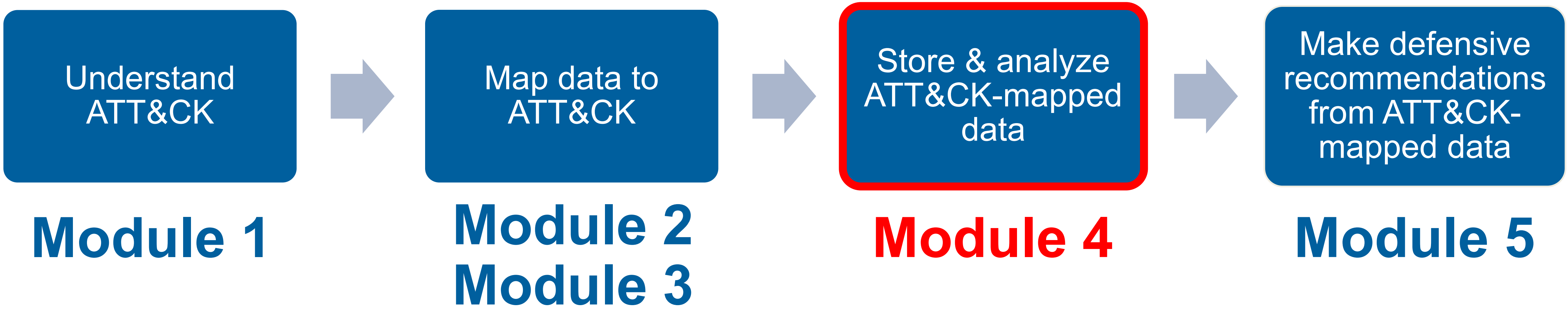
Module 4:
Storing and Analyzing ATT&CK-Mapped Data

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

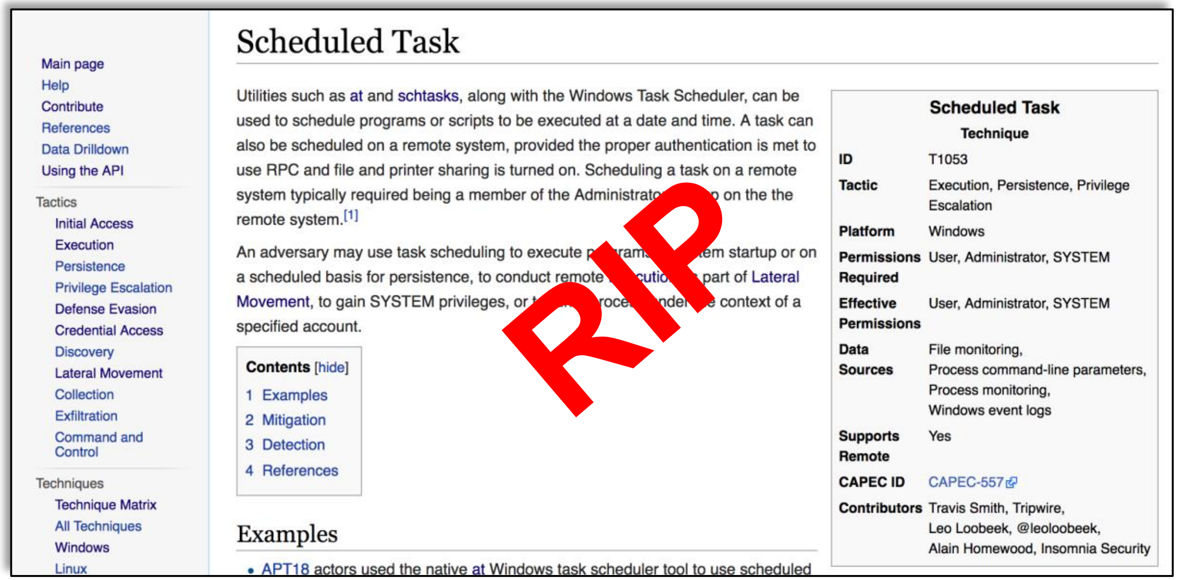
Considerations When Storing ATT&CK-Mapped Intel

- **Who’s consuming it?**
  - Human or machine?
  - Requirements?
- **How will you provide context?**
  - Include full text?
- **How detailed will it be?**
  - Just a Technique, or a Procedure?
  - How will you capture that detail? (Free text?)
- **How will you link it to other intel?**
  - Incident, group, campaign, indicator…
- **How will you import and export data?**
  - Format?

The community is still figuring this out!

Ways to Store and Display ATT&CK-Mapped Intel

¯_(ツ)_/¯



Scheduled Task

Utilities such as at and schtasks, along with the Windows Task Scheduler, can be used to schedule programs or scripts to be executed at a date and time. A task can also be scheduled on a remote system, provided the proper authentication is met to use RPC and file and printer sharing is turned on. Scheduling a task on a remote system typically required being a member of the Administrators group on the the remote system.[1]

An adversary may use task scheduling to execute programs at system startup or on a scheduled basis for persistence, to conduct remote Execution as part of Lateral Movement, to gain SYSTEM privileges, or to run a process under the context of a specified account.

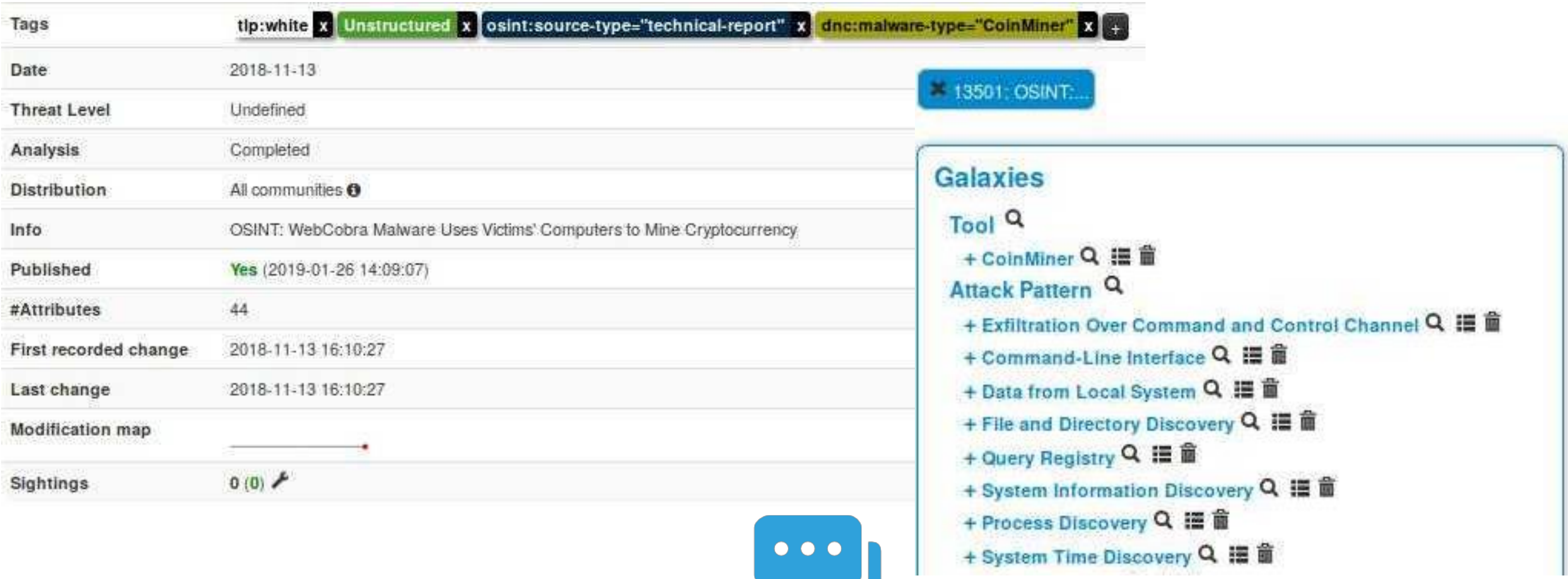
Contents [hide]
1 Examples
2 Mitigation
3 Detection
4 References

Scheduled Task	
	Technique
ID	T1053
Tactic	Execution, Persistence, Privilege Escalation
Platform	Windows
Permissions Required	User, Administrator, SYSTEM
Effective Permissions	User, Administrator, SYSTEM
Data Sources	File monitoring, Process command-line parameters, Process monitoring, Windows event logs
Supports Remote	Yes
CAPEC ID	CAPEC-557
Contributors	Travis Smith, Tripwire, Leo Loobeek, @leoloobeek, Alain Homewood, Insomnia Security

Examples

- APT18 actors used the native at Windows task scheduler tool to use scheduled

Ways to Store and Display ATT&CK-Mapped Intel



Tags	tlp:white x Unstructured x osint:source-type="technical-report" x dnc:malware-type="CoinMiner" x +
Date	2018-11-13
Threat Level	Undefined
Analysis	Completed
Distribution	All communities 🛈
Info	OSINT: WebCobra Malware Uses Victims' Computers to Mine Cryptocurrency
Published	Yes (2019-01-26 14:09:07)
#Attributes	44
First recorded change	2018-11-13 16:10:27
Last change	2018-11-13 16:10:27
Modification map	
Sightings	0 (0)

✖ 13501: OSINT:...

Galaxies

Tool

- + CoinMiner

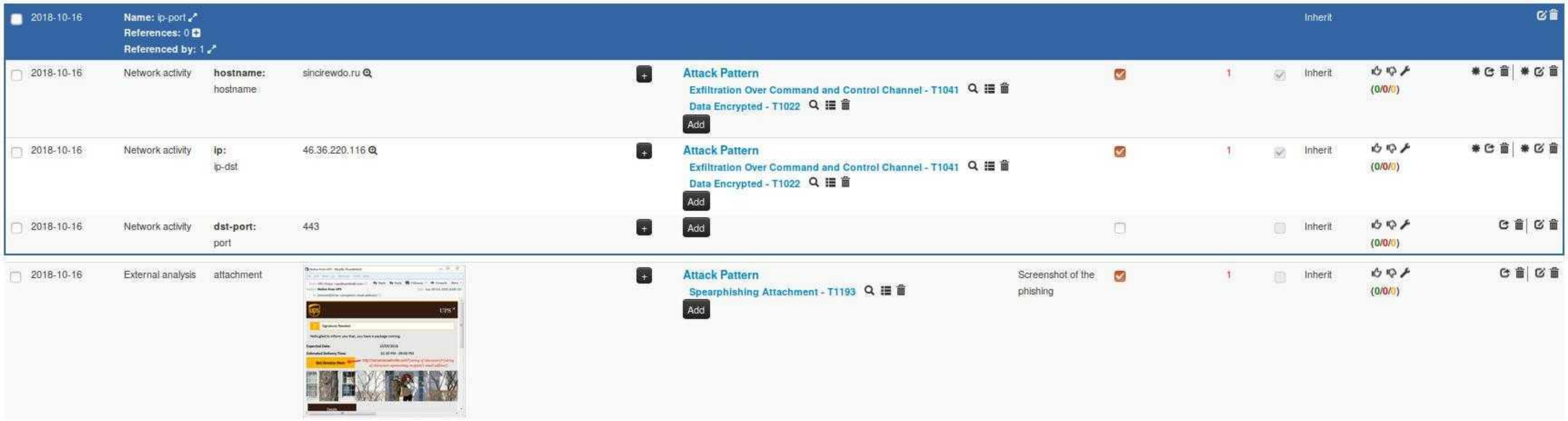
Attack Pattern

- + Exfiltration Over Command and Control Channel
- + Command-Line Interface
- + Data from Local System
- + File and Directory Discovery
- + Query Registry
- + System Information Discovery
- + Process Discovery
- + System Time Discovery

MISP
Threat Sharing

Courtesy of Alexandre Dulaunoy

Ways to Store and Display ATT&CK-Mapped Intel



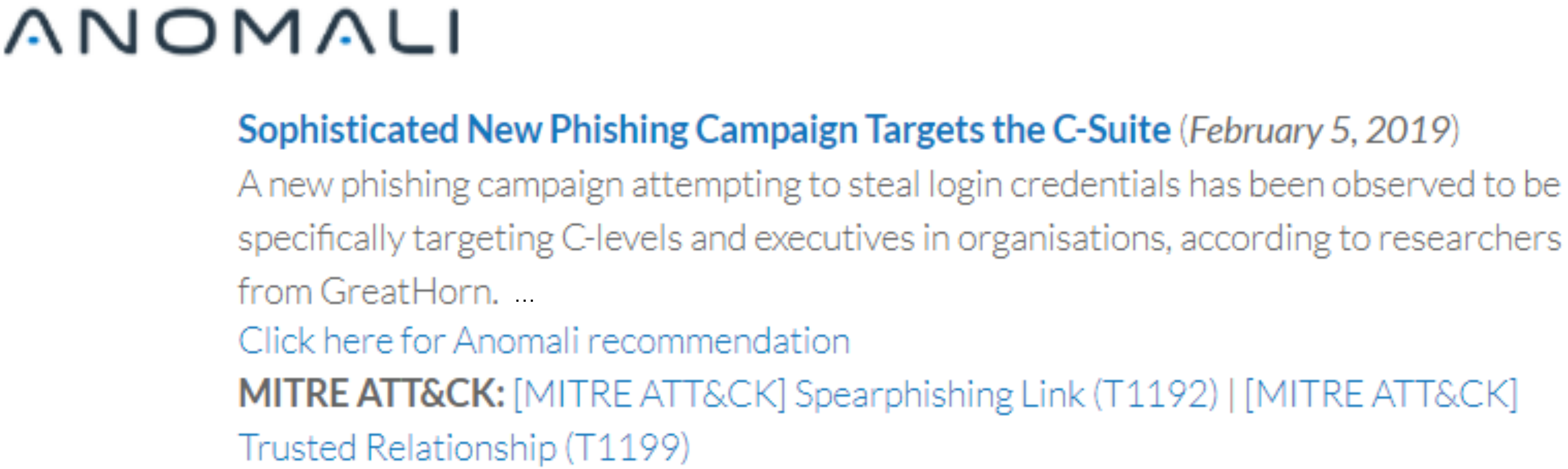
☐	2018-10-16	**Name:** ip-port **References:** 0 **Referenced by:** 1									Inherit	
☐	2018-10-16	Network activity	**hostname:** hostname	sincirewdo.ru	+	Attack Pattern Exfiltration Over Command and Control Channel - T1041 Data Encrypted - T1022 Add		☑	1	☑	Inherit	(0/0/0)
☐	2018-10-16	Network activity	**ip:** ip-dst	46.36.220.116	+	Attack Pattern Exfiltration Over Command and Control Channel - T1041 Data Encrypted - T1022 Add		☑	1	☑	Inherit	(0/0/0)
☐	2018-10-16	Network activity	**dst-port:** port	443	+	Add		☐		☐	Inherit	(0/0/0)
☐	2018-10-16	External analysis	attachment		+	Attack Pattern Spearphishing Attachment - T1193 Add	Screenshot of the phishing	☑	1	☐	Inherit	(0/0/0)

Courtesy of Alexandre Dulaunoy

Ability to link to indicators and files

MISP
Threat Sharing

Ways to Express and Store ATT&CK-Mapped Intel



ANOMALI

Sophisticated New Phishing Campaign Targets the C-Suite (*February 5, 2019*)

A new phishing campaign attempting to steal login credentials has been observed to be specifically targeting C-levels and executives in organisations, according to researchers from GreatHorn. ...

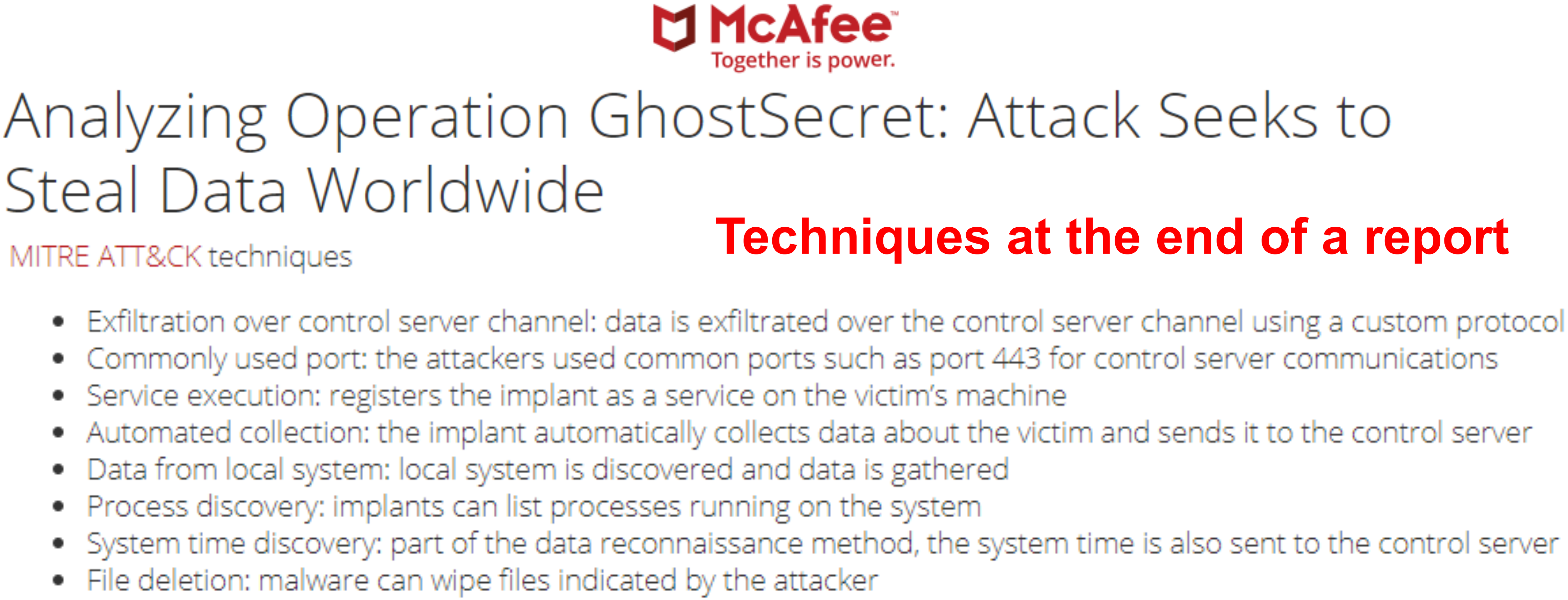
Click here for Anomali recommendation

MITRE ATT&CK: [MITRE ATT&CK] Spearphishing Link (T1192) | [MITRE ATT&CK] Trusted Relationship (T1199)

Techniques at the end of a report

https://www.anomali.com/blog/weekly-threat-briefing-google-spots-attacks-exploiting-ios-zero-day-flaws

Ways to Express and Store ATT&CK-Mapped Intel



McAfee
Together is power.

Analyzing Operation GhostSecret: Attack Seeks to Steal Data Worldwide

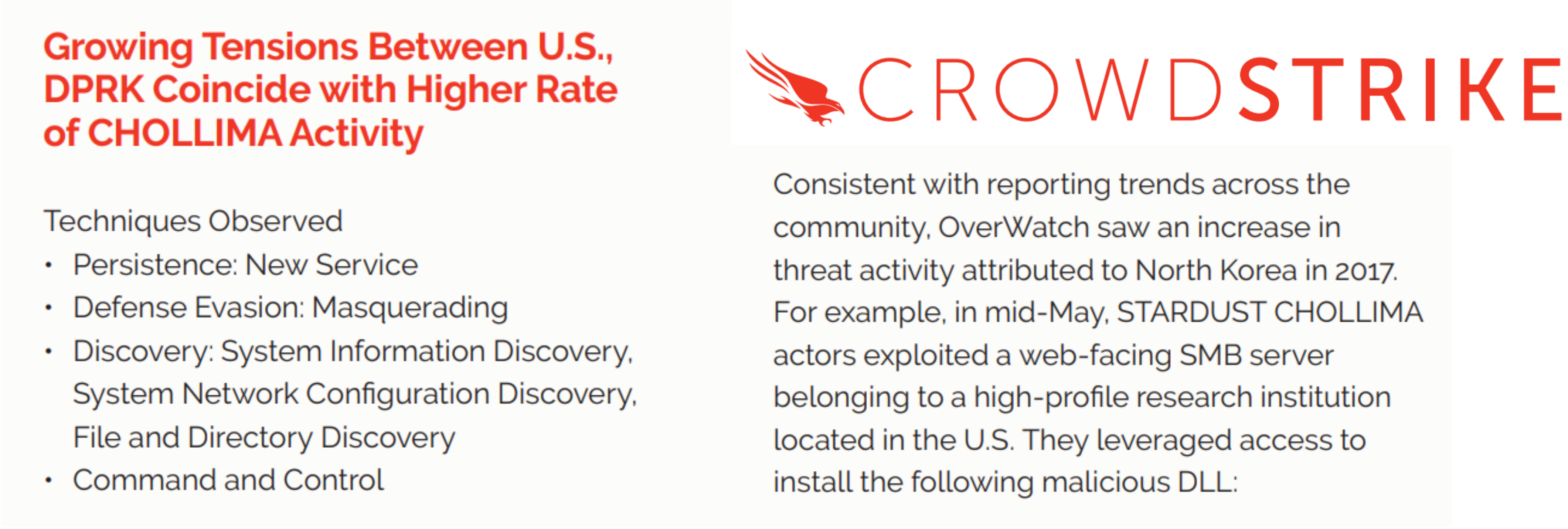
MITRE ATT&CK techniques

- Exfiltration over control server channel: data is exfiltrated over the control server channel using a custom protocol
- Commonly used port: the attackers used common ports such as port 443 for control server communications
- Service execution: registers the implant as a service on the victim's machine
- Automated collection: the implant automatically collects data about the victim and sends it to the control server
- Data from local system: local system is discovered and data is gathered
- Process discovery: implants can list processes running on the system
- System time discovery: part of the data reconnaissance method, the system time is also sent to the control server
- File deletion: malware can wipe files indicated by the attacker

Techniques at the end of a report

https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/analyzing-operation-ghostsecret-attack-seeks-to-steal-data-worldwide/

Ways to Express and Store ATT&CK-Mapped Intel



Growing Tensions Between U.S., DPRK Coincide with Higher Rate of CHOLLIMA Activity

Techniques Observed

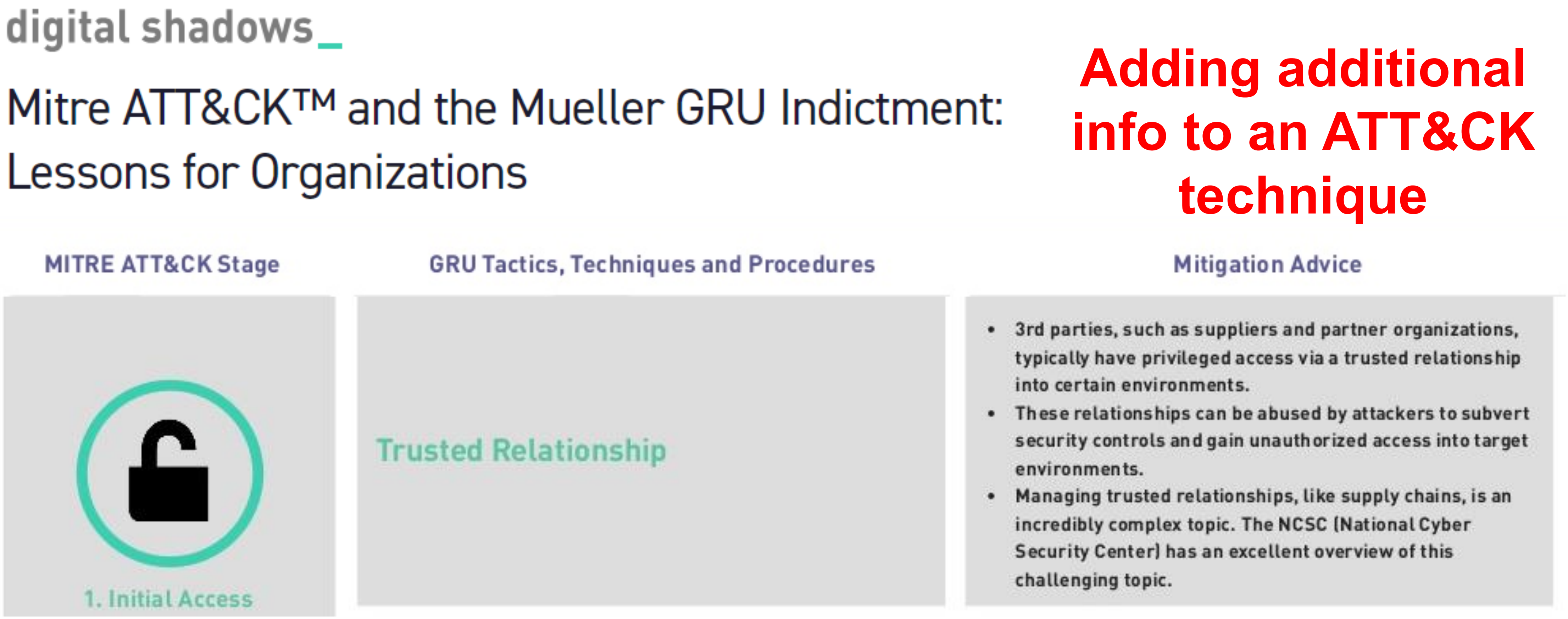
- Persistence: New Service
- Defense Evasion: Masquerading
- Discovery: System Information Discovery, System Network Configuration Discovery, File and Directory Discovery
- Command and Control

Consistent with reporting trends across the community, OverWatch saw an increase in threat activity attributed to North Korea in 2017. For example, in mid-May, STARDUST CHOLLIMA actors exploited a web-facing SMB server belonging to a high-profile research institution located in the U.S. They leveraged access to install the following malicious DLL:

Techniques at the beginning of a report

https://www.crowdstrike.com/resources/reports/2018-crowdstrike-global-threat-report-blurring-the-lines-between-statecraft-and-tradecraft/

Ways to Express and Store ATT&CK-Mapped Intel



digital shadows_

Mitre ATT&CK™ and the Mueller GRU Indictment: Lessons for Organizations

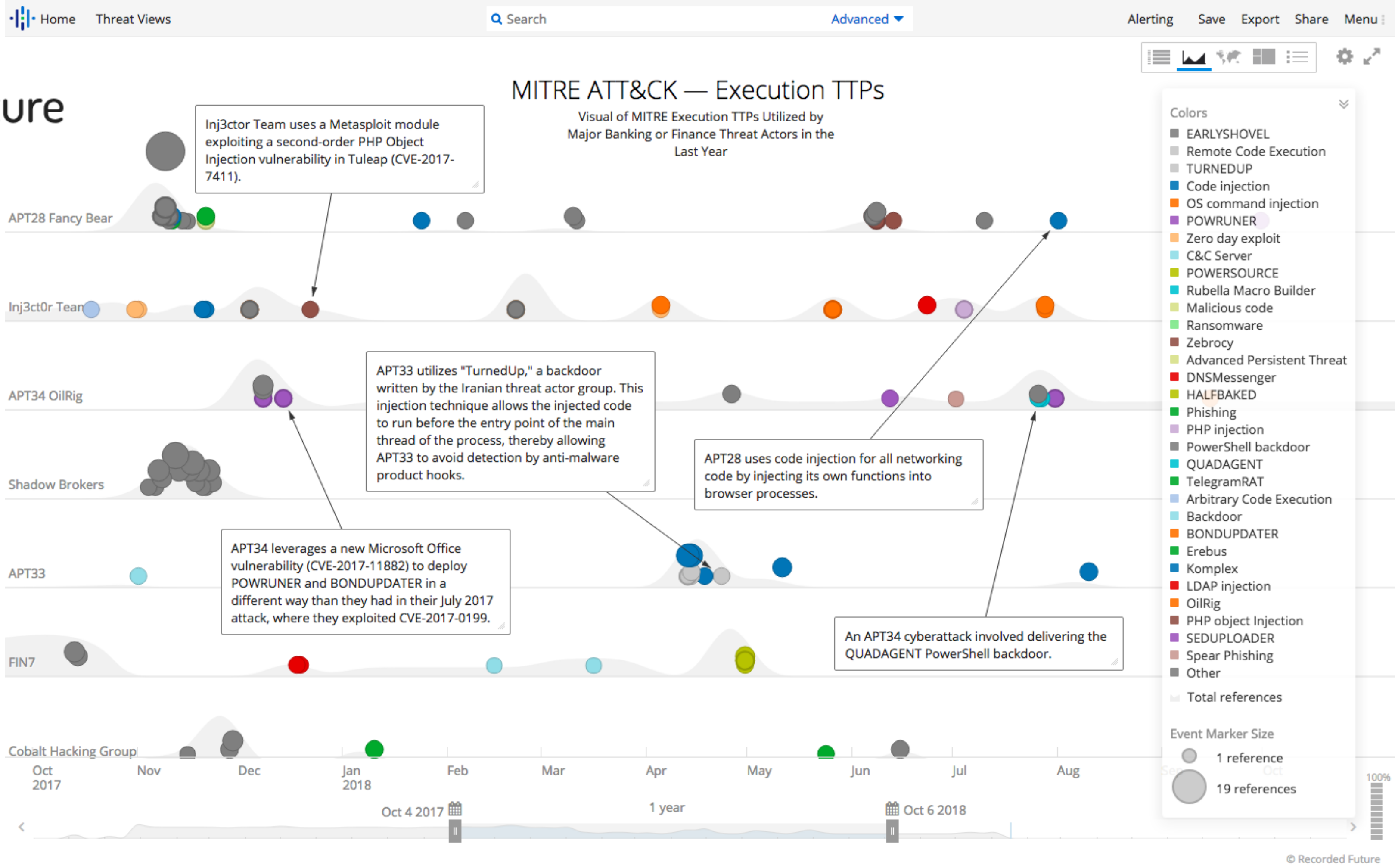
MITRE ATT&CK Stage	GRU Tactics, Techniques and Procedures	Mitigation Advice
1. Initial Access	Trusted Relationship	• 3rd parties, such as suppliers and partner organizations, typically have privileged access via a trusted relationship into certain environments. • These relationships can be abused by attackers to subvert security controls and gain unauthorized access into target environments. • Managing trusted relationships, like supply chains, is an incredibly complex topic. The NCSC (National Cyber Security Center) has an excellent overview of this challenging topic.

Adding additional info to an ATT&CK technique

https://www.digitalshadows.com/blog-and-research/mitre-attck-and-the-mueller-gru-indictment-lessons-for-organizations/

Ways to Express and Store ATT&CK-Mapped Intel

Recorded Future



MITRE ATT&CK — Execution TTPs

Visual of MITRE Execution TTPs Utilized by Major Banking or Finance Threat Actors in the Last Year

Inj3ctor Team uses a Metasploit module exploiting a second-order PHP Object Injection vulnerability in Tuleap (CVE-2017-7411).

APT33 utilizes "TurnedUp," a backdoor written by the Iranian threat actor group. This injection technique allows the injected code to run before the entry point of the main thread of the process, thereby allowing APT33 to avoid detection by anti-malware product hooks.

APT28 uses code injection for all networking code by injecting its own functions into browser processes.

APT34 leverages a new Microsoft Office vulnerability (CVE-2017-11882) to deploy POWRUNER and BONDUPDATER in a different way than they had in their July 2017 attack, where they exploited CVE-2017-0199.

An APT34 cyberattack involved delivering the QUADAGENT PowerShell backdoor.

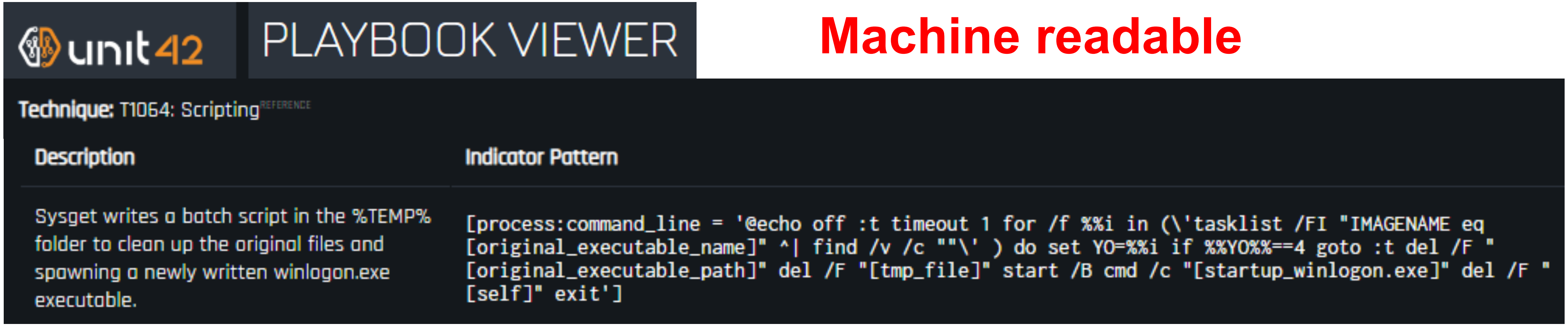
With timestamps

https://www.recordedfuture.com/mitre-attack-framework/

MITRE

Ways to Express and Store ATT&CK-Mapped Intel

Machine readable

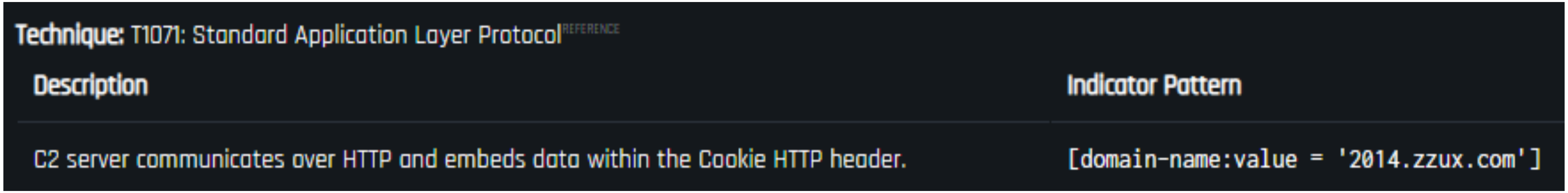


unit42 PLAYBOOK VIEWER

Technique: T1064: Scripting REFERENCE

<table>
<tr><th>Description</th><th>Indicator Pattern</th></tr>
<tr><td>Sysget writes a batch script in the %TEMP% folder to clean up the original files and spawning a newly written winlogon.exe executable.</td><td>[process:command_line = '@echo off :t timeout 1 for /f %%i in (\'tasklist /FI "IMAGENAME eq [original_executable_name]" ^| find /v /c ""\') do set YO=%%i if %%YO%%==4 goto :t del /F "[original_executable_path]" del /F "[tmp_file]" start /B cmd /c "[startup_winlogon.exe]" del /F "[self]" exit']</td></tr>
</table>

Linking techniques to indicators

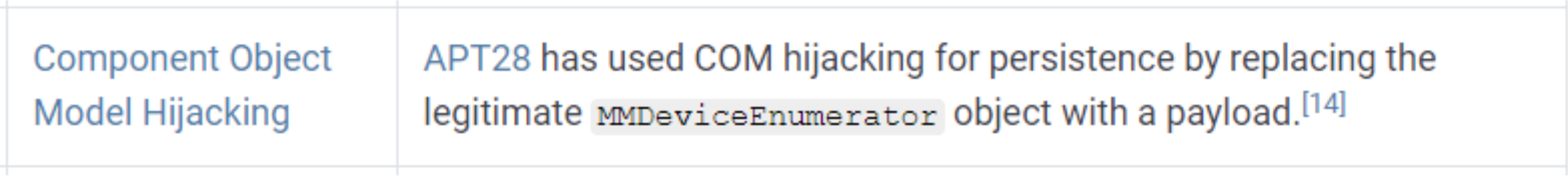


Technique: T1071: Standard Application Layer Protocol REFERENCE

Description	Indicator Pattern
C2 server communicates over HTTP and embeds data within the Cookie HTTP header.	[domain-name:value = '2014.zzux.com']

https://pan-unit42.github.io/playbook_viewer/

Ways to Express and Store ATT&CK-Mapped Intel

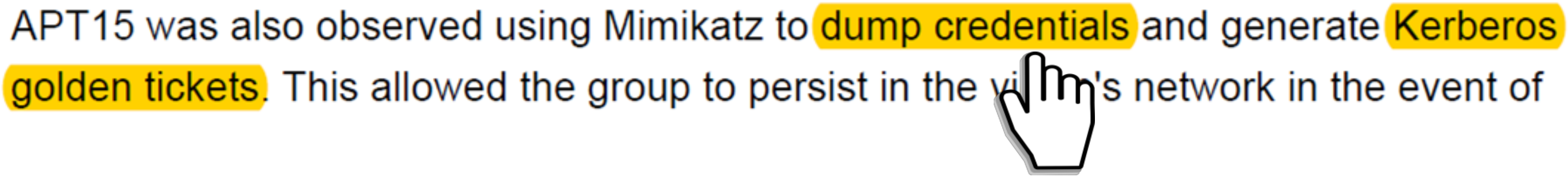


Component Object Model Hijacking	APT28 has used COM hijacking for persistence by replacing the legitimate `MMDeviceEnumerator` object with a payload.[14]

https://attack.mitre.org/groups/G0007/

What else could we do?

Full-Text Report



APT15 was also observed using Mimikatz to dump credentials and generate Kerberos golden tickets. This allowed the group to persist in the vi's network in the event of

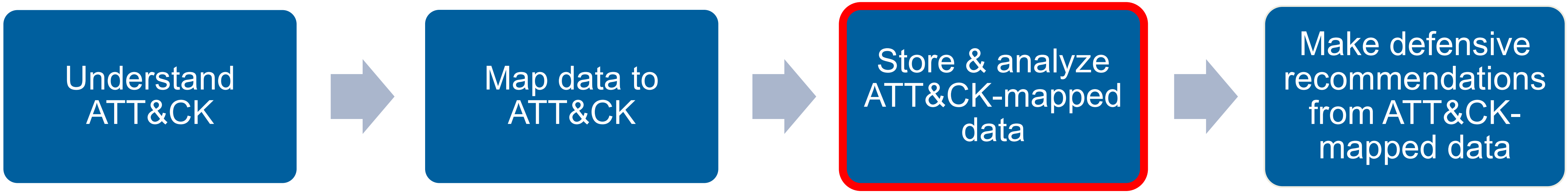
https://www.nccgroup.trust/us/about-us/newsroom-and-events/blog/2018/march/apt15-is-alive-and-strong-an-analysis-of-royalcli-and-royaldns/

ATT&CK Technique

Credential Dumping (T1003)

Process of Applying ATT&CK to CTI

So now we have some ATT&CK-mapped intel…



Understand ATT&CK

Map data to ATT&CK

Store & analyze ATT&CK-mapped data

Make defensive recommendations from ATT&CK-mapped data

What can we *do* with it?

APT28 Techniques*

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Automated Exfiltration	Commonly Used Port
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Data Compressed	Communication Through Removable Media
Hardware Additions	Command-Line Interface	AppCert DLLs	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discover	Distributed Component Object Model	Clipboard Data	Data Encrypted	Connection Proxy
Replication Through Removable Media	Control Panel Items	AppInit DLLs	AppInit DLLs	Bypass User Account Contr	Credential Dumping	File and Directory Discovery	Exploitation of Remote Services	Data from Information Repositories	Data Transfer Size Limits	Custom Command and Control Protocol
Spearphishing Attachment	Dynamic Data Exchange	Application Shimming	Application Shimming	Clear Command History	Credentials in Files	Network Service Scanning	Logon Scripts	Data from Local System	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol
Spearphishing Link	Execution through API	Authentication Package	Bypass User Account Contr	CMSTP	Credentials in Registry	Network Share Discovery	Pass the Hash	Data from Network Shared Drive	Exfiltration Over Command and Control Channel	Data Encoding
Spearphishing via Service	Execution through Module Load	BITS Jobs	DLL Search Order Hijacking	Code Signing	Exploitation for Credential Access	Password Policy Discovery	Pass the Ticket	Data from Removable Media	Exfiltration Over Other Network Medium	Data Obfuscation
Supply Chain Compromise	Exploitation for Client Execution	Bootkit	Dylib Hijacking	Component Firmware	Forced Authentication	Peripheral Device Discovery	Remote Desktop Protocol	Data Staged	Exfiltration Over Physical Medium	Domain Fronting
Trusted Relationship	Graphical User Interface	Browser Extensions	Exploitation for Privilege Escalation	Component Object Model Hijacking	Hooking	Permission Groups Discove	Remote File Copy	Email Collection	Scheduled Transfer	Fallback Channels
Valid Accounts	InstallUtil	Change Default File Association	Extra Window Memory Injection	Control Panel Items	Input Capture	Process Discovery	Remote Services	Input Capture		Multi-hop Proxy
	Launchctl	Component Firmware	File System Permissions Weakness	DCShadow	Input Prompt	Query Registry	Replication Through Removable Media	Man in the Browser		Multi-Stage Channels
	Local Job Scheduling	Component Object Model Hijacking	Hooking	Deobfuscate/Decode Files o Information	Kerberoasting	Remote System Discovery	Shared Webroot	Screen Capture		Multiband Communication
	LSASS Driver	Create Account	Image File Execution Option Injection	Disabling Security Tools	Keychain	Security Software Discovery	SSH Hijacking	Video Capture		Multilayer Encryption
	Mshta	DLL Search Order Hijacking	Launch Daemon	DLL Search Order Hijacking	LLMNR/NBT-NS Poisoning	System Information Discove	Taint Shared Content			Port Knocking
	PowerShell	Dylib Hijacking	New Service	DLL Side-Loading	Network Sniffing	System Network Configuration Discovery	Third-party Software			Remote Access Tools
	Regsvcs/Regasm	External Remote Services	Path Interception	Exploitation for Defense Evasion	Password Filter DLL	System Network Connection Discovery	Windows Admin Shares			Remote File Copy
	Regsvr32	File System Permissions Weakness	Plist Modification	Extra Window Memory Injection	Private Keys	System Owner/User Discovery	Windows Remote Management			Standard Application Layer Protocol
	Rundll32	Hidden Files and Directories	Port Monitors	File Deletion	Replication Through Removable Media	System Service Discovery				Standard Cryptographic Protocol
	Scheduled Task	Hooking	Process Injection	File System Logical Offsets	Securityd Memory	System Time Discovery				Standard Non-Application Layer Protocol
	Scripting	Hypervisor	Scheduled Task	Gatekeeper Bypass	Two-Factor Authentication Interception					Uncommonly Used Port
	Service Execution	Image File Execution Option Injection	Service Registry Permission Weakness	Hidden Files and Directories						Web Service
	Signed Binary Proxy Execution	Kernel Modules and Extensions	Setuid and Setgid	Hidden Users						
	Signed Script Proxy Execution	Launch Agent	SID-History Injection	Hidden Window						
	Source	Launch Daemon	Startup Items	HISTCONTROL						
	Space after Filename	Launchctl	Sudo	Image File Execution Options Injection						
	Third-party Software	LC_LOAD_DYLIB Addition	Sudo Caching	Indicator Blocking						
	Trap	Local Job Scheduling	Valid Accounts	Indicator Removal from Tools						
	Trusted Developer Utilities	Login Item	Web Shell	Indicator Removal on Host						
	User Execution	Logon Scripts		Indirect Command Execution						
	Windows Management Instrumentation	LSASS Driver		Install Root Certificate						
	Windows Remote Management	Modify Existing Service		InstallUtil						
		Netsh Helper DLL		Launchctl						
		New Service		LC_MAIN Hijacking						
		Office Application Startup		Masquerading						
		Path Interception		Modify Registry						
		Plist Modification		Mshta						
		Port Knocking		Network Share Connection Removal						
		Port Monitors		NTFS File Attributes						
		Rc.common		Obfuscated Files or Information						
		Re-opened Applications		Plist Modification						
		Redundant Access		Port Knocking						

*from open source reporting we've mapped

MITRE

APT29 Techniques

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	**Account Manipulation**	**Account Discovery**	AppleScript	Audio Capture	**Automated Exfiltration**	**Commonly Used Port**
Exploit Public-Facing Application	CMSTP	**Accessibility Features**	**Accessibility Features**	Binary Padding	Bash History	**Application Window Discovery**	Application Deployment Software	Automated Collection	**Data Compressed**	Communication Through Removable Media
Hardware Additions	**Command-Line Interface**	AppCert DLLs	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discover	Distributed Component Object Model	**Clipboard Data**	Data Encrypted	Connection Proxy
Replication Through Removable Media	Control Panel Items	AppInit DLLs	AppInit DLLs	**Bypass User Account Contro**	**Credential Dumping**	**File and Directory Discovery**	Exploitation of Remote Services	Data from Information Repositories	**Data Transfer Size Limits**	Custom Command and Control Protocol
Spearphishing Attachment	Dynamic Data Exchange	Application Shimming	Application Shimming	Clear Command History	**Credentials in Files**	Network Service Scanning	Logon Scripts	**Data from Local System**	**Exfiltration Over Alternative Protocol**	**Custom Cryptographic Protocol**
Spearphishing Link	Execution through API	Authentication Package	**Bypass User Account Contro**	CMSTP	Credentials in Registry	Network Share Discovery	**Pass the Hash**	**Data from Network Shared Drive**	Exfiltration Over Command and Control Channel	**Data Encoding**
Spearphishing via Service	Execution through Module Load	BITS Jobs	DLL Search Order Hijacking	**Code Signing**	Exploitation for Credential Access	Password Policy Discovery	**Pass the Ticket**	**Data from Removable Media**	Exfiltration Over Other Network Medium	**Data Obfuscation**
Supply Chain Compromise	**Exploitation for Client Execution**	Bootkit	Dylib Hijacking	Component Firmware	Forced Authentication	Peripheral Device Discovery	Remote Desktop Protocol	Data Staged	Exfiltration Over Physical Medium	**Domain Fronting**
Trusted Relationship	Graphical User Interface	Browser Extensions	**Exploitation for Privilege Escalation**	Component Object Model Hijacking	Hooking	Permission Groups Discove	**Remote File Copy**	**Email Collection**	Scheduled Transfer	**Fallback Channels**
Valid Accounts	InstallUtil	Change Default File Association	Extra Window Memory Injection	Control Panel Items	**Input Capture**	**Process Discovery**	Remote Services	**Input Capture**		**Multi-hop Proxy**
	Launchctl	Component Firmware	File System Permissions Weakness	**DCShadow**	Input Prompt	Query Registry	Replication Through Removable Media	Man in the Browser		Multi-Stage Channels
	Local Job Scheduling	Component Object Model Hijacking	Hooking	Deobfuscate/Decode Files o Information	Kerberoasting	Remote System Discovery	Shared Webroot	**Screen Capture**		Multiband Communication
	LSASS Driver	Create Account	Image File Execution Option Injection	Disabling Security Tools	Keychain	**Security Software Discovery**	SSH Hijacking	Video Capture		**Multilayer Encryption**
	Mshta	DLL Search Order Hijacking	Launch Daemon	DLL Search Order Hijacking	LLMNR/NBT-NS Poisoning	**System Information Discove**	Taint Shared Content			Port Knocking
	PowerShell	Dylib Hijacking	**New Service**	DLL Side-Loading	Network Sniffing	**System Network Configuration Discovery**	Third-party Software			Remote Access Tools
	Regsvcs/Regasm	External Remote Services	Path Interception	Exploitation for Defense Evasion	Password Filter DLL	System Network Connection Discovery	**Windows Admin Shares**			**Remote File Copy**
	Regsvr32	File System Permissions Weakness	Plist Modification	Extra Window Memory Injection	**Private Keys**	**System Owner/User Discovery**	Windows Remote Management			**Standard Application Layer Protocol**
	Rundll32	Hidden Files and Directories	Port Monitors	**File Deletion**	Replication Through Removable Media	**System Service Discovery**				**Standard Cryptographic Protocol**
	Scheduled Task	Hooking	Process Injection	File System Logical Offsets	Securityd Memory	**System Time Discovery**				Standard Non-Application Layer Protocol
	Scripting	Hypervisor	**Scheduled Task**	Gatekeeper Bypass	Two-Factor Authentication Interception					Uncommonly Used Port
	Service Execution	Image File Execution Option Injection	Service Registry Permission Weakness	Hidden Files and Directories						**Web Service**
	Signed Binary Proxy Execution	Kernel Modules and Extensions	Setuid and Setgid	Hidden Users						
	Signed Script Proxy Execution	Launch Agent	**SID-History Injection**	Hidden Window						
	Source	Launch Daemon	Startup Items	HISTCONTROL						
	Space after Filename	Launchctl	Sudo	Image File Execution Options Injection						
	Third-party Software	LC_LOAD_DYLIB Addition	Sudo Caching	Indicator Blocking						
	Trap	Local Job Scheduling	**Valid Accounts**	Indicator Removal from Tools						
	Trusted Developer Utilities	Login Item	Web Shell	**Indicator Removal on Host**						
	User Execution	Logon Scripts		Indirect Command Execution						
	Windows Management Instrumentation	LSASS Driver		Install Root Certificate						
	Windows Remote Management	Modify Existing Service		InstallUtil						
		Netsh Helper DLL		Launchctl						
		New Service		LC_MAIN Hijacking						
		Office Application Startup		**Masquerading**						
		Path Interception		Modify Registry						
		Plist Modification		Mshta						
		Port Knocking		Network Share Connection Removal						
		Port Monitors		**NTFS File Attributes**						
		Rc.common		**Obfuscated Files or Information**						
		Re-opened Applications		Plist Modification						
		Redundant Access		Port Knocking						

MITRE

Comparing APT28 and APT29

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	🟨 Access Token Manipulation	🟨 Access Token Manipulation	🟩 Account Manipulation	🟦 Account Discovery	AppleScript	Audio Capture	🟩 Automated Exfiltration	🟩 Commonly Used Port
Exploit Public-Facing Application	[illegible]	🟦 Accessibility Features	🟦 Accessibility Features	🟨 Binary Padding	Bash History	🟦 Application Window Discovery	Application Deployment Software	🟨 Automated Collection	🟩 Data Compressed	🟨 Communication Through Removable Media
Hardware Additions	🟩 Command-Line Interface	AppCert DLLs	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discover	Distributed Component Object Model	🟩 Clipboard Data	🟨 Data Encrypted	🟨 Connection Proxy
🟨 Replication Through Removable Media	Control Panel Items	AppInit DLLs	AppInit DLLs	🟦 Bypass User Account Contr	🟩 Credential Dumping	🟩 File and Directory Discovery	🟨 Exploitation of Remote Services	🟨 Data from Information Repositories	🟦 Data Transfer Size Limits	Custom Command and Control Protocol
🟩 Spearphishing Attachment	🟨 Dynamic Data Exchange	Application Shimming	Application Shimming	Clear Command History	🟩 Credentials in Files	🟨 Network Service Scanning	🟨 Logon Scripts	🟩 Data from Local System	🟦 Exfiltration Over Alternative Protocol	🟩 Custom Cryptographic Protocol
🟦 Spearphishing Link	🟨 Execution through API	Authentication Package	🟦 Bypass User Account Contr	CMSTP	Credentials in Registry	Network Share Discovery	🟩 Pass the Hash	🟦 Data from Network Shared Drive	🟨 Exfiltration Over Command and Control Channel	🟩 Data Encoding
Spearphishing via Service	Execution through Module Load	BITS Jobs	DLL Search Order Hijacking	🟦 Code Signing	Exploitation for Credential Access	Password Policy Discovery	🟩 Pass the Ticket	🟩 Data from Removable Media	Exfiltration Over Other Network Medium	🟩 Data Obfuscation
Supply Chain Compromise	🟦 Exploitation for Client Execution	🟨 Bootkit	Dylib Hijacking	Component Firmware	Forced Authentication	🟨 Peripheral Device Discovery	Remote Desktop Protocol	🟨 Data Staged	🟨 Exfiltration Over Physical Medium	🟦 Domain Fronting
Trusted Relationship	Graphical User Interface	Browser Extensions	🟩 Exploitation for Privilege Escalation	🟨 Component Object Model Hijacking	Hooking	Permission Groups Discove	🟩 Remote File Copy	🟦 Email Collection	🟨 Scheduled Transfer	🟩 Fallback Channels
🟩 Valid Accounts	InstallUtil	Change Default File Association	Extra Window Memory Injection	Control Panel Items	🟩 Input Capture	🟩 Process Discovery	Remote Services	🟩 Input Capture		🟦 Multi-hop Proxy
	Launchctl	Component Firmware	File System Permissions Weakness	🟩 DCShadow	Input Prompt	🟨 Query Registry	🟨 Replication Through Removable Media	Man in the Browser		Multi-Stage Channels
	Local Job Scheduling	🟨 Component Object Model Hijacking	Hooking	🟨 Deobfuscate/Decode Files o Information	Kerberoasting	Remote System Discovery	Shared Webroot	🟩 Screen Capture		Multiband Communication
	LSASS Driver	Create Account	Image File Execution Option Injection	Disabling Security Tools	Keychain	🟩 Security Software Discovery	SSH Hijacking	Video Capture		🟦 Multilayer Encryption
	Mshta	DLL Search Order Hijacking	Launch Daemon	DLL Search Order Hijacking	🟨 LLMNR/NBT-NS Poisoning	🟩 System Information Discove	Taint Shared Content			Port Knocking
	🟦 PowerShell	Dylib Hijacking	🟩 New Service	DLL Side-Loading	🟨 Network Sniffing	🟩 System Network Configuration Discovery	Third-party Software			Remote Access Tools
	Regsvcs/Regasm	External Remote Services	Path Interception	🟨 Exploitation for Defense Evasion	Password Filter DLL	System Network Connection Discovery	🟦 Windows Admin Shares			🟩 Remote File Copy
	Regsvr32	File System Permissions Weakness	Plist Modification	Extra Window Memory Injection	🟩 Private Keys	🟩 System Owner/User Discovery	Windows Remote Management			🟩 Standard Application Layer Protocol
	🟩 Rundll32	🟨 Hidden Files and Directories	Port Monitors	🟩 File Deletion	🟨 Replication Through Removable Media	🟦 System Service Discovery				🟩 Standard Cryptographic Protocol
	🟩 Scheduled Task	Hooking	🟨 Process Injection	File System Logical Offsets	Securityd Memory	🟦 System Time Discovery				Standard Non-Application Layer Protocol
	🟩 Scripting	Hypervisor	🟩 Scheduled Task	Gatekeeper Bypass	Two-Factor Authentication Interception					Uncommonly Used Port
	🟩 Service Execution	Image File Execution Option Injection	Service Registry Permission Weakness	🟨 Hidden Files and Directories						🟦 Web Service
	Signed Binary Proxy Execution	Kernel Modules and Extensions	Setuid and Setgid	Hidden Users						
	Signed Script Proxy Execution	🟨 Launch Agent	🟩 SID-History Injection	Hidden Window						
	Source	Launch Daemon	Startup Items	HISTCONTROL						
	Space after Filename	Launchctl	Sudo	Image File Execution Options Injection						
	Third-party Software	LC_LOAD_DYLIB Addition	Sudo Caching	Indicator Blocking						
	Trap	Local Job Scheduling	🟩 Valid Accounts	Indicator Removal from Tools						
	Trusted Developer Utilities	Login Item	Web Shell	🟩 Indicator Removal on Host						
	🟩 User Execution	🟨 Logon Scripts		🟨 Indirect Command Execution						
	🟦 Windows Management Instrumentation	LSASS Driver		🟨 Install Root Certificate						
	Windows Remote Management	Modify Existing Service		InstallUtil						
		Netsh Helper DLL		Launchctl						
		🟩 New Service		LC_MAIN Hijacking						
		🟨 Office Application Startup		🟩 Masquerading						
		Path Interception		🟨 Modify Registry						
		Plist Modification		Mshta						
		Port Knocking		Network Share Connection Removal						
		Port Monitors		🟦 NTFS File Attributes						
		Rc.common		🟩 Obfuscated Files or Information						
		Re-opened Applications		Plist Modification						
		Redundant Access		Port Knocking						

Overlay known gaps

🟨	APT28
🟦	APT29
🟩	Both groups

MITRE

ATT&CK Navigator

- One option for getting started with storing and analyzing in a simple way
- Open source (JSON), so you can customize it
- Allows you you visualize data

ATT&CK Navigator Demo Video

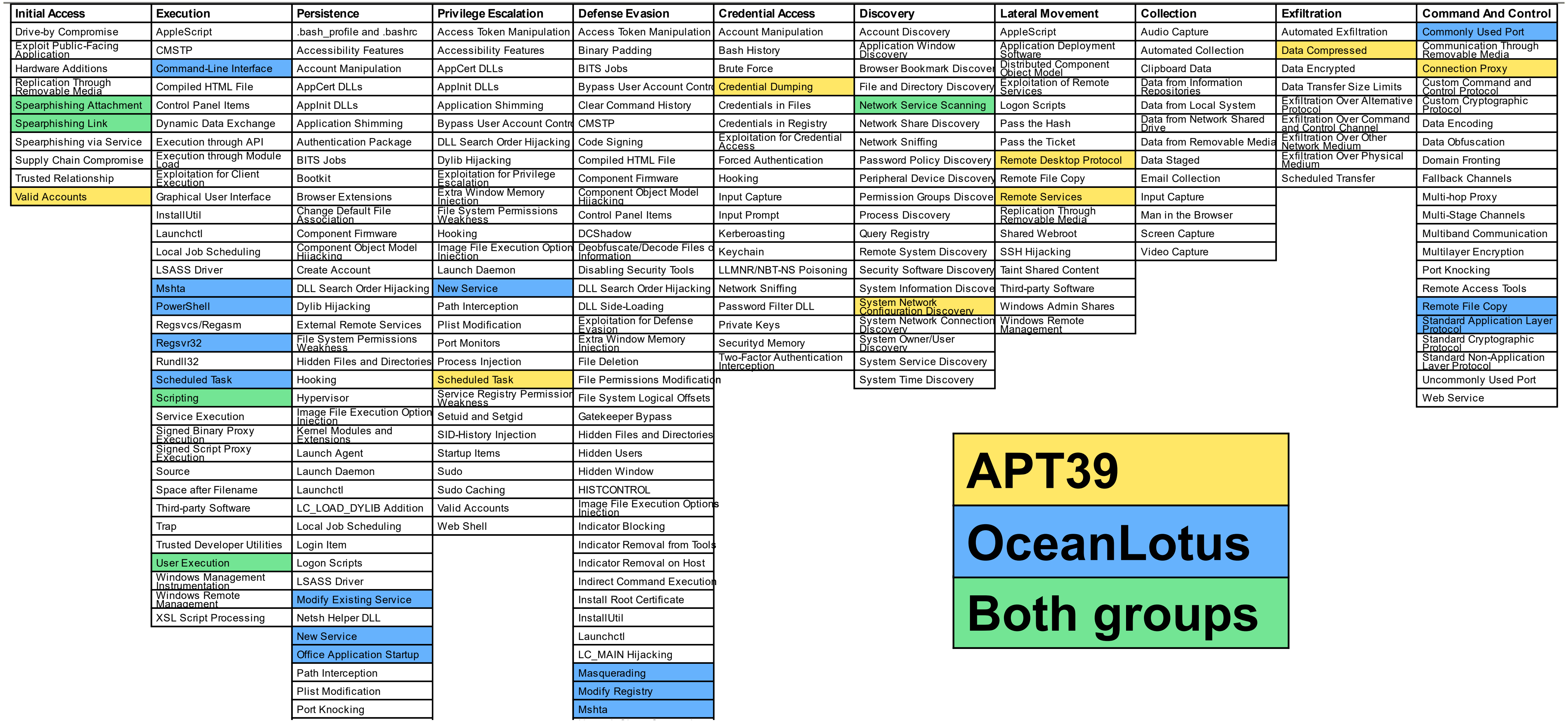
Exercise 4: Comparing Layers in ATT&CK Navigator

- **Docs you will need are at attack.mitre.org/training/cti under Exercise 4**
  - Step-by-step instructions are in the “Comparing Layers in Navigator” PDF
  - Techniques are listed in the “APT39 and Cobalt Kitty techniques” PDF

1. **Open ATT&CK Navigator: http://bit.ly/attacknav**
2. **Enter techniques from APT39 and Cobalt Kitty/OceanLotus into separate Navigator layers with a unique score for each layer’s techniques**
3. **Combine the layers in Navigator to create a third layer**
4. **Make your third layer look pretty**
5. **Make a list of the techniques that overlap between the two groups**

- ***Please pause. We suggest giving yourself 15 minutes for this exercise.***

Exercise 4: Comparing Layers in ATT&CK Navigator



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

🟨 **APT39**

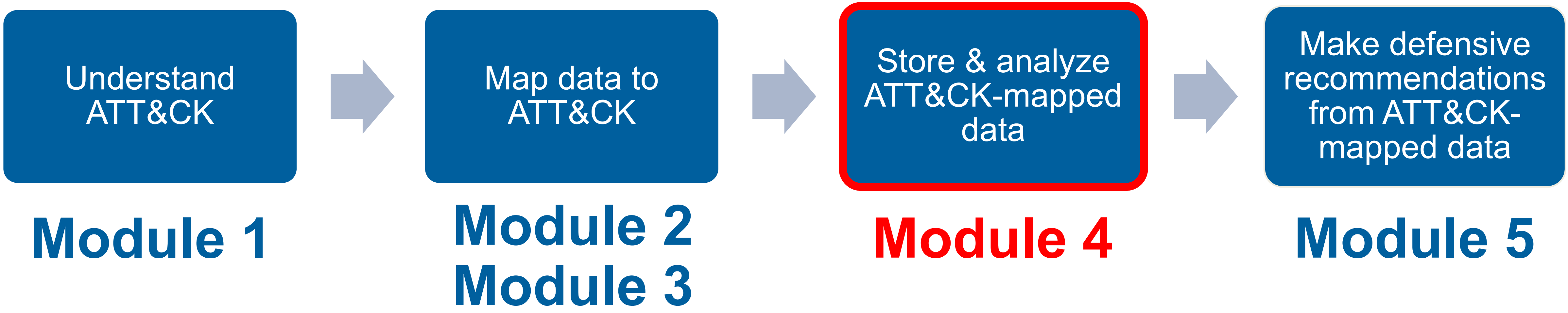
🟦 **OceanLotus**

🟩 **Both groups**

Exercise 4: Comparing Layers in ATT&CK Navigator

- **Here are the overlapping techniques:**
  1. Spearphishing Attachment
  2. Spearphishing Link
  3. Scheduled Task
  4. Scripting
  5. User Execution
  6. Registry Run Keys/Startup Folder
  7. Network Service Scanning

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 4