B(lue)Sides

Experiences from four years in the trenches

that will change the way you think about your detection capability

Eleni Philippou

Cybersecurity consultant @ PwC

BSides Cyprus - October 2019

About me

- Cybersecurity consultant @PwC
- Three years @BankOfEngland SOC
- Intelligence Driven ID&R proponent
- I think a lot about models and methods

About this talk

Misperceptions and insights
(tech and beyond) on building a
(truly) effective detection capability

What am I presenting?

Not the #HolyGrailOfDetection but rather my personal experience and views on building an effective detection capability

On pretty good detection capability

- that isn’t

For the past year, I’ve been asking my clients…

“How do you detect attacks against your assets?”

#1

“We have contracted an MSSP to monitor our network…”

- but have no idea what they are doing

#2

"We have invested in best of breed security products…"

- but are not absolutely sure why
- we have some idea what they are doing

#3

“We are collecting all logs in a SIEM…”

- still not sure what to do with those
(i.e. nobody really monitors because it’s a mess)

#4

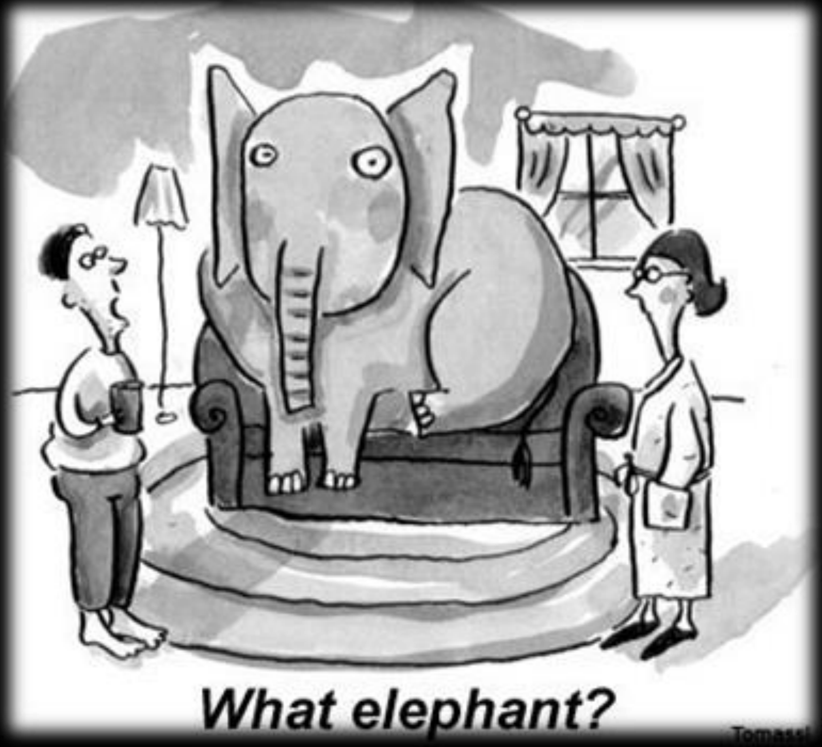
“We are doing regular pentests and red team exercises…”

- and they find critical findings <u>every time </u>so…

(Heart)breaking news

- It ain’t gonna work!

#ButYouAlreadyKnew



BUT......
WHHHHYYYYYYYYY?????
imgflip.com

#1

“We have contracted an MSSP to monitor our network…”

#1

You know your organisation better than any MSSP ever will

…if you don’t, how are you sure your MSSP is doing a good job?

#2

“We have invested in best of breed security products…”

#2

Even the best products cannot detect all attacks.

No tool can substitute a capable analyst.

"We are collecting all logs in a SIEM…"

#3

#3

Collecting the logs is not enough.

Collecting ***all*** the logs is a very bad idea.

#4

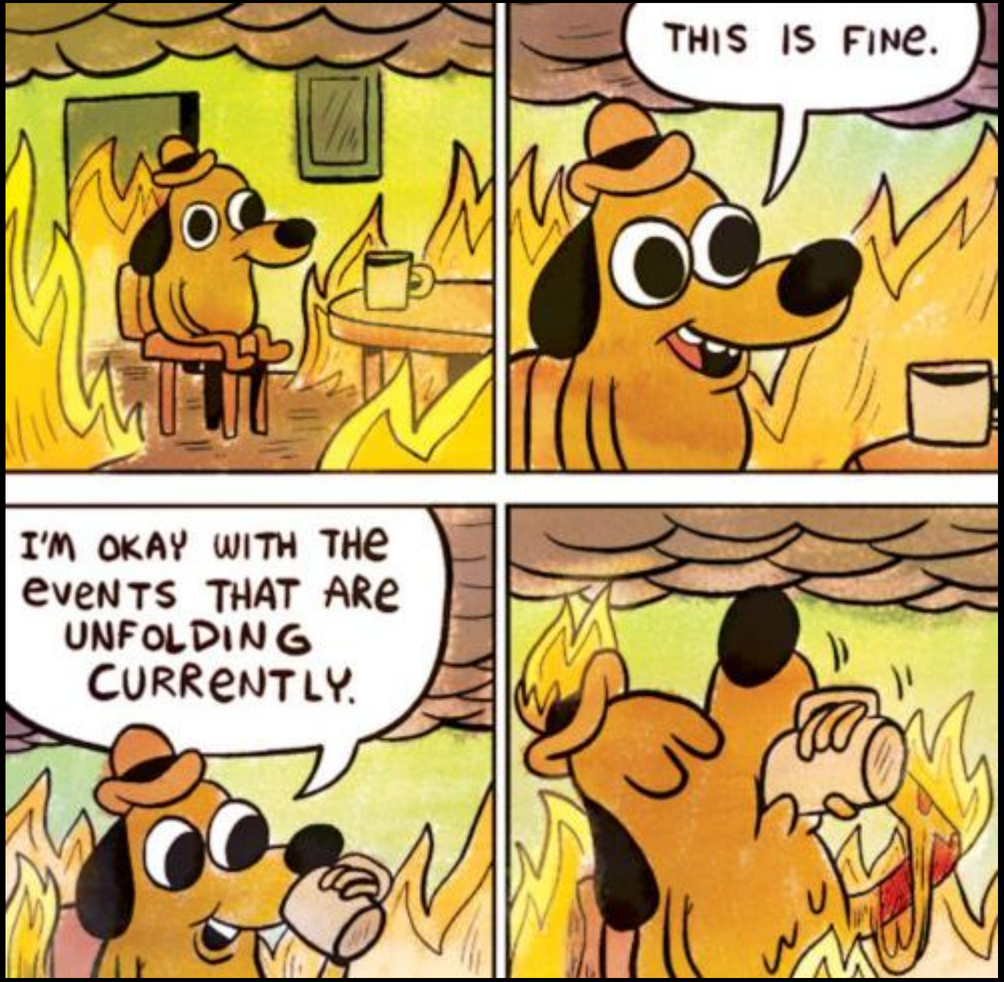
“We are doing regular pentests and red team exercises…”

#4

Pentests and Red Teams are not designed to substitute your blue team.

Just saying…

404
Detection
Capability
Not Found!



On pretty good detection capability

- that actually is!

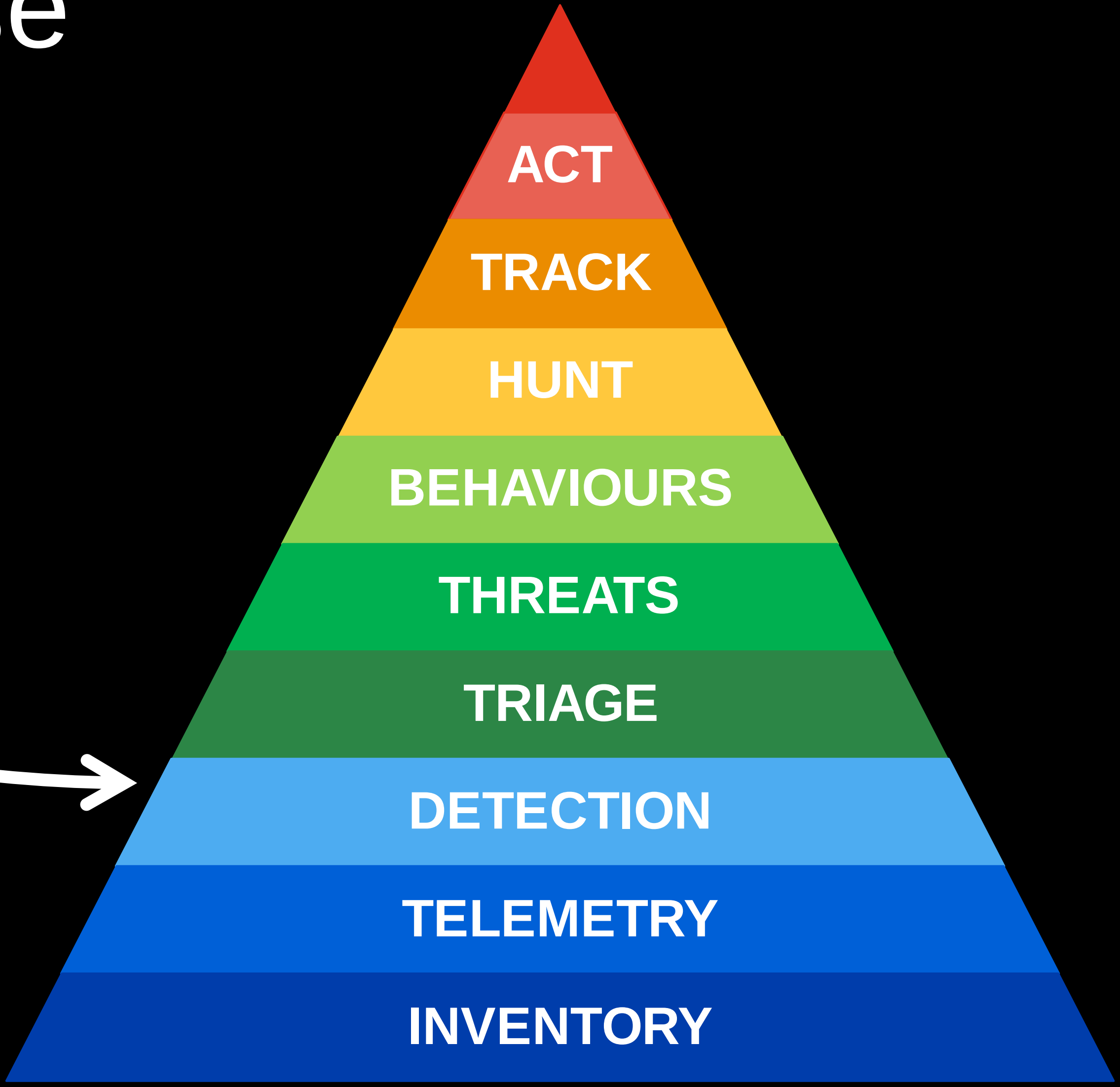
“You don’t reach the mountaintop from the mountaintop. You start from the bottom and climb up”.

The Incident Response Hierarchy of Needs

- Matt Swann

Most companies start here…

…instead of here



Know WHAT you are defending before you try defending it!

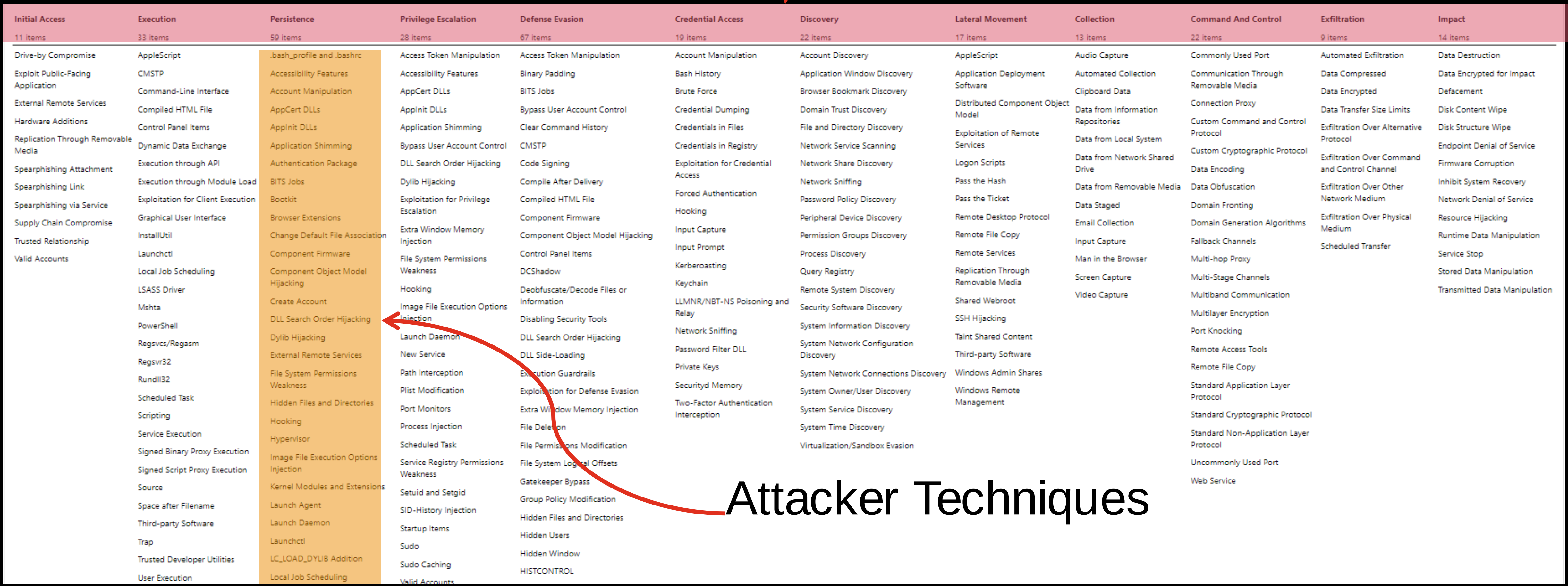
“Every battle is won before it is fought”

THREAT INTELLIGENCE
SO HOT RIGHT NOW
imgflip.com

The ATT&CK Matrix

- MITRE

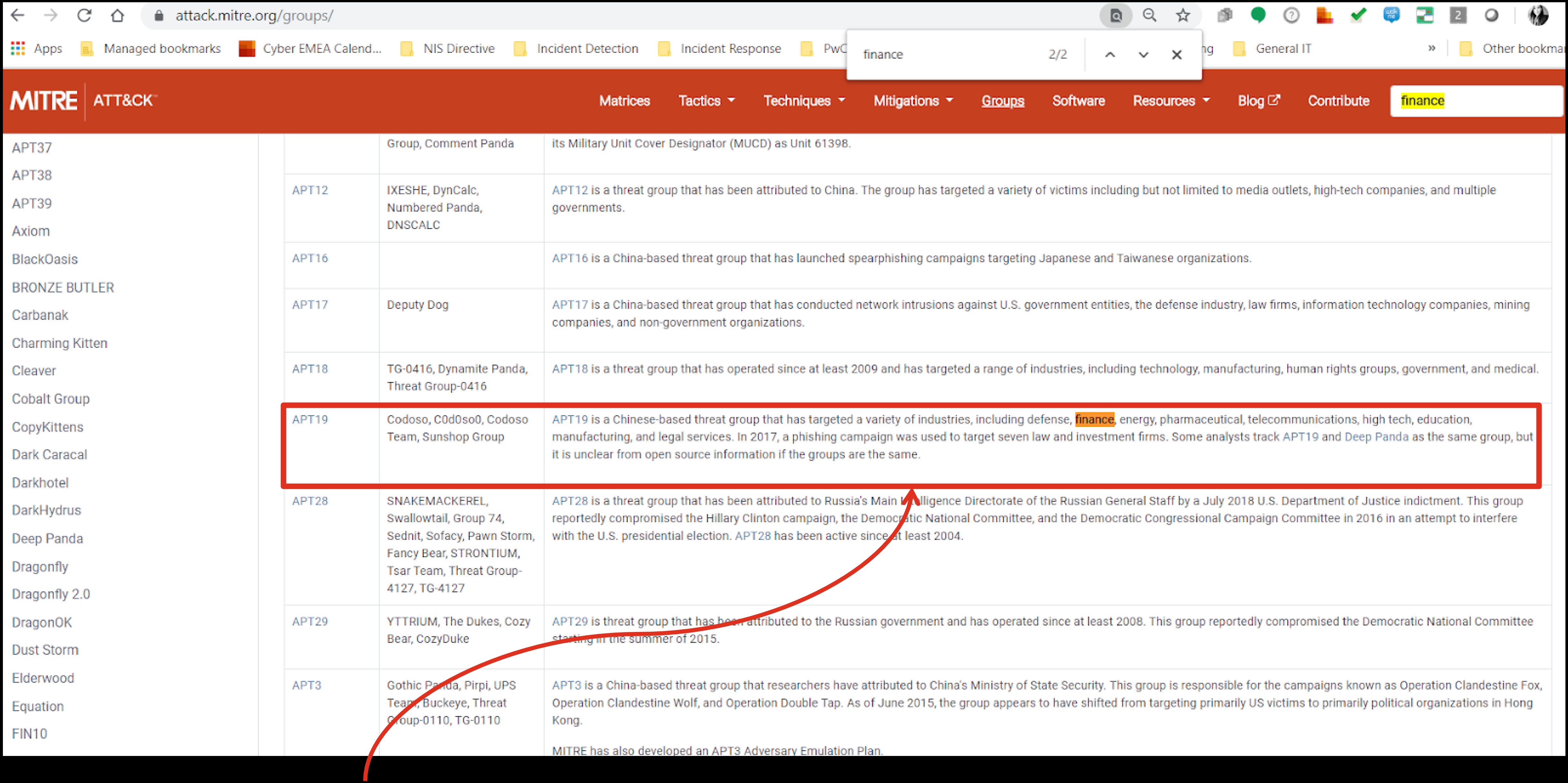
Attacker Tactics



Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
11 items	33 items	59 items	28 items	67 items	19 items	22 items	17 items	13 items	22 items	9 items	14 items
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Data Destruction
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed	Data Encrypted for Impact
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Connection Proxy	Data Encrypted	Defacement
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	Domain Trust Discovery	Exploitation of Remote Services	Data from Information Repositories	Custom Command and Control Protocol	Data Transfer Size Limits	Disk Content Wipe
Replication Through Removable Media	Control Panel Items	AppInit DLLs	Application Shimming	Clear Command History	Credentials in Files	File and Directory Discovery	Logon Scripts	Data from Local System	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Structure Wipe
Spearphishing Attachment	Dynamic Data Exchange	Application Shimming	Bypass User Account Control	CMSTP	Credentials in Registry	Network Service Scanning	Pass the Hash	Data from Network Shared Drive	Data Encoding	Exfiltration Over Command and Control Channel	Endpoint Denial of Service
Spearphishing Link	Execution through API	Authentication Package	DLL Search Order Hijacking	Code Signing	Exploitation for Credential Access	Network Share Discovery	Pass the Ticket	Data from Removable Media	Data Obfuscation	Exfiltration Over Other Network Medium	Firmware Corruption
Spearphishing via Service	Execution through Module Load	BITS Jobs	Dylib Hijacking	Compile After Delivery	Forced Authentication	Network Sniffing	Remote Desktop Protocol	Data Staged	Domain Fronting	Exfiltration Over Physical Medium	Inhibit System Recovery
Supply Chain Compromise	Exploitation for Client Execution	Bootkit	Exploitation for Privilege Escalation	Compiled HTML File	Hooking	Password Policy Discovery	Remote File Copy	Email Collection	Domain Generation Algorithms	Scheduled Transfer	Network Denial of Service
Trusted Relationship	Graphical User Interface	Browser Extensions	Extra Window Memory Injection	Component Firmware	Input Capture	Peripheral Device Discovery	Remote Services	Input Capture	Fallback Channels		Resource Hijacking
Valid Accounts	InstallUtil	Change Default File Association	File System Permissions Weakness	Component Object Model Hijacking	Input Prompt	Permission Groups Discovery	Replication Through Removable Media	Man in the Browser	Multi-hop Proxy		Runtime Data Manipulation
	Launchctl	Component Firmware	Hooking	Control Panel Items	Kerberoasting	Process Discovery	Shared Webroot	Screen Capture	Multi-Stage Channels		Service Stop
	Local Job Scheduling	Component Object Model Hijacking	Image File Execution Options Injection	DCShadow	Keychain	Query Registry	SSH Hijacking	Video Capture	Multiband Communication		Stored Data Manipulation
	LSASS Driver	Create Account	Launch Daemon	Deobfuscate/Decode Files or Information	LLMNR/NBT-NS Poisoning and Relay	Remote System Discovery	Taint Shared Content		Multilayer Encryption		Transmitted Data Manipulation
	Mshta	DLL Search Order Hijacking	New Service	Disabling Security Tools	Network Sniffing	Security Software Discovery	Third-party Software		Port Knocking		
	PowerShell	Dylib Hijacking	Path Interception	DLL Search Order Hijacking	Password Filter DLL	System Information Discovery	Windows Admin Shares		Remote Access Tools		
	Regsvcs/Regasm	External Remote Services	Plist Modification	DLL Side-Loading	Private Keys	System Network Configuration Discovery	Windows Remote Management		Remote File Copy		
	Regsvr32	File System Permissions Weakness	Port Monitors	Execution Guardrails	Securityd Memory	System Network Connections Discovery			Standard Application Layer Protocol		
	Rundll32	Hidden Files and Directories	Process Injection	Exploitation for Defense Evasion	Two-Factor Authentication Interception	System Owner/User Discovery			Standard Cryptographic Protocol		
	Scheduled Task	Hooking	Scheduled Task	Extra Window Memory Injection		System Service Discovery			Standard Non-Application Layer Protocol		
	Scripting	Hypervisor	Service Registry Permissions Weakness	File Deletion		System Time Discovery			Uncommonly Used Port		
	Service Execution	Image File Execution Options Injection	Setuid and Setgid	File Permissions Modification		Virtualization/Sandbox Evasion			Web Service		
	Signed Binary Proxy Execution	Kernel Modules and Extensions	SID-History Injection	File System Logical Offsets							
	Signed Script Proxy Execution	Launch Agent	Startup Items	Gatekeeper Bypass							
	Source	Launch Daemon	Sudo	Group Policy Modification							
	Space after Filename	Launchctl	Sudo Caching	Hidden Files and Directories							
	Third-party Software	LC_LOAD_DYLIB Addition	Valid Accounts	Hidden Users							
	Trap	Local Job Scheduling		Hidden Window							
	Trusted Developer Utilities			HISTCONTROL							
	User Execution										

Attacker Techniques

Anyone said…knowledge base of attacker **TTPs?**



APT37
APT38
APT39
Axiom
BlackOasis
BRONZE BUTLER
Carbanak
Charming Kitten
Cleaver
Cobalt Group
CopyKittens
Dark Caracal
Darkhotel
DarkHydrus
Deep Panda
Dragonfly
Dragonfly 2.0
DragonOK
Dust Storm
Elderwood
Equation
FIN10

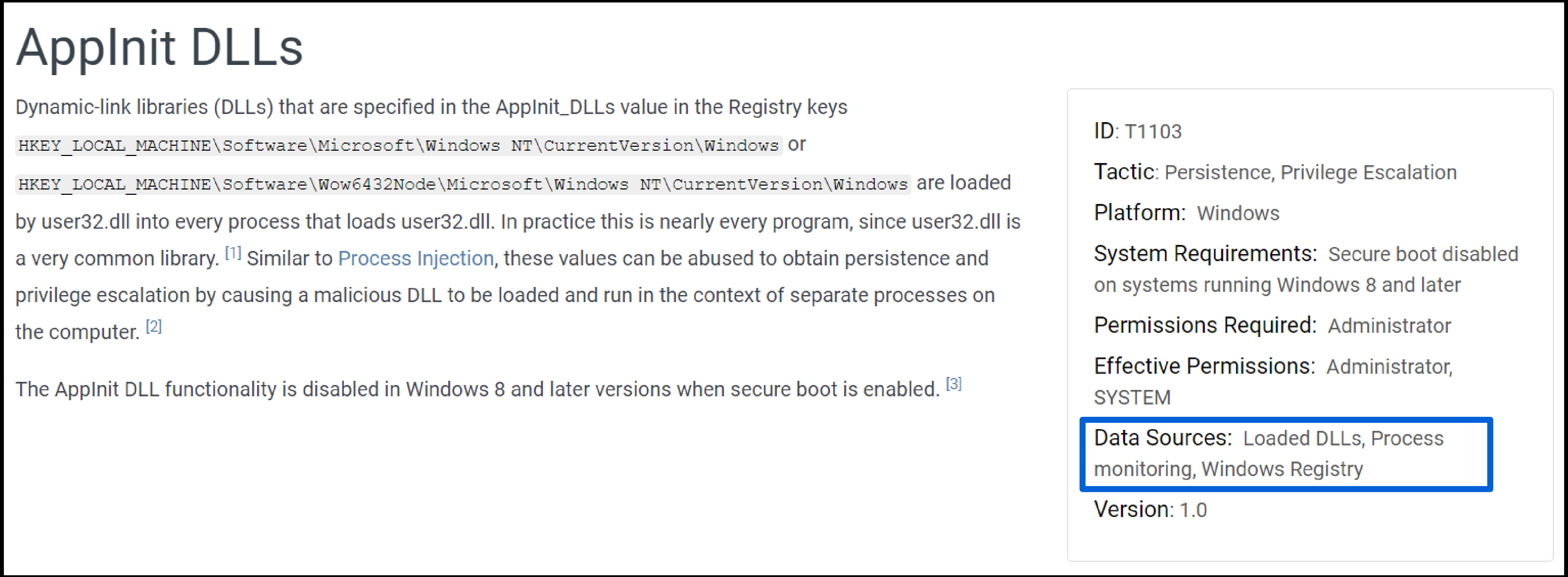
	Group, Comment Panda	its Military Unit Cover Designator (MUCD) as Unit 61398.
APT12	IXESHE, DynCalc, Numbered Panda, DNSCALC	APT12 is a threat group that has been attributed to China. The group has targeted a variety of victims including but not limited to media outlets, high-tech companies, and multiple governments.
APT16		APT16 is a China-based threat group that has launched spearphishing campaigns targeting Japanese and Taiwanese organizations.
APT17	Deputy Dog	APT17 is a China-based threat group that has conducted network intrusions against U.S. government entities, the defense industry, law firms, information technology companies, mining companies, and non-government organizations.
APT18	TG-0416, Dynamite Panda, Threat Group-0416	APT18 is a threat group that has operated since at least 2009 and has targeted a range of industries, including technology, manufacturing, human rights groups, government, and medical.
APT19	Codoso, C0d0so0, Codoso Team, Sunshop Group	APT19 is a Chinese-based threat group that has targeted a variety of industries, including defense, finance, energy, pharmaceutical, telecommunications, high tech, education, manufacturing, and legal services. In 2017, a phishing campaign was used to target seven law and investment firms. Some analysts track APT19 and Deep Panda as the same group, but it is unclear from open source information if the groups are the same.
APT28	SNAKEMACKEREL, Swallowtail, Group 74, Sednit, Sofacy, Pawn Storm, Fancy Bear, STRONTIUM, Tsar Team, Threat Group-4127, TG-4127	APT28 is a threat group that has been attributed to Russia's Main Intelligence Directorate of the Russian General Staff by a July 2018 U.S. Department of Justice indictment. This group reportedly compromised the Hillary Clinton campaign, the Democratic National Committee, and the Democratic Congressional Campaign Committee in 2016 in an attempt to interfere with the U.S. presidential election. APT28 has been active since at least 2004.
APT29	YTTRIUM, The Dukes, Cozy Bear, CozyDuke	APT29 is threat group that has been attributed to the Russian government and has operated since at least 2008. This group reportedly compromised the Democratic National Committee starting in the summer of 2015.
APT3	Gothic Panda, Pirpi, UPS Team, Buckeye, Threat Group-0110, TG-0110	APT3 is a China-based threat group that researchers have attributed to China's Ministry of State Security. This group is responsible for the campaigns known as Operation Clandestine Fox, Operation Clandestine Wolf, and Operation Double Tap. As of June 2015, the group appears to have shifted from targeting primarily US victims to primarily political organizations in Hong Kong. MITRE has also developed an APT3 Adversary Emulation Plan.

WHO would target your assets?

“Knowing yourself is the beginning of all wisdom”

What do you see?

- Data sources their quality and the visibility they give you



AppInit DLLs

Dynamic-link libraries (DLLs) that are specified in the AppInit_DLLs value in the Registry keys `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Windows` or `HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Windows` are loaded by user32.dll into every process that loads user32.dll. In practice this is nearly every program, since user32.dll is a very common library. [1] Similar to Process Injection, these values can be abused to obtain persistence and privilege escalation by causing a malicious DLL to be loaded and run in the context of separate processes on the computer. [2]

The AppInit DLL functionality is disabled in Windows 8 and later versions when secure boot is enabled. [3]

ID: T1103

Tactic: Persistence, Privilege Escalation

Platform: Windows

System Requirements: Secure boot disabled on systems running Windows 8 and later

Permissions Required: Administrator

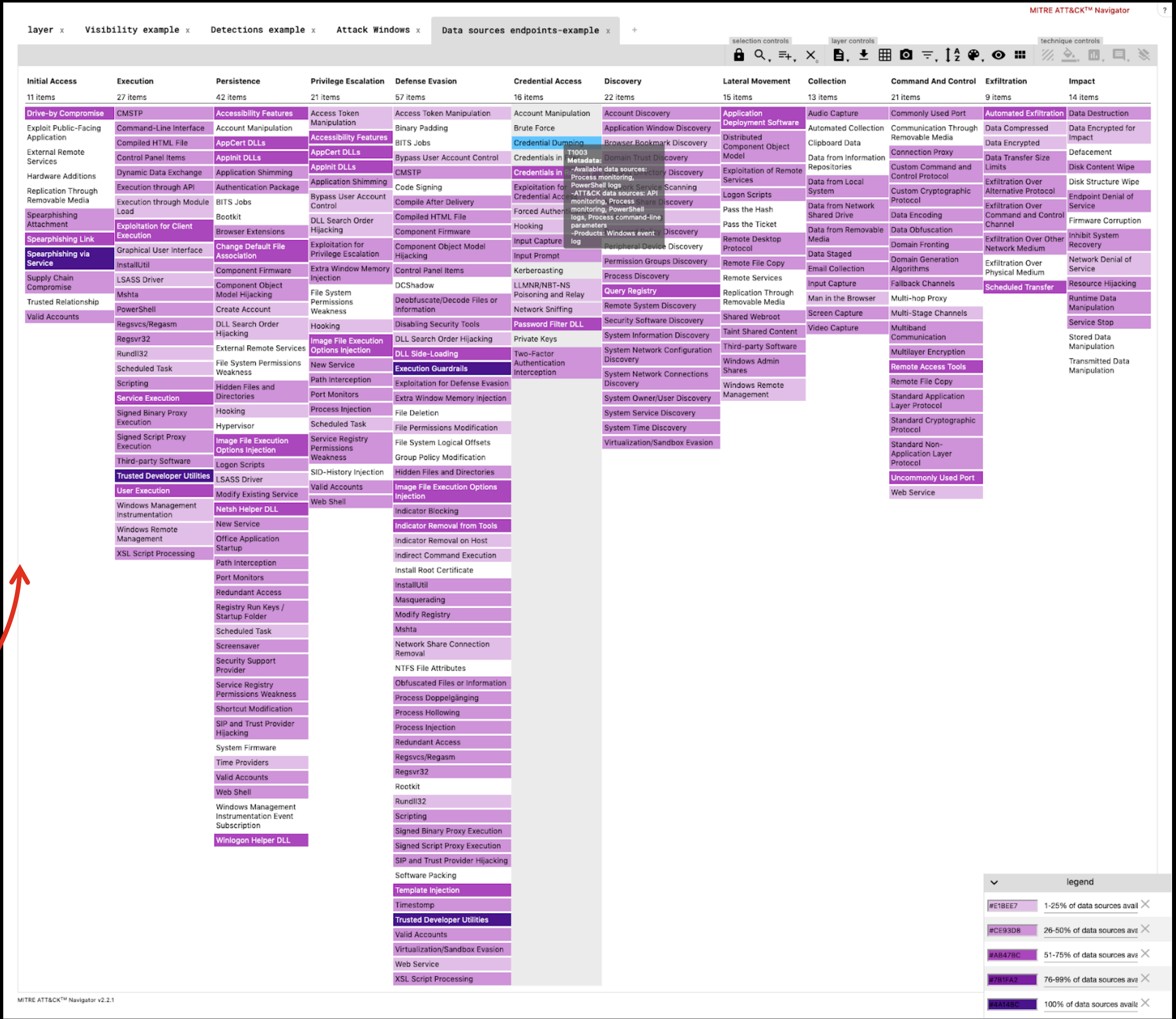
Effective Permissions: Administrator, SYSTEM

Data Sources: Loaded DLLs, Process monitoring, Windows Registry

Version: 1.0

Understanding your visibility

Check it Out:
ATT&CK Navigator
https://mitre-attack.github.io/attack-navigator/enterprise/



Initial Access 11 items
- Drive-by Compromise
- Exploit Public-Facing Application
- External Remote Services
- Hardware Additions
- Replication Through Removable Media
- Spearphishing Attachment
- Spearphishing Link
- Spearphishing via Service
- Supply Chain Compromise
- Trusted Relationship
- Valid Accounts

Execution 27 items
- CMSTP
- Command-Line Interface
- Compiled HTML File
- Control Panel Items
- Dynamic Data Exchange
- Execution through API
- Execution through Module Load
- Exploitation for Client Execution
- Graphical User Interface
- InstallUtil
- LSASS Driver
- Mshta
- PowerShell
- Regsvcs/Regasm
- Regsvr32
- Rundll32
- Scheduled Task
- Scripting
- Service Execution
- Signed Binary Proxy Execution
- Signed Script Proxy Execution
- Third-party Software
- Trusted Developer Utilities
- User Execution
- Windows Management Instrumentation
- Windows Remote Management
- XSL Script Processing

Persistence 42 items
- Accessibility Features
- Account Manipulation
- AppCert DLLs
- AppInit DLLs
- Application Shimming
- Authentication Package
- BITS Jobs
- Bootkit
- Browser Extensions
- Change Default File Association
- Component Firmware
- Component Object Model Hijacking
- Create Account
- DLL Search Order Hijacking
- External Remote Services
- File System Permissions Weakness
- Hidden Files and Directories
- Hooking
- Hypervisor
- Image File Execution Options Injection
- Logon Scripts
- LSASS Driver
- Modify Existing Service
- Netsh Helper DLL
- New Service
- Office Application Startup
- Path Interception
- Port Monitors
- Redundant Access
- Registry Run Keys / Startup Folder
- Scheduled Task
- Screensaver
- Security Support Provider
- Service Registry Permissions Weakness
- Shortcut Modification
- SIP and Trust Provider Hijacking
- System Firmware
- Time Providers
- Valid Accounts
- Web Shell
- Windows Management Instrumentation Event Subscription
- Winlogon Helper DLL

Privilege Escalation 21 items
- Access Token Manipulation
- Accessibility Features
- AppCert DLLs
- AppInit DLLs
- Application Shimming
- Bypass User Account Control
- DLL Search Order Hijacking
- Exploitation for Privilege Escalation
- Extra Window Memory Injection
- File System Permissions Weakness
- Hooking
- Image File Execution Options Injection
- New Service
- Path Interception
- Port Monitors
- Process Injection
- Scheduled Task
- Service Registry Permissions Weakness
- SID-History Injection
- Valid Accounts
- Web Shell

Defense Evasion 57 items
- Access Token Manipulation
- Binary Padding
- BITS Jobs
- Bypass User Account Control
- CMSTP
- Code Signing
- Compile After Delivery
- Compiled HTML File
- Component Firmware
- Component Object Model Hijacking
- Control Panel Items
- DCShadow
- Deobfuscate/Decode Files or Information
- Disabling Security Tools
- DLL Search Order Hijacking
- DLL Side-Loading
- Execution Guardrails
- Exploitation for Defense Evasion
- Extra Window Memory Injection
- File Deletion
- File Permissions Modification
- File System Logical Offsets
- Group Policy Modification
- Hidden Files and Directories
- Image File Execution Options Injection
- Indicator Blocking
- Indicator Removal from Tools
- Indicator Removal on Host
- Indirect Command Execution
- Install Root Certificate
- InstallUtil
- Masquerading
- Modify Registry
- Mshta
- Network Share Connection Removal
- NTFS File Attributes
- Obfuscated Files or Information
- Process Doppelgänging
- Process Hollowing
- Process Injection
- Redundant Access
- Regsvcs/Regasm
- Regsvr32
- Rootkit
- Rundll32
- Scripting
- Signed Binary Proxy Execution
- Signed Script Proxy Execution
- SIP and Trust Provider Hijacking
- Software Packing
- Template Injection
- Timestomp
- Trusted Developer Utilities
- Valid Accounts
- Virtualization/Sandbox Evasion
- Web Service
- XSL Script Processing

Credential Access 16 items
- Account Manipulation
- Brute Force
- Credential Dumping
- Credentials in Files
- Credentials in Registry
- Exploitation for Credential Access
- Forced Authentication
- Hooking
- Input Capture
- Input Prompt
- Kerberoasting
- LLMNR/NBT-NS Poisoning and Relay
- Network Sniffing
- Password Filter DLL
- Private Keys
- Two-Factor Authentication Interception

T1003
Metadata:
-Available data sources: Process monitoring, PowerShell logs
-ATT&CK data sources: API monitoring, Process monitoring, PowerShell logs, Process command-line parameters
-Products: Windows event log

Discovery 22 items
- Account Discovery
- Application Window Discovery
- Browser Bookmark Discovery
- Domain Trust Discovery
- File and Directory Discovery
- Network Service Scanning
- Network Share Discovery
- Network Sniffing
- Password Policy Discovery
- Peripheral Device Discovery
- Permission Groups Discovery
- Process Discovery
- Query Registry
- Remote System Discovery
- Security Software Discovery
- System Information Discovery
- System Network Configuration Discovery
- System Network Connections Discovery
- System Owner/User Discovery
- System Service Discovery
- System Time Discovery
- Virtualization/Sandbox Evasion

Lateral Movement 15 items
- Application Deployment Software
- Distributed Component Object Model
- Exploitation of Remote Services
- Logon Scripts
- Pass the Hash
- Pass the Ticket
- Remote Desktop Protocol
- Remote File Copy
- Remote Services
- Replication Through Removable Media
- Shared Webroot
- Taint Shared Content
- Third-party Software
- Windows Admin Shares
- Windows Remote Management

Collection 13 items
- Audio Capture
- Automated Collection
- Clipboard Data
- Data from Information Repositories
- Data from Local System
- Data from Network Shared Drive
- Data from Removable Media
- Data Staged
- Email Collection
- Input Capture
- Man in the Browser
- Screen Capture
- Video Capture

Command And Control 21 items
- Commonly Used Port
- Communication Through Removable Media
- Connection Proxy
- Custom Command and Control Protocol
- Custom Cryptographic Protocol
- Data Encoding
- Data Obfuscation
- Domain Fronting
- Domain Generation Algorithms
- Fallback Channels
- Multi-hop Proxy
- Multi-Stage Channels
- Multiband Communication
- Multilayer Encryption
- Remote Access Tools
- Remote File Copy
- Standard Application Layer Protocol
- Standard Cryptographic Protocol
- Standard Non-Application Layer Protocol
- Uncommonly Used Port
- Web Service

Exfiltration 9 items
- Automated Exfiltration
- Data Compressed
- Data Encrypted
- Data Transfer Size Limits
- Exfiltration Over Alternative Protocol
- Exfiltration Over Command and Control Channel
- Exfiltration Over Other Network Medium
- Exfiltration Over Physical Medium
- Scheduled Transfer

Impact 14 items
- Data Destruction
- Data Encrypted for Impact
- Defacement
- Disk Content Wipe
- Disk Structure Wipe
- Endpoint Denial of Service
- Firmware Corruption
- Inhibit System Recovery
- Network Denial of Service
- Resource Hijacking
- Runtime Data Manipulation
- Service Stop
- Stored Data Manipulation
- Transmitted Data Manipulation

legend

#E1BEE7	1-25% of data sources avail
#CE93D8	26-50% of data sources ava
#AB47BC	51-75% of data sources ava
#7B1FA2	76-99% of data sources ava
#4A148C	100% of data sources availa

MITRE ATT&CK™ Navigator v2.2.1

“A petabyte of data is a terrible thing to waste”

Developing Detection Analytics

1. Something you read
2. Something you tried
3. Something you know

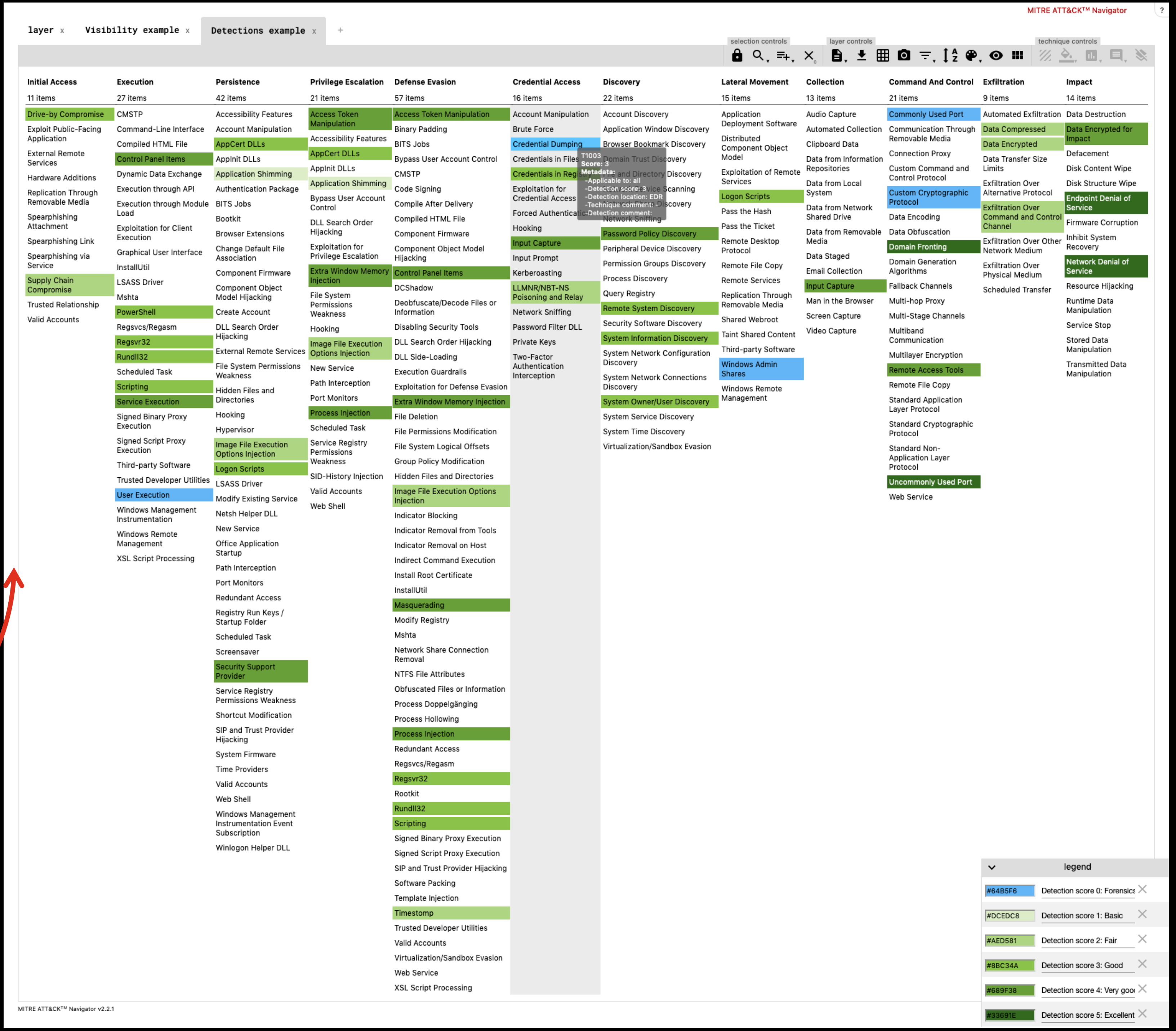
DETECTIONLAB

CALDERA

METTA

Understanding your detection coverage

Detection coverage is bias prone!
-no, you have not covered everything



Initial Access
11 items

- Drive-by Compromise
- Exploit Public-Facing Application
- External Remote Services
- Hardware Additions
- Replication Through Removable Media
- Spearphishing Attachment
- Spearphishing Link
- Spearphishing via Service
- Supply Chain Compromise
- Trusted Relationship
- Valid Accounts

Execution
27 items

- CMSTP
- Command-Line Interface
- Compiled HTML File
- Control Panel Items
- Dynamic Data Exchange
- Execution through API
- Execution through Module Load
- Exploitation for Client Execution
- Graphical User Interface
- InstallUtil
- LSASS Driver
- Mshta
- PowerShell
- Regsvcs/Regasm
- Regsvr32
- Rundll32
- Scheduled Task
- Scripting
- Service Execution
- Signed Binary Proxy Execution
- Signed Script Proxy Execution
- Third-party Software
- Trusted Developer Utilities
- User Execution
- Windows Management Instrumentation
- Windows Remote Management
- XSL Script Processing

Persistence
42 items

- Accessibility Features
- Account Manipulation
- AppCert DLLs
- AppInit DLLs
- Application Shimming
- Authentication Package
- BITS Jobs
- Bootkit
- Browser Extensions
- Change Default File Association
- Component Firmware
- Component Object Model Hijacking
- Create Account
- DLL Search Order Hijacking
- External Remote Services
- File System Permissions Weakness
- Hidden Files and Directories
- Hooking
- Hypervisor
- Image File Execution Options Injection
- Logon Scripts
- LSASS Driver
- Modify Existing Service
- Netsh Helper DLL
- New Service
- Office Application Startup
- Path Interception
- Port Monitors
- Redundant Access
- Registry Run Keys / Startup Folder
- Scheduled Task
- Screensaver
- Security Support Provider
- Service Registry Permissions Weakness
- Shortcut Modification
- SIP and Trust Provider Hijacking
- System Firmware
- Time Providers
- Valid Accounts
- Web Shell
- Windows Management Instrumentation Event Subscription
- Winlogon Helper DLL

Privilege Escalation
21 items

- Access Token Manipulation
- Accessibility Features
- AppCert DLLs
- AppInit DLLs
- Application Shimming
- Bypass User Account Control
- DLL Search Order Hijacking
- Exploitation for Privilege Escalation
- Extra Window Memory Injection
- File System Permissions Weakness
- Hooking
- Image File Execution Options Injection
- New Service
- Path Interception
- Port Monitors
- Process Injection
- Scheduled Task
- Service Registry Permissions Weakness
- SID-History Injection
- Valid Accounts
- Web Shell

Defense Evasion
57 items

- Access Token Manipulation
- Binary Padding
- BITS Jobs
- Bypass User Account Control
- CMSTP
- Code Signing
- Compile After Delivery
- Compiled HTML File
- Component Firmware
- Component Object Model Hijacking
- Control Panel Items
- DCShadow
- Deobfuscate/Decode Files or Information
- Disabling Security Tools
- DLL Search Order Hijacking
- DLL Side-Loading
- Execution Guardrails
- Exploitation for Defense Evasion
- Extra Window Memory Injection
- File Deletion
- File Permissions Modification
- File System Logical Offsets
- Group Policy Modification
- Hidden Files and Directories
- Image File Execution Options Injection
- Indicator Blocking
- Indicator Removal from Tools
- Indicator Removal on Host
- Indirect Command Execution
- Install Root Certificate
- InstallUtil
- Masquerading
- Modify Registry
- Mshta
- Network Share Connection Removal
- NTFS File Attributes
- Obfuscated Files or Information
- Process Doppelgänging
- Process Hollowing
- Process Injection
- Redundant Access
- Regsvcs/Regasm
- Regsvr32
- Rootkit
- Rundll32
- Scripting
- Signed Binary Proxy Execution
- Signed Script Proxy Execution
- SIP and Trust Provider Hijacking
- Software Packing
- Template Injection
- Timestomp
- Trusted Developer Utilities
- Valid Accounts
- Virtualization/Sandbox Evasion
- Web Service
- XSL Script Processing

Credential Access
16 items

- Account Manipulation
- Brute Force
- Credential Dumping
- Credentials in Files
- Credentials in Registry
- Exploitation for Credential Access
- Forced Authentication
- Hooking
- Input Capture
- Input Prompt
- Kerberoasting
- LLMNR/NBT-NS Poisoning and Relay
- Network Sniffing
- Password Filter DLL
- Private Keys
- Two-Factor Authentication Interception

T1003
Score: 3
Metadata:
-Applicable to: all
-Detection score: 3
-Detection location: EDR
-Technique comment: -
-Detection comment:

Discovery
22 items

- Account Discovery
- Application Window Discovery
- Browser Bookmark Discovery
- Domain Trust Discovery
- File and Directory Discovery
- Network Service Scanning
- Network Share Discovery
- Network Sniffing
- Password Policy Discovery
- Peripheral Device Discovery
- Permission Groups Discovery
- Process Discovery
- Query Registry
- Remote System Discovery
- Security Software Discovery
- System Information Discovery
- System Network Configuration Discovery
- System Network Connections Discovery
- System Owner/User Discovery
- System Service Discovery
- System Time Discovery
- Virtualization/Sandbox Evasion

Lateral Movement
15 items

- Application Deployment Software
- Distributed Component Object Model
- Exploitation of Remote Services
- Logon Scripts
- Pass the Hash
- Pass the Ticket
- Remote Desktop Protocol
- Remote File Copy
- Remote Services
- Replication Through Removable Media
- Shared Webroot
- Taint Shared Content
- Third-party Software
- Windows Admin Shares
- Windows Remote Management

Collection
13 items

- Audio Capture
- Automated Collection
- Clipboard Data
- Data from Information Repositories
- Data from Local System
- Data from Network Shared Drive
- Data from Removable Media
- Data Staged
- Email Collection
- Input Capture
- Man in the Browser
- Screen Capture
- Video Capture

Command And Control
21 items

- Commonly Used Port
- Communication Through Removable Media
- Connection Proxy
- Custom Command and Control Protocol
- Custom Cryptographic Protocol
- Data Encoding
- Data Obfuscation
- Domain Fronting
- Domain Generation Algorithms
- Fallback Channels
- Multi-hop Proxy
- Multi-Stage Channels
- Multiband Communication
- Multilayer Encryption
- Remote Access Tools
- Remote File Copy
- Standard Application Layer Protocol
- Standard Cryptographic Protocol
- Standard Non-Application Layer Protocol
- Uncommonly Used Port
- Web Service

Exfiltration
9 items

- Automated Exfiltration
- Data Compressed
- Data Encrypted
- Data Transfer Size Limits
- Exfiltration Over Alternative Protocol
- Exfiltration Over Command and Control Channel
- Exfiltration Over Other Network Medium
- Exfiltration Over Physical Medium
- Scheduled Transfer

Impact
14 items

- Data Destruction
- Data Encrypted for Impact
- Defacement
- Disk Content Wipe
- Disk Structure Wipe
- Endpoint Denial of Service
- Firmware Corruption
- Inhibit System Recovery
- Network Denial of Service
- Resource Hijacking
- Runtime Data Manipulation
- Service Stop
- Stored Data Manipulation
- Transmitted Data Manipulation

legend

#64B5F6	Detection score 0: Forensics
#DCEDC8	Detection score 1: Basic
#AED581	Detection score 2: Fair
#8BC34A	Detection score 3: Good
#689F38	Detection score 4: Very goo
#33691E	Detection score 5: Excellent

MITRE ATT&CK™ Navigator v2.2.1

“One Team, Two Team, Red Team, Blue Team!”

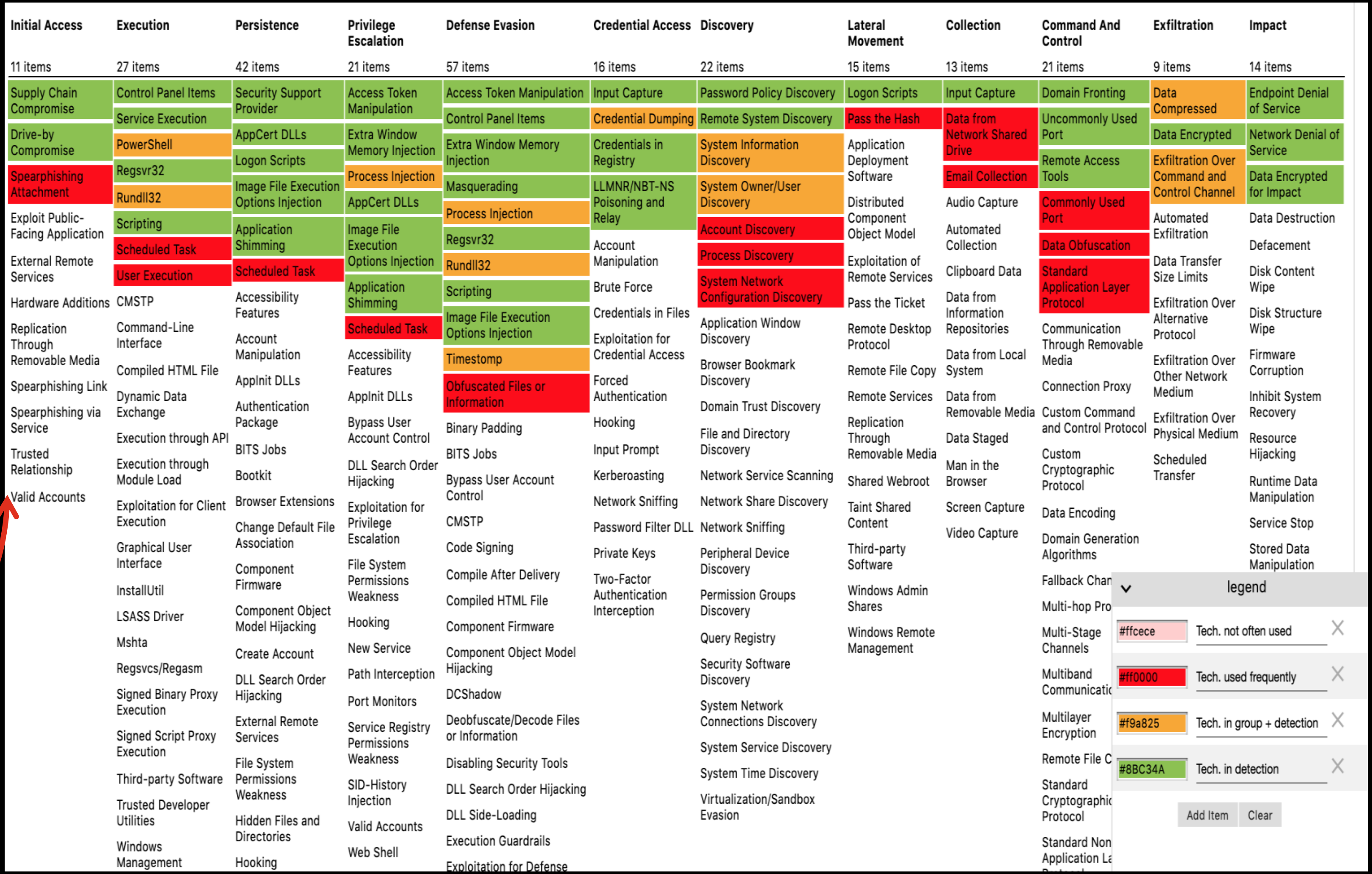
Building confidence in your detection capability

-a.k.a. how to know it’s working

Four approaches:

1. Test it yourself (but Bias!)
2. Test it with someone else (think Purple Team)
3. Have someone put it to the test (think Red Team)
4. Wait for someone to put it to the test (ATTAAACK!)

Use that to identify the gaps…



Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
11 items	27 items	42 items	21 items	57 items	16 items	22 items	15 items	13 items	21 items	9 items	14 items
🟩 Supply Chain Compromise	🟩 Control Panel Items	🟩 Security Support Provider	🟩 Access Token Manipulation	🟩 Access Token Manipulation	🟩 Input Capture	🟩 Password Policy Discovery	🟩 Logon Scripts	🟩 Input Capture	🟩 Domain Fronting	🟧 Data Compressed	🟩 Endpoint Denial of Service
🟩 Drive-by Compromise	🟩 Service Execution	🟩 AppCert DLLs	🟩 Extra Window Memory Injection	🟩 Control Panel Items	🟧 Credential Dumping	🟩 Remote System Discovery	🟥 Pass the Hash	🟥 Data from Network Shared Drive	🟩 Uncommonly Used Port	🟩 Data Encrypted	🟩 Network Denial of Service
🟥 Spearphishing Attachment	🟧 PowerShell	🟩 Logon Scripts	🟧 Process Injection	🟩 Extra Window Memory Injection	🟩 Credentials in Registry	🟧 System Information Discovery	Application Deployment Software	🟥 Email Collection	🟩 Remote Access Tools	🟧 Exfiltration Over Command and Control Channel	🟩 Data Encrypted for Impact
Exploit Public-Facing Application	🟩 Regsvr32	🟩 Image File Execution Options Injection	🟩 AppCert DLLs	🟩 Masquerading	🟩 LLMNR/NBT-NS Poisoning and Relay	🟧 System Owner/User Discovery	Distributed Component Object Model	Audio Capture	🟥 Commonly Used Port	Automated Exfiltration	Data Destruction
External Remote Services	🟧 Rundll32	🟩 Application Shimming	🟩 Image File Execution Options Injection	🟧 Process Injection	Account Manipulation	🟥 Account Discovery	Exploitation of Remote Services	Automated Collection	🟥 Data Obfuscation	Data Transfer Size Limits	Defacement
Hardware Additions	🟩 Scripting	🟥 Scheduled Task	🟩 Application Shimming	🟩 Regsvr32	Brute Force	🟥 Process Discovery	Pass the Ticket	Clipboard Data	🟥 Standard Application Layer Protocol	Exfiltration Over Alternative Protocol	Disk Content Wipe
Replication Through Removable Media	🟥 Scheduled Task	Accessibility Features	🟥 Scheduled Task	🟧 Rundll32	Credentials in Files	🟥 System Network Configuration Discovery	Remote Desktop Protocol	Data from Information Repositories	Communication Through Removable Media	Exfiltration Over Other Network Medium	Disk Structure Wipe
Spearphishing Link	🟥 User Execution	Account Manipulation	Accessibility Features	🟩 Scripting	Exploitation for Credential Access	Application Window Discovery	Remote File Copy	Data from Local System	Connection Proxy	Exfiltration Over Physical Medium	Firmware Corruption
Spearphishing via Service	CMSTP	AppInit DLLs	AppInit DLLs	🟩 Image File Execution Options Injection	Forced Authentication	Browser Bookmark Discovery	Remote Services	Data from Removable Media	Custom Command and Control Protocol	Scheduled Transfer	Inhibit System Recovery
Trusted Relationship	Command-Line Interface	Authentication Package	Bypass User Account Control	🟧 Timestomp	Hooking	Domain Trust Discovery	Replication Through Removable Media	Data Staged	Custom Cryptographic Protocol		Resource Hijacking
Valid Accounts	Compiled HTML File	BITS Jobs	DLL Search Order Hijacking	🟥 Obfuscated Files or Information	Input Prompt	File and Directory Discovery	Shared Webroot	Man in the Browser	Data Encoding		Runtime Data Manipulation
	Dynamic Data Exchange	Bootkit	Exploitation for Privilege Escalation	Binary Padding	Kerberoasting	Network Service Scanning	Taint Shared Content	Screen Capture	Domain Generation Algorithms		Service Stop
	Execution through API	Browser Extensions	File System Permissions Weakness	BITS Jobs	Network Sniffing	Network Share Discovery	Third-party Software	Video Capture	Fallback Chan		Stored Data Manipulation
	Execution through Module Load	Change Default File Association	Hooking	Bypass User Account Control	Password Filter DLL	Network Sniffing	Windows Admin Shares		Multi-hop Pro		
	Exploitation for Client Execution	Component Firmware	New Service	CMSTP	Private Keys	Peripheral Device Discovery	Windows Remote Management		Multi-Stage Channels		
	Graphical User Interface	Component Object Model Hijacking	Path Interception	Code Signing	Two-Factor Authentication Interception	Permission Groups Discovery			Multiband Communicatic		
	InstallUtil	Create Account	Port Monitors	Compile After Delivery		Query Registry			Multilayer Encryption		
	LSASS Driver	DLL Search Order Hijacking	Service Registry Permissions Weakness	Compiled HTML File		Security Software Discovery			Remote File C		
	Mshta	External Remote Services	SID-History Injection	Component Firmware		System Network Connections Discovery			Standard Cryptographic Protocol		
	Regsvcs/Regasm	File System Permissions Weakness	Valid Accounts	Component Object Model Hijacking		System Service Discovery			Standard Non Application La		
	Signed Binary Proxy Execution	Hidden Files and Directories	Web Shell	DCShadow		System Time Discovery					
	Signed Script Proxy Execution	Hooking		Deobfuscate/Decode Files or Information		Virtualization/Sandbox Evasion					
	Third-party Software			Disabling Security Tools							
	Trusted Developer Utilities			DLL Search Order Hijacking							
	Windows Management			DLL Side-Loading							
				Execution Guardrails							
				Exploitation for Defense							

legend

#ffcece	Tech. not often used	X
🟥 #ff0000	Tech. used frequently	X
🟧 #f9a825	Tech. in group + detection	X
🟩 #8BC34A	Tech. in detection	X

Add Item Clear

Tip: Maps of your detection capability can be overlaid with maps of what the Red Team has tried, or what your top adversaries are usually doing to uncover your detection gaps!

TL;DR

If you want to detect attacks against your assets…

1. Prepare to get your hands dirty

- MSSPs, Products, SIEMS and Pentests cannot do the trick if you don't.

2. Adopt a structured approach

- Two models to get you started: The Incident Response Hierarchy of Needs and ATT&CK

3. Visualise, visualise, visualise

- To know where you are at, where you are going to and track your progress.

ONE DOES NOT SIMPLY
SAY THANK YOU WITHOUT A MEME
memes.com

Go Explore!