DAY 4

EFFECTIVE IMPLEMENTATION OF MITRE ATT&CK FRAMEWORK

PRESENTED BY: ADITYA JAMKHANDE

SOMETHING ABOUT ME

- **Experience:**
  - 10+ years in Cybersecurity
  - Security Analysis
  - Incident Handling and response
  - Security Architecture and Strategy
  - SIEM Engineering
  - Vulnerability management
  - SOAR

- **Socials:**
  - LinkedIn: https://www.linkedin.com/in/aditya-j-8a246368
  - Twitter Handle: @ADITYAJAMKHANDE

- **Project Delivered in:**
  - India
  - Australia
  - Belgium

- **Current Company:**
  - Euroclear, Belgium

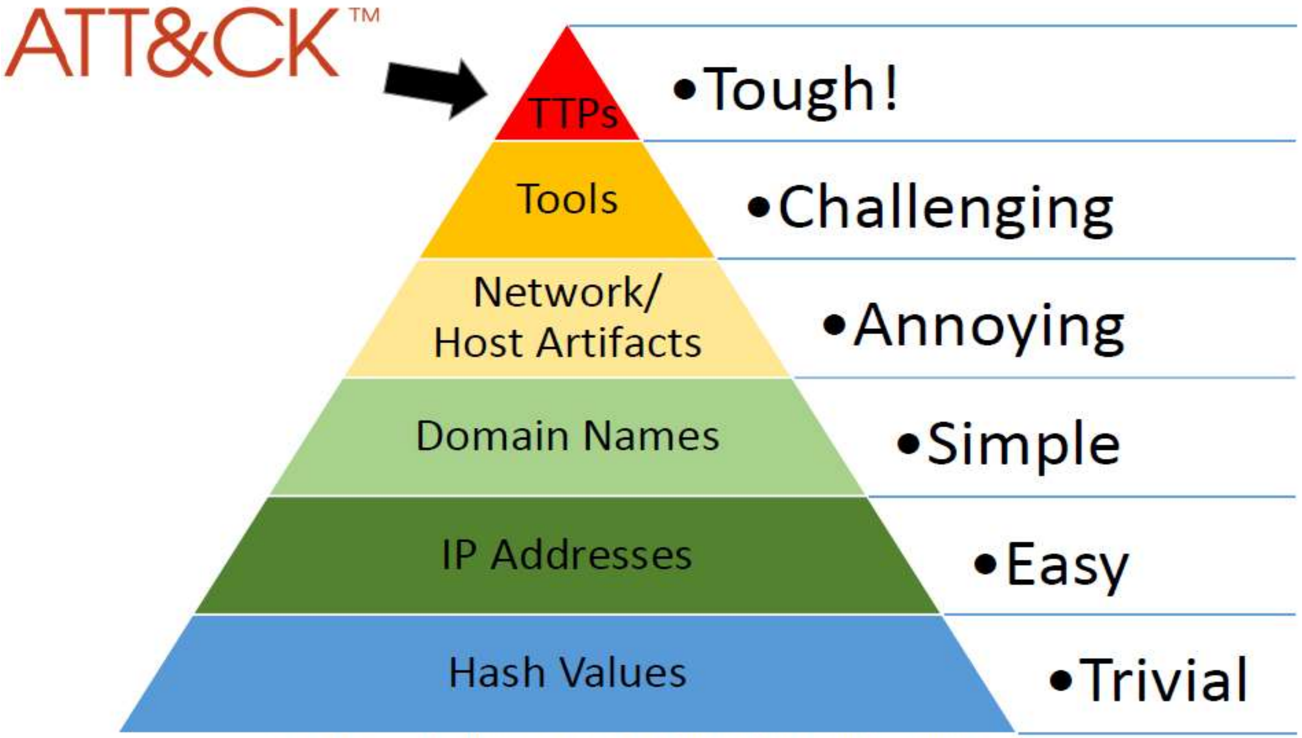
CHALLENGING QUESTIONS FOR DEFENDERS

- How effective are my defenses?
- Do I have a chance at detecting APT29 or APT28 or any other adversary group?
- Is the data I'm collecting useful?
- Do I have overlapping tool coverage?
- Will this new product/technology help my organization's defenses?
- How can I strategize my defences and strengthen the security posture?

WHAT IS MITRE ATT&CK ?

- ATT&CK is a knowledge base of cyber adversary behavior and taxonomy for adversarial actions across their lifecycle.
- ATT&CK has two parts:
- ATT&CK for Enterprise: which covers behavior against enterprise IT networks and cloud.
- ATT&CK for Mobile: which focuses on behavior against mobile devices.

DAVID BIANCO’S PYRAMID OF PAIN



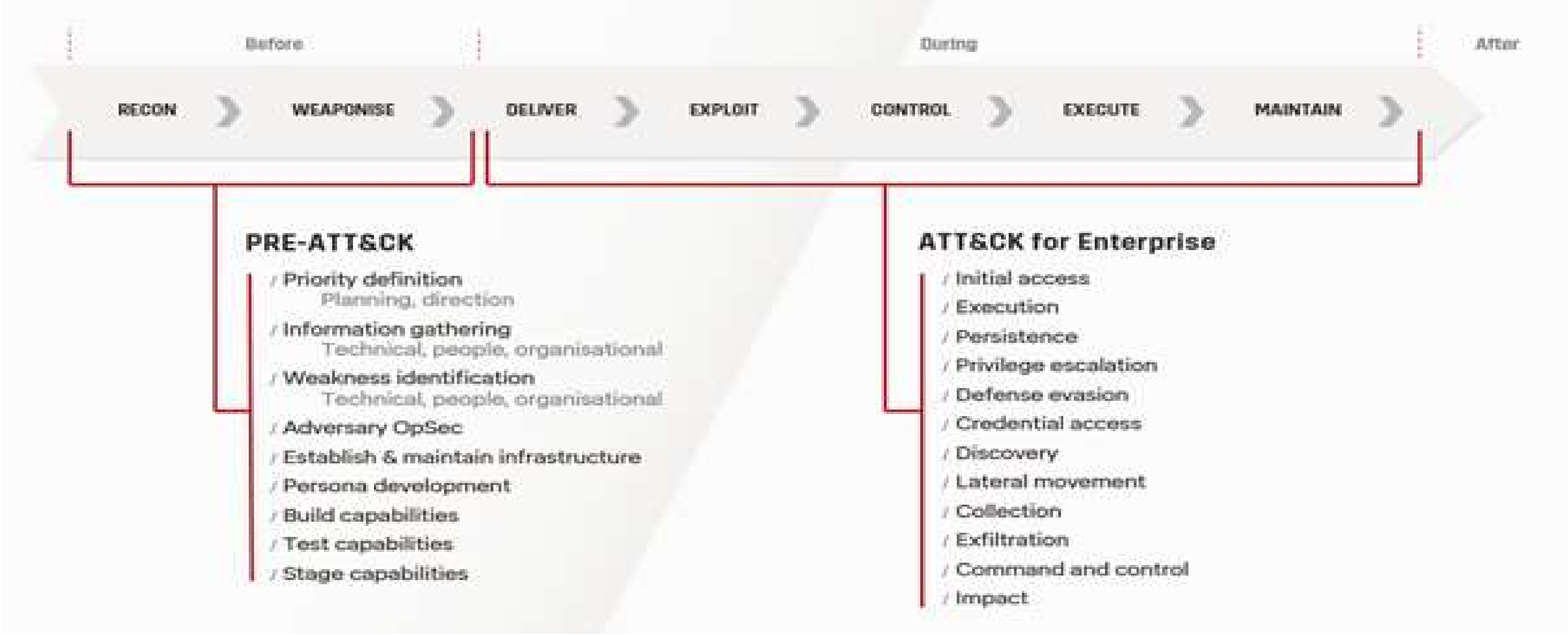
Source: David Bianco, https://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html

David Bianco’s Pyramid of Pain

WHY DID MITRE DEVELOP ATT&CK?

- MITRE started ATT&CK in 2013 to document common tactics, techniques, and procedures (TTPs)
- It was created out of a need to document adversary behaviors for use within a MITRE research project called FMX
- Investigate use of endpoint telemetry data and analytics to improve post-compromise detection of adversaries operating within enterprise networks
- ATT&CK was used as the basis for testing the efficacy of the sensors and analytics under FMX
- Served as the common language which both offense and defense could use to improve over time

OVERVIEW OF THE ADVERSARY LIFECYCLE



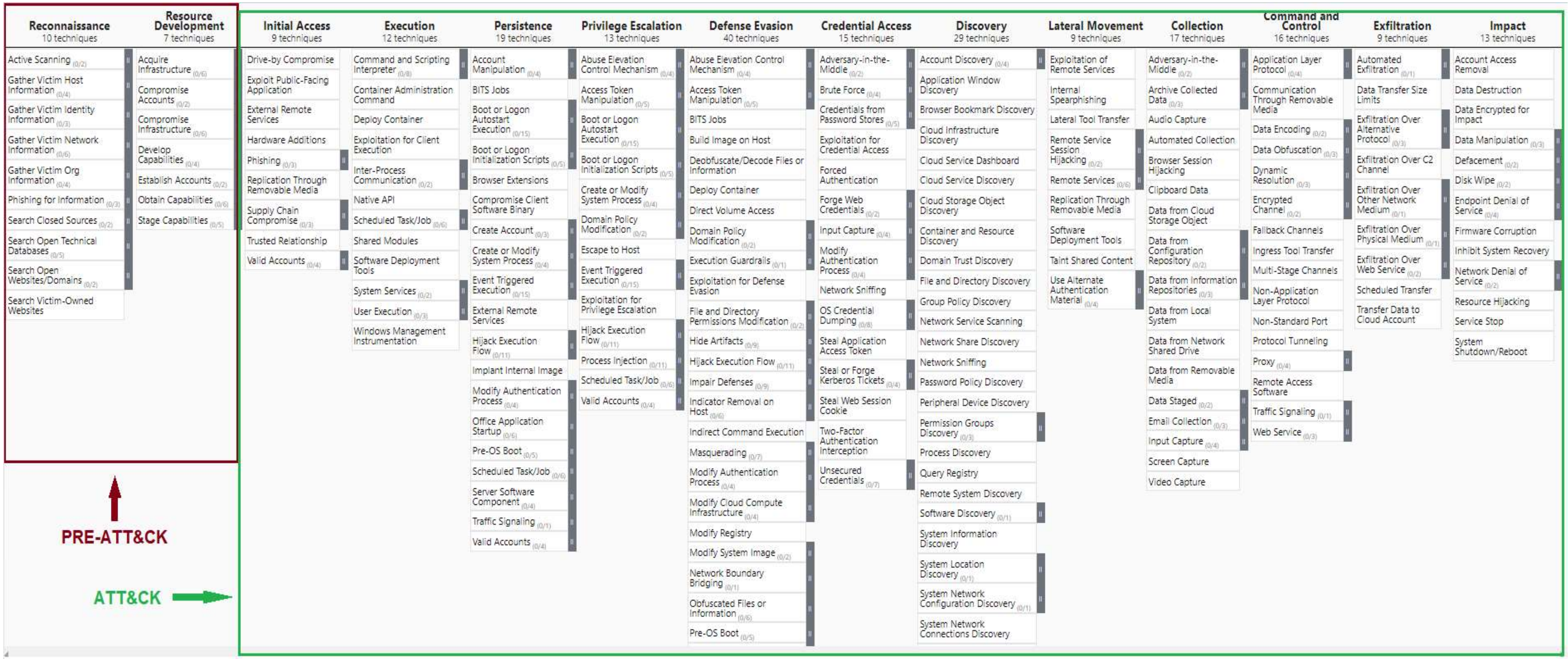
PRE-ATT&CK

- / Priority definition
  Planning, direction
- / Information gathering
  Technical, people, organisational
- / Weakness identification
  Technical, people, organisational
- / Adversary OpSec
- / Establish & maintain infrastructure
- / Persona development
- / Build capabilities
- / Test capabilities
- / Stage capabilities

ATT&CK for Enterprise

- / Initial access
- / Execution
- / Persistence
- / Privilege escalation
- / Defense evasion
- / Credential access
- / Discovery
- / Lateral movement
- / Collection
- / Exfiltration
- / Command and control
- / Impact

OVERVIEW OF THE ADVERSARY LIFECYCLE



Reconnaissance 10 techniques	Resource Development 7 techniques	Initial Access 9 techniques	Execution 12 techniques	Persistence 19 techniques	Privilege Escalation 13 techniques	Defense Evasion 40 techniques
Active Scanning (0/2)	Acquire Infrastructure (0/6)	Drive-by Compromise	Command and Scripting Interpreter (0/8)	Account Manipulation (0/4)	Abuse Elevation Control Mechanism (0/4)	Abuse Elevation Control Mechanism (0/4)
Gather Victim Host Information (0/4)	Compromise Accounts (0/2)	Exploit Public-Facing Application	Container Administration Command	BITS Jobs	Access Token Manipulation (0/5)	Access Token Manipulation (0/5)
Gather Victim Identity Information (0/3)	Compromise Infrastructure (0/6)	External Remote Services	Deploy Container	Boot or Logon Autostart Execution (0/15)	Boot or Logon Autostart Execution (0/15)	BITS Jobs
Gather Victim Network Information (0/6)	Develop Capabilities (0/4)	Hardware Additions	Exploitation for Client Execution	Boot or Logon Initialization Scripts (0/5)	Boot or Logon Initialization Scripts (0/5)	Build Image on Host
Gather Victim Org Information (0/4)	Establish Accounts (0/2)	Phishing (0/3)	Inter-Process Communication (0/2)	Browser Extensions	Create or Modify System Process (0/4)	Deobfuscate/Decode Files or Information
Phishing for Information (0/3)	Obtain Capabilities (0/6)	Replication Through Removable Media	Native API	Compromise Client Software Binary	Domain Policy Modification (0/2)	Deploy Container
Search Closed Sources (0/2)	Stage Capabilities (0/5)	Supply Chain Compromise (0/3)	Scheduled Task/Job (0/6)	Create Account (0/3)	Escape to Host	Direct Volume Access
Search Open Technical Databases (0/5)		Trusted Relationship	Shared Modules	Create or Modify System Process (0/4)	Event Triggered Execution (0/15)	Domain Policy Modification (0/2)
Search Open Websites/Domains (0/2)		Valid Accounts (0/4)	Software Deployment Tools	Event Triggered Execution (0/15)	Exploitation for Privilege Escalation	Execution Guardrails (0/1)
Search Victim-Owned Websites			System Services (0/2)	External Remote Services	Hijack Execution Flow (0/11)	Exploitation for Defense Evasion
			User Execution (0/3)	Hijack Execution Flow (0/11)	Process Injection (0/11)	File and Directory Permissions Modification (0/2)
			Windows Management Instrumentation	Implant Internal Image	Scheduled Task/Job (0/6)	Hide Artifacts (0/9)
				Modify Authentication Process (0/4)	Valid Accounts (0/4)	Hijack Execution Flow (0/11)
				Office Application Startup (0/6)		Impair Defenses (0/9)
				Pre-OS Boot (0/5)		Indicator Removal on Host (0/6)
				Scheduled Task/Job (0/6)		Indirect Command Execution
				Server Software Component (0/4)		Masquerading (0/7)
				Traffic Signaling (0/1)		Modify Authentication Process (0/4)
				Valid Accounts (0/4)		Modify Cloud Compute Infrastructure (0/4)
						Modify Registry
						Modify System Image (0/2)
						Network Boundary Bridging (0/1)
						Obfuscated Files or Information (0/6)
						Pre-OS Boot (0/5)

Credential Access 15 techniques	Discovery 29 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 16 techniques	Exfiltration 9 techniques	Impact 13 techniques
Adversary-in-the-Middle (0/2)	Account Discovery (0/4)	Exploitation of Remote Services	Adversary-in-the-Middle (0/2)	Application Layer Protocol (0/4)	Automated Exfiltration (0/1)	Account Access Removal
Brute Force (0/4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (0/3)	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Credentials from Password Stores (0/5)	Browser Bookmark Discovery	Lateral Tool Transfer	Audio Capture	Data Encoding (0/2)	Exfiltration Over Alternative Protocol (0/3)	Data Encrypted for Impact
Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (0/2)	Automated Collection	Data Obfuscation (0/3)	Exfiltration Over C2 Channel	Data Manipulation (0/3)
Forced Authentication	Cloud Service Dashboard	Remote Services (0/6)	Browser Session Hijacking	Dynamic Resolution (0/3)	Exfiltration Over Other Network Medium (0/1)	Defacement (0/2)
Forge Web Credentials (0/2)	Cloud Service Discovery	Replication Through Removable Media	Clipboard Data	Encrypted Channel (0/2)	Exfiltration Over Physical Medium (0/1)	Disk Wipe (0/2)
Input Capture (0/4)	Cloud Storage Object Discovery	Software Deployment Tools	Data from Cloud Storage Object	Fallback Channels	Exfiltration Over Web Service (0/2)	Endpoint Denial of Service (0/4)
Modify Authentication Process (0/4)	Container and Resource Discovery	Taint Shared Content	Data from Configuration Repository (0/2)	Ingress Tool Transfer	Scheduled Transfer	Firmware Corruption
Network Sniffing	Domain Trust Discovery	Use Alternate Authentication Material (0/4)	Data from Information Repositories (0/3)	Multi-Stage Channels	Transfer Data to Cloud Account	Inhibit System Recovery
OS Credential Dumping (0/8)	File and Directory Discovery		Data from Local System	Non-Application Layer Protocol		Network Denial of Service (0/2)
Steal Application Access Token	Group Policy Discovery		Data from Network Shared Drive	Non-Standard Port		Resource Hijacking
Steal or Forge Kerberos Tickets (0/4)	Network Service Scanning		Data from Removable Media	Protocol Tunneling		Service Stop
Steal Web Session Cookie	Network Share Discovery		Data Staged (0/2)	Proxy (0/4)		System Shutdown/Reboot
Two-Factor Authentication Interception	Network Sniffing		Email Collection (0/3)	Remote Access Software		
Unsecured Credentials (0/7)	Password Policy Discovery		Input Capture (0/4)	Traffic Signaling (0/1)		
	Peripheral Device Discovery		Screen Capture	Web Service (0/3)		
	Permission Groups Discovery (0/3)		Video Capture			
	Process Discovery					
	Query Registry					
	Remote System Discovery					
	Software Discovery (0/1)					
	System Information Discovery					
	System Location Discovery (0/1)					
	System Network Configuration Discovery (0/1)					
	System Network Connections Discovery					

WHAT ARE "TACTICS", "TECHNIQUES", "SUB-TECHNIQUES" AND "PROCEDURES"?

- **Tactics:**
  - Tactics represent the "why" of an ATT&CK technique or sub-technique
  - It is the adversary's tactical goal: the reason for performing an action
  - Example: An adversary may want to achieve credential access

- **Techniques:**
  - Techniques represent "how" an adversary achieves a tactical goal by performing an action
  - Example: an adversary may dump credentials to achieve credential access

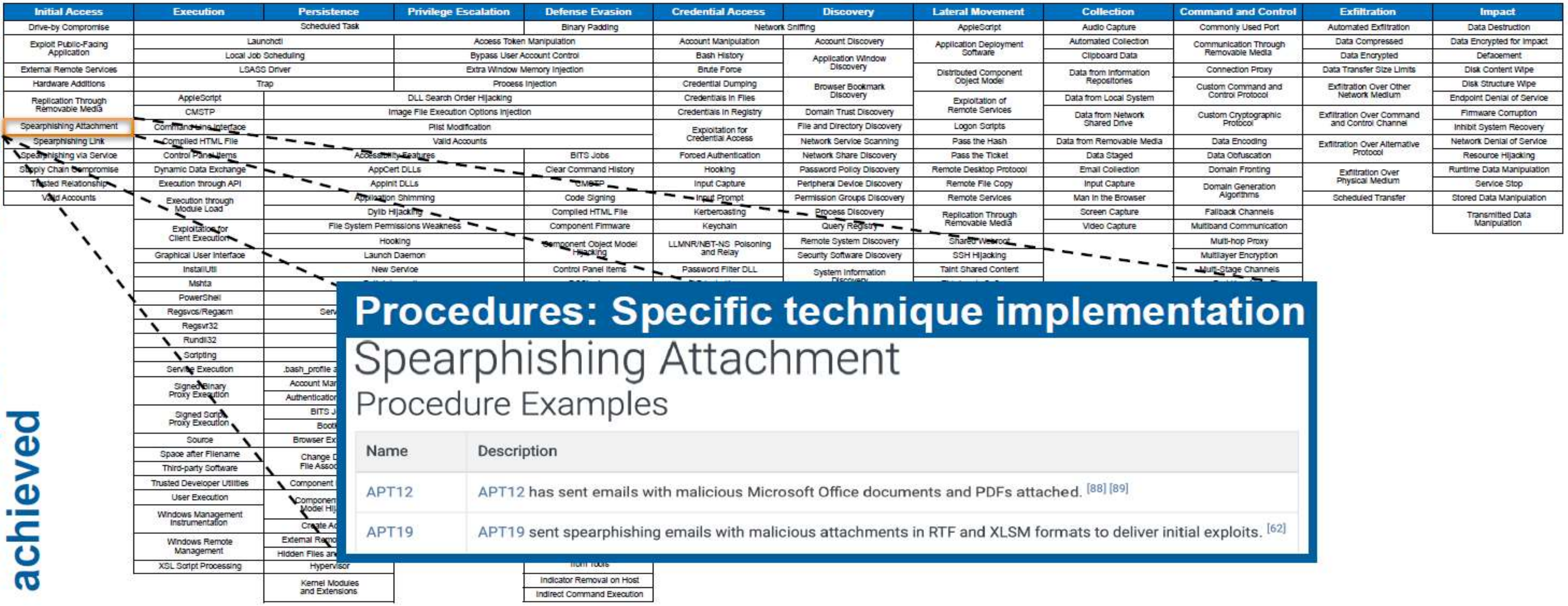
- **Sub-techniques:**
  - Sub-techniques are a more specific description of the adversarial behavior used to achieve a goal
  - They describe behavior at a lower level than a technique
  - Example: an adversary may dump credentials by accessing the Local Security Authority (LSA) Secrets

- **Procedures:**
  - Procedures are the specific implementation that the adversary uses for techniques or sub-techniques
  - These are categorized in ATT&CK as the observed in the wild use of techniques in the "Procedure Examples" section of technique pages

WHAT ARE "TACTICS", "TECHNIQUES", "SUB-TECHNIQUES" AND "PROCEDURES"?

Tactics: the adversary's technical goals

Techniques: how the goals are achieved



Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Drive-by Compromise	Scheduled Task			Binary Padding	Network Sniffing		AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Data Destruction
Exploit Public-Facing Application	Launchctl		Access Token Manipulation		Account Manipulation	Account Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed	Data Encrypted for Impact
	Local Job Scheduling		Bypass User Account Control		Bash History	Application Window Discovery		Clipboard Data		Data Encrypted	Defacement
External Remote Services	LSASS Driver		Extra Window Memory Injection		Brute Force		Distributed Component Object Model	Data from Information Repositories	Connection Proxy	Data Transfer Size Limits	Disk Content Wipe
Hardware Additions	Trap		Process Injection		Credential Dumping	Browser Bookmark Discovery			Custom Command and Control Protocol	Exfiltration Over Other Network Medium	Disk Structure Wipe
Replication Through Removable Media	AppleScript	DLL Search Order Hijacking			Credentials in Files		Exploitation of Remote Services	Data from Local System			Endpoint Denial of Service
	CMSTP	Image File Execution Options Injection			Credentials in Registry	Domain Trust Discovery		Data from Network Shared Drive	Custom Cryptographic Protocol	Exfiltration Over Command and Control Channel	Firmware Corruption
Spearphishing Attachment	Command-Line Interface	Plist Modification			Exploitation for Credential Access	File and Directory Discovery	Logon Scripts				Inhibit System Recovery
Spearphishing Link	Compiled HTML File	Valid Accounts				Network Service Scanning	Pass the Hash	Data from Removable Media	Data Encoding	Exfiltration Over Alternative Protocol	Network Denial of Service
Spearphishing via Service	Control Panel Items	Accessibility Features		BITS Jobs	Forced Authentication	Network Share Discovery	Pass the Ticket	Data Staged	Data Obfuscation		Resource Hijacking
Supply Chain Compromise	Dynamic Data Exchange	AppCert DLLs		Clear Command History	Hooking	Password Policy Discovery	Remote Desktop Protocol	Email Collection	Domain Fronting	Exfiltration Over Physical Medium	Runtime Data Manipulation
Trusted Relationship	Execution through API	AppInit DLLs		CMSTP	Input Capture	Peripheral Device Discovery	Remote File Copy	Input Capture	Domain Generation Algorithms		Service Stop
Valid Accounts	Execution through Module Load	Application Shimming		Code Signing	Input Prompt	Permission Groups Discovery	Remote Services	Man in the Browser		Scheduled Transfer	Stored Data Manipulation
		Dylib Hijacking		Compiled HTML File	Kerberoasting	Process Discovery	Replication Through Removable Media	Screen Capture	Fallback Channels		Transmitted Data Manipulation
	Exploitation for Client Execution	File System Permissions Weakness		Component Firmware	Keychain	Query Registry		Video Capture	Multiband Communication		
		Hooking		Component Object Model Hijacking	LLMNR/NBT-NS Poisoning and Relay	Remote System Discovery	Shared Webroot		Multi-hop Proxy		
	Graphical User Interface	Launch Daemon				Security Software Discovery	SSH Hijacking		Multilayer Encryption		
	InstallUtil	New Service		Control Panel Items	Password Filter DLL	System Information Discovery	Taint Shared Content		Multi-Stage Channels		
	Mshta										
	PowerShell										
	Regsvcs/Regasm	Serv									
	Regsvr32										
	Rundll32										
	Scripting										
	Service Execution	.bash_profile a									
	Signed Binary Proxy Execution	Account Mar									
		Authenticatio									
	Signed Script Proxy Execution	BITS J									
		Boot									
	Source	Browser Ex									
	Space after Filename	Change D File Assoc									
	Third-party Software										
	Trusted Developer Utilities	Component									
	User Execution	Componen Model Hij									
	Windows Management Instrumentation	Create Ac									
	Windows Remote Management	External Remo									
		Hidden Files an									
	XSL Script Processing	Hypervisor		from Tools							
		Kernel Modules and Extensions		Indicator Removal on Host							
				Indirect Command Execution							

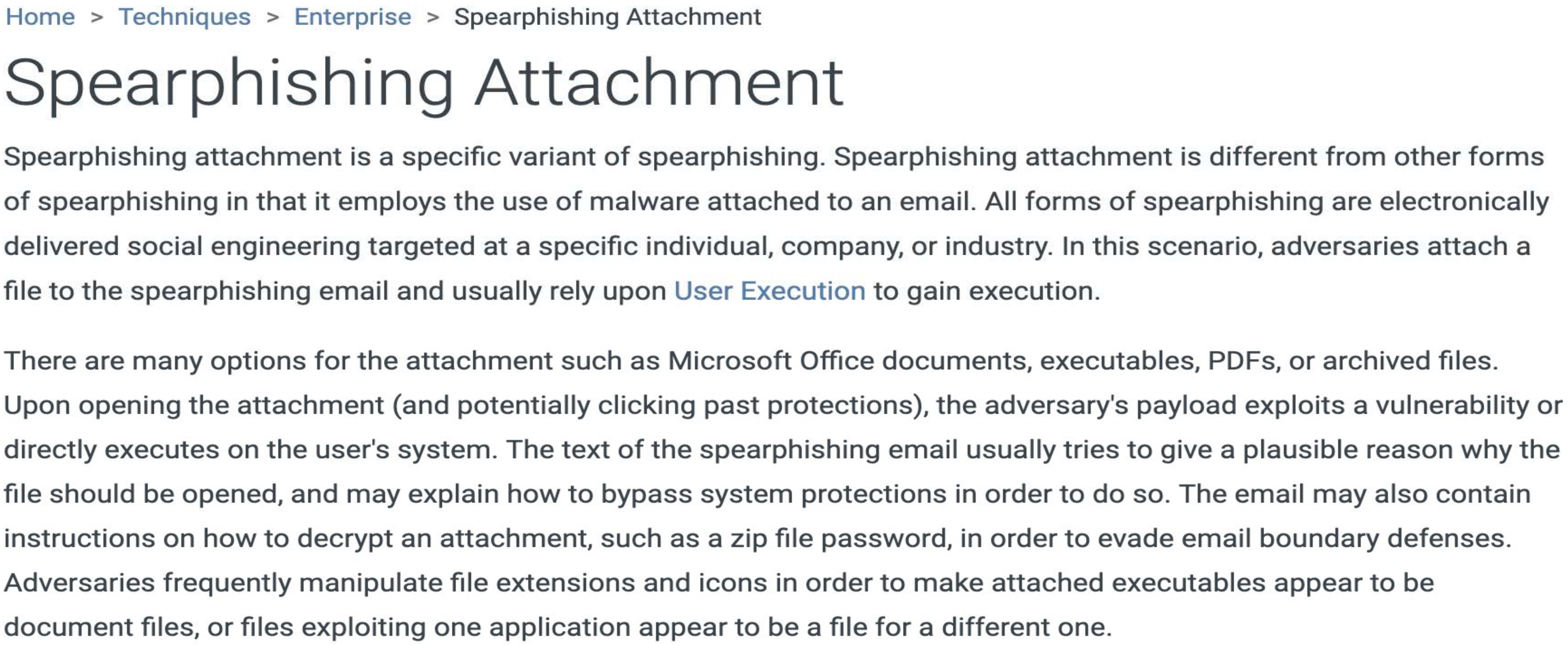
Procedures: Specific technique implementation

Spearphishing Attachment

Procedure Examples

Name	Description
APT12	APT12 has sent emails with malicious Microsoft Office documents and PDFs attached. [88] [89]
APT19	APT19 sent spearphishing emails with malicious attachments in RTF and XLSM formats to deliver initial exploits. [62]

TECHNIQUE: SPEARPHISHING ATTACHMENT



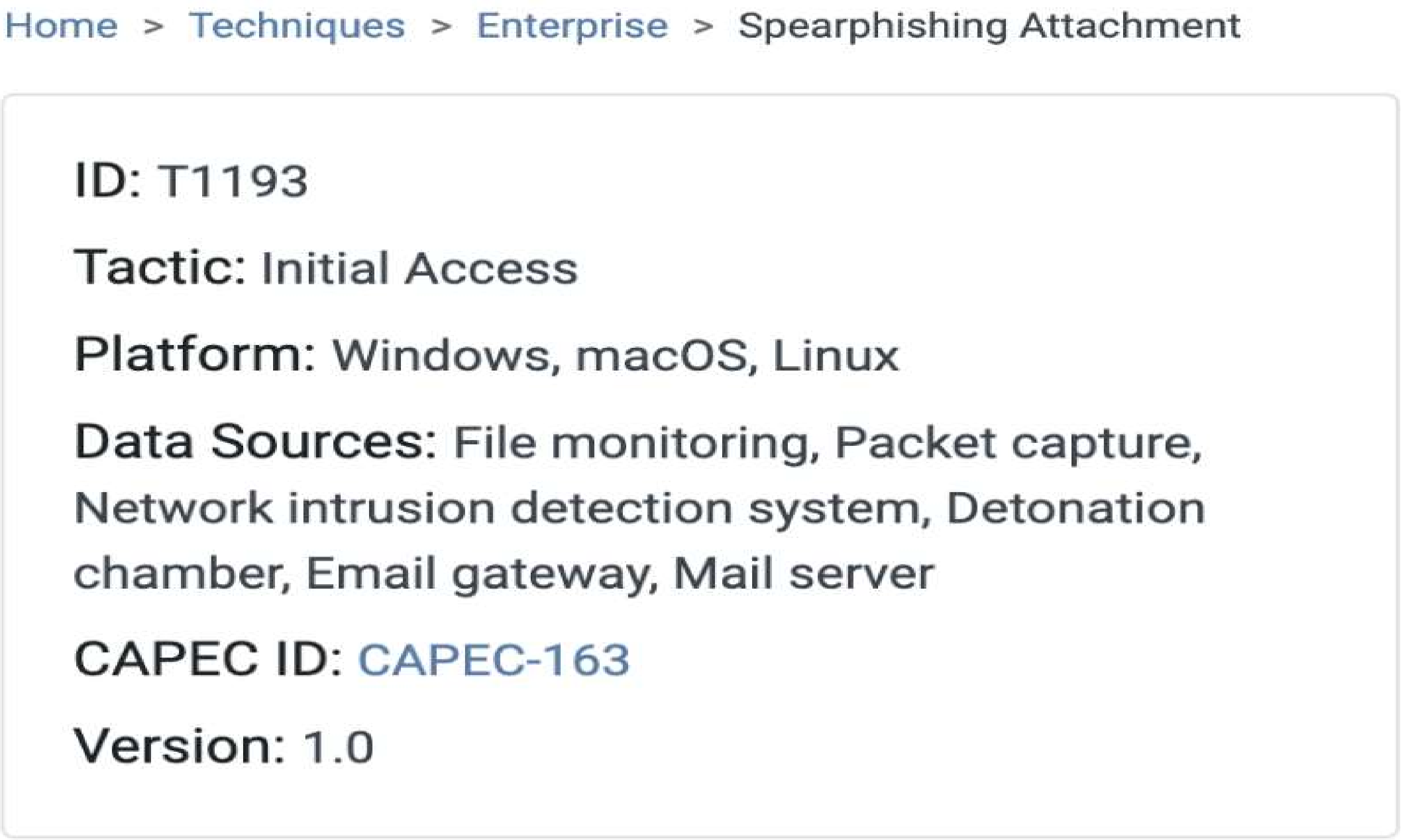
Home > Techniques > Enterprise > Spearphishing Attachment

Spearphishing Attachment

Spearphishing attachment is a specific variant of spearphishing. Spearphishing attachment is different from other forms of spearphishing in that it employs the use of malware attached to an email. All forms of spearphishing are electronically delivered social engineering targeted at a specific individual, company, or industry. In this scenario, adversaries attach a file to the spearphishing email and usually rely upon User Execution to gain execution.

There are many options for the attachment such as Microsoft Office documents, executables, PDFs, or archived files. Upon opening the attachment (and potentially clicking past protections), the adversary's payload exploits a vulnerability or directly executes on the user's system. The text of the spearphishing email usually tries to give a plausible reason why the file should be opened, and may explain how to bypass system protections in order to do so. The email may also contain instructions on how to decrypt an attachment, such as a zip file password, in order to evade email boundary defenses. Adversaries frequently manipulate file extensions and icons in order to make attached executables appear to be document files, or files exploiting one application appear to be a file for a different one.

TECHNIQUE: SPEARPHISHING ATTACHMENT



Home > Techniques > Enterprise > Spearphishing Attachment

ID: T1193

Tactic: Initial Access

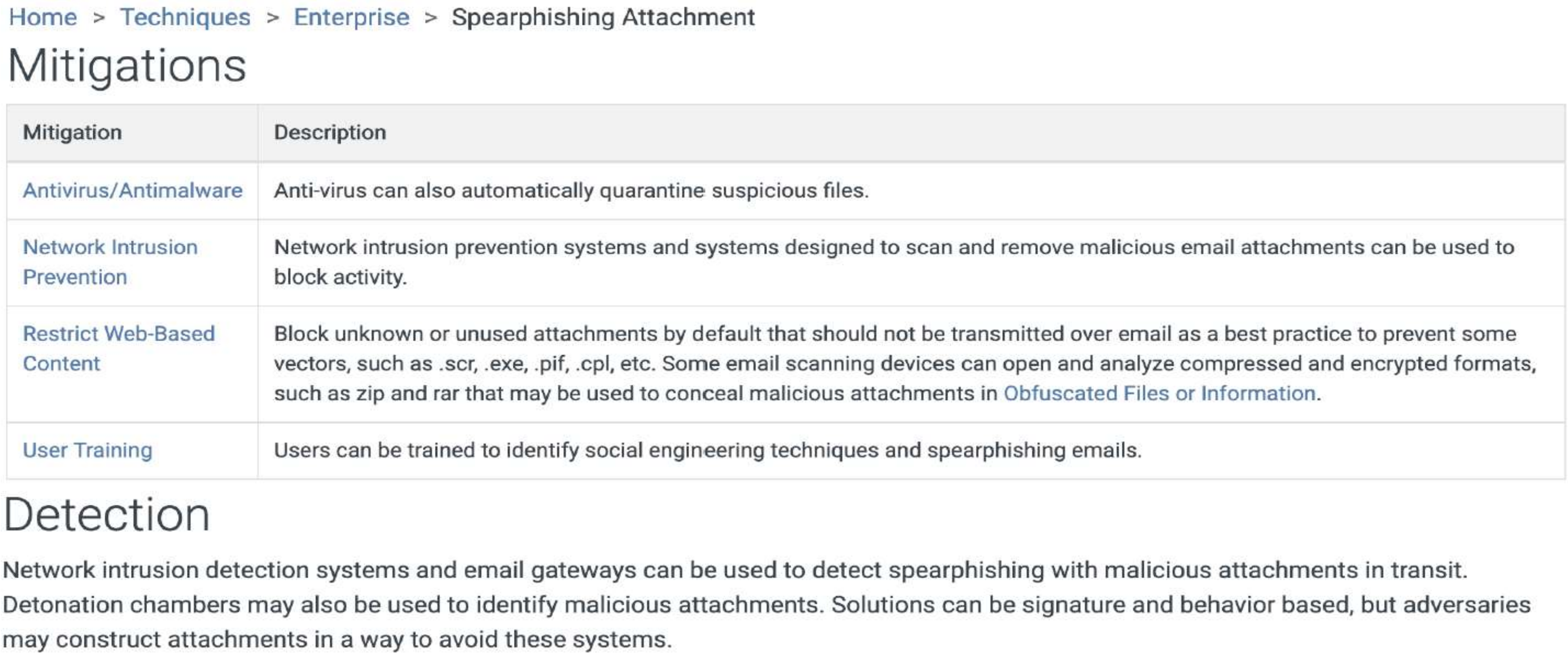
Platform: Windows, macOS, Linux

Data Sources: File monitoring, Packet capture, Network intrusion detection system, Detonation chamber, Email gateway, Mail server

CAPEC ID: CAPEC-163

Version: 1.0

TECHNIQUE: SPEARPHISHING ATTACHMENT



Home > Techniques > Enterprise > Spearphishing Attachment

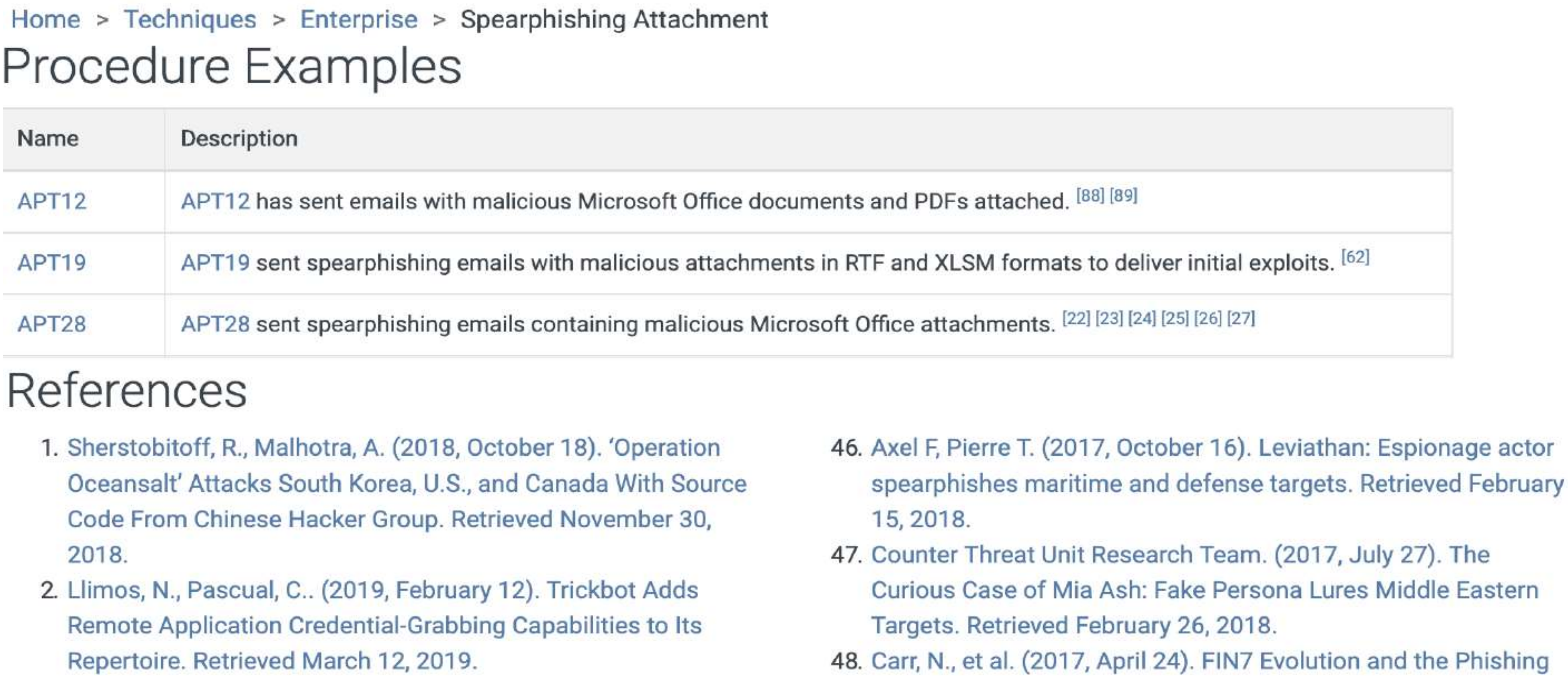
Mitigations

Mitigation	Description
Antivirus/Antimalware	Anti-virus can also automatically quarantine suspicious files.
Network Intrusion Prevention	Network intrusion prevention systems and systems designed to scan and remove malicious email attachments can be used to block activity.
Restrict Web-Based Content	Block unknown or unused attachments by default that should not be transmitted over email as a best practice to prevent some vectors, such as .scr, .exe, .pif, .cpl, etc. Some email scanning devices can open and analyze compressed and encrypted formats, such as zip and rar that may be used to conceal malicious attachments in Obfuscated Files or Information.
User Training	Users can be trained to identify social engineering techniques and spearphishing emails.

Detection

Network intrusion detection systems and email gateways can be used to detect spearphishing with malicious attachments in transit. Detonation chambers may also be used to identify malicious attachments. Solutions can be signature and behavior based, but adversaries may construct attachments in a way to avoid these systems.

TECHNIQUE: SPEARPHISHING ATTACHMENT



Home > Techniques > Enterprise > Spearphishing Attachment

Procedure Examples

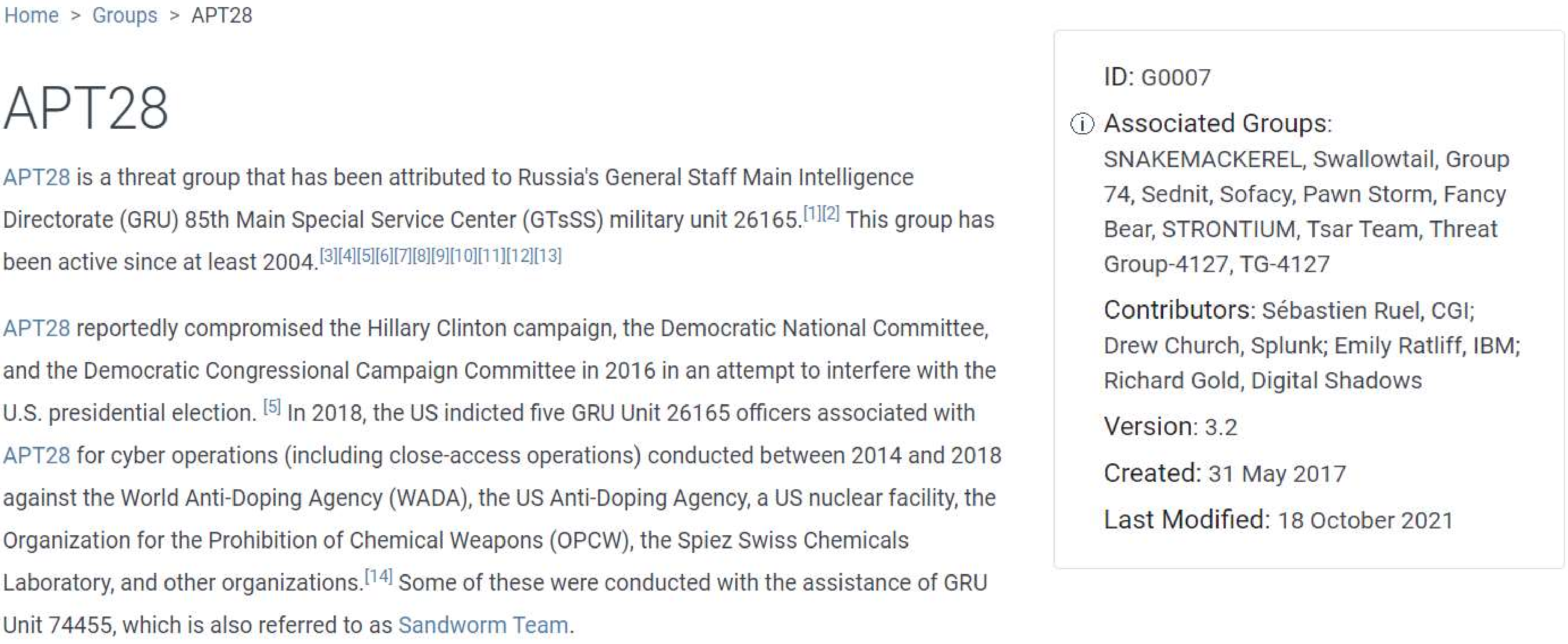
Name	Description
APT12	APT12 has sent emails with malicious Microsoft Office documents and PDFs attached. [88] [89]
APT19	APT19 sent spearphishing emails with malicious attachments in RTF and XLSM formats to deliver initial exploits. [62]
APT28	APT28 sent spearphishing emails containing malicious Microsoft Office attachments. [22] [23] [24] [25] [26] [27]

References

1. Sherstobitoff, R., Malhotra, A. (2018, October 18). 'Operation Oceansalt' Attacks South Korea, U.S., and Canada With Source Code From Chinese Hacker Group. Retrieved November 30, 2018.
2. Llimos, N., Pascual, C.. (2019, February 12). Trickbot Adds Remote Application Credential-Grabbing Capabilities to Its Repertoire. Retrieved March 12, 2019.

46. Axel F, Pierre T. (2017, October 16). Leviathan: Espionage actor spearphishes maritime and defense targets. Retrieved February 15, 2018.
47. Counter Threat Unit Research Team. (2017, July 27). The Curious Case of Mia Ash: Fake Persona Lures Middle Eastern Targets. Retrieved February 26, 2018.
48. Carr, N., et al. (2017, April 24). FIN7 Evolution and the Phishing

GROUP: APT28



Home > Groups > APT28

APT28

APT28 is a threat group that has been attributed to Russia's General Staff Main Intelligence Directorate (GRU) 85th Main Special Service Center (GTsSS) military unit 26165.[1][2] This group has been active since at least 2004.[3][4][5][6][7][8][9][10][11][12][13]

APT28 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. [5] In 2018, the US indicted five GRU Unit 26165 officers associated with APT28 for cyber operations (including close-access operations) conducted between 2014 and 2018 against the World Anti-Doping Agency (WADA), the US Anti-Doping Agency, a US nuclear facility, the Organization for the Prohibition of Chemical Weapons (OPCW), the Spiez Swiss Chemicals Laboratory, and other organizations.[14] Some of these were conducted with the assistance of GRU Unit 74455, which is also referred to as Sandworm Team.

ID: G0007

ⓘ Associated Groups: SNAKEMACKEREL, Swallowtail, Group 74, Sednit, Sofacy, Pawn Storm, Fancy Bear, STRONTIUM, Tsar Team, Threat Group-4127, TG-4127

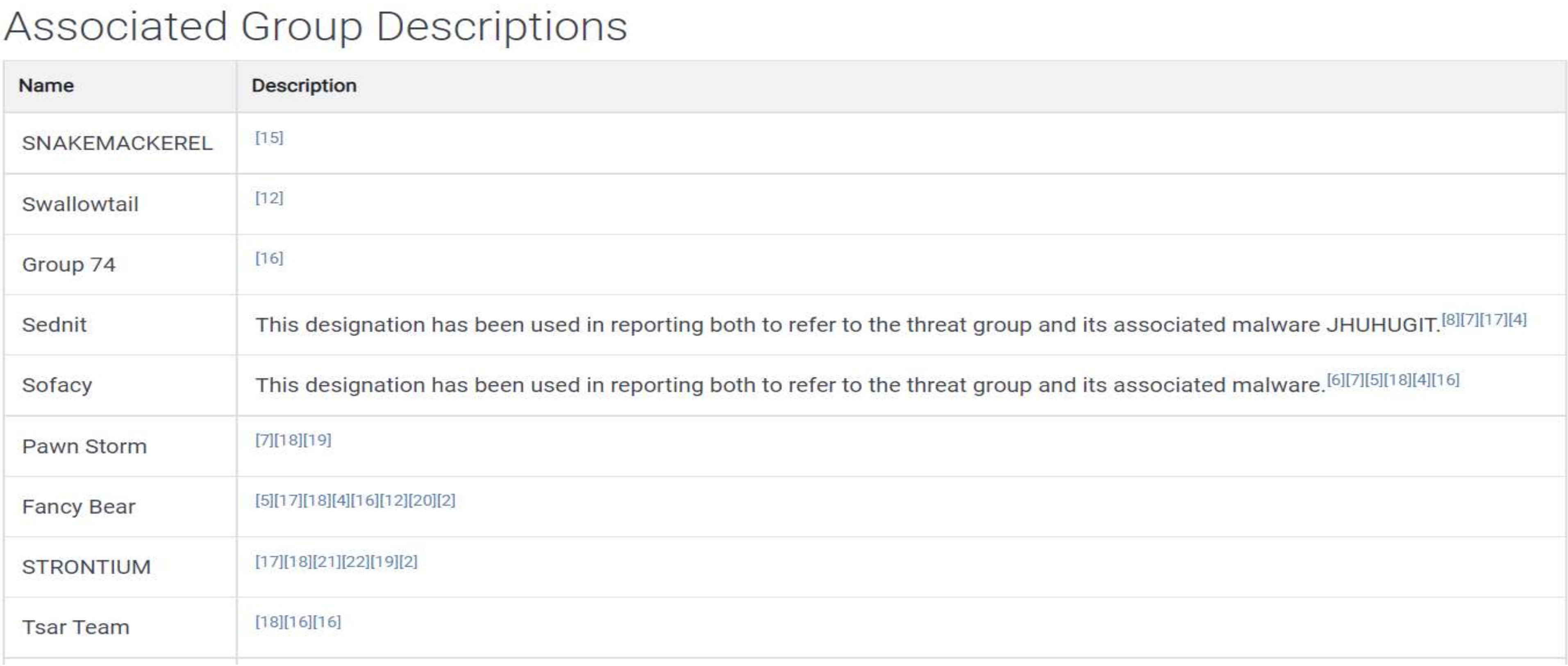
Contributors: Sébastien Ruel, CGI; Drew Church, Splunk; Emily Ratliff, IBM; Richard Gold, Digital Shadows

Version: 3.2

Created: 31 May 2017

Last Modified: 18 October 2021

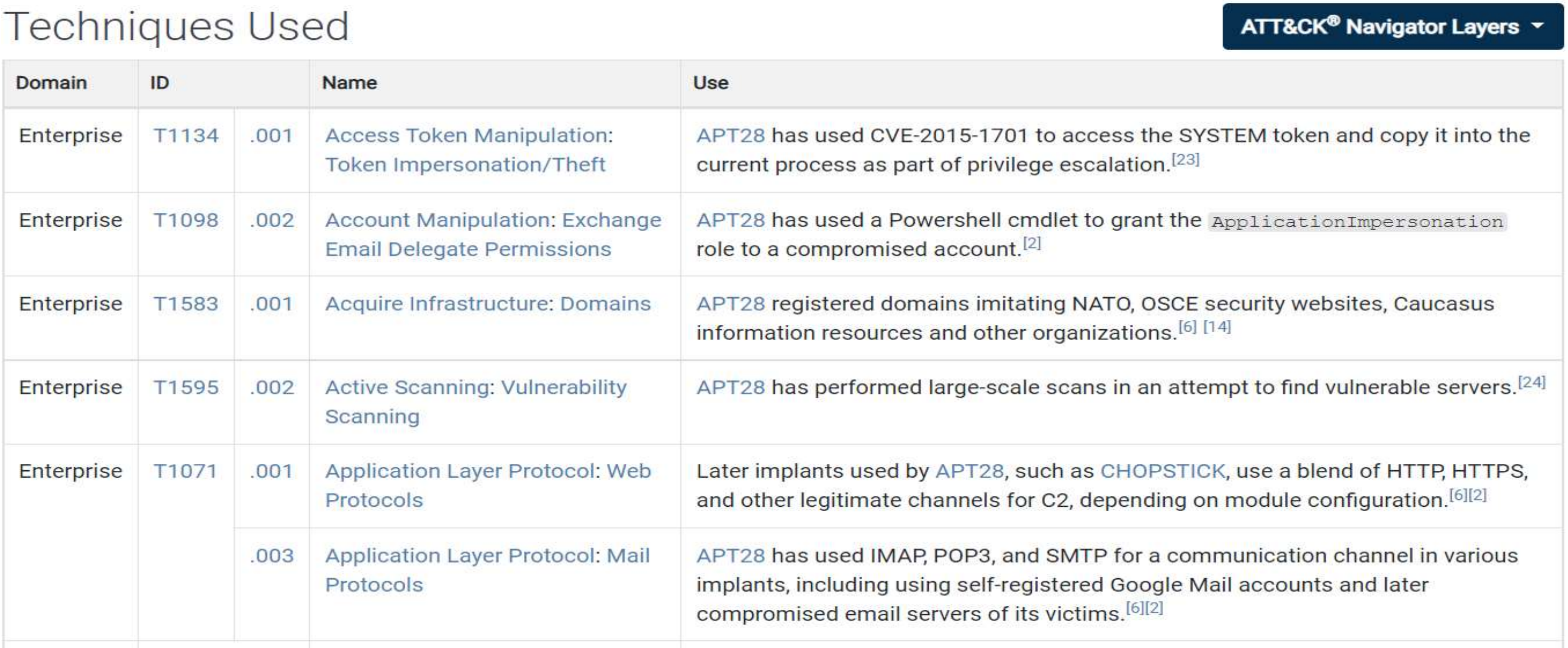
GROUP: APT28



Associated Group Descriptions

Name	Description
SNAKEMACKEREL	[15]
Swallowtail	[12]
Group 74	[16]
Sednit	This designation has been used in reporting both to refer to the threat group and its associated malware JHUHUGIT.[8][7][17][4]
Sofacy	This designation has been used in reporting both to refer to the threat group and its associated malware.[6][7][5][18][4][16]
Pawn Storm	[7][18][19]
Fancy Bear	[5][17][18][4][16][12][20][2]
STRONTIUM	[17][18][21][22][19][2]
Tsar Team	[18][16][16]

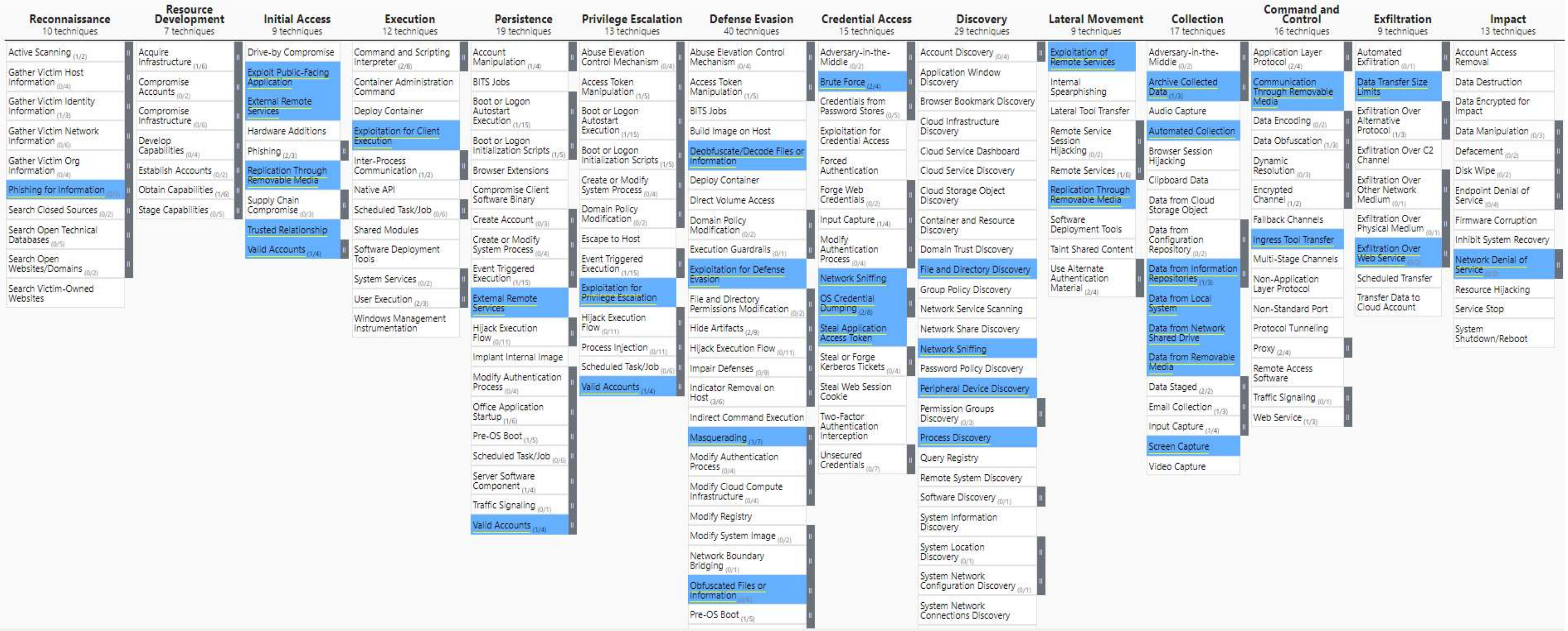
GROUP: APT28



Techniques Used

Domain	ID		Name	Use
Enterprise	T1134	.001	Access Token Manipulation: Token Impersonation/Theft	APT28 has used CVE-2015-1701 to access the SYSTEM token and copy it into the current process as part of privilege escalation.[23]
Enterprise	T1098	.002	Account Manipulation: Exchange Email Delegate Permissions	APT28 has used a Powershell cmdlet to grant the `ApplicationImpersonation` role to a compromised account.[2]
Enterprise	T1583	.001	Acquire Infrastructure: Domains	APT28 registered domains imitating NATO, OSCE security websites, Caucasus information resources and other organizations.[6] [14]
Enterprise	T1595	.002	Active Scanning: Vulnerability Scanning	APT28 has performed large-scale scans in an attempt to find vulnerable servers.[24]
Enterprise	T1071	.001	Application Layer Protocol: Web Protocols	Later implants used by APT28, such as CHOPSTICK, use a blend of HTTP, HTTPS, and other legitimate channels for C2, depending on module configuration.[6][2]
		.003	Application Layer Protocol: Mail Protocols	APT28 has used IMAP, POP3, and SMTP for a communication channel in various implants, including using self-registered Google Mail accounts and later compromised email servers of its victims.[6][2]

GROUP: APT28



Reconnaissance
10 techniques

- Active Scanning (1/2)
- Gather Victim Host Information (0/4)
- Gather Victim Identity Information (1/3)
- Gather Victim Network Information (0/6)
- Gather Victim Org Information (0/4)
- Phishing for Information (0/3)
- Search Closed Sources (0/2)
- Search Open Technical Databases (0/5)
- Search Open Websites/Domains (0/2)
- Search Victim-Owned Websites

Resource Development
7 techniques

- Acquire Infrastructure (1/6)
- Compromise Accounts (0/2)
- Compromise Infrastructure (0/6)
- Develop Capabilities (0/4)
- Establish Accounts (0/2)
- Obtain Capabilities (1/6)
- Stage Capabilities (0/5)

Initial Access
9 techniques

- Drive-by Compromise
- Exploit Public-Facing Application
- External Remote Services
- Hardware Additions
- Phishing (2/3)
- Replication Through Removable Media
- Supply Chain Compromise (0/3)
- Trusted Relationship
- Valid Accounts (1/4)

Execution
12 techniques

- Command and Scripting Interpreter (2/8)
- Container Administration Command
- Deploy Container
- Exploitation for Client Execution
- Inter-Process Communication (1/2)
- Native API
- Scheduled Task/Job (0/6)
- Shared Modules
- Software Deployment Tools
- System Services (0/2)
- User Execution (2/3)
- Windows Management Instrumentation

Persistence
19 techniques

- Account Manipulation (1/4)
- BITS Jobs
- Boot or Logon Autostart Execution (1/15)
- Boot or Logon Initialization Scripts (1/5)
- Browser Extensions
- Compromise Client Software Binary
- Create Account (0/3)
- Create or Modify System Process (0/4)
- Event Triggered Execution (1/15)
- External Remote Services
- Hijack Execution Flow (0/11)
- Implant Internal Image
- Modify Authentication Process (0/4)
- Office Application Startup (1/6)
- Pre-OS Boot (1/5)
- Scheduled Task/Job (0/6)
- Server Software Component (1/4)
- Traffic Signaling (0/1)
- Valid Accounts (1/4)

Privilege Escalation
13 techniques

- Abuse Elevation Control Mechanism (0/4)
- Access Token Manipulation (1/5)
- Boot or Logon Autostart Execution (1/15)
- Boot or Logon Initialization Scripts (1/5)
- Create or Modify System Process (0/4)
- Domain Policy Modification (0/2)
- Escape to Host
- Event Triggered Execution (1/15)
- Exploitation for Privilege Escalation
- Hijack Execution Flow (0/11)
- Process Injection (0/11)
- Scheduled Task/Job (0/6)
- Valid Accounts (1/4)

Defense Evasion
40 techniques

- Abuse Elevation Control Mechanism (0/4)
- Access Token Manipulation (1/5)
- BITS Jobs
- Build Image on Host
- Deobfuscate/Decode Files or Information
- Deploy Container
- Direct Volume Access
- Domain Policy Modification (0/2)
- Execution Guardrails (0/1)
- Exploitation for Defense Evasion
- File and Directory Permissions Modification (0/2)
- Hide Artifacts (2/9)
- Hijack Execution Flow (0/11)
- Impair Defenses (0/9)
- Indicator Removal on Host (3/6)
- Indirect Command Execution
- Masquerading (1/7)
- Modify Authentication Process (0/4)
- Modify Cloud Compute Infrastructure (0/4)
- Modify Registry
- Modify System Image (0/2)
- Network Boundary Bridging (0/1)
- Obfuscated Files or Information [illegible]
- Pre-OS Boot (1/5)

Credential Access
15 techniques

- Adversary-in-the-Middle (0/2)
- Brute Force (2/4)
- Credentials from Password Stores (0/5)
- Exploitation for Credential Access
- Forced Authentication
- Forge Web Credentials (0/2)
- Input Capture (1/4)
- Modify Authentication Process (0/4)
- Network Sniffing
- OS Credential Dumping (2/8)
- Steal Application Access Token
- Steal or Forge Kerberos Tickets (0/4)
- Steal Web Session Cookie
- Two-Factor Authentication Interception
- Unsecured Credentials (0/7)

Discovery
29 techniques

- Account Discovery (0/4)
- Application Window Discovery
- Browser Bookmark Discovery
- Cloud Infrastructure Discovery
- Cloud Service Dashboard
- Cloud Service Discovery
- Cloud Storage Object Discovery
- Container and Resource Discovery
- Domain Trust Discovery
- File and Directory Discovery
- Group Policy Discovery
- Network Service Scanning
- Network Share Discovery
- Network Sniffing
- Password Policy Discovery
- Peripheral Device Discovery
- Permission Groups Discovery (0/3)
- Process Discovery
- Query Registry
- Remote System Discovery
- Software Discovery (0/1)
- System Information Discovery
- System Location Discovery (0/1)
- System Network Configuration Discovery (0/1)
- System Network Connections Discovery

Lateral Movement
9 techniques

- Exploitation of Remote Services
- Internal Spearphishing
- Lateral Tool Transfer
- Remote Service Session Hijacking (0/2)
- Remote Services (1/6)
- Replication Through Removable Media
- Software Deployment Tools
- Taint Shared Content
- Use Alternate Authentication Material (2/4)

Collection
17 techniques

- Adversary-in-the-Middle (0/2)
- Archive Collected Data (1/3)
- Audio Capture
- Automated Collection
- Browser Session Hijacking
- Clipboard Data
- Data from Cloud Storage Object
- Data from Configuration Repository (0/2)
- Data from Information Repositories (1/3)
- Data from Local System
- Data from Network Shared Drive
- Data from Removable Media
- Data Staged (2/2)
- Email Collection (1/3)
- Input Capture (1/4)
- Screen Capture
- Video Capture

Command and Control
16 techniques

- Application Layer Protocol (2/4)
- Communication Through Removable Media
- Data Encoding (0/2)
- Data Obfuscation (1/3)
- Dynamic Resolution (0/3)
- Encrypted Channel (1/2)
- Fallback Channels
- Ingress Tool Transfer
- Multi-Stage Channels
- Non-Application Layer Protocol
- Non-Standard Port
- Protocol Tunneling
- Proxy (2/4)
- Remote Access Software
- Traffic Signaling (0/1)
- Web Service (1/3)

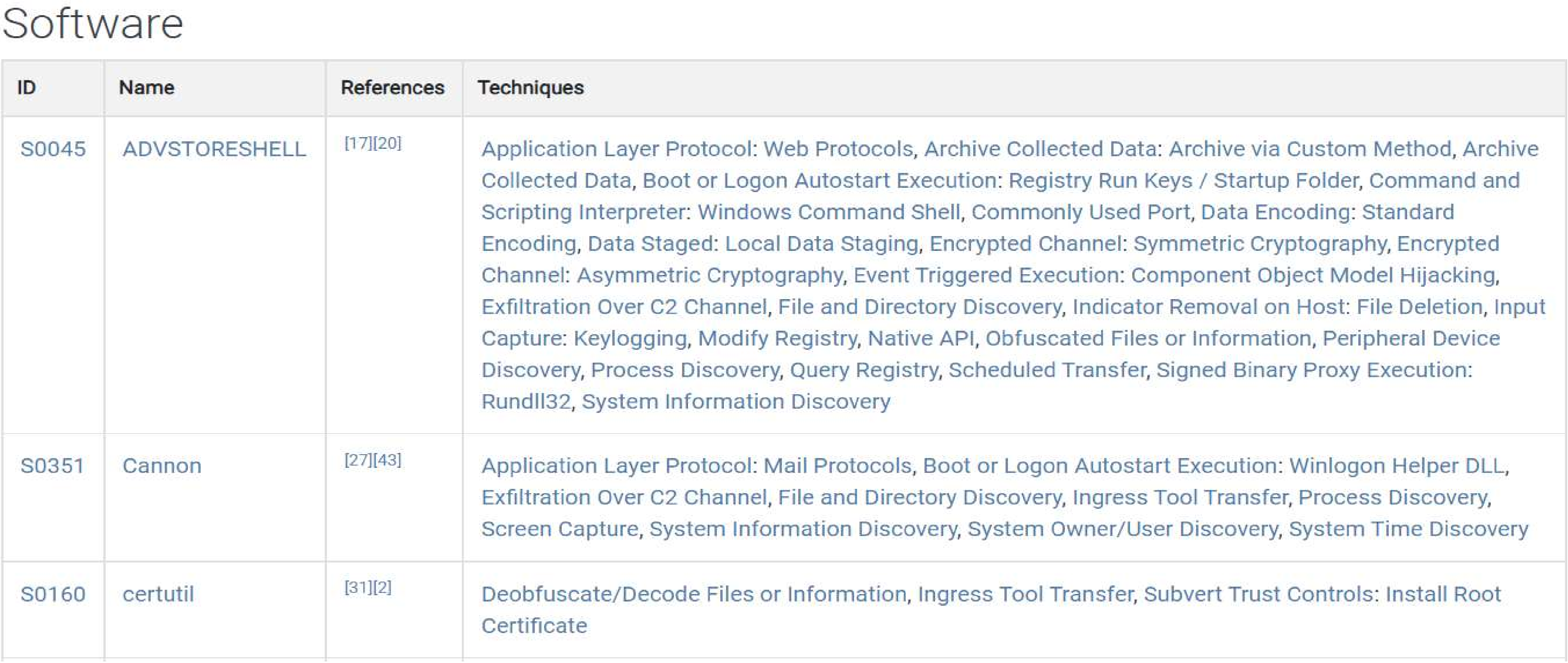
Exfiltration
9 techniques

- Automated Exfiltration (0/1)
- Data Transfer Size Limits
- Exfiltration Over Alternative Protocol (1/3)
- Exfiltration Over C2 Channel
- Exfiltration Over Other Network Medium (0/1)
- Exfiltration Over Physical Medium (0/1)
- Exfiltration Over Web Service (0/2)
- Scheduled Transfer
- Transfer Data to Cloud Account

Impact
13 techniques

- Account Access Removal
- Data Destruction
- Data Encrypted for Impact
- Data Manipulation (0/3)
- Defacement (0/2)
- Disk Wipe (0/2)
- Endpoint Denial of Service (0/4)
- Firmware Corruption
- Inhibit System Recovery
- Network Denial of Service (0/2)
- Resource Hijacking
- Service Stop
- System Shutdown/Reboot

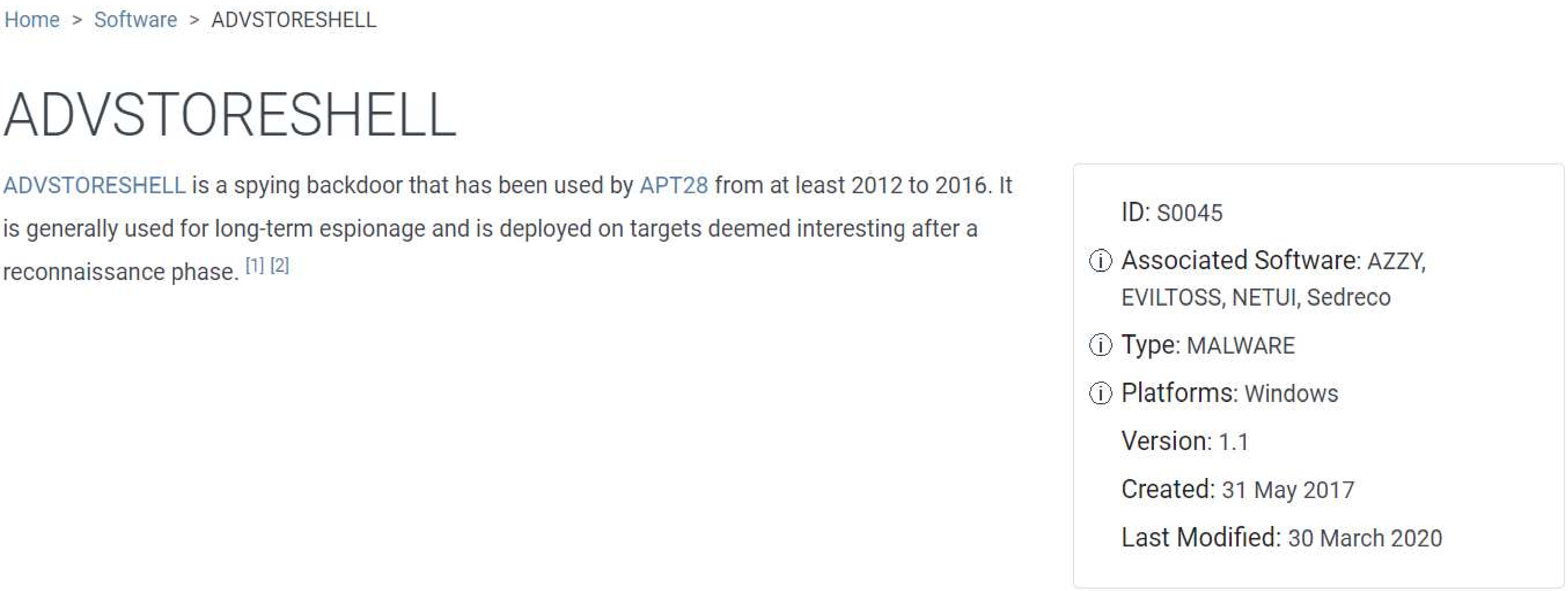
GROUP: APT28



Software

ID	Name	References	Techniques
S0045	ADVSTORESHELL	[17][20]	Application Layer Protocol: Web Protocols, Archive Collected Data: Archive via Custom Method, Archive Collected Data, Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder, Command and Scripting Interpreter: Windows Command Shell, Commonly Used Port, Data Encoding: Standard Encoding, Data Staged: Local Data Staging, Encrypted Channel: Symmetric Cryptography, Encrypted Channel: Asymmetric Cryptography, Event Triggered Execution: Component Object Model Hijacking, Exfiltration Over C2 Channel, File and Directory Discovery, Indicator Removal on Host: File Deletion, Input Capture: Keylogging, Modify Registry, Native API, Obfuscated Files or Information, Peripheral Device Discovery, Process Discovery, Query Registry, Scheduled Transfer, Signed Binary Proxy Execution: Rundll32, System Information Discovery
S0351	Cannon	[27][43]	Application Layer Protocol: Mail Protocols, Boot or Logon Autostart Execution: Winlogon Helper DLL, Exfiltration Over C2 Channel, File and Directory Discovery, Ingress Tool Transfer, Process Discovery, Screen Capture, System Information Discovery, System Owner/User Discovery, System Time Discovery
S0160	certutil	[31][2]	Deobfuscate/Decode Files or Information, Ingress Tool Transfer, Subvert Trust Controls: Install Root Certificate

GROUP: APT28



Home > Software > ADVSTORESHELL

ADVSTORESHELL

ADVSTORESHELL is a spying backdoor that has been used by APT28 from at least 2012 to 2016. It is generally used for long-term espionage and is deployed on targets deemed interesting after a reconnaissance phase. [1] [2]

ID: S0045

ⓘ Associated Software: AZZY, EVILTOSS, NETUI, Sedreco

ⓘ Type: MALWARE

ⓘ Platforms: Windows

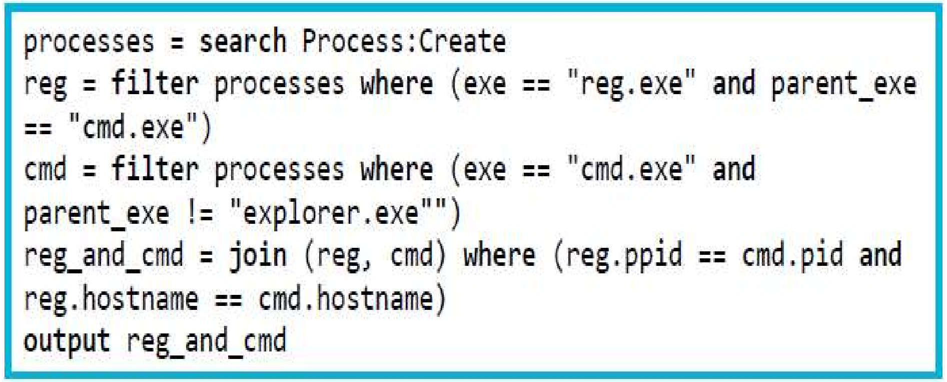
Version: 1.1

Created: 31 May 2017

Last Modified: 30 March 2020

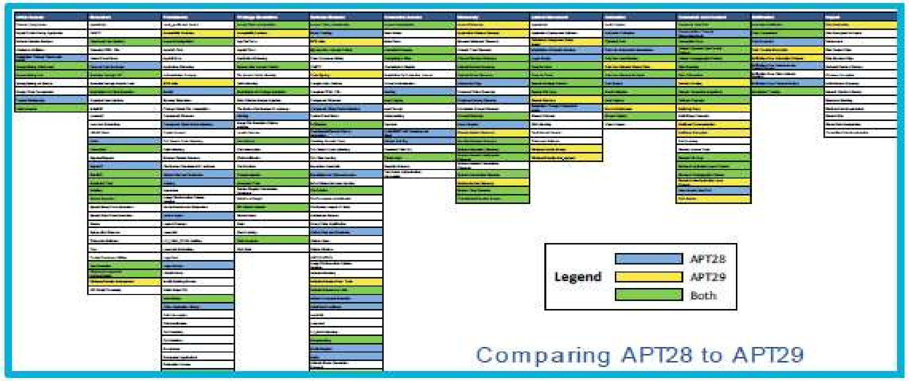
ATT&CK USE CASES

- **Detection**



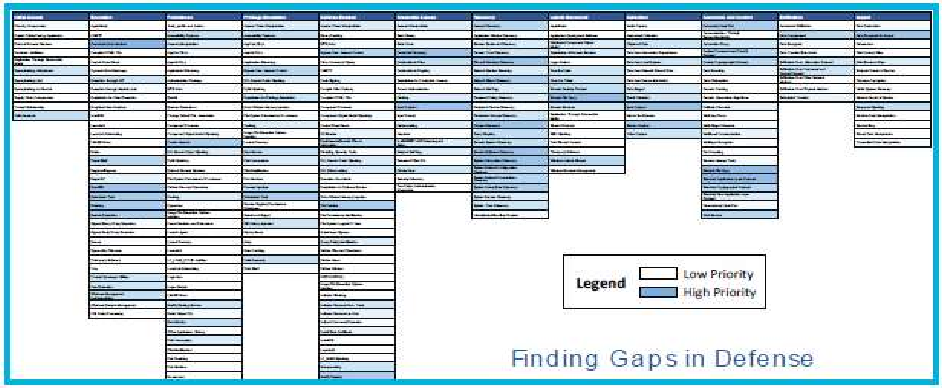
```
processes = search Process:Create
reg = filter processes where (exe == "reg.exe" and parent_exe
== "cmd.exe")
cmd = filter processes where (exe == "cmd.exe" and
parent_exe != "explorer.exe"")
reg_and_cmd = join (reg, cmd) where (reg.ppid == cmd.pid and
reg.hostname == cmd.hostname)
output reg_and_cmd
```

- **Threat Intelligence**


Legend
🟦 APT28
🟨 APT29
🟩 Both

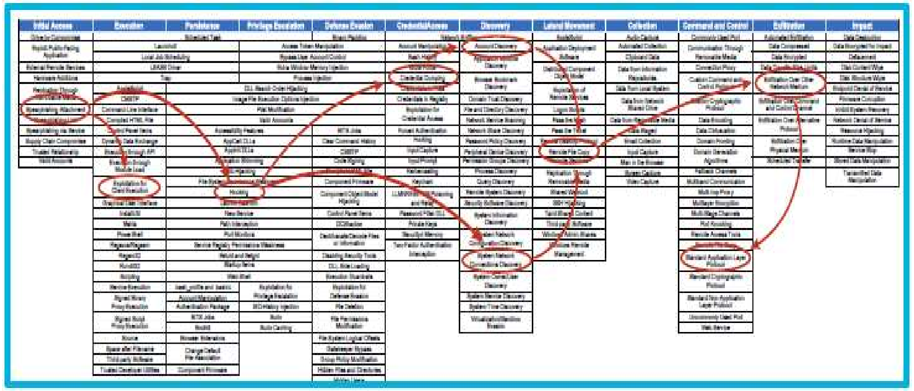
Comparing APT28 to APT29

- **Assessment and Engineering**


Legend
□ Low Priority
🟦 High Priority

Finding Gaps in Defense

- **Adversary Emulation**



DETECTION: FIND THE BEHAVIOR

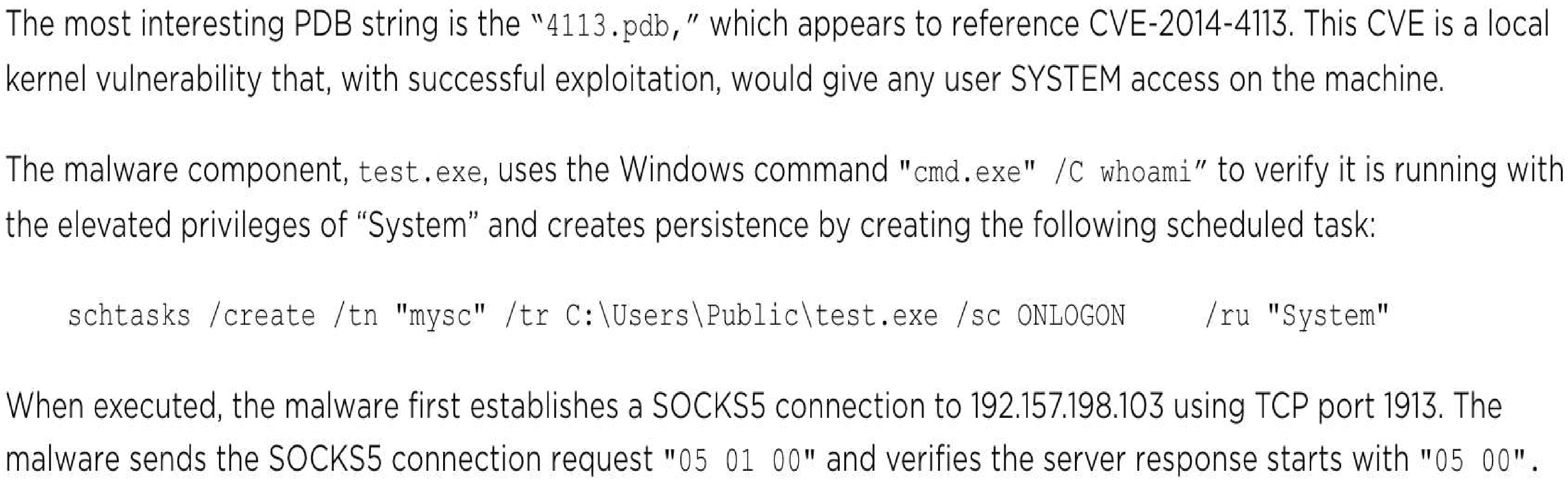
- Different mindset from looking for indicators

- Look for what the adversary or software does

- Focus on initial compromise and post-compromise details

- Info that may not be useful for ATT&CK mapping:
  - Static malware analysis
  - Infrastructure registration information
  - Industry/victim targeting information

DETECTION: FIND THE BEHAVIOR



The most interesting PDB string is the "4113.pdb," which appears to reference CVE-2014-4113. This CVE is a local kernel vulnerability that, with successful exploitation, would give any user SYSTEM access on the machine.

The malware component, test.exe, uses the Windows command "cmd.exe" /C whoami" to verify it is running with the elevated privileges of "System" and creates persistence by creating the following scheduled task:

```
schtasks /create /tn "mysc" /tr C:\Users\Public\test.exe /sc ONLOGON     /ru "System"
```

When executed, the malware first establishes a SOCKS5 connection to 192.157.198.103 using TCP port 1913. The malware sends the SOCKS5 connection request "05 01 00" and verifies the server response starts with "05 00".

DETECTION: RESEARCH THE BEHAVIOR

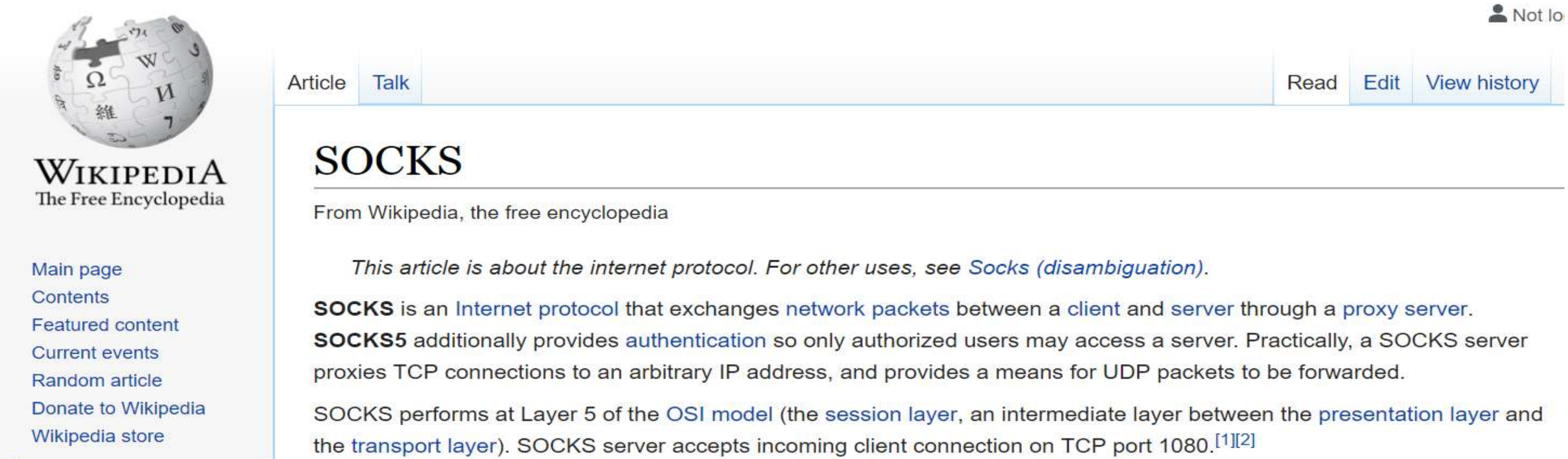
- CTI analysts may not be familiar with adversary/software behavior

- Encourage them to do additional research:
  - of your own team or organization (defenders/red teamers)
  - of external resources

- Time-consuming, but builds better analysis

- Understanding of core behavior helps with next steps

DETECTION: RESEARCH THE BEHAVIOR



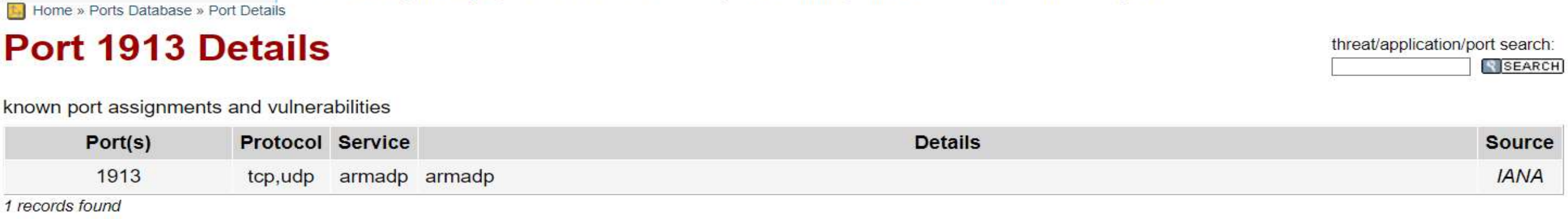
SOCKS

From Wikipedia, the free encyclopedia

This article is about the internet protocol. For other uses, see Socks (disambiguation).

SOCKS is an Internet protocol that exchanges network packets between a client and server through a proxy server. **SOCKS5** additionally provides authentication so only authorized users may access a server. Practically, a SOCKS server proxies TCP connections to an arbitrary IP address, and provides a means for UDP packets to be forwarded.

SOCKS performs at Layer 5 of the OSI model (the session layer, an intermediate layer between the presentation layer and the transport layer). SOCKS server accepts incoming client connection on TCP port 1080.[1][2]



Home » Ports Database » Port Details
threat/application/port search:
SEARCH

Port 1913 Details

known port assignments and vulnerabilities

Port(s)	Protocol	Service	Details	Source
1913	tcp,udp	armadp	armadp	*IANA*

1 records found

DETECTION: TRANSLATE THE BEHAVIOR INTO A TACTIC

- What is the adversary trying to accomplish?
- Often requires domain expertise
- Finished intel can give you context
- Only 12 options:

  - Initial Access
  - Execution
  - Persistence
  - Privilege Escalation
  - Defense Evasion
  - Credential Access
  - Discovery
  - Lateral Movement
  - Collection
  - Command and Control
  - Exfiltration
  - Impact

DETECTION: TRANSLATE THE BEHAVIOR INTO A TACTIC

- “When executed, the malware first establishes a SOCKS5 connection to 192.157.198.103 using TCP port 1913. … Once the connection to the server is established, the malware expects a message containing at least three bytes from the server. These first three bytes are the command identifier. The following commands are supported by the malware … “
- A connection in order to command the malware to do something
- Command and Control

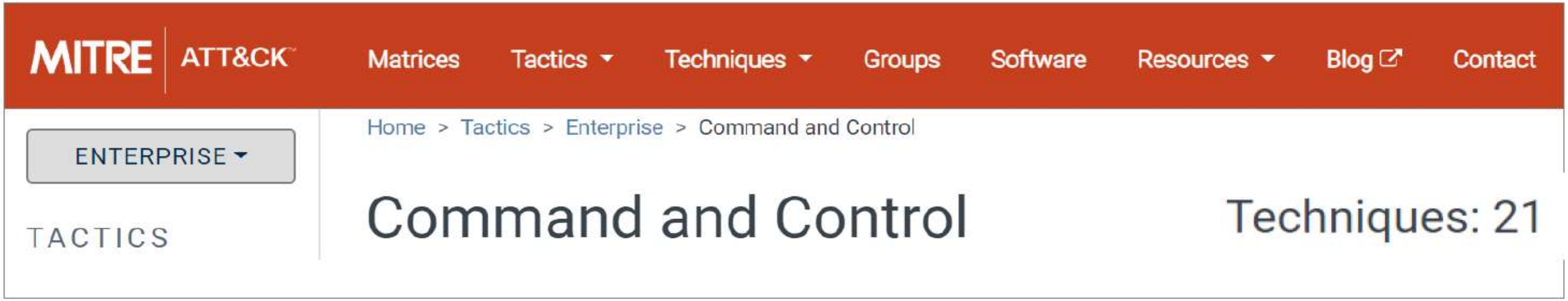
DETECTION: TRANSLATE THE BEHAVIOR INTO A TACTIC

- Often the toughest part
- Not every behavior is necessarily a technique

- Key strategies:
  - Look at the list of Techniques for the identified Tactic

  - Search attack.mitre.org
    - Try key words
    - Try "procedure"-level detail
    - Try specific command strings

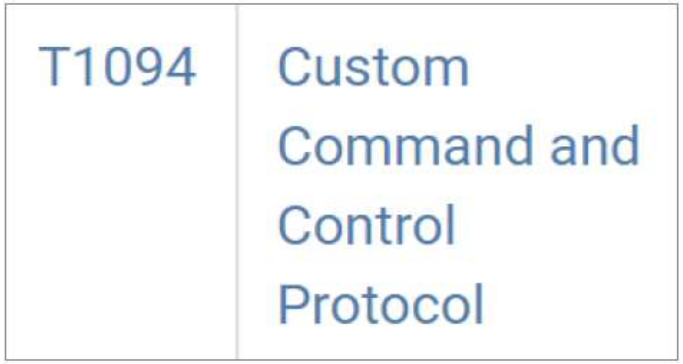
DETECTION: TRANSLATE THE BEHAVIOR INTO A TACTIC



Home > Tactics > Enterprise > Command and Control

Command and Control

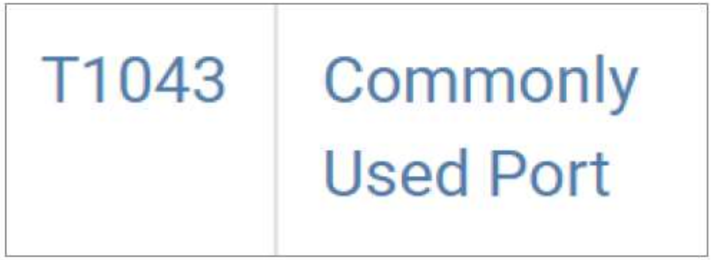
Techniques: 21



T1094	Custom Command and Control Protocol

Protocol vs. Port

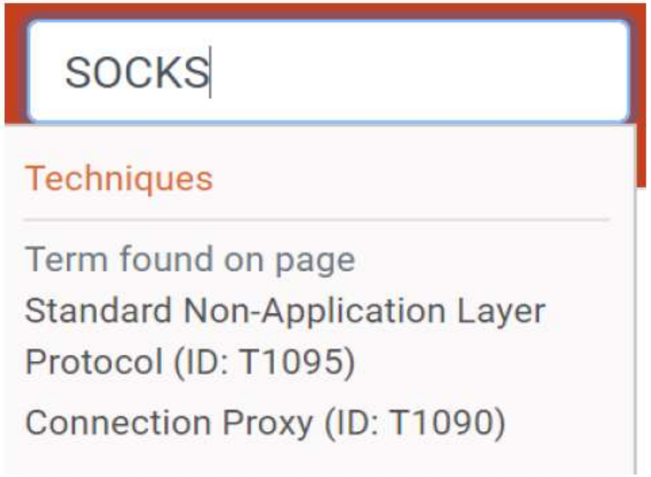
→ 2 techniques?



T1043	Commonly Used Port

DETECTION: TRANSLATE THE BEHAVIOR INTO A TACTIC

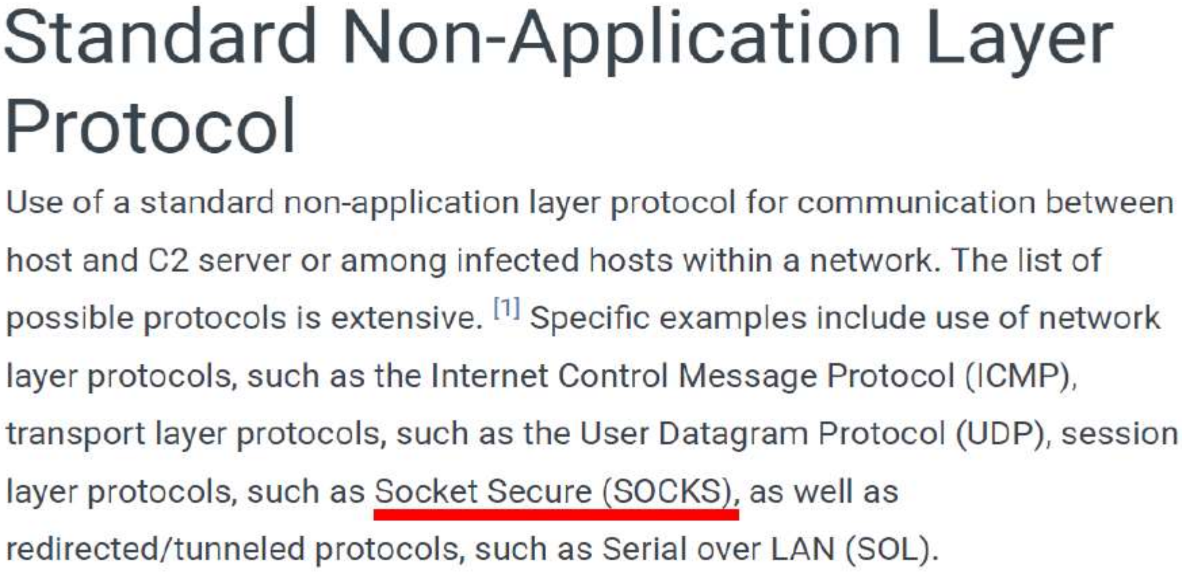
“the malware first establishes a SOCKS5 connection”


SOCKS

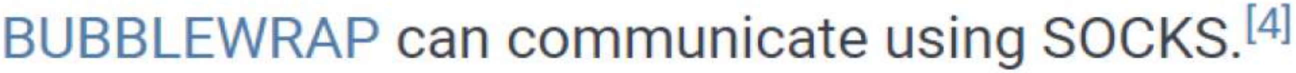
Techniques

Term found on page
Standard Non-Application Layer Protocol (ID: T1095)

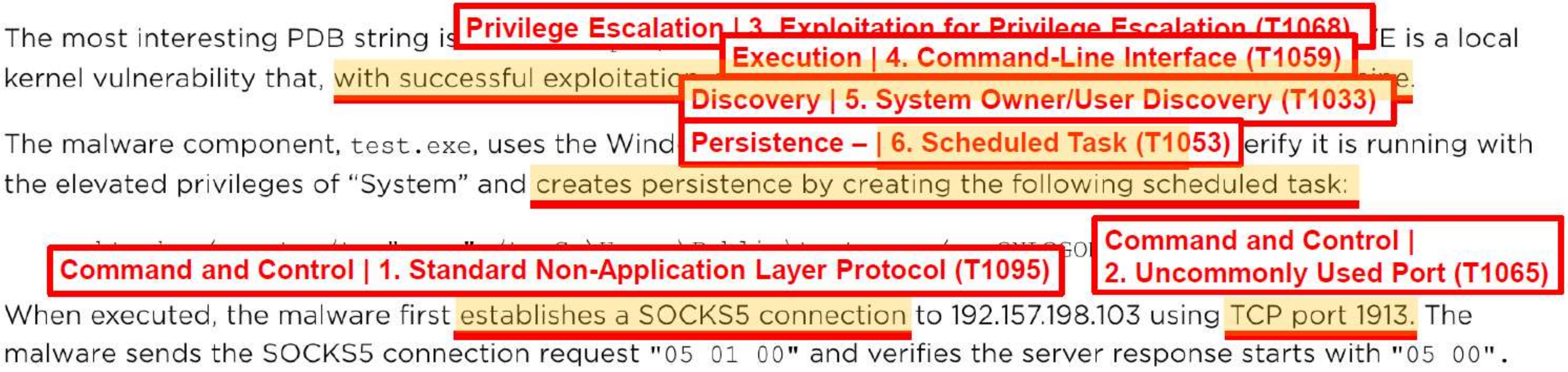
Connection Proxy (ID: T1090)


Standard Non-Application Layer Protocol

Use of a standard non-application layer protocol for communication between host and C2 server or among infected hosts within a network. The list of possible protocols is extensive. [1] Specific examples include use of network layer protocols, such as the Internet Control Message Protocol (ICMP), transport layer protocols, such as the User Datagram Protocol (UDP), session layer protocols, such as Socket Secure (SOCKS), as well as redirected/tunneled protocols, such as Serial over LAN (SOL).


BUBBLEWRAP can communicate using SOCKS.[4]

DETECTION: TRANSLATE THE BEHAVIOR INTO A TACTIC



The most interesting PDB string is E is a local kernel vulnerability that, with successful exploitatio e.

Privilege Escalation | 3. Exploitation for Privilege Escalation (T1068)

Execution | 4. Command-Line Interface (T1059)

Discovery | 5. System Owner/User Discovery (T1033)

Persistence – | 6. Scheduled Task (T1053)

The malware component, `test.exe`, uses the Wind erify it is running with the elevated privileges of “System” and creates persistence by creating the following scheduled task:

Command and Control | 1. Standard Non-Application Layer Protocol (T1095)

Command and Control | 2. Uncommonly Used Port (T1065)

When executed, the malware first establishes a SOCKS5 connection to 192.157.198.103 using TCP port 1913. The malware sends the SOCKS5 connection request `"05 01 00"` and verifies the server response starts with `"05 00"`.

ASSESSMENT AND ENGINEERING

- Based on the type of visibility decisions should be driven on what you collect
  - What are the tools and technology you choose?
  - What is the current coverage?
  - Are the gaps identified?
  - Will they help you in building effective and efficient defenses?
- Look at the bigger picture beyond detection
- Increase awareness among the stake holders

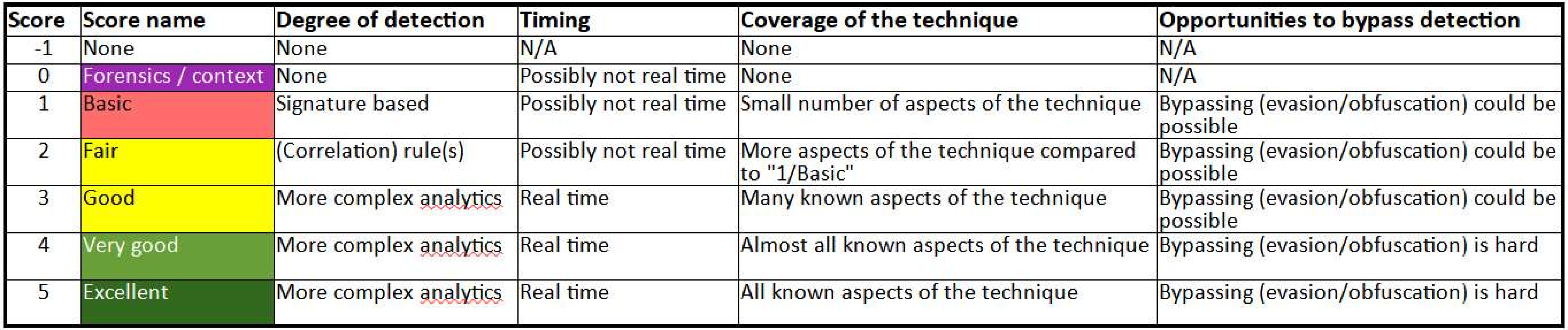
ASSESSMENT AND ENGINEERING

- Collect one log source at a time to improve ATT&CK visibility
- Places to start:
  - rabobank-cdc/DeTTECT
  - https://github.com/rabobank-cdc/DeTTECT
  - Windows Event logs
  - https://www.malwarearchaeology.com/cheat-sheets
  - Sysmon
  - https://github.com/SwiftOnSecurity/sysmon-config

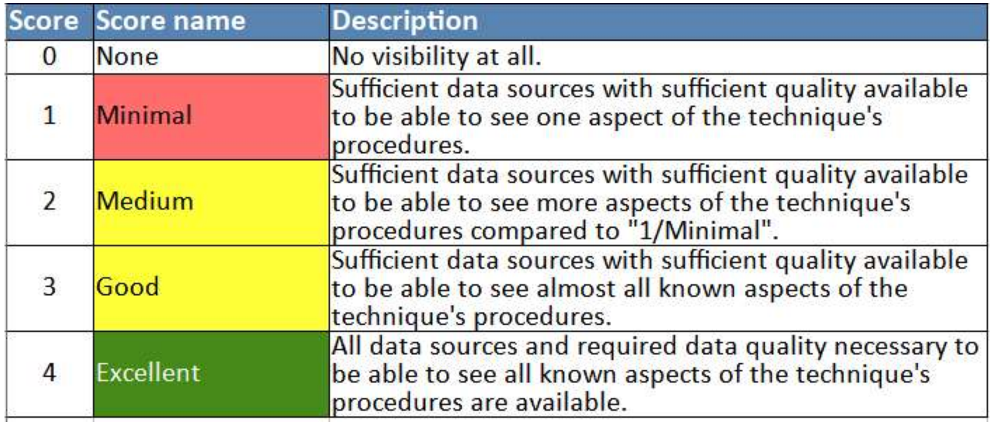
EXAMPLE : DETT&CT

- DeTT&CT provides the following functionality:
  - Administrate and score the quality of your data sources.
  - Get insight on the visibility you have on for example endpoints.
  - Map your detection coverage.
  - Map threat actor behaviors.
  - Compare visibility, detection coverage and threat actor behaviors to uncover possible improvements in detection and visibility (which is based on your available data sources). This can help you to prioritize your blue teaming efforts.

HOW TO SCORE DETECTION'S FOR ASSESSMENT?

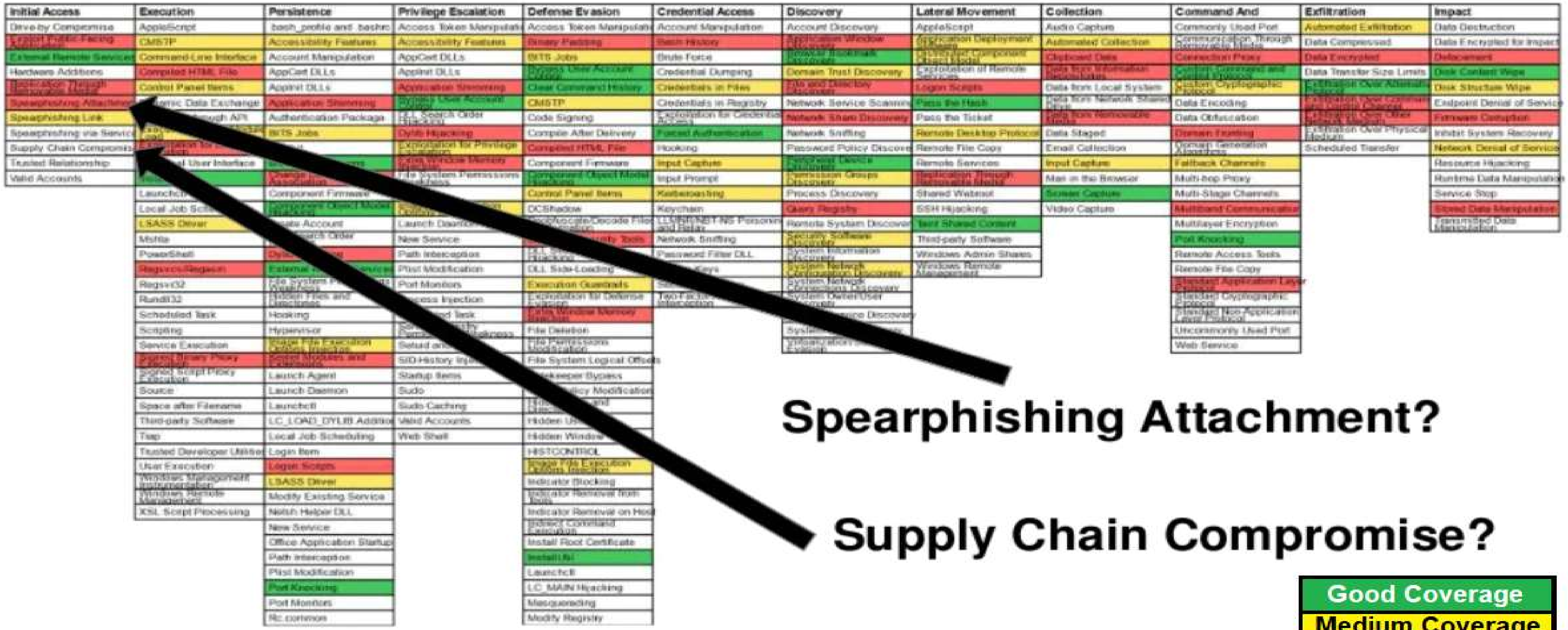


Score	Score name	Degree of detection	Timing	Coverage of the technique	Opportunities to bypass detection
-1	None	None	N/A	None	N/A
0	Forensics / context	None	Possibly not real time	None	N/A
1	Basic	Signature based	Possibly not real time	Small number of aspects of the technique	Bypassing (evasion/obfuscation) could be possible
2	Fair	(Correlation) rule(s)	Possibly not real time	More aspects of the technique compared to "1/Basic"	Bypassing (evasion/obfuscation) could be possible
3	Good	More complex analytics	Real time	Many known aspects of the technique	Bypassing (evasion/obfuscation) could be possible
4	Very good	More complex analytics	Real time	Almost all known aspects of the technique	Bypassing (evasion/obfuscation) is hard
5	Excellent	More complex analytics	Real time	All known aspects of the technique	Bypassing (evasion/obfuscation) is hard



Score	Score name	Description
0	None	No visibility at all.
1	Minimal	Sufficient data sources with sufficient quality available to be able to see one aspect of the technique's procedures.
2	Medium	Sufficient data sources with sufficient quality available to be able to see more aspects of the technique's procedures compared to "1/Minimal".
3	Good	Sufficient data sources with sufficient quality available to be able to see almost all known aspects of the technique's procedures.
4	Excellent	All data sources and required data quality necessary to be able to see all known aspects of the technique's procedures are available.

ASSESSMENT OF THE GAPS



Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And	Exfiltration	Impact
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	[illegible]amic 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	[illegible]ough 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	🟨 [illegible]	🟨 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 [illegible]	[illegible]	🟨 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	[illegible]l User Interface	🟩 [illegible]	🟥 Extra Window Memory Injection	Component Firmware	🟨 Input Capture	🟩 Peripheral Device Discovery	Remote Services	🟨 Input Capture	🟨 Fallback Channels		Resource Hijacking
Valid Accounts	🟩 [illegible]	🟥 Change [illegible] 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
	Launchct[illegible]	Component Firmware	[illegible]	🟨 Control Panel Items	🟨 Kerberoasting	Process Discovery	Shared Webroot	🟩 Screen Capture	Multi-Stage Channels		Service Stop
	Local Job Sc[illegible]	🟩 Component Object Model Hijacking	🟨 [illegible]	DCShadow	Keychain	🟥 Query Registry	SSH Hijacking	Video Capture	🟥 Multiband Communication		🟥 Stored Data Manipulation
	🟨 LSASS Driver	[illegible]ate Account	Launch Daem[illegible]	Deobfuscate/Decode Files or Information	LLMNR/NBT-NS Poisoning and Relay	Remote System Discovery	🟩 Taint Shared Content		Multilayer Encryption		Transmitted Data Manipulation
	Mshta	[illegible]arch Order Hijacking	New Service	🟥 [illegible]ity Tools	Network Sniffing	🟨 Security Software Discovery	Third-party Software		🟩 Port Knocking		
	PowerShell	🟥 Dyl[illegible]	Path Interception	DLL [illegible] Hijacking	Password Filter DLL	System Information Discovery	Windows Admin Shares		Remote Access Tools		
	🟥 Regsvcs/Regasm	🟩 External [illegible]	Plist Modification	DLL Side-Loading	[illegible] Keys	🟨 System Network Configuration Discovery	Windows Remote Management		Remote File Copy		
	Regsvr32	File System P[illegible] Weakness	Port Monitors	🟨 Execution Guardrails	[illegible]	System Network Connections Discovery			🟥 Standard Application Layer Protocol		
	Rundll32	Hidden Files and Directories	[illegible]cess Injection	Exploitation for Defense Evasion	Two-Factor Authentication Interception	System Owner/User Discovery			Standard Cryptographic Protocol		
	Scheduled Task	Hooking	[illegible]ed Task	🟥 Extra Window Memory Injection		[illegible]ice Discovery			Standard Non-Application Layer Protocol		
	Scripting	Hypervisor	[illegible] Perm[illegible]ness	File Deletion		Syste[illegible]			Uncommonly Used Port		
	Service Execution	🟨 Image File Execution Options Injection	Setuid an[illegible]	File Permissions Modification		Virtualization[illegible] Evasion			Web Service		
	🟥 Signed Binary Proxy Execution	🟥 Kernel Modules and Extensions	SID-History Inj[illegible]	File System Logical Offsets							
	Signed Script Proxy Execution	Launch Agent	Startup Items	[illegible]ekeeper Bypass							
	Source	Launch Daemon	Sudo	[illegible]licy Modification							
	Space after Filename	Launchctl	Sudo Caching	Hi[illegible] and Direc[illegible]							
	Third-party Software	LC_LOAD_DYLIB Addition	Valid Accounts	Hidden Us[illegible]							
	Trap	Local Job Scheduling	Web Shell	Hidden Window							
	Trusted Developer Utilities	Login Item		HISTCONTROL							
	User Execution	🟥 Logon Scripts		🟨 Image File Execution Options Injection							
	Windows Management Instrumentation	🟨 LSASS Driver		Indicator Blocking							
	Windows Remote Management	Modify Existing Service		Indicator Removal from Tools							
	XSL Script Processing	Netsh Helper DLL		Indicator Removal on Host							
		New Service		Indirect Command Execution							
		Office Application Startup		Install Root Certificate							
		Path Interception		🟩 InstallUtil							
		Plist Modification		Launchctl							
		🟩 Port Knocking		LC_MAIN Hijacking							
		Port Monitors		Masquerading							
		Rc.common		Modify Registry							

Spearphishing Attachment?

Supply Chain Compromise?

- 🟩 Good Coverage
- 🟨 Medium Coverage
- 🟥 Low Coverage
- ⬜ No Coverage

ASSESSMENT AND ENGINEERING CONCLUSIONS

- Plan out your tools and log monitoring strategy based on coverage
- Determine what techniques your current logs and technology detect and remediate
  - Review the documentation
  - Check with the vendor
- Identify what changes can be done to the environment
  - Configuration changes?
  - acquiring new detection tools?
  - map the gaps the tool can fill
- Plan to use the resources based on the security budget

THANK YOU !!

AND KEEP USING ATT&CK TO DETTECT ;)