Module 1: Introducing the Training and Understanding ATT&CK

Using MITRE ATT&CK™ for Cyber Threat Intelligence Training

Katie Nickels and Adam Pennington

MITRE

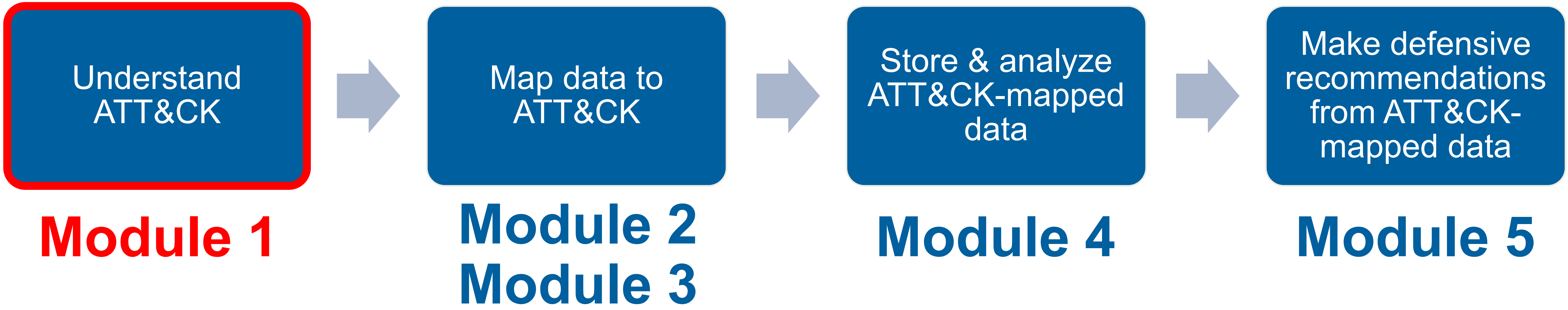
Training Overview

- **Five modules consisting of YouTube videos and exercises are available at attack.mitre.org/training/cti**
- **Module 1: Introducing training and understanding ATT&CK**
  A. Topic introduction (Video)
- **Module 2: Mapping to ATT&CK from finished reporting**
  A. Topic introduction (Video)
  B. Exercise 2: Mapping to ATT&CK from finished reporting
  (Do it yourself with materials on attack.mitre.org/training/cti)
  C. Going over Exercise 2 (Video)
- **Module 3: Mapping to ATT&CK from raw data**
  A. Topic introduction (Video)
  B. Exercise 3: Mapping to ATT&CK from raw data
  (Do it yourself with materials on attack.mitre.org/training/cti)
  C. Going over Exercise 3 (Video)

Training Overview

- **Module 4: Storing and analyzing ATT&CK-mapped intel**
  A. Topic introduction (Video)
  B. Exercise 4: Comparing layers in ATT&CK Navigator
  (Do it yourself with materials on attack.mitre.org/training/cti)
  C. Going over Exercise 4 (Video)
- **Module 5: Making ATT&CK-mapped data actionable with defensive recommendations**
  A. Topic introduction (Video)
  B. Exercise 5: Making defensive recommendations
  (Do it yourself with materials on attack.mitre.org/training/cti)
  C. Going over Exercise 5 and wrap-up (Video)

Process of Applying ATT&CK to CTI



Understand ATT&CK

Module 1

Map data to ATT&CK

Module 2
Module 3

Store & analyze ATT&CK-mapped data

Module 4

Make defensive recommendations from ATT&CK-mapped data

Module 5

Introduction to ATT&CK and Applying it to CTI

Tough Questions for Defenders

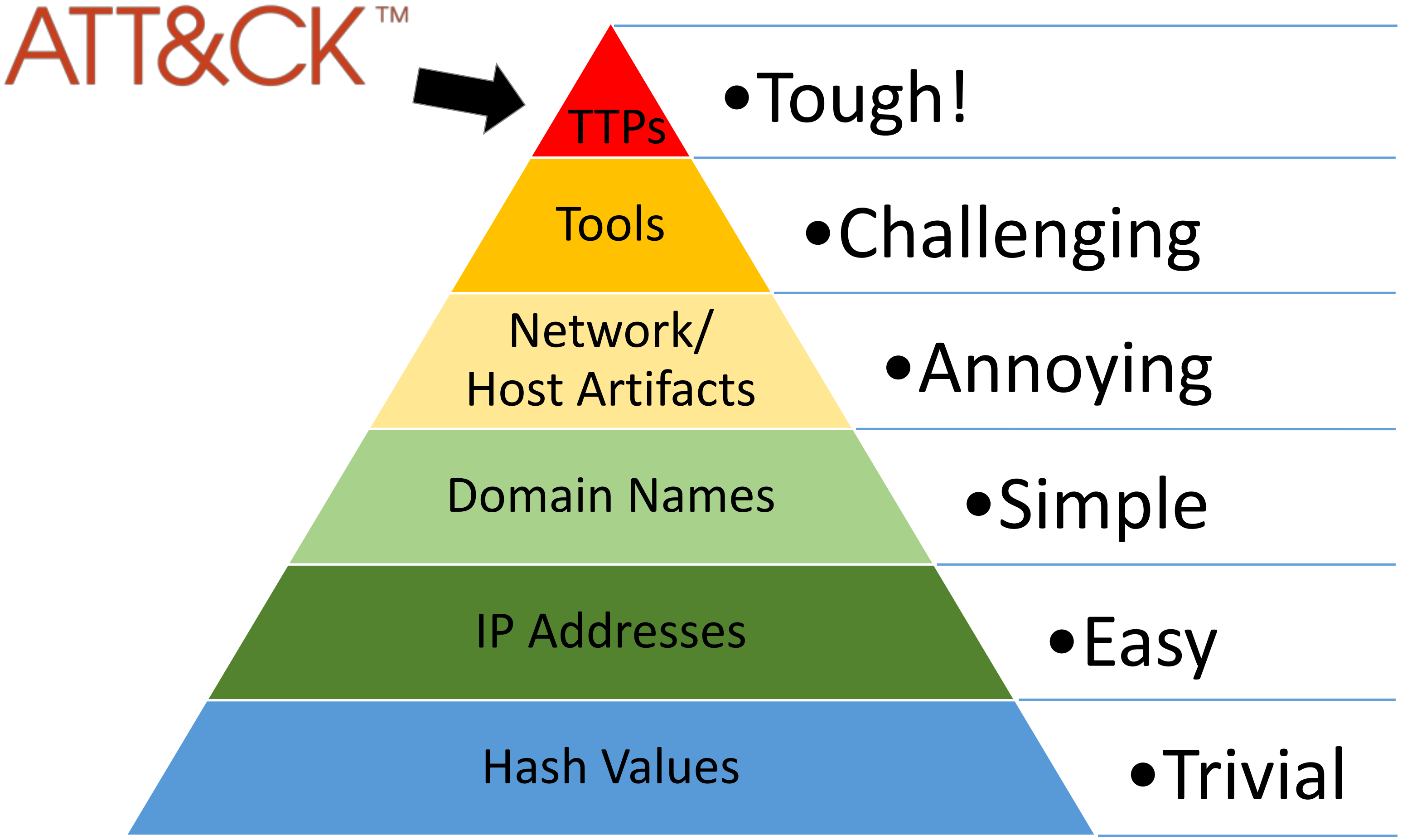
- How effective are my defenses?
- Do I have a chance at detecting APT29?
- Is the data I'm collecting useful?
- Do I have overlapping tool coverage?
- Will this new product help my organization's defenses?

What is ATT&CK?

A knowledge base of adversary behavior

- ***Based on real-world observations***
- ***Free, open, and globally accessible***
- ***A common language***
- ***Community-driven***

The Difficult Task of Detecting TTPs



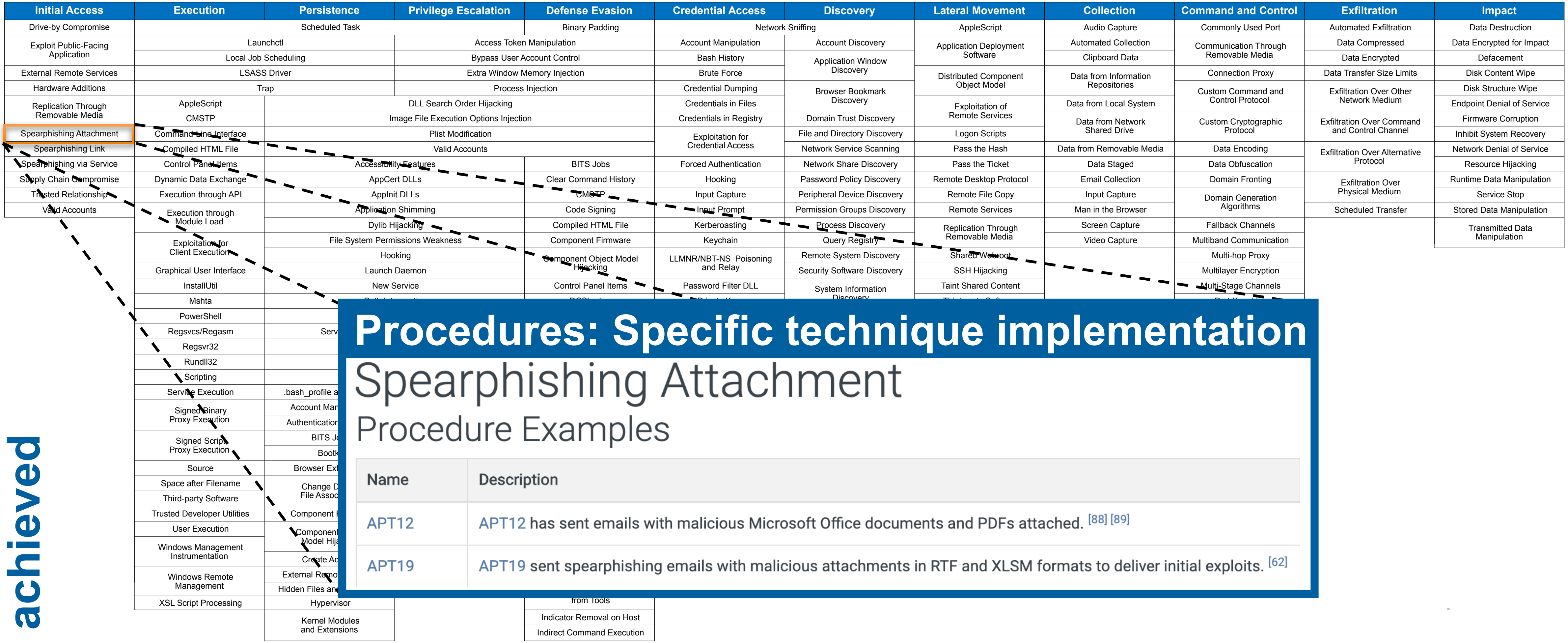
Source: David Bianco, https://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html

David Bianco's Pyramid of Pain

Breaking Down ATT&CK

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 Man									
		Authentication									
	Signed Script Proxy Execution	BITS Jo									
		Bootk									
	Source	Browser Ext									
	Space after Filename	Change D File Assoc									
	Third-party Software										
	Trusted Developer Utilities	Component F									
	User Execution	Component Model Hija									
	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							

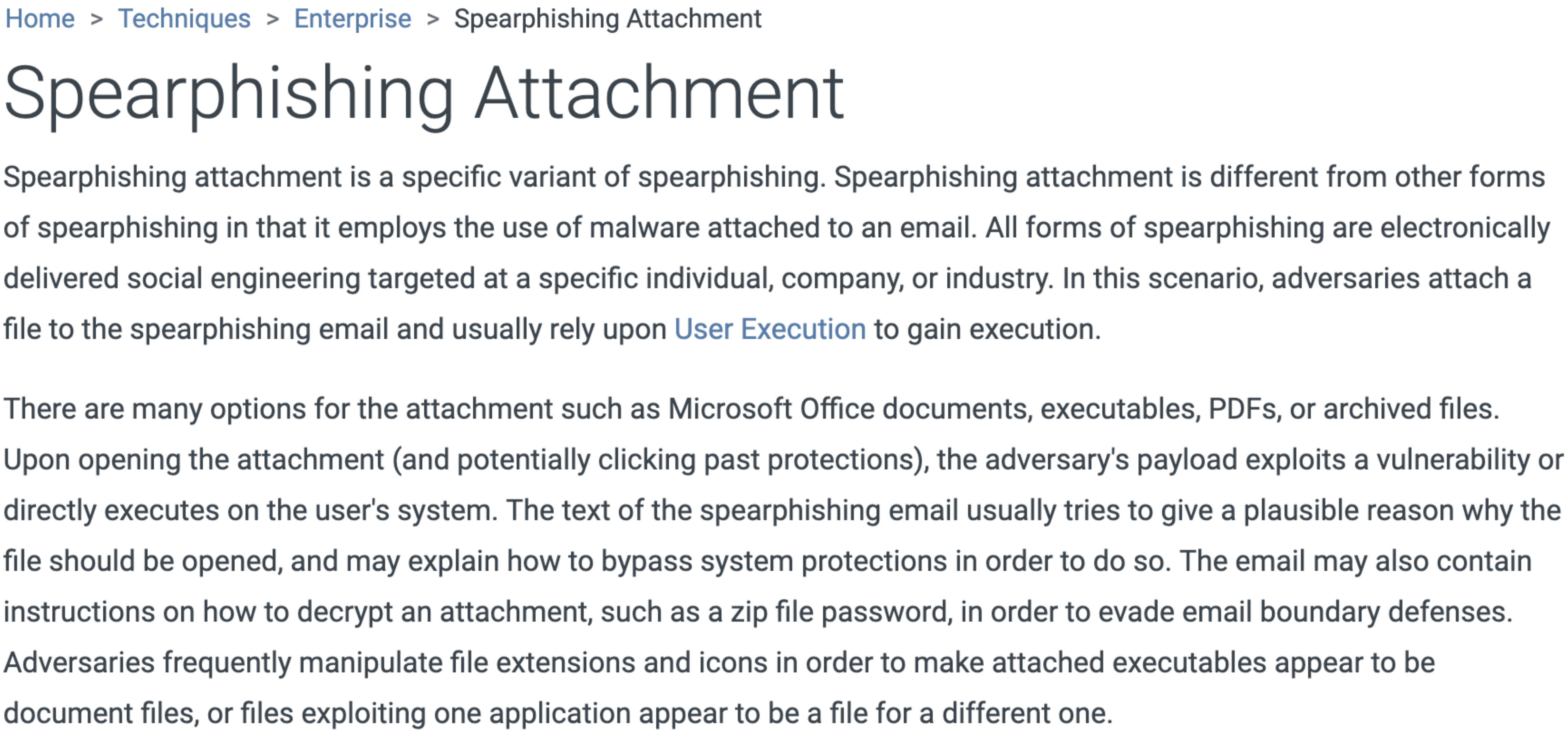
Procedures: Specific technique implementation

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



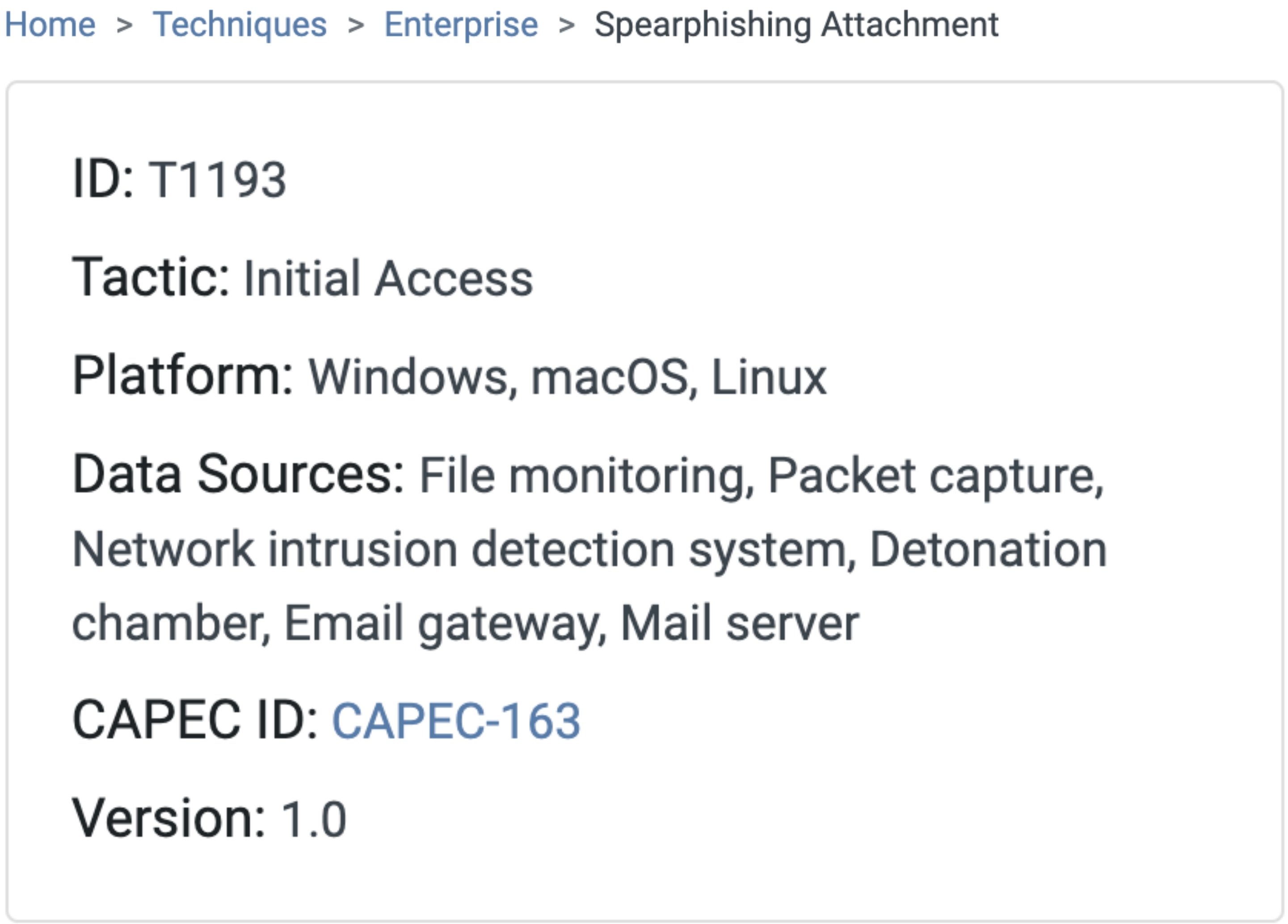
Home > Techniques > Enterprise > Spearphishing Attachment

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

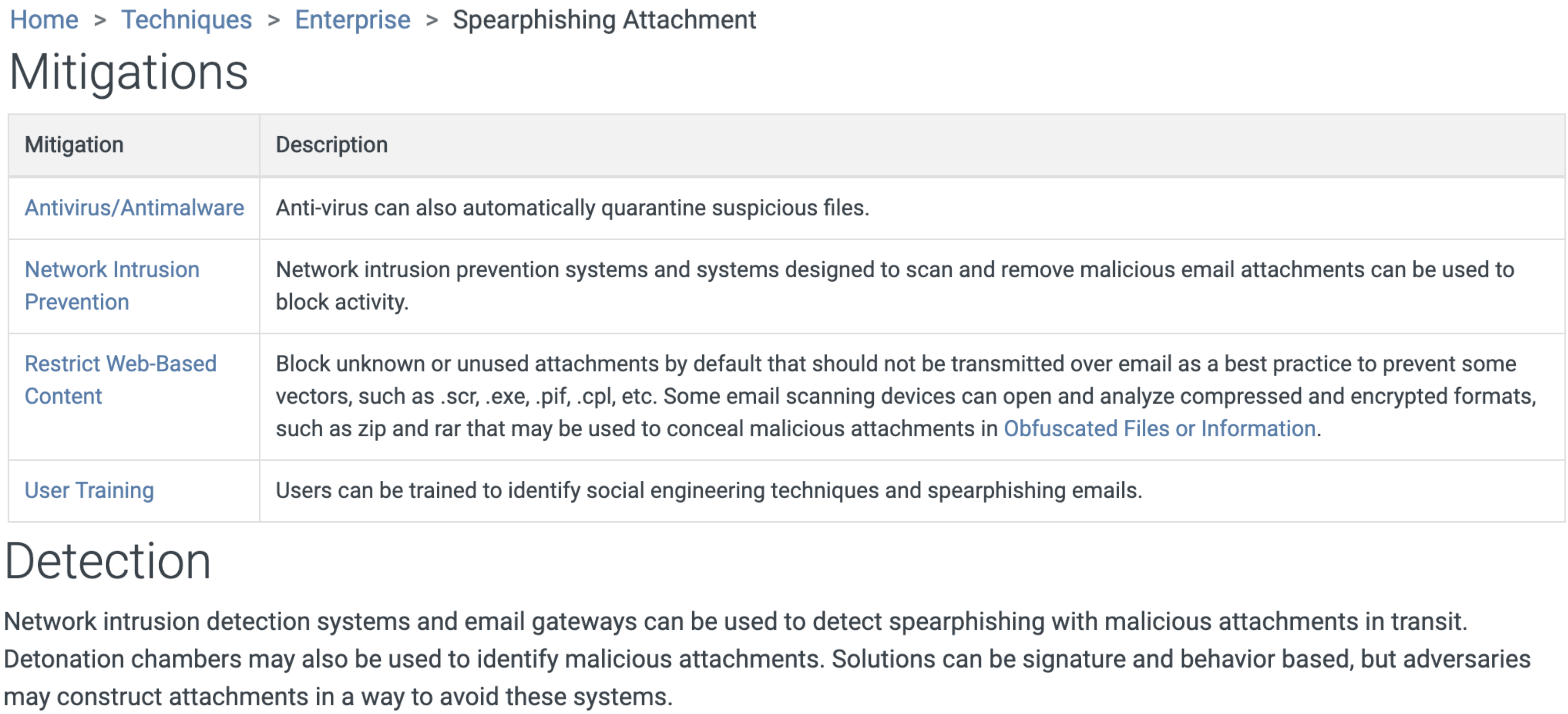
Platform: Windows, macOS, Linux

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

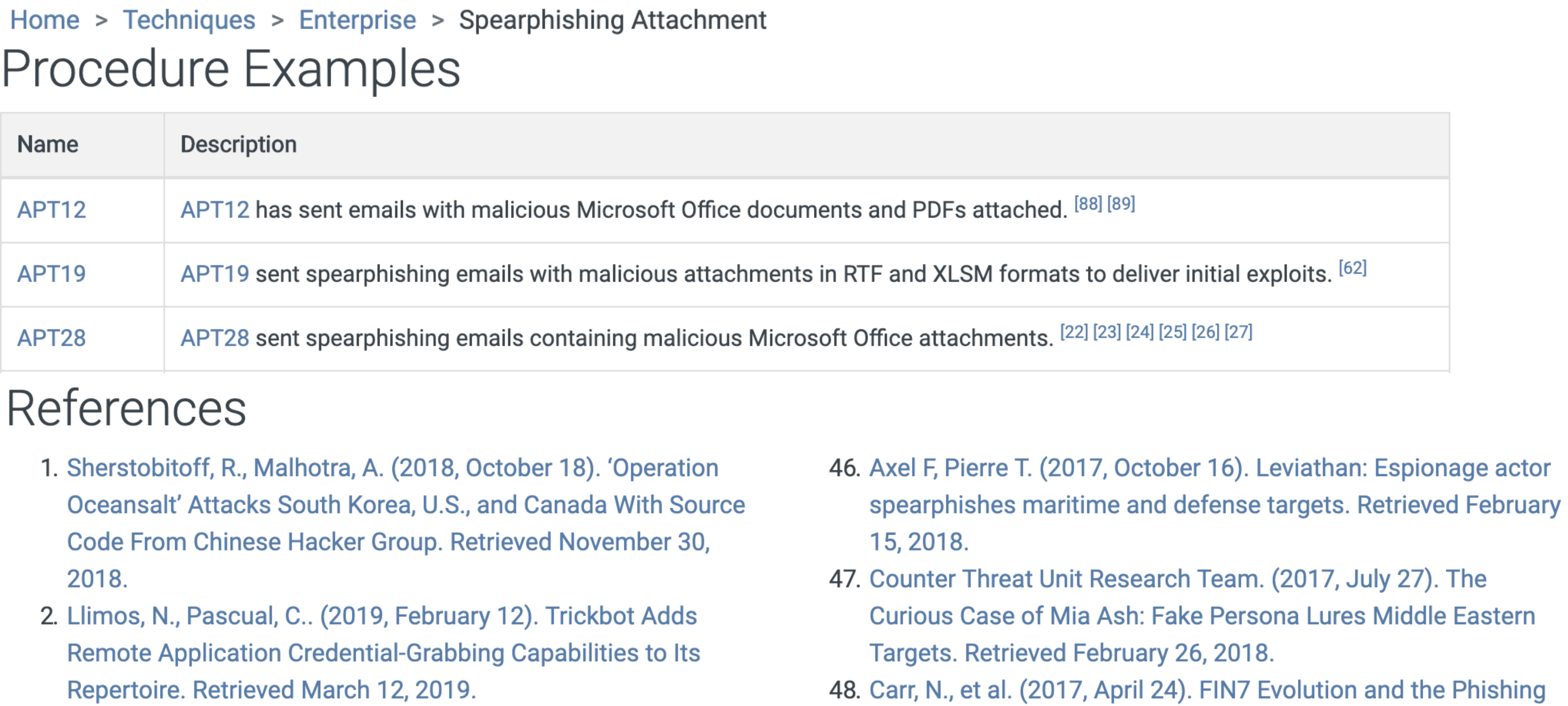
Mitigations

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

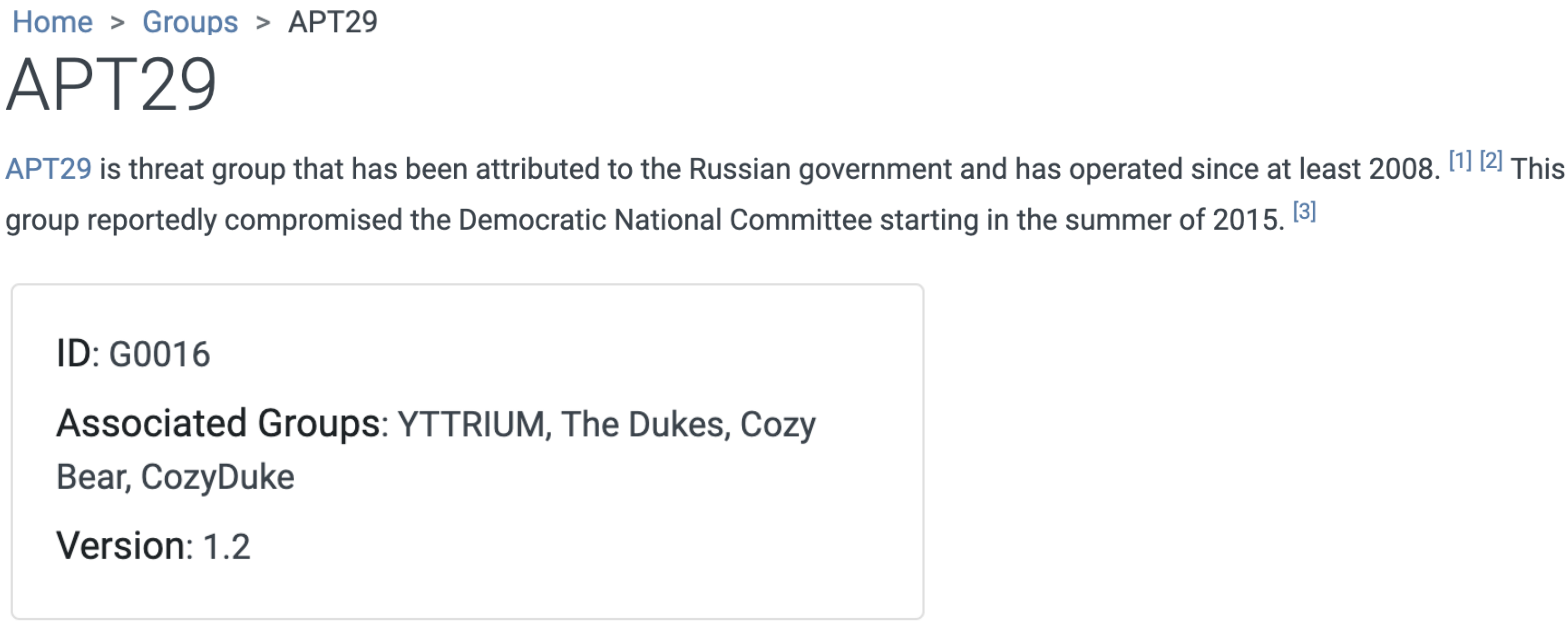
Name	Description
APT12	APT12 has sent emails with malicious Microsoft Office documents and PDFs attached. [88] [89]
APT19	APT19 sent spearphishing emails with malicious attachments in RTF and XLSM formats to deliver initial exploits. [62]
APT28	APT28 sent spearphishing emails containing malicious Microsoft 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: APT29



Home > Groups > APT29

APT29

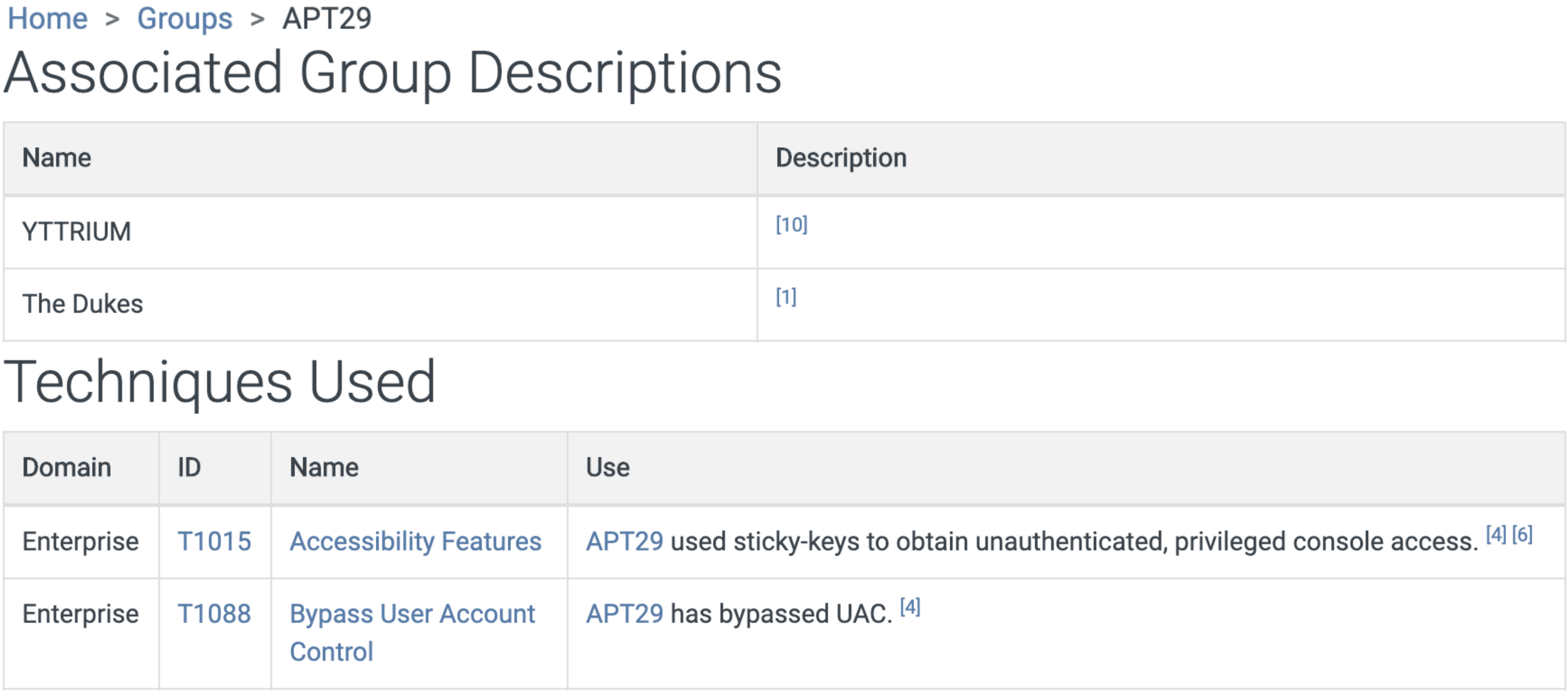
APT29 is threat group that has been attributed to the Russian government and has operated since at least 2008. [1] [2] This group reportedly compromised the Democratic National Committee starting in the summer of 2015. [3]

ID: G0016

Associated Groups: YTTRIUM, The Dukes, Cozy Bear, CozyDuke

Version: 1.2

Group: APT29



Home > Groups > APT29

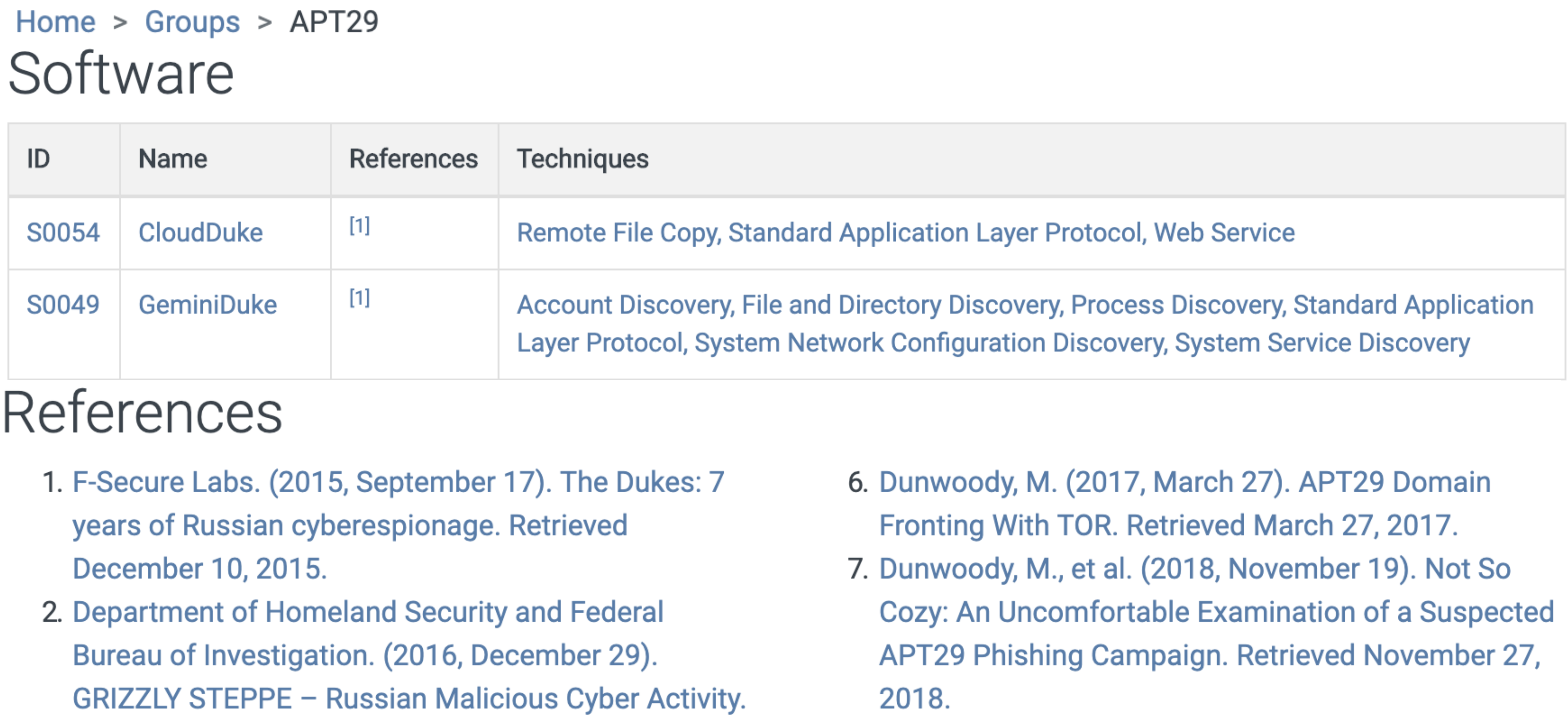
Associated Group Descriptions

Name	Description
YTTRIUM	[10]
The Dukes	[1]

Techniques Used

Domain	ID	Name	Use
Enterprise	T1015	Accessibility Features	APT29 used sticky-keys to obtain unauthenticated, privileged console access. [4] [6]
Enterprise	T1088	Bypass User Account Control	APT29 has bypassed UAC. [4]

Group: APT29



Home > Groups > APT29

Software

ID	Name	References	Techniques
S0054	CloudDuke	[1]	Remote File Copy, Standard Application Layer Protocol, Web Service
S0049	GeminiDuke	[1]	Account Discovery, File and Directory Discovery, Process Discovery, Standard Application Layer Protocol, System Network Configuration Discovery, System Service Discovery

References

1. F-Secure Labs. (2015, September 17). The Dukes: 7 years of Russian cyberespionage. Retrieved December 10, 2015.
2. Department of Homeland Security and Federal Bureau of Investigation. (2016, December 29). GRIZZLY STEPPE – Russian Malicious Cyber Activity.

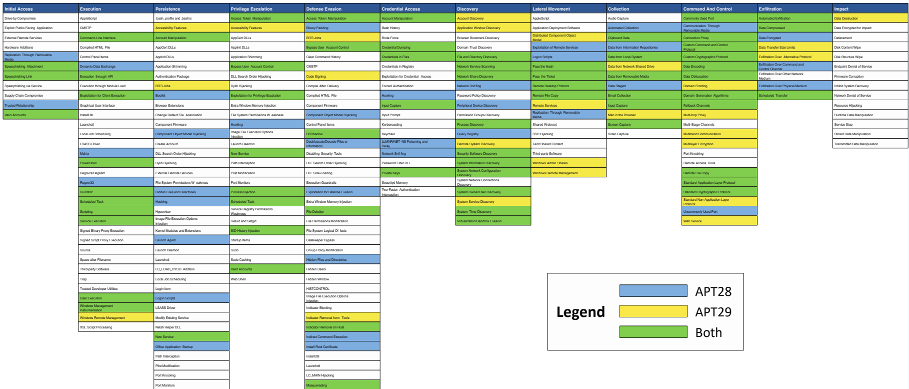
6. Dunwoody, M. (2017, March 27). APT29 Domain Fronting With TOR. Retrieved March 27, 2017.
7. Dunwoody, M., et al. (2018, November 19). Not So Cozy: An Uncomfortable Examination of a Suspected APT29 Phishing Campaign. Retrieved November 27, 2018.

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

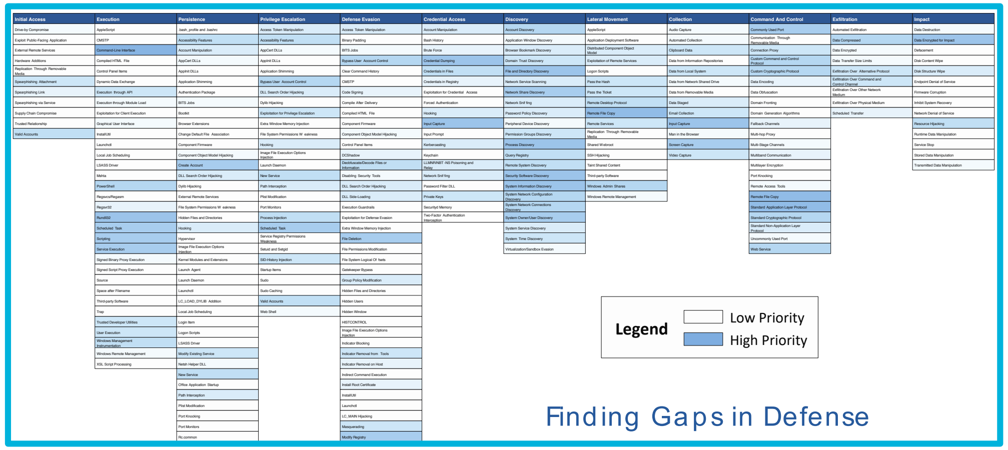
🟦 APT28

🟨 APT29

🟩 Both

Comparing APT28 to APT29

Assessment and Engineering



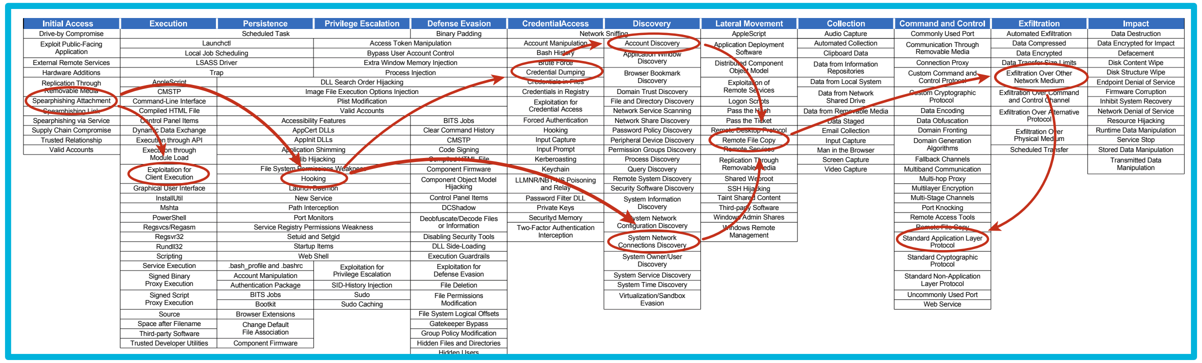
Legend

□ Low Priority

🟦 High Priority

Finding Gaps in Defense

Adversary Emulation



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

ATT&CK and CTI

Threat Intelligence – How ATT&CK Can Help

- **Use knowledge of adversary behaviors to inform defenders**

- **Structuring threat intelligence with ATT&CK allows us to…**
  - *Compare* behaviors
    - Groups to each other
    - Groups over time
    - Groups to defenses
  - *Communicate* in a common language

Communicate to Defenders

Registry Run Keys / Startup Folder (T1060)

ATT&CK

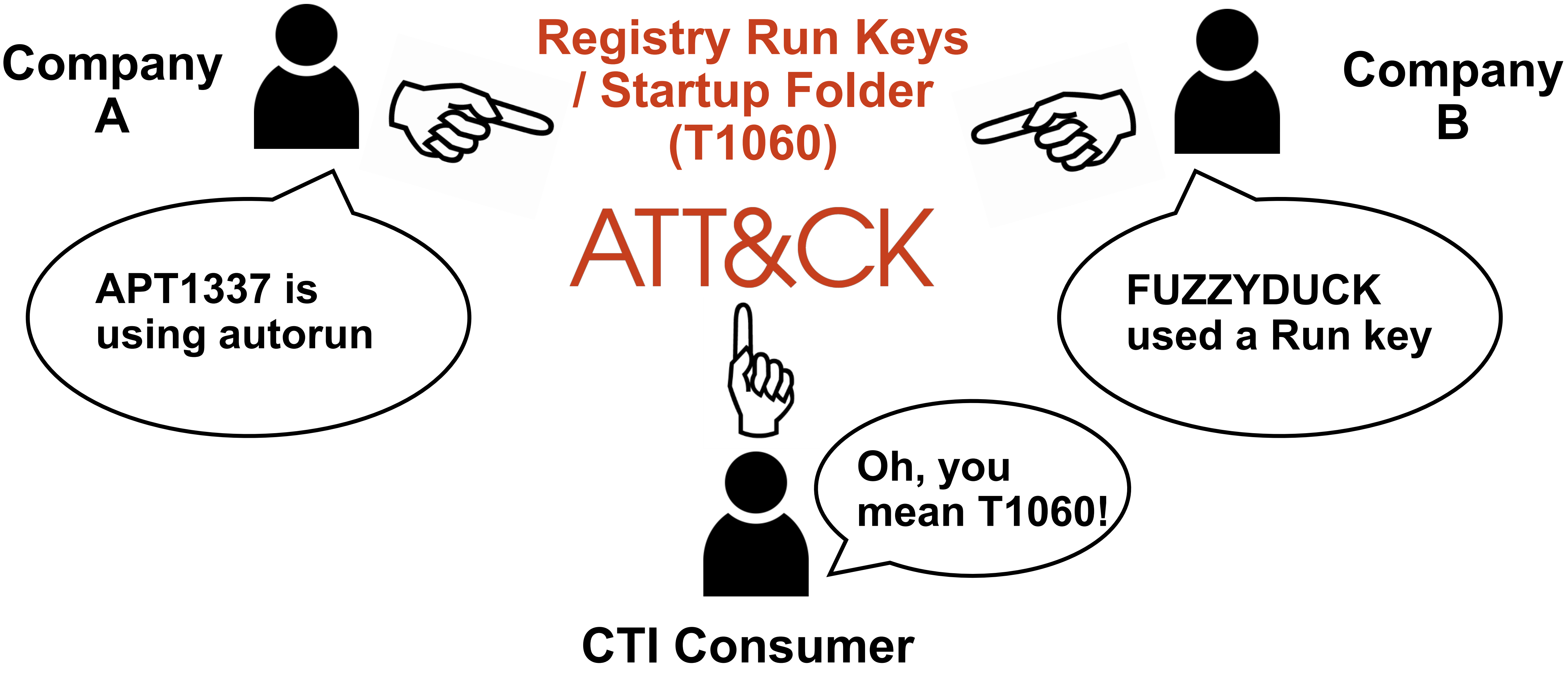
THIS is what the adversary is doing! The Run key is AdobeUpdater.

Oh, we have Registry data, we can detect that!

CTI Analyst

Defender

Communicate Across the Community



Company A

Company B

Registry Run Keys / Startup Folder (T1060)

ATT&CK

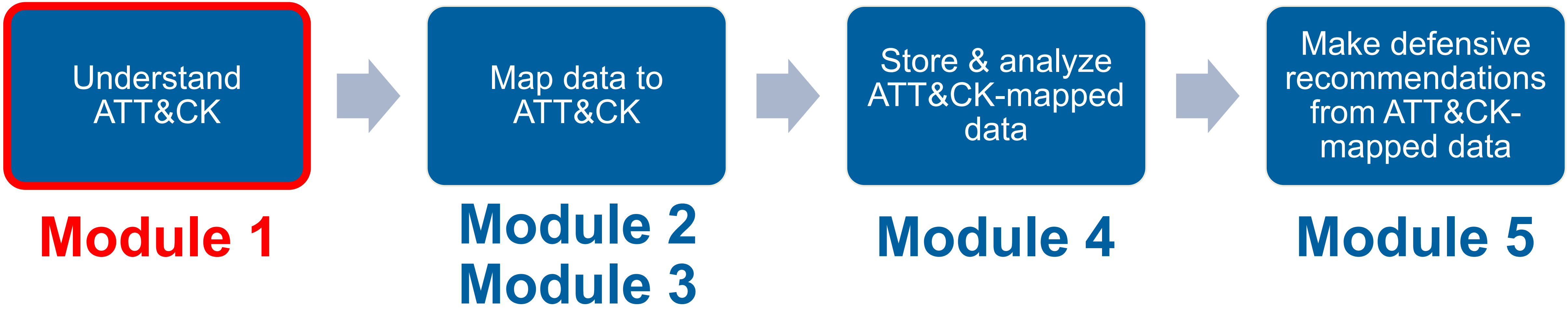
APT1337 is using autorun

FUZZYDUCK used a Run key

Oh, you mean T1060!

CTI Consumer

Process of Applying ATT&CK to CTI



Understand ATT&CK

Module 1

Map data to ATT&CK

Module 2
Module 3

Store & analyze ATT&CK-mapped data

Module 4

Make defensive recommendations from ATT&CK-mapped data

Module 5

End of Module 1