phishing (3)

Adversaries may send spearphishing emails with a malicious link in an attempt to gain access to victim systems. Spearphishing with a link is a specific variant of spearphishing. It is different from other forms of spearphishing in that it employs the use of links to download malware contained in email, instead of attaching malicious files to the email itself, to avoid defenses that may inspect email attachments.

All forms of spearphishing are electronically delivered social engineering targeted at a specific individual, company, or industry. In this case, the malicious emails contain links. Generally, the links will be accompanied

ID: T1566.002

Sub-technique of: T1566

Tactic: Initial Access

Platforms: Linux, Office 365, SaaS, Windows, macOS

Data Sources: DNS records, Detonation chamber, Email gateway, Mail server, Packet capture, SSL/TLS inspection, Web proxy

4. **Run the python script "`techniques_data_sources_vis.py`" from the command line. What does it output?**

- **Technique and data source mappings**

Now that we understand what STIX properties the Python script is using, and that it is pulling from the TAXII server, let's go ahead and actually run it!

Close out of the Text Editor where we viewed the Python code. Open a new terminal and execute each of the following commands in sequence:

- `cd Desktop/FOR578\ Exercises/Ex\ 5.2`
- `cd attack-scripts/`
- `python3 -m venv env`
- `source env/bin/activate`
- `cd scripts`

```
sansforensics@siftworkstation: ~
$ cd Desktop/FOR578\ Exercises/Ex\ 5.2
sansforensics@siftworkstation: ~/Desktop/FOR578 Exercises/Ex 5.2
$ cd attack-scripts/
sansforensics@siftworkstation: ~/Desktop/FOR578 Exercises/Ex 5.2/attack-scripts
$ python3 -m venv env
sansforensics@siftworkstation: ~/Desktop/FOR578 Exercises/Ex 5.2/attack-scripts
$ source env/bin/activate
(env) sansforensics@siftworkstation: ~/Desktop/FOR578 Exercises/Ex 5.2/attack-scripts
$ cd scripts
(env) sansforensics@siftworkstation: ~/Desktop/FOR578 Exercises/Ex 5.2/attack-scripts/scripts
$
```

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets

These commands set up and activate a virtual environment from which we can run the Python script. Note that your prompt now starts with "(env)", indicating you are in a virtual environment.

We are now ready to execute the Python script itself. Execute the following command:

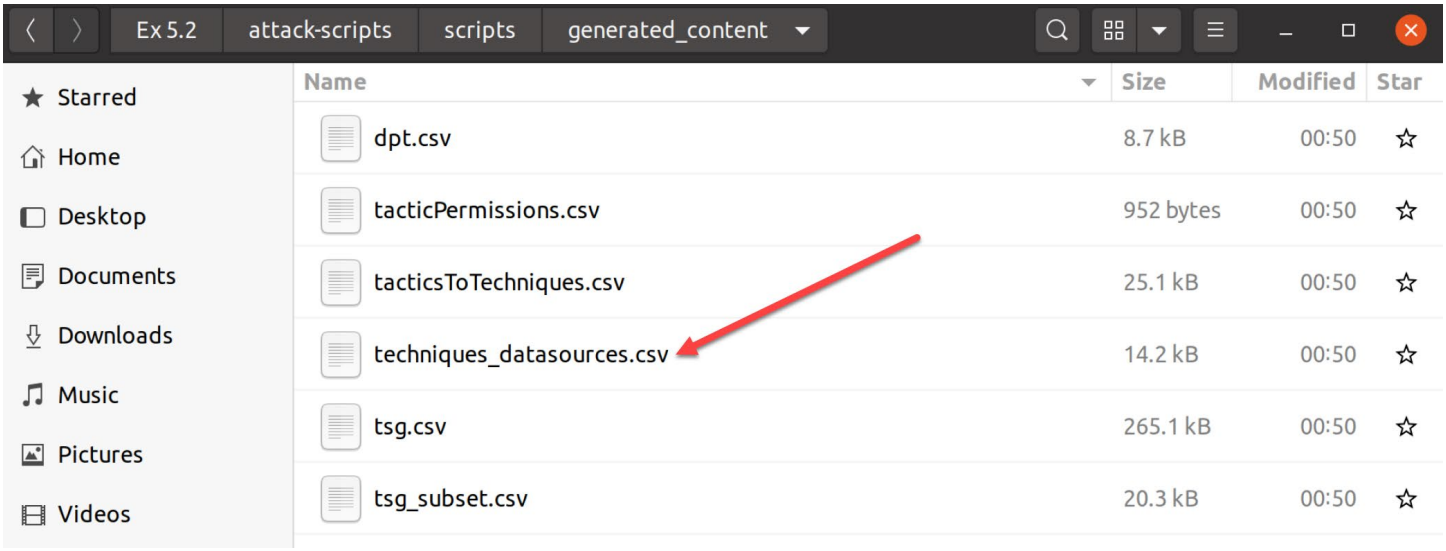
```
python3 techniques_data_sources_vis.py -v
```

Once it successfully runs, your screen should look like the below. As we know from examining the Python script, this script has connected out to the MITRE TAXII server and pulled down STIX.

```
(env) sansforensics@siftworkstation: ~/Desktop/FOR578 Exercises/Ex 5.2/attack-scripts/scripts
$ python3 techniques_data_sources_vis.py -v
establishing connection... done!
retrieving data |          | 100%
parsing data... done!
writing output to directory generated_content... done!

(env) sansforensics@siftworkstation: ~/Desktop/FOR578 Exercises/Ex 5.2/attack-scripts/scripts
$
```

Next, we want to examine the output from the script. In your Files explorer, navigate to the Ex 5.2 folder > attack-scripts > scripts > generated_content. Observe that there is a .csv file there named "techniques_datasources.csv".



Double-click "techniques_datasources.csv", and when LibreOffice opens, simply accept the defaults and click OK. In LibreOffice, we can observe that the Python script pulled down technique names and mapped each one to a corresponding data source.

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets
Technet24

	A	B
1	technique	data source
2	network device configuration dump	netflow/enclave netflow
3	network device configuration dump	network protocol analysis
4	rommonkit	netflow/enclave netflow
5	rommonkit	network protocol analysis
6	snmp (mib dump)	netflow/enclave netflow
7	snmp (mib dump)	network protocol analysis
8	data from configuration repository	netflow/enclave netflow

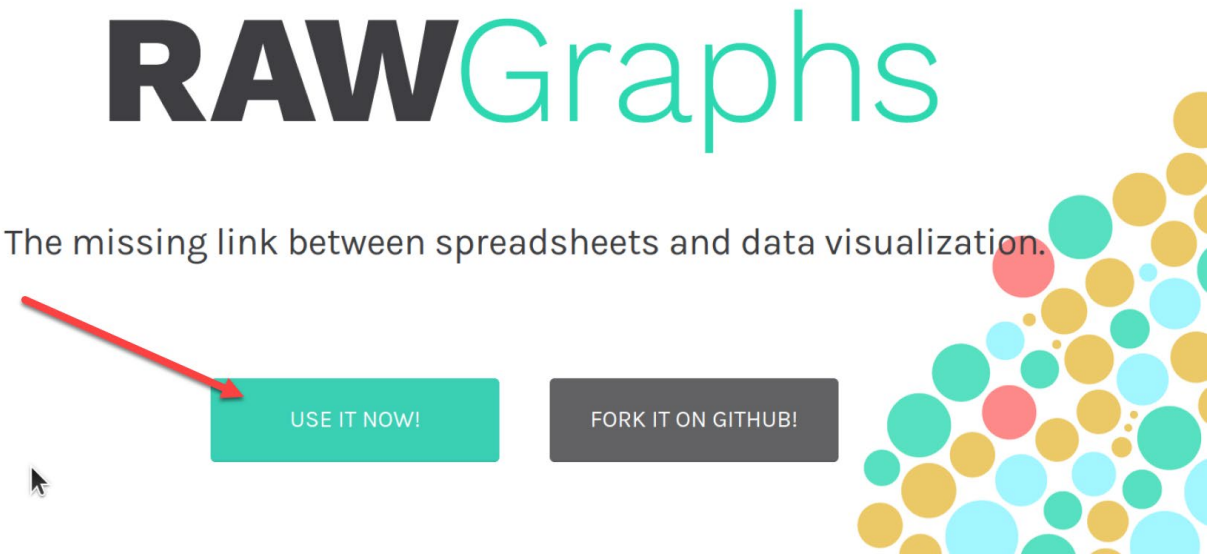
If we wanted to, we could further filter these techniques to just the ones observed in our SpaderTech intrusion, but for now, this is a useful list we could pass to our defenders so they understand what data sources (in bulk) can be used to try to identify the different techniques.

5. **Which data sources from our dataset could help us cover the largest number of techniques? Determine this by creating a Circular Dendrogram mapping techniques to data sources using rawgraphs.io.**

- **Windows event logs, netflow/enclave netflow, network protocol analysis, and DLL monitoring**

Visualizations can be a great way to express a lot of data at once, as we've already observed. We want to create a visualization that will easily show what data sources cover the most techniques. To do this, we can use the free website rawgraphs.io.

In your VM, open up Firefox and navigate to the website rawgraphs.io, then select "Use it now!"

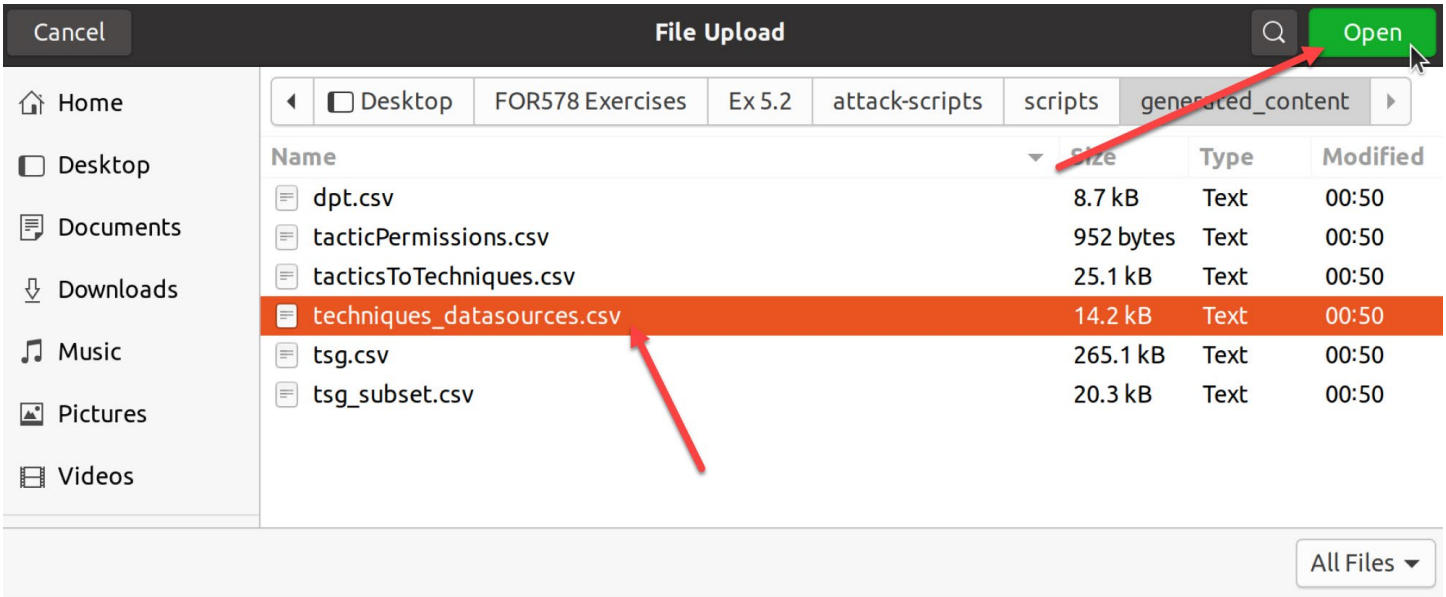


In the "Load your data" prompt, select "Upload a file" in the left menu and then click in the box on the right to navigate to the file we want to analyze from our Ex 5.2 folder, "techniques_datasources.csv". The full path of this file is Desktop/FOR578 Exercises/Ex 5.2/attack-scripts/scripts/generated_content. Select "Open".

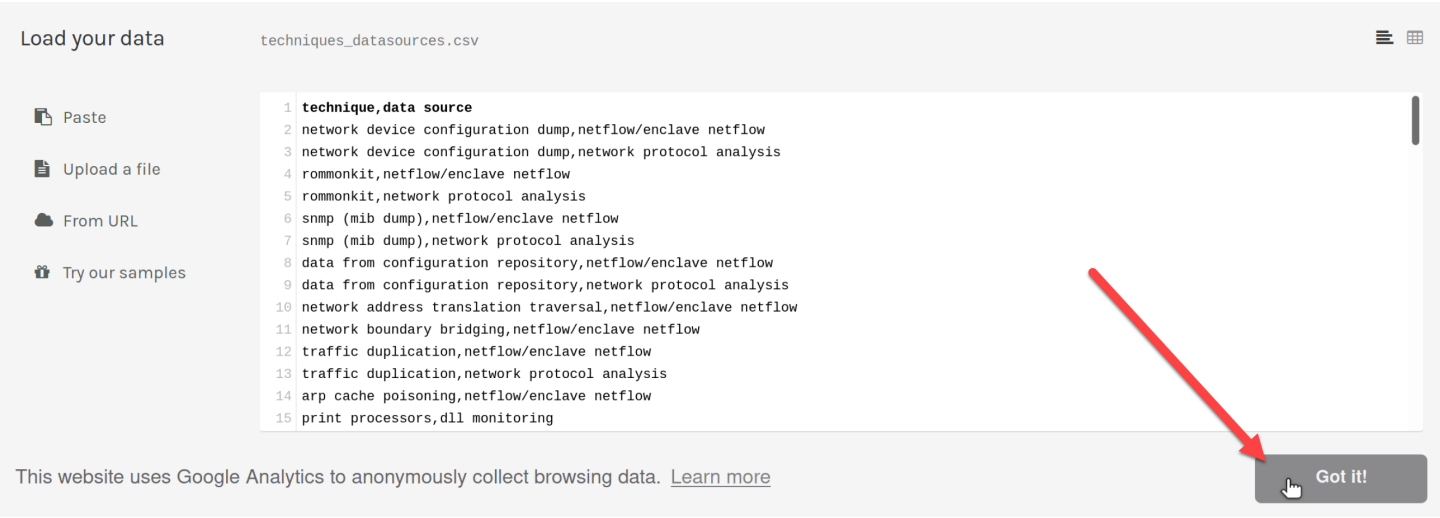
© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets





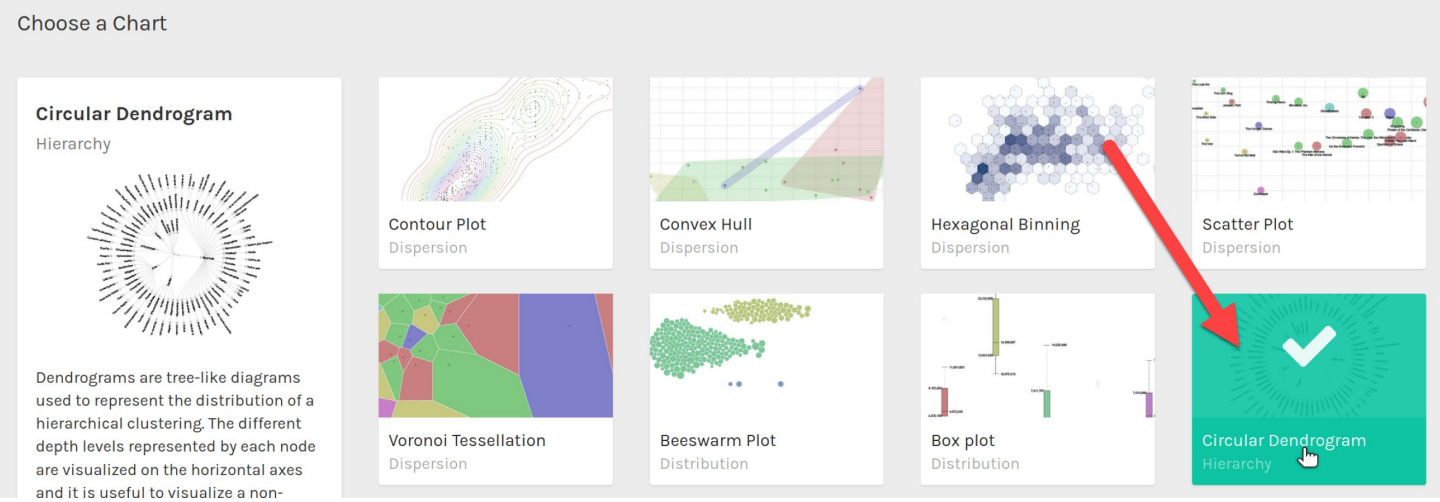
Now we should see our data loaded in RawGraphs. Click "Got it!" in the lower right to proceed.



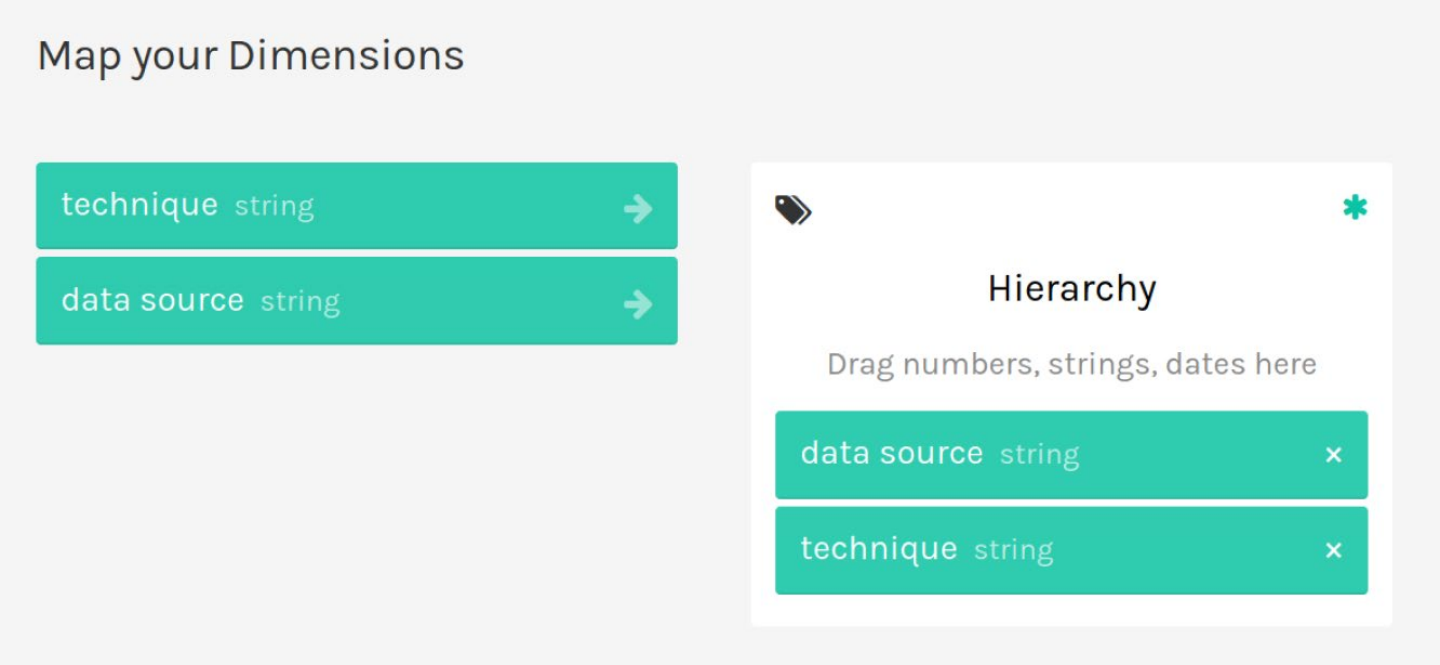
© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets
Technet24

Next, scroll down to the "Choose a Chart" section. You can experiment with various chart types, but we will select "Circular Dendrogram".



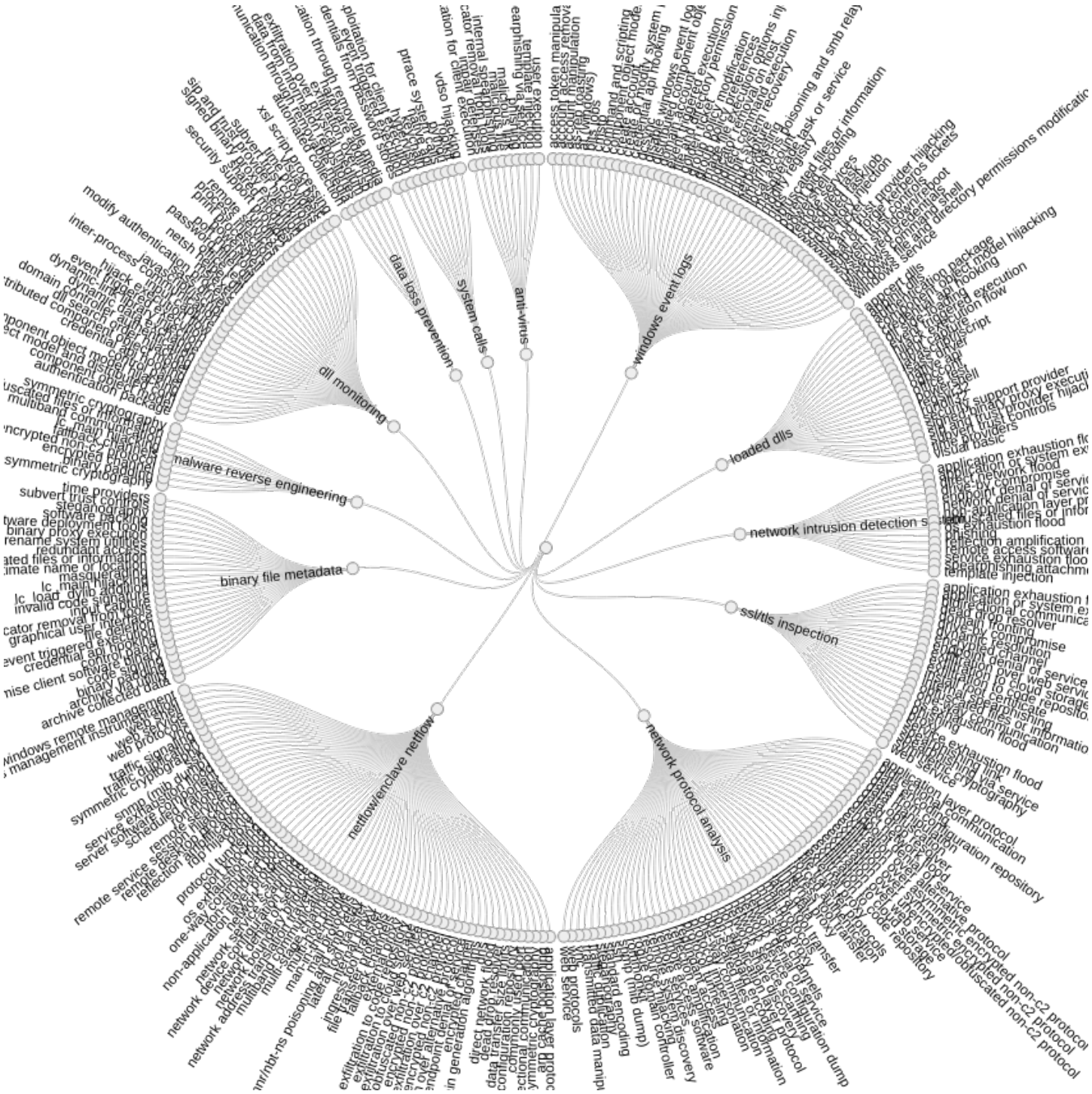
Continue scrolling down the page. Now we come to the section "Map your Dimensions" where we have to tell RawGraphs how we want our data organized. Drag the "technique" field from the left into the "Hierarchy" box on the right. Next, drag the "data source" field above it. When completed, your window should look like the one below.



© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets

Now we scroll down to "Customize your Visualization". Here we observe that we have a neat visualization—the data sources are in the middle, and the ATT&CK techniques those data sources can be identified with are on the outside. From this visualization, we can observe that four data sources seem to cover the most techniques: Windows event logs, netflow/enclave netflow, network protocol analysis, and DLL monitoring. Of course, you might have different answers. If you choose, you can use the options in RawGraphs to further customize your visualization.



© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets

Technet24

Exercise: Key Takeaways

- **We used a Python script created by MITRE to automatically pull technique-to-data-source mappings from the MITRE TAXII server. We identified STIX objects and a custom property and also observed that STIX is "behind the scenes" of the ATT&CK website as well as many CTI tools we use.**

- **Using the data we automatically pulled, we created a visualization that helped us determine which data sources may be most useful to help us identify ATT&CK techniques.**

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets

This page intentionally left blank.

https://t.me/learningnets

Technet24

Exercise 5.3: Building a Group Heatmap

Objectives

- Apply Excel PivotTables to data to produce meaningful metrics
- Learn how to produce group heatmaps
- Identify intelligence gaps and patterns from group trending

Scenario: With an understanding of the PINKIEPIE, DERPYHOOVES, and RAINBOWDASH Activity Groups, we want to be able to apply ongoing knowledge in the CTI team and across the DFIR and SOC teams to create a Group Heatmap to communicate the current threat landscape to management and identify any noteworthy patterns or intelligence gaps that may now need to be filled.

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets

Exercise – Tasks

1. Using the group definition for DERPYHOOVES, your fellow analysts have completed a historical evaluation of documented intrusions against your network. This evaluation resulted in recommendations for the attribution of a number of incidents to be changed to DERPYHOOVES.

Your company tracks analysis of intrusion attempts in a ticketing system. On your request, the administrators of the ticketing software have provided you with a dump of all ticketed intrusion attempts over the past year, their respective date, and group attribution. A copy of this file is on the class USB under the **Ex 5.3** folder named "*Intrusion Ticket Dump.csv"*.

Open the CSV in Microsoft Excel. In order to perform differential analysis on the group trends before and after knowledge of DERPYHOOVES is applied, create a copy of the data into a second sheet named "updated" and save the file as a Microsoft Excel document (xlsx). In your "updated" sheet, change the attribution of the following tickets to DERPYHOOVES:

45, 46, 56, 57, 58, 75, 76, 78, 79, 81

2. Create a group heatmap of the *original* data by creating a PivotTable in a new sheet with columns representing groups, and rows representing the month of the year. Colorize the group monthly data, column totals, and row totals each separately using the green-to-red "conditional formatting" feature of Excel.

3. We desire a measurement of relative activity levels as measured by distinct adversaries attempting intrusions against our organization each month. This measurement can provide the overall percentage of known adversaries targeting us each month. Enhance the PivotTable by adding a column to the far right with a count of distinct groups active for each month. For instance, if only PINKIEPIE, RAINBOWDASH, and FLUTTERSHY are active in September, then the number of distinct groups active would be 3.

We also desire a measurement of the overall activity level for each group across the history of our dataset in terms of the number of months each is active. If expressed as a percentage, this measurement can provide the probability of observing each group in any given month. Enhance the PivotTable by adding a row below the table providing a count of the number of total months in the dataset each group was active. For example, if APPLEBLOOM is active in only October and November, the number of months active for this group will be 2.

4. Repeat steps 2–3 for the "updated" sheet that includes DERPYHOOVES attribution.

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets
Technet24

Exercise: Questions

1. Compare the original and updated heatmaps.

How has the identification of DERPYHOOVES changed the heatmap overall between the original and updated versions?

- _____

What do these changes mean for the company?

- _____

What do these changes mean for CTI analysts?

- _____

2. Does DERPYHOOVES seem to show an activity pattern aligning to any other tracked group? Describe any such pattern alignments, and formulate a hypothesis as to what might explain each.

- _____

_____

_____

_____

_____

Does this pattern suggest any specific intelligence gaps? Explain.

- _____

_____

_____

_____

3. One group seems to demonstrate very reliable operations on a monthly basis. Which group is that?

- _____

Are there any exceptions to this pattern?

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets

- _____

_____

4. The month of August is interesting. It is different from the other months in at least two ways. What are they?

- _____

_____

Formulate a hypothesis as to what might explain this.

- _____

_____

What steps would be necessary to validate this hypothesis?

- _____

_____

_____

_____

_____

_____

5. Look at the month of April. In terms of the other group activity that month, why might the activity for APPLEBLOOM, DERPYHOOVES, and Pending Attribution be significant?

- _____

_____

_____

_____

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets

Technet24

Exercise: Tasks with Step-by-Step

For this exercise, you will use Microsoft Excel on any currently supported Windows operating system.

NOTE: The solutions and screenshots provided were collected from a Windows 10 operating system running Microsoft Excel 2016. Different operating systems and Office versions may have interface differences that do not precisely align with what is displayed in the solution provided below.

Complete the tasks below to be able to answer the questions:

1. Using the group definition for DERPYHOOVES, your fellow analysts have completed a historical evaluation of documented APT intrusions against your network. This evaluation resulted in recommendations for the attribution of a number of incidents to be changed to DERPYHOOVES.

Your company tracks analysis of intrusion attempts in a ticketing system. On your request, the administrators of the ticketing software have provided you with a dump of all ticketed intrusion attempts over the past year, their respective date, and group attribution. A copy of this file is on the class USB under "*Exercises/Ex 5.3"* named "*Intrusion Ticket Dump.csv."*

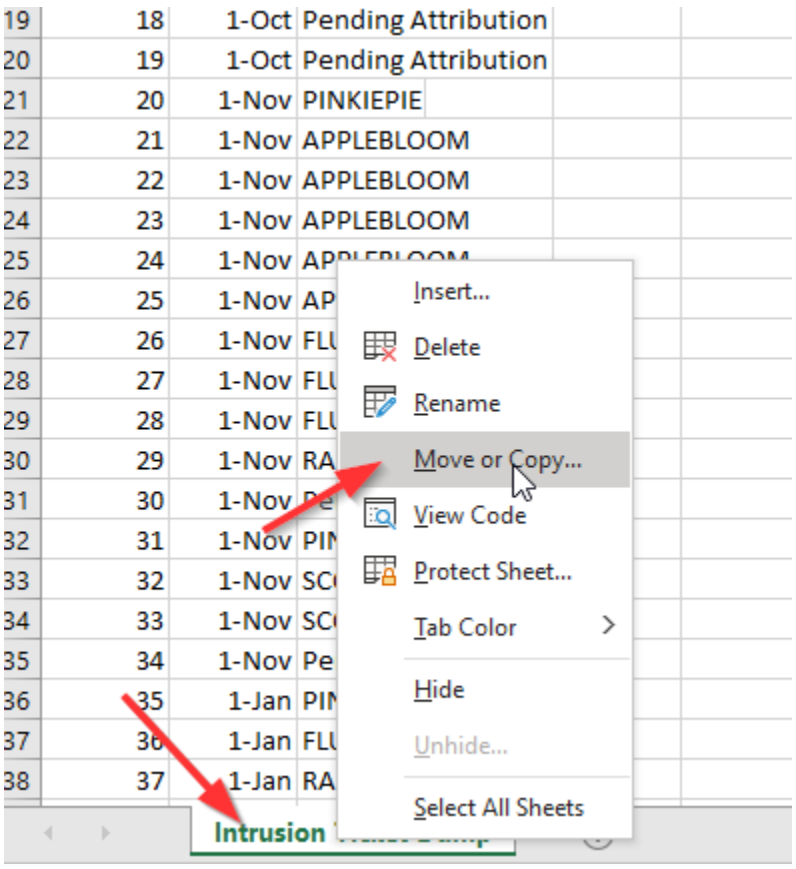
Open the CSV in Microsoft Excel. In order to perform differential analysis on the group trends before and after knowledge of DERPYHOOVES is applied, create a copy of the data into a second sheet named "updated" and save the file as a Microsoft Excel document (xlsx). In your "updated" sheet, change the attribution of the following tickets to DERPYHOOVES:

45, 46, 56, 57, 58, 75, 76, 78, 79, 81

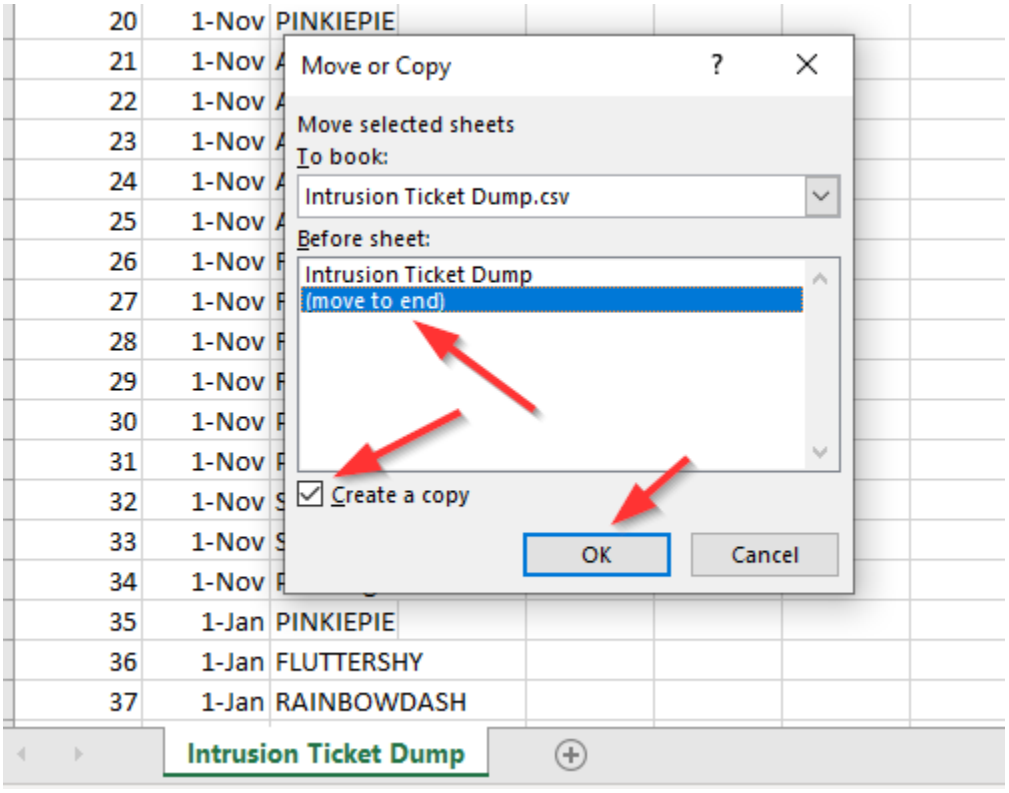
© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets

After double-clicking on the CSV file, you should see the current sheet (named "Intrusion Ticket Dump") at the bottom of the window. Right-click on this; select "Move or Copy."



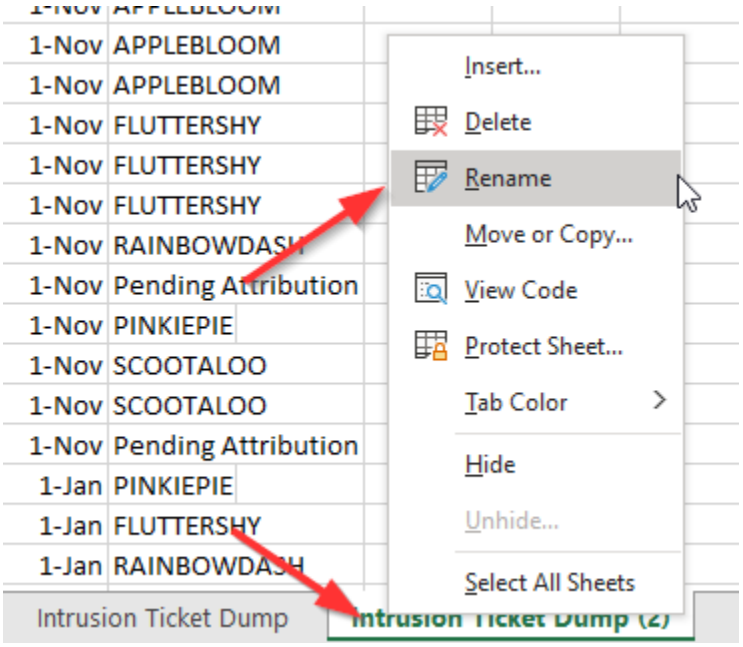
Highlight "(move to end)," check "Create a copy," and click "OK."



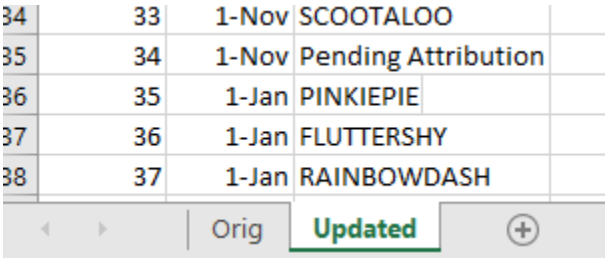
© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets
Technet24

It might also be helpful to rename the tabs using “Rename” in the right-click menu.

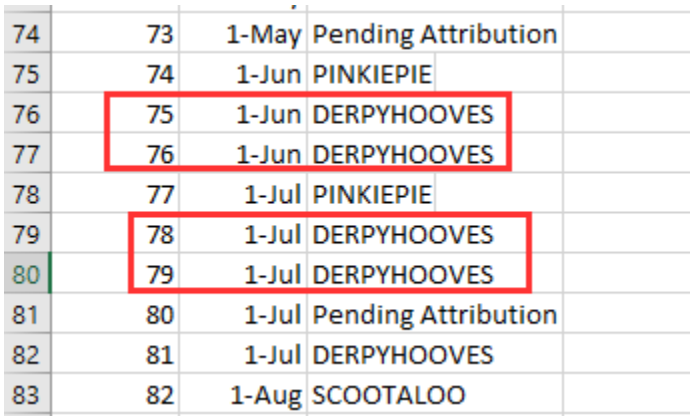


Below, the tabs are renamed “Orig” (which will not be modified) and “Updated” (which will).



At this point, save as a “.xslx” Excel document prior to proceeding.

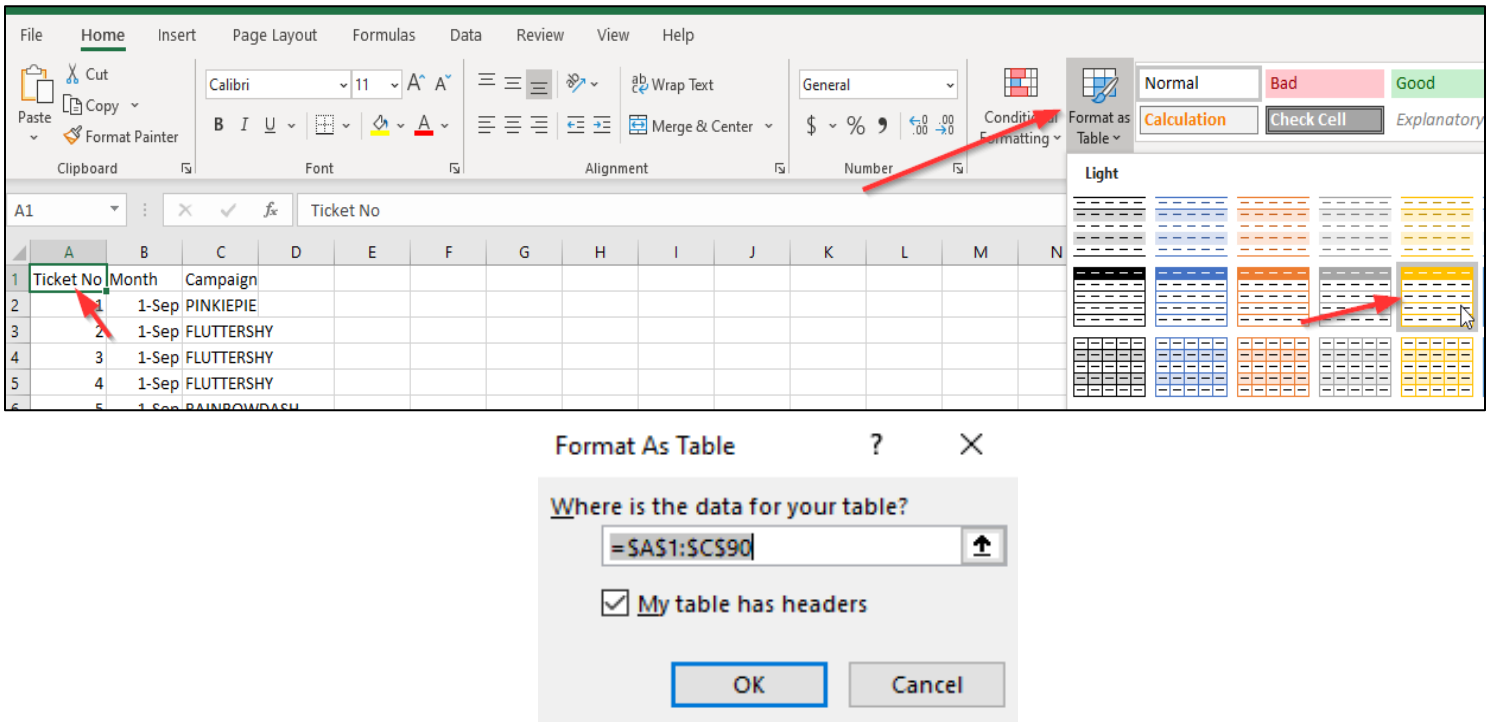
In the “Updated” tab, at each of the indicated ticket numbers (45, 46, 56, 57, 58, 75, 76, 78, 79, 81), in the “Campaign” column, change the text “Pending Attribution” to “DERPYHOOVES.” (Our analysts have labeled our activity groups as Campaigns, we will educate them on the difference later, but for now, we will refer to campaigns and groups interchangeably for this exercise.)



© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets

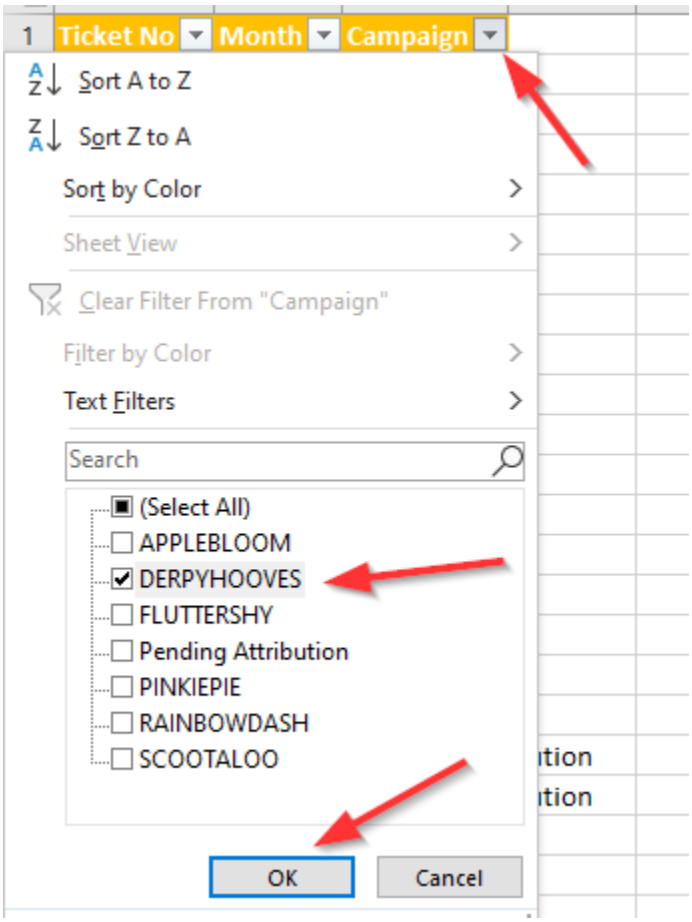
To verify all of the associated ticket numbers were changed, select the first cell (Ticket No) and choose Format as Table and select a preferred style. Then click OK on the default cell range ($A$1:$C$90).



Now scroll to the top of the table and use the Campaign autofilter to only display DERPYHOOVES rows.

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets
Technet24



Each of the tickets whose attribution has been changed to DERPYHOOVES should be displayed.

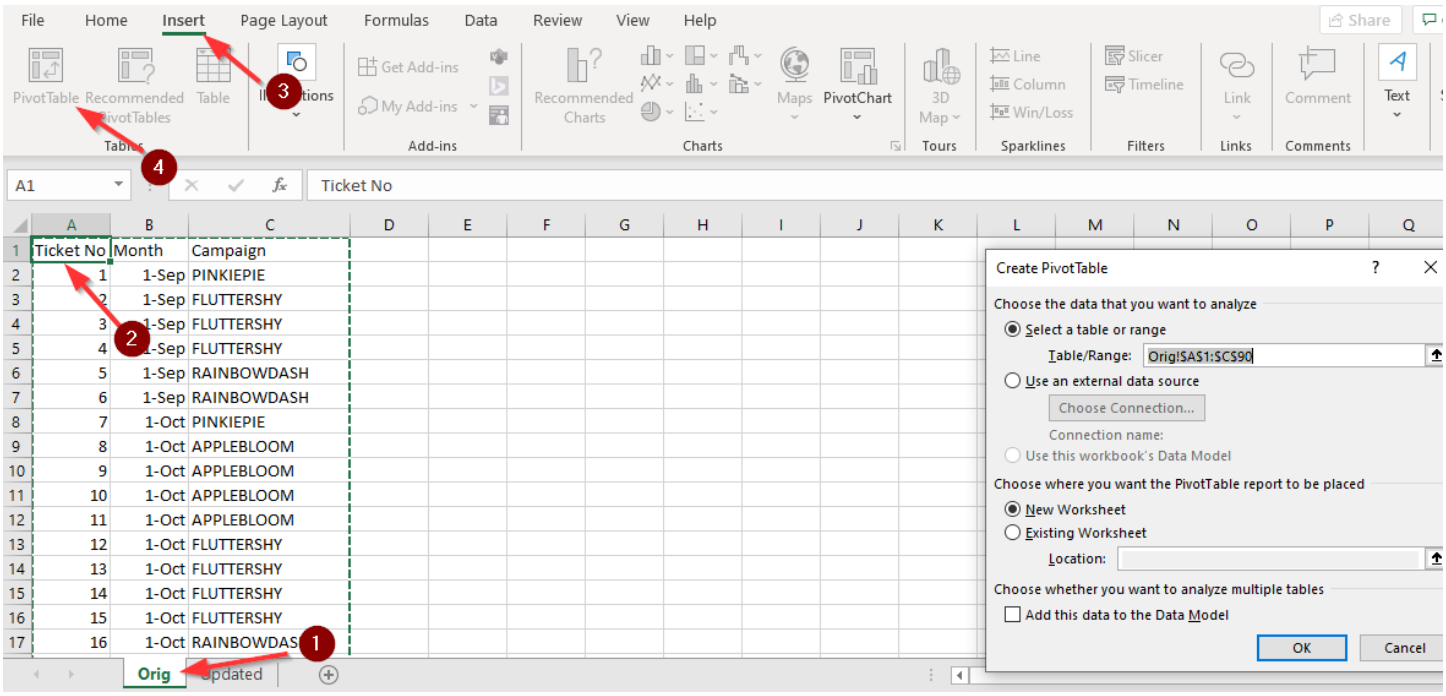
	A	B	C
1	Ticket No	Month	Campaign
46	45	1-Feb	DERPYHOOVES
47	46	1-Feb	DERPYHOOVES
57	56	1-Mar	DERPYHOOVES
58	57	1-Mar	DERPYHOOVES
59	58	1-Mar	DERPYHOOVES
76	75	1-Jun	DERPYHOOVES
77	76	1-Jun	DERPYHOOVES
79	78	1-Jul	DERPYHOOVES
80	79	1-Jul	DERPYHOOVES
82	81	1-Jul	DERPYHOOVES

2. Create a group heatmap of the *original* data by creating a PivotTable in a new sheet with columns representing groups and rows representing the month of the year. Colorize the group monthly data, column totals, and row totals each separately using the green-to-red "conditional formatting" feature of Excel.

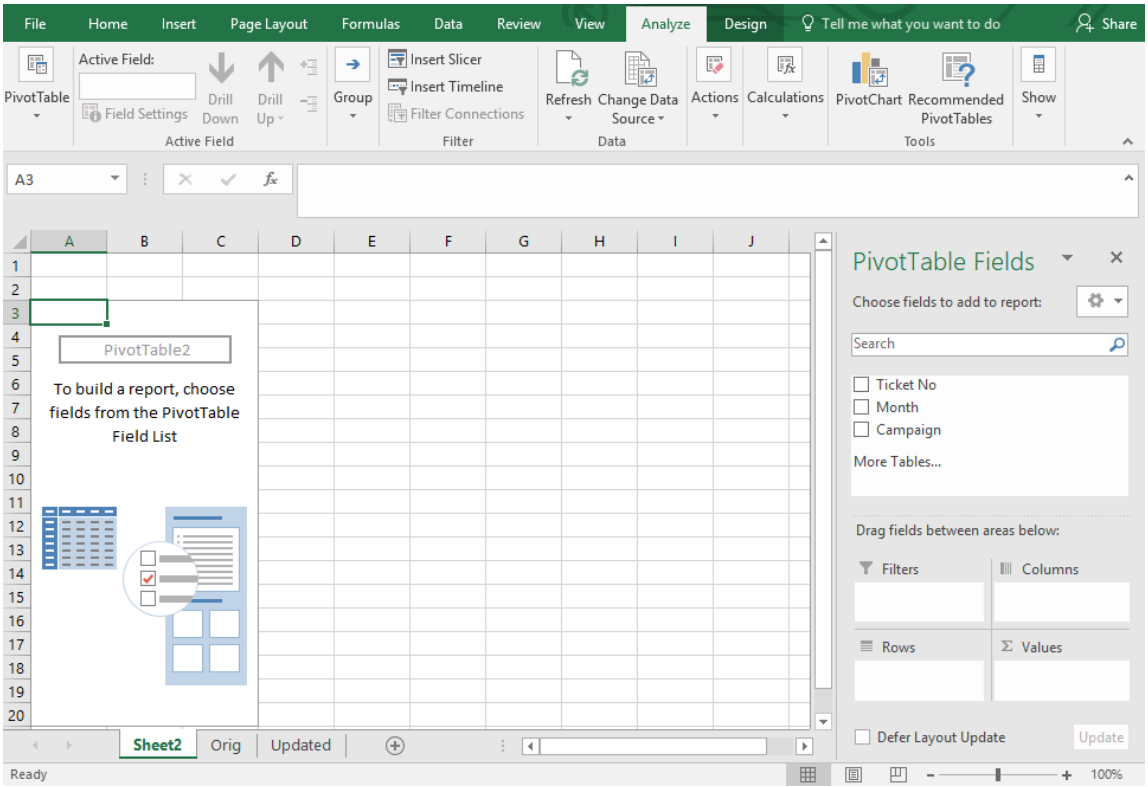
In the "Orig" tab (1), select a cell with data populated (2). In the "Insert" tab (3) at the top left, select PivotTable (4).

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets



Accept the defaults. A new, empty PivotTable will appear, as illustrated below.

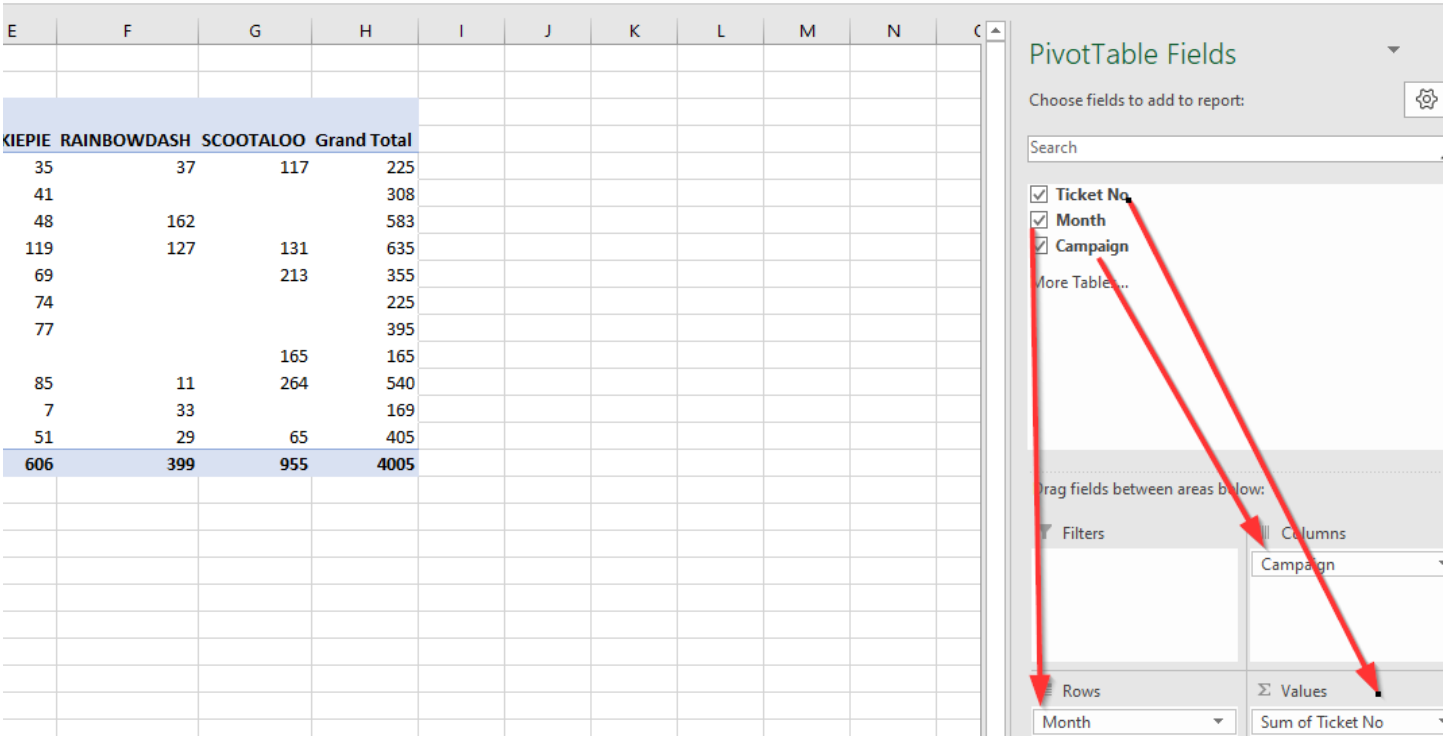


Drag “Month” into the “Rows” field in the right panel. Drag “Campaign” into “Columns” and “Ticket No” into “Values.”

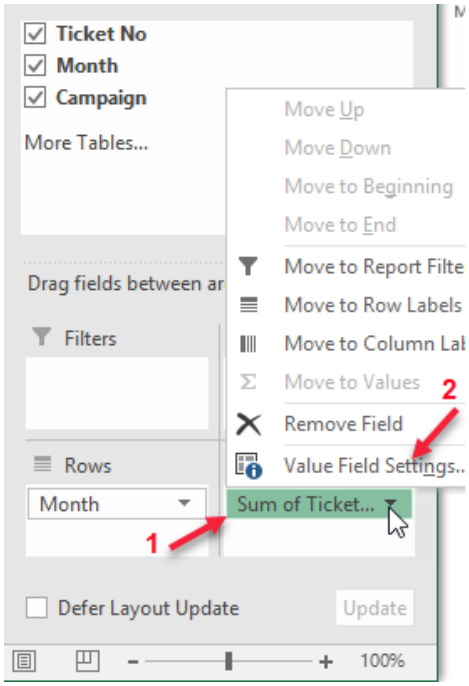
© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets

Technet24

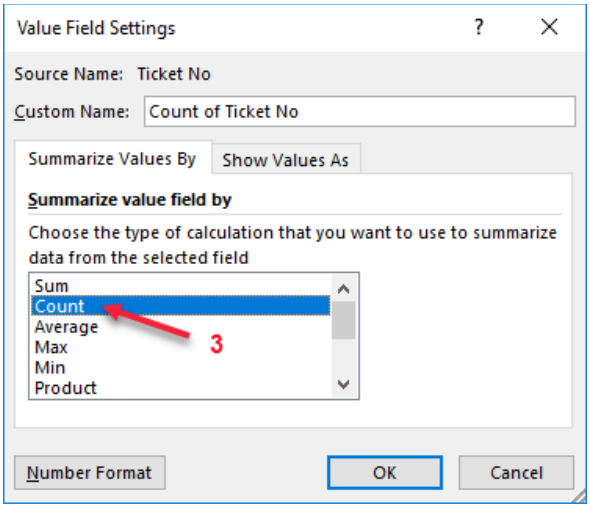


The default calculation for numerical values in the "Values" section is "Sum." This means the ticket numbers will be added together. What we want is the number of tickets, so we have to change this to "Count." Click on "Sum of Ticket…" (1) and select "Value Field Settings…" (2). Change it from Sum to Count (3).



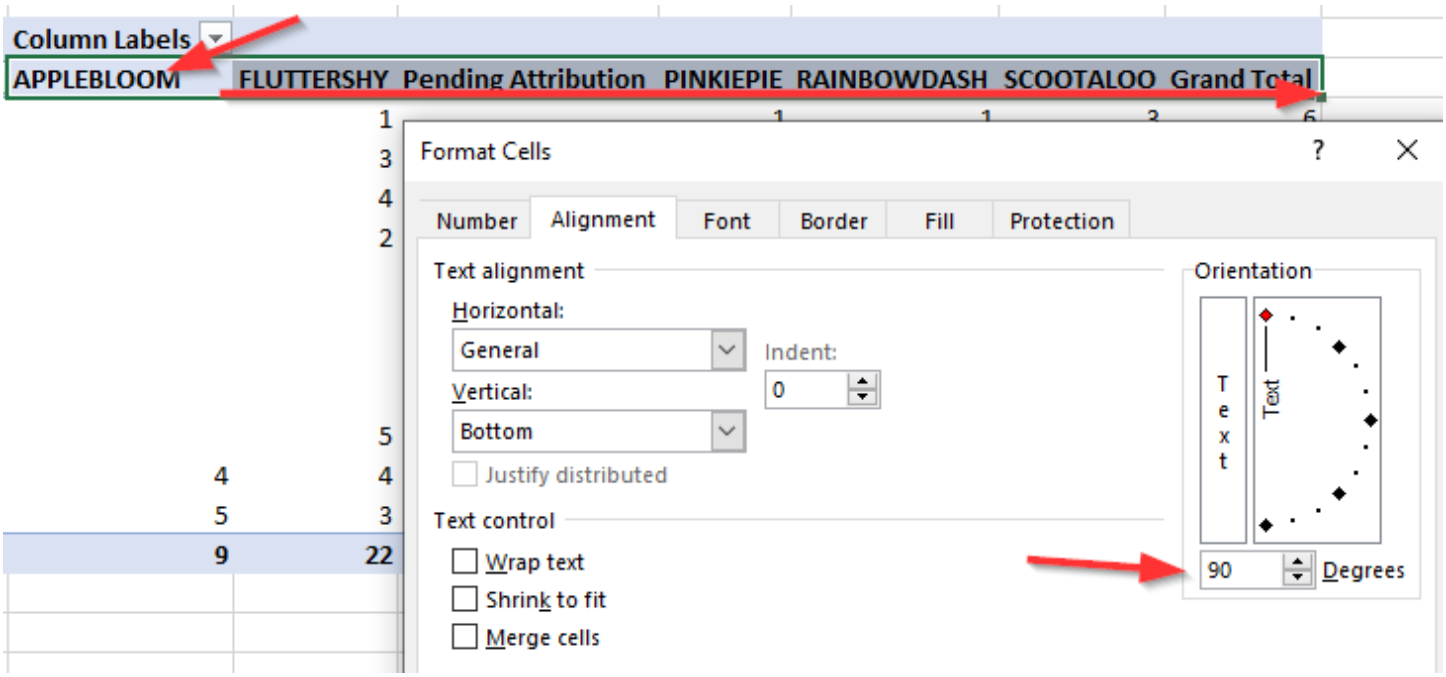
© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets



Some minor formatting changes, which can significantly improve legibility of the data and interpreting later questions, are recommended. Specifically:

- Rotate text for the column headers. To do this, highlight all of the group name headers, right-click, select "Format Cells," click the Alignment tab, and set "Orientation" on the right to "90 degrees."



- Minimize the width of the columns. We can do this by double-clicking between each column, or by manually resizing them.
- Relocate the "Pending Attribution" column to the right, just to the left of "Grand Total" by right-clicking on "Pending Attribution" and choose "Move" > "Move 'Pending Attribution' to End."

© 2021 Robert M. Lee and SANS Institute

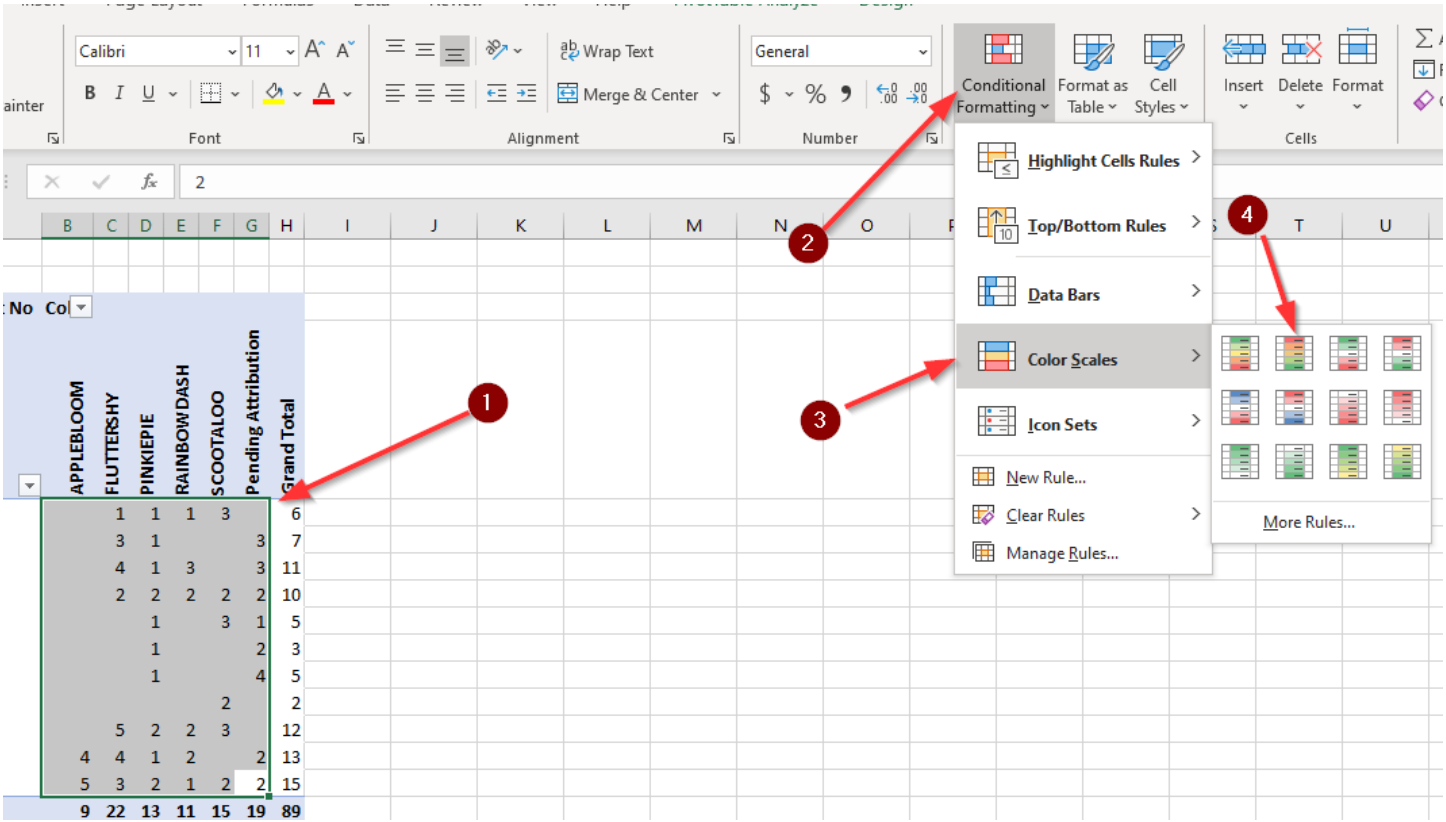
https://t.me/learningnets
Technet24

Count of Ticket No	Column Labels						
Row Labels	APPLEBLOOM	FLUTTERSHY	PINKIEPIE	RAINBOWDASH	SCOOTALOO	Pending Attribution	Grand Total
1-Jan		1	1	1	3		6
1-Feb		3	1			3	7
1-Mar		4	1	3		3	11
1-Apr		2	2	2	2	2	10
1-May			1		3	1	5
1-Jun			1			2	3
1-Jul			1			4	5
1-Aug					2		2
1-Sep		5	2	2	3		12
1-Oct	4	4	1	2		2	13
1-Nov	5	3	2	1	2	2	15
Grand Total	**9**	**22**	**13**	**11**	**15**	**19**	**89**

We will use *conditional formatting* to automatically create a *heatmap* of the data in the table. To apply conditional formatting to an area, select the data to be formatted (1), followed by the desired formatting style from the Conditional Formatting dropdown (2). Conditional formatting will colorize each cell according to its relative value among the set of cells highlighted, allowing for the easy creation of what are known as "heatmaps." Start with the values for each group, for each month. Select the Color Scale (3) in the first row, second column labeled "Red – Yellow – Green Color Scale" (4).

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets



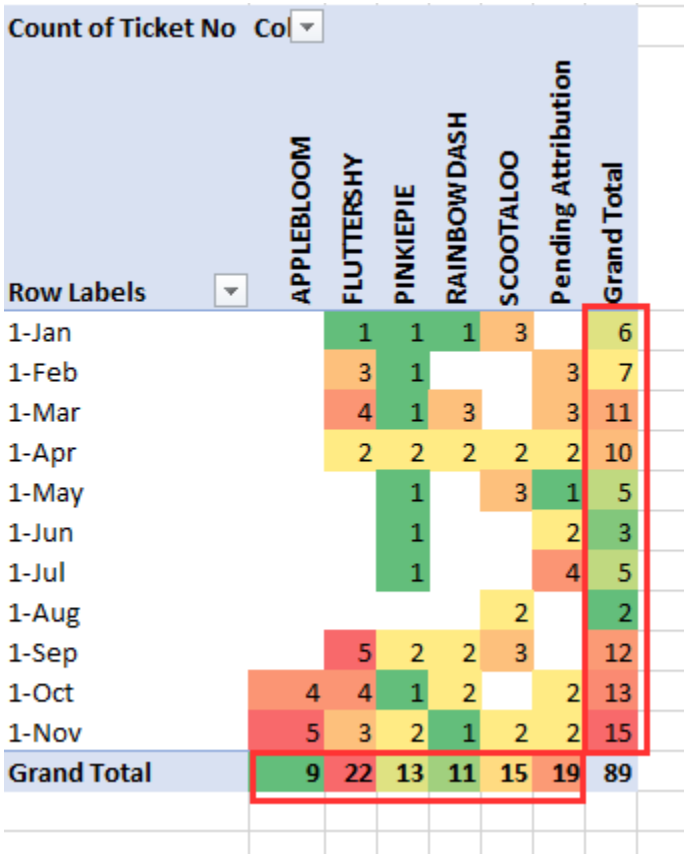
After this step, you should see the table look like the one below, with all attributions and months conditionally formatted, but the total row and column still unformatted.

Count of Ticket No Co	APPLEBLOOM	FLUTTERSHY	PINKIEPIE	RAINBOWDASH	SCOOTALOO	Pending Attribution	Grand Total
1-Jan		1	1	1	3		6
1-Feb		3	1			3	7
1-Mar		4	1	3		3	11
1-Apr		2	2	2	2	2	10
1-May			1		3	1	5
1-Jun			1			2	3
1-Jul			1			4	5
1-Aug					2		2
1-Sep		5	2	2	3		12
1-Oct	4	4	1	2		2	13
1-Nov	5	3	2	1	2	2	15
Grand Total	9	22	13	11	15	19	89

Repeat this for the Grand Total column by itself, and again for the Grand Total row. This will colorize each of these sets of cells independently from the other sets of cells that have been colorized.

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets
Technet24



Count of Ticket No	Col						
Row Labels	APPLEBLOOM	FLUTTERSHY	PINKIEPIE	RAINBOWDASH	SCOOTALOO	Pending Attribution	Grand Total
1-Jan		1	1	1	3		6
1-Feb		3	1			3	7
1-Mar		4	1	3		3	11
1-Apr		2	2	2	2	2	10
1-May			1		3	1	5
1-Jun			1			2	3
1-Jul			1			4	5
1-Aug					2		2
1-Sep		5	2	2	3		12
1-Oct	4	4	1	2		2	13
1-Nov	5	3	2	1	2	2	15
Grand Total	**9**	**22**	**13**	**11**	**15**	**19**	**89**

Optionally, replace the labels of the total row/column and the column header for the months displayed to be more descriptive than simply “Grand Total” and “Row Labels,” respectively. You may also adjust the color scheme of the PivotTable to your liking. The final version should look like the screenshot below.

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets

Count of Ticket No	Col							
Row Labels	APPLEBLOOM	FLUTTERSHY	PINKIEPIE	RAINBOWDASH	SCOOTALOO	Pending Attribution	Total
1-Jan		1	1	1	3		6
1-Feb		3	1			3	7
1-Mar		4	1	3		3	11
1-Apr		2	2	2	2	2	10
1-May			1		3	1	5
1-Jun			1			2	3
1-Jul			1			4	5
1-Aug					2		2
1-Sep		5	2	2	3		12
1-Oct	4	4	1	2		2	13
1-Nov	5	3	2	1	2	2	15
Total	**9**	**22**	**13**	**11**	**15**	**19**	**89**

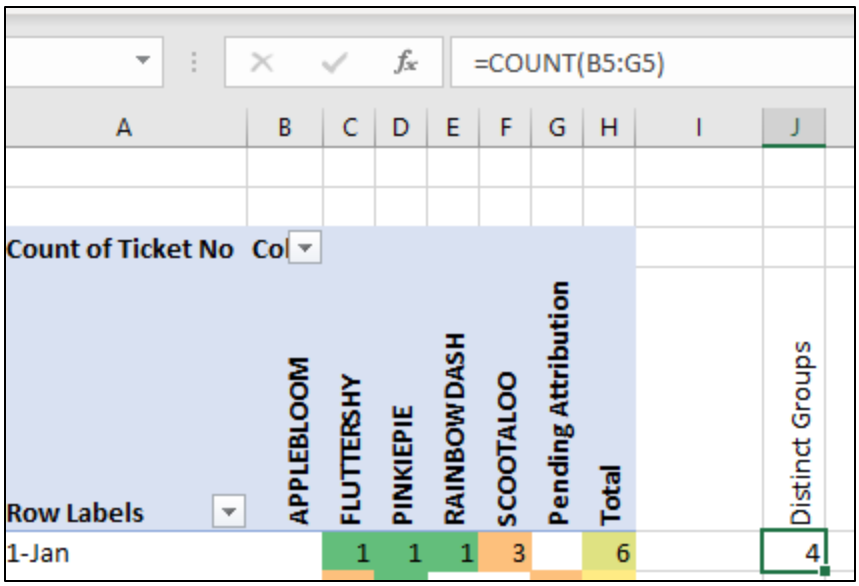
By independently formatting the final "Total" row and column, the larger numbers in these cells will not skew the conditional formatting of the interior cells and allow more subtle patterns to stand out. Analysts may also find it valuable to colorize "Pending Attribution" separately if these numbers are much larger than the rest of the attributed counts for the period covered by the table.

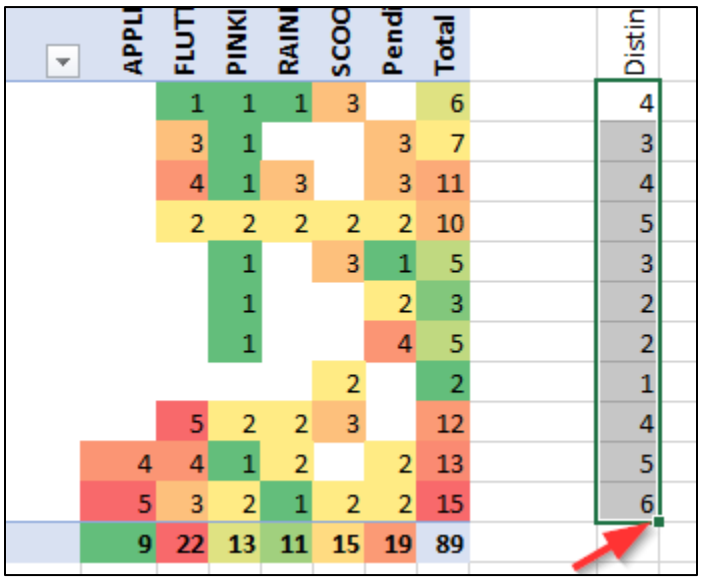
3. We want a measurement of relative activity levels as measured by distinct adversaries attempting intrusions against our organization each month. This measurement can provide the overall percentage of known adversaries targeting us each month.

Enter "Distinct Groups" in J4. In J5 type "=COUNT(B5:G5)" and push enter. Drag the value down the J row stopping at J15 to populate the other values.

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets
Technet24





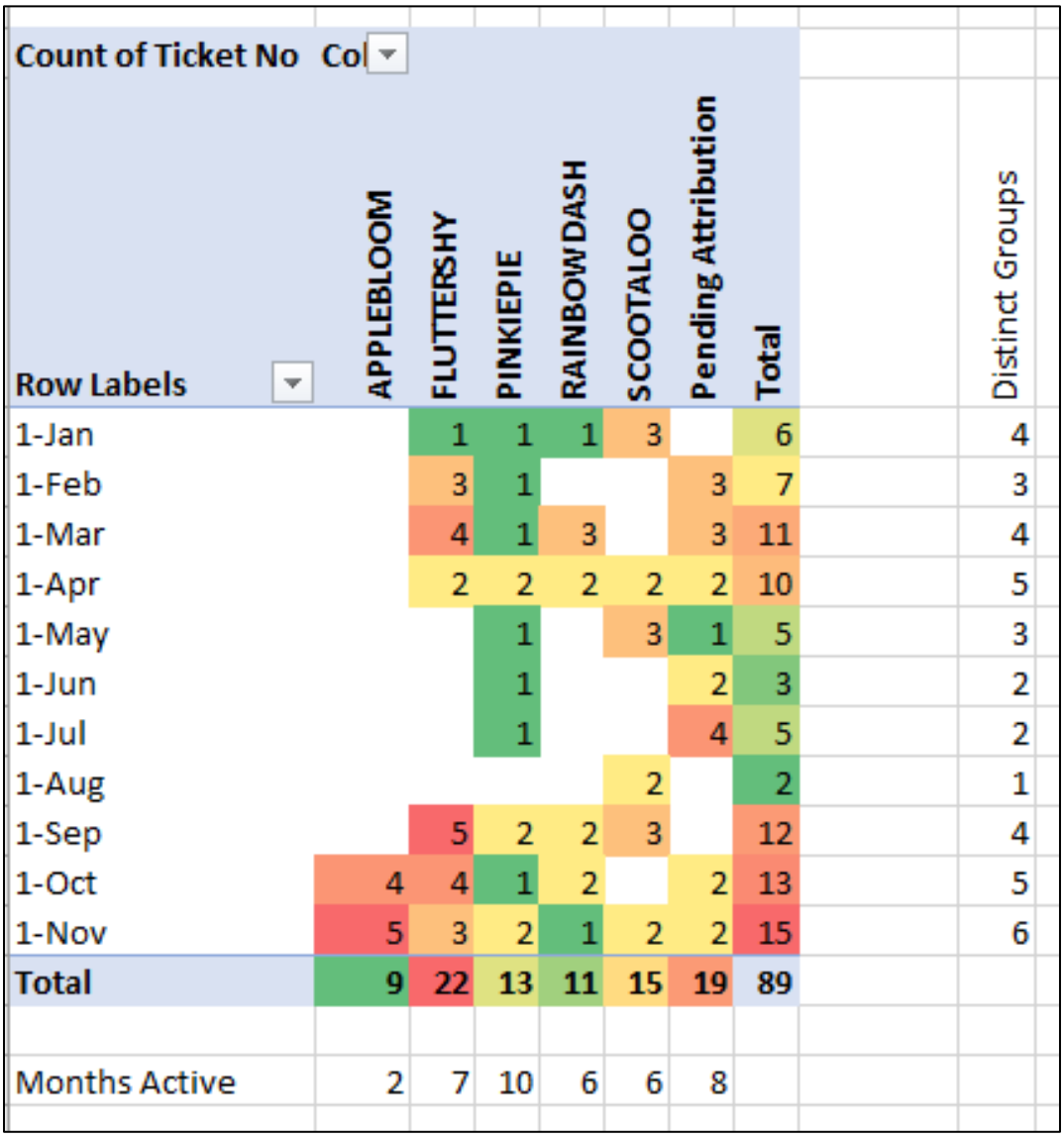
Now, if only PINKIEPIE, RAINBOWDASH, SCOOTALOO, and FLUTTERSHY are active in September, then the number of distinct groups active would be four.

We also desire a measurement of the overall activity level for each group across the history of our dataset in terms of the number of months each is active. If expressed as a percentage, this measurement can provide the probability of observing each group in any given month. Enhance the PivotTable by adding a row below the table providing a count of the number of total months in the dataset each group was active. For example, if APPLEBLOOM is active in only October and November, the number of months active for this group will be 2.

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets

Similarly, in cell A18 type “Months Active” and in B18-G18 the formula “=COUNT(B5:B15)” counts the number of cells in the set {B5, B6, B7, B8, B9, B10, B11, B12, B13, B14, B15} that contain a value. These are the months in which the first group listed (APPLEBLOOM) was active. Hitting the <ENTER> key will populate this cell with the value 2. Now select cell B18 and highlight cells to the right over to G18. This will fill to the right the same formula.



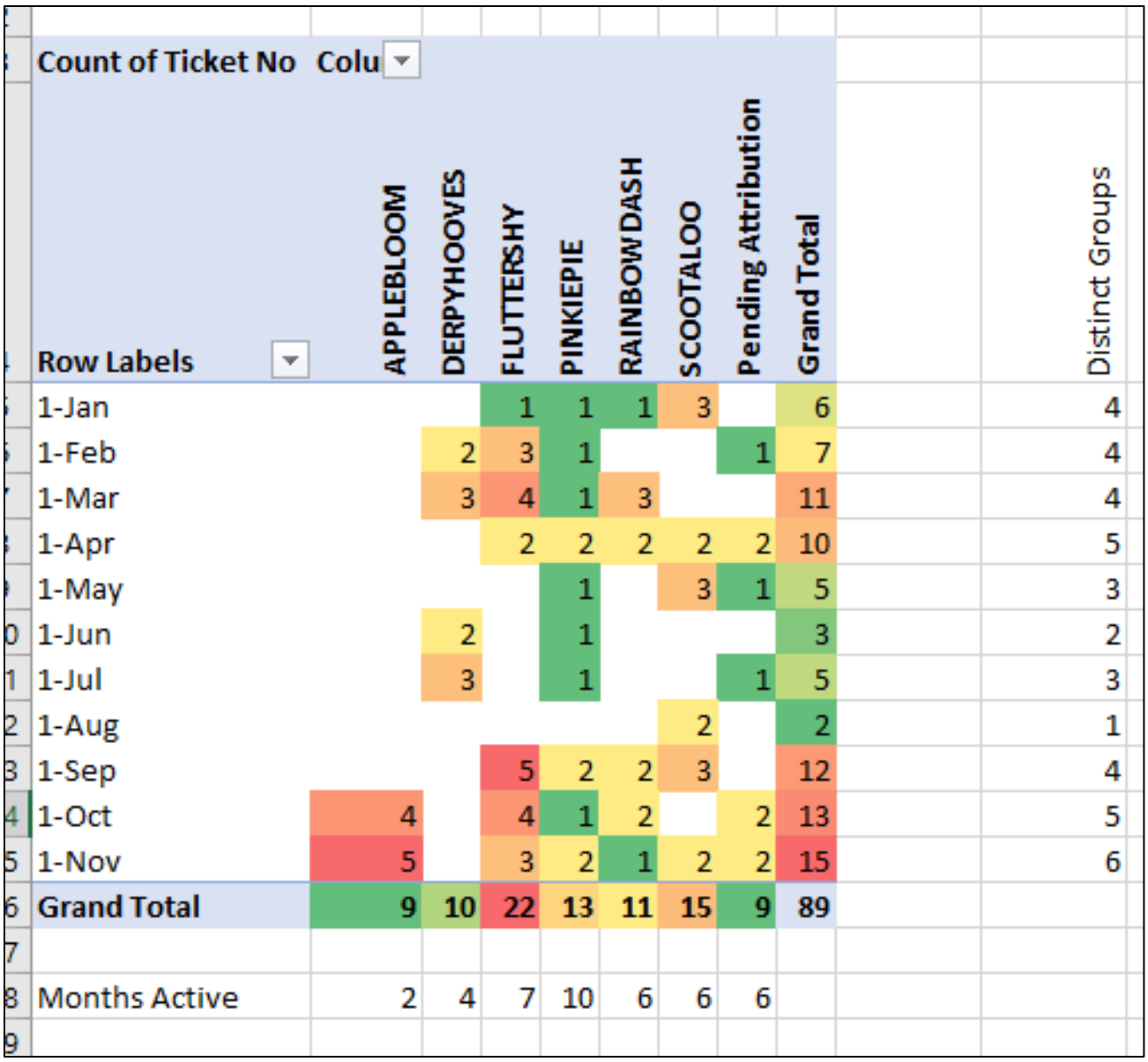
Count of Ticket No	Col								
Row Labels	APPLEBLOOM	FLUTTERSHY	PINKIEPIE	RAINBOWDASH	SCOOTALOO	Pending Attribution	Total		Distinct Groups
1-Jan		1	1	1	3		6		4
1-Feb		3	1			3	7		3
1-Mar		4	1	3		3	11		4
1-Apr		2	2	2	2	2	10		5
1-May			1		3	1	5		3
1-Jun			1			2	3		2
1-Jul			1			4	5		2
1-Aug					2		2		1
1-Sep		5	2	2	3		12		4
1-Oct	4	4	1	2		2	13		5
1-Nov	5	3	2	1	2	2	15		6
Total	9	22	13	11	15	19	89		
Months Active	2	7	10	6	6	8			

4. Repeat steps 2–3 for the “updated” sheet that includes DERPYHOOVES attribution to include Column H.

After repeating identical actions for steps 2–3 above on the “updated” data, the resulting group heatmap is as follows.

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets
Technet24



Count of Ticket No	Colu									
Row Labels	APPLEBLOOM	DERPYHOOVES	FLUTTERSHY	PINKIEPIE	RAINBOWDASH	SCOOTALOO	Pending Attribution	Grand Total		Distinct Groups
1-Jan			1	1	1	3		6		4
1-Feb		2	3	1			1	7		4
1-Mar		3	4	1	3			11		4
1-Apr			2	2	2	2	2	10		5
1-May				1		3	1	5		3
1-Jun		2		1				3		2
1-Jul		3		1			1	5		3
1-Aug						2		2		1
1-Sep			5	2	2	3		12		4
1-Oct	4		4	1	2		2	13		5
1-Nov	5		3	2	1	2	2	15		6
Grand Total	**9**	**10**	**22**	**13**	**11**	**15**	**9**	**89**		
Months Active	2	4	7	10	6	6	6			

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets

Exercise: Questions with Answers

1. Compare the original and updated heatmaps.

How has the identification of DERPYHOOVES changed the heatmap overall between the original and updated versions?

- **A new group increases to six the total number of groups known to be operating against Edison International and its companies. In addition, the number of incidents whose attribution is still "pending" has been reduced.**

What do these changes mean for the company?

- **The known threat landscape is larger. An assessment of intent by DERPYHOOVES may reveal additional technologies or protected data not known to be the target of existing groups, raising the level of overall organizational risk.**

What do these changes mean for CTI analysts?

- **Fewer intrusion attempts whose attribution is "pending" means a greater overall understanding of the known threat landscape. Pending attribution intrusions represent intelligence gaps of unknown risk to the organization long term. As they are reduced, so is uncertainty around the overall assessment of the threat landscape the organization operates within.**

2. Does DERPYHOOVES seem to show an activity pattern aligning to any other tracked group? Describe any such pattern alignments, and formulate a hypothesis as to what might explain each.

- **DERPYHOOVES displays a complementary pattern to SCOOTALOO. When DERPYHOOVES is active, SCOOTALOO is not, and vice versa. The only gap is October but there are 2 cases in the Pending attribution field. If the Pending Attribution cases are either DERPYHOOVES or SCOOTALOO and not the others, then the pattern holds. We'd want to take a look at those 2 cases and determine if DERPYHOOVES and SCOOTALOO share other commonalities. As an example, they could be the same team but tracked with distinct requirements as two different Activity Groups. We wouldn't combine the groups, but it would give some helpful analysis to our analysts to know that when we're tracking one group we should not see activity from the other group.**

3. One group seems to demonstrate very reliable operations on a monthly basis. Which group is that?

- **PINKIEPIE is active nearly every single month, typically only executing a single intrusion attempt per month.**

Are there any exceptions to this pattern?

- **PINKIEPIE executed two intrusion attempts in April, September, and November. August is the only month in which PINKIEPIE was not observed.**

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets
Technet24

4. The month of August is interesting. It is different from the other months in at least two ways. What are they?

   - **This month is the only month that PINKIEPIE was not active, the month with the fewest number of distinct groups observed, and the month with the fewest overall intrusion attempts.**

   Formulate a hypothesis as to what might explain this.

   - **One potential explanation is that there were issues with the technology collecting and analyzing data for the purposes of CTI and network defense. Another is that there is a major national holiday in this month, and all of our groups operate out of that country.**

   What steps would be necessary to validate this hypothesis?

   - **Communication and coordination with individuals tasked with maintaining these systems should be able to answer questions about any outages (widespread or specific to network defenders' capabilities). In order to validate the hypothesis of a national holiday, at least regional if not national origin of the actors would need to be determined, and a major holiday identified that would reasonably explain the observation.**

5. Look at the month of April. In terms of the other group activity that month, why might the activity for APPLEBLOOM, DERPYHOOVES, and Pending Attribution be significant?

   - **APPLEBLOOM and DERPYHOOVES are the only two groups not active during April. Widespread activity by a high number of groups like this is often stimulated by zero-day exploits deployed and shared that remain unpatched for a number of days to weeks. It seems strange looking just at this month that only these two groups were silent. DERPYHOOVES can possibly be explained by the periodic nature of its operations not aligning to this month. However, considering how rarely APPLEBLOOM has been seen, the widespread activity from other groups, and the presence of two intrusion attempts that are pending attribution, it seems possible that these could represent activity by APPLEBLOOM that was not properly identified as such.**

Exercise: Key Takeaways

- **By using simple features in Microsoft Excel such as PivotTables and conditional formatting, we can create useful group heatmaps that allow tracking activity over time. Many features in paid tools can actually be recreated using Excel, which is why it is the best CTI tool of all time.**

- **By analyzing our heatmap, we now have multiple hypotheses on how groups operate that provide additional insights and potential requirements for us to try to fulfill.**

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets

This page intentionally left blank.

https://t.me/learningnets

Technet24

Exercise 5.4: Creating and Defending an Attribution Model

Objectives

- Utilize skills developed in the course to create an attribution model, identify hypotheses, collect against them, perform analysis, and disseminate that information

Scenario: *The Edison International Executives want to know if DERPYHOOVES is the Chinese government.*

Exercise Preparation

In this scenario, you are not bound to any specific resources.

The walkthrough of this lab will be related to an entirely different scenario so as not to bias you. It will show the methodology but not give you any answers related to this scenario, since there are no set answers and the scenario is defined by you.

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets

Part 1: Generate Hypotheses and Define Attribution Models

Identify three hypotheses for who may be the actor behind DERPYHOOVES. In reality, you would define far more hypotheses so as not to bias yourself, but in the interest of time, choose three. From those three, you will generate one Attribution Model each.

1. The first step in the ACH process is to formulate hypotheses.

- Formulate hypotheses as to the attribution (entity/organization/state/etc.):

H1._____

H2._____

H3._____

2. Create an Attribution Model for each entity, listing characteristics that could be uniquely identifying and observed as it relates to the activity conducted. Identify at least five items for each Attribution Model (normally, there would be a rolling collection of activity far more than five items).

- **H1:**

_____

_____

_____

_____

_____

- **H2:**

_____

_____

_____

_____

_____

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets

Technet24

- **H3:**

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets

Part 1: Example Answers

Identify three hypotheses for who may be responsible for the scenario that you have chosen. In reality, you would define far more hypotheses so as not to bias yourself, but in the interest of time, choose three. From those three, you will generate one Attribution Model each.

3. The first step in the ACH process is to formulate hypotheses.

- Formulate hypotheses as to the attribution (entity/organization/state/etc.):

  H1. United States

  H2. Russia

  H3. China

4. Create an Attribution Model for each entity, listing characteristics that could be uniquely identifying and observed as it relates to the activity conducted. Identify at least five items for each Attribution Model (normally there would be a rolling collection of activity far more than five items).

- **H1:**

  Intelligence operations support US Military Operations (e.g., Middle East).

  Tradecraft leveraged from leaked documents, such as Snowden leaks.

  Supply chain access and highly sophisticated implants.

  Increased activity around U.S. geopolitical tension and time periods.

  Time zones and temporal events that align with U.S. work periods and holidays.

- **H2:**

  Targeting of NATO allies and ex-USSR states, especially militaries and embassies.

  Cyrillic language use and Russian keyboard settings consistently leveraged.

  Time zones and temporal events that align with Russian work periods and holidays.

  Operations aligned with the different distinct missions of government agencies such as SVR, GRU, and FSB.

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets

Technet24

Exploits and malware revealed by or leveraged by cyber-criminal elements in Russia.

- **H3:**

  Targeting of dissidents and victims where espionage would map to the 5 Year Plan.

  Chinese keyboard settings and language consistently used.

  Time zones and temporal events that align with Chinese work periods and holidays.

  Operations aligned with the different missions of organizations such as the PLA.

  Access to traditionally well-defended and hard-to-get IP space such as Great Firewall or certain university IP ranges in China.

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets

Part 2: Collect Data to Compare to the Hypotheses

1. Support the hypotheses with evidence.

The next step in the ACH process is to identify all the evidence supporting the hypotheses we've identified. Focus on key evidence given in various reports of trusted sources.

E1._____

E2._____

E3._____

E4._____

E5._____

E6._____

E7._____

E8._____

E9._____

E10._____

E11._____

E12._____

E13._____

E14._____

E15_____

E16._____

E17._____

E18._____

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets

Technet24

2. Map the evidence to the threat component.

To understand the confidence in your assessment, you now must classify your evidence according to which element of threat it pertains.

- Classify each piece of evidence as one of intent, opportunity, or capability. Leverage your Attribution Model to determine where the evidence should fit. If it is not descriptive, that is OK.

Intent:

_____

Opportunity:

_____

Capability:

_____

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets

Note: You will structure your matrix like the one below. Do not do the analysis in this exercise, though. The "+," "-," and "0" aspect of the exercise should be done in Exercise 5.3.

Threat Comp.	Evidence	Hypotheses			
		H1	**H2**	**H3**	**Other**
Intent					
Opportunity					
Capability					

3. **Compare the evidence.**

   Build the matrix for determining the diagnosticity of the evidence or the degree to which it supports each hypothesis. For convenience, this matrix is provided here. For each piece of evidence in order, determine its level of support to each of the three hypotheses and document it in the table. You may use the evidence list assembled from the previous step, or room is provided to write it on the table for easier comparison.

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets

Technet24

4. **Refine the matrix.**

   At this point, it should be clear which evidence is not of diagnostic value.

   - Identify the pieces of evidence that are not of diagnostic value:

     _____

     _____

     _____

     _____

     _____

     _____

5. **Prioritize the hypotheses.**

   Perform the hypothesis comparison. Prioritize the hypotheses, starting with those having the most refuting evidence at the bottom and building up to those with the most supporting evidence. Consider this the vertical comparison, whereas step 3 was the horizontal comparison.

   - Prioritize the hypotheses:

     Rank Order

     _____

     _____

     _____

     _____

6. **Evidentiary dependence.**

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets

Are there any pieces of evidence on which your assessment of the highest-likelihood hypothesis heavily depends? Are there only one or two pieces of evidence that, if omitted, would change your assessment?

- Identify the one or two most critical pieces of evidence to your assessment. Note their confidence, volatility, or underlying assumptions.

7. Report conclusions.

You're ready to provide your finalized assessment. Write one paragraph describing your conclusion, capturing all the necessary elements to properly qualify your report (including estimative language and evidentiary dependency, as well as intelligence gaps) and make it complete (including alternative hypotheses and any rejected evidence of note).

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets
Technet24

Exercise: Sample Walkthrough for Unrelated Dragonfly Case

1. Support the hypotheses with evidence.

The next step in the ACH process is to identify all the evidence available to answer the question of attribution.

a. Identify at least 18 pieces of evidence:

E1. *Spear phishing with PDFs used.*

E2. *Spear phishing spanned February–June 2013.*

E3. *Spear phishing targeted U.S. and U.K. companies.*

E4. *Watering hole delivery vector with LightsOut kit used.*

E5. *Watering hole delivery vector began in June 2013.*

E6. *The Hello exploit kit is used with a watering hole delivery vector.*

E7. *The Hello exploit kit began to be used in September 2013.*

E8. *Software vendor sites running content management software were compromised, and software updates were bundled with Backdoor.Oldrea.*

E9. *The software updates compromised were for ICS applications.*

E10. *Majority of victims are in the United States.*

E11. *All remaining victims are European (largest target group in aggregate).*

E12. *Oldrea (aka Havex/Energetic Bear RAT) malware appears customized for this campaign, accounting for 95% of infections.*

E13. *Shared backdoor was Karagany, used occasionally.*

E14. *Attackers shifted targets and increased pace in March 2014.*

E15. *Attackers seemed to operate 9 a.m.–6 p.m., M–F, in UTC+4 time zone.*

E16. *Attackers executed multistage (multi-Kill-Chain) intrusions.*

E17. *Oldrea collects system information, data from outlook, and various ICS software configurations.*

E18. *Four (Former East Germany) victim countries are former Soviet client states.*

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets

2. **Map the evidence to threat component.**

To understand the confidence in your assessment, you now must classify your evidence according to which element of threat it pertains.

b. Classify each piece of evidence as one of intent, opportunity, or capability.

Threat Comp.	Evidence	Hypotheses			
		US	**China**	**Russia**	**Other**
Intent	**E3.** Spear phishing targeted U.S. and U.K.				
	E9. Software updates compromised were for ICS apps.				
	E10. Majority of victims are in the United States.				
	E11. Other victims are European (largest target group in aggregate).				
	E17. Oldrea collects system information, data from outlook, and various ICS software configurations.				
Opportunity	**E2.** Spear phishing spanned February–June 2013.				
	E5. Watering hole delivery began in June 2013.				
	E7. Hello exploit kit use began in September 2013.				
	E14. Attackers shifted targets and increased pace in March 2014.				
	E15. Attackers operated 9 a.m.–6 p.m., M–F, in UTC+4.				
Capability	**E1**. Spear phishing with PDFs used.				
	E4. Watering hole delivery with LightsOut kit used.				
	E6. Hello exploit kit is used with a watering hole delivery vector.				
	E8. Software vendor sites running content management software were compromised, and software updates were bundled with Backdoor.Oldrea.				
	E12. Oldrea (aka Havex/Energetic Bear RAT) malware appears customized for this campaign, accounting for 95% of infection.				
	E16. Attackers executed multistage (multi-Kill-Chain) intrusions.				

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets

Technet24

3. **Compare the evidence.**

Build the matrix for determining the diagnosticity of the evidence or the degree to which it supports each hypothesis. For convenience, this matrix is provided here.

- For each piece of evidence in order, determine its level of support to each of the three hypotheses and document it in the table. You may use the evidence list assembled from the previous step, or room is provided to write it in the table for easier comparison.

Threat Comp.	Evidence	Hypotheses			
		US	**China**	**Russia**	**Other**
Intent	**E3.** Spear phishing targeted U.S. and U.K.	--	+	+	+
	E9. Software updates compromised were for ICS apps.	+		+	
	E10. Majority of victims are in the United States.	--	+	+	+
	E11. Other victims are European (largest target group in aggregate).	-	+	+	
	E17. Oldrea collects system information, data from outlook, and various ICS software configurations.			+	
Opportunity	**E2.** Spear phishing spanned February–June 2013.				
	E5. Watering hole delivery began in June 2013.				
	E7. Hello exploit kit use began in September 2013.				
	E14. Attackers shifted targets and increased pace in March 2014.			+	
	E15. Attackers operated 9 a.m.–6 p.m., M–F, in UTC+4.			+	
Capability	**E1**. Spear phishing with PDFs used.	+	+	+	+
	E4. Watering-hole delivery with LightsOut kit used.	+	+	+	+
	E6. Hello exploit kit is used with a watering hole delivery vector.	+	+	+	+
	E8. Software vendor sites running content management software were compromised, and software updates were bundled with Backdoor.Oldrea.	+	+	+	+
	E12. Oldrea (aka Havex/Energetic Bear RAT) malware appears customized for this campaign, accounting for 95% of infection.	+	+	+	+
	E16. Attackers executed multistage (multi-Kill-Chain) intrusions.	+	+	+	+

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets

4. Refine the matrix.

At this point, it should be clear which evidence is not of diagnostic value.

- Identify the pieces of evidence here that are not of diagnostic value:

E2, E5, E7, E1, E4, E6, E8, E12, and E16 have no diagnostic value. The revised matrix follows.

Threat Comp.	Evidence	Hypotheses			
		US	**China**	**Russia**	**Other**
Intent	**E3.** Spear phishing targeted United States and U.K.	--	+	+	+
	E9. Software updates compromised were for ICS apps.	+		+	
	E10. Majority of victims are in the United States.	--	+	+	+
	E11. Other victims are European (largest target group in aggregate).	-	+	+	
	E17. Oldrea collects system information, data from outlook, and various ICS software configurations.			+	
Opportunity	**E2.** Spear phishing spanned February–June 2013.				
	E5. Watering hole delivery began June 2013.				
	E7. Hello exploit kit use began September 2013.				
	E14. Attackers shifted targets and increased pace March 2014.			+	
	E15. Attackers operated 9 a.m.–6 p.m., M–F, in UTC+4.			+	
Capability	**E1**. Spear phishing with PDFs used.	+	+	+	+
	E4. Watering-hole delivery with LightsOut kit used.	+	+	+	+
	E6. Hello exploit kit is used with a watering hole delivery vector.	+	+	+	+
	E8. Software vendor sites and running content management software were compromised, and software updates were bundled with Backdoor.Oldrea.	+	+	+	+
	E12. Oldrea (aka Havex/Energetic Bear RAT) malware appears customized for this campaign, accounting for 95% of infection.	+	+	+	+
	E16. Attackers executed multistage (multi-Kill-Chain) intrusions.	+	+	+	+

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets

Technet24

5. Prioritize the hypotheses.

Perform the hypothesis comparison. Prioritize the hypotheses, starting with those having the most refuting evidence at the bottom and building up to those with the most supporting evidence. Consider this the vertical comparison, whereas step 3 was the horizontal comparison.

- Prioritize the hypotheses:

Rank Order

Russia

China

Other

United States

6. Evidentiary dependence.

Are there any pieces of evidence on which your assessment of the highest-likelihood hypothesis heavily depends? Are there only one or two pieces of evidence that, if omitted, would change your assessment?

- Identify the one or two most critical pieces of evidence to your assessment. Note their confidence, volatility, or underlying assumptions.

The conclusion is dependent on two pieces of evidence supporting opportunity: The outbreak of the Ukrainian crisis aligning with a targeting shift by the campaign, and the time zone of the operators, both offering loose support for the RF hypothesis over the IR hypothesis. This is compounded by no other diagnostic evidence for "opportunity."

7. Report conclusions.

You're ready to provide your finalized assessment. Write one paragraph describing your conclusion, capturing all the necessary elements to properly qualify your report (including estimative language and evidentiary dependency, as well as intelligence gaps) and make it complete (including alternative hypotheses and any rejected evidence of note).

In June 2014, Symantec released a report on a campaign dubbed Dragonfly that had been targeting Industrial Control Systems (ICSs) targets. I assess with low confidence based on the evidence provided in the report that this campaign is attributable to Russian actors. The capabilities demonstrated are assessed to be available to the United States, China, Russia, Iran, North Korea, and other entities executing operations in cyberspace. Evidence of intent most strongly favors actors operating in the general interests of Russia or Iran with relatively equal weight, but alignment of the pattern of activity on a daily basis plus targeting shift at the same time as reported Russian engagement in Ukraine indicate that this hypothesis is the strongest. The lack of other evidence characterizing the adversary's opportunity plus a lack of any capability that distinctly aligns with one country or another makes this hypothesis low confidence.

© 2021 Robert M. Lee and SANS Institute

https://t.me/learningnets