



**2023
FIRST
Cyber Threat
Intelligence
Conference**

Berlin, Germany
November 6-8, 2023



Threat Quantification & Prioritization 101: A Practical Guide to Building (& Maintaining) Your Cyber Threat Profile

Simone Kraus, Orange Cyberdefense
Scott Small, Tidal Cyber
November 6, 2023

COPYRIGHT

Copyright © by Forum of Incident Response and Security Teams, Inc.

FIRST.org is the name under which Forum of Incident Response and Security Teams, Inc. conducts business.

This training material is licensed under Creative Commons Attribution-Non-Commercial-Share-Alike 4.0 (CC BY-NC-SA 4.0)

FIRST.org makes no representation, expressed or implied, with regard to the accuracy of the information contained in this material and cannot accept any legal responsibility or liability for any errors or omissions that may be made.

All trademarks are property of their respective owners.

Permissions beyond the scope of this license may be available at first-licensing@first.org

About the Speakers

- Simone

Security Analyst

DARC Team Orange Cyberdefense

<https://twitter.com/simonekrausora1>

<https://medium.com/@simone.kraus>

LinkedIn: "Simone Kraus"

<https://www.linkedin.com/in/simone-kraus-904080299/>



- Scott

Cyber Threat Intel Director

Tidal Cyber Adversary Intel Team

<https://twitter.com/IntelScott>

LinkedIn: "Scott Small"

<https://www.tidalcyber.com/blog>

<https://www.brighttalk.com/channel/19703/>



Packed Agenda!

Breaks as needed! 😊

- **08:30–09:00:** Introduction, What is a Threat Profile?, The Importance of Quantification, Our Approach
- **09:00–09:45:** Cyber Threat Quantification: Case Study & Guidance
- **09:45–10:30:** Taking Action on Your Threat Profile, TTPs & Scoring, CTI Extraction
- **10:30–11:00:** Threat Hunting, Detection Engineering, Use Case

Resources

<https://www.first.org/conference/berlin2023/program#pThreat-Quantification-Prioritization-101-A-Practical-Guide-to-Building-Maintaining-Your-Cyber-Threat-Profile>

- **No tools or materials are required for the workshop**
- **But a laptop with internet is helpful** for following along/browsing to resources of interest live alongside the presenters
- **Review/download of all resources is optional!** We will focus mainly on methodologies & workflows, but specific resources are provided for those who want to dive deeper as we go



**2023
FIRST
Cyber Threat
Intelligence
Conference**

Berlin, Germany
November 6-8, 2023

Importance of Threat
Quantification





**2023
FIRST
Cyber Threat
Intelligence
Conference**

Berlin, Germany
November 6-8, 2023

What is a Threat Profile?



What is a Threat Profile?

A buzzword?

‘Threat-Modeling’, the buzz word!



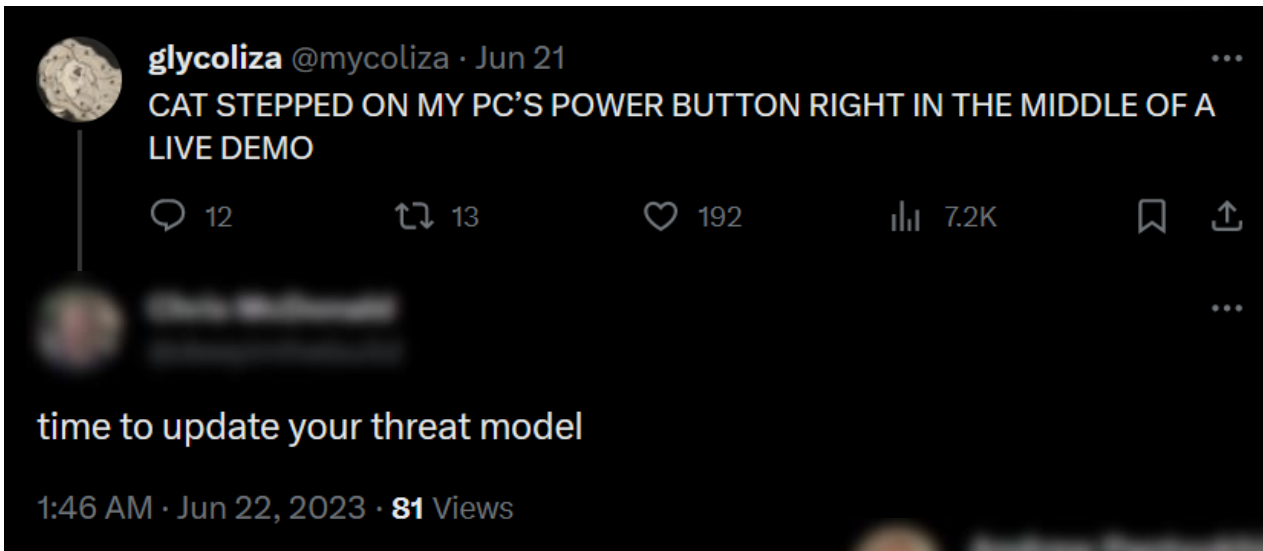
[\[Name\]](#) Follow

5 min read · Jul 13, 2020

What is a Threat Profile?

~~A buzzword~~

A meme?



What is a Threat Profile?

~~A buzzword~~

~~A meme~~

Simplest definition:

A collection of threats

What is a Threat Profile?

~~A buzzword~~

~~A meme~~

Slightly more granular definition:

A prioritized (rank-ordered) collection of relevant threats



**2023
FIRST
Cyber Threat
Intelligence
Conference**

Berlin, Germany
November 6-8, 2023

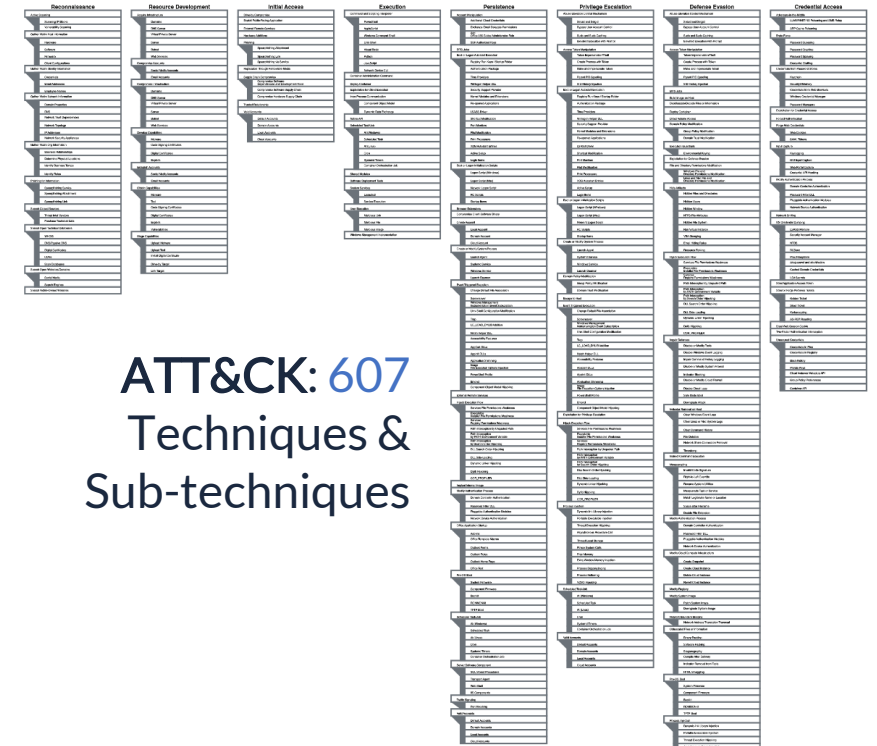
The Importance of Quantification



Threat Landscape: A Few Truths

The landscape is growing: **more threats** (groups & malware) are identified each year

- Mandiant: **3,500** groups (+900), **588** new malware families
- Microsoft: **300** actors (**160** nation state + **50** ransomware)
- Google: **270** state actors, associated w/ **50+** countries
- 2023: Now **over 600** ATT&CK Techniques & Sub-Techniques



ATT&CK: 607
Techniques &
Sub-techniques

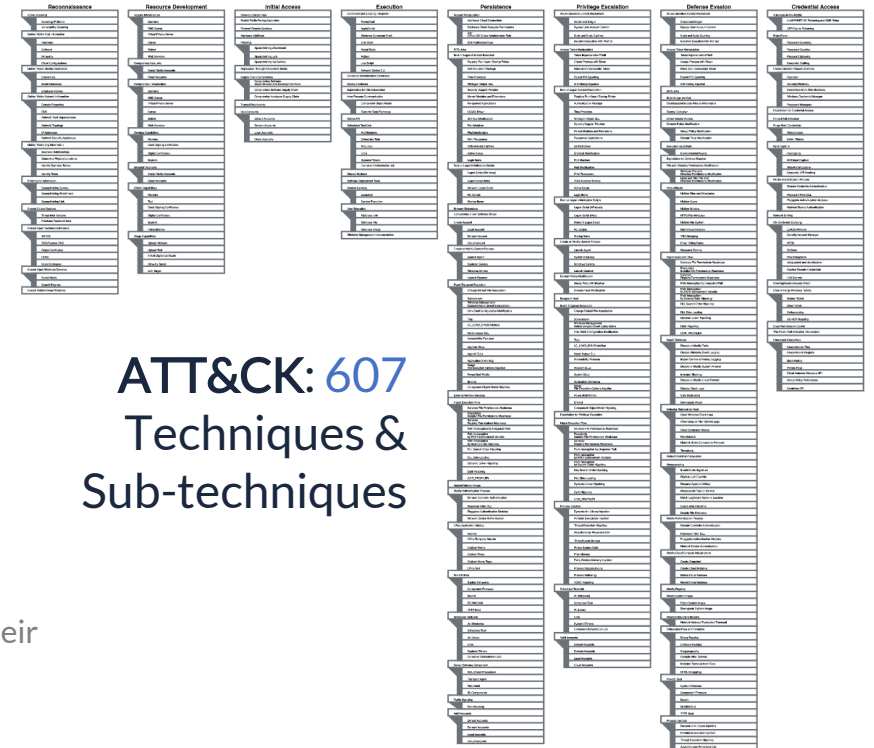
Threat Landscape: A Few Truths

The landscape is growing: **more threats** (groups & malware) are identified each year

- Mandiant: **3,500** groups (+900), **588** new malware families
- Microsoft: **300** actors (**160** nation state + **50** ransomware)
- Google: **270** state actors, associated w/ **50+** countries
- 2023: Now **over 600** ATT&CK Techniques & Sub-Techniques

Threat intelligence **resources are usually limited**

- Budgets are tight – in many cases stagnant, shrinking, or at least not keeping pace with threat landscape expansion
 - December 2022 Neustar survey: 49% of companies did not have sufficient budget to address their cybersecurity needs
- **No team** can track and address every threat at all times



ATT&CK: 607
Techniques &
Sub-techniques

Threat Landscape: A Few Truths

The landscape is growing: **more threats** (groups & malware) are identified each year

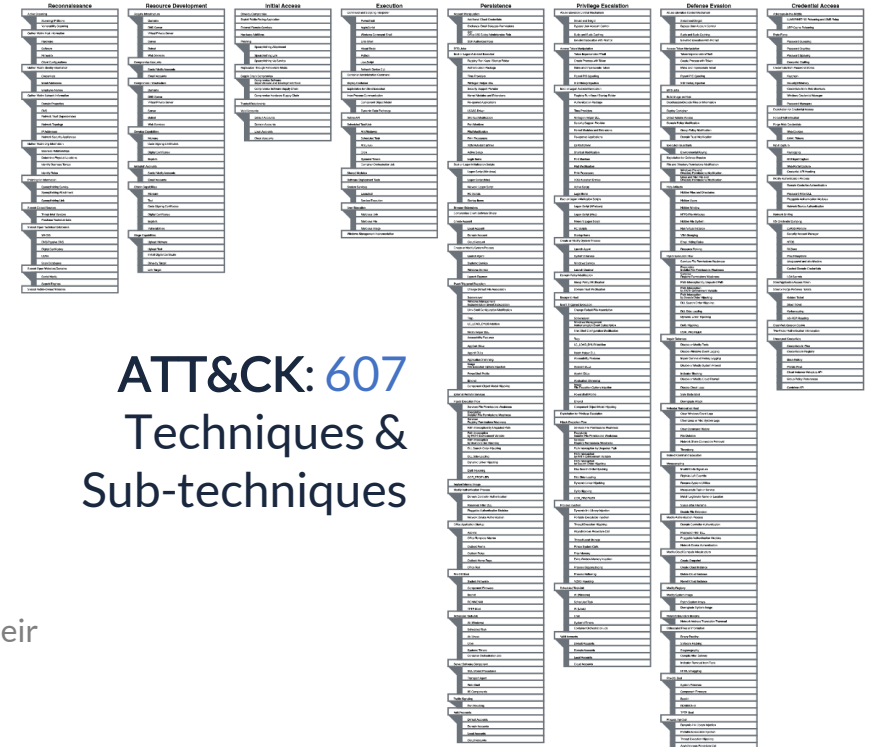
- Mandiant: **3,500** groups (+900), **588** new malware families
- Microsoft: **300** actors (**160** nation state + **50** ransomware)
- Google: **270** state actors, associated w/ **50+** countries
- 2023: Now **over 600** ATT&CK Techniques & Sub-Techniques

Threat intelligence **resources are usually limited**

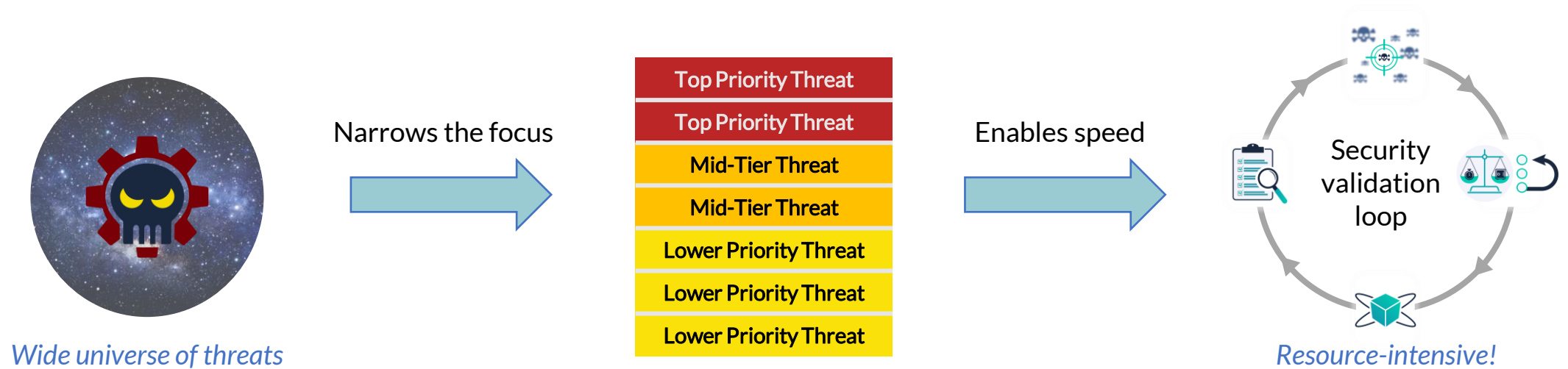
- Budgets are tight – in many cases stagnant, shrinking, or at least not keeping pace with threat landscape expansion
 - December 2022 Neustar survey: 49% of companies did not have sufficient budget to address their cybersecurity needs
- **No team** can track and address every threat at all times

Threat prioritization is a *must*

- Prioritization can only happen with consistency, repeatability, and limited bias **via quantification**



The Importance of Threat Quantification: Visualized



But don't take our word for it... A few classic case studies/examples:

- [Nationwide: Using Threat Intelligence to Focus ATT&CK Activities \(YouTube\)](#)
- [Red Canary: How to prioritize effectively with Threat Modeling and ATT&CK \(YouTube\)](#)
- [Katie Nickels: Resistance Isn't Futile \(YouTube\)](#)
- [John Hubbard: Hunting for Post-Exploitation Stage Attacks \(YouTube\)](#)
- [Sajid Nawaz Khan: Adversarial Threat Modelling \(GitHub\)](#)
- [Andy Piazza: Quantifying Threat Actors with Threat Box \(Medium\)](#)
- [Katie Nickels: Getting Started with ATT&CK: Threat Intelligence \(Medium\)](#)
- [Katie Nickels & Adam Pennington: Using ATT&CK for CTI Training \(ATT&CK\)](#)
- [Emulation Planning for Purple Teams \(AttackIQ Academy\)](#)

All listed here: github.com/tidalcyber/cyber-threat-profiling

2023
FIRST
Cyber Threat
Intelligence
Conference

Berlin, Germany
November 6-8, 2023

Threat Profiling's Value (& Limitations)



Value & Strengths + Challenges & Limitations

- Benefits of following a threat profiling methodology: **Structure, Repeatability, Relevance, Evidence-based, Proactive**
- Existing approaches generally fall short in at least 1 of 3 ways
- Pursuit of near-perfect data often deters/impedes efforts
- Caution: This is a *starting point!*

Factor	Limitation	Our Approach
Defensive Scope/Coverage	Asset- or system-centric	Enterprise (Organization)-centric
Threat Scope/Coverage	Focus on high-level threat categories or scenarios	<p>Focus on adversaries supports progressive pivoting from organizational context to identification of relevant threats and their capabilities & behaviors, and ultimately to relevant defenses</p> <p>Surface granular adversarial behaviors that align with discrete defensive capabilities</p>
Complexity	Lengthy, usually require SME input	Can be completed by staff with varied skill levels and across team roles/disciplines

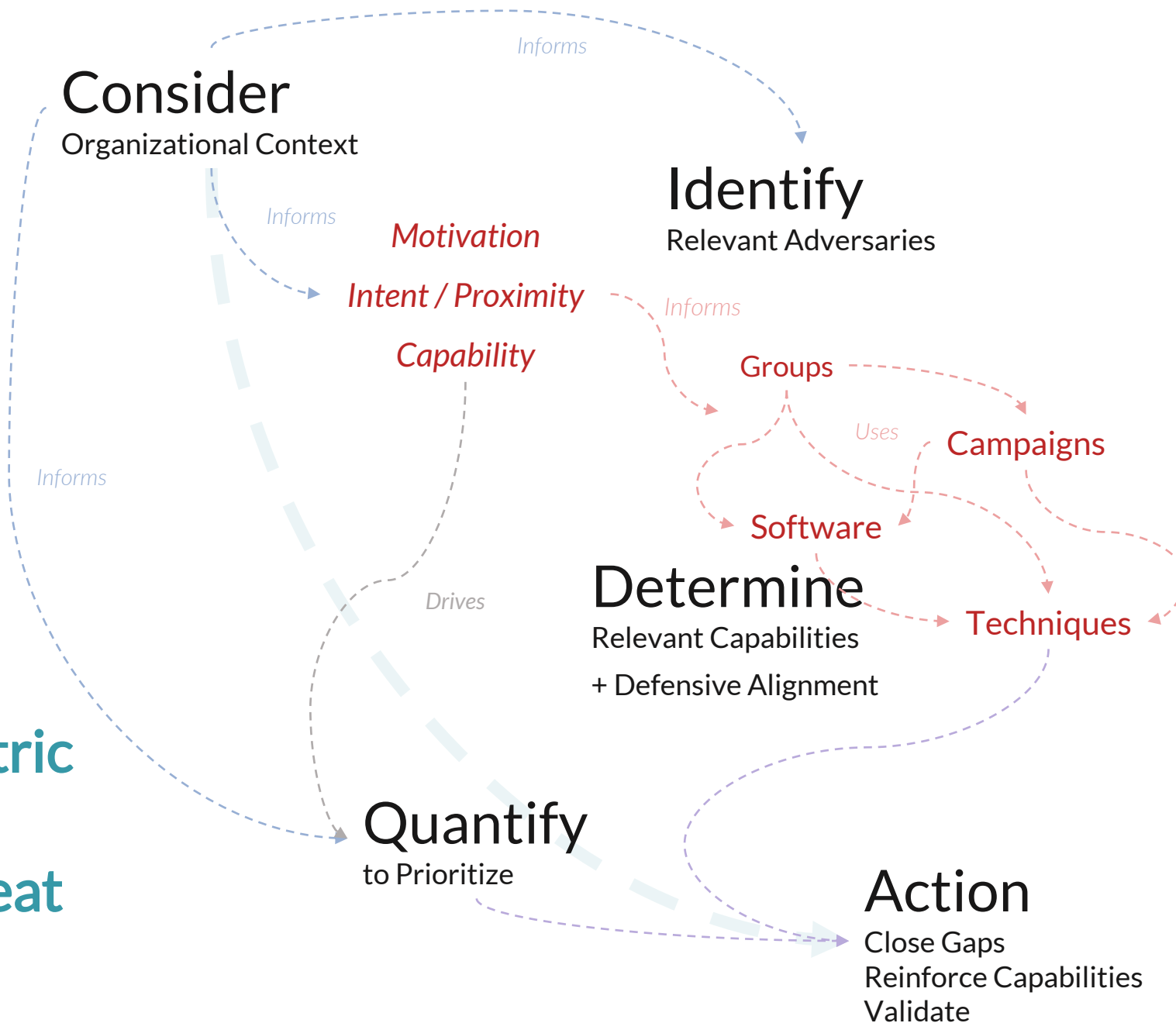
Threat Profiling Approach: Key Elements

- Consider Organizational Context
- Identify Relevant Adversaries
 - Determine Relevant Capabilities
 - Defensive Alignment
- Quantify to Prioritize
- Take Action!

Threat Profiling Approach: Key Elements

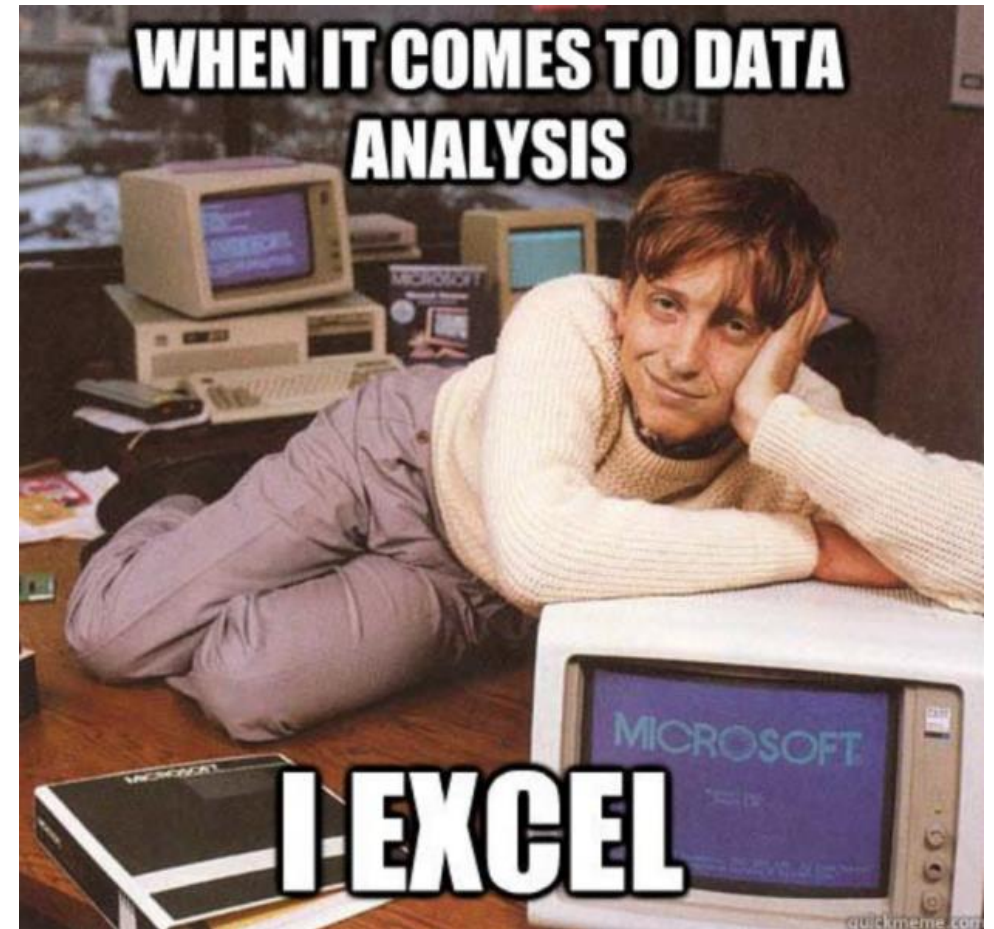
- Consider Organizational Context
- **Identify Relevant Adversaries**
 - **Determine Relevant Capabilities**
 - Defensive Alignment
- **Quantify to Prioritize**
- Take Action!

Enterprise-Centric Adversary Behavioral Threat Profiling



Threat Profile: Logistics

- Threat Profile: A prioritized **list** of relevant threats
 - Adversaries, capabilities, & techniques
- *Any list-documentation* tool or software will do
 - Notetaking/word processor
 - Spreadsheet software (simple calculations)
 - Scripts and/or dashboarding software as you mature
- Threat Profiling: It's About the **Mindset**



2023
FIRST
Cyber Threat
Intelligence
Conference

Berlin, Germany
November 6-8, 2023

Case Study: European
Healthcare Organization



General Guidance: Quantifying Complex Threat Concepts

- Threat = **Intent** x **Capability** x Opportunity
- What we will accomplish:
 - Measure threats according to factors including **Proximity/Intent**, “density”, **Capability & Capacity**, and **organizational priority**
 - **Prioritize (rank order)** based on relative final weightings/scores
- Scoring ranges: Scale relative to your team’s resources, bandwidth, and/or current maturity/expertise:
 - **1-5 is most common in practice**
 - 2- to 3-point all the way to 100-point



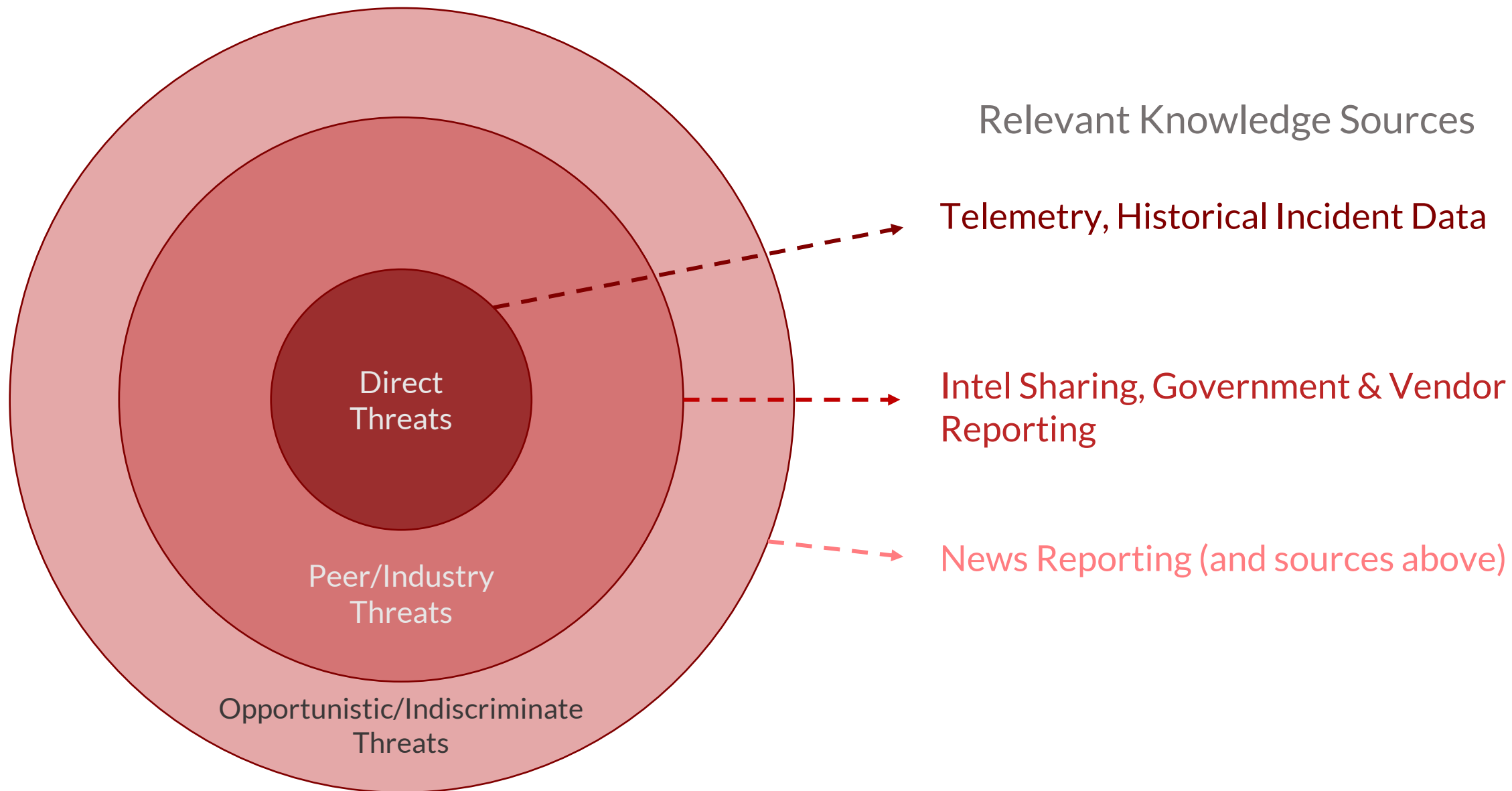
**2023
FIRST
Cyber Threat
Intelligence
Conference**

Berlin, Germany
November 6-8, 2023

Identify Relevant Adversaries
(Populating our List)



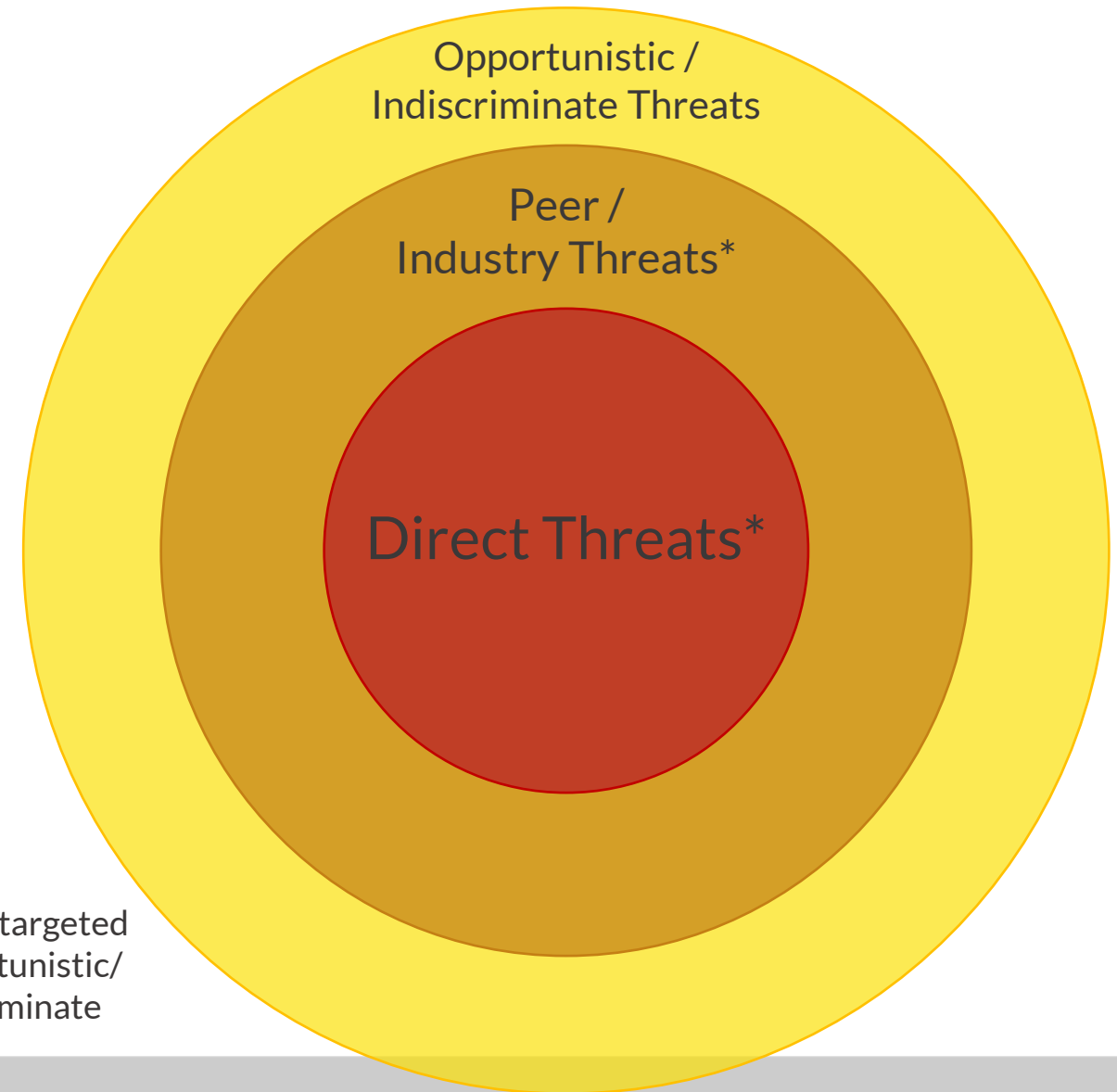
Surfacing Relevant Adversaries



Approximating Adversary Intent

- We rarely have clear evidence pointing to adversaries' ultimate intentions
- Look to the **growing body** of cyber incident evidence to gauge approximations of them
 - We believe a **critical mass of data now exists**
- General recommendation: **Three "proximity" tiers**
 - Note as you go!

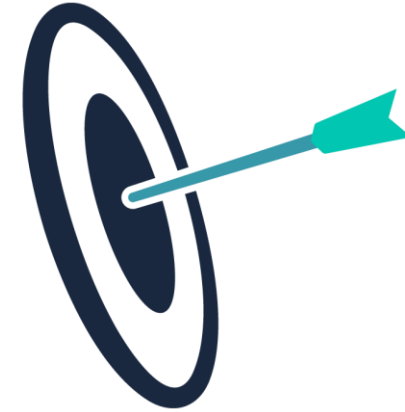
A Practical Approach to Approximating Adversary Intent



* May be targeted or opportunistic/indiscriminate

Surfacing Direct Threats

- Smart to include what you already know!
 - (But some teams like to perform independent assessments)
- Lean on your partners – many teams aren't consistently attributing threats
 - (And that's ok! See especially Ch. 5 of [The Risk Business](#) by Levi Gundert)



Adversary or Campaign Name	Proximity Tier	Evidence	Proximity Score
Andariel	Direct Threat	Our team attributed with moderate confidence a 2021 incident to this group	5
Wizard Spider	Direct Threat	Our endpoint vendor has quarantined multiple samples of malware distributed by this group	5
TA1337	Direct Threat	Our email security vendor blocked phishing emails attributed to this group	5

Surfacing Proximate Threats

- **Common CTI metadata:** victim sector, location, and/or organization size
- **Common sources:** government and national CERT advisories, public or commercial vendor reporting, independent analyses (incident response or malware analysis/threat research blogs)
- **Aggregation resources** will save you time!

Some Favorites:

ETDA/ThaiCERT: Threat Encyclopedia: apt.etcha.or.th/cgi-bin/aptgroups.cgi

AlienVault OTX: otx.alienvault.com

MISP Threat Actor Galaxy: github.com/MISP/misp-galaxy/blob/main/clusters/threat-actor.json

SecureWorks Cyber Threat Group Profiles: secureworks.com/research/threat-profiles

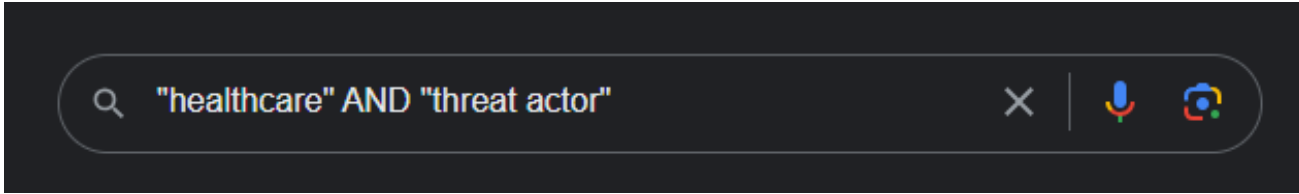
Palo Alto Unit42 Playbooks: pan-unit42.github.io/playbook_viewer

CrowdStrike Adversary Industries: adversary.crowdstrike.com/en-US/industries

[APT Groups & Operations \(public Google Sheet\)](#)

Tidal structured Group metadata (ATT&CK & public sources): app.tidalcyber.com/groups

Surfacing Proximate Threats: Case Study Examples



(20 threats)

MITRE | ATT&CK

Matrices | Tactics | Techniques | Data Sources | Mitigations | Groups | Software | Campaigns | Resources | Blog | Contribute | Search

healthcare

C0010, Campaign C0010
C0010 C0010 was a cyber espionage campaign conducted by UNC3890 that targeted Israeli shipping, government, aviation, energy, and **healthcare** organizations. Security researcher assess UNC3890 conducts operations in support of Iranian interests, and noted several limited technical connections to Iran, including PDB strings and Far...

Orangeworm, Group G0071
Orangeworm Orangeworm is a group that has targeted organizations in the **healthcare** sector in the United States, Europe, and Asia since at least 2015, likely for the purpose of corporate espionage.[1] ID: G0071 Contributors: Elger Vinicius S. Rodrigues, @elgervinicius, CYB...

Tonto Team, Earth Akhlut, BRONZE HUNTLEY, CactusPete, Karma Panda, Group G0131
... by 2020 they expanded operations to include other Asian as well as Eastern European countries. Tonto Team has targeted government, military, energy, mining, financial, education, **healthcare**, and technology organizations, including through the Heartbeat Campaign (2009-2012) and Operation Bitter Biscuit (2017).[1][2][3][4][5][6] ID: G0131 ⓘ Associated Groups: Earth Akhlut, BRONZ...

Leviathan, MUDCARP, Kryptonite Panda, Gadolinium, BRONZE MOHAWK, TEMP.Jumper, APT40, TEMP.Periscope, Group G0065
... filiated front company.[1] Active since at least 2009, Leviathan has targeted the following sectors: academia, aerospace/aviation, biomedical, defense industrial base, government, **healthcare**, manufacturing, maritime, and transportation across the US, Canada, Europe, the Middle East, and Southeast Asia.[1][2][3] ID: G0065 ⓘ Associated Groups: MUDCARP, Kryptonite Panda, Gadolinium...

Deep Panda, Shell Crew, WebMasters, KungFu Kittens, PinkPanther, Black Vine, Group G0009
... Deep Panda Deep Panda is a suspected Chinese threat group known to target many industries, including government, defense, financial, and telecommunications. [1] The intrusion into **healthcare** company Anthem has been attributed to Deep Panda. [2] This group is also known as Shell Crew, WebMasters, KungFu Kittens, and PinkPanther. [3] Deep Panda also appears to be known as Black V...

menuPass, Cicada, POTASSIUM, Stone Panda, APT10, Red Apollo, CVNX, HOGFISH, Group G0045
... Chinese Ministry of State Security's (MSS) Tianjin State Security Bureau and worked for the Huaying Haitai Science and Technology Development Company.[1][2] menuPass has targeted **healthcare**, defense, aerospace, finance, maritime, biotechnology, energy, and government sectors globally, with an emphasis on Japanese organizations. In 2016 and 2017, the group is known to have targ...

APT41, Wicked Panda, Group G0096
... archers have assessed as Chinese state-sponsored espionage group that also conducts financially-motivated operations. Active since at least 2012, APT41 has been observed targeting **healthcare**, telecom, technology, and video game industries in 14 countries. APT41 overlaps at least partially with public reporting on groups including BARIUM and Wintti Group.[1][2] ID: G0096 ⓘ Assoc...

Tropic Trooper, Pirate Panda, KeyBoy, Group G0081
... Trooper is an unaffiliated threat group that has led targeted campaigns against targets in Taiwan, the Philippines, and Hong Kong. Tropic Trooper focuses on targeting government, **healthcare**, transportation, and high-tech industries and has been active since 2011.[1][2][3] ID: G0081 ⓘ Associated Groups: Pirate Panda, KeyBoy Contributors: Edward Millington; Bart Parys Version: 1...

Surfacing Proximate Threats: Case Study Examples

THREAT PROFILES

Explore the latest threat group definitions and profiles published by the Secureworks® Counter Threat Unit™ (CTU) Research Team.

CYBERCRIME

GOLD RAINFOREST

Objectives Extortion, Financial gain
Aliases Lapsus\$, Strawberry Tempest (Microsoft)
Tools Mimikatz

GOLD RAINFOREST was an international threat group responsible for the compromises of high-profile organisations conducted between mid-2021 and September 2022 under the banner of the Lapsus\$ hack-and-leak group. Originally thought to be financially motivated, group members may have been driven more by the desire to boost their reputations on underground...

[READ MORE](#)

CYBERCRIME

GOLD SOUTHFIELD

Objectives Financial gain, Ransomware
Tools REvil

GOLD SOUTHFIELD was a financially motivated cybercriminal threat group that authored and operated the REvil (aka Sodinokibi) ransomware on behalf of various affiliated threat groups. Operational from April 2019 to January 2023, the group obtained the GandCrab source code from GOLD GARDEN, the operators of GandCrab that voluntarily withdrew their...

[READ MORE](#)

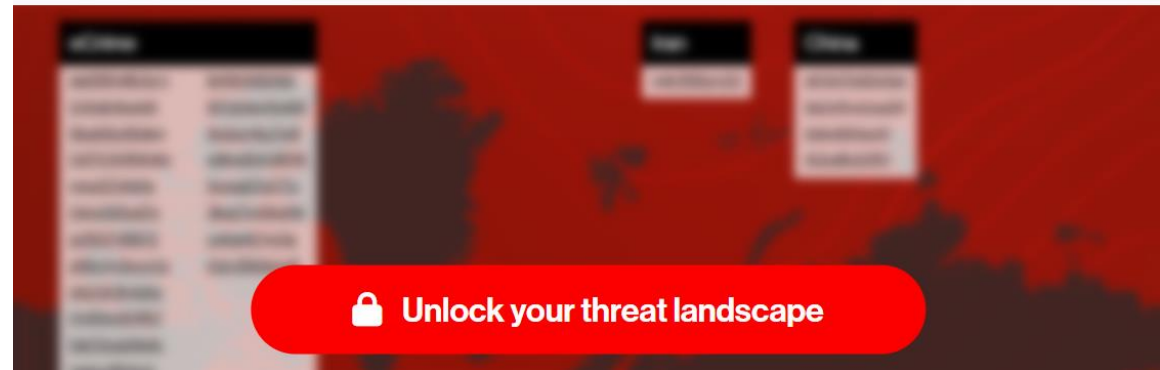
Know them. Find them. Stop them.

Discover the adversaries targeting your industry.

Your Industry: Business Size: Your Country: [Clear](#) [Update Search](#)

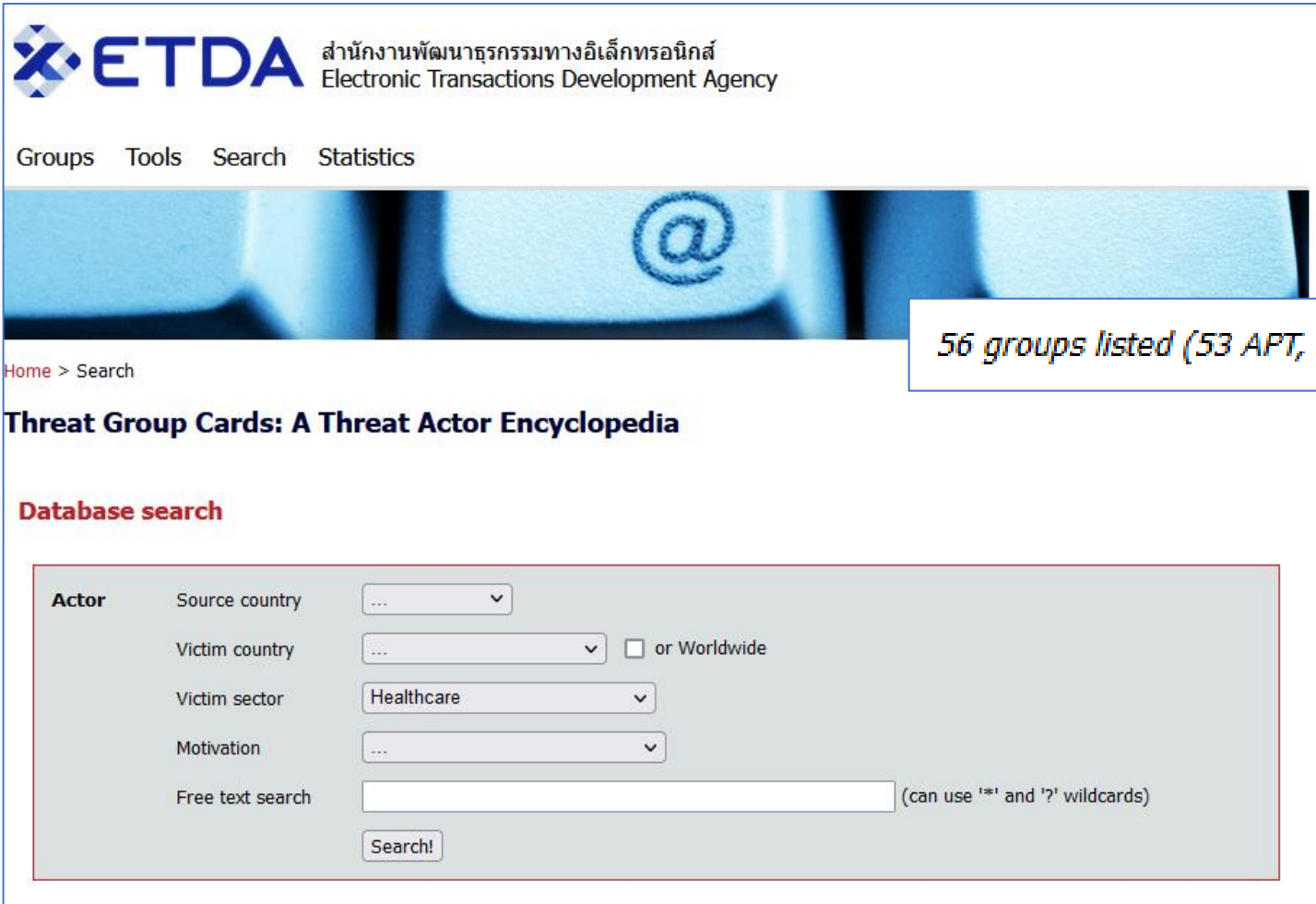
Your Threat Landscape [Back to Global Threat Landscape](#)

 Adversaries potentially targeting you **29** of **225**



[Unlock your threat landscape](#)

Surfacing Proximate Threats: Case Study Examples



The screenshot shows the ETDA (Electronic Transactions Development Agency) website. The header includes the ETDA logo and name in Thai and English. Navigation links for Groups, Tools, Search, and Statistics are visible. A banner image shows a close-up of a keyboard key with an '@' symbol. Below the banner, a search bar is present. A callout box highlights the search results: "56 groups listed (53 APT, 3 other, 0 unknown)". The main content area is titled "Threat Group Cards: A Threat Actor Encyclopedia" and features a "Database search" section with the following filters:

- Actor
- Source country: [Dropdown menu]
- Victim country: [Dropdown menu] or Worldwide
- Victim sector: Healthcare [Dropdown menu]
- Motivation: [Dropdown menu]
- Free text search: [Text input field] (can use '*' and '?' wildcards)
- Search! [Button]



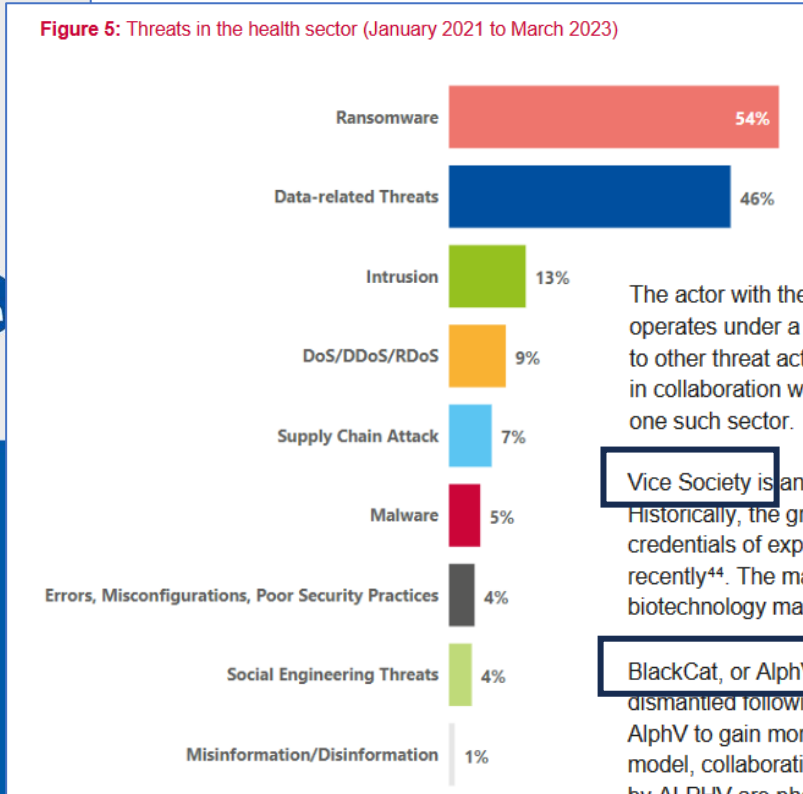
56 groups listed (53 APT, 3 other, 0 unknown)

“Observed”? “Targeted”?

Surfacing Proximate Threats: Case Study Examples



The graphic features the ENISA logo and the European Union flag at the top. Below them is a network diagram with a central red warning triangle and various icons representing healthcare and technology. The main title is 'ENISA THREAT LANDSCAPE: HEALTH SECTOR' in large white letters on a blue background. Below the title, it says '(January 2021 to March 2023)' and 'JULY 2023'.



The actor with the most observed incidents is LockBit 3.0, also referred to as Lockbit Black (20 incidents). The group operates under a Ransomware-as-a-Service (RaaS) model, which enables them to distribute their malicious software to other threat actors. Previous instances of this threat actor group were named LockBit 2.0 and LockBit. By working in collaboration with affiliates, the group extends its reach and targets a diverse range of sectors, healthcare being one such sector.

Vice Society is another ransomware gang that has been involved in high-profile attacks. It has been active since 2019. Historically, the group had been deploying variants of existing ransomware strains by leveraging compromised credentials of exploited internet-facing applications⁴³. The group, however, started deploying their own locker software recently⁴⁴. The main types of entities impacted by Vice Society were hospitals (6 incidents), medical device and biotechnology manufacturers (2 incidents) out of a total of 9 incidents during the reporting period.

BlackCat, or AlphV ransomware group, has been active since November 2021 but got more traction after REvil was dismantled following arrests in Russia at the beginning of 2022. This event provided an opportunity for BlackCat or AlphV to gain more traction and attention. Like other ransomware groups, they employ an affiliate-based business model, collaborating with other threat partners to carry out their attacks. The main types of entities that were impacted by ALPHV are pharmaceutical companies (3 incidents) out of a total of 5 incidents during the reporting period.

Other ransomware groups that have been active during the reporting period include Conti, Hive, LV, RansomEXX, RansomHouse (3 incidents each) and Wizard Spider and REvil (2 incidents each), followed by single instances of other groups.

<https://www.enisa.europa.eu/publications/health-threat-landscape>

Surfacing Proximate Threats: Case Study Examples



<https://www.hhs.gov/sites/default/files/types-threat-actors-threaten-healthcare.pdf>

Named adversary Groups/Software:

LockBit 3.0

Clop*

Royal*

BianLian

Lapsus\$*

KillNet

Andariel*

APT41*

NoName057(16)

*In ATT&CK (v13)

Surfacing Proximate Threats: Case Study Examples



<https://www.cyfirma.com>



Named adversary Groups/Software
("observed campaigns"):

TA505* (6)

MISSION2025* (3)

Cozy Bear* (3)

Stone Panda* (2)

Lazarus Group* (2)

Fancy Bear* (1)

*In ATT&CK (v13)

Note as you go!



**2023
FIRST
Cyber Threat
Intelligence
Conference**

Berlin, Germany
November 6-8, 2023

Threat Prioritization ("Quantifying" our List)



What Now? Key Inclusion/Narrowing Factors

Ranked by feasibility (in the presenter's experience):

1. Referenced by multiple sources
 - a. Source quality/reliability/confidence (“Source Value”) – “Targeted” vs. “Observed” activity?
2. Wider industry vs. specific sub-sector vs. immediate Peer impact ← Note as you go!
3. Threat has (ATT&CK) TTPs? (Bandwidth limitations)

Surfacing Proximate Threats: Tally the Results

ATT&CK Website	Secureworks	Thai CERT	ENISA	HHS	Cyfirma
Operation Wocao	LAPSUS\$	APT1	LockBit 3.0	LockBit 3.0	TA505
Whitefly	GOLD SOUTHFIELD	APT18	Vice Society	Clop	menuPass
C0010	REvil	APT28	BlackCat	Royal	APT29
Fox Kitten		APT33	Conti	BianLian	APT10
Leviathan		APT37	Hive	Lapsus\$	Lazarus Group
EXOTIC LILY		APT41	LV	KillNet	APT28
Tonto Team		APT-C-36	RansomEXX	Andariel	
Tropic Trooper		BlackTech	RansomHouse	APT41	
APT41		Carbanak	Wizard Spider	NoName057(16)	
Orangeworm		Cleaver	REvil		
LAPSUS\$		Dark Caracal			
menuPass		Darkhotel			
Deep Panda		FIN4			
FIN4		FIN8			
Clop		Fox Kitten			
EKANS		Higaisa			
Pysa		Indrik Spider			
Bandook		Kimsuky			
		Magic Hound			
		menuPass			
		Mofang			
		MuddyWater			
		Orangeworm			
		Suckfly			
		TA505			
		Tropic Trooper			
		Whitefly			
		Winnti Group			
		Wizard Spider			

58 total threats identified		
Threat	Sum of "Source Value"	Sources Referenced (6 Total)
LAPSUS\$	6	3
APT41	6	3
LockBit 3.0	5	2
Clop	5	2
menuPass	4	3
REvil	3	2
Tropic Trooper	3	2
Orangeworm	3	2
FIN4	3	2
Whitefly	3	2
Wizard Spider	3	2
Fox Kitten	3	2
Royal	3	1
NoName057(16)	3	1
Andariel	3	1
BianLian	3	1
KillNet	3	1
APT28	2	2
TA505		
Pysa		
LV		
Leviathan		
Conti		
Operation Wocao		
RansomHouse		
Deep Panda		

“Top 5” Threats = ~30 minutes of work
(At least they’re unlikely to be “wrong”!)

Surfacing Proximate Threats: Tally the Results

Also a Proximate threat

Also a Proximate threat

Score boost (relevance)

Score boost (relevance)

Score boost (relevance)

Adversary or Campaign Name	Proximity Tier	Evidence	Proximity Score
Andariel	Direct Threat	Our team attributed with moderate confidence a 2021 incident to this group	5
Wizard Spider	Direct Threat	Our endpoint vendor has quarantined multiple samples of malware distributed by this group	5
TA1337	Direct Threat	Our email security vendor blocked phishing emails attributed to this group	5
APT41	Proximate Threat	Per news reporting, carried out a campaign targeting our largest competitor (our closest peer)	4
LAPSUS\$	Proximate Threat	Per our ISAC, targeted another peer org (one that manufactures significantly different products but with a similar geographic & supplier footprint)	4
Vice Society	Proximate Threat	Per public reporting, linked to several attacks involving European healthcare orgs (specific companies not known)	4
menuPass	Proximate Threat	Per public reporting, linked to attacks involving entities in our industry generally	3
FIN4	Proximate Threat	Per public reporting, linked to attacks involving entities in our industry generally	3



**2023
FIRST
Cyber Threat
Intelligence
Conference**

Berlin, Germany
November 6-8, 2023

Indiscriminate Threats: Measuring Intent & Prevalence

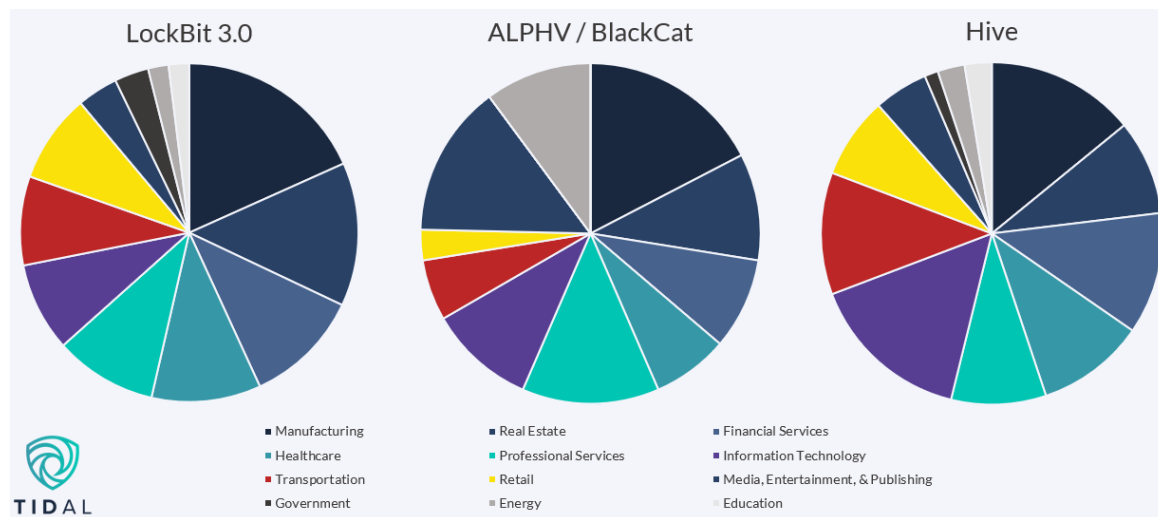


“Opportunistic” & Indiscriminate Threats

- Some of the most difficult to threat profile
 - However, there is often considerable data around them (not necessarily standardized...)
- What ultimately determines thresholds? **You**
 - Lean on the metrics, even imperfect ones
 - Critical thinking: *Why* would a top/trending adversary look at/target you?

CRIMEWARE

SocGhosh Diversifies and Expands Its Malware Staging Infrastructure to Counter Defenders



Groups

APT29

ADD TO MATRIX

Suspected Attribution: Russia

Motivation: Cyber Espionage

Observed Countries: Austria, Brazil, China, France, Germany, Hungary, Japan, Republic of Korea, Mexico, Netherlands, New Zealand, Norway, Portugal, Spain, Turkey, Ukraine, United Kingdom, United States, Uzbekistan

Observed Sectors: Aerospace, Education, Energy, Financial Services, Government, Insurance, Legal, Manufacturing, Media, NGOs, Non Profit, Pharmaceuticals, Technology, Telecommunications, Think Tanks

Sources: MITRE, Tidal Cyber

Quantifying “Indiscriminate” Ransomware Threats

Threat	Healthcare - Public Victims	Total Victims	Ratio of Healthcare
clop	142	1507	9%
lockbit3	44	1266	3%
lockbit2	23	1006	2%
pysa	22	308	7%
alphv	17	625	3%
royal	15	192	8%
hiveleak	14	207	7%
everest	12	133	9%
conti	11	333	3%
bianlian	11	354	3%
vicesociety	9	174	5%
karakurt	8	74	11%
blackbyte	8	131	6%
snatch	6	116	5%
avaddon	6	142	4%
quantum	6	68	9%
blackbasta	5	247	2%
ransomhouse	5	58	9%
marketo	5	32	16%
sunencrypt	4	30	13%
trigona	4	45	9%
lorenz	4	72	6%
xinglocker	4	21	19%
noescape	3	101	3%
ransomexx	3	46	7%

Threat	Healthcare - Public Victims	Total Victims	Ratio of Healthcare
clop	142	1507	9%
lockbit3	44	1266	3%
pysa	22	308	7%
alphv	17	625	3%
royal	15	192	8%
everest	12	133	9%
bianlian	11	354	3%
vicesociety	9	174	5%
karakurt	8	74	11%
blackbyte	8	131	6%
snatch	6	116	5%

Threat	Healthcare - Public Victims	Total Victims	Ratio of Healthcare
projectrelic	1	5	20%
xinglocker	4	21	19%
daixin	2	11	18%
Omega	1	6	17%
redalert	1	6	17%
marketo	5	32	16%
karakurt	8	74	11%
clop	142	1507	9%
everest	12	133	9%
ransomhouse	5	58	9%
royal	15	192	8%

Our Current Threat Profile

Adversary or Campaign Name	Proximity Tier	Evidence	Proximity Score
Andariel	Direct Threat	Our team attributed with moderate confidence a 2021 incident to this group	5
Wizard Spider	Direct Threat	Our endpoint vendor has quarantined multiple samples of malware distributed by this group	5
TA1337	Direct Threat	Our email security vendor blocked phishing emails attributed to this group	5
LockBit	Proximate Threat	Noted as an industry threat in multiple high-reliability reports and a leading healthcare ransomware group, in terms of total victims	4
APT41	Proximate Threat	Per news reporting, carried out a campaign targeting our largest competitor (our closest peer)	4
LAPSUS\$	Proximate Threat	Per our ISAC, targeted another peer org (one that manufactures significantly different products but with a similar geographic & supplier footprint)	4
Vice Society	Proximate Threat	Per public reporting, linked to several attacks involving European healthcare orgs (specific companies not known)	4
menuPass	Proximate Threat	Per public reporting, linked to attacks involving entities in our industry generally	3
FIN4	Proximate Threat	Per public reporting, linked to attacks involving entities in our industry generally	3
Cl0p Actors	Proximate Threat	A leading healthcare ransomware group, in terms of total and proportion of victims	3
Royal Ransomware Actors	Proximate Threat	A leading healthcare ransomware group, in terms of total and proportion of victims	3
Everest Ransomware Actors	Proximate Threat	A leading healthcare ransomware group, in terms of total and proportion of victims	2
Karakurt Extortion Group	Proximate Threat	A leading healthcare ransomware group, especially in terms of proportion of victims	2



**2023
FIRST
Cyber Threat
Intelligence
Conference**

Berlin, Germany
November 6-8, 2023

Further Quantification:
“Capacity” & Capabilities



Key (Practical) Quantification Factors

Ranked by feasibility (in the presenter's experience):

1. Proximity Tier ✓
2. Reference count
 - a. Especially references where Proximity exists (points towards “targeting”?)
3. Source count/prevalence
4. Activity *recency*
 - a. Does the group even still exist? (e.g., ransomware disruptions)
 - b. Every team will vary but...2 years for “still active”, 6 months-1 year for “recently active”
5. Adversary capability/capacity/sophistication
6. Activity *levels*

Quantification: Adversary Software “Density”

LAPSUS\$	APT41	LockBit Ransomware Actors & Affiliates	Clop	menuPass	GOLD SOUTHFIELD	Tropic Trooper	Orangeworm	Whitefly	Wizard Spider	Fox Kitten
Mimikatz	ASPXSpy	7-Zip	Clop	AdFind	Revil	BITSAdmin	Arp	Mimikatz	AdFind	China Chopper
Ntldsutil	BITSAdmin	AdFind	LEMURLOOT	certutil	ConnectWise	KeyBoy	cmd		Bazar	Chisel
	BLACKCOFFEE	Advanced IP Scanner		ChChes		PoisonIvy	ipconfig		BloodHound	Nmap
	certutil	Advanced Port Scanner		cmd		ShadowPad	Kwampirs		Cobalt Strike	Pay2Key
	China Chopper	AdvancedRun		Cobalt Strike		USBferry	Net		Conti	PsExec
	Cobalt Strike	AnyDesk		Ecipekac		YAHOOYAH	netstat		Dyre	TightVNC
	Derusbi	Atera Agent		esentutil			route		Emotet	
	dsquery	Backstab		EvilGrab			Systeminfo		Empire	
	Empire	Bat Armor		FYAnti					GrimAgent	
	ftp	BloodHound		Impacket					Mimikatz	
	gh0st RAT	Chocolatey		Mimikatz					Net	
	ipconfig	ConnectWise		Net					Nltest	
	KEYPLUG	Defender Control		Ntldsutil					Ping	
	MESSAGETAP	ExtPassword		P8RAT					PsExec	
	Mimikatz	FileZilla		Ping					Ryuk	
	Net	FreeFileSync		PlugX					TrickBot	
	netstat	GMER		PoisonIvy						
	njRAT	Impacket		PowerSploit						
	Ping	LaZagne		PsExec						
	PlugX	Ligolo		pwdump						
	PowerSploit	LockBit 3.0		QuasarRAT						
	pwdump	LostMyPassword		RedLeaves						
	ROCKBOOT	MEGAsync		SNUGRIDE						
	ShadowPad	Mimikatz		SodaMaster						
	Winnti for Linux	PasswordFox		UPPERCUT						
	ZxShell	PCHunter								
		Plink								
		PowerTool								
		ProcDump								
		Process Hacker								
		PsExec								
		Rclone								
		Seatbelt								
		SoftPerfect Network Scanner								
		Splashtop								
		TDSSKiller								
		TeamViewer								
		ThunderShell								
		WinSCP								

Quantification: Adversary “Capacity”

- Probably the most subjective factor
- **Use structured criteria**
- Start in the middle, then compare relatively
- Scoring may be biased on information availability
- Recommendation: Assign lower scores if not enough details exist
- It's ok to assign low scores!

MEASUREMENTS OF THREAT ACTOR SOPHISTICATION

- Attack Precision
- Cross-platform Capabilities
- Targeting
- OPSEC
- Resilience
- Stealth

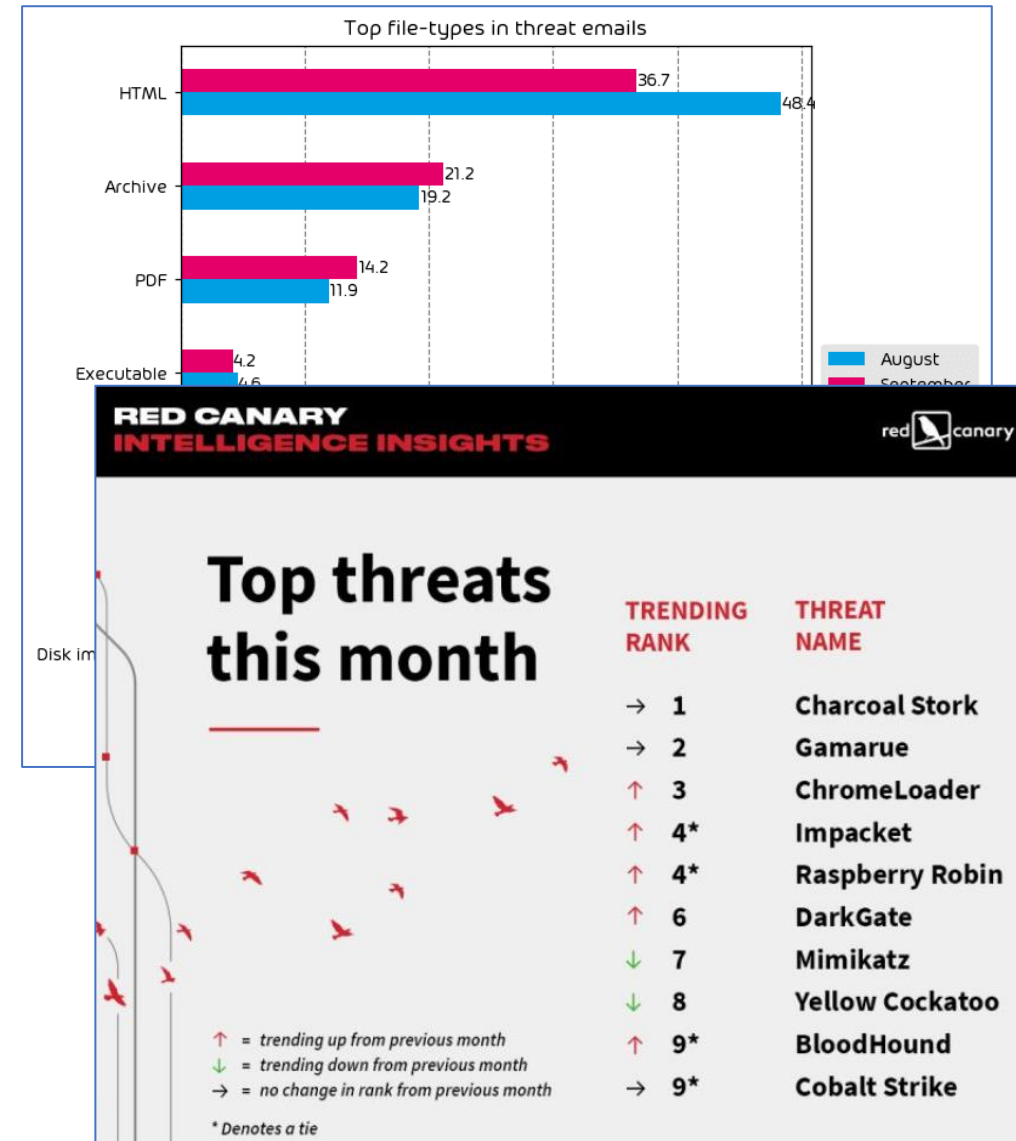
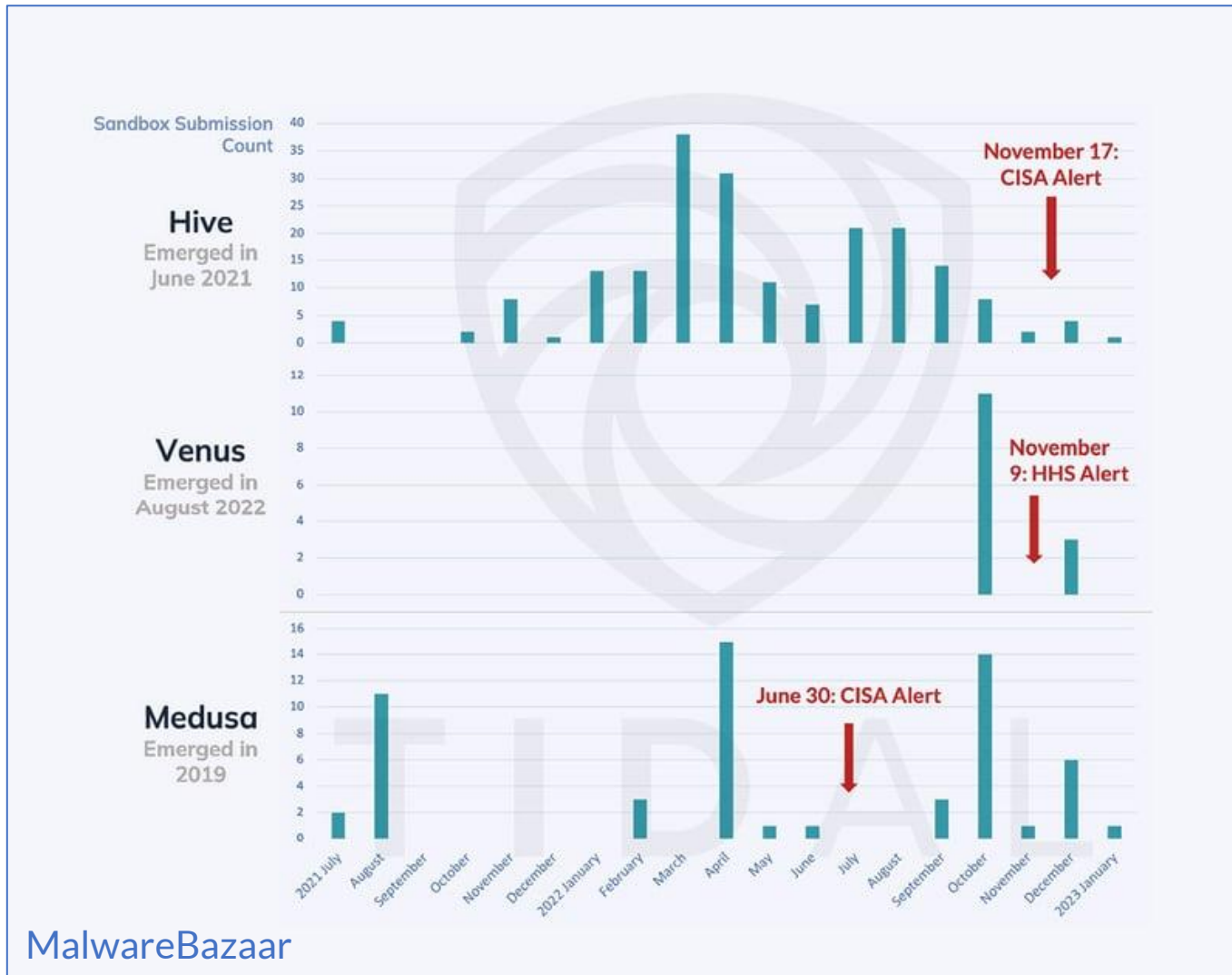


[Sophisticuffs: The Rumble Over Adversary Sophistication](#) (Paul Jaramillo)

Quantification: Adversary “Capacity”

Weighting	Level	Criteria	Representative Examples
5	Superior	Characterized by groups suspected of possessing near-unlimited or very large supplies of resources. Groups often consist of many operators who generally possess high levels of skill and OPSEC. Funding is typically high and provided by a state, but may be supplemented with illicit sources. Often uses custom, sophisticated tooling (alongside existing tools) and has usually been associated with multiple novel techniques or exploits.	The most advanced/prolific APTs (e.g. APT28, Lazars Group)
4	High	Characterized by groups suspected of possessing very large resource supplies. Group members generally possess high levels of skill and OPSEC. Funding is relatively high and may be provided by a state or illicit sources. May use custom, sophisticated tooling alongside existing tools, and might be known to periodically use novel techniques or exploits.	-Major/well-known APTs supporting major adversarial nations (e.g. APT41, Fox Kitten) -The most advanced/prolific ransomware-as-a-service operations (e.g. LockBit, ALPHV/BlackCat)
3	Moderate	Characterized by possessing access to many resources, including funding which may come from a nation-state or illicit means. These groups may be linked to a considerable volume of attacks but may also have mixed levels of success and/or periodic OPSEC blunders. May use custom tooling, but it typically does not display extreme sophistication. (This is also a common assignment for APTs and major crimeware operations when knowledge gaps remain.)	-Many APTs -Many prolific initial access threats (e.g. QakBot, SocGhosh, Emotet)
1-2	Low/Limited	May be individual actors or groups, generally smaller and/or loosely organized ones. Adversaries here may claim or threaten attacks often but do not consistently follow through, at least successfully. Funding is usually limited and not at nation-state scale. Operators and their tools are usually not highly sophisticated, although some successful attacks may have occurred. Custom tools and novel exploits are uncommon. This is also a common assignment when significant knowledge gaps remain.	-Hacktivists -Lower-tier APTs & ransomware groups (including where knowledge is limited) -Infostealer campaigns

Quantification: Activity Levels – Technical Sources





**2023
FIRST
Cyber Threat
Intelligence
Conference**

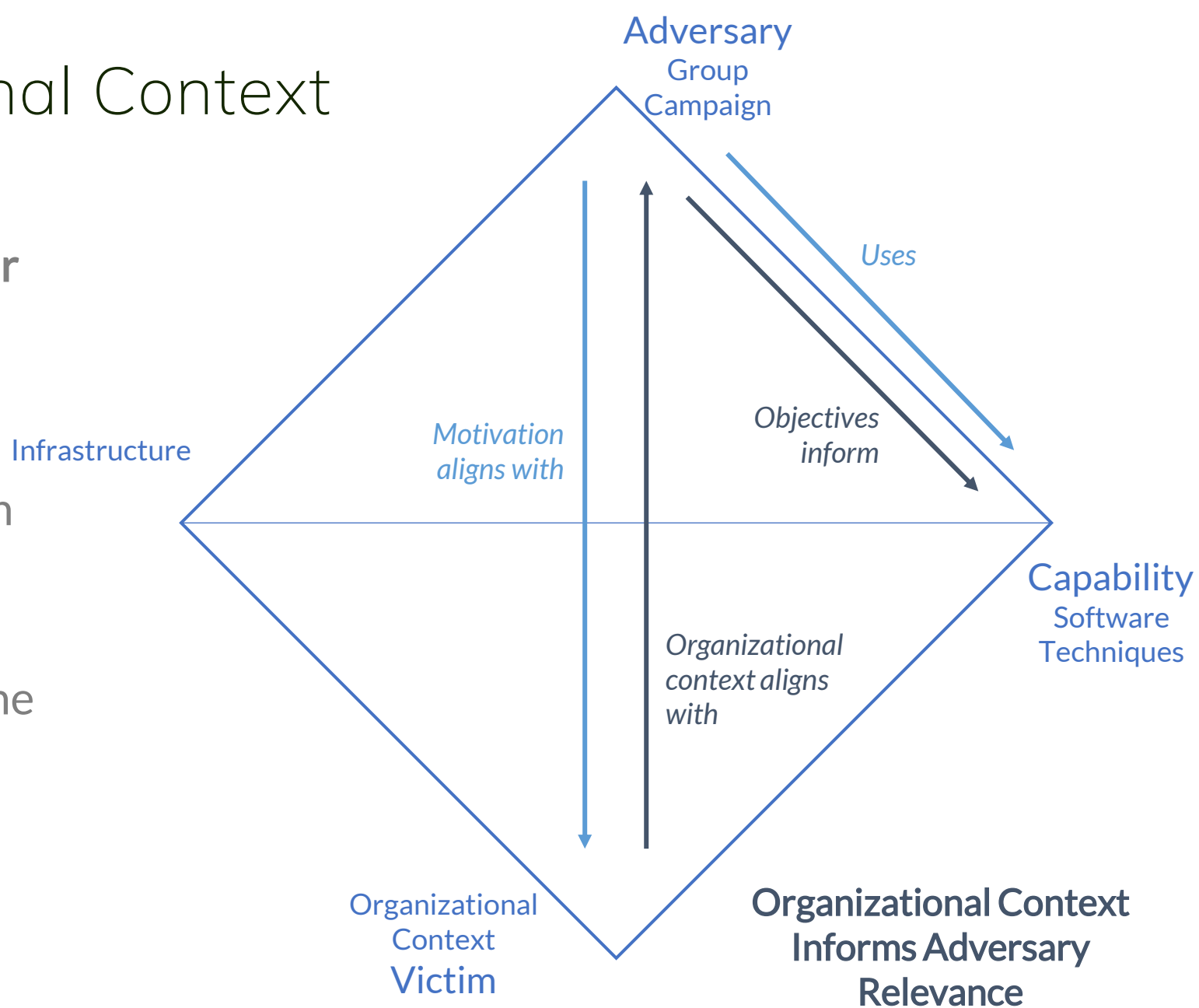
Berlin, Germany
November 6-8, 2023

Consider Organizational
Context



Consider Organizational Context

- **Goal:** Determine a few logical characteristics most unique to your organization, which informs the general types of adversaries that might impact it
- A strong threat profile starts with introspection
- First, consider broad *types* of adversaries that might threaten the organization
- Helps orient, validate, filter, & supplement later research, and drive relevance throughout



Organizational Considerations			Effect on CIA if compromised			Adversary Motivations			
Business Function (Annual Report Section)	Analyst Context	Priority Ranking	C	I	A	Espionage	Financial Gain	Destruction	Est. \$ Impact
Primary Markets/ Contracts	We support major US space launch programs; Army/Navy Air Force programs (missiles & torpedos); an asteroid redirection effort; an emerging nuclear fission program	1	✓		✓	✓		✓	High
Research & Development	R&D efforts are critical to maintaining our leadership position. We possess many US & foreign patents, trademarks & trade secrets	2	✓			✓			High
Suppliers and Raw Materials	Supply base continues to consolidate ; we sometimes depend on sole suppliers	3			✓			✓	High
Information Technology & Security	We process, store & transmit large amounts of confidential information & IP related to internal operations and associated with subcontractors & customers	4	✓	✓		✓	✓		Medium
Production	Assembly traditionally performed at a single site in California but opened a new site in Arizona and are exploring another in the UK	5			✓			✓	High
Human Capital	We permit certain support task to be performed remotely	6	✓		✓	✓			Low
Environmental Matters	We are continue to pay for remediation costs associated with environmental contamination at one of our production sites	7			✓			✓	Low



**2023
FIRST
Cyber Threat
Intelligence
Conference**

Berlin, Germany
November 6-8, 2023

Common Next Questions



Common next questions

1. What about threats that haven't been seen impacting our sector yet? (How do we predict the next big thing?)
 - a. You can't! No one really can...
 - b. Our process narrowed from thousands of global threats to dozens of relevant ones, and even this is probably too much for most teams to address/validate each. Why focus on something else?
2. How do I correlate/deduplicate among threat names?
 - a. github.com/StrangerealIntel/EternalLiberty
3. Why add "low-priority" threats at all (1's or 2's)?
 - a. A really good habit and procedural habit to follow. Threat levels change – good to show you've been tracking it!




2023
FIRST
Cyber Threat
Intelligence
Conference

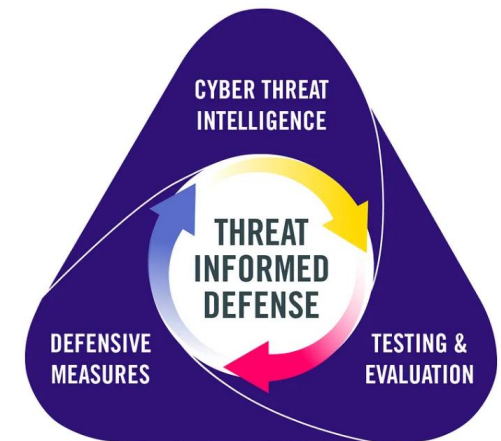
Berlin, Germany
November 6-8, 2023

Taking Action on Your
Threat Profile – Threat
Informed Defense
Approach



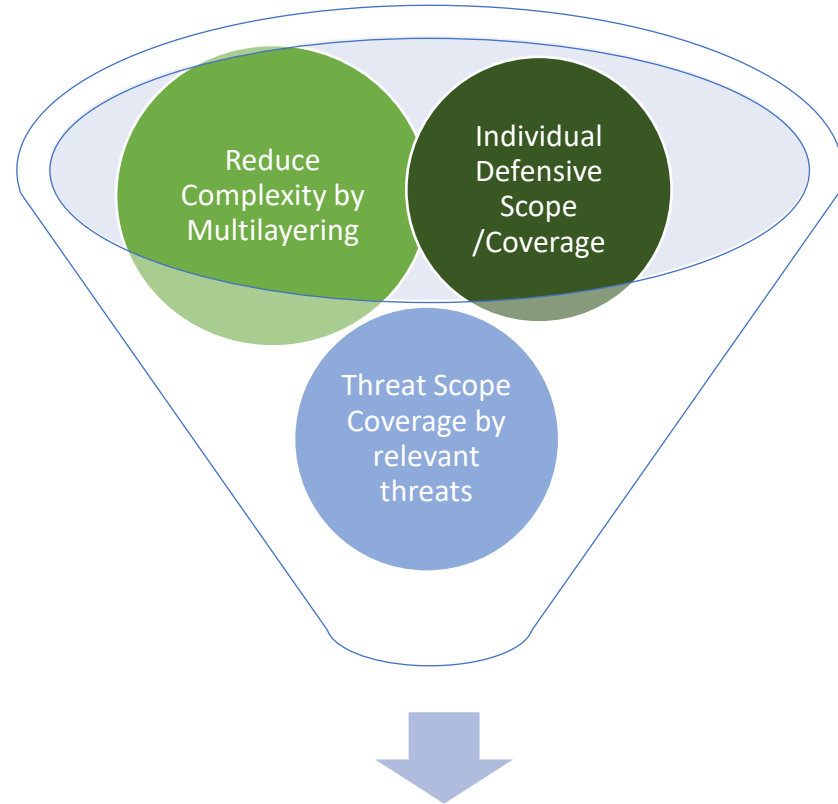
Threat Informed Defense – Taking action on your threat profile with the TID approach

 ATT&CK® Evaluations	 Center for Threat Informed Defense	 MITRE ATT&CK Defender™
Cyber Threat Intelligence	Defensive Engagement & Measures	Collaboration & Sharing
<ul style="list-style-type: none">Analyze with the help of MITRE Resources & Tools to increase the operational effectiveness	<ul style="list-style-type: none">Breach & Attack Simulation with Proof-of-Value and Proof-of-ConceptTest and evaluation to understand true defensive postureSystematically advance the ability to detect and prevent	<ul style="list-style-type: none">Share your experience and resultsCollaborate and share with the community



Threat-Informed defense enables a continual feedback loop.

The goal is to gain a **deep TECHNICAL understanding**.



Enterprise-Centric Adversary Behavioral Threat Profiling

Enterprise-centric Threat Profile with MITRE ATT&CK Multilayering – Top ATT&CK Techniques WHERE TO START – Use Case Workshop



Operational Effectiveness – Ecosystem & BP

https://github.com/cert-orangecyberdefense/ransomware_map

<https://mitre-engenuity.org/cybersecurity/center-for-threat-informed-defense/our-work/cti-blueprints/>

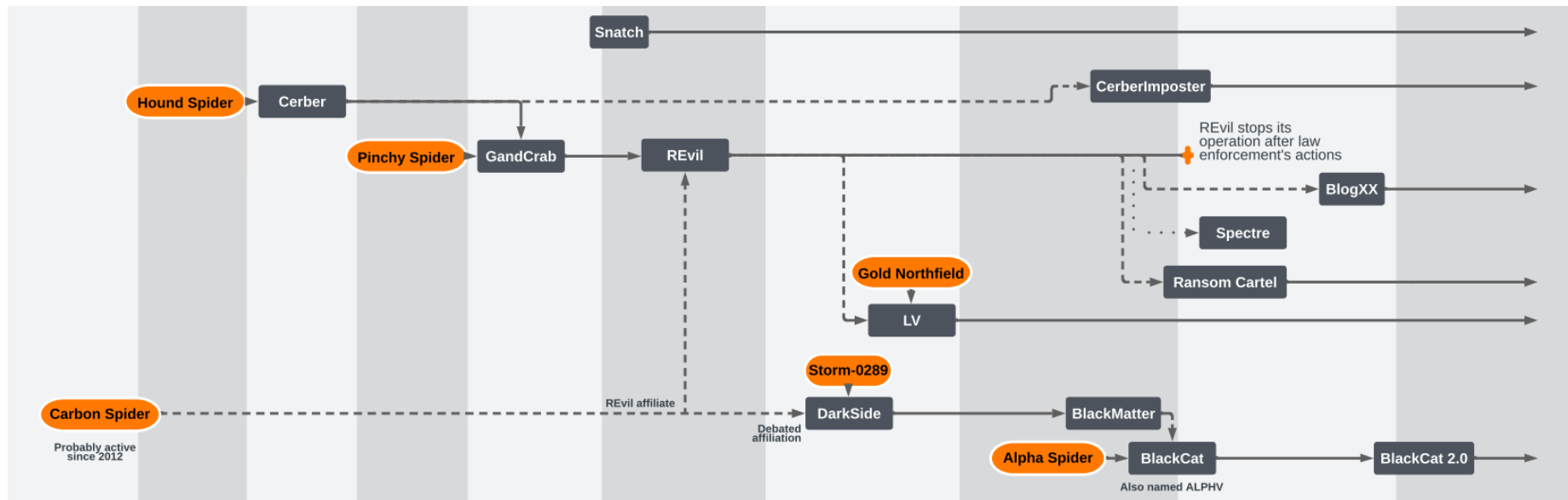
MITRE
ENGENUITY
A Foundation for Public Good

CTI BLUEPRINTS

MITRE ATT&CK TABLE

Table 1: Caption

Tactics	Technique	Technique Name	Procedure	DFEND	Deployed Control
Initial Access	T1189	Drive by compromise	<ul style="list-style-type: none"> Elevate privileges using Local Privilege Escalation (LPE) exploit if this key is enabled, CVE-2018-8453 exploited. Makes use of compromise webpages like forums to download REvil when accessed. 	https://d3fend.mitre.org/offensivetechnique/attack/T1189/	
Initial Access	T1190	Exploit Public-Facing Application	<ul style="list-style-type: none"> Arrives via any the following exploits: <ul style="list-style-type: none"> CVE-2018-13379 CVE-2019-0725 CVE-2019-11510 CVE-2021-30116 	https://d3fend.mitre.org/offensivetechnique/attack/T1190/	
Initial Access	T1566.001	Phishing: Spearphishing Attachment	<ul style="list-style-type: none"> Spam emails with attached MS Office Word documents including malicious macro to download ransomware to target system. Arrives via phishing emails, sometimes with Qaboot or IceID 	https://d3fend.mitre.org/offensivetechnique/attack/T1566.001/	
Initial Access	T1195	Supply Chain Compromise	<ul style="list-style-type: none"> Compromised Kazuya VSA servers were used to push out REvil to victims. 	https://d3fend.mitre.org/offensivetechnique/attack/T1195/	
Discovery	T1016	System Network	<ul style="list-style-type: none"> Uses native API to 	https://d3fend.mitre.org/offensivetechnique/attack/T1016/	



Defensive Engagement preparation – Multilayering avoiding analytical errors

<https://www.cisa.gov/sites/default/files/2023-01/Best%20Practices%20for%20MITRE%20ATTCK%20Mapping.pdf>

Reduction of analytical error with multilayering	0. Understand ATT&CK	1. Find the Behavior	2. Research the Behavior	3. Identify the Tactics	4. Identify the (sub-) Techniques
Leaping to Conclusions			A premature decision on TTPs without thorough examination of the behavior or artifacts can result in an erroneous mapping and a flawed final product.	Identifying the wrong tactic may occur by "leaping" to a conclusion that does not align with the report details or accumulated artifacts.	Identifying the wrong techniques may occur by "leaping" to a conclusion that doesn't align with the report details or accumulated artifacts.
Opportunity Multilayering			The more CTI reports are layered in the matrices, the more the examination and behavior of artifacts accuracy increase by numbers.	Tactics can be compared with multiple matrices and are automatically defined by the extracted technique in the matrices.	With tools like POWERED SUIT and multilayering the identification of the right technique increases with every matrix added.
Missed Opportunities	Without an understanding of ATT&CK, other possible mappings will not be considered and consequently missed.	Identification of all behaviors in a report may be overlooked.	Understanding how the behavior works may highlight other potential related mappings.		
New Opportunities Multilayering	CTI platforms with multilayering explain the techniques in the mapping. Even if there would be a lack of understanding, the number of repetitive use of one technique emphasize the right mapping.	Behavior that would be overlooked are now much more visible in comparison with other CTI reports	Multilayering highlight the most common techniques and is a starting point for prevention, mitigation and detection		
Miscategorization	Without an understanding of ATT&CK, the distinctions between two similar yet different techniques may result in an inaccurate mapping	Identification of applicable behaviors may be overlooked.	Selecting the wrong technique can occur without thorough research, understanding, or by misreading the behavior and technical details.	Misreading and insufficient research on the data or even the incorrect use of ATT&CK search can result in misidentification of the tactic.	Mapping the wrong technique is possible without researching and understanding other technique options.
Opportunity Multilayering	Accurate mapping with multilayering avoid error in analyzing similar techniques by approving a technique that is repeatable used in other CTI reports and references.	Behavior is approved by multilayering showing the most used behavior which is than an indicator that they aren't overlooked.	Even if one CTI report has a wrong technique with multilayering the misreading of behavior and technical details neutralize wrong assumption by approving other techniques for the described attack of a threat actor.	Tactics in a multilayered matrices environment are approved by the increasing number of matrices with same TTPs	Sub-Techniques are approved in other matrices. The more technique sets, and community references contain the same sub-technique, the higher the accuracy is. Multilayering emphasizes more research and accuracy where one or two sources would have gaps in research or understanding

Multilayering threat actors in the healthcare – holistic threat profile to understand their campaigns and capabilities

The screenshot displays the TIDAL CYBER Enterprise Edition interface, which is a threat intelligence platform. The main content is a large matrix of threat capabilities, organized into columns representing different stages of an attack cycle. The columns are: Reconnaissance, Resource Development, Initial Access, Execution, Persistence, Privilege Escalation, Defense Evasion, Credential Access, Discovery, Lateral Movement, Collection, Command and Control, Exfiltration, and Impact. Each cell in the matrix contains a list of specific techniques, such as 'Vulnerability Scanning', 'Acquire Access', 'Drive-by Compromise', 'Command and Scripting Interpreter', 'Account Manipulation', 'Abuse Elevation Control Mechanism', 'Brute Force', 'Account Discovery', 'Exploitation of Remote Services', 'Archive Collected Data', 'Application Layer Protocol', 'Exfiltration Over Alternative Protocol', and 'Data Destruction'. The interface also shows a browser window at the top with several tabs open, including 'Healthcare APT+Ran...', 'CISA Royal AA23-0...', 'Trend Micro Royal L...', '#StopRansomware...', 'U.S. CISA BlanUan...', 'Truebot - ClOp Rans...', 'REvil TheDFIRRepo...', 'REvil Trendmicro A...', and 'MITRE-REvil PAPE...'. The TIDAL CYBER logo and 'ENTERPRISE EDITION' are visible in the top left corner.

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Vulnerability Scanning	Acquire Access	Drive-by Compromise	Command and Scripting Interpreter (4)	Account Manipulation	Abuse Elevation Control Mechanism (1)	Abuse Elevation Control Mechanism (1)	Brute Force (2)	Account Discovery (1)	Exploitation of Remote Services	Archive Collected Data (2)	Application Layer Protocol (3)	Exfiltration Over Alternative Protocol (2)	Data Destruction
Software	Domains	Exploit Public-Facing Application	JavaScript	BITS Jobs	Bypass User Account Control	Bypass User Account Control	Password Cracking	Domain Account	Lateral Tool Transfer	Archive via Custom Method	DNS	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Data Encrypted for Impact
IP Addresses	Virtual Private Server	External Remote Services	PowerShell	Boot or Logon Autostart Execution (1)	Access Token Manipulation (2)	Access Token Manipulation (2)	Password Spraying	Application Window Discovery	Remote Desktop Protocol	Archive via Utility	File Transfer Protocols	Defacement (1)	Defacement (1)
	Digital Certificates	Phishing (2)	Unix Shell	Registry Run Keys / Startup Folder	Create Account (1)	Create Process with Token	Credentials from Web Browsers	Domain Trust Discovery	SMB Windows Admin Shares	Automated Collection	Web Protocols	Exfiltration Over Unencrypted Non-C2 Protocol	Internal Defacement
	Malware	Spearghishing Attachment	Windows Command Shell	Create Account (1)	Token Impersonation/Theft	Token Impersonation/Theft	Keylogging	File and Directory Discovery	VNC	Clipboard Data	Standard Encoding	Inhibit System Recovery	Inhibit System Recovery
	Code Signing Certificates	Spearghishing Link	Exploitation for Client Execution	Local Account	Boot or Logon Autostart Execution (1)	Boot or Logon Autostart Execution (1)	OS Credential Dumping (3)	Network Service Discovery	Windows Remote Management	Data from Local System	Protocol Impersonation	Exfiltration Over C2 Channel	Resource Hijacking
	Malware	Replication Through Removable Media	Native API	Create or Modify System Process (1)	Registry Run Keys / Startup Folder	Registry Run Keys / Startup Folder	LSASS Memory	Network Share Discovery	Replication Through Removable Media	Data from Network Shared Drive	Domain Generation Algorithms	Exfiltration Over Web Service (1)	Service Stop
	Tool	Supply Chain Compromise (1)	Scheduled Task/Job (1)	Windows Service	Deobfuscate/Decode Files or Information	Deobfuscate/Decode Files or Information	NTDS	Peripheral Device Discovery	Software Deployment Tools	Local Data Staging	Asymmetric Cryptography	Exfiltration to Cloud Storage	System Shutdown/Reboot
		Compromise Software Supply Chain	Shared Modules	Accessibility Features	Group Policy Modification	Group Policy Modification	Security Account Manager	Permission Groups Discovery		Remote Data Staging	Symmetric Cryptography	Transfer Data to Cloud Account	
		Valid Accounts (2)	Software Deployment Tools	External Remote Services	Environmental Keying	Environmental Keying	Kerberoasting	Domain Groups		Keylogging	Fallback Channels		
		Domain Accounts	Service Execution	Hijack Execution Flow (3)	Windows Service	Windows Service	Unsecured Credentials (1)	Local Groups		Screen Capture	Ingress Tool Transfer		
		Local Accounts	User Execution (1)	DLL Search Order Hijacking	Group Policy Modification	Group Policy Modification	Credentials in Files	Process Discovery			Multi-Stage Channels		
			Malicious File	DLL Side-Loading	Accessibility Features	Accessibility Features		Query Registry			Non-Application Layer Protocol		
			Windows Management Instrumentation	Dynamic Linker Hijacking	Exploitation for Privilege Escalation	Exploitation for Privilege Escalation		Remote System Discovery			Non-Standard Port		
				Bootkit	Hijack Execution Flow (3)	Hijack Execution Flow (3)		Software Discovery (1)			Protocol Tunneling		
				Scheduled Task/Job (1)	DLL Search Order Hijacking	DLL Search Order Hijacking		Security Software Discovery			Proxy (2)		
				Scheduled Task	DLL Side-Loading	DLL Side-Loading		System Information Discovery			Domain Fronting		
				Web Shell	Dynamic Linker Hijacking	Dynamic Linker Hijacking		System Language Discovery			Multi-hop Proxy		
				Valid Accounts (2)	Process Injection	Impair Defenses (2)		System Network Configuration Discovery			Remote Access Software		
				Domain Accounts	Scheduled Task/Job (1)	Disable or Modify System Firewall		System Network Connections Discovery			Web Service (1)		
				Local Accounts	Scheduled Task	Disable or Modify Tools		System Owner/User Discovery			Dead Drop Resolver		
					Valid Accounts (2)	Clear Command History		System Service Discovery					
					Domain Accounts	Clear Windows Event Logs		Virtualization/Sandbox Discovery					
					Local Accounts	File Deletion							
						Timestamp							

2023
FIRST
Cyber Threat
Intelligence
Conference

Berlin, Germany
November 6-8, 2023

Top TTPs Healthcare &
Scoring



Enterprise-centric top TTPs healthcare as a starting point to prevent, mitigate and detect 1/3

Top Initial Access Techniques

- T1566 Phishing
- T1190 Exploit Public-Facing Application
- **T1133 External Remote Services (And a Persistence Technique)**
- T1068 Valid Accounts

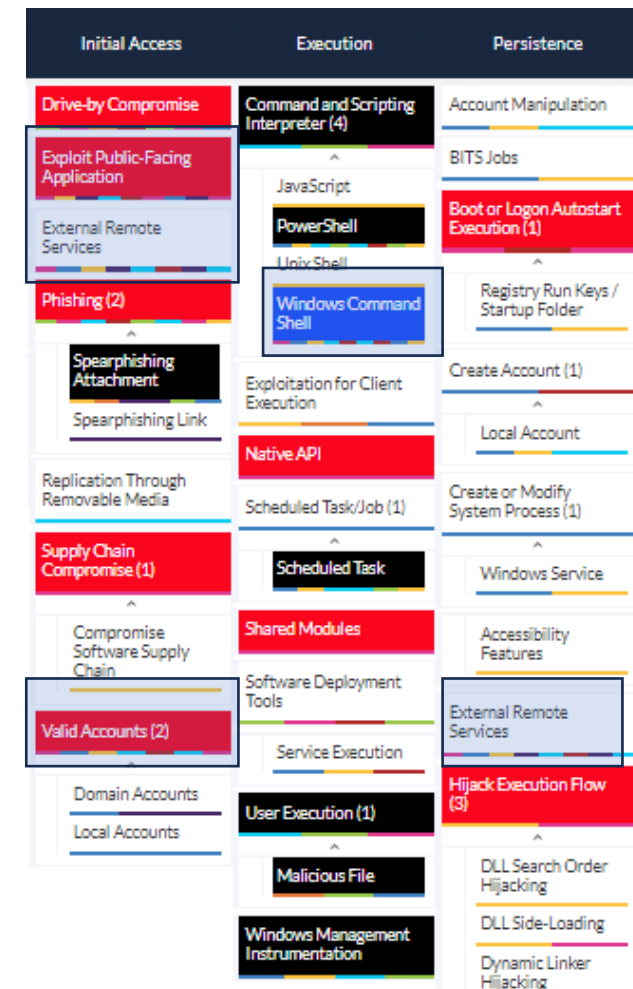
Top Techniques Execution

- T1059.003 Windows Command Shell

Top Techniques Persistence

- T1133 External Remote Services
- **T1068 Valid Accounts (And a Persistence Technique)**

=> Which tools do the adversaries use for External Remote Services and Valid Accounts?



Enterprise centric top TTPs as a starting point to prevent, mitigate and detect 2/3

Privilege Escalation

- T1484.001 Group Policy Modification

Defensive Evasion

- T1484.001 Group Policy Modification

=> another great choke point for privilege escalation and defensive evasion

Credential Access

- T1003.001 OS Credential Dumping: LSASS Memory

Discovery

- T1046 Network Service Discovery
- T1082 System Information Discovery

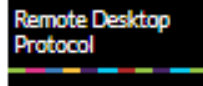
Detection

ID	Data Source	Data Component	Detects
DS0026	Active Directory	Active Directory Object Creation	Monitor for newly constructed active directory objects, such as Windows EID 5137.
		Active Directory Object Deletion	Monitor for unexpected deletion of an active directory object, such as Windows EID 5141.
		Active Directory Object Modification	Monitor for changes made to AD settings for unexpected modifications to user accounts, such as deletions or potentially malicious changes to user attributes (credentials, status, etc.).
DS0017	Command	Command Execution	Monitor executed commands and arguments that may modify Group Policy Objects (GPOs) to subvert the intended discretionary access controls for a domain, usually with the intention of escalating privileges on the domain.



Enterprise centric top TTPs as a starting point to prevent, mitigate and detect 3/3

Lateral Movement



- T1021.001 Remote Desktop Protocol

Collection

- T1005 Data from Local System

Command and Control

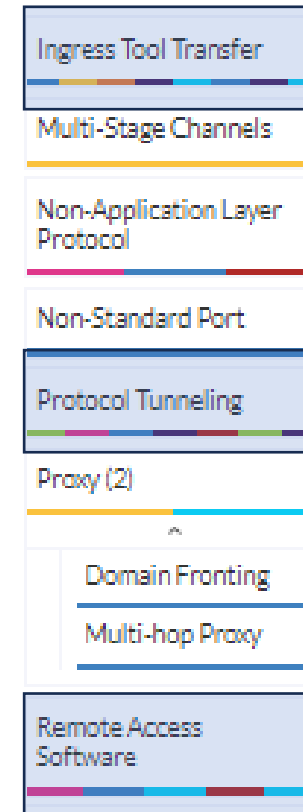
- T1572 Protocol Tunneling
- T1105 Ingress Tool Transfer
- T1219 Remote Access Software

Exfiltration

- T1567 Exfiltration Over Web Service

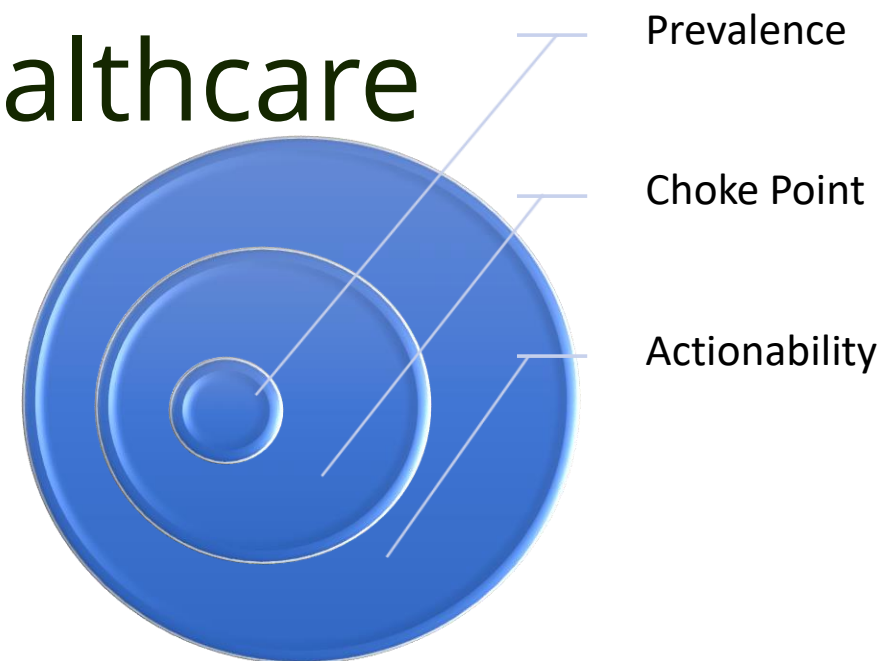
Precursor Ransomware Impact

- T1490 Inhibit System Recovery before T1486 Data Encrypted for Impact



Scoring Top TTPs for Healthcare

- Counts from CTI
- Data Sources
- Analytics
- Groups
- CIS Community Defense Model top Safeguards



Rank	Technique ID	Technique Name	Tactic	Count from CTI	Mapped Data Sources	# Sigma Analytics	# Atomic Tests	Groups	Top CIS Safeguards
1	T1021.001	Remote Desktop Protocol	Lateral Movement	4	4	12	4	6	42
2	T1190	Exploit Public-Facing Application	Initial Access	9	2	43	0	6	33
3	T1133	External Remote Services	Initial Access	6	5	9	1	5	24
4	T1566.001	Phishing	Initial Access	8	4	11	2	5	
5	T1082	System Information Discovery	Discovery	8	3	19	29	7	
6	T1046	Network Service Discovery	Discovery	7	3	9	10	5	
7	T1486	Data Encrypted for Impact	Impact	7	6	7	8	6	
8	T1484.001	Group Policy Modification	Privilege Escalation	6	4	2	2	3	
9	T1068	Valid Accounts	Execution	5	3	43	0	5	
10	T1567	Exfiltration Over Web Service	Exfiltration	5	5	5	0	4	
11	T1219	Remote Access Software	Command and Control	4	4	32	11	3	
12	T1572	Protocol Tunneling	Command and Control	3	3	14	4	4	
13	T1105	Ingress Tool Transfer	Command and Control	3	4	48	29	5	
14	T1003.001	LSASS Memory	Credential Access	2	4	72	13	4	
15	T1005	Data from Local System	Collection	1	4	9	1	4	
16	T1490	Inhibit System Recovery	Impact	1	7	17	10	4	

Scoring Top TTPs with the Mitigation (Phishing MITRE Engenuity Calculator)

- <https://medium.com/@simone.kraus/mitre-engenuity-calculator-and-scoring-1c9f2f3f8f9e>

Scoring Matrix	Top 10 Techniques (10)		Mitigations										Mitigations												
	M1015 - Active Directory Configuration	M1017 - User Training	M1018 - User Account Management	M1021 - Restrict Web-Based Content	M1022 - Restrict File and Directory Permissions	M1025 - Privileged Process Integrity	M1026 - Privileged Account Management	M1027 - Password Policies	M1028 - Operating System Configuration	M1029 - Remote Data Storage	M1030 - Network Segmentation	M1031 - Network Intrusion Prevention	M1032 - Multifactor Authentication	M1033 - Limit Software Installation	M1035 - Limit Access to Resource Over Network	M1037 - Filter Network Traffic	M1038 - E-mail Quarantine	M1040 - Behavior Prevention on Endpoint	M1041 - Encrypt Sensitive Information	M1042 - Disable or Remove Feature or Program	M1043 - Audit	M1045 - Antivirus/Antimalware	M1051 - Update Software	M1054 - Software Configuration	
T1003 - OS Credential Dumping	12	16	0	0	0	11	16	16	13	0	0	0	0	0	0	0	11	11	0	11	0	0	0	0	117
T1003.001 - OS Credential Dumping: LSASS Memory	0	1	0	0	0	1	1	1	1	0	0	0	0	0	0	0	1	0	0	1	0	0	0	0	7
T1003.002 - OS Credential Dumping: Security Account Manager	0	1	0	0	0	0	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	4
T1003.003 - OS Credential Dumping: NTDS	0	1	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	4
T1003.004 - OS Credential Dumping: LSA Secrets	0	1	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	3
T1003.005 - OS Credential Dumping: Cached Domain Credentials	1	1	0	0	0	0	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	5
T1003.006 - OS Credential Dumping: DCSync	1	1	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	4
T1204 - User Execution	12	12	0	11	0	0	0	0	0	0	11	0	0	0	0	11	11	0	0	0	0	0	0	0	56
T1204.001 - User Execution: Malicious Link	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2
T1204.002 - User Execution: Malicious File	0	1	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	3
T1552 - Unsecured Credentials	11	11	0	0	12	0	11	13	0	0	0	0	0	0	0	0	0	0	0	0	14	0	11	0	83
T1552.001 - Unsecured Credentials: Credentials in Files	0	1	0	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	4
T1552.002 - Unsecured Credentials: Credentials in Registry	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	3
T1552.004 - Unsecured Credentials: Private Key	0	0	0	0	1	0	0	1	0	0	0	0	0	0	0	0	0	1	0	0	1	0	0	0	4
T1552.006 - Unsecured Credentials: Group Policy Preferences	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0	3
T1072 - Software Deployment Tools	10	10	10	0	0	0	10	10	10	10	0	10	0	0	0	0	0	0	0	0	0	0	10	0	90
T1557 - Adversary-in-the-Middle	0	11	0	0	0	0	0	0	0	11	12	0	0	11	12	0	0	11	12	0	0	0	0	0	80
T1557.001 - Adversary-in-the-Middle:LLMNR/NBT-NS Poisoning and S	0	0	0	0	0	0	0	0	0	1	1	0	0	0	1	0	0	0	1	0	0	0	0	0	4
T1557.002 - Adversary-in-the-Middle:ARP Cache Poisoning	0	1	0	0	0	0	0	0	0	0	1	0	0	1	1	0	0	1	1	0	0	0	0	0	6
T1213 - Data from Information Repositories	0	11	11	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	11	0	0	0	33
T1213.002 - Data from Information Repositories: Sharepoint	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	3
T1539 - Steal Web Session Cookie	10	10	0	0	0	0	0	0	0	0	0	10	0	0	0	0	0	0	0	0	0	0	0	10	30
T1566 - Phishing	0	13	0	13	0	0	0	0	0	0	11	0	0	0	0	0	0	0	0	0	0	12	0	12	61
T1566.001 Phishing: Spearphishing Attachment	0	1	0	1	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	1	0	1	5
T1566.002 Phishing: Spearphishing Link	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	4	
T1566.003 Phishing: Spearphishing via Service	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2
T1528 - Steal Application Access Token	0	10	10	10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	10	0	0	0	0	40
T1176 - Browser Extension	0	10	0	0	0	0	0	0	0	0	0	10	0	0	10	0	0	0	0	10	0	10	0	0	50
Results	33	114	31	34	12	11	37	39	13	10	21	34	20	10	11	12	21	22	22	12	11	45	12	31	22

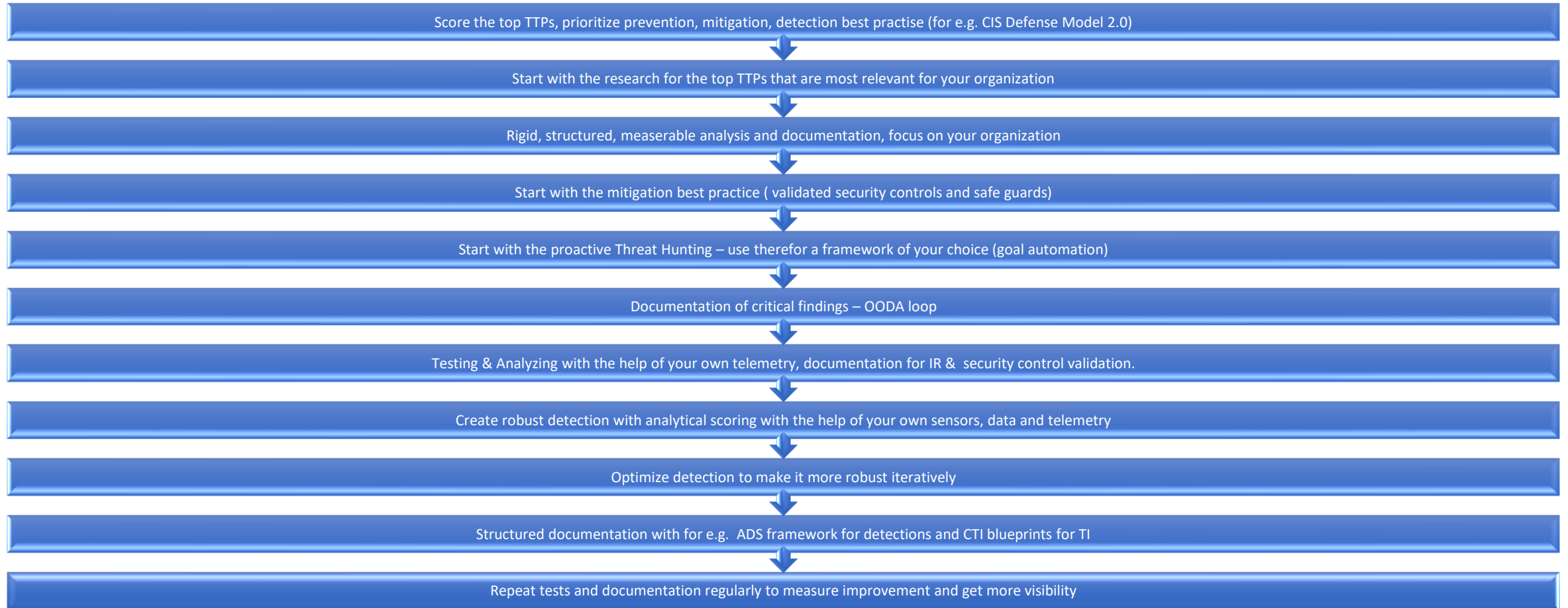
2023
FIRST
**Cyber Threat
Intelligence
Conference**

Berlin, Germany
November 6-8, 2023

Defensive Engagement &
Measures



Defensive Engagement & Measures



RMM Tools Healthcare – Mapping for Ransomware Groups

Focus on specific tools that are relevant for your sector

RMM Tools Healthcare									
Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration
Windows Command Shell	Registry Run Keys / Startup Folder	Bypass User Account Control	Bypass User Account Control	Credentials from Password Stores (1)	File and Directory Discovery	Lateral Tool Transfer	Data from Local System	Domain Generation Algorithms	Exfiltration Over Web Service
Scheduled Task	Domain Account	Registry Run Keys / Startup Folder	Hidden Files and Directories	Credentials from Web Browsers	Process Discovery	Remote Desktop Protocol	Keylogging	Symmetric Cryptography	
Software Deployment Tools	Windows Service	Windows Service	Hidden Window	Keylogging	Query Registry	SMB/Windows Admin Shares	Video Capture	Ingress Tool Transfer	
Service Execution	Scheduled Task	Scheduled Task	Masquerading	Credentials In Files	System Information Discovery	Software Deployment Tools		Non-Application Layer Protocol	
Windows Management Instrumentation			Modify Registry		System Location Discovery			Non-Standard Port	
			Software Packing		System Network Configuration Discovery			Protocol Tunneling	
			Code Signing		System Network Connections Discovery			Proxy	
					System Owner/User Discovery			Remote Access Software	
								Web Service	

RMM Tools Recommendation Mitigation CISA

Implement best practices to block phishing emails.

Audit remote access tools on your network to identify currently used and/or authorized RMM software.

Review logs for execution of RMM software to detect abnormal use of programs running as a portable executable.

Use security software to detect instances of RMM software only being loaded in memory.

Implement application controls to manage and control execution of software, including allowlisting RMM programs. (See NSA Cybersecurity Information sheet Enforce Signed Software Execution Policies).

Tradecraft Uncertainty – Research T1219 helps to predict attacks

Tradecraft Uncertainty

Which techniques are attackers likely to employ in my environment?

What distinct procedures can be used to carry out these techniques?

Which operations are different between these procedures?

Telemetry Uncertainty

What telemetry is generated by known distinct procedures?

What characteristics (fields/values) of this telemetry can be used to identify actions that may be the result of an attacker?

Event 17, Sysmon

General Details

Pipe Created:
RuleName: -
EventType: CreatePipe
UtcTime: 2023-10-04 19:48:19.920
ProcessGuid: {bd6ed866-c183-651d-cc02-000000000d00}
ProcessId: 2376
PipeName: **\adprinterpipe**
Image: C:\Program Files (x86)AnyDesk\AnyDesk.exe

Event 1, Sysmon

General Details

Process Create:
RuleName: technique_id=T1204,technique_name=User Execution
UtcTime: 2023-10-04 19:48:19.394
ProcessGuid: {bd6ed866-c183-651d-cc02-000000000d00}
ProcessId: 2376
Image: C:\Program Files (x86)AnyDesk\AnyDesk.exe
FileVersion: 8.0.3
Description: AnyDesk
Product: AnyDesk
Company: AnyDesk Software GmbH
OriginalFileName: -
CommandLine: "C:\Program Files (x86)AnyDesk\AnyDesk.exe" --control
CurrentDirectory: C:\Windows\system32\

Image Performance Performance Graph GPU Graph Threads TCP/IP Security Environment

Count: 11

TID	CPU	Cycles Delta	Suspend Count	Start Address
3804				ntdll.dll!TpCallbackIndependent+0x140
4328				AnyDesk.exe+0x53ac90
7584				ntdll.dll!TpCallbackIndependent+0x140
1820				AnyDesk.exe+0x1ce5
5144				gdiplus.dll!GdiplusStartup+0x1a80
3300				AnyDesk.exe+0x53ac90
7148				AnyDesk.exe+0x53ac90
5148				AnyDesk.exe+0x53ac90
392				AnyDesk.exe+0x53ac90
4492				AnyDesk.exe+0x53ac90
2092				AnyDesk.exe+0x53ac90

Image File

AnyDesk

Version: 8.0.3.0
Build Time: Fri Sep 22 10:14:12 2023
Path: C:\Program Files (x86)AnyDesk\AnyDesk.exe
Command line: "C:\Program Files (x86)AnyDesk\AnyDesk.exe" --control
Current directory: C:\Windows\System32\
Autostart Location: C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup\AnyDesk.lnk
Parent: explorer.exe(4468)

<https://posts.specterops.io/reactive-progress-and-tradecraft-innovation-b616f85b6c0a>

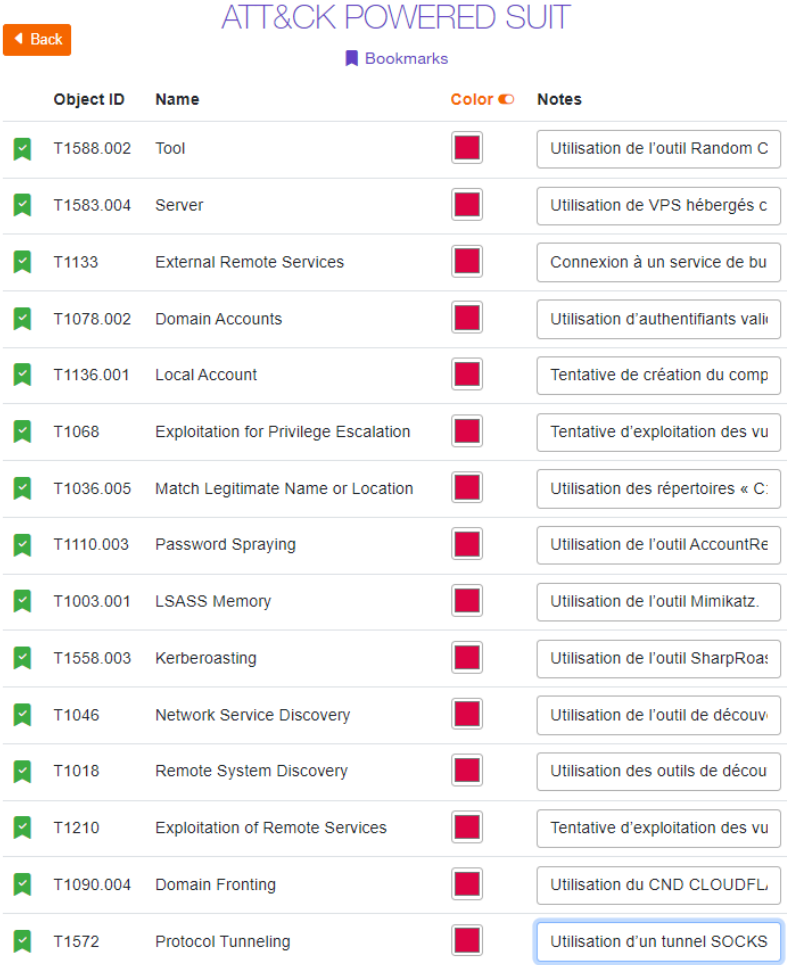
2023
FIRST
Cyber Threat
Intelligence
Conference

Berlin, Germany
November 6-8, 2023

Extracting CTI with the
D3FEND FIN12



Analyzing a CTI Healthcare report – CERT France extraction with D3FEND and Map it to the MITRE ATT&CK

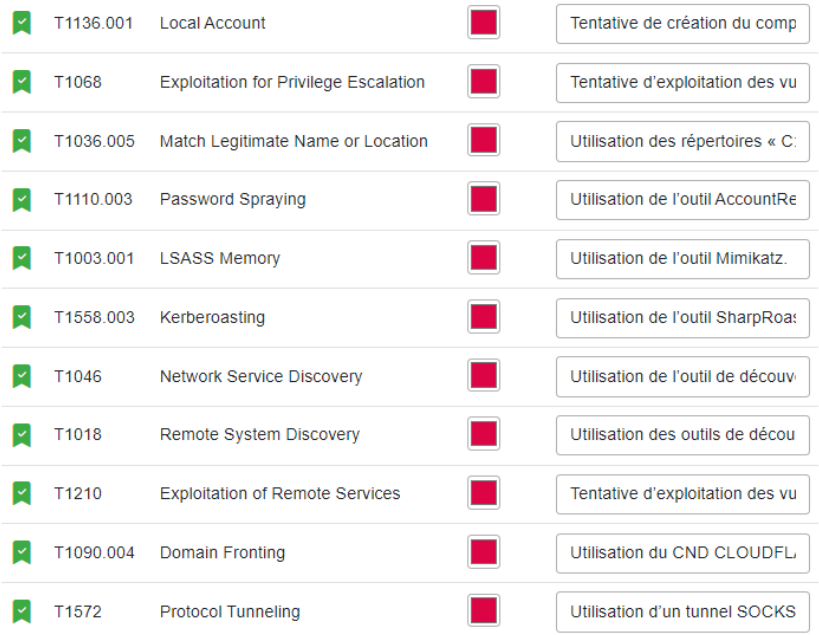


ATT&CK POWERED SUIT

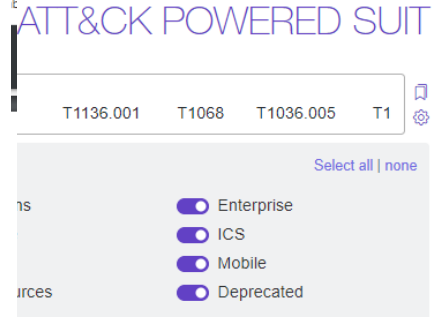
← Back

Bookmarks

Object ID	Name	Color	Notes
T1588.002	Tool	Red	Utilisation de l'outil Random C
T1583.004	Server	Red	Utilisation de VPS hébergés c
T1133	External Remote Services	Red	Connexion à un service de bu
T1078.002	Domain Accounts	Red	Utilisation d'authentifiants vali
T1136.001	Local Account	Red	Tentative de création du comp
T1068	Exploitation for Privilege Escalation	Red	Tentative d'exploitation des vu
T1036.005	Match Legitimate Name or Location	Red	Utilisation des répertoires « C:
T1110.003	Password Spraying	Red	Utilisation de l'outil AccountRe
T1003.001	LSASS Memory	Red	Utilisation de l'outil Mimikatz.
T1558.003	Kerberoasting	Red	Utilisation de l'outil SharpRoa:
T1046	Network Service Discovery	Red	Utilisation de l'outil de découv
T1018	Remote System Discovery	Red	Utilisation des outils de décou
T1210	Exploitation of Remote Services	Red	Tentative d'exploitation des vu
T1090.004	Domain Fronting	Red	Utilisation du CND CLOUDFL
T1572	Protocol Tunneling	Red	Utilisation d'un tunnel SOCKS



T1136.001	Local Account	Red	Tentative de création du comp
T1068	Exploitation for Privilege Escalation	Red	Tentative d'exploitation des vu
T1036.005	Match Legitimate Name or Location	Red	Utilisation des répertoires « C:
T1110.003	Password Spraying	Red	Utilisation de l'outil AccountRe
T1003.001	LSASS Memory	Red	Utilisation de l'outil Mimikatz.
T1558.003	Kerberoasting	Red	Utilisation de l'outil SharpRoa:
T1046	Network Service Discovery	Red	Utilisation de l'outil de découv
T1018	Remote System Discovery	Red	Utilisation des outils de décou
T1210	Exploitation of Remote Services	Red	Tentative d'exploitation des vu
T1090.004	Domain Fronting	Red	Utilisation du CND CLOUDFL
T1572	Protocol Tunneling	Red	Utilisation d'un tunnel SOCKS

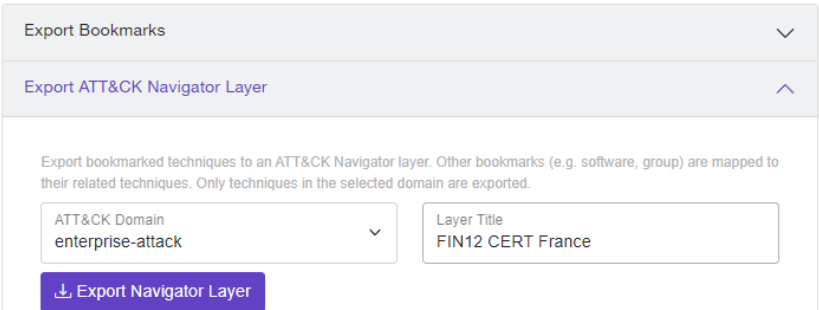


ATT&CK POWERED SUIT

T1136.001 T1068 T1036.005 T1

Select all | none

- Enterprise
- ICS
- Mobile
- Deprecated



Export Bookmarks

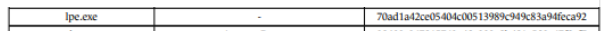
Export ATT&CK Navigator Layer

Export bookmarked techniques to an ATT&CK Navigator layer. Other bookmarks (e.g. software, group) are mapped to their related techniques. Only techniques in the selected domain are exported.

ATT&CK Domain: enterprise-attack

Layer Title: FIN12 CERT France

Export Navigator Layer



Name	ID	Notes
lpc.exe	70ad1a42ce05404c00513989c949c83a94fcc92	
AccountPartners	3860033c791c7c1c003006b6f81c003c20a-c7	

Tools that can be used during targeting. Tools can be open used for malicious purposes by an adversary, but (unlike poses (ex: PsExec situation can involve the procurement of commercial

that can be used during targeting. Use of servers n operation. During post-compromise activity, luding for Command and Control. Adversaries may use ions, as in Drive-by Compromise

Technique
 Services to initially access and/or persist within a network. Less mechanisms allow users to connect to internal . There are often remote service gateways that manage services. Services such as Windows...

Technique
 Domain account as a means of gaining Initial Access, n. (Citation: TechNet Credential Theft) Domain accounts

Mapping Capabilities & Tools latest Fin12 campaign

- Cobalt Strike
- SystemBC
- AccountRestore
- Mimikatz
- SharpRoast
- Softperfect Network Scanner
- PingCastle
- Bloodhound

3.1 Tableau de TTP

Phase	Technique	Nom	Commentaire
Resource Development	T1588.002	Obtain Capabilities: Tool	Utilisation de l'outil Random C2 Profile Generator pour générer le profil <i>Malleable C2 Cobalt Strike</i> .
Resource Development	T1583.004	Acquire Infrastructure: Server	Utilisation de VPS hébergés chez VULTR comme serveurs C2 SystemBC , et utilisation du port 4177.
Initial Access	T1133	External Remote Services	Connexion à un service de bureau à distance.
Initial Access	T1078.002	Valid Accounts: Domain Accounts	Utilisation d'authentifiants valides pour se connecter à un service de bureau à distance.
Persistence	T1136.001	Create Account: Local Account	Tentative de création du compte « supp ».
Privilege Escalation	T1068	Exploitation for Privilege Escalation	Tentative d'exploitation des vulnérabilités <i>LocalPotato</i> (CVE-2023-21746) et CVE-2022-24521.
Defense Evasion	T1036.005	Masquerading: Match Legitimate Name or Location	Utilisation des répertoires « C:\Users\Public\Music\ » et « C:\Users\[user]\Downloads\ ».
Credential Access	T1110.003	Brute Force: Password Spraying	Utilisation de l'outil AccountRestore avec le dictionnaire « Passwordar.txt ».
Credential Access	T1003.001	OS Credential Dumping: LSASS Memory	Utilisation de l'outil Mimikatz .
Credential Access	T1558.003	Steal or Forge Kerberos Tickets: Kerberoasting	Utilisation de l'outil SharpRoast .
Discovery	T1046	Network Service Discovery	Utilisation de l'outil de découverte réseau Softperfect Network Scanner .
Discovery	T1018	Remote System Discovery	Utilisation des outils de découverte PingCastle et BloodHound .
Lateral Movement	T1210	Exploitation of Remote Services	Tentative d'exploitation des vulnérabilités <i>PrintNightmare</i> (CVE-2021-34527), <i>BlueKeep</i> (CVE-2019-0708) et <i>ZeroLogon</i> (CVE-2020-1472).
Command and Control	T1090.004	Proxy: Domain Fronting	Utilisation du CND CLOUDFLARE afin de dissimuler le serveur C2 Cobalt Strike final.
Command and Control	T1572	Protocol Tunneling	Utilisation d'un tunnel SOCKS5 via l'implant SystemBC .

Mapping Fin12 Capabilities latest CERT Alert France

Fin12 Capabilities & ...

SystemBC Cobalt Strike Rando... FIN12 CERT France... SystemBC AccountRestore SharpRoast SoftPerfect Networ... PingCastle BloodHound

Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control
Server	External Remote Services	PowerShell	Account Manipulation	SID-History Injection	SID-History Injection	Password Spraying	Domain Account	Exploitation of Remote Services	Archive Collected Data	Protocol Tunneling
Virtual Private Server	Domain Accounts	Native API	Security Support Provider	Security Support Provider	Match Legitimate Name or Location	Credentials from Password Stores (2)	Local Account	Pass the Hash		Domain Fronting
Tool		Scheduled Task/Job	Local Account	Exploitation for Privilege Escalation	Rogue Domain Controller	Credentials from Web Browsers	Domain Trust Discovery	Pass the Ticket		
			External Remote Services	Scheduled Task/Job	Pass the Hash	Windows Credential Manager	Group Policy Discovery			
			Scheduled Task/Job	Domain Accounts	Pass the Ticket	DCSync	Network Service Discovery			
			Domain Accounts		Domain Accounts	LSA Secrets	Password Policy Discovery			
					Time Based Evasion	LSASS Memory	Domain Groups			
						Security Account Manager	Local Groups			
						Steal or Forge Authentication Certificates	Query Registry			
						Golden Ticket	Remote System Discovery			
						Kerberoasting	System Information Discovery			
						Silver Ticket	System Owner/User Discovery			
						Private Keys	Time Based Evasion			

Fin12 Tidal – Details External Remote Services Useful Analytics

External Remote Services



Vendors (18)

Groups (27)

Software (7)

Data Sources (5)

Campaigns (7)

References (45)

Analytics (9)

Name ↑	Repository
External Remote RDP Logon from Public IP	Sigma
External Remote SMB Logon from Public IP	Sigma
Failed Logon From Public IP	Sigma

Analytic Detail

External Remote RDP Logon from Public IP

Detects Technique(s): [Brute Force](#), [External Remote Services](#), [Valid Accounts](#)

Location: https://github.com/SigmaHQ/sigma/blob/60b8e9b70ffaf49b17abfcae4a0ea08f2da7f71/rules/windows/builtin/security/account_management/win_security_successful_external_remote_rdp_login.yml

Source: SIGMA

Contributors: [Micah Babinski \(@micahbabinski\)](#), [Zach Mathis \(@yamatosecurity\)](#)

License: [Detection Rule License 1.1](#)

Detects successful logon from public IP address via RDP. This can indicate a publicly-exposed RDP port.

```
selection: EventID: 4624 LogonType: 10filter_ipv4: IPAddress|cidr: - 127.0.0.0/8 - 10.0.0.0/8 - 172.16.0.0/12 - 192.168.0.0/16filter_ipv6:- IPAddress: ::1 # IPv6 loopback-
IPAddress|startswith: - 'fe80:' # link-local address - fc # private address range fc00::/7 - fd # private address range fc00::/7filter_empty: IPAddress: '-'condition: selection
and not 1 of filter_*
```


Some Artifacts and Command Line as starting point for Threat Hunting and Detection Engineering PrintNightmare 2/2

- Batch files and SHA1 hash
- Specific executable and DLLs

Nom de fichier	Chemin	SHA1	Commentaire
LPE-Exploit-RunAsUser.bat	C:\Users\[user]\Downloads\PrintNightmare-Manual\Attacker\	e2a68116d52182f207c087f349e04e049982d431	CVE-2021-34527
Step1-RunAsAdmin.bat	C:\Users\[user]\Downloads\PrintNightmare-Manual\Attacker\	fae6068d4433b33751bf7de866d7f2900aa15139	CVE-2021-34527
Step2-RunAsUser.bat	C:\Users\[user]\Downloads\PrintNightmare-Manual\Attacker\	d69420a636dacfbafaf01f7153692c197e9b6400	CVE-2021-34527
spn.exe	C:\Users\[user]\Downloads\PrintNightmare-Manual\Attacker\Release\	68a07540fbf58fe743636b7fc8f0370c84134eb3	CVE-2021-34527
spn_nf3.exe	C:\Users\[user]\Downloads\PrintNightmare-Manual\Attacker\Release\	58cb839dbc0232874b6fed9a354d4cc6d355cbac	CVE-2021-34527
spider.dll	C:\Users\[user]\Downloads\PrintNightmare-Manual\Attacker\share\	1e0ec6994400413c7899cd5c59bdb6397dea7b5	CVE-2021-34527
spider_32.dll	C:\Users\[user]\Downloads\PrintNightmare-Manual\Attacker\share\	35ff55bcf493e1b936dc6e978a981ee2a75543a1	CVE-2021-34527
CreShar.exe	C:\Users\[user]\Downloads\PrintNightmare-Manual\C#-CreateShare\	a00ebf699ea0759e7bf4af65ddd741133c38484	CVE-2021-34527
MakeMeGood.bat	C:\Users\[user]\Downloads\PrintNightmare-Manual\Victim\	df12386df2c0fcf65522282914424d63da962d79	CVE-2021-34527
bks.exe	C:\Users\[user]\Downloads\8.1.5\bluekeep\	-	CVE-2019-0708

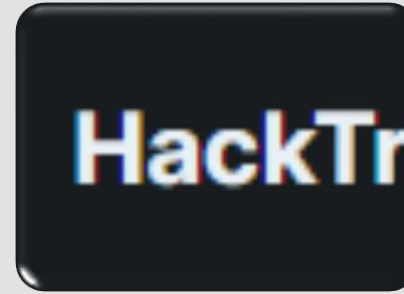
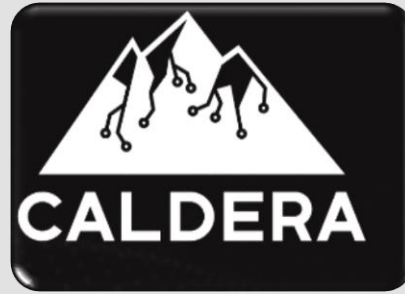
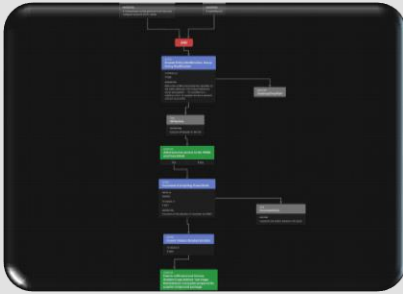
2023
FIRST
Cyber Threat
Intelligence
Conference

Berlin, Germany
November 6-8, 2023

Emulate & Threat
Hunting Healthcare RMM
Tools



Defensive Engagement – Emulate or Simulate threat actors & top TTPs in the Healthcare with BAS Tools & Atomic Red Team



Preparation with the Attack Flow as a playbook for the threat actor

BAS Tools MITRE Caldera

Purple Teaming with BAS

Pentesting or Red Teaming test examples of different websites like HackTricks or Atomic Red Team

Vulnerabilities testing with the help of websites like – Exploit-DB

Threat Hunting RMM Tools

PEAK Framework David Bianco



ABLE translated into threat informed defense



Example for AnyDesk



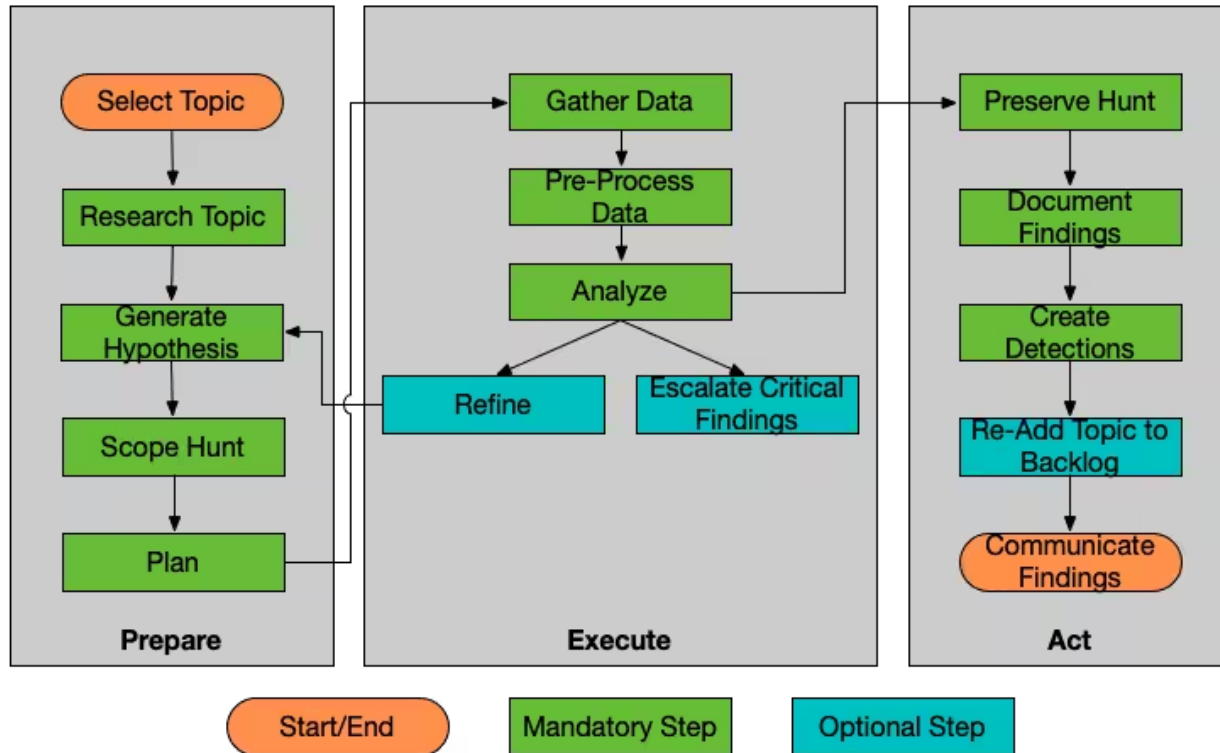
Test and telemetry results



Other Sigma rules for RMM Tools

Hypothesis-Driven Hunting Process PEAK Framework @David Bianco

Hypothesis-Driven Hunting Process in the PEAK Framework



- Come up with a topic – select a MITRE ATT&CK technique
- Make it testable
- Refine as necessary
- Holistic Thread Modeling – structured analysis
- Cyber Threat Intelligence and Cyber Threat Profiling => multilayering hypothesis (ACH)
- Defensive Engagement: test, rigid, repeat
- Refine results in a **OODA-Loop**

PEAK framework translated into Threat Informed Defense

David Biancos ABLE

- Actor: the threat actor you're looking for
- Behavior: the specific activity your trying to find (TTPs)
- Location: End-user's dektop, internet-facing web server etc.
- Evidence: data sources you need to consult the activity

Threat Informed Defense Enterprise-Centric ABLE:

- Actor: the threat actor you're looking for is contextual organizational analyzed (CSIRT, IR, own incidents and artifacts, vulnerabilities etc.)
- Behavior: the specific activity known from multilayering the capabilities (TTPs)
- Location: End-user's dektop, internet-facing web server etc. **Organization's network**
- Evidence: data sources you need to consult the activity within the organization (which data source do you have available? What do you see and which data is missing?)

ABLE for RMM Tools

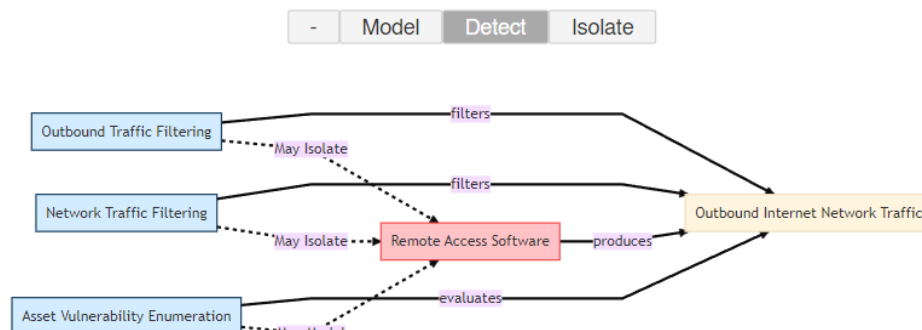
Threat Informed Defense Enterprise-Centric ABLE:

- Actor: We're looking for ransomware groups in the healthcare using RMM Tools (evidence-based)
- Behavior: the known technique is T1219 and the abuse of legitimate tools for external remote access T1133
- Location: End-user's desktop, End-user's AppData or ProgramData and your network traffic (flow, content and connection creation)

- Evidence: Which data source do you have available in your environment? Can you log everything? Do you have any data gaps?

Relevant Data Sources for T1219:

- Network Traffic
 - Network Connection Creation
 - Network Traffic Content
 - Network Traffic Flow
- Process => process creation



ABLE Phase 1. Prepare: Setting the Stage for your hunt

- **Select Topic: T1219 Remote Access Software**

- **Research Topic:**

- Learn about the specific relevant RMM tools for Healthcare Ransomwaregroups
- Detection of such Tools
- MITRE ATT&CK documentation T1219
- Command Lines to test and detect
- Specific threat actor comparison
- Use platforms and tools like HUNTER, D3FEND & KAPE (forensics) for technical details and specific research

- **Generate Hypothesis:** Threat actor could establish a C2 connection via a remote tool - external remote access to move laterally.

- **Scope Hunt:** Try to find all RMM Tools in the environment. Differentiate abnormal behavior from normal by finding outlier.

- **Plan:**

- Gathering the data from the Logs & Telemetry
- Using Sysmon and Telemetry, Testing with Atomic and other research sources, to understand the results in the own environment (security tools)
- Start Hunting with the suggested technique in HUNTER or with a own created query
- Focus on sensors and data source like network connection, traffic & flow, proces creation etc.

ABLE Phase 1. Research RMM Tools Healthcare Ransomware groups – Example AnyDesk download and execution

AnyDesk

Atera RMM

LogMeIn

ManageEngine

Netsupport Manager Application

Ngrok

PsExec

Putty

Quasar RAT

rsocx

RealVNC

Splashtop

TeamViewer

Command

```
AnyDesk.exe --install "%ProgramFiles(x86)%\AnyDesk" --start-with-win --silent
```

The screenshot displays the TIDAL CYBER interface with several panels:

- Analytic Detail:** Shows detection information for AnyDesk, including the location of the temporary artifact and a detection rule license.
- Atomic Test #2 - AnyDesk Files Detected Test on Windows:** Provides instructions on how an adversary might trick a user into downloading AnyDesk. It lists supported platforms (Windows) and an auto-generated GUID: 6b8b7391-5c0a-4f8c-baee-78d8ce0ce330. It includes attack commands for running with PowerShell and cleanup commands for removing the file.
- KapeFiles / Targets / Apps / AnyDesk.tkape:** Shows a configuration file for AnyDesk with a list of targets and their file masks. The targets include logs for user profiles and program data, as well as video recordings.
- Files:** A file explorer view showing a directory structure with folders like .github, Modules, Targets, Disabled, and Antivirus.

ABLE Phase 1. Research RMM Tools Healthcare Ransomware groups – Test download and installation in your environment

AnyDesk

Atera RMM
LogMeIn
ManageEngine
Netsupport Manager Application
Ngrok
PsExec
Putty
Quasar RAT
rsocx
RealVNC
Splashtop
TeamViewer
Tor C2

- Evidence: data sources you need to consult - the activity within the organization (which data source do you have available?)
 - Network Traffic
 - Network Connection Creation
 - Sysmon EID 3
 - Network Traffic Content
 - Protocols 443
 - Network Traffic Flow
 - Invariant **net.anydesk.com**
 - (File creation EID 11 Sysmon for downloading the tool)
 - Process creation
 - Windows Event 4688 or Sysmon EID 1
- Artifacts during installation own telemetry example:
 - During installation startup folder AnyDesk.Ink with Sysmon EID 11 file creation
 - Command line contains AnyDesk and --control
 - Several registry keys
 - `\REGISTRY\MACHINE\SOFTWARE\Classes\AnyDesk\shell\open\command\`
 - `"C:\Program Files\AnyDesk\AnyDesk.exe" "%1"`
 - Pipe creation found in own telemetry
 - `\adprinterpipe`

ABLE Phase 2 Execute: Gather data and escalate critical findings

- Gather Data
- Pre-Process Data
 - Convert to JSON or CSV
 - Normalize logs
 - Throw out nonsensical values
- Analyze
 - Clustering
 - Visualization
 - Least/most frequency/occurrence
 - (outlier)
- Refine Hypothesis
- Escalate Critical Findings

```
1 title: Remote Access Tool - AnyDesk Silent Installation
2 id: 114e7f1c-f137-48c8-8f54-3889c24ce4b9
3 status: test
4 description: Detects AnyDesk Remote Desktop silent installation. Which can be used by attackers to gain remote access.
5 references:
6   - https://twitter.com/TheDFIRReport/status/142336119926816776?s=28
7   - https://support.anydesk.com/Automatic_Deployment
8 author: Jan Trenčanský
9 date: 2021/03/05
10 modified: 2023/03/05
11 tags:
12   - attack_command_and_control
13   - attack.t1219
14 logsource:
15   category: process_creation
16   product: windows
17 detection:
18   selection:
19     CommandLine|contains|all:
20     - '--install'
21     - '--start-with-win'
22     - '--silent'
23   condition: selection
24 fields:
25   - CommandLine
26   - ParentCommandLine
27   - CurrentDirectory
28 falsepositives:
29   - Legitimate deployment of AnyDesk
30 level: high
```

```
1 index=* source=WinEventLog:* AND ((CommandLine*"--install*") AND (CommandLine*"--start-with-win*") AND (CommandLine*"--silent*")) | table CommandLine,ParentCommandLine,CurrentDirectory
```

```
DeviceProcessEvents | where ((ProcessCommandLine contains @'--install' and ProcessCommandLine contains @'--start-with-win' and ProcessCommandLine contains @'--silent')
```

```
Event 1, Sysmon
General Details
Process Create:
RuleName: technique_id=T1059.003;technique_name=Windows Command Shell
UtcTime: 2023-10-04 19:48:16.584
ProcessGuid: {bd6ed866-c180-651d-c702-000000000000}
ProcessId: 5136
Image: C:\Users\observer\Desktop\AnyDesk.exe
FileVersion: 8.0.3
Description: AnyDesk
Product: AnyDesk
Company: AnyDesk Software GmbH
OriginalFileName: -
CommandLine: AnyDesk.exe --install "C:\Program Files (x86)\AnyDesk" --start-with-win --silent
CurrentDirectory: C:\Users\observer\Desktop\
User: DESKTOP-MM6F536\observer
LogonGuid: {bd6ed866-11f5-650e-fb2b-040000000000}
LogonId: 0x42BFB
TerminalSessionId: 1
IntegrityLevel: High
Hashes: SHA1=1895D7C4F785F92E4885191FD812822593CBC73F,MD5=37E172BE64B12F3207300D11B74656B8,SHA256=BC747E3BF7B6E02C09F3D18DD0E64EEF62B940B2F16C9C72E647EEC85CF0138,IMPHASH=0000000000000000000000000000000000000000
ParentProcessGuid: {bd6ed866-c010-651d-ba02-000000000000}
```

TIDEC-ABLE Phase 3 Act. Preserve Hunt and Document Findings

- Preserve Hunt: create your own knowledge base or wiki, documentation etc.
- Documents Finding: report on findings and incidents escalated
- Create Detections: Convert your findings into production detection rules or signatures to help catch similar threats in the future. Or send your detailed findings to the detection engineers if that's how your organization rolls. Either way, using hunts to improve automated detection is the other key driver behind continuous improvement of your security posture.
- Re-Add Topic to Backlog: new ideas and future hunting
- Communication Findings: Collaboration & Sharing

Other RMM Tools Sigma rules examples

- Atera:
https://github.com/SigmaHQ/sigma/blob/04f72b9e78f196544f8f1331b4d9158df34d7ecf/rules/windows/builtin/application/win_software_atera_rmm_agent_install.yml
- Ngrok:
https://github.com/SigmaHQ/sigma/blob/e78cb13cfdd5f2308e720e432ccb2e73e39d2d60/rules/windows/network_connection/net_connection_win_ngrok_tunnel.yml
- Splashtop
https://github.com/The-DFIR-Report/Sigma-Rules/blob/c253c57c627b6d8cbcfa06320a3ad1ba2b9dedd4/win_network_splashtop.yml
- https://github.com/The-DFIR-Report/Sigma-Rules/blob/c253c57c627b6d8cbcfa06320a3ad1ba2b9dedd4/win_software_splashtop.yml
- Hunting
https://github.com/SigmaHQ/sigma/blob/60b8e9b70ffaf49b17abfcae4a0ea08f2da7f71/rules/windows/dns_query/dns_query_win_remote_access_software_domains.yml

sigma / rules / windows / builtin / application / win_software_atera_rmm_agent_install.yml

frack113 Order rules

Code Blame 23 lines (23 loc) · 739 Bytes

```
1 title: Atera Agent Installation
2 id: 87261fb2-69d0-42fe-b9de-88c6b5f65a43
3 status: experimental
4 description: Detects successful installation of Atera Remote Monitoring & Management (RMM) agent as recently found to be used by Conti operators
5 references:
6   - https://www.advintel.io/post/secret-backdoor-behind-conti-ransomware-operation-introducing-atera-agent
7 date: 2021/09/01
8 modified: 2021/10/13
9 author: Bhabesh Raj
10 level: high
11 logsource:
12   service: application
13   product: windows
14 tags:
15   - attack.t1219
16 detection:
17   selection:
18     EventID: 1033
19     Provider_Name: MsiInstaller
20     Message|contains: AteraAgent
21   condition: selection
22 falsepositives:
23   - Legitimate Atera agent installation
```

2023
FIRST
Cyber Threat
Intelligence
Conference

Berlin, Germany
November 6-8, 2023

Pyramid of Pain &
Summitting the Pyramid –
Cyber Analytic
Engineering in CTI



Pyramid of Pain - Downloading AnyDesk

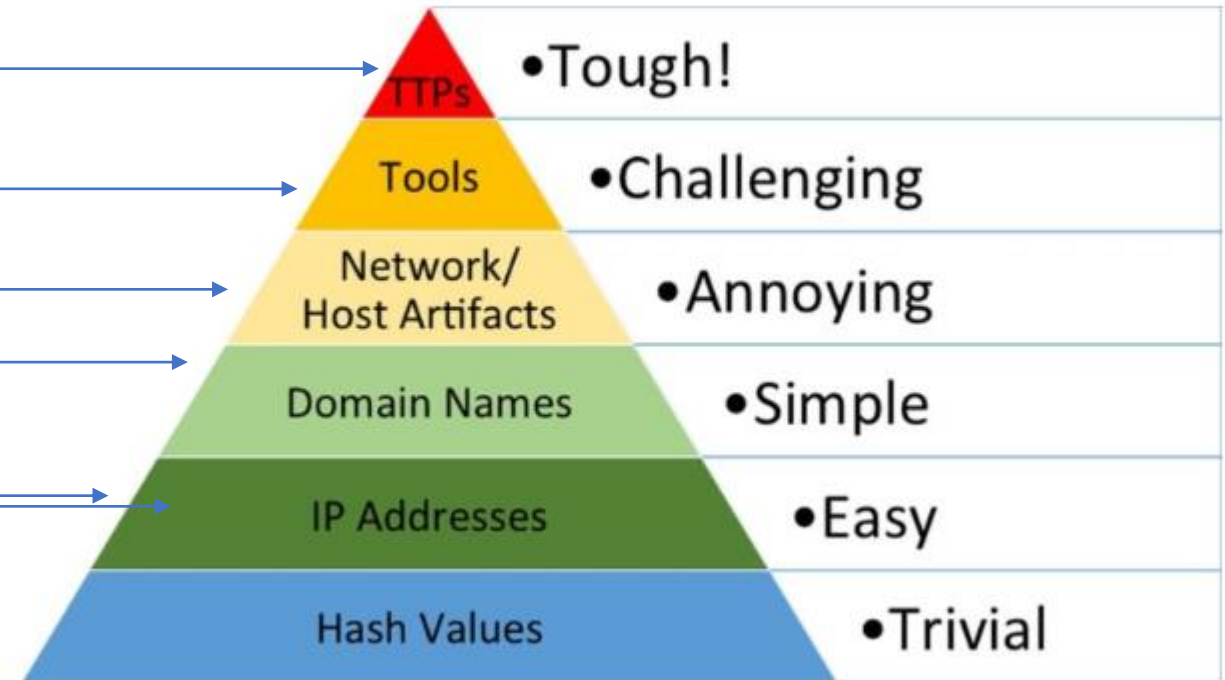
Event 3, Sysmon

General Details

Network connection detected:
RuleName: technique_id=T1036,technique_name=Masquerading
UtcTime: 2023-09-23 00:08:04.884
ProcessGuid: {bd6ed866-b7a6-651d-8302-00000000d00}
ProcessId: 2896
Image: C:\Users\observer\Desktop\AnyDesk.exe
User: DESKTOP-MM6F536\observer
Protocol: tcp
Initiated: true
SourceIsIpv6: false
SourceIp: 192.168.146.147
SourceHostname: DESKTOP-MM6F536
SourcePort: 62453
SourcePortName: -
DestinationIsIpv6: false
DestinationIp: 57.128.101.75
DestinationHostname: relay-bfa30227.net.anydesk.com
DestinationPort: 443
DestinationPortName: https

Log Name: Microsoft-Windows-Sysmon/Operational
Source: Sysmon
Event ID: 3
Level: Information
User: SYSTEM
OpCode: Info
More Information: [Event Log Online Help](#)

Logged: 10/4/2023 9:06:19 PM
Task Category: Network connection detected (rule: NetworkK
Keywords:
Computer: DESKTOP-MM6F536



Pyramid of Pain - Installation of AnyDesk

Event 1, Sysmon

General Details

```
Process Create:  
RuleName: technique_id=T1059.003,technique_name=Windows Command Shell  
UtcTime: 2023-10-04 19:48:16.584  
ProcessGuid: {bd6ed866-c180-651d-c702-000000000d00}  
ProcessId: 5136  
Image: C:\Users\observer\Desktop\AnyDesk.exe  
FileVersion: 8.0.3  
Description: AnyDesk  
Product: AnyDesk  
Company: AnyDesk Software GmbH  
OriginalFileName: -  
CommandLine: AnyDesk.exe --install "C:\Program Files (x86)AnyDesk" --start-with-win --silent  
CurrentDirectory: C:\Users\observer\Desktop\  
User: DESKTOP-MM6FS36\observer  
LogonGuid: {bd6ed866-11f5-650e-fb2b-040000000000}  
LogonId: 0x42BFB  
TerminalSessionId: 1  
IntegrityLevel: High  
Hashes: SHA1=1895D7C4F785F92E48B5191FD812822593CBC73F,MD5=37E172BE64B12F3207300D11B  
00000000000000000000000000000000  
ParentProcessGuid: {bd6ed866-c010-651d-ba02-000000000d00}
```

The diagram illustrates the 'Pyramid of Pain' for the installation of AnyDesk, showing the difficulty of various indicators of compromise (IOCs) from top to bottom:

- TTPs** (Tactics, Techniques, and Procedures): •Tough!
- Tools**: •Challenging
- Network/Host Artifacts**: •Annoying
- Domain Names**: •Simple
- IP Addresses**: •Easy
- Hash Values**: •Trivial

Arrows from the Sysmon event details point to the corresponding levels in the pyramid:

- The **RuleName** (technique_id=T1059.003,technique_name=Windows Command Shell) points to the **TTPs** level.
- The **Product** (AnyDesk) and **Company** (AnyDesk Software GmbH) fields point to the **Tools** level.
- The **Hashes** (SHA1 and MD5) point to the **Hash Values** level.

Summitting the Pyramid – TID Analysis **AnyDesk**

SUMMITTING THE PYRAMID
Level Up Your Analytics

Event 17, Sysmon

General Details

Pipe Created:
RuleName: -
EventType: CreatePipe
UtcTime: 2023-10-04 19:48:19.920
ProcessGuid: {bd6ed866-c183-651d-cc02-000000000d00}
ProcessId: 2376
PipeName: \adprinterpipe
Image: C:\Program Files (x86)AnyDesk\AnyDesk.exe
User: DESKTOP-[REDACTED]

HKCR\anydesk\shell\open\command
Pipe created \adprinterpipe

CORE TO TECHNIQUE
T1053:Sysmon ID 13
TargetObject=
"HKLM\SOFTWARE\
Microsoft\Windows NT\
CurrentVersion\Schedule\
TaskCache\Tree

T1219 Event AppDomain Pipe creation: ID 53505 Pipe IPC

IMPLEMENTATIONS
Event ID 5136 T1556:
mdDS-KeyCredentialLink

PRE-EXISTING TOOL
Sysmon ID 1:
OriginalFileName:schtasks.exe

OriginalFileName AnyDesk.exe:
"C:\Program Files
(x86)AnyDesk\AnyDesk.exe" --control

ADVERSARY TOOL
Event ID 4104
ScriptBlockText
| contains: vaultcmd

Event EID 3 net.anydesk.com

EPHEMERAL
Event ID 4688
22dc9f0490f5ae
9f014d1acb7ed5641

SHA 1: 1895D7C4F785F92E48B5191FD812822593CBC73F, Symon EID 1 or 4688

MITRE ENGENUITY. | Center for Threat Informed Defense

Analytical Scoring - How Robust is the detection?

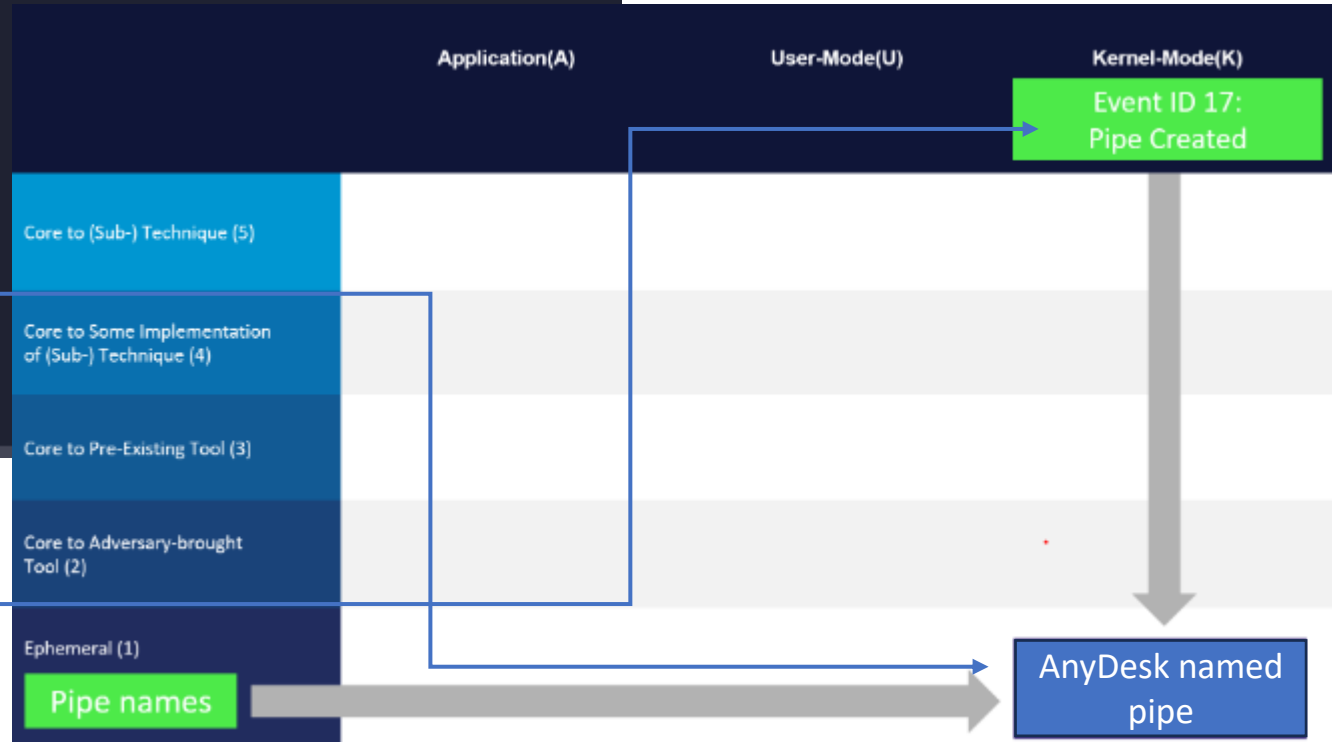
```
title: AnyDesk Suspicious Pipe Creation
id: f7784b57-a6f1-4113-9d84-1c92f02ca078
status: experimental
description: Detects the creation of a pipe specific related to AnyDesk
references:
  - https://www.hybrid-analysis.com/sample/99dcdda32ee45835489890b3bcc273116bdcf6c263e0cf6f74542ea3d56b78a1/60e21d53d4e6ff722e5617e6
author: Simone Kraus (Orange Cyberdefense)
date: 2023/10/05
tags:
  - attack.command_and_control
  - attack.attack.t1219 #Remote Access Software
logsource:
  product: windows
  category: pipe_created
detection:
  selection:
    - PipeName|startswith:
      - '\adprinterpipe'
  condition: selection
falsepositives:
  - Legitimate use of AnyDesk
level: high
```

- Step 1: Scoring the analytic's sensor data
- Step 2: Break down each of the observables
- Step 3: Analyze the selection or condition of the analytic
- Step 4: Give the analytic a final score

Event 17, Sysmon

General Details

Pipe Created:
RuleName: -
EventType: CreatePipe
UtcTime: 2023-10-04 19:48:19.920
ProcessGuid: {bd6ed866-c183-651d-cc02-000000000d00}
ProcessId: 2376
PipeName: \adprinterpipe
Image: C:\Program Files (x86)\AnyDesk\AnyDesk.exe
User: DESKTOP-



2023
FIRST
Cyber Threat
Intelligence
Conference

Berlin, Germany
November 6-8, 2023

Use Case Ransomware -
LockBit



USE CASE LockBit – Joint Cybersecurity Advisory with the BSI

- Multilayering approach using the latest Threat Intelligence
- Prioritize your Cybersecurity Threat Profile enterprise-centric

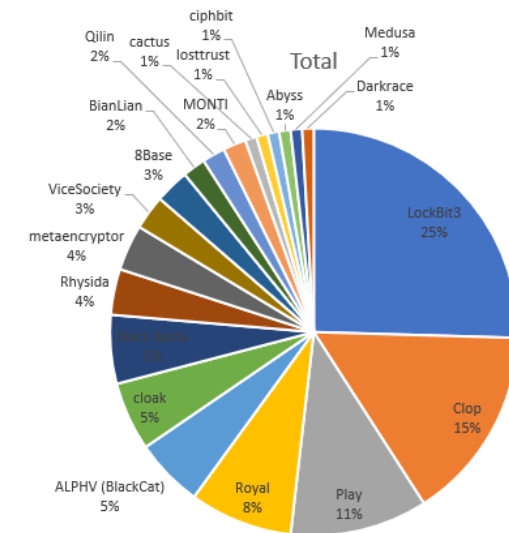
The image shows the cover of a 'JOINT CYBERSECURITY ADVISORY' report. The title 'LockBit' is prominently displayed in large white letters on a dark blue background. Above the title, it says 'JOINT CYBERSECURITY ADVISORY'. Below the title, there is a section for 'Co-Authored by:' followed by logos of various international cybersecurity organizations including CISA, MS-ISAC, Communications Security Establishment Canada, National Cyber Security Centre, Australian Government, ACSC, République Française, and Federal Office for Information Security. The report is marked as 'TLP: CLEAR' and has a 'Product ID: AA23-165A' and a date of 'June 14, 2023'. At the bottom, there is a dark blue banner with the text 'UNDERSTANDING RANSOMWARE THREAT ACTORS: LockBit' and a graphic of a glowing red archway.

The Cy-X group LockBit as Use Case – Latest Ransomware & Extortion operation

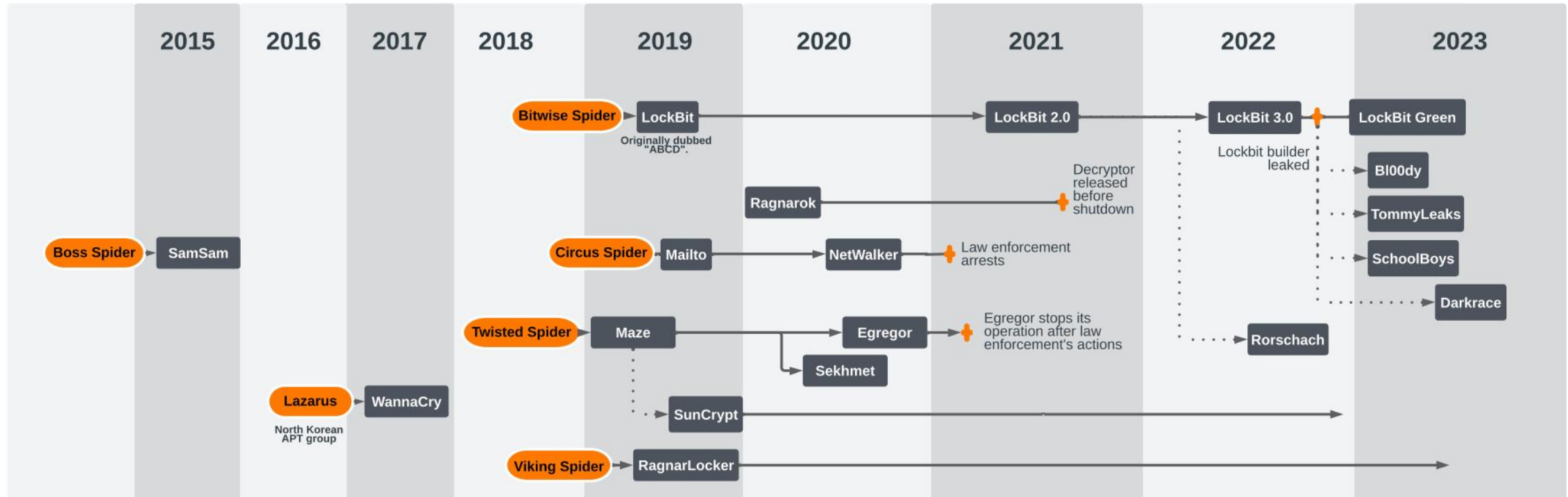


General Information:

- In 2022, LockBit was the most deployed ransomware and again in July 2023 (Tidal Research)
- The BSI has currently classified the ransomware group as the most dangerous cybercrime player in the world.
- Organizations of all sizes are among the victims of LockBit.



Lockbit in the Ransomware Ecosystem



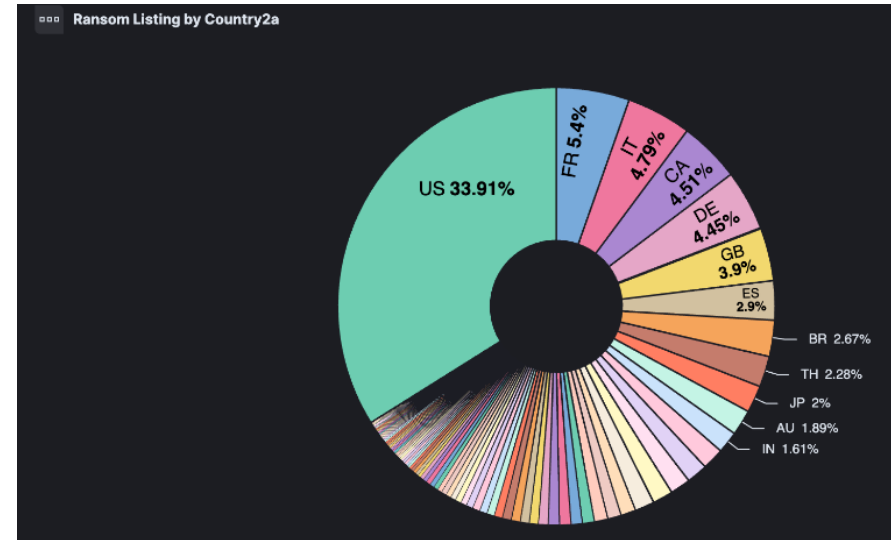
Methods of LockBit

- Assuring payment by allowing affiliates to receive ransom payments before sending a cut to the core group
- Disparaging other RaaS groups
- Engaging in publicity-generating activities
- Developing point-and-click interface for its ransomware

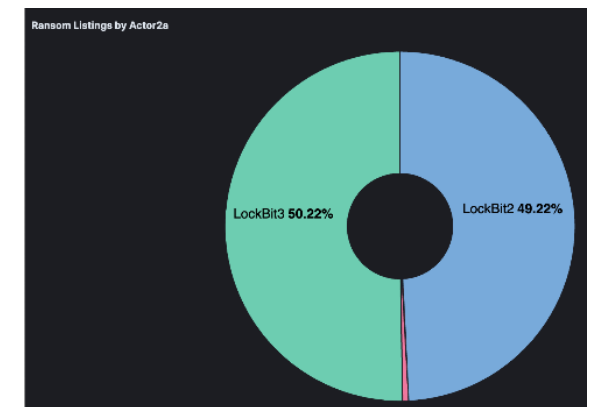
Different LockBit versions – OCD Research (64 events)

Name of the Strain*	Number of Inscances
Lockbit 2.0 (Lockbit Red)	26
Lockbit 3.0 (Lockbit Black)	23
Lockbit	21
Lockbit Green	1
Lockbit (pre-encrpytion)	1

50:49 of all Lockbit attacks are Lockbit3.0 and Lockbit2.0



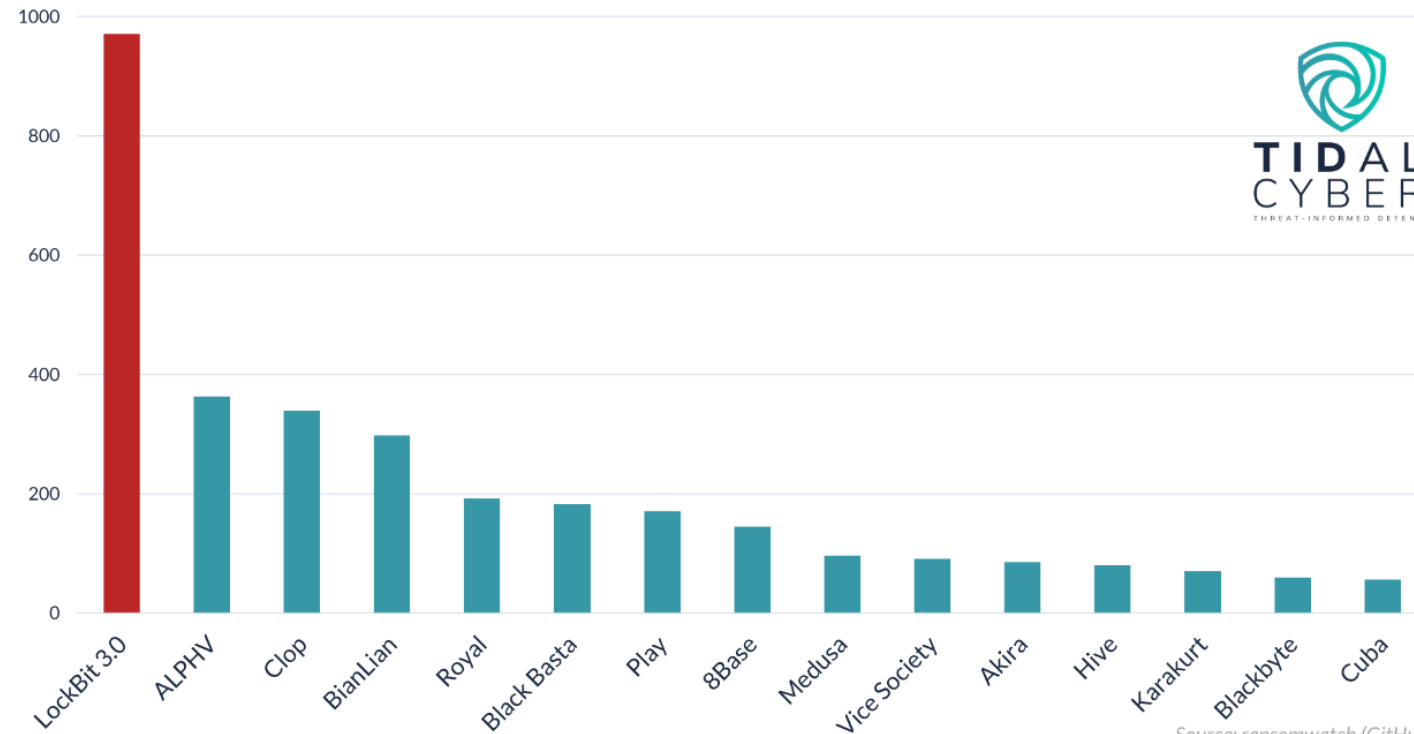
4.45% of all Lockbit attacks happen in Germany



Top Ransomware & Extortion Operations Tidal Cyber Research

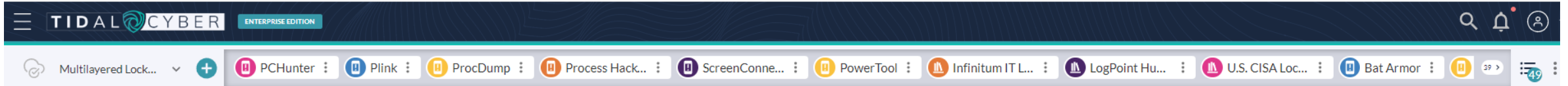
Top Ransomware & Extortion Operations

By Claimed Victim Count, July 2022-July 2023



Source: ransomwatch (GitHub)

Storytelling Multilayering – Latest LockBit Research & Tools



Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
1 Drive-by Compromise	PowerShell	Account Manipulation	Abuse Elevation Control Mechanism (1)	Abuse Elevation Control Mechanism (1)	LLMNR/NBT-NS Poisoning and SMB Relay	Account Discovery (2)	Lateral Tool Transfer	LLMNR/NBT-NS Poisoning and SMB Relay	Application Layer Protocol (2)	Data Transfer Size Limits	Data Destruction
Exploit Public-Facing Application	Windows Command Shell	Boot or Logon Autostart Execution (3)	Bypass User Account Control	Bypass User Account Control	Brute Force	Domain Account Local Account	Remote Desktop Protocol	Archive Collected Data (1)	File Transfer Protocols	Exfiltration Over Alternative Protocol (2)	Data Encrypted for Impact
External Remote Services	Component Object Model	Registry Run Keys / Startup Folder	SID-History Injection	SID-History Injection	Credentials from Password Stores (3)	Debugger Evasion	SMB/Windows Admin Shares	Automated Collection	Web Protocols	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Internal Defacement
Phishing	Native API	Security Support Provider	Token Impersonation/Theft	Token Impersonation/Theft	Credentials from Web Browsers	Domain Trust Discovery	Software Deployment Tools	Screen Capture	Domain Generation Algorithms	Exfiltration Over Unencrypted Non-C2 Protocol	Inhibit System Recovery
Valid Accounts (2)	Scheduled Task/Job (1)	Shortcut Modification	Boot or Logon Autostart Execution (3)	Debugger Evasion	Keychain	File and Directory Discovery	Pass the Hash	Video Capture	Encrypted Channel	Exfiltration Over C2 Channel	Service Stop
Default Accounts	Scheduled Task	Domain Account	Registry Run Keys / Startup Folder	Group Policy Modification	Windows Credential Manager	Group Policy Discovery	Pass the Ticket	Non-Application Layer Protocol	Ingress Tool Transfer	Exfiltration Over Web Service (1)	
Domain Accounts	Software Deployment Tools	Windows Service	Security Support Provider	Environmental Keying	Network Service	Network Service Discovery		Protocol Tunneling	Non-Application Layer Protocol	Exfiltration to Cloud Storage	
	Service Execution	External Remote Services	Shortcut Modification	DLL Search Order Hijacking	OS Credential Dumping (8)	Network Share Discovery		Proxy	Remote Access Software		
	User Execution (1)	DLL Search Order Hijacking	Windows Service	DLL Side-Loading	Cached Domain Credentials	Network Sniffing		Web Service			
	Malicious File	DLL Side-Loading	Group Policy Modification	Impair Defenses (4)	DCSync	Password Policy Discovery					
	Windows Management Instrumentation	Pre-OS Boot	Disable or Modify System Firewall	Disable Windows Event Logging	/etc/passwd and /etc/shadow	Peripheral Device Discovery					
		Scheduled Task/Job (1)	Disable or Modify System Tools	Safe Mode Boot	LSA Secrets	Process Discovery					
		Scheduled Task	DLL Search Order Hijacking	Indicator Removal (3)	NTDS	Remote System Discovery					
		Valid Accounts (2)	DLL Side-Loading	Clear Persistence	Steal or Forge Authentication Certificates	System Information Discovery					
		Default Accounts	Process Injection	Clear Windows Event Logs	Golden Ticket	System Language Discovery					
		Domain Accounts	Scheduled Task/Job (1)	File Deletion	Kerberoasting	System Network Configuration Discovery					
			Default Accounts	Match Legitimate Name or Location	Silver Ticket	System Owner/User Discovery					
			Domain Accounts	Modify Registry	Credentials In Files						
					Private Keys						

11

11

9

9

10

1

4

2

3

7

8

5

6

7

Compare multilayered capabilities of LockBit with the latest threat landscape OCD & top 10 ransomware techniques MITRE Engenuity Calculator techniques 1/2

T1189 Drive by Compromise

T1072 Software Deployment Tools

T1133 External Remote Services

T1548.002 Abuse Elevation Control Mechanism

T1562.001 Disable or Modify Tools

T1003.001 OS Credential Dumping

T1082 System Information Discovery

T1046 Network Service Discovery

T1572 Protocol Tunneling

T1567 Exfiltration Over Web Service

1. Phishing - T1566 (73524)



2. Query Registry - T1012 (24030)



3. Native API - T1106 (14691)



4. Modify Registry - T1112 (12800)



5. Brute Force - T1110 (7692)



6. Software Discovery - T1518 (6534)



7. File Deletion - T1070.004 (5416)



8. Hidden Files and Directories -... (4720)



9. Domain Generation Algorithms -... (4481)



10. Credentials from Web Browsers... (4291)



× 1. T1003 - OS Credential Dumping

× 2. T1204 - User Execution

× 3. T1552 - Unsecured Credentials

× 4. T1072 - Software Deployment Tools

× 5. T1557 - Adversary-in-the-Middle

× 6. T1213 - Data from Information Repositories

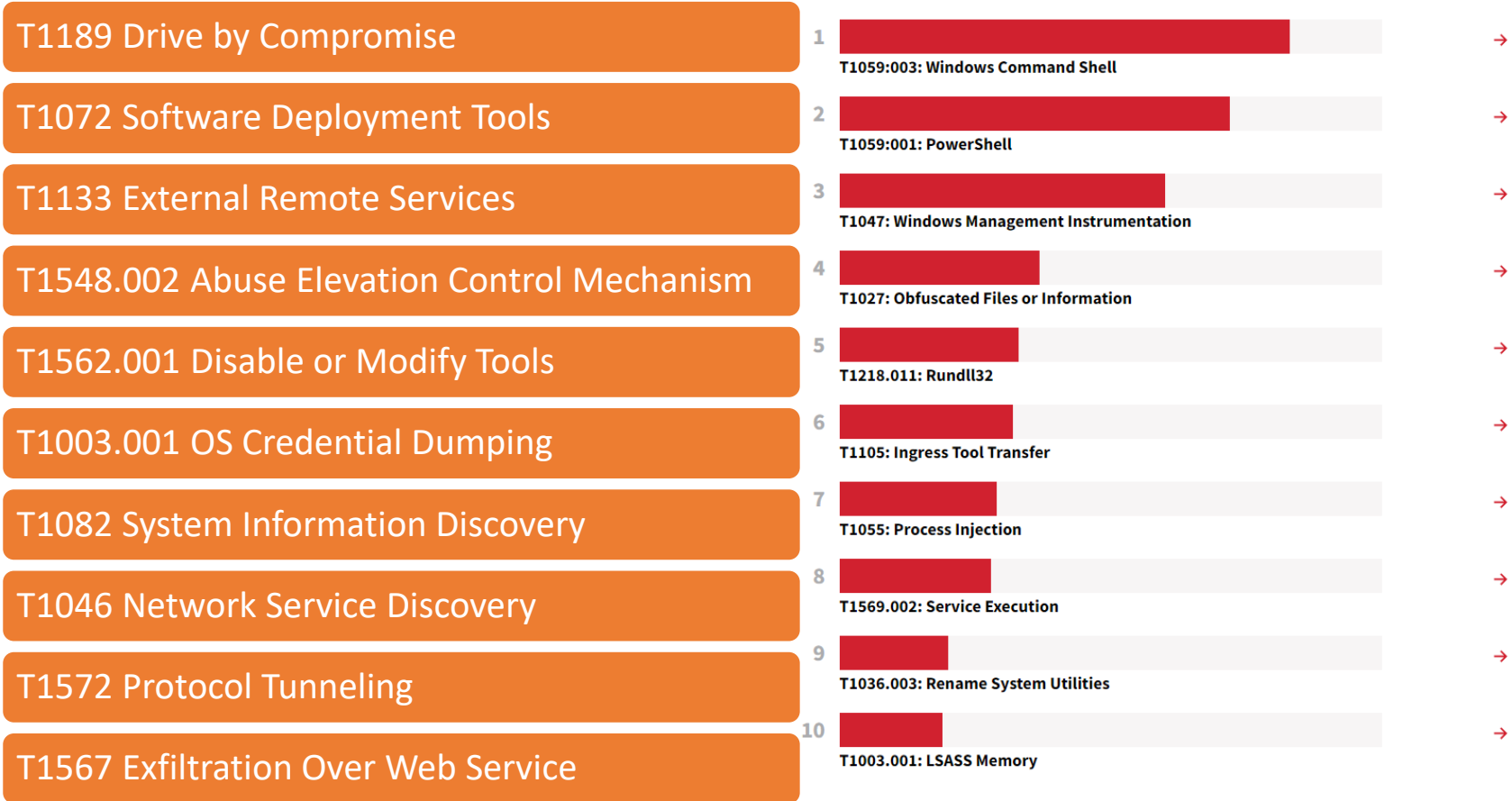
× 7. T1539 - Steal Web Session Cookie

× 8. T1566 - Phishing

× 9. T1176 - Browser Extensions

× 10. T1185 - Browser Session Hijacking

Compare multilayered capabilities of LockBit with the latest threat landscape OCD & top 10 Red Canary, Picus 2/2



Techniques (12)

- Boot or Logon Autostart Execution**
 ID: T1547
 Parent Technique: None
 Tactics: Persistence, Privilege Escalation
- Command and Scripting Interpreter**
 ID: T1059
 Parent Technique: None
 Tactics: Execution
- Disable or Modify Tools**
 ID: T1562.001
 Parent Technique: Impair Defenses
 Tactics: Defense Evasion
- Impair Defenses**
 ID: T1562
 Parent Technique: None
 Tactics: Defense Evasion
- Masquerading**
 ID: T1036
 Parent Technique: None
 Tactics: Defense Evasion
- OS Credential Dumping**
 ID: T1003
 Parent Technique: None
 Tactics: Credential Access
- PowerShell**
 ID: T1059.001
 Parent Technique: Command and Scripting Interpreter
 Tactics: Execution
- Process Injection**
 ID: T1055
 Parent Technique: None
 Tactics: Privilege Escalation, Defense Evasion
- Registry Run Keys / Startup Folder**
 ID: T1547.001
 Parent Technique: Boot or Logon Autostart Execution
 Tactics: Persistence, Privilege Escalation
- Scheduled Task/Job**
 ID: T1053
 Parent Technique: None
 Tactics: Execution, Persistence, Privilege Escalation
- System Information Discovery**
 ID: T1082
 Parent Technique: None
 Tactics: Discovery
- Windows Command Shell**
 ID: T1059.003
 Parent Technique: Command and Scripting Interpreter
 Tactics: Execution

MHHHHHH...WAIT A MINUTE...is the multilayering the wrong approach?

Or is Lock Bit successful because we're hunting wrong ghosts?



How does LockBit use the top layered techniques – CISA AA23-165a 1/2

T1189 Drive by Compromise

T1072 Software Deployment Tools

T1133 External Remote Services

T1548.002 Abuse Elevation Control Mechanism

T1562.001 Disable or Modify Tools

T1003.001 OS Credential Dumping

T1082 System Information Discovery

T1046 Network Service Discovery

T1572 Protocol Tunneling

T1567 Exfiltration Over Web Service

T1189: LockBit affiliates gain access to a system through a user visiting a website over the normal course of browsing.

T1072: LockBit affiliates may use **Chocolatey**, a command line package manager for Windows

T1133: LockBit affiliates exploit RDP to gain access to victims' networks.

T1548.002: LockBit affiliates may use ucmDccwCOM Method in **UACMe**, a GitHub collection of User Account Control (UAC) bypass techniques.

T1562.001: Terminates antimalware-protected processes.

Bypasses PowerShell execution policy.

Disables Microsoft Defender.

Terminates and removes EDR software.

Terminates and circumvents EDR processes and services.

How does LockBit use the top layered techniques – CISA AA23-165a 2/2

T1189 Drive by Compromise

T1072 Software Deployment Tools

T1133 External Remote Services

T1548.002 Abuse Elevation Control Mechanism

T1562.001 Disable or Modify Tools

T1003.001 OS Credential Dumping

T1082 System Information Discovery

T1046 Network Service Discovery

T1572 Protocol Tunneling

T1567 Exfiltration Over Web Service

T1003.001: Obtains credentials by dumping the contents of Local Security Authority Subsystem Service (LSASS).

T1082: Performs numerous security-oriented checks to enumerate system information with the software **Seatbelt**

LockBit affiliates will enumerate system information to include hostname, host configuration, domain information, local drive configuration, remote shares, and mounted external storage devices.

T1046: Maps a victim's network to identify potential access vectors with the **Advanced Internet Protocol Scanner**

T1572: Enables LockBit affiliate actors to avoid detection with **PuTTY**

T1567: LockBit affiliates use publicly available file sharing services to exfiltrate a target's data with tools like **Rclone, FreeFileSync, MEGA** and exfiltrates it to the **Cloud Storage**

Surprising Results Multilayering LockBits capabilities

- Phishing is NOT THE MOST COMMON Initial Access but **Drive by Compromise**
- **Software Deployment Tools** are more common than PowerShell or WMI

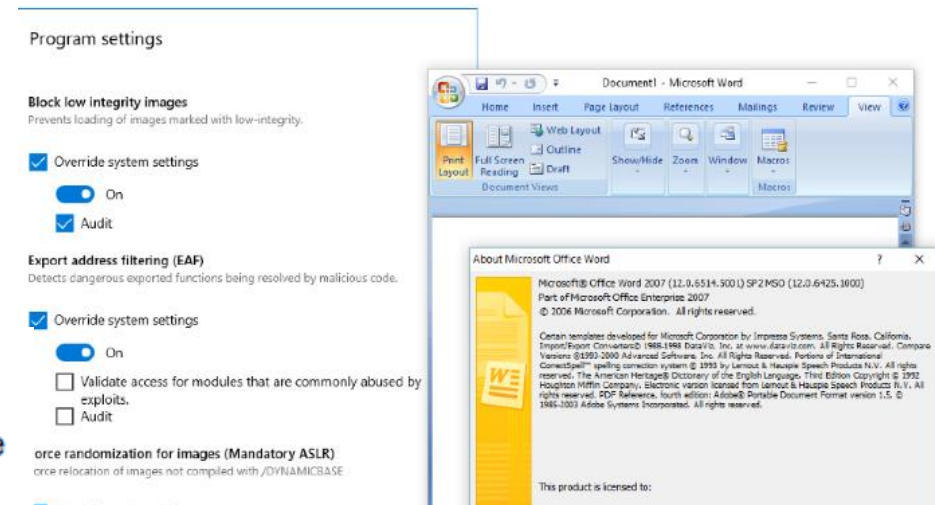
Establish an application allowlist of approved software applications and binaries that are allowed to be executed on a system. This measure prevents unwanted software to be run. Usually, application allowlist software can also be used to define blocklists so that the execution of certain programs can be blocked, for example `cmd.exe` or `PowerShell.exe` [CPG 2.Q].

- **Remote Access Software** is an important **C2** technique for LockBit

Restrict service accounts from remotely accessing other systems. Configure group policy to **Deny log on locally**, **Deny log on through Terminal Services**, and **Deny access to this computer from the network for all service accounts** to limit the ability for compromised service accounts to be used for lateral movement.

- One of the most important choke point would be to **prevent the software deployment** of for e.g **Chocolatey**, **Seabelt**, **UACMe (AWL, ACL)**
- You can prevent the encryption if you **detect service stop** but also **data destruction**

Take care which websites you visit!
Implement Windows Defender Exploit Guard (WDEG) and Enhanced Mitigation Experience Toolkit (EMET)



Security Compliance Toolkit and Baselines

This set of tools allows enterprise security administrators to download, analyze, test, edit and store Microsoft-recommended security configuration baselines for Windows and other Microsoft products, while comparing them against other security configurations.

Important! Selecting a language below will dynamically change the complete page content to that language.

Select language

English

Download

Caldera and Atomic Red Team - Emulation or Simulation Example LockBit

Lockbit Adversary ID: d627004b-d627004b-d627004b-d627004b

Lockbit Ransomware

+ Add Ability + Add Adversary Fact Breakdown Objective: default Change Export Save Profile Delete Profile

defense-evasion 25.93% discovery 7.41% credential-access 14.82% multiple 18.52% lateral-movement 3.71% impact 22.23%

Ordering	Name	Tactic	Technique	Executors	Requires	Unlocks
1	Rundll32 with Ordinal Value	defense-evasion	Signed Binary Proxy Execution: Rundll32	cmd		
2	Windows - Discover domain trusts with nltest	discovery	Domain Trust Discovery	cmd		
3	Basic Permission Groups Discovery Windows (Domain)	discovery	Permission Groups Discovery: Domain Groups	cmd		
4	Cached Credential Dump via Cmdkey	credential-access	OS Credential Dumping: Cached Domain Credentials	cmd		

2 TTPs – CISA/BSI und Umsetzung in das Tabletop

Technique	CISA/BSI description Lockbit	Test
T1560.001 Archive via Utility	LockBit-Affiliates können 7-zip verwenden, um gesammelte Daten vor der Exfiltration zu komprimieren und/oder zu verschlüsseln.	Daten komprimieren und mit Passwort für Exfiltration mit 7zip sperren
T1548.002 Bypass User Account Control	LockBit-Affiliates können die ucmDccwCOM-Methode in UACMe verwenden, einer GitHub-Sammlung von Umgehungstechniken für die Benutzerkontensteuerung (User Account Control, UAC).	WinPwn - UAC-Umgehung der ccmstp-Technik
T1003.005 Cached Domain Credentials	LockBit-Affiliates bewegen sich lateral über Netzwerke hinweg und greifen auf Domänencontroller zu.	Zwischengespeicherter Anmeldedaten-Dump über Cmdkey
T1070.001 Clear Windows Event Logs	Die ausführbare LockBit-Datei löscht die Windows-Ereignisprotokolldateien.	Protokolle löschen
T1486 Data Encrypted for Impact	LockBit 3.0 verschlüsselt Daten auf Zielsystemen, um die Verfügbarkeit von System- und Netzwerkressourcen zu unterbrechen. LockBit-Affiliates können Windows- und Linux-Geräte sowie VMware-Instanzen verschlüsseln.	Daten verschlüsselt mit GPG4Win PureLocker Lösegeldforderung wird simuliert.

infosecn1nja / red-team-scripts Public

<> Code Issues Pull requests Actions Projects Security Insights

Files

main

Go to file

- ASR Rules Bypass.vba
- BYOVD_kill_av_edr.c
- Generate-Mustang-Panda-LNK.p...
- Invoke-AtomicEnterpriseLayer.ps1
- LICENSE
- Lockbit_Ransomware_Atomic_Si...
- README.md
- gen-chm.py
- pluginx.profile

red-team-scripts / Lockbit_Ransomware_Atomic_Simulation.ps1

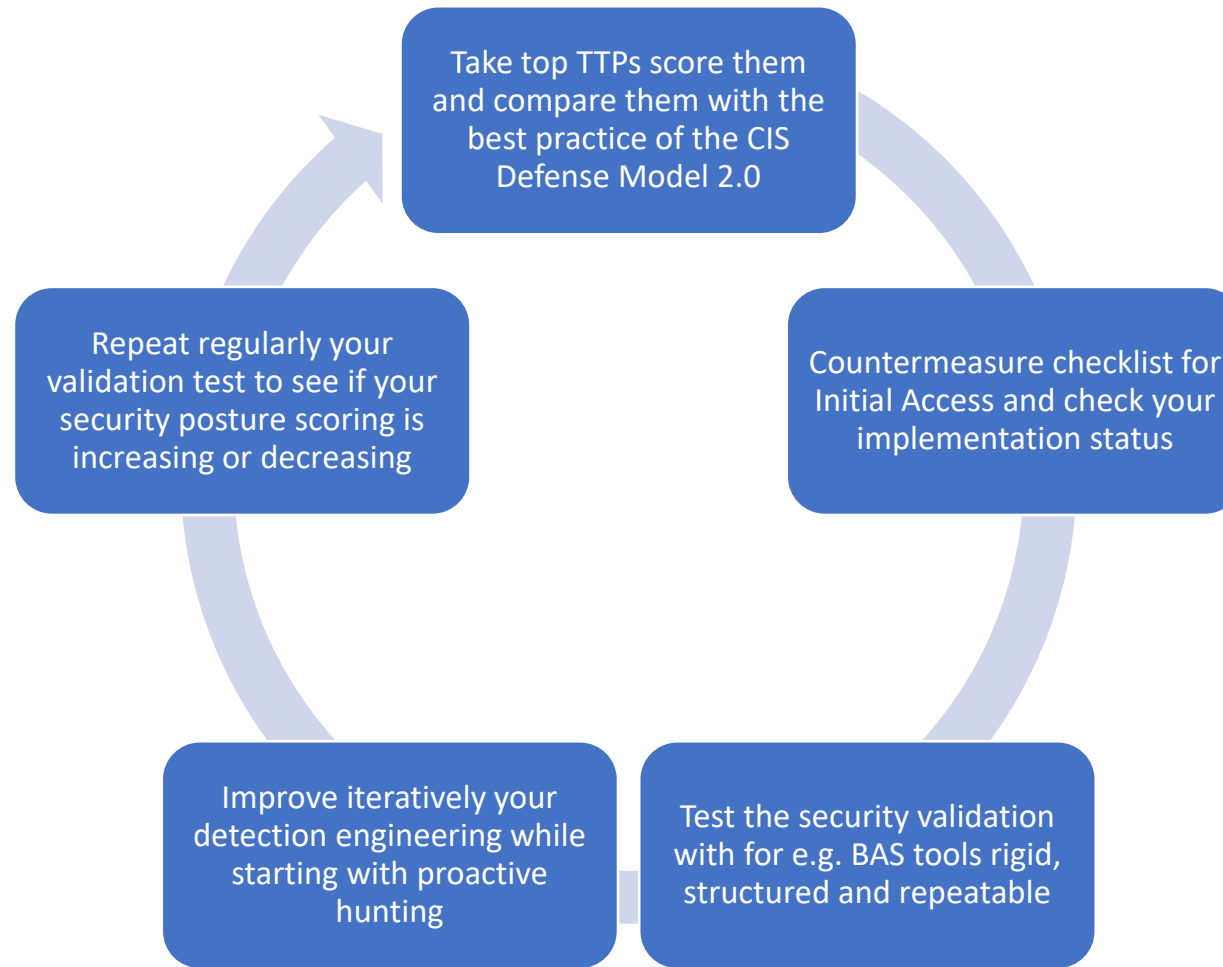
infosecn1nja Update Lockbit_Ransomware_Atomic_Simulation.ps1

Code Blame 129 lines (97 loc) · 4.65 KB

```

1 # Lockbit Ransomware Atomic Simulation
2 # Author : Rahmat Nurfauzi (@infosecn1nja)
3 # Date : 16/05/2023
4 # Simulate Lockbit Ransomware tactics, techniques, and procedures (TTP) with atomic red team to validate security controls
5 #
6 # References
7 # https://www.mandiant.com/resources/blog/unc2165-shifts-to-evade-sanctions
8 # https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-075a
9 # https://research.nccgroup.com/2022/08/19/back-in-black-unlocking-a-lockbit-3-0-ransomware-attack/
10 # https://unit42.paloaltonetworks.com/lockbit-2-ransomware/
11 #
12
13 Set-ExecutionPolicy Bypass -Force
    
```

Threat Informed Defense - Measures example LockBit



Initial Access- LockBit Ransomware PREVENTION (1/4)

The following actions are general recommendations and counter measures for LockBit CISA Alert AA23_165A

Counter Measure	Description	Implementation Status
Consider implementing sandboxed browsers	Sandboxed browsers can protect systems from malware originating from web browsing. Sandboxed browsers isolate the host machine from malicious code.	
Require all accounts with password logins	with password logins (e.g., service account, admin accounts, and domain admin accounts) to comply with NIST standards for developing and managing password policies [CPG 2.L].	
Implement filters at the email gateway	to filter out emails with known malicious indicators, such as known malicious subject lines, and block suspicious IP addresses at the firewall [CPG 2.M].	
Install a web application firewall	and configure with appropriate rules to protect enterprise assets.	
Segment networks	to prevent the spread of ransomware. Network segmentation can help prevent the spread of ransomware by controlling traffic flows between—and access to— various subnetworks and by restricting adversary lateral movement.	

Initial Access- LockBit Ransomware PREVENTION (2/4)

The following actions are general recommendations and counter measures for LockBit CISA Alert AA23_165A

Counter Measure	Description	Implementation Status
Follow the least-privilege best practice	by requiring administrators to use administrative accounts for managing systems and use simple user accounts for non-administrative tasks [CPG 2.E].	
Enforce the management of and audit user accounts with administrative privileges.	Configure access controls according to the principle of least privilege [CPG 2.E].	
Implement time-based access for accounts set at the admin level and higher	For example, the Just-in-Time (JIT) access method provisions privileged access when needed and can support enforcement of the principle of least privilege (as well as the Zero Trust model). This is a process where a network-wide policy is set in place to automatically disable admin accounts at the Active Directory level when the account is not in direct need. Individual users may submit their requests through an automated process that grants them access to a specified system for a set timeframe when they need to support the completion of a certain task.	
Keep all operating systems, software, and firmware up to date	Timely patching is one of the most efficient and cost-effective steps an organization can take to minimize its exposure to cybersecurity threats.	

Initial Access- LockBit Ransomware PREVENTION (3/4)

The following actions are general recommendations and counter measures for LockBit CISA Alert AA23_165A

Counter Measure	Description	Implementation Status
Restrict service accounts from remotely accessing other systems.	Configure group policy to Deny log on locally, Deny log on through Terminal Services, and Deny access to this computer from the network for all service accounts to limit the ability for compromised service accounts to be used for lateral movement.	
Block direct internet access for administration interfaces	(e.g., application protocol interface (API)) and for remote access.	
Require phishing-resistant multifactor authentication (MFA)	for all services to the extent possible, particularly for webmail, virtual private networks, and privileged accounts that access critical systems [CPG 2.H].	
Consolidate, monitor, and defend internet gateways.		
Install, regularly update, and enable real-time detection for antivirus software	on all hosts.	
Raise awareness for phishing threats in your organization	Phishing is one of the primary infection vectors in ransomware campaigns, and all employees should receive practical training on the risks associated with the regular use of email.	

Initial Access- LockBit Ransomware PREVENTION (4/4)

The following actions are general recommendations and counter measures for LockBit CISA Alert AA23_165A

Counter Measure	Description	Implementation Status
Consider adding an external email warning banner	for emails sent to or received from outside of your organization [CPG 2.M].	
Review internet-facing services and disable any services that are no longer a business requirement	to be exposed or restrict access to only those users with an explicit requirement to access services, such as SSL, VPN, or RDP. If internet-facing services must be used, control access by only allowing access from an admin IP range [CPG 2.X].	
Review domain controllers, servers, workstations, and active directories	for new and/or unrecognized accounts.	
Regularly verify the security level of the Active Directory domain	by checking for misconfigurations.	

Summary – Taking action on your profile

What have
we learned?
WHERE TO
START

- How to use Threat Informed Defense enterprise-centric for your cyber threat profile
- Operational Effectiveness with CTI Blueprint & the ransomware ecosystem graph
- What is multilayering and how can we avoid analytical errors
- How to extract and map a CTI Reports with the D3FEND example FIN12 for Healthcare CERT France
- Mapping and creating a Cyber Threat Profile for FIN12 – Scoring TTPs
- RMM Tools threat actors use against the Healthcare
- Threat Hunting with PEAK – T1219 with AnyDesk
- Detection Engineering with the MITRE CTID approach Summiting the pyramid
- Use Case LockBit – top TTPs, emulation and measures, recommendations



**2023
FIRST
Cyber Threat
Intelligence
Conference**

**Berlin, Germany
November 6-8, 2023**

Resources



Relevant Existing Threat Profiling Frameworks & Methodologies

- Enterprise Threat Model Technical Report: <https://www.mitre.org/sites/default/files/2021-11/pr-18-1613-ngci-enterprise-threat-model-technical-report.pdf>
- Process for Attack Simulation and Threat Analysis (PASTA): <https://versprite.com/blog/what-is-pasta-threat-modeling/>
- Guide for Conducting Risk Assessments: <https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-30r1.pdf>
- STRIDE: [https://learn.microsoft.com/en-us/previous-versions/commerce-server/ee823878\(v=cs.20\)](https://learn.microsoft.com/en-us/previous-versions/commerce-server/ee823878(v=cs.20))
- DREAD: <https://adam.shostack.org/modsec08/Shostack-ModSec08-Experiences-Threat-Modeling-At-Microsoft.pdf>
- LINDDUN: <https://people.cs.kuleuven.be/~kim.wuyts/LINDDUN/LINDDUN.pdf>
- Factor Analysis of Risk Information (FAIR™): <https://www.fairinstitute.org/what-is-fair>
- Trike: <http://www.octotrike.org/>
- Visual, Agile and Simple Threat (VAST): <https://threatmodeler.com/threat-modeling-methodologies-vast/>
- Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE®): <https://resources.sei.cmu.edu/library/asset-view.cfm?assetID=8419>

Threat Informed Defense & Holistic Threat Modeling

- <https://www.orange cyberdefense.com/de/resources/whitepaper-holistic-threat-modeling>
- <https://medium.com/@simone.kraus>
- <https://center-for-threat-informed-defense.github.io/attack-flow/ui/>
- <https://www.tidalcyber.com/blog>
- <https://github.com/center-for-threat-informed-defense/cti-blueprints/wiki>
- https://github.com/SigmaHQ/sigma/blob/60b8e9b70ffaf49b17abfcae4a0ea08f2da7f71/rules/windows/dns_query/dns_query_win_remote_access_software_domains.yml
- <https://center-for-threat-informed-defense.github.io/summitting-the-pyramid/scoringanalytic/>
- https://www.cisa.gov/sites/default/files/2023-08/CSRB_Lapsus%24_508c.pdf
- <https://github.com/redcanaryco/atomic-red-team/blob/master/atomics/T1219/T1219.md#atomic-test-2---anydesk-files-detected-test-on-windows>
- https://www.cisa.gov/sites/default/files/2023-03/aa23-061a-stopransomware-royal-ransomware_0.pdf
- https://jsac.jpCERT.or.jp/archive/2023/pdf/JSAC2023_1_1_yamashige-nakatani-tanaka_en.pdf
- https://www.cisa.gov/sites/default/files/2023-06/aa23-165a_understanding_TA_LockBit_0.pdf



2023
FIRST
**Cyber Threat
Intelligence
Conference**

Berlin, Germany
November 6-8, 2023

Thank you

