Motorhead

Purple Team Case Study

@brysonbort

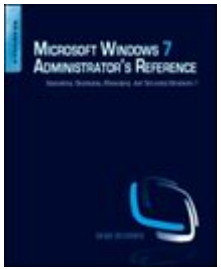
SCYTHE

ICS

SCYTHE GRIMM

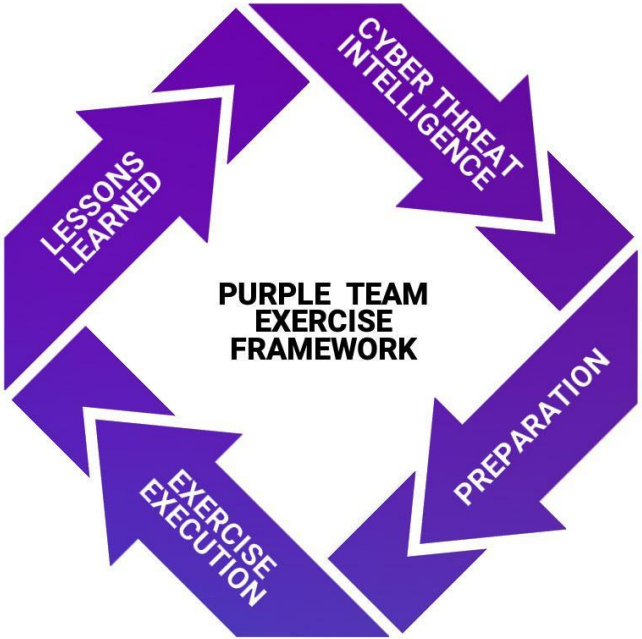
T1033 - System Owner/User Discovery

- Chief Technology Officer - SCYTHE
- Purple Team Exercise Framework (PTEF)
- C2 Matrix Co-Creator
- 10 years @ Citi leading offensive security team
- Certified SANS Instructor: SEC560, SEC504
- Author SEC564: Red Team Exercises and Adversary Emulation
- CVSSv3.1 Working Group Voting Member; Recently: EPSS
- GFMA: Threat-Led Pentest Framework
- ISSA Fellow; NSI Technologist Fellow



Agenda

- Executive Summary
- Goals
- Cyber Threat Intelligence
- Preparation
- Adversary Emulation Plans
- Exercise Execution
- Results
- Lessons Learned



https://www.scythe.io/ptef

Executive Summary - Purple Team Exercise

- 6 week Purple Team Exercise - Assumed Breach scenario
- A Purple Team is a virtual team where the following teams work together:
  - Cyber Threat Intelligence - team to research and provide adversary behavior
  - Red Team - offensive team in charge of emulating adversaries
  - Blue Team - the defenders. Security Operations Center (SOC), Hunt Team, Digital Forensics and Incident Response (DFIR), and/or Managed Security Service Provides (MSSP)
- SCYTHE was hired to perform all 3 roles
- $0 spend on new technology
  - Only tuning current security controls

Executive Summary - Cyber Threat Intelligence

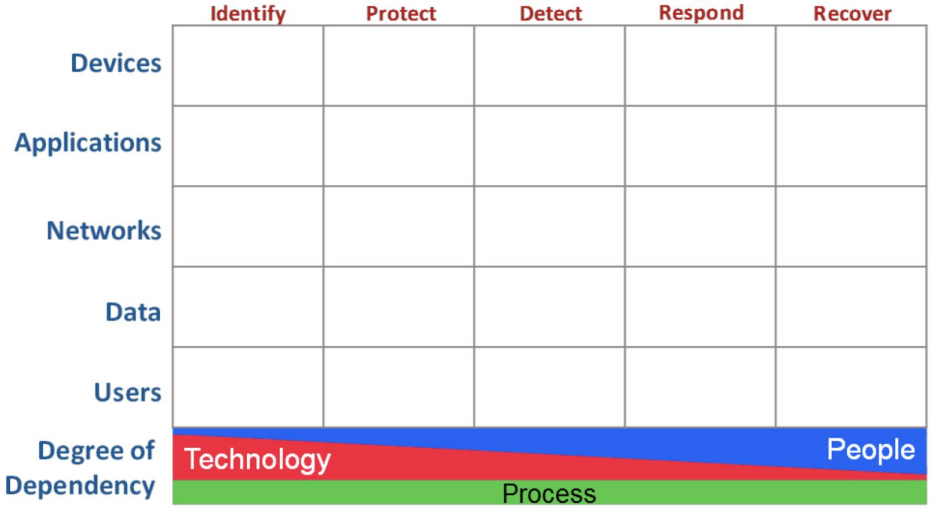
- Week 1 - Baseline testing: synthetic malware execution and command and control over HTTPS; ensure visibility and access to current controls
- Week 2 - APT19: low sophistication Chinese threat actor
- Week 3 - Buhtrap: medium sophistication Russian threat actor
- Week 4 - APT33: medium sophistication Iranian threat actor
- Week 5 - APT3: high sophistication Chinese threat actor
- Week 6 - Free Play: red team plan based on situational awareness from previous weeks. Tested for Active Directory, Microsoft Exchange, and lateral movement

Threat Detection is Hard

- Uncertainty aka Attackers change
- Improve Detection aka Alerting
- Multi-Stage Detection aka Context

- OWASP Top 10:

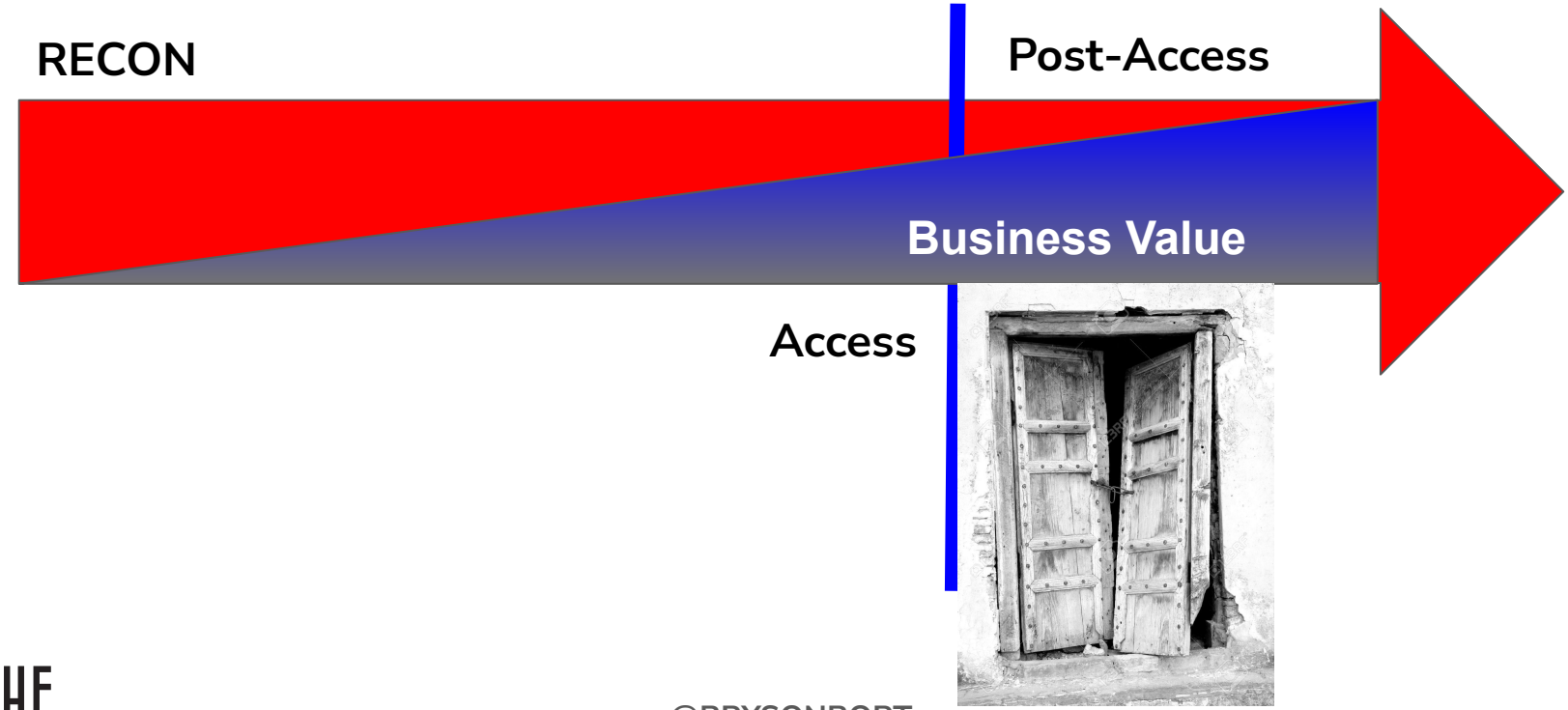
[Insufficient Logging & Monitoring]



https://owasp.org/www-project-cyber-defense-matrix/

https://medium.com/anton-on-security/on-threat-detection-uncertainty-7eac9b22adb6

Executive Summary: Assumed Breach



Executive Summary - Baseline

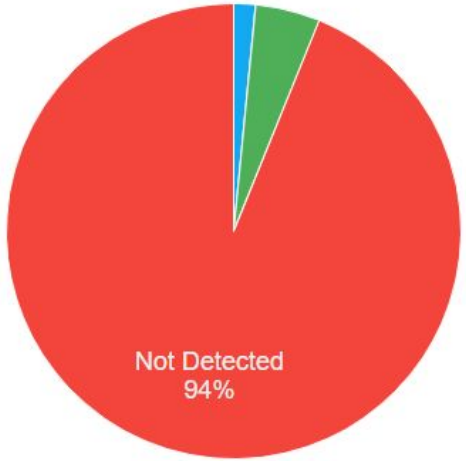
- 94% of Adversary Behavior was undetected
- 3 test cases detected by current controls
- 1 test case blocked

Baseline Result
Known threats have the ability to achieve their objective without being detected

Campaigns Aggregated	5
Test Cases Completed:	65
Test Cases Passed:	4
Detected:	3
Blocked:	1
Test Cases Failed:	61
Not Detected:	61
Test Cases Not Completed:	0
To Be Determined:	0

Overall Score

Lower



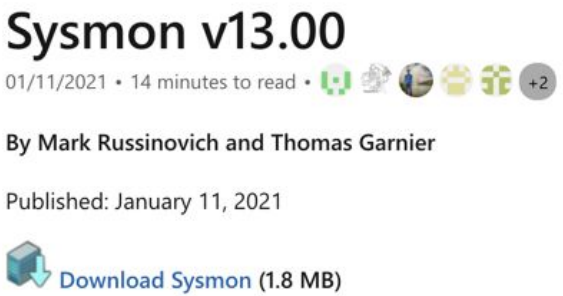
SCYTHE

Sysmon

System Monitor (*Sysmon*) is a persistent Windows system service and device driver to monitor and log system activity to the Windows event log.

It provides detailed information about

- process creations,
- network connections, and
- changes to file creation time.



https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon

Executive Summary - End State

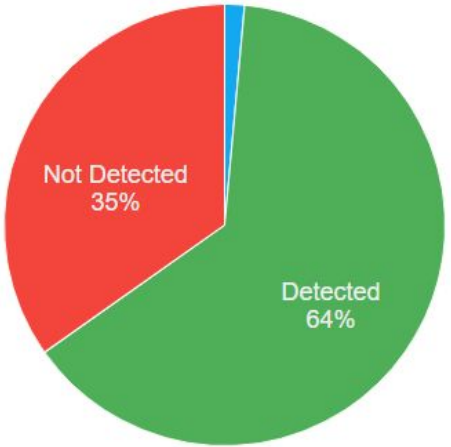
- $0 technology spend to achieve 64% detection rate
- Enabled telemetry (Sysmon)
- Created logic for alerts on EVENTSENTRY

End State Result
Known threats will be detected and responded to before achieving objective

Campaigns Aggregated	5
Test Cases Completed:	69
Test Cases Passed:	45
Detected:	44
Blocked:	1
Test Cases Failed:	24
Not Detected:	24
Test Cases Not Completed:	0
To Be Determined:	0

Overall Score

Above Average



SCYTHE

Goals and Objectives

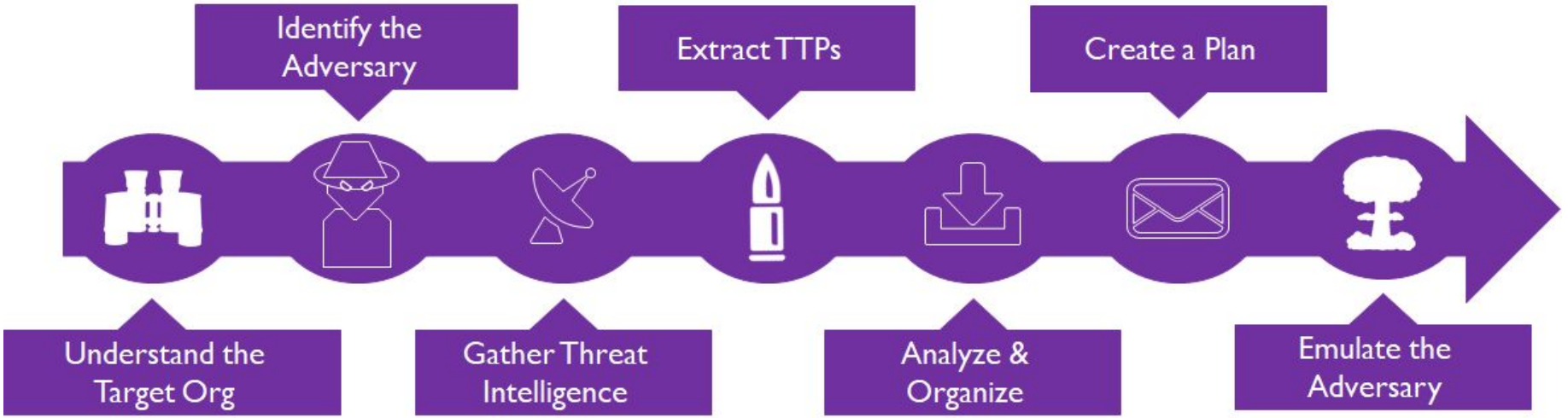
"NMFTA seeks assistance in measuring the effectiveness of their network security threat detection capabilities through a structured "Purple Team" exercise. This is the first purple team exercise by the NMFTA and they would like to increase adversary sophistication throughout the exercise."

- Identify adversaries with the opportunity, intent, and capability to attack
- Consume Cyber Threat Intelligence and create Adversary Emulation Plans
- Emulate the adversary against production environment
- Determine if security controls detected, alerted, and/or prevented the activity
- Tune security controls by enabling detective and alerting controls
- Use current capabilities - $0 increase in tools

SCYTHE

NMFTA National Motor Freight Traffic Association, Inc.

Cyber Threat Intelligence



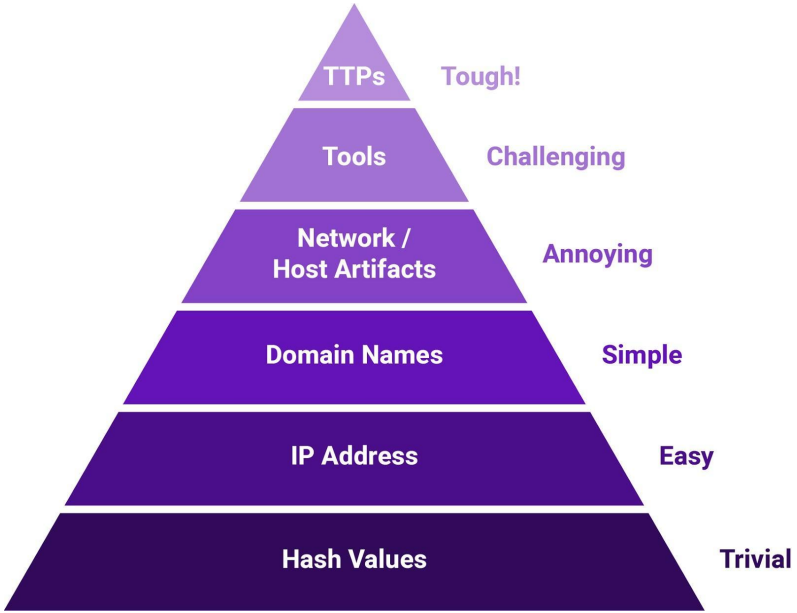
SCYTHE

Purple Team Exercise Flow

1. Cyber Threat Intelligence, Exercise Coordinator, or Red Team presents the adversary, TTPs, and technical details
2. Attendees have a table-top discussion of security controls and expectations for TTP
3. Red Team emulates the TTP
4. Blue Team (SOC, Hunt team, DFIR) analysts follow process to detect and respond to TTP
5. Share screen if TTP was identified, received alert, logs, or any forensic artifacts
6. Document results - what worked and what did not
7. Perform any adjustments or tuning to security controls to increase visibility
8. Repeat TTP
9. Document any feedback and/or additional Action Items for Lessons Learned
10. Repeat from step 1 for next TTP

What are TTPs? Adversary Behavior

David Bianco: http://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html



So, Why is Detection Hard?

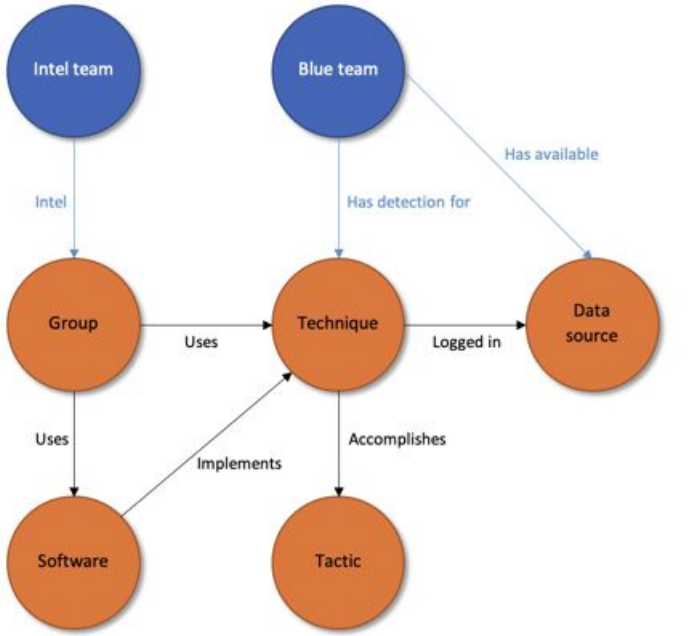
- Today's environments are complex and messy
- Detection needs PEOPLE
  - People don't scale
- Detection needs DATA
  - Data comes from many sources, owned by many people
  - Context is key
- Detection needs TRIAGE (rules, logic)
- Attackers don't want to be detected
  - Ransomware does, but at the end
- Detection is about intent, not only activity

https://medium.com/anton-on-security/why-is-threat-detection-hard-42aa479a197f

DETT&CT

Blue Team

- Data Sources
- Visibility
- Detection



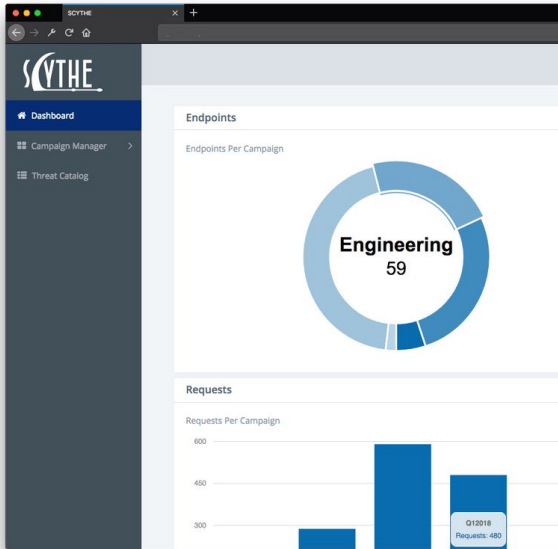
https://www.mbsecure.nl/blog/2019/5/dettact-mapping-your-blue-team-to-mitre-attack

Roles and Responsibilities

Role	Assigned	Responsibility
Cyber Threat Intelligence	SCYTHE	Cyber Threat Intelligence, Threat Emulation Plan
Red Team Operator	SCYTHE	Preparation, Exercise Execution
Blue Team	SCYTHE	Preparation, Exercise Execution
Exercise Coordinator	Jorge Orchilles	Lead point of contact throughout the entire Purple Team Exercise. Responsible to ensure Cyber Threat Intelligence is provided. Ensures all Preparation steps are taken prior to Exercise Execution. During Exercise Execution, record minutes, notes, action items, and feedback. Send daily emails with those notes as well as guidance for what's planned for the next day. Compile and deliver Lessons Learned.
Internal Operations	NMFTA	Sponsor, Preparation, Spectator, Remediation

Planning - Attack Infrastructure (SCYTHE)

- Enterprise-Grade platform for Adversary Emulation
  - Creating custom, controlled, synthetic malware
  - Deployed on Google Cloud Platform (for this exercise)
- Emulate known threat actors against an enterprise network
  - **Consistently execute** adversary behaviors
  - **Continually assess** security controls
  - **Decreased evaluation time** of security technologies
  - **Identify blind spots** for blue teams
  - **Force-multiplier for red team** resources
  - **Measure and improve response** of people and process



SCYTHE

https://t.me/learninghets

@BRYSONBORT
@JORGEORCHILLES

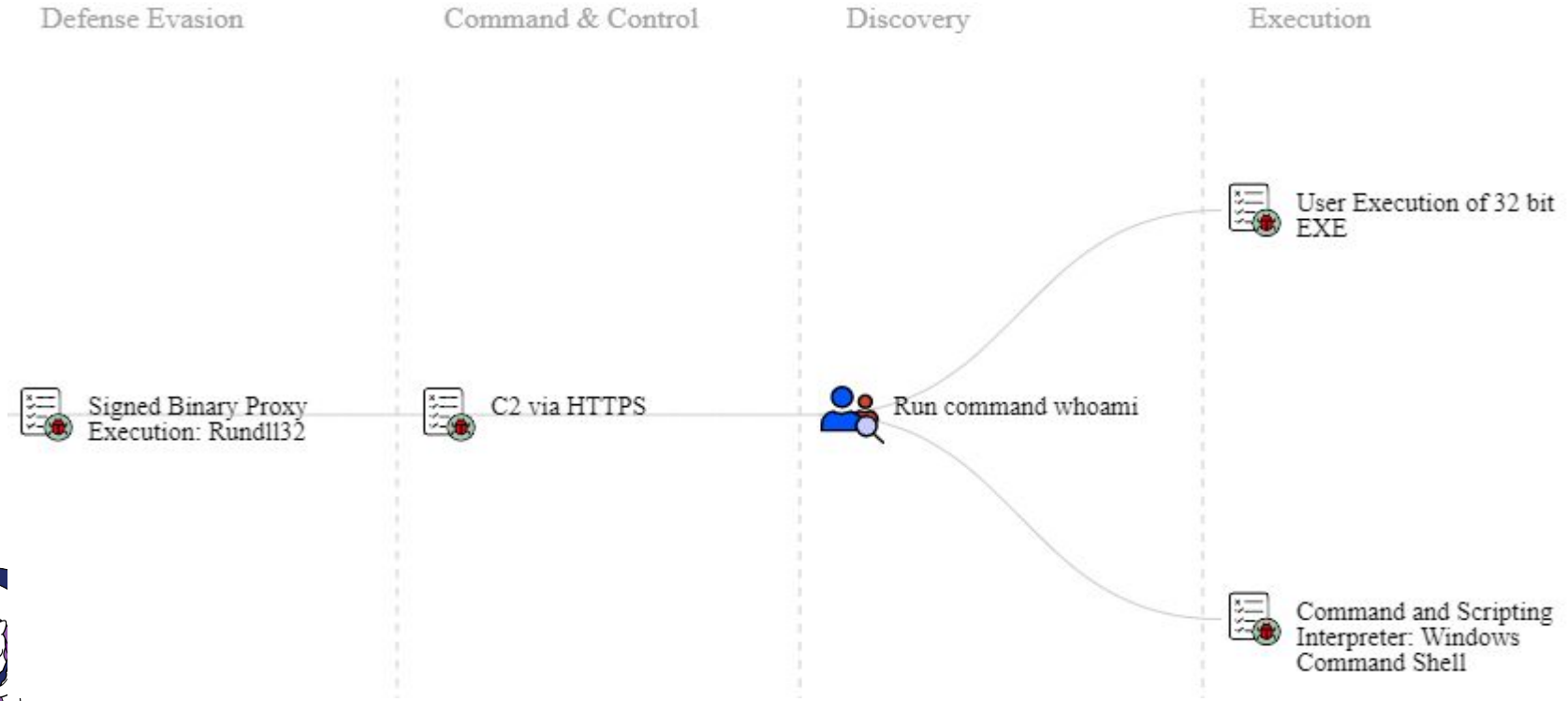
Planning - Target Systems and Accounts

- Created multiple systems in production environment
  - WIN10-SCYTHE - standard user and jump point
  - WIN10-SCYTHE2 - local admin (testing)
  - WIN10-SCYTHE3 - standard user for testing (Baseline)
  - SCYTHE-SER-DOM - standard user
- Created production account in Active Directory - enabled email
- Ensured all security controls enabled as a normal operations
  - Anti-Virus
  - Firewalls
  - SIEM logging and alerting
  - Email Security - multiple controls

Week 1 - Baseline

- As SCYTHE was playing both the Blue and Red Team, we needed a week to gain situational awareness
- Red Team:
  - Created basic synthetic malware
  - Executed it through User Execution and RunDLL32.exe
  - Establish Command and Control (C2) over HTTPS
  - Ran whoami from command line
- Blue Team
  - Ensure visibility and access to current controls
  - Local logging
  - Remote logging to SIEM
  - Alerts, rules, and logic configuration

Week 1 - Planning



Week 1 - Baseline Result

Test Cases

CAMPAIGN ACTIONS

	Phase	Technique	Test Case	Status	Outcome	Tags	Action
	All	search ...	search ...	All	All	All	
	Discovery	System Owner/User Discovery	Run command whoami	Completed	Not Detected		
	Command & Control	T1071.001	C2 via HTTPS	Completed	Not Detected		
	Execution	T1204.002	User Execution of 32 bit EXE	Completed	Not Detected		
	Defense Evasion	T1218.011	Signed Binary Proxy Execution: Rundll32	Completed	Not Detected		
	Execution	T1059.003	Command and Scripting Interpreter: Windows Command Shell	Completed	Not Detected		

Week 1 - Baseline Result

Campaigns Aggregated	1
Test Cases Completed:	5
Test Cases Passed:	0
Detected:	0
Blocked:	0
Test Cases Failed:	5
Not Detected:	5
Test Cases Not Completed:	0
To Be Determined:	0

Overall Score

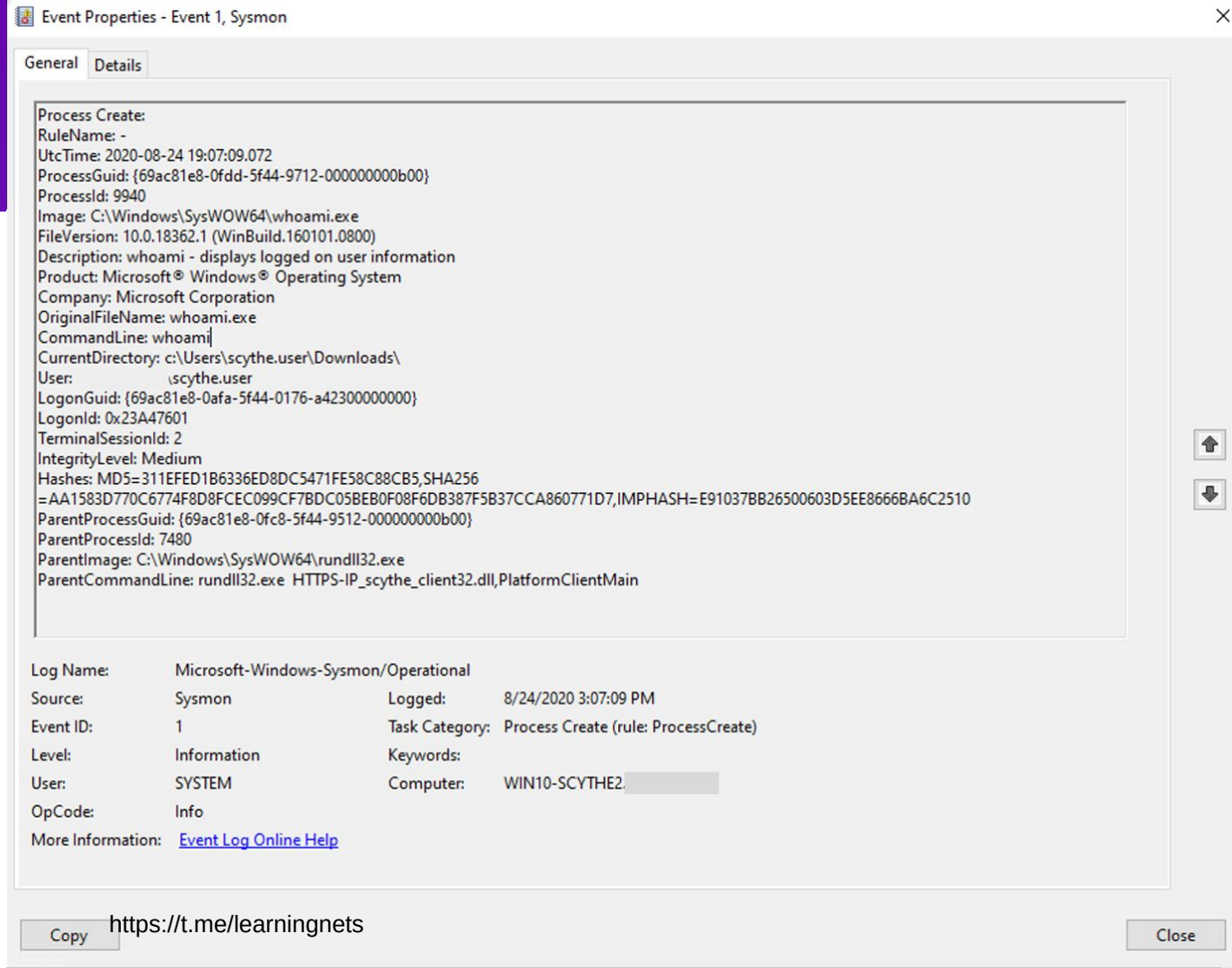
Lower

Week 1 - Implemented Controls

- Install Sysmon on all hosts
  - System Monitor (Sysmon) is a Windows system service and device driver that, once installed on a system, remains resident across system reboots to monitor and log system activity to the Windows event log.
  - It provides detailed information about process creations, network connections, and changes to file creation time
- Enable Sysmon Event ID 1 Process Creation to detect any executable, including: rundll32.exe, cmd.exe, whoami.exe
- Send Sysmon logs to SIEM 

- Configure EventSentry with rules/logic to alert
- Email alerts to operations team

Sysmon



EventSentry

Hybrid SIEM with native Active Directory + NetFlow Monitoring

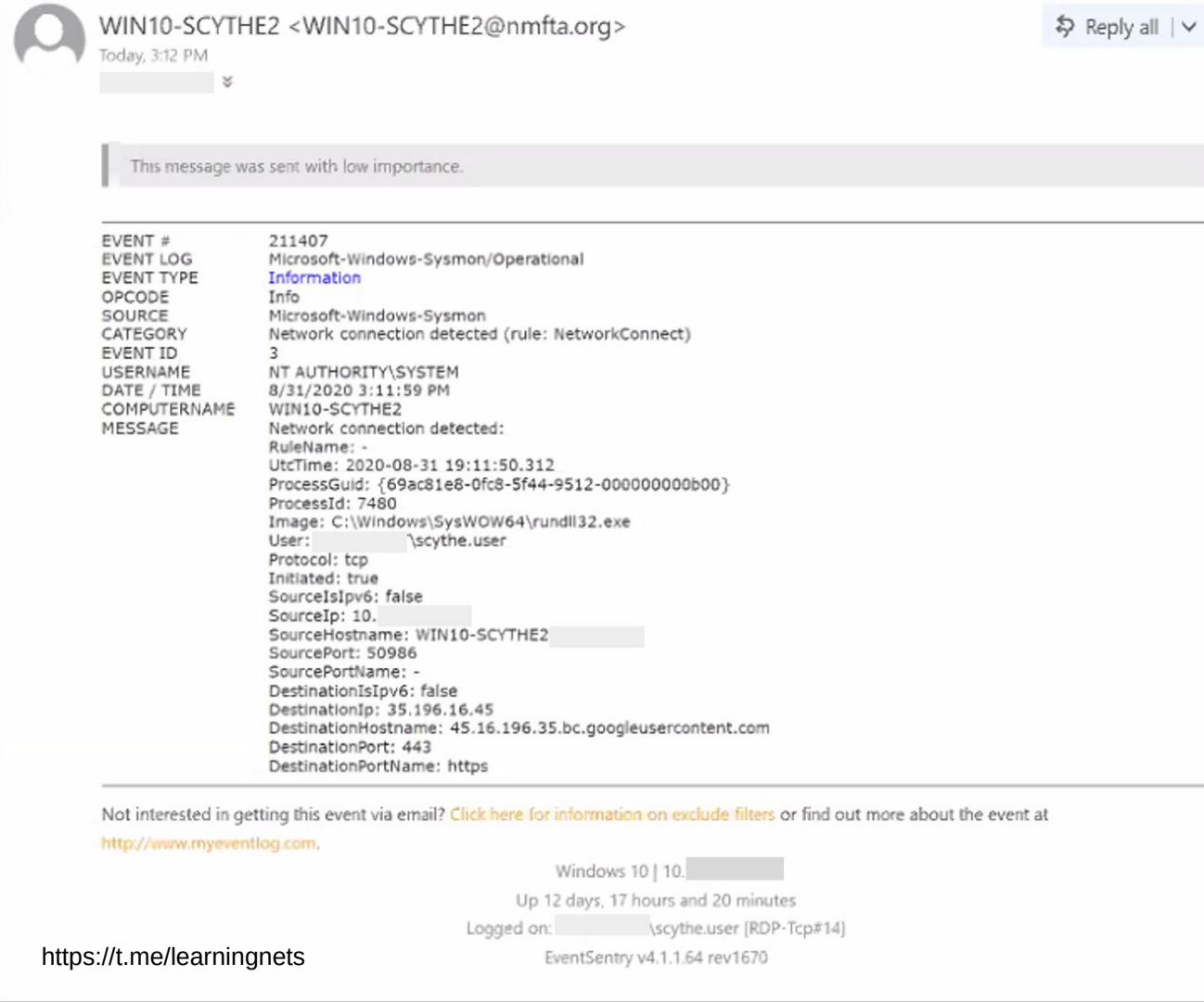
- Powerful & flexible real-time log analysis & alerting engine
  - Detect lateral movement and suspicious activity
  - Automatic remediation
  - No relevant impact on monitored hosts
- Native Sysmon integration (reporting, alerting & remediation)
- Reveals insecure OS & application settings
- Identifies services / drivers / tasks, software & browser extensions

System Health Monitoring
All relevant system metrics
Complete SW/HW inventory

AD Monitoring
AD & Group Policy changes
Identify high-risk accounts
Password reminder emails

NetFlow
Detect malicious traffic
Identify traffic patterns
Automatically respond to threats

Alerting



Week 1 - Detection

Test Cases

CAMPAIGN ACTIONS

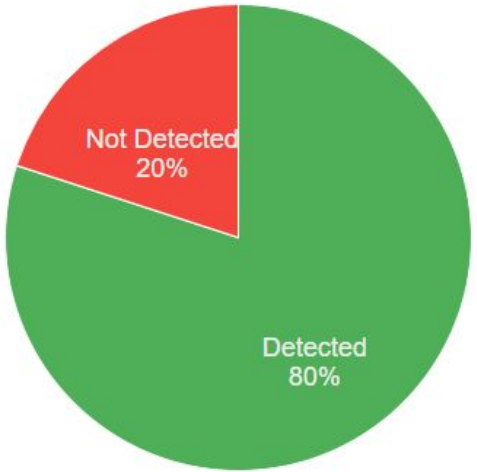
	Phase	Technique	Test Case	Status	Outcome	Tags	Action
	All	search ...	search ...	All	All	All	
	Discovery	System Owner/User Discovery	Run command whoami	Completed	Detected		
	Execution	T1204.002	User Execution of 32 bit EXE	Completed	Detected		
	Defense Evasion	T1218.011	Signed Binary Proxy Execution: Rundll32	Completed	Detected		
	Execution	T1059.003	Command and Scripting Interpreter: Windows Command Shell	Completed	Detected		
	Command & Control	C2 via HTTPS	C2 via HTTPS	Completed	Not Detected		

Week 1 - Detection

Overall Score

Superior

Campaigns Aggregated	1
Test Cases Completed:	5
Test Cases Passed:	4
Detected:	4
Blocked:	0
Test Cases Failed:	1
Not Detected:	1
Test Cases Not Completed:	0
To Be Determined:	0

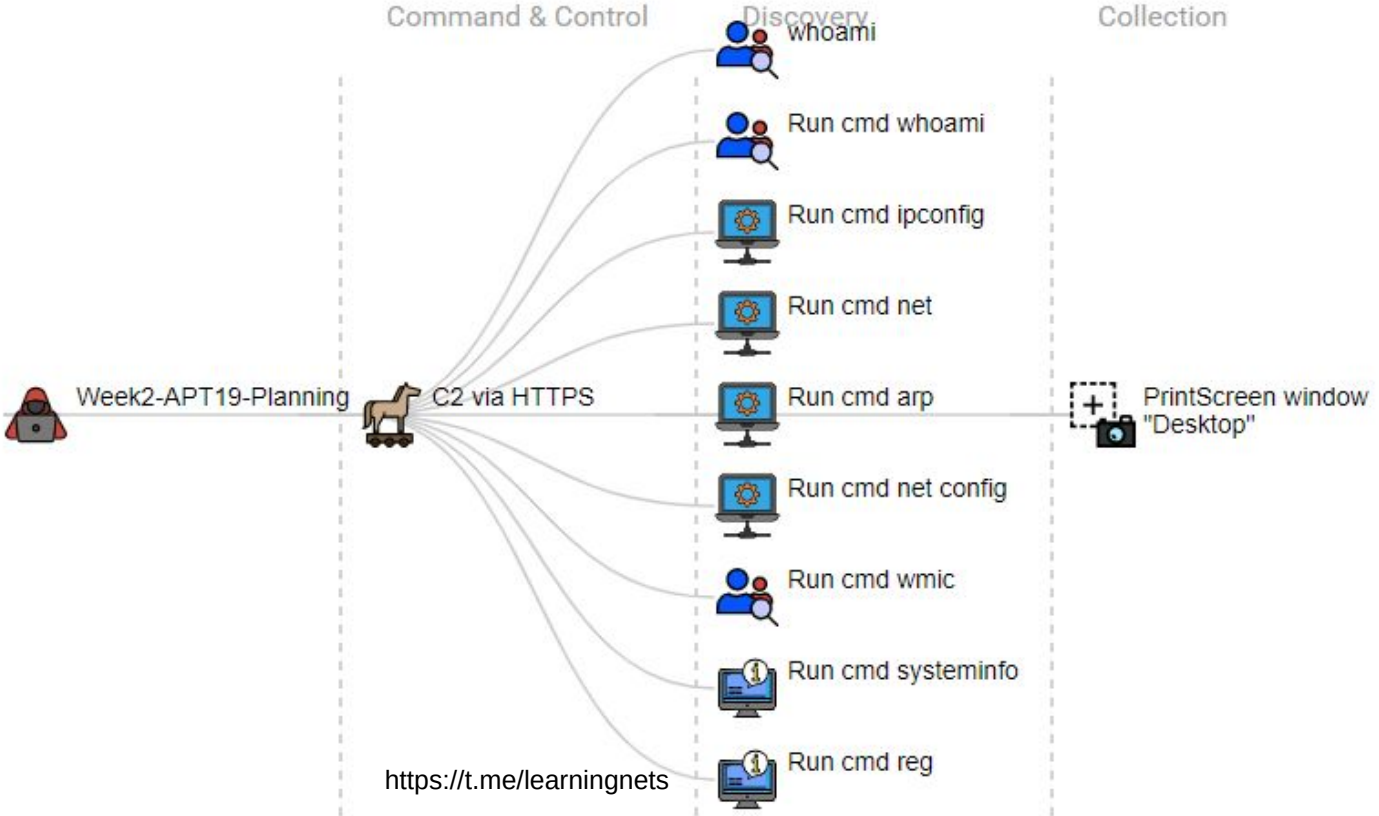


SCYTHE

Week 2 - APT19

Tactic	Description
Description	APT19 is a Chinese-based threat group that has targeted a variety of industries, including defense, finance, energy, pharmaceutical, telecommunications, high tech, education, manufacturing, and legal services.
Objective	Exist in the network to enumerate systems and information in order to maintain Command and Control to support future attacks.
Command and Control	Application Layer Protocol: Web Protocols (T1.071.001); Encrypted Channel (T1573)
Initial Access	Spearphishing attachment (T1193); Spearphishing link (T1192)
Execution	User Execution (T1204); Hidden Windows (T1143); PowerShell (T1086); Command and Scripting Interpreter: Windows Command Shell (T1059.003)
Discover	System Owner/User Discovery (T1033); System Information Discovery (T1082) System Network Configuration Discovery (T1016)
Collection	Screen Capture (T1113)

Week 2 APT19 - Planning



https://t.me/learningnets

Week 2 APT19 - Baseline

Overall Score

Lower

Campaigns Aggregated	1
Test Cases Completed:	11
Test Cases Passed:	0
Detected:	0
Blocked:	0
Test Cases Failed:	11
Not Detected:	11
Test Cases Not Completed:	0
To Be Determined:	0

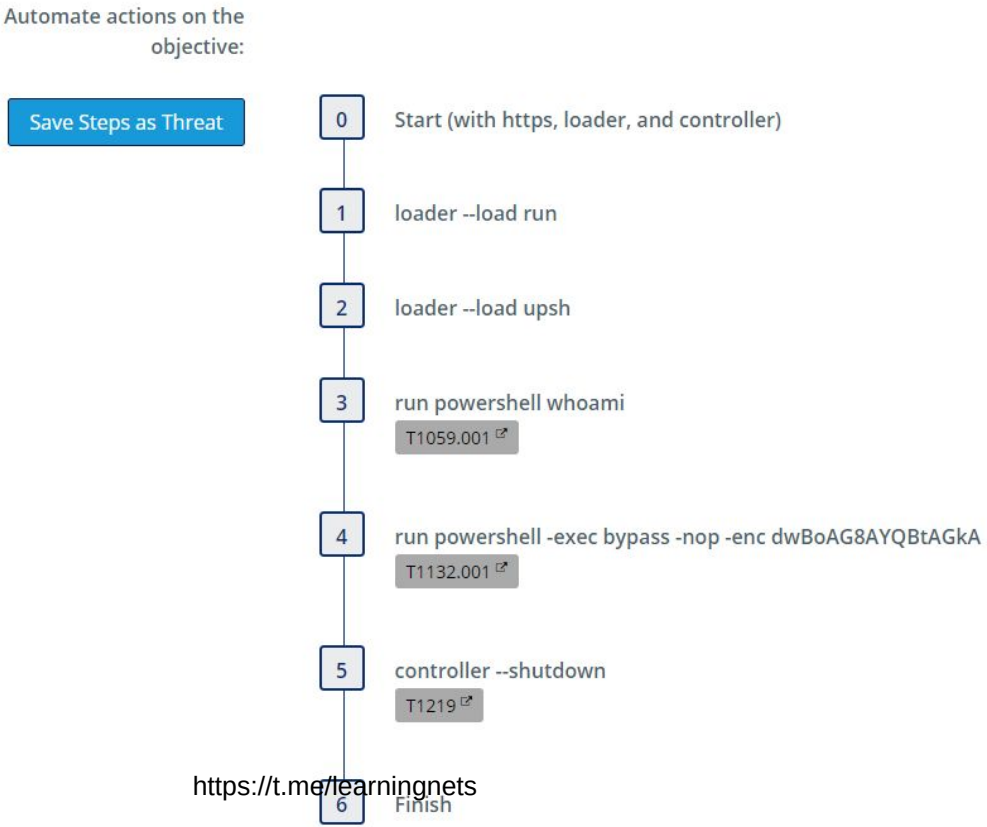
Week 2 - Implemented Controls

- Detecting and alerting for system discovery activities with Sysmon Event ID 1 Process Creation
    - ipconfig
    - netstat
    - dir, tree, ls, find, locate
    - net share, net view
- Detecting Command and Control activities:
    - **Sysmon Event ID 3 Network Connection** - Use threat intelligence or collections of known malicious addresses/IPs
    - **Sysmon Event ID 11 File Create** - Use Endpoint detection tools to help with the identification of known malicious dropper and Command & Control executables

Detecting powershell.exe

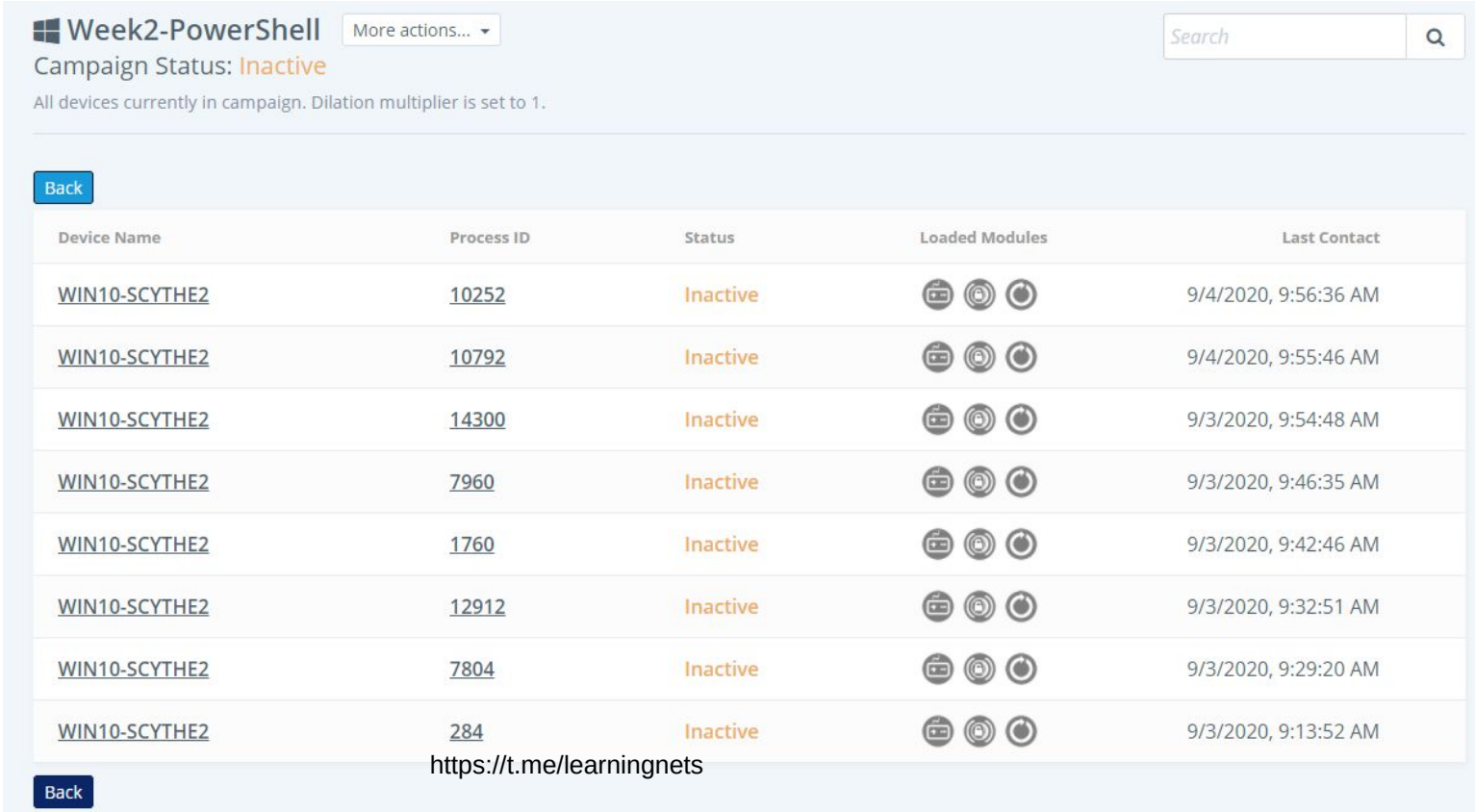
- Detecting powershell.exe with Sysmon Event ID 1 Process Creation
- “We do not use powershell.exe”
- Turned on alerting for Sysmon Event ID 1 w/powershell.exe
- Over 100 alerts per day
- NMFTA realized that they do use powershell.exe (thanks KACE)
- Had to tune out that alert
- Required retesting the same threat many times

Testing powershell.exe



SCYTHE

Testing powershell.exe... many times

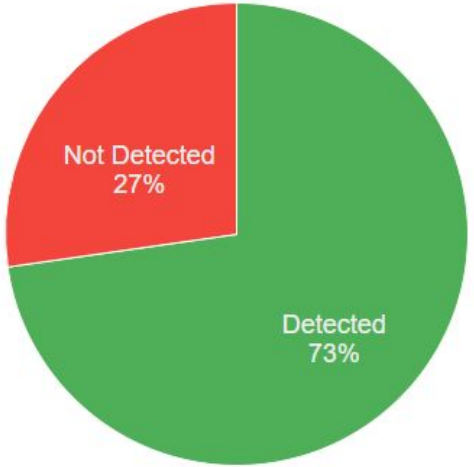


Week 2 APT19 - Detection

Overall Score

Above Average

Campaigns Aggregated	1
Test Cases Completed:	11
Test Cases Passed:	8
Detected:	8
Blocked:	0
Test Cases Failed:	3
Not Detected:	3
Test Cases Not Completed:	0
To Be Determined:	0

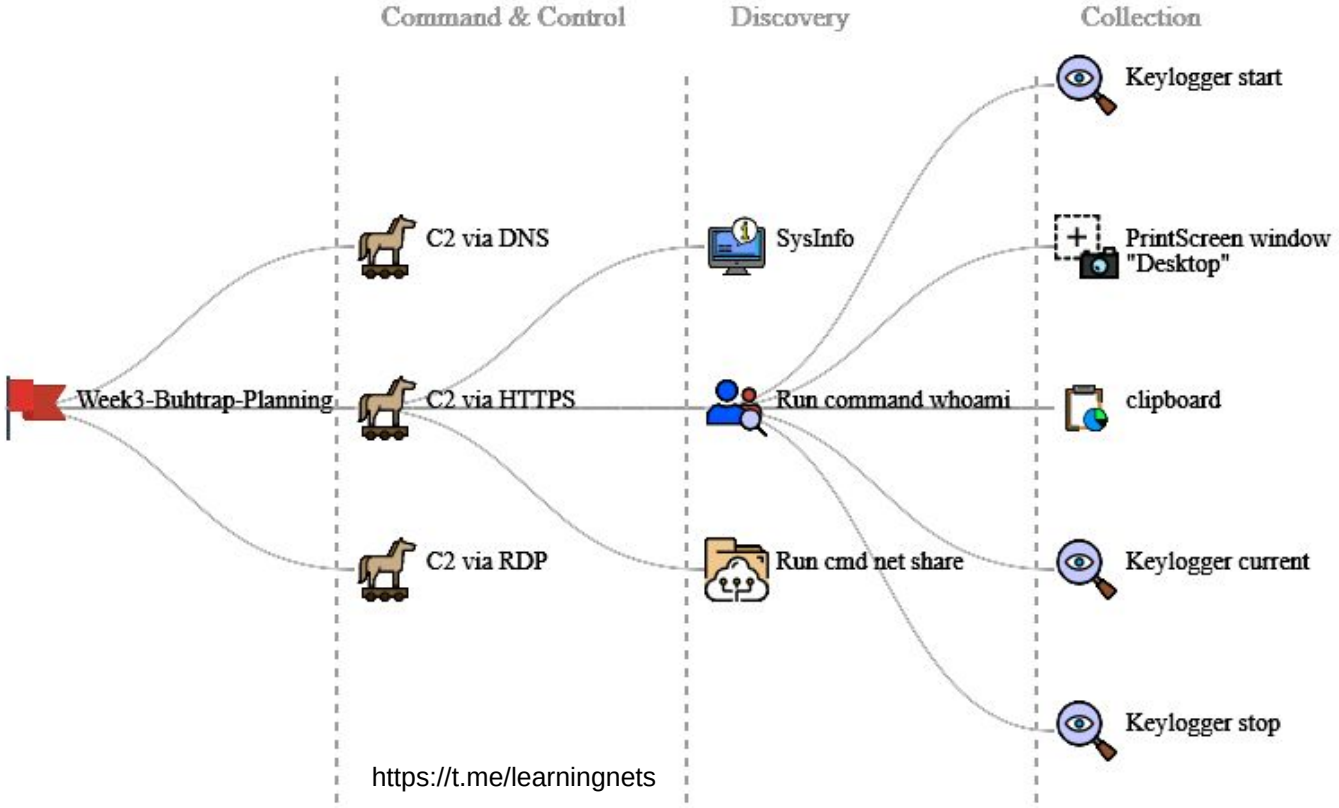


SCYTHE

Week 3 - Buhtrap

Tactic	Description
Description	Buhtrap group is a criminal team evolved from attacks against bank clients to attacks directly targeting financial institutions. At the moment, the group is known to target Russian and Ukrainian banks
Objective	Financial gain with over 1.8 billion rubles
Command and Control	Application Layer Protocol: Web Protocols (T1.071.001); Encrypted Channel (T1573); Custom Command and Control Protocol (T1094) - DNS Tunnelling & RDP
Initial Access	Spearphishing Link (T1192)
Execution	User Execution (T1204); Command and Scripting Interpreter: Windows Command Shell (T1059.003)
Defense Evasion	Deobfuscate/Decode Files or Information (T1140)
Discovery	File and Directory Discovery (T1083); Network Share Discovery (T1135)
Persistence	Scheduled Task (T1053)
Credential Access	Input Capture (T1056); Clipboard Data (T1115)

Week 3 Buhtrap - Planning



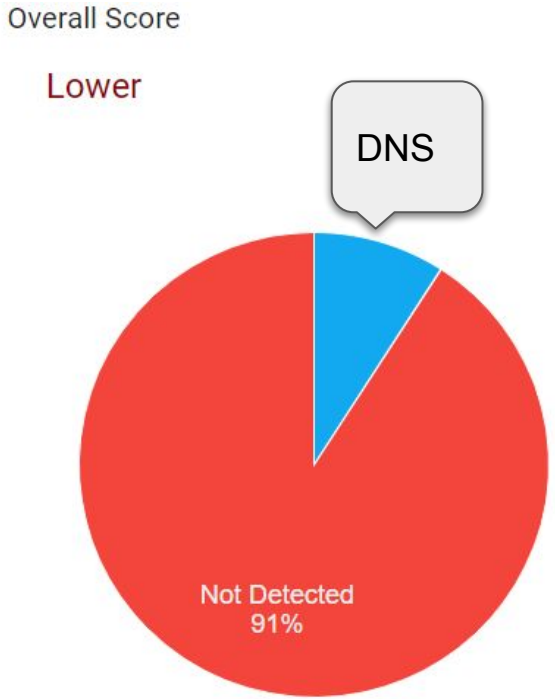
https://t.me/learningnets

Command and Control Channels

- While most adversaries operate over HTTP and HTTPS, there are other channels that may be used as long-haul C2
- Domain Name Service (DNS)
- Remote Desktop Protocol (RDP)
- LetMeOutOfYour.net - test for multiple egressing ports

Week 3 Buhtrap - Baseline

Campaigns Aggregated	1
Test Cases Completed:	11
Test Cases Passed:	1
Detected:	0
Blocked:	1
Test Cases Failed:	10
Not Detected:	10
Test Cases Not Completed:	0
To Be Determined:	



Week 3 - Implemented Controls

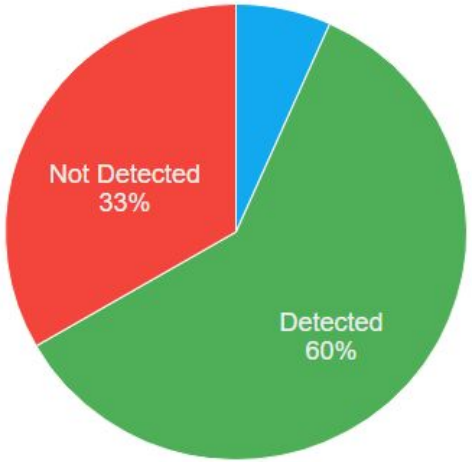
- Block Remote Desktop Protocol outbound - fixed in minutes
- Detecting Command and Control activities:
  - **Sysmon Event ID 3 Network Connection** - Use threat intelligence or collections of known malicious addresses/IPs
    - Monitor /Control /Proxy DNS requests
    - HTTPS exfiltration - Use threat intelligence for detecting activity to known malicious locations
- Detecting Windows API calls
  - Using Endpoint protection tools that have the ability to monitor for Windows API calls for information gathering techniques
    - Screen prints
    - Key logging
    - clipboard

Week 3 Buhtrap - Detection

Overall Score

Above Average

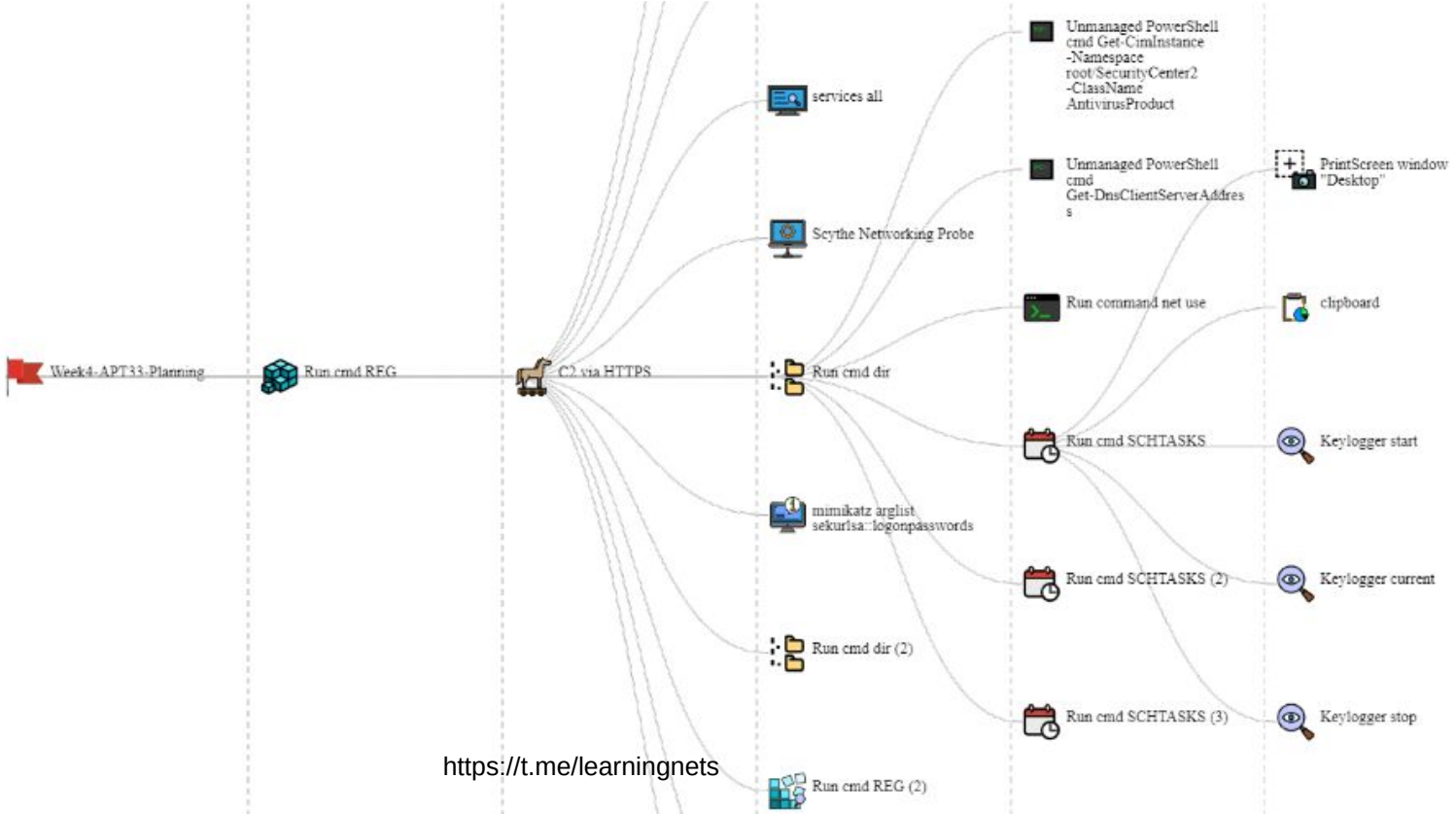
Campaigns Aggregated	1
Test Cases Completed:	15
Test Cases Passed:	10
Detected:	9
Blocked:	1
Test Cases Failed:	5
Not Detected:	5
Test Cases Not Completed:	0
To Be Determined:	0



Week 4 - APT33

Tactic	Description
Description	APT33 is a suspected Iranian threat group that has carried out operations since at least 2013. The group has targeted organizations in the United States, Saudi Arabia, and South Korea, in multiple industries including governments, research, chemical, engineering, manufacturing, consulting, finance, telecoms, and several other sectors.
Objective	Establishing persistent access to partners and suppliers of targets. Mounting supply chain attacks
Defense Evasion	T1132 - Data Encoding; T1480 - Execution Guardrails: Kill dates in payload; T1027 - Obfuscated Files or Information T1086 – PowerShell
Discovery	T1040 - Network Sniffing
Privilege Escalation	T1068 - Exploitation for Privilege Escalation
Persistence	T1060 - Registry Run Keys / Startup Folder; T1053 - Scheduled Task
Credential Access	T1003 - Credential Dumping: Publicly available tools like Mimikatz

Week 4 APT33 - Planning



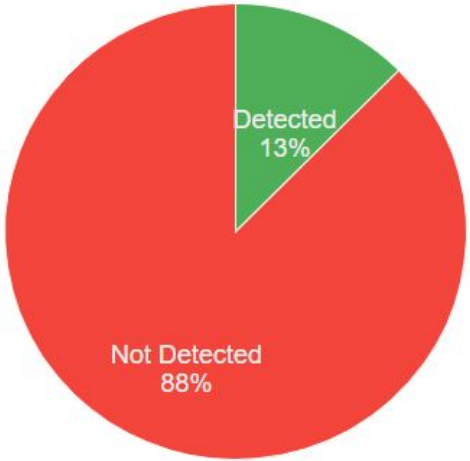
Week 4 APT33 - Baseline

Campaigns Aggregated	1
Test Cases Completed:	24
Test Cases Passed:	3
Detected:	3
Blocked:	0
Test Cases Failed:	21
Not Detected:	21
Test Cases Not Completed:	0
To Be Determined:	0

Overall Score

Lower

Scheduled Tasks



SCYTHE

Week 4 - Implemented Controls

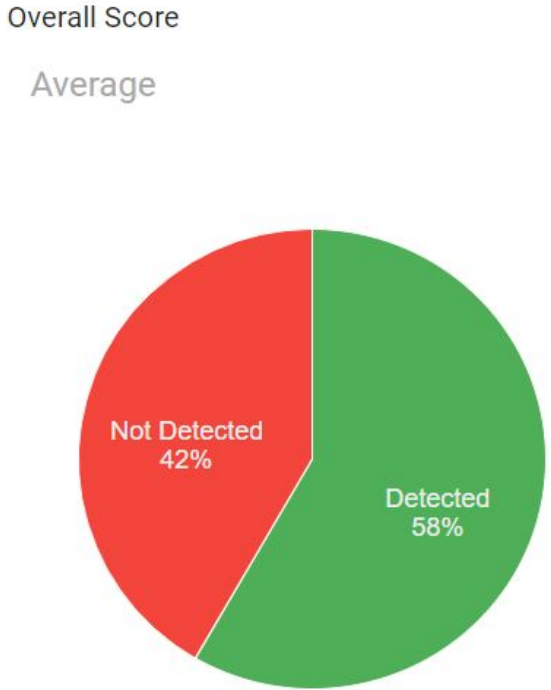
- Detecting system persistence activities:
  - **Sysmon Event ID 1 Process creation**
    - **Powershell** and CMD are commonly used for downloading and running executables or commands used to develop a strong hold on victim machines
  - **Sysmon Event ID 11 File Creation** - Dropper files
  - **Sysmon Event ID 12 Registry Modification** (Object create and delete)
  - **Sysmon Event ID 13 Registry Modification** (Value Set)
  - **Sysmon Event ID 14 Registry Modification** (Key and Value Rename)
    - Startup persistence: Scheduled Tasks & Run on Startup

Registry Keys

- Detecting registry key modifications are easy:
  - Sysmon Event ID 12 Registry Modification (Object create and delete)
  - Sysmon Event ID 13 Registry Modification (Value Set)
  - Sysmon Event ID 14 Registry Modification (Key and Value Rename)
- But extremely noisy:
  - Tied to monitor specific objects/keys related to below based on TTPs:
    - Startup activities
    - Stored Credentials
    - Accessibility features for input/image capture

Week 4 APT33 - Detection

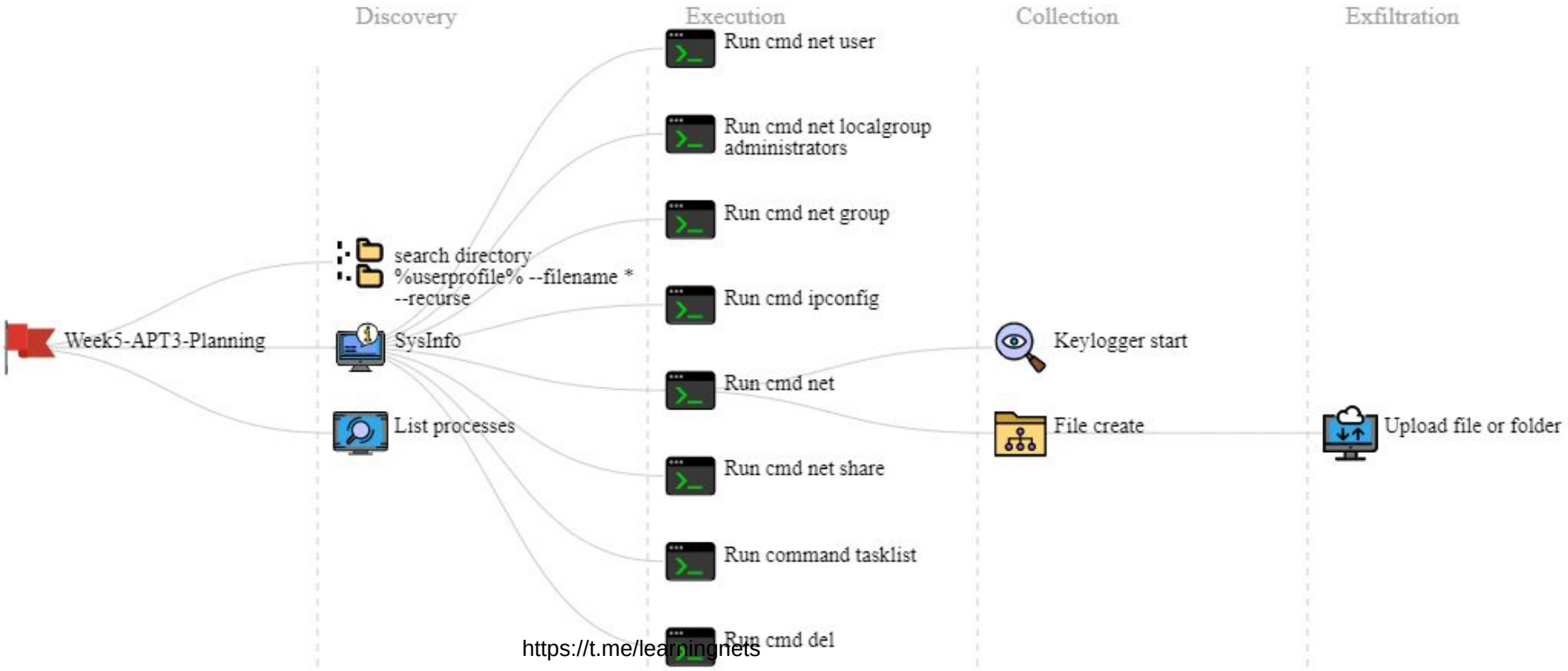
Campaigns Aggregated	1
Test Cases Completed:	24
Test Cases Passed:	14
Detected:	14
Blocked:	0
Test Cases Failed:	10
Not Detected:	10
Test Cases Not Completed:	0
To Be Determined:	0



Week 5 - APT3

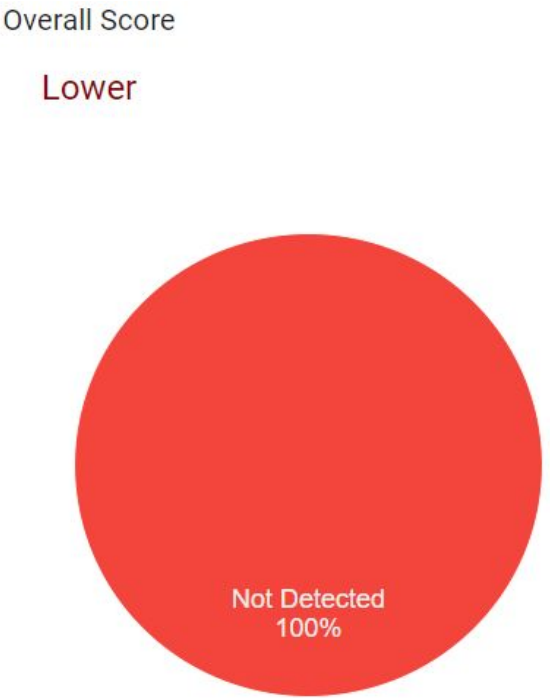
Tactic	Description
Description	APT3 is a China-based threat group that researchers have attributed to China's Ministry of State Security. This group is responsible for the campaigns known as Operation Clandestine Fox, Operation Clandestine Wolf, and Operation Double Tap. As of June 2015, the group appears to have shifted from targeting primarily US victims to primarily political organizations in Hong Kong.
Objective	Establishing persistent access to partners and suppliers of targets. Mounting supply chain attacks
Command and Control	Application Layer Protocol: Web Protocols (T1.071.001); Encrypted Channel (T1573)
Execution	User Execution (T1204); Command and Scripting Interpreter: Windows Command Shell (T1059.003)
Discovery	File and Directory Discovery (T1083)
Collection	Data from Local System (T1005); Data Staged (T1074); Input Capture (T1056)
Exfiltration	Exfiltration Over C2 Channel (T1041)

Week 5 APT3 - Plan



Week 5 APT3 - Baseline

Campaigns Aggregated	1
Test Cases Completed:	14
Test Cases Passed:	0
Detected:	0
Blocked:	0
Test Cases Failed:	14
Not Detected:	14
Test Cases Not Completed:	0
To Be Determined:	



Week 5 - Implemented Controls

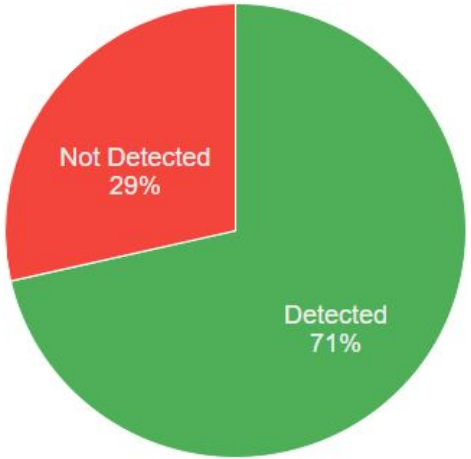
- Detecting Windows API calls
  - Using Endpoint protection tools that have the ability to monitor for Windows API calls for information gathering techniques: Screen prints, Key logging, clipboard
- Detecting Data Exfiltration activities:
  - **Sysmon Event ID 8 Create Remote Thread** - executables like rundll32.exe can be run remotely to kick of data collection and exfiltration
  - **Sysmon Event ID 11 File Creation** - Sensitive information copied to new files. Files can be encrypted or obfuscated using different techniques like changing file types, embedding in other files
  - **Sysmon Event ID 3 Network Connection** - Use threat intelligence or collections of known malicious addresses/IPs
    - Monitor /Control /Proxy DNS requests
    - HTTPS exfiltration - Use threat intelligence for detecting activity to known malicious locations

Week 5 APT3 - Detection

Campaigns Aggregated	1
Test Cases Completed:	14
Test Cases Passed:	10
Detected:	10
Blocked:	0
Test Cases Failed:	4
Not Detected:	4
Test Cases Not Completed:	0
To Be Determined:	0

Overall Score

Above Average

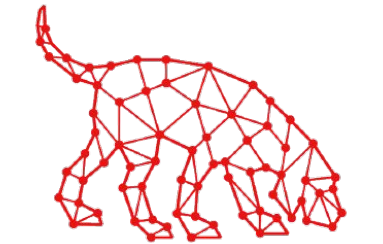


Week 6 - Free Play

- The final week of the exercise was reserved for Red Team free play
- Based on what has been learned and observed
- Focus and plan:
  - Windows Domain Controller Critical vulnerability - ZEROLOGIN
  - Microsoft Exchange
  - Domain Discovery
  - Lateral Movement

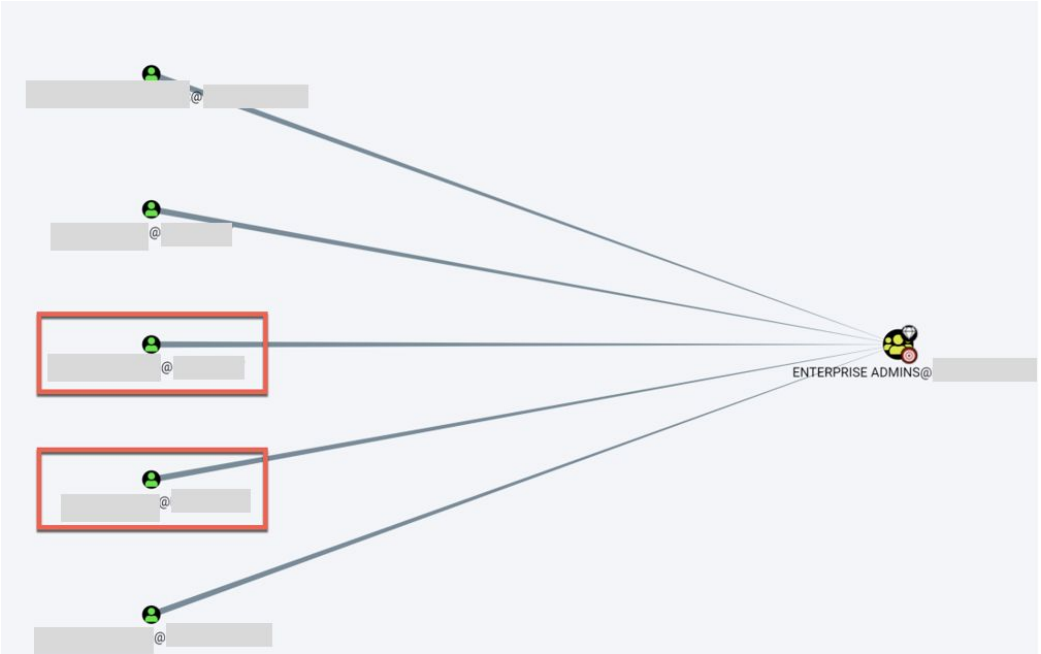
Bloodhound - Data Collection

- Sharphound was executed on WIN10-SCYTHE2
- Executes a large number of LDAP queries against the Domain Controller
- Discovers all users, machines, groups and ACL's
- Connects to all workstations and servers within the domain to identify local administrators and users with RDP privileges
- Not Detected - requires additional logging to detect LDAP queries and correlate successful logins across the domain



Standard Users found in Enterprise Admin Group

- Excessive number of users found in Enterprise Admin Group
- Notified NMFTA
- Resolved in minutes



SCYTHE

Microsoft Exchange and Windows Domain

- Two critical vulnerabilities being actively exploited in the wild
  - CVE-2020-0688 - RCE on Microsoft Exchange
  - CVE-2020-1472 - Zerologon - Reset Domain Controller credential
- Exploitation would provide immediate Domain Admin permissions
- Neither system was vulnerable
- Very quick patch management policy and process
  - Confirmed it was being followed during the 6 week engagement

Lateral Movement

- Lateral movement from WIN10-SCYTHE to WIN1-SCYTHE2
  - Failed due to antivirus and anti-exploit controls
- Numerous attempts were made utilizing various techniques
  - Psexec powershell
  - Powershell remoting
  - Lateral movement via Empire
  - Lateral movement via Scythe

Kerberoasting

- Discovered by Tim Medin of Red Siege
- Any domain authenticated user can request a service ticket
  - A portion of the ticket is encrypted using the service's password hash
  - Account to service mapping information can be obtained by requesting a list of Service Principal Names (SPN) from Active Directory
- No need to interact with the service
- Service does not even need to exist, just the account
  - Effective for old, defunct service accounts
  - Many service accounts have passwords that never expire
- Grab Tickets and then crack with Hashcat
- Result: a single account was identified as being Kerberoastable

Port scanning

- A port scan was run from WIN10-SCYTHE2
- The local subnet was scanned for all available TCP ports
- An alert was generated from an internal Honeypot


```
Nmap scan report for
Host is up, received arp-response (0.00s latency).
Scanned at 2020-09-29 15:32:20 Eastern Daylight Time for 16380s
Not shown: 65524 filtered ports, 3 closed ports
Reason: 65524 no-responses and 3 resets
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT     STATE SERVICE          REASON          VERSION
80/tcp   open  http             syn-ack ttl 64 VMware ESXi Server httpd
427/tcp  open  svrloc?          syn-ack ttl 64
443/tcp  open  ssl/https        syn-ack ttl 64 VMware ESXi SOAP API 6.7.0
902/tcp  open  ssl/vmware-auth  syn-ack ttl 64 VMware Authentication Daemon 1.10 (Uses VNC, SOAP)
5989/tcp open  ssl/wbem         syn-ack ttl 64 SBLIM Small Footprint CIM Broker
8000/tcp open  http-alt?        syn-ack ttl 64
8300/tcp open  tmi?             syn-ack ttl 64
9080/tcp open  ssl/soap         syn-ack ttl 64 gSOAP 2.8
MAC Address: 80:18:44:DE:69:54 (Dell)
Service Info: Host:                    ; CPE: cpe:/o:vmware:esxi, cpe:/o:vmware:ESXi:6.7.0
```

```
Nmap scan report for
Host is up, received arp-response (0.00s latency).
Scanned at 2020-09-29 15:32:20 Eastern Daylight Time for 16371s
Not shown: 65531 closed ports
Reason: 65531 resets
PORT     STATE SERVICE   REASON          VERSION
22/tcp   open  ssh       syn-ack ttl 64 OpenSSH 7.4 (protocol 2.0)
80/tcp   open  http      syn-ack ttl 64 Dell iDRAC 8 admin httpd (
443/tcp  open  ssl/http  syn-ack ttl 64 Dell iDRAC 8 admin httpd (
5900/tcp open  websocket syn-ack ttl 64 libwebsockets
MAC Address: 50:9A:4C:A8:4C:8A (Dell)
Service Info: CPE: cpe:/o:dell:idrac8_firmware
```

Exfiltration

- SCYTHE was used to create a 2 GB file
- The file was then exfiltrated to the SCYTHE Server
- No alerts were triggered

Network visibility is needed, such as netflow to analyze data from these test cases. EventSentry has modules for this.

End State

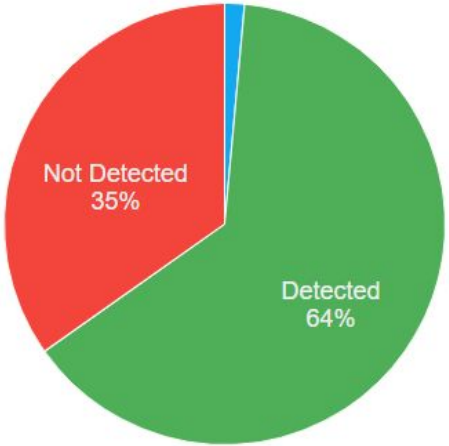
- $0 technology spend to achieve 64% detection rate
- Enabled telemetry (Sysmon)
- Enable logic for alerts on EVENTSENTRY

End State Result
Known threats will be detected and responded to before achieving objective

Campaigns Aggregated	5
Test Cases Completed:	69
Test Cases Passed:	45
Detected:	44
Blocked:	1
Test Cases Failed:	24
Not Detected:	24
Test Cases Not Completed:	0
To Be Determined:	0

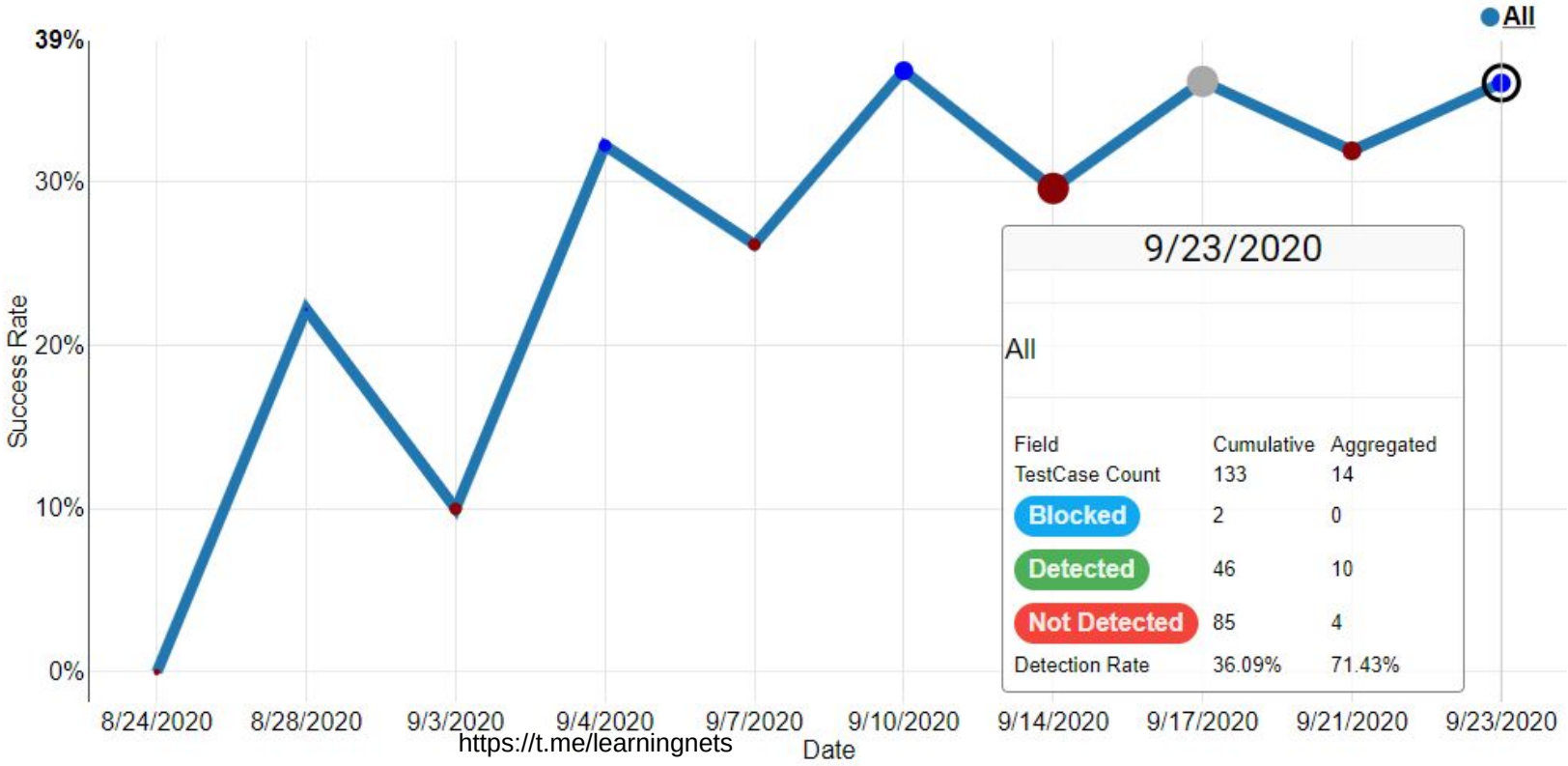
Overall Score

Above Average



SCYTHE

Trending - 72% detection rate



Recommendations

- Continue testing to ensure security controls/tuning is not degraded
- Consider network level detection for Command and Control and Exfiltration
- Increase sophistication level of threat actors as new threats are created
- Leverage the largest, public library of Adversary Emulation plans: https://github.com/scythe-io/community-threats

APT19	Organized
APT33	Create APT33_v2_scythe_threat.json (#23)
APT41	APT41 VFS files uploaded (#35)
Buhtrap	Organized
Chimera	Create Chimera_layer.json (#18)
ClipboardStealer	Create ClipboardStealer_scythe_threat.json (...
CozyBear	Organized
DeepPanda	Uploaded SCYTHE Threat (#12)
Emotet	Create emotet_layer.json
EvilCorp	Updated based on Talos CTI (#17)
HoneyBee	Init Commit: HoneyBee (#21)
Maze	Add flags for improved automation on reg/t...
Orangeworm	Add files via upload (#10)
PowerShell	Upload SCYTHE Threat and Navigator (#20)
Ransomware	Organized
SLOTHFULMEDIA	Slothfulmedia navigator json (#31)
SpeakUp	Create SpeakUp_for_OSX_scythe_threat.json

Recommendations

- Validate your assumptions
- Use ATT&CK and DETT&CT as a guide
- Find **your** detection average
- Advanced goals: 1-10-60*
  - When do my tools see it?
  - When does my team see it?
  - How long to respond?
  - How long to contain/remediate?

*https://www.crowdstrike.com/blog/crowdstrike-cto-explains-breakout-time-a-critical-metric-in-stopping-breaches/

Sharing to the Community

- Purple Team Exercise Framework is free: https://scythe.io/ptef
- Adversary Emulation Plans are free: https://github.com/scythe-io/community-threats
- Sysmon configurations are free: https://github.com/olafhartong/sysmon-modular
- All alert/logic created for NMFTA will be shared with the community via EventSentry: https://www.eventsentry.com/

Thank You!