

The Cisco Live! logo, featuring the word "CISCO" in a dark blue, sans-serif font, followed by "Live!" in a dark blue, cursive script font.

CISCO *Live!*

The text "Let's go" in a large, dark blue, sans-serif font, positioned to the left of a bright white sunburst graphic that radiates across the right side of the image.

Let's go

#CiscoLiveAPJC



The bridge to possible

Evaluating and Improving Defenses with MITRE ATT&CK

A free and open approach!

Tim Snow, Cyber Architect, APJC
@TimSnowIT
BRKSEC-2227

CISCO *Live!*

#CiscoLiveAPJC

Agenda

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

Cisco Webex App

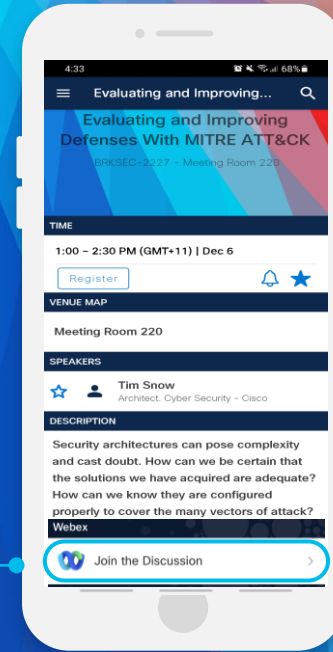
Questions?

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 December 22, 2023.



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

Your Speaker



- IT Architect with domain experience in Enterprise Networks (Campus, WAN, DC), Security and Applications
- 20+ Year CCIE
- 18 Years at Cisco in multiple roles

Prior to Cisco

- Comp. Sci major – Michigan
- Developer
- TAC L3 and SecOps



About Me



- Canadian, Husband, Father
- Tinkerer – IOT systems
(automate the things that don't need to be automated)
- 3D Printing and Robotics
As a way to show my kids tech
- Retro Arcade gaming –
growing up in the 80's
- Lifelong beginner at golf

What is this session about?

Background:

- Security through compliance == complex and disjointed
- Checking boxes rarely counters threats

Process:

- Using 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!

- 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



For Your
Reference

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

Time for a little game. Can you guess?

1. Enterprise-class business and service provider
 - Full-service and turn-key
 - Considered a technical and strategy leader
2. Multi-national, multi-million-dollar org based in Eastern Europe
3. Specializes in Full-Service Data Encryption and Transport
 - Provides or outsources entire chain for customers, both commercial and government
4. Over 125k server environment, heavily “invested” in healthcare
 - Developed Conti, Ryuk, Trickbot

Any guesses???

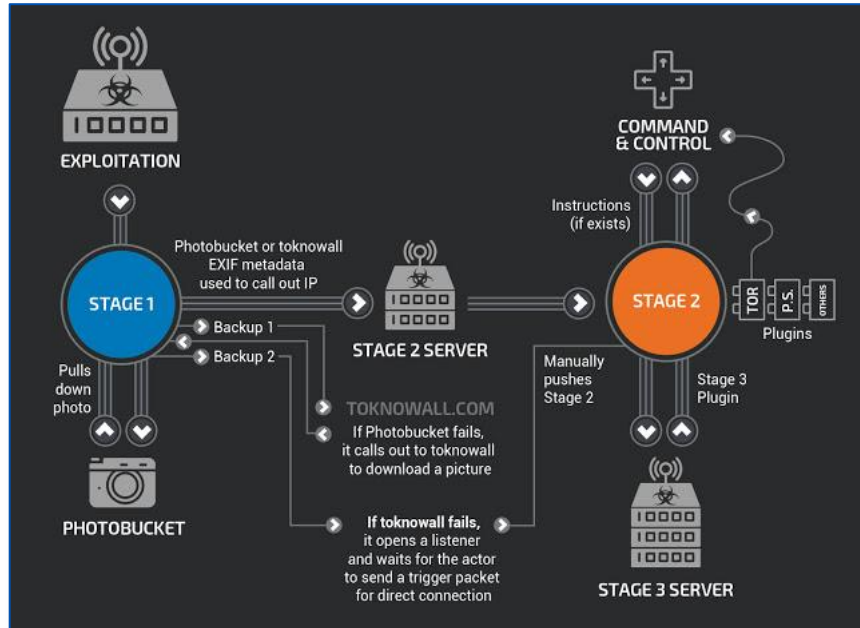
Wizard Spider (a.k.a. UNC1878, Grim Spider, TempMisMaster, etc.

(<https://attack.mitre.org/groups/G0102/>)

(<https://www.theregister.com/2022/05/18/wizard-spider-ransomware-conti/>)

Should <insert APT here> scare you?

Exciting stuff makes the news...Effective practices and remediations 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 - cpycat 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

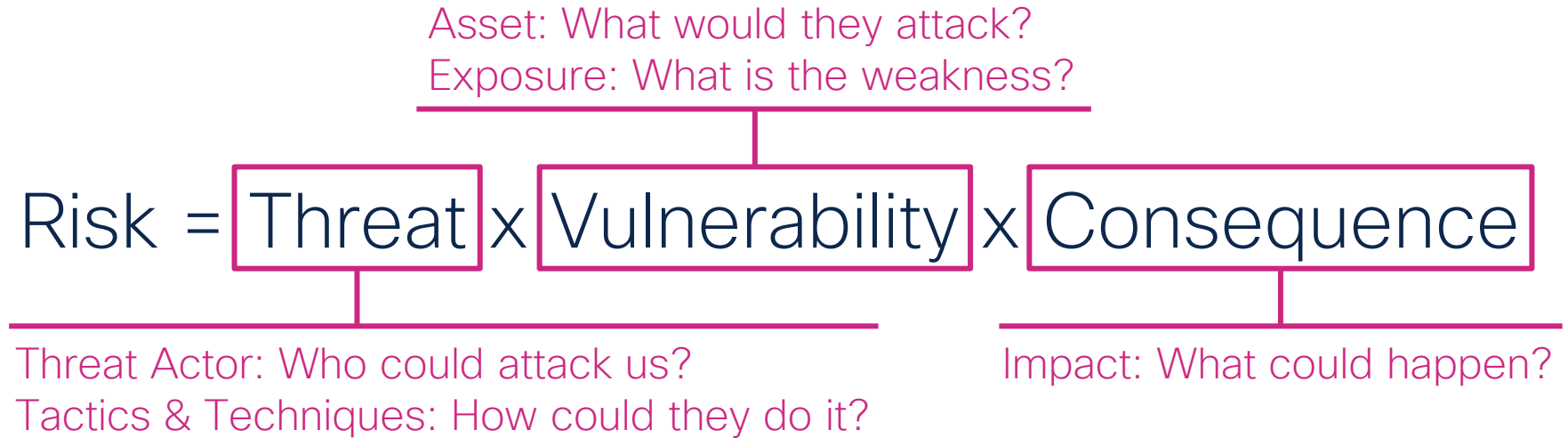
<https://blog.talosintelligence.com/2018/05/VPNFilter.html>

Don't chase other peoples' boogiemen

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

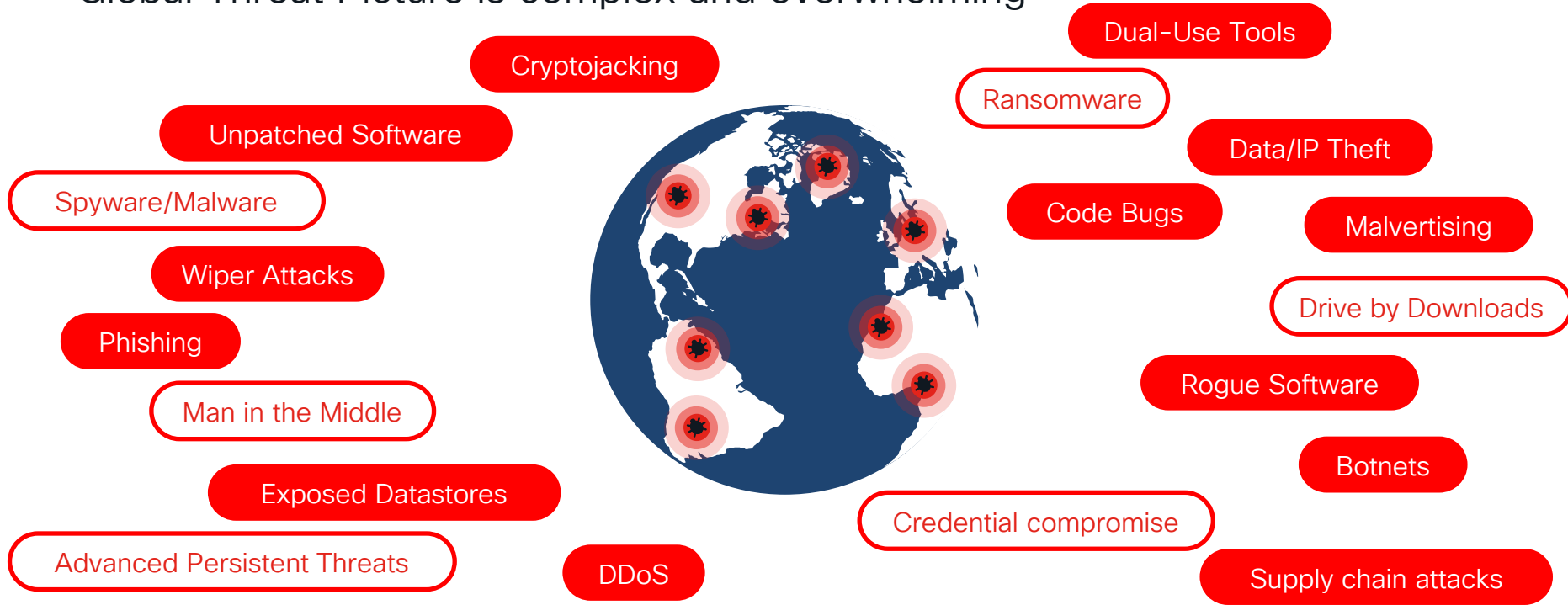
- Likely tactics?
 - Everyone exposed to ransomware, phishing: the devil is in the details
 - Ex. Unlikely to see Quantum insert exploits on politically insignificant sites, Magecart in non-commerce, etc.
- Likely adversaries?
 - Threat actors usually concentrate on certain vertical/geography
 - Could be implicated by political affinity, downstream customers (e.g. ISPs for government, banks serving sector)
 - “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

Cybersecurity Risk Formula



But where do we start?

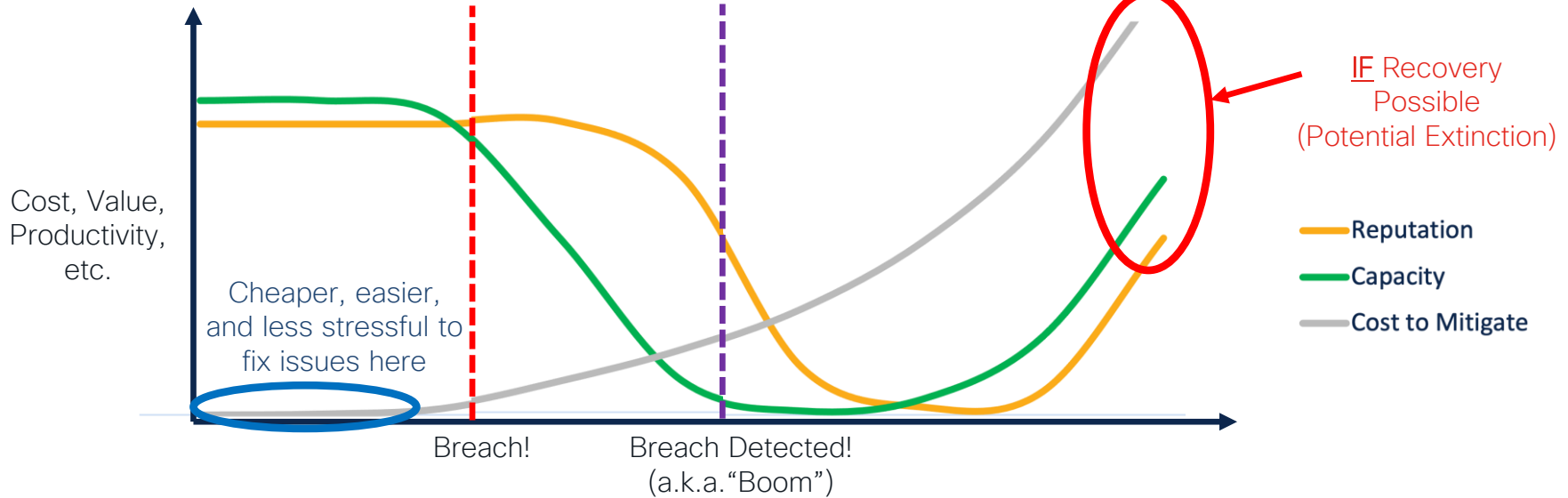
Global Threat Picture is complex and overwhelming



We need to narrow our focus!

Earlier Detection == Cheaper Mitigation

Predicting, deterring, and early detection reduce cost and workload



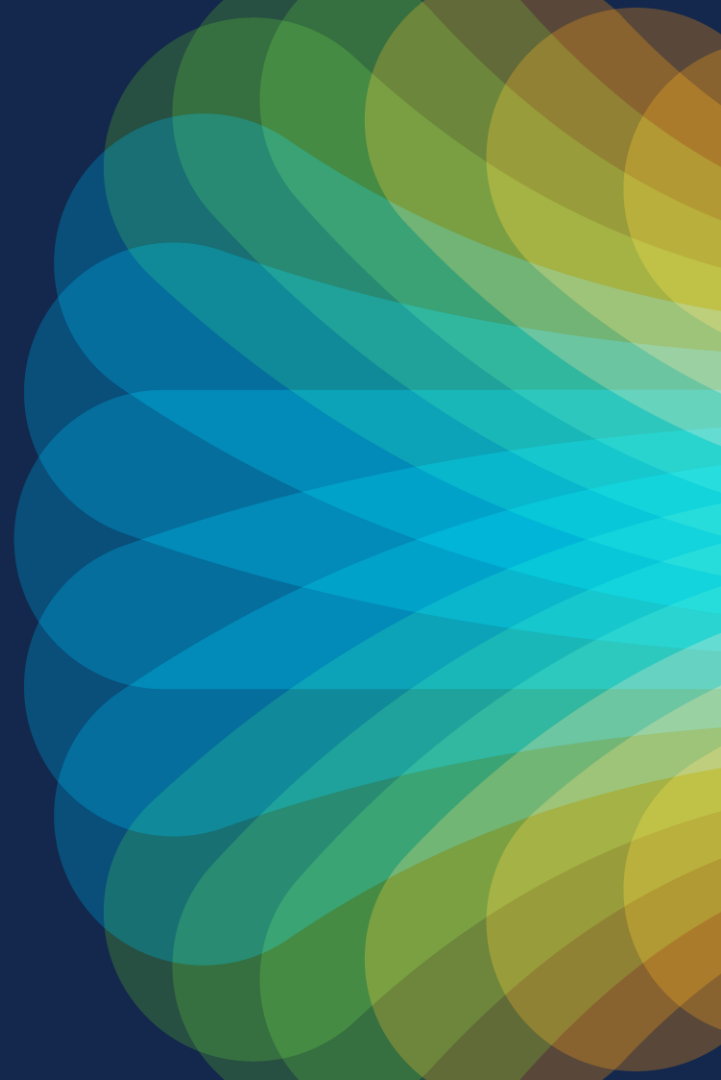
- Better to be “left of boom” – a period when you still have a chance to prepare and avert a crisis
- Earlier & effective controls = better performance, lower pressure/cost, preserved reputation
- CTI relieves pressure! Not just for Global corporations/governments...we all need it!

“If you know the enemy
and **KNOW YOURSELF**,
you need not fear
the result of a
hundred battles.”

~ Sun Tzu



MITRE ATT&CK Crash Course



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

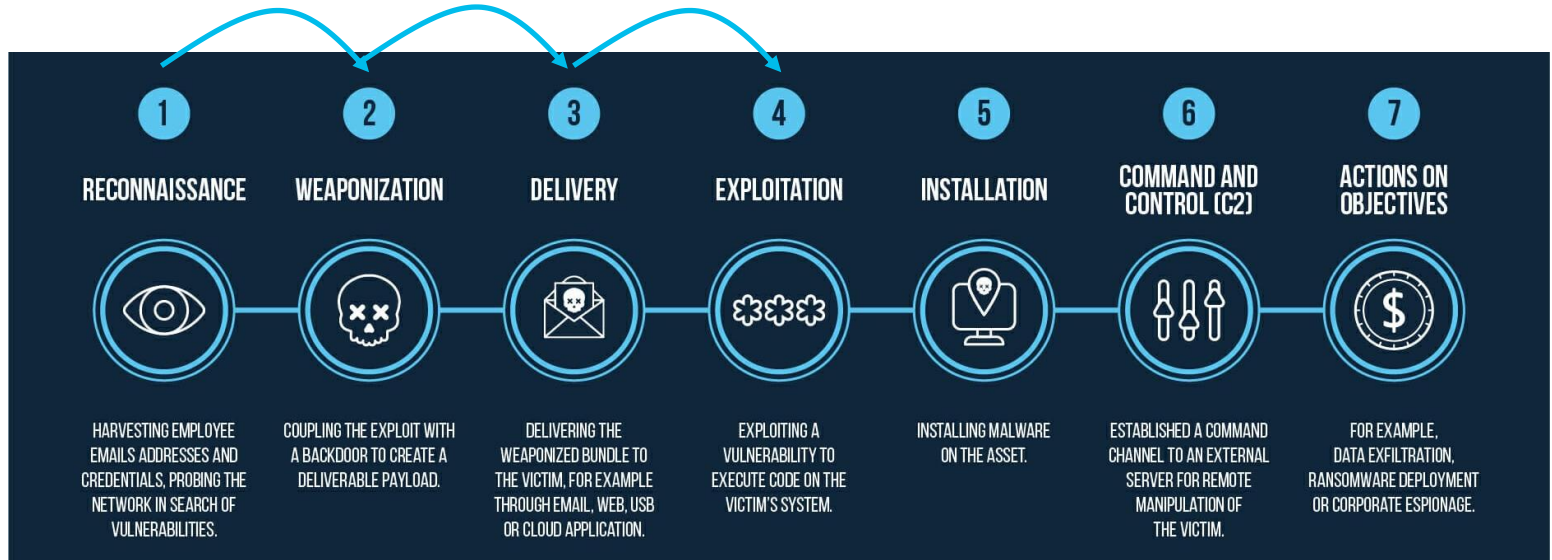
- Who is MITRE Corporation?
 - Not-for-profit, US company with multiple federally funded R&D centers (FFRDCs)
 - Public-private partnerships in many areas, including cybersecurity
 - Same folks who brought us CVE database/list
- What is ATT&CK
 - **A**dversarial **T**tactics, **T**echniques, and **C**ommon **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.

MITRE

ATT&CK™
Adversarial Tactics, Techniques
& Common Knowledge

Visualizing the kill chain

CYBER KILL CHAIN VS. MITRE ATT&CK



Cyber Kill Chain focuses on the steps of a cyberattack, whereas MITRE ATT&CK focuses on the tactics and techniques employed by cyber attackers

MITRE ATT&CK – TTP's

CYBER KILL CHAIN VS. MITRE ATT&CK



What is a Tactic?

CYBER KILL CHAIN VS. MITRE ATT&CK



Tactics represent the "why" of an ATT&CK technique.

It is the adversary's **tactical goal**: the reason for performing an action.

For 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](#)

What is a Technique?

CYBER KILL CHAIN VS. MITRE ATT&CK



Techniques represent 'how' an adversary achieves a tactical goal by performing an action.

For example, an adversary may dump credentials to achieve credential access.

There are currently 201 Enterprise Techniques

T1003 – Credential Dumping
T1040 – Network Sniffing
T1056 – Input Capture
T1110 – Brute Force

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.

Sub-Techniques

CYBER KILL CHAIN VS. MITRE ATT&CK



Sub-techniques are a more specific description of the adversarial behavior used to achieve a goal. They describe behavior at a lower level than a technique.

For example, an adversary may dump credentials by accessing the Local Security Authority (LSA) Secrets

T1003 - Credential Dumping

001 LSAAS Memory

....

004 LSA Secrets

....

008 /etc/passwd

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]

What is a Procedure?

Procedures are the specific **implementation** the adversary uses for techniques or sub-techniques.

For example, a procedure could be an adversary using a sysinternals tool to dump the local system policy, password hashes, etc and then run mimikatz to read the memory dump.

Procedures are categorized in ATT&CK as the observed “**in the wild**” use of techniques in the "Procedure Examples" section of technique pages

```
Windows PowerShell
Copyright (C) 2009 Microsoft Corporation. All rights reserved.

PS C:\Windows\system32> cd C:\Users\raj\Desktop
PS C:\Users\raj\Desktop> .\minikatz.exe

##### minikatz 2.2.0 (x64) #18362 Mar  8 2020 18:30:37
## ^ ##  "A La Vie, A L'Amour" - (oe.eo)
## < > ##  /*** Benjamin DELPY 'gentilkiwi' ( benjamin@gentilkiwi.com )
##  < > ##  /****> http://blog.gentilkiwi.com/minikatz
'## o ##'  Vincent LE TOUX ( vincent.letoux@gmail.com )
'#####'  > http://pingcastle.com / http://mysmartlogon.com   ***/

minikatz # privilege::debug
Privilege '20' OK

minikatz #
minikatz # sekurlsa::minidump C:\Users\raj\Downloads\Procdump\mem.dmp
Switch to MINIDUMP : 'C:\Users\raj\Downloads\Procdump\mem.dmp'

minikatz # sekurlsa::logonpasswords
Opening : 'C:\Users\raj\Downloads\Procdump\mem.dmp' file for minidump...

Authentication Id : 0 ; 334696 (00000000:00051b68)
Session           : Interactive from 1
User Name         : raj
Domain           : WIN-NFMRD371TKD
Logon Server      : WIN-NFMRD371TKD
Logon Time        : 4/2/2020 9:11:54 PM
SID              : S-1-5-21-3008983562-280188460-17735145-1000

New
[00000003] Primary
* Username : raj
* Domain   : WIN-NFMRD371TKD
* LM       : b757bf5c0d87722faad3b435b51404ee
* NtLm     : 7ce21f17c0aee7fb9ceba532d0546ad6
* SHA1     : 139f69c93c042496a8e758ec5930662c6cccafb

tspkg :
* Username : raj
* Domain   : WIN-NFMRD371TKD
* Password : 1234

wdigest :
* Username : raj
* Domain   : WIN-NFMRD371TKD
* Password : 1234

kerberos :
* Username : raj
* Domain   : WIN-NFMRD371TKD
* Password : 1234

ssp :
crednan :
[00000000]
* Username : pentest
* Domain   : 192.168.1.111
* Password : 123
```

The Smash and Grab



https://media.yourobserver.com/img/photos/2022/04/28/photo-1-9672-20110110173546_11100.jpg?31a214c4405663fd4bc7e33e8c8cedcc07d61559
https://as1.ftcdn.net/v2/img/02/77/16/52/1000_F_277165295_Qlw1T1YPPlu53uMhIi3kIBb9ZFxFPePf.jpg
<https://content.api.news/v3/images/bin/02143ab9e54077b712accad3fa3f612b?width=320>

The Heist



<https://www.theguardian.com/world/2017/oct/04/brazil-bank-robbery-sao-paulo-tunnel>

eastnews.co.ug/blow-by-blow-account-of-how-police-tracked-nwsc-dressed-robbers&server=hkg1&prefs=&tagging=&nref

<https://www.observebd.com/news.php?id=416493>

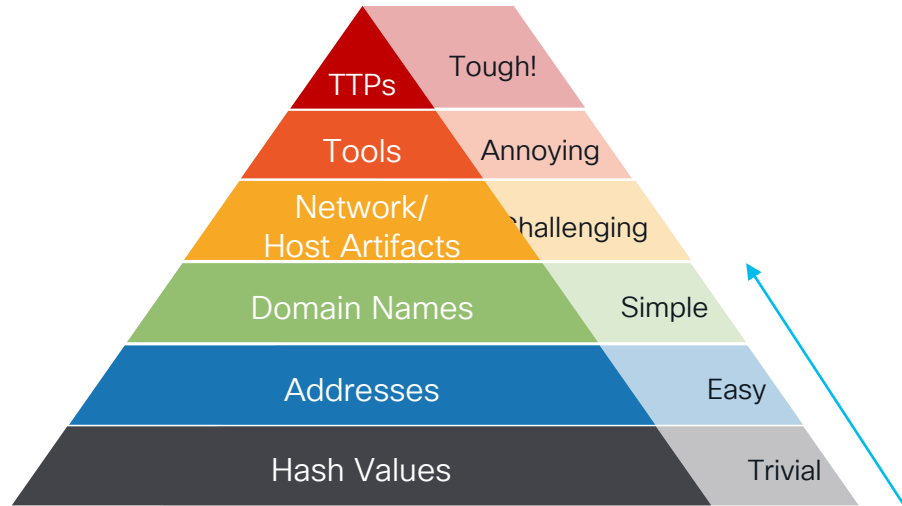
What MITRE ATT&CK is NOT!

- A Compliance Framework
- An Architecture
- A miracle cure or all-encompassing guide
- A guarantee of Efficacy or Success
 - Coverages is not always indicative of detections
 - Not all Techniques or Sub-techniques are equal in impact
 - Same technique may have vastly different risk depending on factors such as environment, host, threat etc.
- Lastly – It is not Exhaustive.
 - ATT&CK draws on public knowledge
 - Many TTPs are not yet public or discovered



ATT&CK changes our focus

Concentrate on the root of the problem to achieve security enlightenment



From David Biacco:

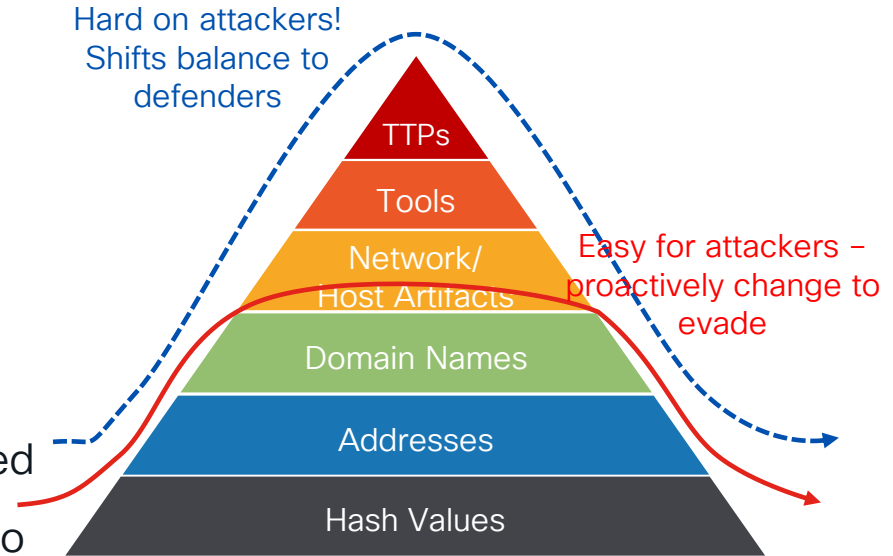
<https://www.eventtracker.com/blog/2015/february/the-pyramid-of-pain/>

- 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
- 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

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Active Scanning	Acquire Infrastructure	Drive-by Compromise	Command and Control	Account Manipulation	Abuse Privilege	Abuse Privilege	Abuse Privilege	Account Discovery	Account Discovery	Account Discovery	Account Discovery	Account Discovery	Account Discovery
...	...	...	...	...	...	...	...	...	...	...	...	...	...

- 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



14 Tactics

201 Techniques &
424 Sub-techniques

Employed By

143 Groups

Implemented Thru

760 Software
Applications

43 Mitigations

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

Key platforms:

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

Enterprise | Mobile | ICS

The 5 W's plus an H of Threat Modeling

My English teacher would be so proud...

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

Understand your ATT&CK Model Relationships

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

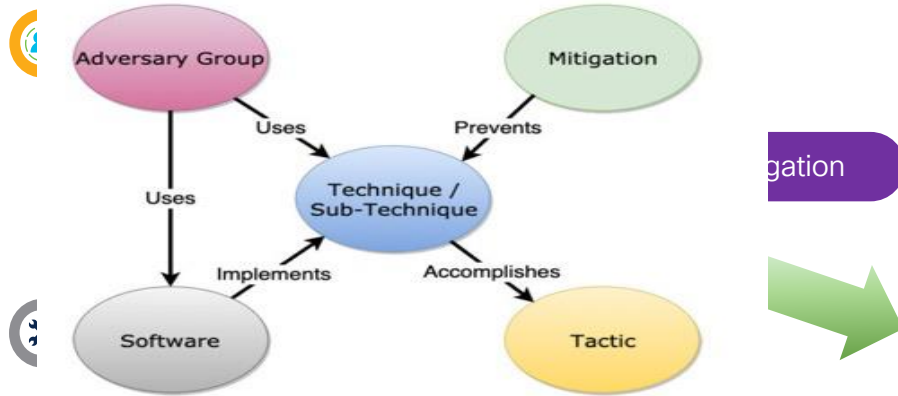
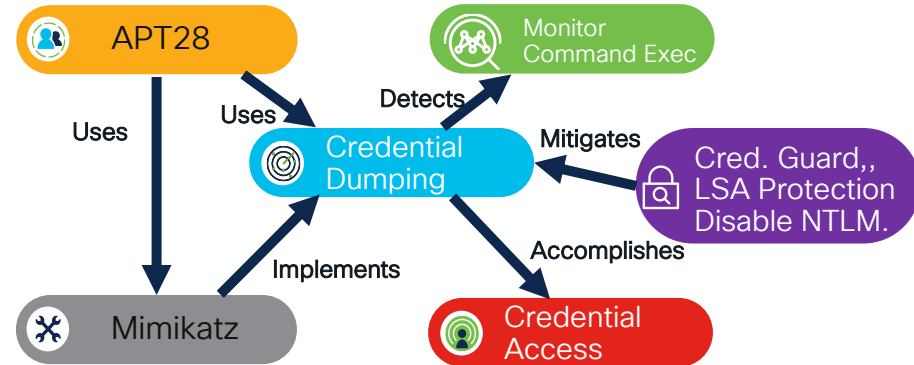


Figure 3. ATT&CK Model Relationships

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

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



Before we start – let's understand our environment

We're a 30k employee healthcare network, based in APJC

- 6 hospital campuses, 50 out-patient clinics & urgent care facilities.
- Well architected infrastructure, but due for refresh
- Windows endpoints, Windows/Linux servers 80/20, with shift to Cloud (~30% of workloads and slowly increasing)
- Staffing: 15 FTEs dedicated to security (CISO, 3 Managers, 2 architects, 9 Engineer/Analysts)
- Training and operating – not enough time!
- ~50 vendors in or adjacent to Security

Navigator Demo

Know your Enemy



MITRE ATT&CK®

attack.mitre.org

MITRE | ATT&CK®

Matrices ▼Tactics ▼Techniques ▼Defenses ▼CTI ▼Resources ▼BenefactorsBlog ↗

Search 🔍

ATT&CK v14 has been released! Check out the [blog post](#) or [release notes](#) for more information.

Getting StartedTake a TourContributeBlog ↗FAQRandom Page ▼

MITRE ATT&CK® is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community.

With the creation of ATT&CK, MITRE is fulfilling its mission to solve problems for a safer world — by bringing communities together to develop more effective cybersecurity. ATT&CK is open and available to any person or organization for use at no charge.

ATT&CK Matrix for Enterprise

layout: flat ▼show sub-techniqueshide sub-techniques

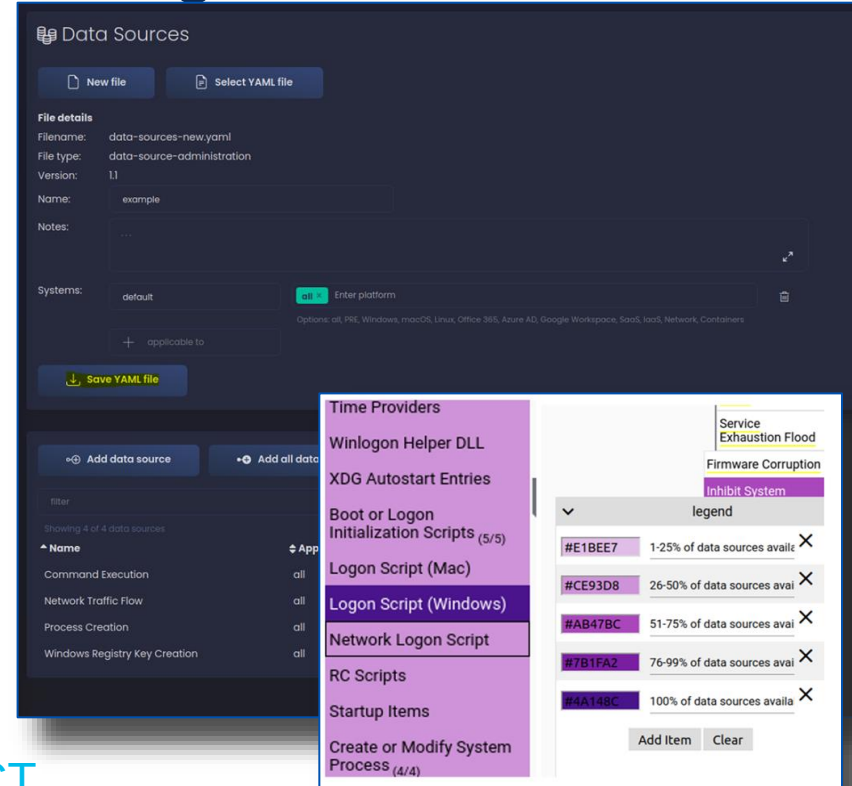
Reconnaissance 10 techniques	Resource Development 8 techniques	Initial Access 10 techniques	Execution 14 techniques	Persistence 20 techniques	Privilege Escalation 14 techniques	Defense Evasion 43 techniques	Credential Access 17 techniques	Discovery 32 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 17 techniques	Exfiltration 9 techniques	Impact 14 techniques
Active Scanning (3) Gather Victim Host Information (4) Gather Victim Identity Information (3) Gather Victim Network Information (4) Gather Victim Org Information (4) Phishing for Information (4) Search Closed Sources (2) Search Open Technical Databases (5) Search Open Websites/Domains (3) Search Victim-Owned Websites	Acquire Access Acquire Infrastructure (8) Compromise Accounts (3) Compromise Infrastructure (7) Develop Capabilities (4) Establish Accounts (3) Obtain Capabilities (6) Stage Capabilities (6) Trusted Relationship Valid Accounts (4)	Drive-by Compromise Exploit Public-Facing Application External Remote Services Hardware Additions Phishing (4) Replication Through Removable Media Supply Chain Compromise (3) Trusted Relationship Valid Accounts (4)	Cloud Administration Command Command and Scripting Interpreter (9) Container Administration Command Deploy Container Exploitation for Client Execution Inter-Process Communication (3) Native API Scheduled Task/Job (5) Serverless Execution Shared Modules Software Deployment Tools System Services (2) User Execution (3) Windows Management Instrumentation	Account Manipulation (6) BITS Jobs Boot or Logon Autostart Execution (14) Boot or Logon Initialization Scripts (6) Browser Extensions Compromise Client Software Binary Create Account (3) Create or Modify System Process (4) Event Triggered Execution (16) External Remote Services Hijack Execution Flow (12) Implant Internal Image Modify Authentication	Abuse Elevation Control Mechanism (5) Access Token Manipulation (3) Access Token Manipulation (6) BITS Jobs Build Image on Host Debugger Evasion Deobfuscate/Decode Files or Information Deploy Container Direct Volume Access Domain Policy Modification (2) Execution Guardrails (1) File and Directory Permissions Modification (2) Hide Artifacts (11) Hijack Execution Flow (12) Process Injection (12)	Abuse Elevation Control Mechanism (5) Access Token Manipulation (3) BITS Jobs Build Image on Host Debugger Evasion Deobfuscate/Decode Files or Information Deploy Container Direct Volume Access Domain Policy Modification (2) Execution Guardrails (1) File and Directory Permissions Modification (2) Hide Artifacts (11) Hijack Execution Flow (12) Impair Defenses (11) Steal Application	Adversary-in-the-Middle (2) Brute Force (4) Credentials from Password Stores (6) Exploitation for Credential Access Forced Authentication Forge Web Credentials (2) Input Capture (4) Multi-Factor Authentication Interception Multi-Factor Authentication Request Generation Network Sniffing OS Credential Dumping (8) Steal Application	Account Discovery (4) Application Window Discovery Browser Information Discovery Cloud Infrastructure Discovery Cloud Service Dashboard Cloud Service Discovery Cloud Storage Object Discovery Container and Resource Discovery Debugger Evasion Device Driver Discovery Domain Trust Discovery File and Directory Discovery Group Policy Discovery Log Enumeration Network Service Discovery Network Share Discovery Network Sniffing	Exploitation of Remote Services Internal Spearphishing Lateral Tool Transfer Remote Service Session Hijacking (2) Remote Services (6) Replication Through Removable Media Software Deployment Tools Taint Shared Content Use Alternate Authentication Material (4)	Adversary-in-the-Middle (3) Archive Collected Data (3) Audio Capture Automated Collection Browser Session Hijacking Clipboard Data Data from Cloud Storage Data from Configuration Repository (2) Data from Information Repositories (3) Data from Local System Data from Network Shared Drive Data from Removable Media Data Staged (2)	Application Layer Protocol (4) Communication Through Removable Media Content Injection Data Encoding (2) Data Obfuscation (3) Dynamic Resolution (3) Encrypted Channel (2) Fallback Channels Ingress Tool Transfer Non-Application Layer Protocol Non-Standard Port Protocol Tunneling Proxy (4) Remote Access Software	Automated Exfiltration (1) Data Transfer Size Limits Exfiltration Over Alternative Protocol (3) Exfiltration Over C2 Channel Exfiltration Over Other Network Medium (1) Exfiltration Over Physical Medium (1) Exfiltration Over Web Service (4) Scheduled Transfer Transfer Data to Cloud Account	Account Access Removal Data Destruction Data Encrypted for Impact Data Manipulation (3) Defacement (2) Disk Wipe (2) Endpoint Denial of Service (4) Financial Theft Firmware Corruption Inhibit System Recovery Network Denial of Service (2) Resource Hijacking Service Stop System Shutdown/Reboot

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>



DeTT&CT Demo

Demo brought to you by



Mike McPhee
Architect. Cisco

Raiders of the lost ARP

<https://raidersofthelostarp.tech/>



Best Friends: What makes the Diamond Model a useful threat modeling tool for analysts?

A Retro Feast for the Family: The Cyber Kill Chain

NOVEMBER 22, 2023 MIKE 0 COMMENTS

Americans reading this may be like me and headed towards a food coma. My gift to you? I give you a crowd-pleasing topic for family banter. Rather than argue over controversial topics, avoiding Aunt Mildred's hugs, or snoring through a futile Cowboys game, cook up a retro feast for the family with the Cyber Kill Chain! If you've seen the "Fishes" episode of The Bear, you know how bad things can get. So consider this your safe topic, one everybody can enjoy. Your kids will thank you. Your family will be prepared to defend against nation state threats while bickering over the wishbone. Relative peace AND security? You're welcome.

The Basics of the Cyber Kill Chain



It's been a rough year for Stu. He just never was able to untangle his SOC's stacks. Al drew him with 4 legs, and he missed a CIA bullet about Thanksgiving scams...



Gap Analysis With ATT&CK: Fix Your Posture, Young Man!

NOVEMBER 19, 2023 MIKE 0 COMMENTS

Early adopters certainly focused on using ATT&CK for glamorous use cases like [Threat Intelligence](#) and [Adversary Emulation](#). Conducting gap analysis with ATT&CK to prioritize engineering efforts is a high-return effort for you and your organization. It's my favorite of the use cases because it can help any organization!

Item2ShellEditViewSessionScriptsProfilesToolbeltWindowHelp

Wizard Spider, UNC1878, TEMP xATT&CK® NavigatorRed Team | CALDERAM3FEND Matrix | MITRE D3FENDAnalytics (by technique) | MITRE CjATT&CK Sync

https://mitre-attack.github.io/attack-navigator/#?layerURL=https%3A%2F%2Fattack.mitre.org%2Fgroups%2FG0009%2FG0009-enterprise-layer.json

Deep Panda (G0009) xWizard Spider (G0102) xThreat Picture CLUS 2023 x+

Reconnaissance10 techniques

Active Scanning (0/3)
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 (0/3)
Search Victim-Owned Websites

Resource Development8 techniques

Acquire Access
Acquire Infrastructure (0/8)
Compromise Accounts (0/3)
Compromise Infrastructure (0/7)
Develop Capabilities (0/4)
Establish Accounts (0/3)
Obtain Capabilities (0/6)
Stage Capabilities (0/6)

Initial Access9 techniques

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

mimcphee@MIMCPHEE-M-F06T:~/DeTTECT

~/DeTTECT (master) »

mimcphee@MIMCPHEE-M-F06T

selection controls

layer controls

technique controls

Defense Evasion42 techniques

Adversary-in-the-Middle (0/3)
Brute Force (0/4)
Credentials from Password Stores (0/6)
Exploitation for Credential Access
Forced Authentication
Forge Web Credentials (0/2)
Input Capture (0/4)
Modify Authentication Process (0/8)
Multi-Factor Authentication Interception
Multi-Factor Authentication Request Generation
Network Sniffing
OS Credential Dumping (0/8)
Steal Application Access Token
Steal or Forge Authentication Certificates
Steal or Forge Kerberos Tickets (0/4)

Credential Access17 techniques

Account Discovery (0/4)
Application Window Discovery
Browser Information Discovery
Cloud Infrastructure Discovery
Cloud Service Dashboard
Cloud Service Discovery
Cloud Storage Object Discovery
Container and Resource Discovery
Debugger Evasion
Device Driver Discovery
Domain Trust Discovery
File and Directory Discovery
Group Policy Discovery
Network Service Discovery
Network Share Discovery
Network Sniffing
Password Policy Discovery
Peripheral Device Discovery
Permission Groups Discovery (0/3)

Discovery31 techniques

Exploitation of Remote Services
Internal Spearphishing
Lateral Tool Transfer
Remote Service Session Hijacking (0/2)
Cloud Services
Distributed Component Object
Remote Desktop Protocol
SMB/Windows Admin Shares
SSH
VNC
Windows Remote Management

Lateral Movement9 techniques

Pre-OS Boot (0/5)
Scheduled Task/Job (0/5)
IIS Components
Hijack Execution

MITRE ATT&CK® Navigator v4.8.2

BRKSEC-2227

legend59

How do Cisco tools
align with the
framework?

Cisco Mapping to MITRE ATT&CK

Cisco Security visibility into MITRE ATT&CK®

Desktop Frameworks

These Techniques, from the Windows, macOS, Linux platform subsets of the Enterprise ATT&CK Framework, are associated with detection content for the indicated products.

Having visibility into a technique does not ensure detection or protection against all occurrences of the technique.

Initial Access	Execution	Persistence...	...	[Privilege]	Escalation]	[Defense]	Evasion]	Credential Access	Discovery...	...	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
T1078 Valid Accounts	T1059 Command and Scripting Interpreter	T1546 Event Triggered Execution	T1543 Create or Modify System Process	T1546 Event Triggered Execution	T1055 Process Injection	T1218 System Binary Proxy Execution	T1562 Impair Defenses	T1003 OS Credential Dumping	T1087 Account Discovery	T1057 Process Discovery	T1021 Remote Services	T1056 Input Capture	T1071 Application Layer Protocol	T1048 Exfiltration Over Alternative Protocol	T1489 Service Stop
T1078.001 Default Accounts	T1059.001 PowerShell	T1546.001 Change Default File Association	T1543.002 Systemd Service	T1546.001 Dynamic-Link Library Injection	T1055.001 Compiled HTML File	T1218.001 Disable or Modify Tools	T1562.001 Memory	T1003.001 LSASS	T1087.003 Email Account	T1069 Permission Groups Discovery	T1021.001 Keylogging	T1056.001 Keylogging	T1071.001 Web Protocols	T1048.002 Exfiltration Over Asymmetric Encrypted Protocols	T1489 Data Destruction
T1078.003 Local Accounts	T1059.003 Windows Command Shell	T1546.003 Windows Management Instrumentation...	T1543.003 Windows Service	T1055.003 Thread Execution	T1055.003 Thread Execution	T1218.003 Disable Windows Event Logging	T1562.002 Security Manager	T1003.002 Security Account Manager	T1087.002 Local Account	T1069.001 Local Groups	T1021.002 SMB Windows Admin Shares	T1056.002 Data from Local System	T1071.002 File Transfer Protocols	T1048.001 Data Encrypted for Impact	T1489 Data Destruction
T1132 External Remote Services	T1059.004 Unix Shell	T1546.004 Unix Shell Subscription	T1053 Scheduled Task/Job	T1055.012 Process Hollowing	T1055.012 Process Hollowing	T1218.005 Malware	T1562.003 Impair Command History Logging	T1003.003 NTDS	T1087.001 Domain Account	T1069.002 Domain Groups	T1021.003 Distributed Component Object Model	T1056.003 Archive Collected Data	T1071.003 Mail Protocols	T1048.001 Data Encrypted for Impact	T1489 Data Destruction
T1189 Drive-by Compromise	T1059.005 Visual Basic	T1546.005 Visual Basic	T1053 Scheduled Task/Job	T1055.013 Process Doppelgänger	T1055.013 Process Doppelgänger	T1218.008 Dbcoof	T1562.004 Disable or Modify System Firewall	T1003.004 LSA Secrets	T1087.002 System Configuration...	T1069.002 System Sandbox Evasion	T1021.004 SSH	T1056.004 Archive via Utility	T1071.004 Web Service	T1048.002 Exfiltration Over C2 Channel	T1489 Data Destruction
T1190 Exploit Public...	T1059.006 Python	T1546.006 Python	T1053.002 Task Scheduler	T1055.007 Task Scheduler	T1055.007 Task Scheduler	T1218.009 Regsvr32	T1562.005 Impair Defenses	T1003.005 etw passw...	T1087.003 Discovery	T1069.003 Discovery	T1021.005 Virtualizat...	T1056.005 Discovery	T1071.005 Virtualizat...	T1048.003 Exfiltration Over C2 Channel	T1489 Data Destruction

Initial Access	Execution	Persistence...	...	[Privilege]	Escalation]	[Defense]	Evasion]	Credential Access	Discovery...	...	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
T1078 Valid Accounts	T1059 Command and Scripting Interpreter	T1546 Event Triggered Execution	T1543 Create or Modify System Process	T1546 Event Triggered Execution	T1055 Process Injection	T1218 System Binary Proxy Execution	T1562 Impair Defenses	T1003 OS Credential Dumping	T1087 Account Discovery	T1057 Process Discovery	T1021 Remote Services	T1056 Input Capture	T1071 Application Layer Protocol	T1048 Exfiltration Over Alternative Protocol	T1489 Service Stop
T1078.001 Default Accounts	T1059.001 PowerShell	T1546.001 Change Default File Association	T1543.002 Systemd Service	T1546.001 Dynamic-Link Library Injection	T1055.001 Compiled HTML File	T1218.001 Disable or Modify Tools	T1562.001 Memory	T1003.001 LSASS	T1087.003 Email Account	T1069 Permission Groups Discovery	T1021.001 Keylogging	T1056.001 Keylogging	T1071.001 Web Protocols	T1048.002 Exfiltration Over Asymmetric Encrypted Protocols	T1489 Data Destruction
T1078.003 Local Accounts	T1059.003 Windows Command Shell	T1546.003 Windows Management Instrumentation...	T1543.003 Windows Service	T1055.003 Thread Execution	T1055.003 Thread Execution	T1218.003 Disable Windows Event Logging	T1562.002 Security Manager	T1003.002 Security Account Manager	T1087.002 Local Account	T1069.001 Local Groups	T1021.002 SMB Windows Admin Shares	T1056.002 Data from Local System	T1071.002 File Transfer Protocols	T1048.001 Data Encrypted for Impact	T1489 Data Destruction
T1132 External Remote Services	T1059.004 Unix Shell	T1546.004 Unix Shell Subscription	T1053 Scheduled Task/Job	T1055.012 Process Hollowing	T1055.012 Process Hollowing	T1218.005 Malware	T1562.003 Impair Command History Logging	T1003.003 NTDS	T1087.001 Domain Account	T1069.002 Domain Groups	T1021.003 Distributed Component Object Model	T1056.003 Archive Collected Data	T1071.003 Mail Protocols	T1048.001 Data Encrypted for Impact	T1489 Data Destruction
T1189 Drive-by Compromise	T1059.005 Visual Basic	T1546.005 Visual Basic	T1053 Scheduled Task/Job	T1055.013 Process Doppelgänger	T1055.013 Process Doppelgänger	T1218.008 Dbcoof	T1562.004 Disable or Modify System Firewall	T1003.004 LSA Secrets	T1087.002 System Configuration...	T1069.002 System Sandbox Evasion	T1021.004 SSH	T1056.004 Archive via Utility	T1071.004 Web Service	T1048.002 Exfiltration Over C2 Channel	T1489 Data Destruction
T1190 Exploit Public...	T1059.006 Python	T1546.006 Python	T1053.002 Task Scheduler	T1055.007 Task Scheduler	T1055.007 Task Scheduler	T1218.009 Regsvr32	T1562.005 Impair Defenses	T1003.005 etw passw...	T1087.003 Discovery	T1069.003 Discovery	T1021.005 Virtualizat...	T1056.005 Discovery	T1071.005 Virtualizat...	T1048.003 Exfiltration Over C2 Channel	T1489 Data Destruction

- Secure Cloud Analytics
- Secure Endpoint
- Secure Firewall
- Secure Internet Gateway
- Secure Malware Analytics

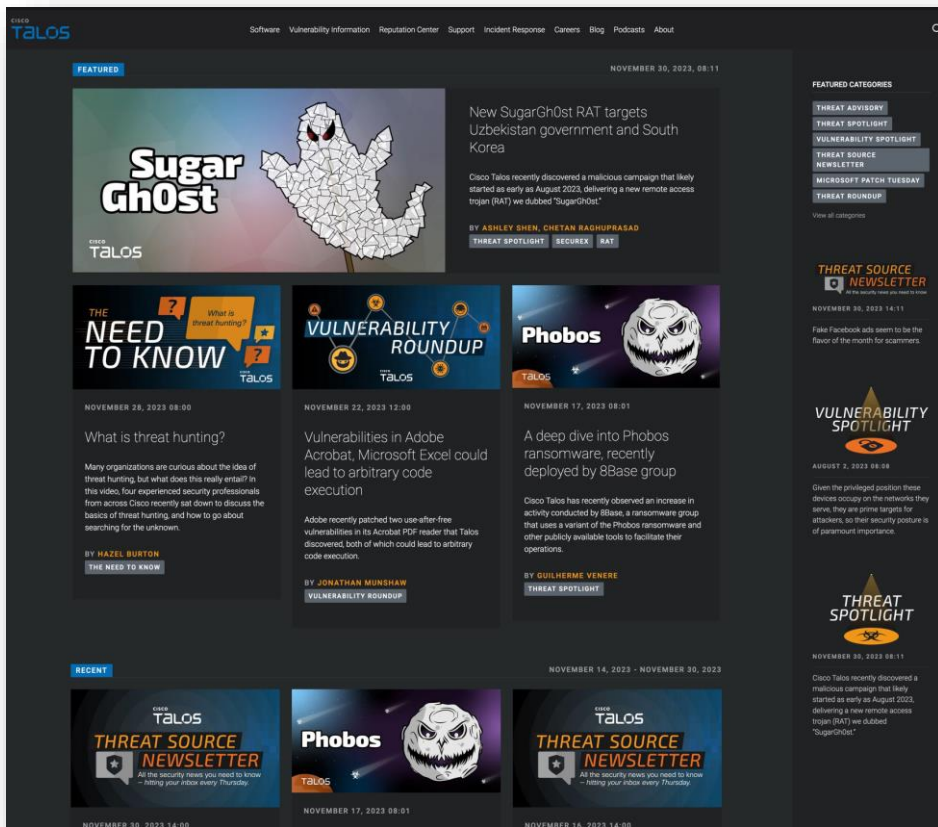
TALOS

#CiscoLiveAPJC

BRKSEC-2227

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

TalosIntelligence.com



- Blogs
- Threat Spotlights
- Beers with Talos
- Software Tools
- Vulnerability Reports
- Searchable Reputation Database



New SugarGh0st RAT targets Uzbekistan government and South Korea

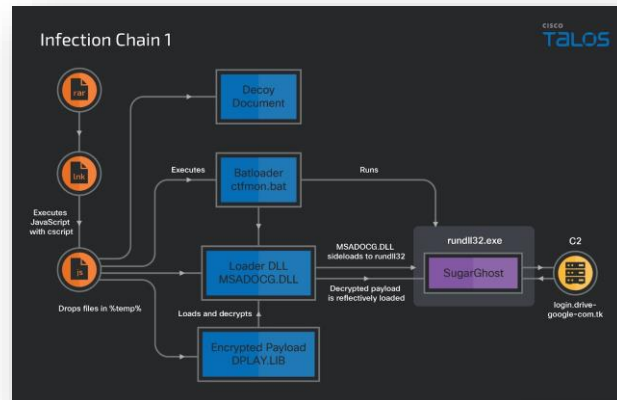
By **Ashley Shen, Chetan Raghuprasad**

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 DynamicWrapperX 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

ATT&CK Technique - Phishing (T1566)

ATT&CK Technique - Valid Accounts (T1078)

Execution

ATT&CK Technique - System Services: Service Execution (T1569.002)

Persistence

ATT&CK Technique - Create Account: Local Accounts (T1136.001)

ATT&CK Technique - Account Manipulation: Device Registration (T1098.005)

Privilege Escalation

ATT&CK Technique - Event Triggered Execution: Image File Execution Options Injection (T1546.012)

Defense Evasion

ATT&CK Technique - Indicator Removal on Host (T1027)

ATT&CK Technique - Indicator Removal on Host: Clear Windows Event Logs (T1070.001)

ATT&CK Technique - Masquerading: Match Legitimate Name or Location (T1036.005)

ATT&CK Technique - Impair Defenses: Disable or Modify System Firewall (T1562.004)

ATT&CK Technique - Modify Registry (T1112)

IOCs

DOMAINS - COMMON:
windows[.]menu

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

HASHES - COMMON:
Apply ps1
D9708BF9795F278B868732D57F42CB0725A6139AFE13E31AE832A5C947099676
defender.vbs
B540D21019AD75047CE74FEDA0E608F56769933556AE2D22D5F4F8B01EE0DA15

HASHES - BLACKCAT:
Reverse-sh (compiled with hardcoded domain):
47AFFAED55D85E1EBE29CF67840A7E9CD8D8620DF8629162A0B1A67F092DCC
stealer:
650BAFE9963CB15CE34060E50E007408DE7012C98668DE0A10386693AA6CD73
Blackcat ransomware:
060CA3F63F3887804420729CDE3FC3D0126C2A0FFC01048BE98F78EAD896767

HASHES - BLACKMATTER:
BlackMatter ransomware:
70AF3EC328E31FF7F64CF80A2F9B8556325C153A329A20620C9879C540839D

Cisco Secure Endpoint flags ATT&CK TTPs

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

The screenshot shows the Cisco Secure Endpoint Dashboard. The top navigation bar includes the Cisco logo, a search bar, and notification icons. The main content area is titled "Dashboard" and features a filter section with "Event Type" set to "Threat Detected" and "Group" set to "All Groups". Below the filter, there are tabs for "File Detection", "Connector Details", and "Comments". The "File Detection" tab is active, showing a list of events. One event is highlighted: "Demo_TeslaCrypt detected lodnxvg.exe as W32.DFC.MalParent". The details for this event are shown in a table with columns for "Detection", "Tactics", and "Techniques". The "Detection" column shows "W32.DFC.MalParent". The "Tactics" column lists "TA0002: Execution", "TA0011: Command and Control", and "TA0042: Resource Depletion". The "Techniques" column lists "T1105: Ingress Tool Transfer", "T1204: User Execution", and "T1204.003: User Execution". A red banner at the bottom of the table indicates "MITRE | ATT&CK".

Detection	Tactics	Techniques
W32.DFC.MalParent	TA0002: Execution, TA0011: Command and Control, TA0042: Resource Depletion	T1105: Ingress Tool Transfer, T1204: User Execution, T1204.003: User Execution

The screenshot shows the Cisco Secure Endpoint Analysis page. The top navigation bar includes the Cisco logo, a search bar, and notification icons. The main content area is titled "Certutil.exe Executed by Schtasks.exe (Demo Data)". Below the title, there is a section for "1 Compromise Observed" with a red indicator for "Require Attention". The "Overview" section shows a table with columns for "Incident Started at", "Incident Discovered on", "Tactics", and "Techniques". The "Tactics" column lists "TA0005: Defense Evasion", "TA0002: Execution", "TA0001: Initial Access", and "TA0003: Persistence". The "Techniques" column lists "T1059: Command and Scripting Interpreter", "T1202: Indirect Command Execution", "T1027: Obfuscated Files or Information", "T1204: User Execution", "T1546: Event Triggered Execution", and "T1566: Phishing". The "Summary" section provides a detailed description of the incident, including the affected host, the user, and the actions taken. The "Remediation" section provides recommendations for the incident, including isolation of the affected hosts and forensic investigation.

Incident Started at	Incident Discovered on	Tactics	Techniques
2023-05-23 19:08:42 EDT	2023-05-23 19:14:09 EDT	TA0005: Defense Evasion, TA0002: Execution, TA0001: Initial Access, TA0003: Persistence	T1059: Command and Scripting Interpreter, T1202: Indirect Command Execution, T1027: Obfuscated Files or Information, T1204: User Execution, T1546: Event Triggered Execution, T1566: Phishing

Cisco Secure Firewall Rules to cover TTPs

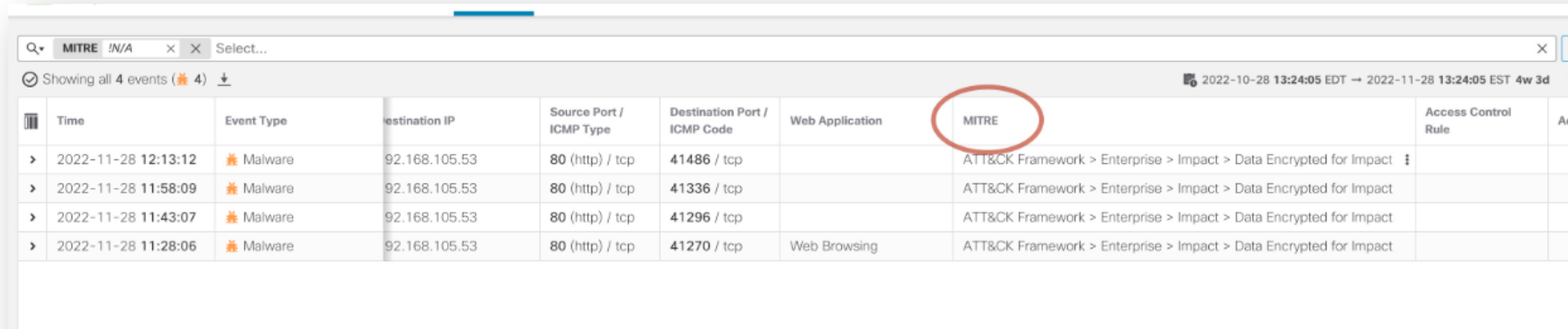
In FTD 7.3, IPS rules can be implemented per tactic or technique.

The screenshot displays the Cisco Defense Orchestrator (DO) interface. The top navigation bar includes 'Defense Orchestrator', 'FMC / Policies / Access Control / Intrusion / Intrusion Policies', and various tabs like 'Analysis', 'Policies', 'Devices', 'Objects', 'Integration', 'Return Home', 'Deploy', and a user profile 'mimcphee@cisco.com'. The main content area shows the configuration for a rule override named 'McPhee-Home-IPS'. The 'Base Policy' is 'Security Over Connectivity' and the 'Mode' is 'Prevention'. The 'Rule Overrides' section is active, showing a list of 78 items. The selected item is 'MITRE / ATT&CK Framework / Enterprise / Privilege Escalation / Exploitation for Privilege Escalation'. The 'Security Level' is 'Enterprise' and the 'Description' states: '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 Action' is set to 'Alert (Default)'. The 'Rule Details' table lists 568 rules, with the first five rules highlighted in green:

Rule ID	Rule Name	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 Privil...

Secure Firewall

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



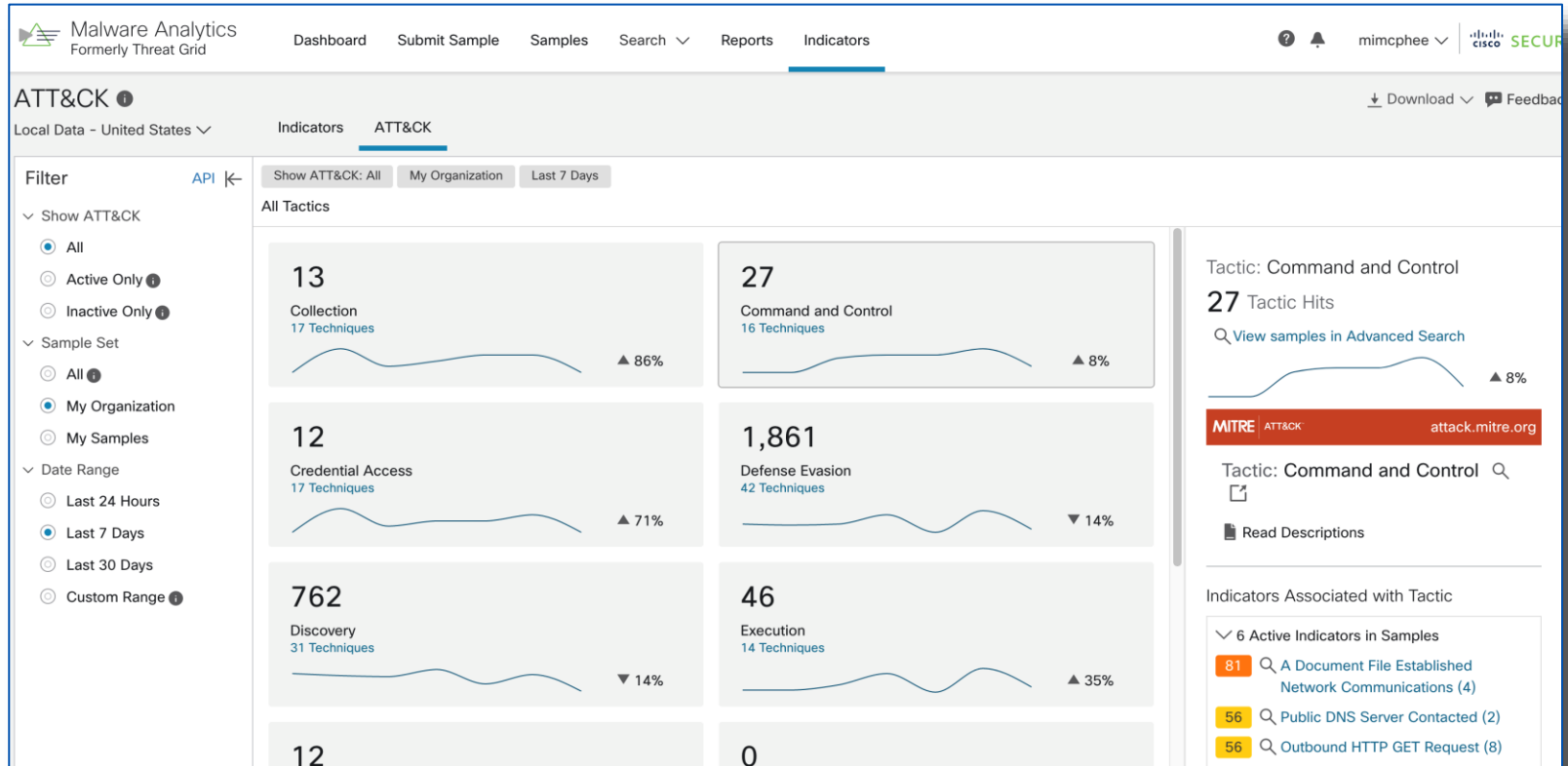
The screenshot shows the Cisco Secure Firewall Unified Event Viewer interface. At the top, there is a search bar with the text "MITRE IN/A" and a "Select..." dropdown. Below the search bar, it says "Showing all 4 events (4)". The main table displays event logs with columns: Time, Event Type, Destination IP, Source Port / ICMP Type, Destination Port / ICMP Code, Web Application, MITRE, Access Control Rule, and Action. The MITRE column is circled in red. The events listed are all Malware events from 2022-11-28, with a consistent MITRE mapping: ATT&CK Framework > Enterprise > Impact > Data Encrypted for Impact.

	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

Cisco Secure Malware Analytics



Cisco Secure Malware Analytics

Malware Analytics
Formerly Threat Grid

Dashboard Submit Sample Samples Search Reports Indicators

Report / Samples / am_delta_918ce329ce3123ec4412b81a92ac32a62bc60961.exe
Local Data - United States

Report FP/FN Resubmit Downloads Feedback

Behavioral Indicators

Only show Indicators with Orbital queries

Title	Categories	ATT&CK	Tags	Hits	Indicator Score
Process Modified File in a User Directory	Dynamic Anomaly		executable file process	2	56
Static Analysis Flagged Artifact As Anomalous	Static Anomaly	Defense Evasion	anomaly static	2	48
Executable Artifact Imports Tool Help Functions	Static Anomaly	Discovery	artifact library PE	6	35
Executable Signing Date Invalid	Attribute		attributes file	1	30
Memory Block Allocation with Read/Write/Execute Permissions	Code Injection	Defense Evasion Privilege Escalation	memory	1	25
PE Contains TLS Callback Entries	Attribute	Defense Evasion	anomaly attributes file	2	24
A Crash Dump File Was Created	Error		artifact crash error file process	1	16
A Fault Report File Was Created	Error		artifact crash error file process	1	16

Report Process Timeline Process Tree MITRE ATT&CK Runtime Video

Cisco Secure Malware Analytics

Behaviours mapped to MITRE ATT&CK within a Sample Submission

Malware Analytics

Formerly Threat Grid

DashboardSubmit SampleSamplesSearchReportsIndicators

Report FP/FN

Resubmit

Downloads

Feedback

MITRE ATT&CK / Samples / am_delta_918ce329ce3123ec4412b81a92ac32a62bc60961.exe

Local Data - United States

Summary

This sample triggered indicators that are associated with the **Defense Evasion**, **Discovery**, and **Privilege Escalation** MITRE ATT&CK™ categories.

Indicator	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Impact	Resource Development	Reconnaissance
Process Modified File in a User Directory														
Static Analysis Flagged Artifact As Anomalous					2 Observables									
Executable Artifact Imports Tool Help Functions							6 Observables							
Executable Signing Date Invalid														
Memory Block Allocation with Read/Write/Execute Permissions				1 Observables	1 Observables									
PE Contains TLS Callback Entries					2 Observables									
A Crash Dump File Was Created														
A Fault Report File Was Created														
Windows Crash Tool Execution Detected														
Executable Signed With Digital Certificate														
Executable with Encrypted Sections					2 Observables									
Executable Imported the IsDebuggerPresent Symbol					2 Observables		2 Observables							

Report

Process Timeline

Process Tree

MITRE ATT&CK

Runtime Video

Cisco Secure Malware Analytics

Malware Analytics
Formerly Threat Grid

Dashboard Submit Sample Samples Search Reports Indicators

MITRE ATT&CK / Samples / am_delta_918ce329ce3123ec4412b81a92ac32a62bc60961.exe

Local Data - United States

Report FP/FN Resubmit Downloads Feedback

Summary
This sample triggered indicators that are associated with the **Defense Evasion**, **Discovery**, and **Privilege Escalation** MITRE ATT&CK™ categories.

Indicator	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Impact	Resource Development	Reconnaissance
Process Modified File in a User Directory														

Static Analysis Flagged Artifact As Anomalous

Indicator Score: 48 Hits: 2

Description
A static analysis rule identified an artifact that has one or more anomalous characteristics. These anomalies may exist due to flaws in the file generation or misunderstandings of the format. Malware may use file anomalies to confuse antivirus parsers and hide code in unusual locations.

Artifact	SHA256	Path	Rule	Description
Artifact 2	8356c74e924c438dbc9c1112e3e210928ba5ce222b173f0c4a1a29477e8cfed9	\\TEMP\\am_delta_918ce329ce3123ec4412b81a92ac32a62bc60961.exe	pe_multi_dos_warning	PE contains multiple DOS warning stubs.
Artifact 1	8356c74e924c438dbc9c1112e3e210928ba5ce222b173f0c4a1a29477e8cfed9	am_delta_918ce329ce3123ec4412b81a92ac32a62bc60961.exe	pe_multi_dos_warning	PE contains multiple DOS warning stubs.

MITRE ATT&CK
attack.mitre.org

Tactic: Defense Evasion 🔍

Technique: Obfuscated Files or Information 📄

Read Descriptions

Executable with Encrypted Sections 2 Observables

Executable Imported the IsDebuggerPresent Symbol 2 Observables

Orbital helps proactively query endpoints for TTPs

The screenshot shows the Orbital web interface with the 'Catalog' tab selected. The left sidebar contains a 'Filters' section with various checkboxes for filtering queries. The main area displays a table of queries with columns for Name, OS, Category, MITRE | ATT&CK®, Updated, and ID. The queries listed include 'Local Group Membership Enumeration Monitoring', 'Logged In Users', 'Powershell Open Source Script Execution Monitoring', 'Windows Event Logs: Account Updated Its Own Group Membership', 'Windows Event Logs: Remote Password Reset', and 'Windows Events For Account Modifications Monitoring'. Each query has associated tags for categories like Posture Assessment, Forensics, and Threat Hunting.

Filters [Reset](#)

Search Catalog Search by Name, ID, OS, Description, Tactics, Techniques, and Sub-Techniques

[Hide Filters](#) [↑](#) [↓](#) [📄](#)

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			
Powershell Open Source Script Execution Monitoring	Windows	Posture Assessment Forensics Threat Hunting			
Windows Event Logs: Account Updated Its Own Group Membership	Windows	Posture Assessment Forensics			
Windows Event Logs: Remote Password Reset	Windows	Forensics			
Windows Events For Account Modifications Monitoring	Windows	Posture Assessment			

[<](#) [1](#) [>](#)

This screenshot shows the details of a query titled 'Windows Event Logs: Account Updated Its Own Group Membership'. The interface includes a search bar, a list of filters, and a table of queries. The selected query is highlighted, and its details are shown on the right. The details include the query's name, description, ID, OS, categories, and MITRE | ATT&CK® reference.

Windows Event Logs: Account Updated Its Own Group Membership [+ Add to new query](#)

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

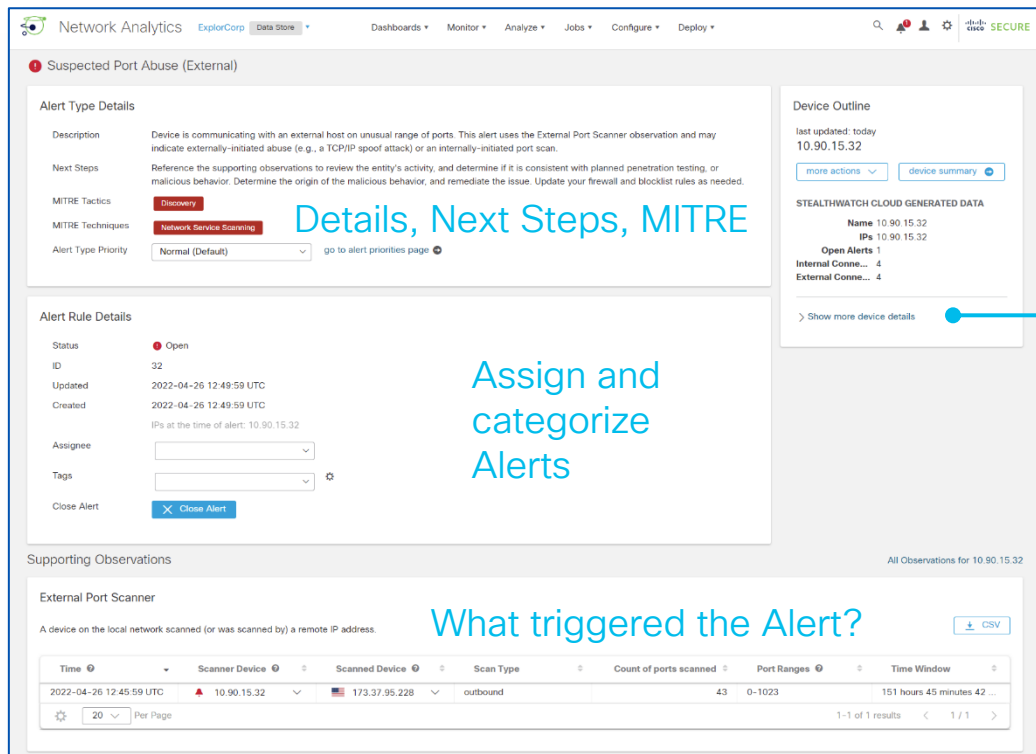
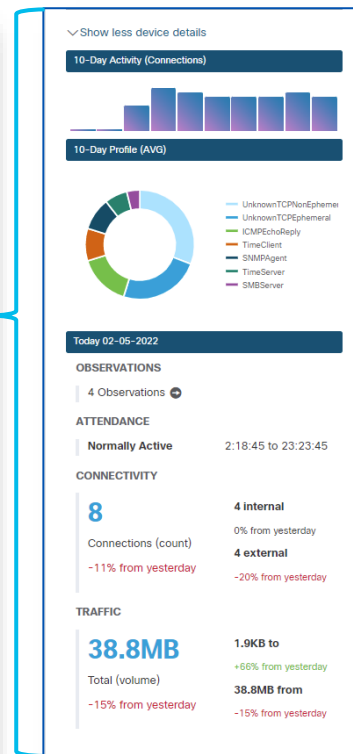
OS Windows

CATEGORIES Posture Assessment
Forensics

MITRE | ATT&CK® TA0003: Persistence

TACTICS TA0003: Persistence

Secure Network Analytics



Device Details

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

Mapping to the MITRE ATT&CK Enterprise matrix

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

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](#)

© 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. 887164323 04/2022

Secure Cloud Analytics – full NDR TTP coverage

The screenshot displays the Cisco Secure Cloud Analytics web interface. The top navigation bar includes 'Monitor', 'Investigate', 'Report', and 'Settings'. A left sidebar lists settings categories like 'Alerts/Watchlists', 'Integrations', and 'Entity Groups'. The main content area is titled 'Priorities Alerts/Watchlists' and features a 'Reset All To Default' button. A modal window is open, showing details for a 'Command And Control' tactic. The modal includes the tactic name, ID (TA0011), last modified date, and a description of the adversary's intent. It also provides a link to 'See Full Details at MITRE ATT&CK (TA0011)'. In the background, a table lists various alert types with their durations and priorities.

Alert Type	Duration	Priority
Confirmed Threat Watchlist	1 Days	Normal
Domain Generation Algorithm	1 Days	Normal
Empire Command and Control	1 Days	Normal
Heartbeat Connection Count	1 Days	Normal

Secure Workload now sorts events by Tactic

Security Summary



Attack Framework ⓘ

[View Alerts](#)[View Forensic Events](#)

Quick select events

Select Severity level ▾



Initial Access 12	Execution 4	Persistence 2	Privilege Escalation 15	Defense Evasion 3	Credentials Access 4	Discovery 4	Lateral Movement 12
<div>☐ 2 Public-facing, privileged workloads</div> <div>☐ 1 Exposed Kubernetes dashboard</div> <div>☐ 3 Vulnerable workloads</div> <div>☐ 3 Unauthorized registries' usage</div> <div>☐ 2 Suspicious deployments</div> <div>☐ 1 Compromised images in registry</div>	<div>☐ 2 Container services</div> <div>☐ 1 Deploy container</div> <div>☐ 1 SSH server running inside container</div>	<div>☐ 2 Writable hostPath mounts</div> <div>☐ 0 Kubernetes cronjob creation</div>	<div>☐ 1 Privileged pods or root pods</div> <div>☐ 4 Privilege escalations enabled</div> <div>☐ 2 Restrict admin-binding ability</div> <div>☐ 2 Multiple cluster admins</div> <div>☐ 4 Access the Kubernetes API servers</div> <div>☐ 2 Writable hostPath mounts</div>	<div>☐ 1 Clear container log</div> <div>☐ 1 Deploy container</div> <div>☐ 1 Delete Kubernetes event</div>	<div>☐ 2 Expose Kubernetes secrets</div> <div>☐ 2 Service account access</div>	<div>☐ 1 Expose Kubernetes dashboards</div> <div>☐ 3 Container resources discovery</div>	<div>☐ 1 Cluster internal networking</div> <div>☐ 2 Access tiller endpoints (HELM 2)</div> <div>☐ 5 Exposed Kubernetes dashboards</div> <div>☐ 4 Core DNS poisonings</div>

Secure Workload

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

Cisco Secure Panoptica

DASHBOARD

OVERVIEW **K8SHIELD**

LAST UPDATE: Jan 27th 2023, 24:12

5 CLUSTER: All clusters

16/16 COMPROMISED NAMESPACES: Finance/finance +15 All

Generate Report

INITIAL ACCESS	EXECUTION	PERSISTENCE	PRIVILEGE ESCALATION	DEFENSE EVASION	CREDENTIALS ACCESS	DISCOVERY	LATERAL MOVEMENT	IMPACT
✓ PUBLIC FACING PRIVILEGED WORKLOAD	△ CONTAINER SERVICE	△ WRITABLE HOSTPATH MOUNT	△ PRIVILEGED PODS/ ROOT PODS	△ CLEAR CONTAINER LOGS	△ EXPOSE KUBERNETES SECRETS	✓ EXPOSED KUBERNETES DASHBOARD	△ CLUSTER INTERNAL NETWORKING	△ DATA DESTRUCTION
✓ EXPOSED KUBERNETES DASHBOARD	△ DEPLOY CONTAINER	△ KUBERNETES CRONJOB CREATION	△ PRIVILEGES ESCALATION ENABLED	△ DEPLOY CONTAINER	△ SERVICEACCOUNT ACCESS	△ CONTAINER RESOURCE DISCOVERY	✓ ACCESS TILLER ENDPOINT (HELM 2)	
△ VULNERABLE WORKLOADS	△ SSH SERVER RUNNING INSIDE CONTAINER		△ RESTRICT ADMIN BINDING ABILITY	△ DELETE KUBERNETES EVENTS			✓ EXPOSED KUBERNETES DASHBOARD	
△ UNAUTHORISED REGISTRIES USAGE			△ MULTIPLE CLUSTER ADMINS				△ CORE DNS POISONING	
△ SUSPICIOUS DEPLOYMENT			△ ACCESS THE KUBERNETES API SERVER					
△ COMPROMISED IMAGES IN REGISTRY			△ WRITABLE HOSTPATH MOUNT					

- Path Analysis
- Code Security
- CI/CD Security
- CSPM
- CWP

<https://www.panoptica.app/blog/enhance-your-container-security-with-the-mitre-attck-framework>

Closing detection gaps and enriching events

Incidents

853 Incidents | 7 New Incidents | 230 Open Incidents

Search: 11 matching results | Filters: Status: Incident Reported

Priority	Name	Source	Created	Assignee	Priority score breakdown
1000	EC2AMAZ-AHQFEJR in group Audit @ 20230417 08:16:38	Secure Endpoint	15 Hours	RR SM	
523	c1-4506-1-g3-14-win10 in group Mars Clients @ 20230411 20:27:12	Secure Endpoint	6 Days	HJ	
392	c1-9300-1-g1-13-ublnx in group Mars Clients @ 20230411 18:26:19	Secure Endpoint	6 Days	JR	
793	c3-9300-1-g1-0-7-win10 in group Audit @ 20230411 08:48:54	Secure Endpoint	7 Days	IS	
1000	Heartbeat Connection Count for Cisco - Lawrenceville Lab (Earth)	Cisco Secure Cloud Anal...	9 Days	SM ST	
873	c1-4506-2-g3-13-win10 in group Mars Clients @ 20230406 13:52:31	Secure Endpoint	11 Days	IS ST	
1000	c5-9300-1-g1-8-win10 in group Pluto Clients @ 20230406 13:52:57	Secure Endpoint	11 Days	ST	
1000	c4-3650-1-g1-8-win10 in group Earth Clients @ 20230406 13:51:59	Secure Endpoint	11 Days	ST	
765	Persistent Remote Control Connections for Cisco - Lawrenceville Lab (Earth)	Cisco Secure Cloud Anal...	22 Days	DH	
924	Alert Chain ff873ab for Cisco - Lawrenceville Lab (Earth)	Cisco Secure Cloud Anal...	1 Month	UM	
	Alert Chain ff873ab for Cisco - Lawrenceville Lab (Earth)	Cisco Secure Cloud Anal...	1 Year	RR SM	

Alert Chain ff873ab for Cisco - Lawrenceville Lab...

Reported by Cisco Secure Cloud Analytics (cisco-espiorcorp-earth) 1 year ago

Assigned RR SM ST

MITRE (.....)

MITRE | ATT&CK View Details

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

Alerts

- Excessive Access Attempts (External) - #1953
- Confirmed Threat Watchlist Hit - #3080
- Confirmed Threat Watchlist Hit - #3422
- Confirmed Threat Watchlist Hit - #3423
- Unusual External Server - #3785
- New Remote Access - #3829
- Confirmed Threat Watchlist Hit - #3830
- Internal Connection Watchlist Hit - #3837
- User Watchlist Hit - #3871
- Confirmed Threat Watchlist Hit - #3889

Sources

- i-06c189f3c85251a7d (x4)
- atl-tme-c2-win10-2.cisco.com
- ip-10-90-12-22.us-east-2.compute.internal
- i-075b9fe21eaa03761 (x2)
- Network
- ip-10-90-12-27.us-east-2.compute.internal

Common Indicators

198.51.100.100, i-06c189f3c85251a7d, i-075b9fe21eaa03761, ip-10-90-12-27.us-east-2.compute.internal, ip-172-31-86-232.us-east-2.compute.internal

Created

2022-04-01T16:00:00Z

Updated

2023-02-01T03:50:00Z

Chaining Patterns - Tactics

Credential Access (TA0006) → Command And Control (TA0011) (x4) → Initial Access (TA0001) - > Command And Control (TA0011) → Persistence (TA0003) → Command And Control (TA0011) (x2)

Chaining Patterns - Techniques

Brute Force (T1110) → Application Layer Protocol (T1071) (x4) → External Remote Services (T1133) → Application Layer Protocol (T1071) → Event Triggered Execution (T1546) → Web Service (T1102) → Application Layer Protocol (T1071)

View Incident Detail

- Helps corollate, ID behaviors, and recommend response
- Imbued in all XDR detections, carried in by tags from others

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

Penetration Test versus Adversary Emulation

Penetration Testing

- Identify and exploit vulnerabilities on a system (or systems) to assess security
- Focused on a specific scope (app, system or a range to scan)
- Outcome is to test prevention, not on detection

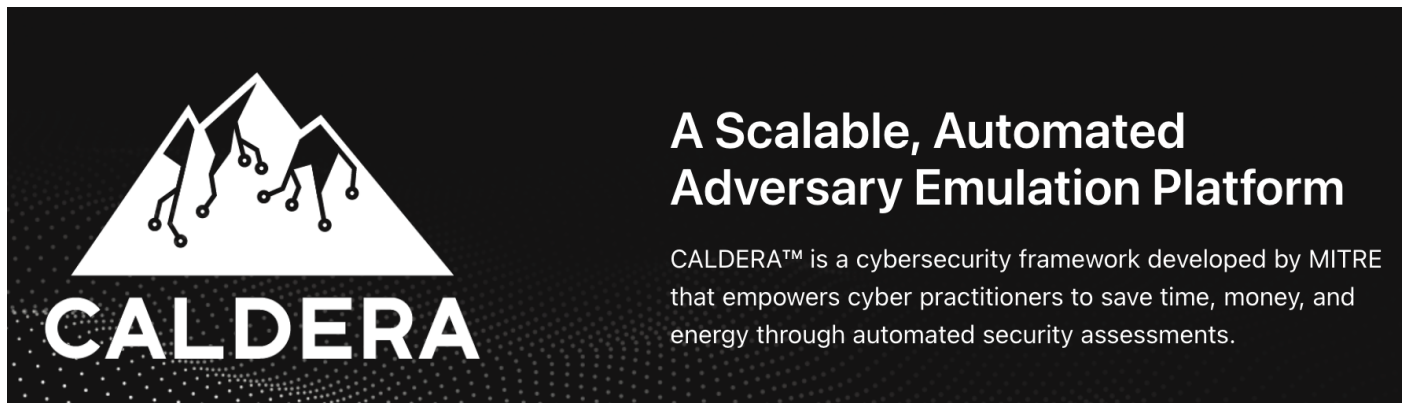
Adversary Emulation

- Assess how resilient we are for a certain adversary group or type
- Focused on the execution of a scenario (can we go from host compromise to data exfil)
- Can be used for both prevention and detection

Both add extensive value in learning techniques used.

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 Definitions

- An **Ability** is at a similar level as an ATT&CK technique. Suite of actions achieving a goal
- **Adversary** describes an actor equipped with abilities
- **Agents** are software programs that connect back to Caldera at certain intervals to get instructions.
- **Operations** (like a playbook) run abilities on agent groups
- **Jitter** allows you to throttle the execution of operations (slow down to prevent detection)
- Caldera **plugins** can be customized to suite your environment, they also extended capabilities not native to Caldera

Some of the cool plugins

- Mock – gives simulated agents to Caldera and allows you to run complete operations with just your laptop
- Sandcat – Caldera default agent. Written in GoLang (cross platform)
Beacons back to C2 server for instructions, execution and sending results
- Response – Gives Incident Response capabilities to the system
- Gameboard – Self descriptive, gives a Red/Blue scoreboard.
- Human – Allows you to simulate a user at the console. Web browsing, create excel sheets, download files or custom commands.

Caldera Demo

Camtasia 2022FileEditModifyTextViewExportWindowHelp

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

172.16.249.140:8888/?#home

agents ×abilities ×adversaries ×

ATT&CKBox

ActivitiesTerminalMay 28 15:25

mike@hackbox: ~/caldera

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

Home

Old Firefox Data

ToolSchool_Zeek

CAMP

agentsabilitiesadversariesoperations

PLUGINSaccessatomiccompasdebriefemufieldmargameboimanxmocksandcatstockpiltraining

CONFIGfact souobjectivplannerscontactsobfuscatorsconfiguration

Create Operation

BRKSEC-2227

Adversary Profiles: which techniques are used, when?

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

CALDERA

agents × abilities × **adversaries ×** operations × debrief × compass ×

Adversary Profiles

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.

Select a profile Carbanak (collection, defense-evasion, credential-dumping, command-and-control, lateral-mover) + New Profile

Carbanak

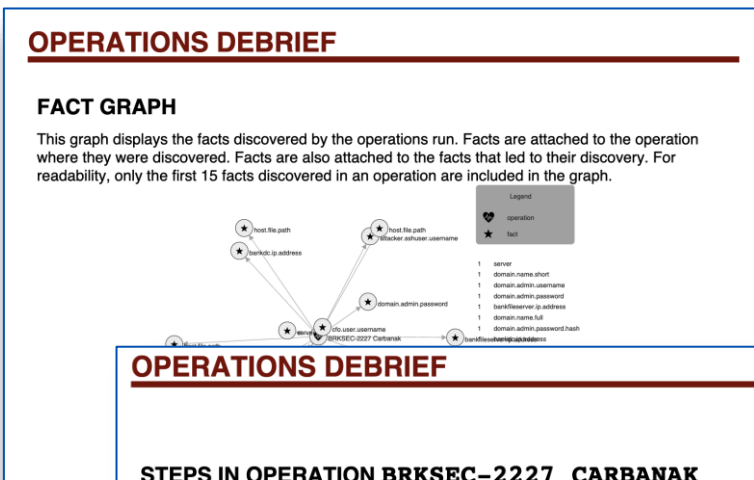
An advanced attacker targeting financial institutions (Emu)

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

collection 25% defense-evasion 12.5% credential-dumping 8.34% command-and-control 16.67% lateral-movement 12.5% discovery 20.84% persistence 4.17%

Ordering	Name	Tactic	Technique	Executors	Requires	Unlocks	Payload	Cleanup
1	Screen Capture (2)	collection	Screen Capture	Windows				
2	Stage 2nd Stage RAT	defense-evasion	Modify Registry	Windows				
3	Execute 2nd Stage RAT	defense-evasion	Deobfuscate/Decode Files or Information	Windows				
4	UAC Bypass and Credential Dumping	credential-dumping	OS Credential Dumping: LSASS Memory	Windows				
5	Read Dumped Credentials	credential-dumping	OS Credential Dumping: LSASS Memory	Windows				
6	Upload Tools for Lateral Movement	command-and-control	Ingress Tool Transfer	Windows				
7	Lateral Tool Transfer	lateral-	Lateral Tool Transfer	Windows				

Extensive PDF and flexible JSON help make the results actionable



CISCO *Live!*

Focus on Fixes

High-level overview of each technique

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. On the left, a sidebar lists various techniques under the 'TECHNIQUES' heading, with 'Drive-by Compromise' highlighted in red. The main content area displays the title 'Drive-by Compromise' and a brief description: '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.' Below this, it states 'Multiple ways of delivering exploit code to a browser exist, including:' followed by a bulleted list: '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.', and '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).' A paragraph follows: '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]'. On the right side of the page, a sidebar provides additional details: 'ID: T1189', 'Sub-techniques: No sub-techniques', 'Tactic: Initial Access', 'Platforms: Linux, SaaS, Windows, macOS', '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', and 'Last Modified: 28 July 2021'. At the bottom right of this sidebar are links for 'Version' and 'Permalink'.

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

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

The screenshot shows the MITRE ATT&CK website. 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 under 'MITIGATIONS', 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. A 'Version Permalink' link and an 'ATT&CK® Navigator Layers' dropdown are also visible. 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

- 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

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.org/>

The image displays two overlapping screenshots from the MITRE Cyber Analytics Repository. The top screenshot shows the 'Analytics (by technique)' page, which lists ATT&CK techniques and their corresponding CAR analytics. The bottom screenshot shows the 'Decoy Network Resource' page, which provides detailed information about a specific decoy network resource, including its definition, how it works, considerations, examples, and digital artifact relationships.

MITRE Cyber Analytics Repository

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-CNR

D3-CNR (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 intents and strategies.
- Targets are used to monitor unallocated 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.

Decoy Network Resource → Network Resource

Download ATT&CK Navigator Layer

Related ATT&CK Techniques:

These mappings are inferred, experimental, and will improve as the knowledge graph grows.

CAPEC: Hyber-focused on App and Web

Concentrate on the root of the problem to achieve security enlightenment



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

3000 - Domains of Attack

- [-] Software - (513)
- [-] Hardware - (515)
- [-] Communications - (512)
- [-] Supply Chain - (437)
- [-] 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)

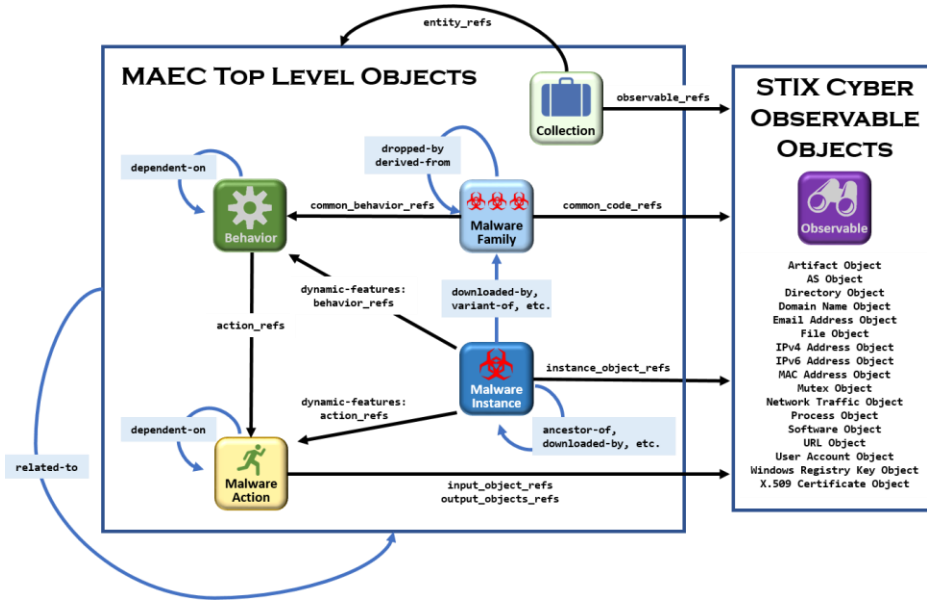
<https://capec.mitre.org/index.html>

MAEC: A Malware language

Concentrate on the root of the problem to achieve security enlightenment

Malware Attribute Enumeration and Characterization (MAEC)

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



<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, Workload, Cloud Analytics, and XDR
- 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.

Lessons when self assessing

- **Don't** assume all techniques are equal – Some are specific, some are generic.
- **Don't** alert on every technique – Focus on the alerts in your environment that you **MUST** know. High fidelity = good
- **Don't** misunderstand your coverage. There are so many possibilities. Measure efficacy of the technique you can detect, not the unknown.
- **Don't** stay in the matrix. Adversaries move faster than models. Be proactive in how to research and detect emerging threats
- **Don't** forget the fundamentals – ATT&CK is a great repo but don't forget training, vulnerability and risk management, zero trust .



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 Cisco Blog Series: <https://blogs.cisco.com/security/mitre-attck-the-magic-of-mitigations>



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>
- BushidoUK's Open-Source Tools for CTI: <https://github.com/BushidoUK/Open-source-tools-for-CTI>



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 Cybre 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>

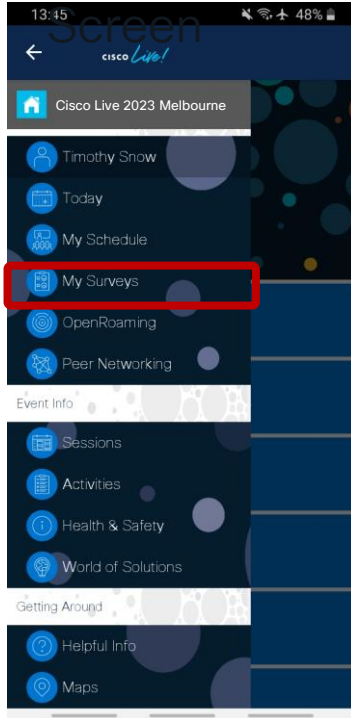
Continue your education



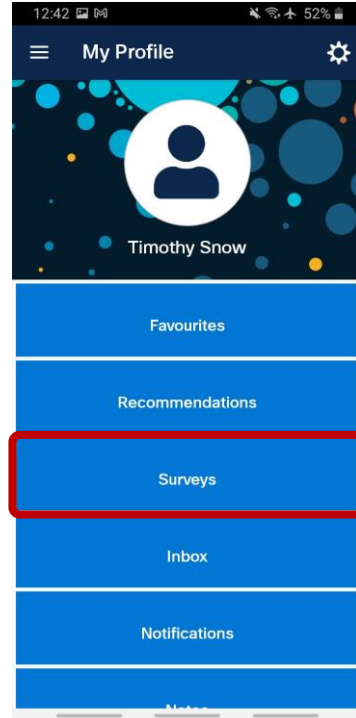
- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Engineer meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

Your feedback matters

Main



Profile



- ☒ Excellent
- ☐ Above Average
- ☐ Average
- ☐ Below Average
- ☐ Poor

Cisco Webex App

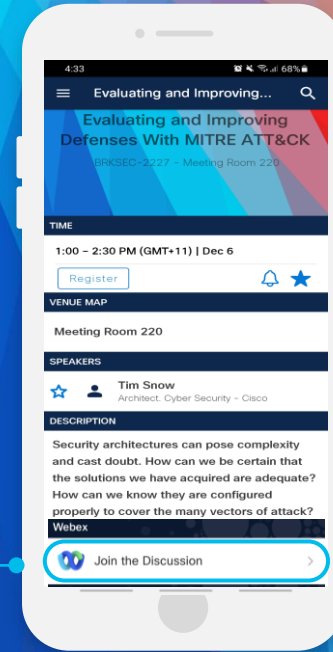
Questions?

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 December 22, 2023.



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



The bridge to possible

Thank you

CISCO *Live!*

#CiscoLiveAPJC