C3iHub
भारतीय प्रौद्योगिकी संस्थान कानपुर
Indian Institute of Technology Kanpur

CS 668:
Module 3.4:
Storing and Analyzing ATT&CK-Mapped Data

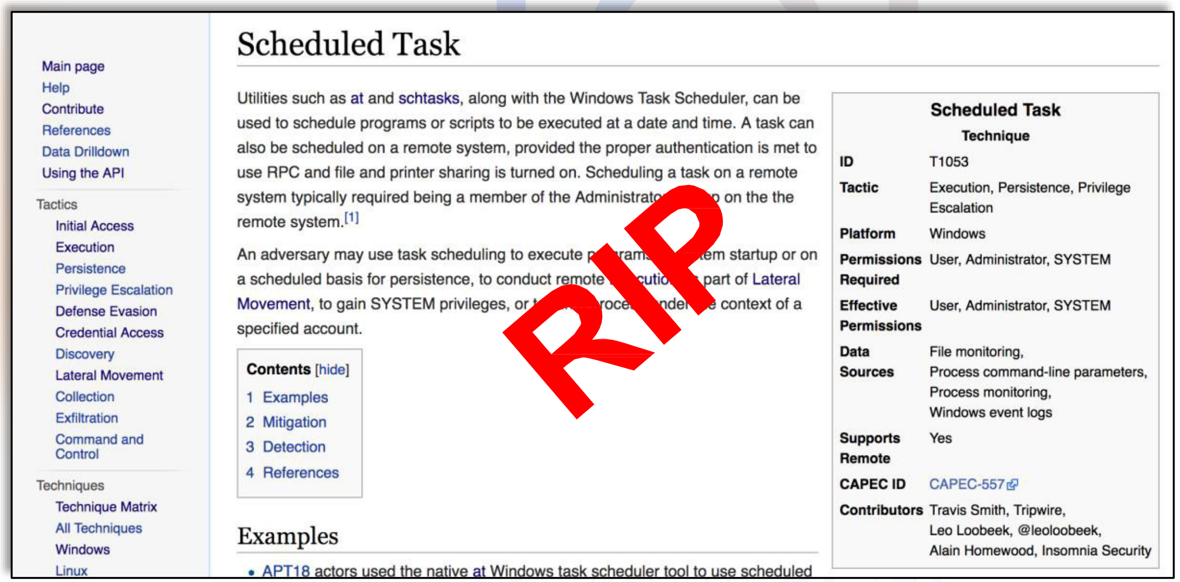
Considerations When Storing ATT&CK-Mapped Intel

- **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)_/¯



Main page
Help
Contribute
References
Data Drilldown
Using the API

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

Techniques
Technique Matrix
All Techniques
Windows
Linux

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 Administrato o on the the remote system.[1]

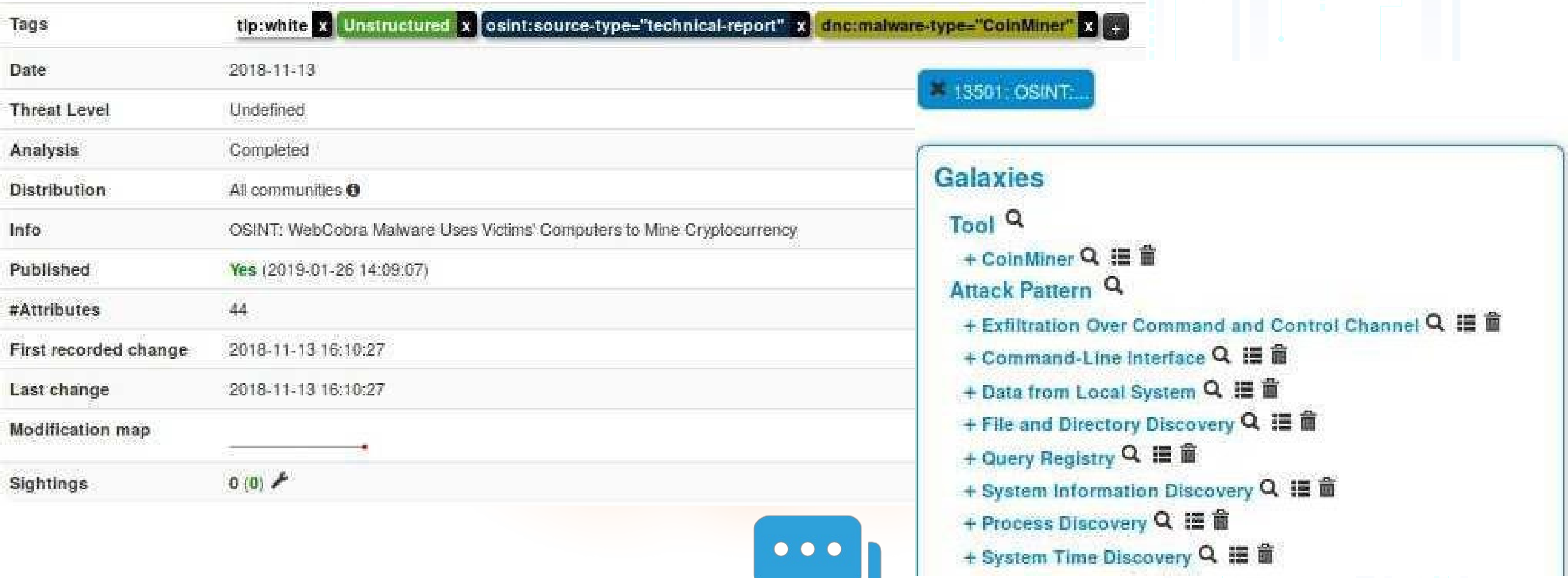
An adversary may use task scheduling to execute p ram em startup or on a scheduled basis for persistence, to conduct remote cutio part of Lateral Movement, to gain SYSTEM privileges, or t roce nde e context of a specified account.

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

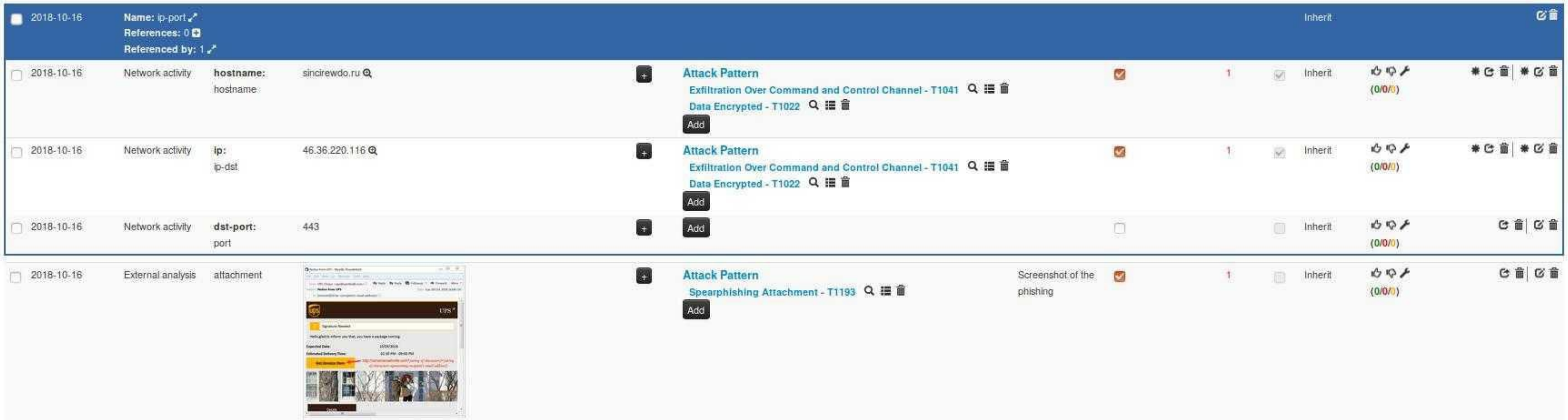
Attack Pattern

+ 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

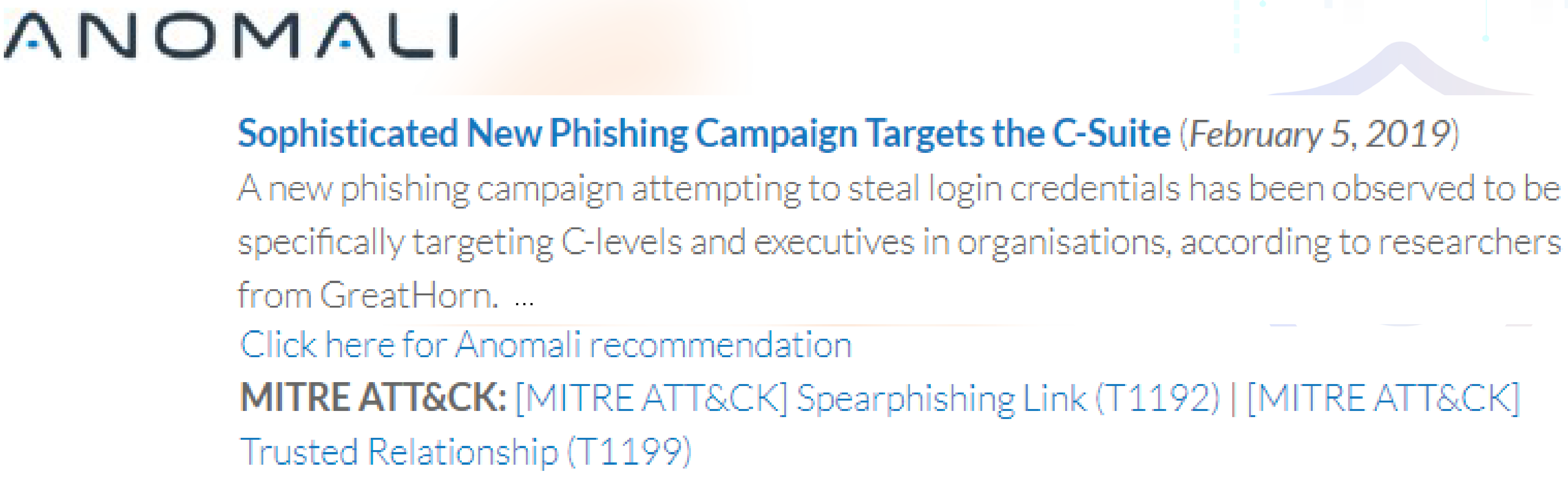


☐	2018-10-16	Name: ip-port References: 0 Referenced by: 1								Inherit	
☐	2018-10-16	Network activity	hostname: hostname	sincirewdo.ru	+	Attack Pattern Exfiltration Over Command and Control Channel - T1041 Data Encrypted - T1022 Add		☑	1	☑ Inherit	(0/0/0)
☐	2018-10-16	Network activity	ip: ip-dst	46.36.220.116	+	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

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. ...

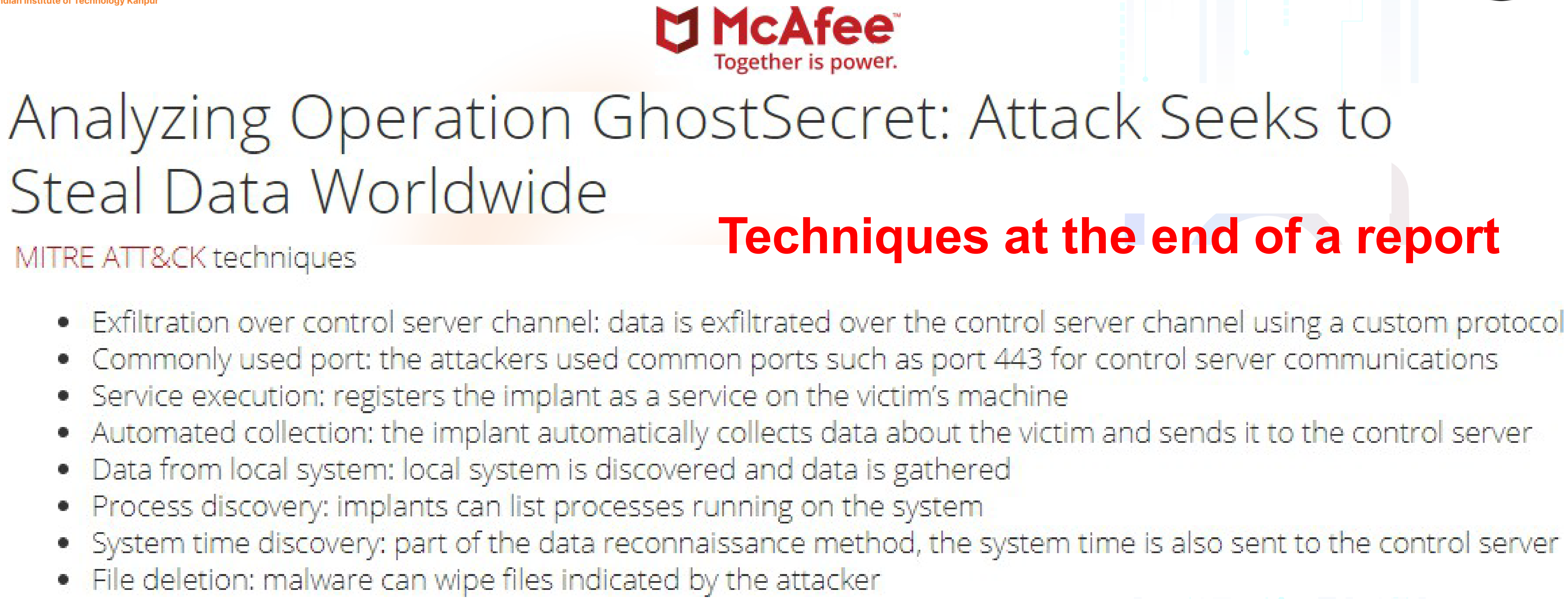
Click here for Anomali recommendation

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



Analyzing Operation GhostSecret: Attack Seeks to Steal Data Worldwide

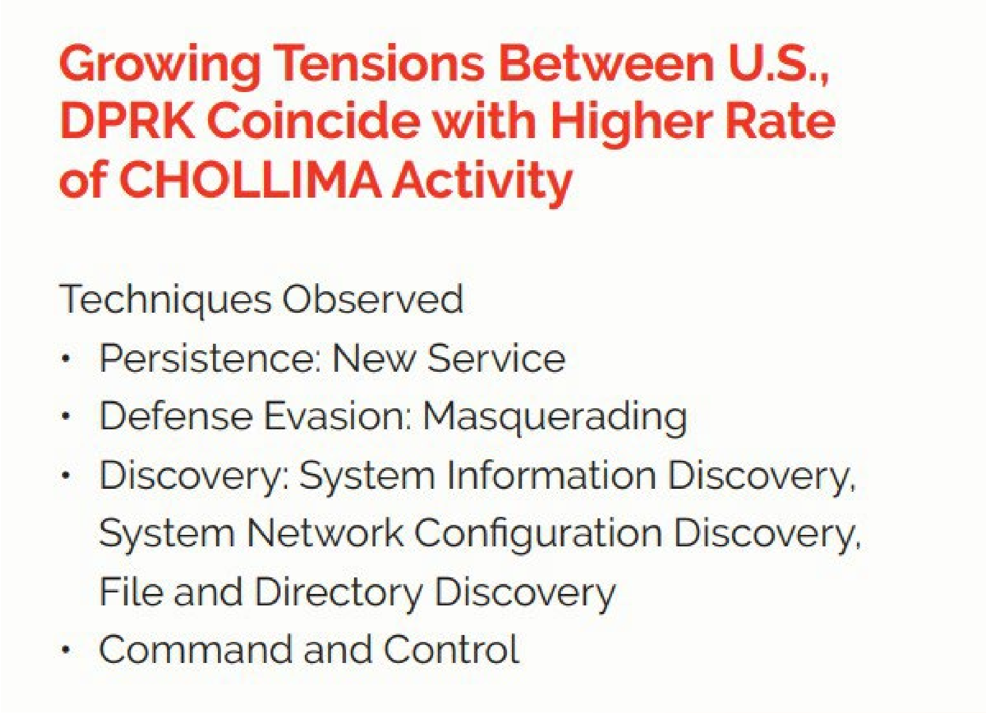
Techniques at the end of a report

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

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

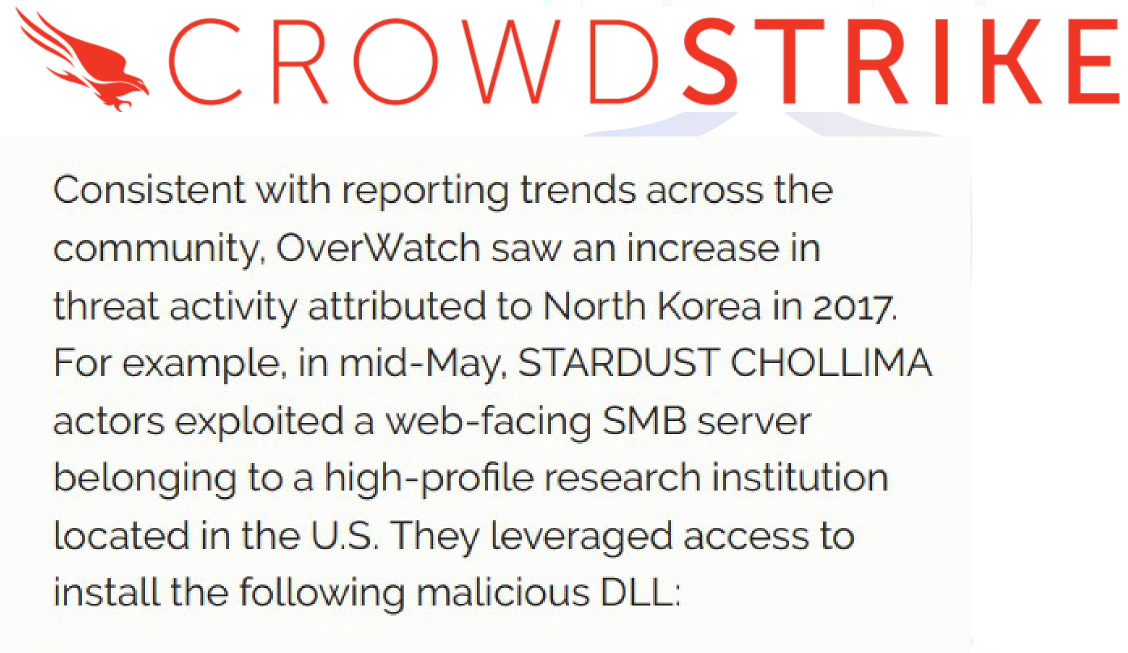
Ways to Express and Store ATT&CK-Mapped Intel



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



CROWDSTRIKE

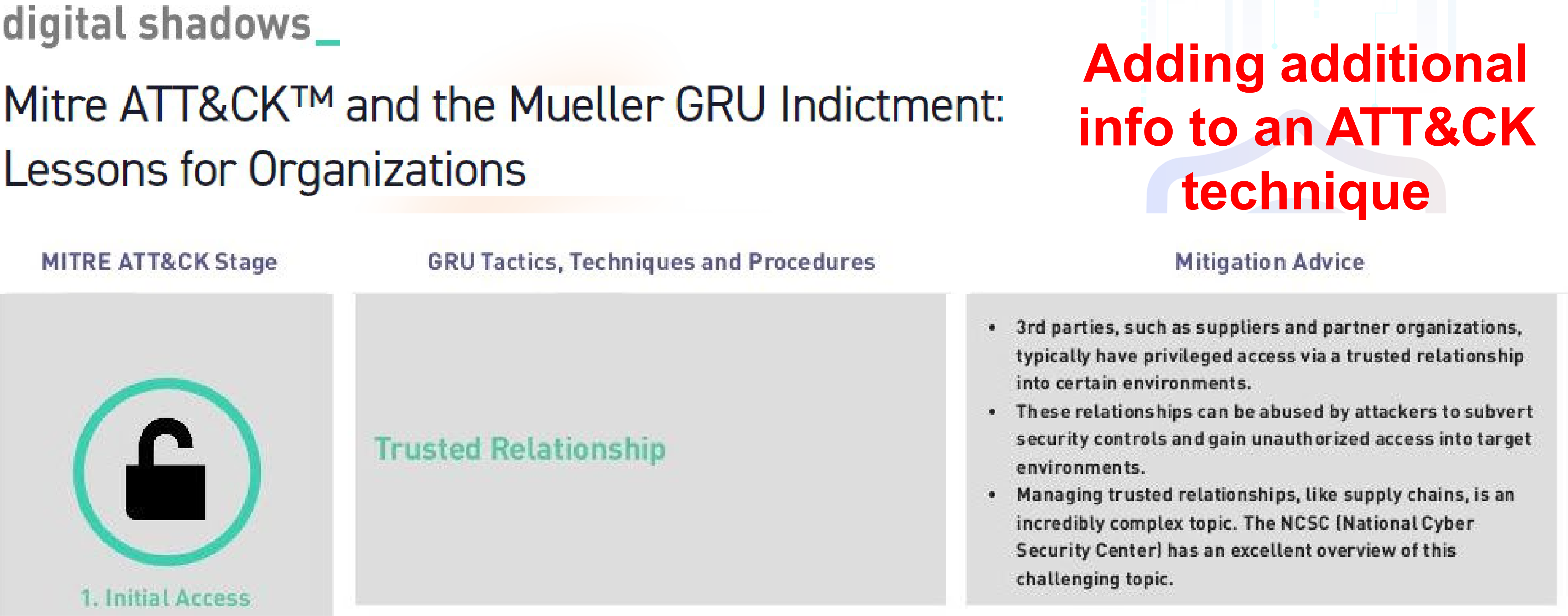
Consistent with reporting trends across the community, OverWatch saw an increase in threat activity attributed to North Korea in 2017. For example, in mid-May, STARDUST CHOLLIMA actors exploited a web-facing SMB server belonging to a high-profile research institution located in the U.S. They leveraged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

Adding additional info to an ATT&CK technique



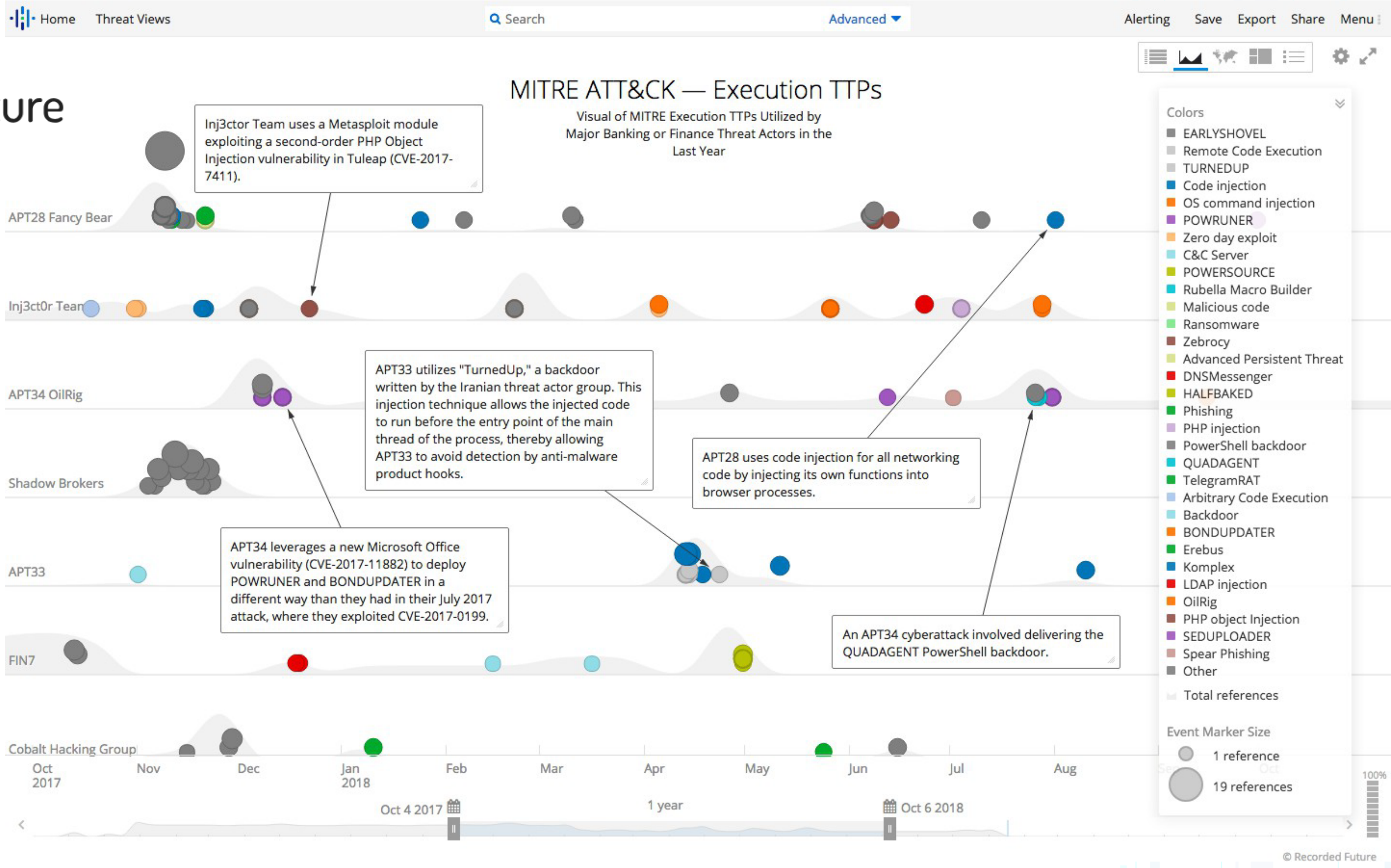
digital shadows_

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.

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



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.

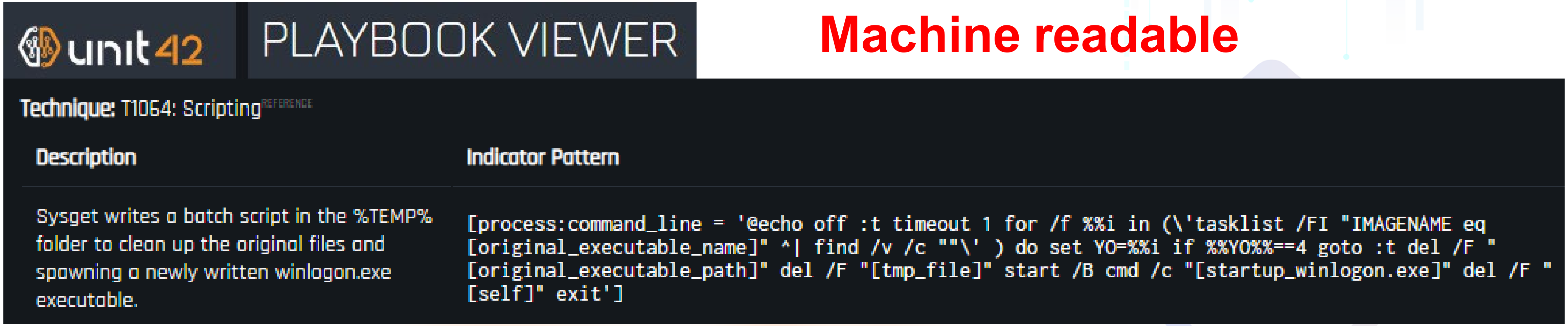
An APT34 cyberattack involved delivering the QUADAGENT PowerShell backdoor.

With timestamps

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

Ways to Express and Store ATT&CK-Mapped Intel

Machine readable

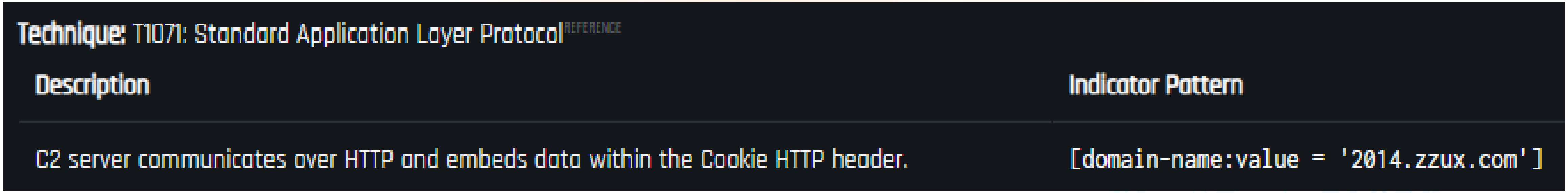


unit42 PLAYBOOK VIEWER

Technique: T1064: Scripting REFERENCE

Description	Indicator Pattern
Sysget writes a batch script in the %TEMP% folder to clean up the original files and spawning a newly written winlogon.exe executable.	`[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']`

Linking techniques to indicators

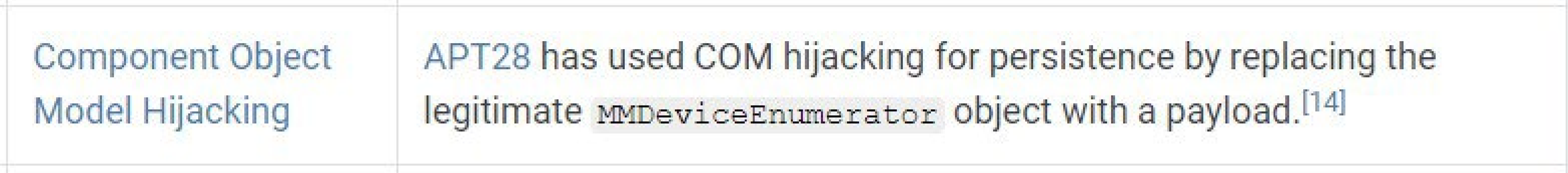


Technique: T1071: Standard Application Layer Protocol REFERENCE

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

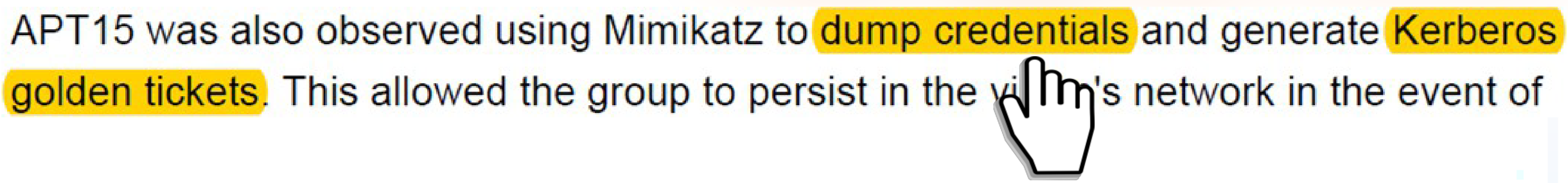


Component Object Model Hijacking	APT28 has used COM hijacking for persistence by replacing the legitimate `MMDeviceEnumerator` object with a payload.[14]

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[illegible]'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)

APT28 Techniques*

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
rive by Compromise	Apple cript	.bash profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account iscovery	Apple cript	Audio Capture	Automated xfiltration	Commonly sed ort
xploit ublic acing Application	CM T	Accessibility eatures	Accessibility eatures	inary adding	ash istory	Application Window iscovery	Application eployment oftware	Automated Collection	ata Compressed	Communication Through Removable Media
ardware Additions	Command ine Interface	AppCert s	AppCert s	IT obs	rute orce	rowser ookmark iscovery	istributed Component b ect Model	Clipboard ata	ata ncrypted	Connection roxy
Replication Through Removable Media	Control anel Items	AppInit s	AppInit s	ypass ser Account Control	Credential umping	ile and irectory iscovery	xploitation of Remote ervices	ata from Information Repositories	ata Transfer i e imits	Custom Command and Control rotocol
pearphishing Attachment	ynamic ata xchange	Application himming	Application himming	Clear Command istory	Credentials in iles	Network ervice canning	ogon cripts	ata from ocal ystem	xfiltration ver Alternative rotocol	Custom Cryptographic rotocol
pearphishing ink	xecution through A I	Authentication ackage	ypass ser Account Control	CM T	Credentials in Registry	Network hare iscovery	ass the ash	ata from Network hared rive	xfiltration ver Command and Control Channel	ata ncoding
pearphishing via ervice	xecution through Module oad	IT obs	earch rder i acking	Code igning	xploitation for Credential Access	assword olicy iscovery	ass the Ticket	ata from Removable Media	xfiltration ver ther Network Medium	ata bfuscation
upply Chain Compromise	xploitation for Client xecution	ootkit	ylib i acking	Component irmware	orced Authentication	eripheral evice iscovery	Remote esktop rotocol	ata taged	xfiltration ver hysical Medium	omain ronting
Trusted Relationship	raphical ser Interface	rowser xtensions	xploitation for rivilege scalation	Component b ect Model i acking	ooking	ermission roups iscovery	Remote ile Copy	mail Collection	cheduled Transfer	allback Channels
alid Accounts	Install til	Change efault ile Association	xtra Window Memory In ection	Control anel Items	Input Capture	rocess iscovery	Remote ervices	Input Capture		Multi hop roxy
	aunchctl	Component irmware	ile ystem ermissions Weakness	C hadow	Input rompt	uery Registry	Replication Through Removable Media	Man in the rowser		Multi tage Channels
	ocal ob cheduling	Component b ect Model i acking	ooking	eobfuscate ecode iles or Information	erberoasting	Remote ystem iscovery	hared Webroot	creen Capture		Multiband Communication
	A river	Create Account	Image ile xecution ptions In ection	isabling ecurity Tools	eychain	ecurity oftware iscovery	i acking	ideo Capture		Multilayer ncryption
	Mshta	earch rder i acking	aunch aemon	earch rder i acking	MNR N T N oisoning	ystem Information iscovery	Taint hared Content			ort nocking
	ower hell	ylib i acking	New ervice	ide oading	Network niffing	ystem Network Configuration iscovery	Third party oftware			Remote Access Tools
	Regsvcs Regasm	xternal Remote ervices	ath Interception	xploitation for efense vasion	assword ilter	ystem Network Connections iscovery	Windows Admin hares			Remote ile Copy
	Regsvr	ile ystem ermissions Weakness	list Modification	xtra Window Memory In ection	rivate eys	ystem wner ser iscovery	Windows Remote Management			tandard Application ayer rotocol
	Rundll	idden iles and irectories	ort Monitors	ile eletion	Replication Through Removable Media	ystem ervice iscovery				tandard Cryptographic rotocol
	cheduled Task	ooking	rocess In ection	ile ystem ogical ffsets	ecurityd Memory	ystem Time iscovery				tandard Non Application ayer rotocol
	cripting	ypervisor	cheduled Task	atekeeper ypass	Two actor Authentication Interception					ncommonly sed ort
	ervice xecution	Image ile xecution ptions In ection	ervice Registry ermissions Weakness	idden iles and irectories						Web ervice
	igned inary roxy xecution	ernel Modules and xtensions	etuid and etgid	idden sers						
	igned cript roxy xecution	aunch Agent	I istory In ection	idden Window						
	ource	aunch aemon	tartup Items	I T C NTR						
	pace after ilename	aunchctl	udo	Image ile xecution ptions In ection						
	Third party oftware	C A I Addition	udo Caching	Indicator locking						
	Trap	ocal ob cheduling	alid Accounts	Indicator Removal from Tools						
	Trusted eveloper tilities	ogin Item	Web hell	Indicator Removal on ost						
	ser xecution	ogon cripts		Indirect Command xecution						
	Windows Management Instrumentation	A river		Install Root Certificate						
	Windows Remote Management	Modify xisting ervice		Install til						
		Netsh elper		aunchctl						
		New ervice		C MAIN i acking						
		ffice Application tartup		Masquerading						
		ath Interception		Modify Registry						
		list Modification		Mshta						
		ort nocking		Network hare Connection Removal						
		ort Monitors		NT ile Attributes						
		Rc.common		bfuscated iles or Information						
		Re opened Applications		list Modification						
		Redundant Access		ort nocking						

*from open source reporting we’ve mapped

APT29 Techniques

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
rive by Compromise	Apple cript	.bash profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account iscovery	Apple cript	Audio Capture	Automated xfiltration	Commonly sed ort
xploit ublic acing Application	CM T	Accessibility eatures	Accessibility eatures	inary adding	ash istory	Application Window iscovery	Application eployment oftware	Automated Collection	ata Compressed	Communication Through Removable Media
ardware Additions	Command ine Interface	AppCert s	AppCert s	IT obs	rute orce	rowser ookmark iscovery	istributed Component b ect Model	Clipboard ata	ata ncrypted	Connection roxy
Replication Through Removable Media	Control anel Items	AppInit s	AppInit s	ypass ser Account Control	Credential umping	ile and irectory iscovery	xploitation of Remote ervices	ata from Information Repositories	ata Transfer i e imits	Custom Command and Control rotocol
pearphishing Attachment	ynamic ata xchange	Application himming	Application himming	Clear Command istory	Credentials in iles	Network ervice canning	ogon cripts	ata from ocal ystem	xfiltration ver Alternative rotocol	Custom Cryptographic rotocol
pearphishing ink	xecution through A I	Authentication ackage	ypass ser Account Control	CM T	Credentials in Registry	Network hare iscovery	ass the ash	ata from Network hared rive	xfiltration ver Command and Control Channel	ata ncoding
pearphishing via ervice	xecution through Module oad	IT obs	earch rder i acking	Code igning	xploitation for Credential Access	assword olicy iscovery	ass the Ticket	ata from Removable Media	xfiltration ver ther Network Medium	ata bfuscation
upply Chain Compromise	xploitation for Client xecution	ootkit	ylib i acking	Component irmware	orced Authentication	eripheral evice iscovery	Remote esktop rotocol	ata taged	xfiltration ver hysical Medium	omain ronting
Trusted Relationship	raphical ser Interface	rowser xtensions	xploitation for rivilege scalation	Component b ect Model i acking	ooking	ermission roups iscove	Remote ile Copy	mail Collection	cheduled Transfer	allback Channels
alid Accounts	Install til	Change efault ile Association	xtra Window Memory In ection	Control anel Items	Input Capture	rocess iscovery	Remote ervices	Input Capture		Multi hop roxy
	aunchctl	Component irmware	ile ystem ermissions Weakness	C hadow	Input rompt	uery Registry	Replication Through Removable Media	Man in the rowser		Multi tage Channels
	ocal ob cheduling	Component b ect Model i acking	ooking	eobfuscate ecode iles or Information	erberoasting	Remote ystem iscovery	hared Webroot	creen Capture		Multiband Communication
	A river	Create Account	Image ile xecution ptions In ection	isabling ecurity Tools	eychain	ecurity oftware iscovery	i acking	ideo Capture		Multilayer ncryption
	Mshta	earch rder i acking	aunch aemon	earch rder i acking	MNR N T N oisoning	ystem Information iscovery	Taint hared Content			ort nocking
	ower hell	ylib i acking	New ervice	ide oading	Network niffing	ystem Network Configuration iscovery	Third party oftware			Remote Access Tools
	Regsvcs Regasm	xternal Remote ervices	ath Interception	xploitation for efense vasion	assword ilter	ystem Network Connection iscovery	Windows Admin hares			Remote ile Copy
	Regsvr	ile ystem ermissions Weakness	list Modification	xtra Window Memory In ection	rivate eys	ystem wner ser iscovery	Windows Remote Management			tandard Application ayer rotocol
	Rundll	idden iles and irectories	ort Monitors	ile eletion	Replication Through Removable Media	ystem ervice iscovery				tandard Cryptographic rotocol
	cheduled Task	ooking	rocess In ection	ile ystem ogical ffsets	ecurityd Memory	ystem Time iscovery				tandard Non Application ayer rotocol
	cripting	ypervisor	cheduled Task	atekeeper ypass	Two actor Authentication Interception					ncommonly sed ort
	ervice xecution	Image ile xecution ptions In ection	ervice Registry ermissio ns Weakness	idden iles and irectories						Web ervice
	igned inary roxy xecution	ernel Modules and xtensions	etuid and etgid	idden sers						
	igned cript roxy xecution	aunch Agent	I istory In ection	idden Window						
	ource	aunch aemon	tartup Items	I T C NTR						
	pace after ilename	aunchctl	udo	Image ile xecution ptions In ection						
	Third party oftware	C A I Addition	udo Caching	Indicator locking						
	Trap	ocal ob cheduling	alid Accounts	Indicator Removal from Tools						
	Trusted eveloper tilities	ogin Item	Web hell	Indicator Removal on ost						
	ser xecution	ogon cripts		Indirect Command xecution						
	Windows Management Instrumentation	A river		Install Root Certificate						
	Windows Remote Management	Modify xisting ervice		Install til						
		Netsh elper		aunchctl						
		New ervice		C MAIN i acking						
		ffice Application tartup		Masquerading						
		ath Interception		Modify Registry						
		list Modification		Mshta						
		ort nocking		Network hare Connection Removal						
		ort Monitors		NT ile Attributes						
		Rc.common		bfuscated iles or Information						
		Re opened Applications		list Modification						
		Redundant Access		ort nocking						

Comparing APT28 and APT29

Initial Access

- rive by Compromise
- xploit ublic acing Application
- ardware Additions
- Replication Through Removable Media
- pearphishing Attachment
- pearphishing ink
- pearphishing via ervice
- upply Chain Compromise
- Trusted Relationship
- alid Accounts

Execution

- Apple cript
- Command ine Interface
- Cont
- ynamic ata xchange
- xecution through A I
- xecution through Module oad
- xploitation for Client xecution
- raphical ser Interface
- Install til
- aunchctl
- ocal ob cheduling
- A river
- Mshta
- ower hell
- Regsvcs Regasm
- Regsvr
- Rundll
- cheduled Task
- cripting
- ervice xecution
- igned inary roxy xecution
- igned cript roxy xecution
- ource
- pace after ilename
- Third party oftware
- Trap
- Trusted eveloper tilities
- ser xecution
- Windows Management Instrumentation
- Windows Remote Management

Persistence

- .bash profile and .bashrc
- Accessibility eatures
- Ap Cert s
- AppInit s
- Application himming
- Authentication ackage
- IT obs
- ootkit
- rowser xtensions
- Change efault ile Association
- Component irmware
- Component b ect Model i acking
- Create Account
- earch rder i acking
- ylib i acking
- xternal Remote ervices
- ile ystem ermissions Weakness
- idden iles and irectories
- ooking
- ypervisor
- Image ile xecution ptions In ection
- ernel Modules and xtensions
- aunch Agent
- aunch aemon
- aunchctl
- C A I Addition
- ocal ob cheduling
- ogin Item
- ogon cripts
- A river
- Modify xisting ervice
- Netsh elper
- New ervice
- ffice Application tartup
- ath Interception
- list Modification
- ort nocking
- ort Monitors
- Rc.common
- Re opened Applications
- Redundant Access

Privilege Escalation

- Access Token Manipulation
- Accessibility eatures
- AppCert s
- AppInit s
- Application himming
- ypass ser Account Control
- earch rder i acking
- i acking
- xploitation for rivilege scalation
- In ection
- ile ystem ermissions Weakness
- ooking
- Image ile xecution ptions In ection
- aunch aemon
- New ervice
- ath Interception
- list Modification
- ort Monitors
- rocess In ection
- cheduled Task
- ervice Registry ermissions Weakness
- etuid and etgid
- I istory In ection
- tartup Items
- udo
- udo Caching
- alid Accounts
- Web hell

Defense Evasion

- Access Token Manipulation
- inary adding
- IT obs
- ypass ser Account Control
- Clear Command istory
- C M T
- Code igning
- omponent irmware
- Co onent b ect Model king
- Control anel Items
- C hadow
- eobfuscate ecode iles or Information
- isabling ecurity Tools
- earch rder i acking
- ide oading
- xploitation for efense vasion
- xtra Window Memory In ection
- ile eletion
- ile ystem ogical ffsets
- atekeeper ypass
- idden iles and irectories
- idden sers
- idden Window
- I T C NTR
- Image ile xecution ptions In ection
- Indicator locking
- Indicator Removal from Tools
- Indicator Removal on ost
- Indirect Command xecution
- Install Root Certificate
- Install til
- aunchctl
- C MAIN i acking
- Masquerading
- Modify Registry
- Mshta
- Network hare Connection Removal
- NT ile Attributes
- bfuscated iles or Information
- list Modification
- ort nocking

Credential Access

- Account Manipulation
- ash istory
- rute orce
- Credential umping
- Credentials in iles
- Credentials in Registry
- xploitation for Credential Access
- orced Authentication
- Input Capture
- Input
- erberoasting
- eychain
- MNR N T N oisoning
- Network niffing
- assword ilter
- rivate eys
- Replication Through Removable Media
- ecurityd Memory
- Two actor Authentication Interception

Discovery

- Account iscovery
- Application Window iscovery
- rowser ookmark iscovery
- ile and irectory iscovery
- Network ervice canning
- Network hare iscovery
- assword olicy iscovery
- eripheral evice iscovery
- ermission roups iscovery
- ro ss iscovery
- uery Registry
- Remote ystem iscovery
- ecurity oftware iscovery
- ystem Information iscovery
- ystem Network Configuration iscovery
- ystem Network Connections iscovery
- ystem wner ser iscovery
- ystem ervice iscovery
- ystem Time iscovery

Lateral Movement

- Apple cript
- Application eployment oftware
- istributed Component b ect Model
- xploitation of Remote ervices
- ass the ash
- Remote esktop rotocol
- Remote ile Copy
- Remote ervices
- Replication Through Removable Media
- hared Webroot
- i acking
- Taint hared Content
- Third party oftware
- Windows Admin hares
- Windows Remote Management

Collection

- Audio Capture
- Automated Collection
- Clipboard ata
- ata from Information Repositories
- ata from ocal ystem
- a from Network hared ive
- ata from Removable Media
- ata taged
- mail Collection
- Input Capture
- Man in the rowser
- creen Capture
- ideo Capture

Exfiltration

- Automated xfiltration
- ata Compressed
- ata ncrypted
- ata Transfer i e imits
- xfiltration ver Alter ive rotocol
- xfiltration ver Command and Control Channel
- xfiltration ver ther Network Medium
- xfiltration ver hysical Medium
- cheduled Transfer

Command and Control

- Commonly sed ort
- Communication Through Removable Media
- Connection roxy
- Custom Command and
- Custom Cryptographic rotocol
- at
- ata bfuscation
- omain ronting
- allback Channels
- Multi hop roxy
- Multi tage Channels
- Multiband Communication
- Multilayer ncryption
- ort nocking
- Remote Access Tools
- Remote ile Copy
- tandard Application ayer rotocol
- tandard Cryptographic rotocol
- tandard Non Application ayer rotocol
- ncommonly sed ort
- Web ervice

Overlay known gaps

APT28

APT29

Both groups

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

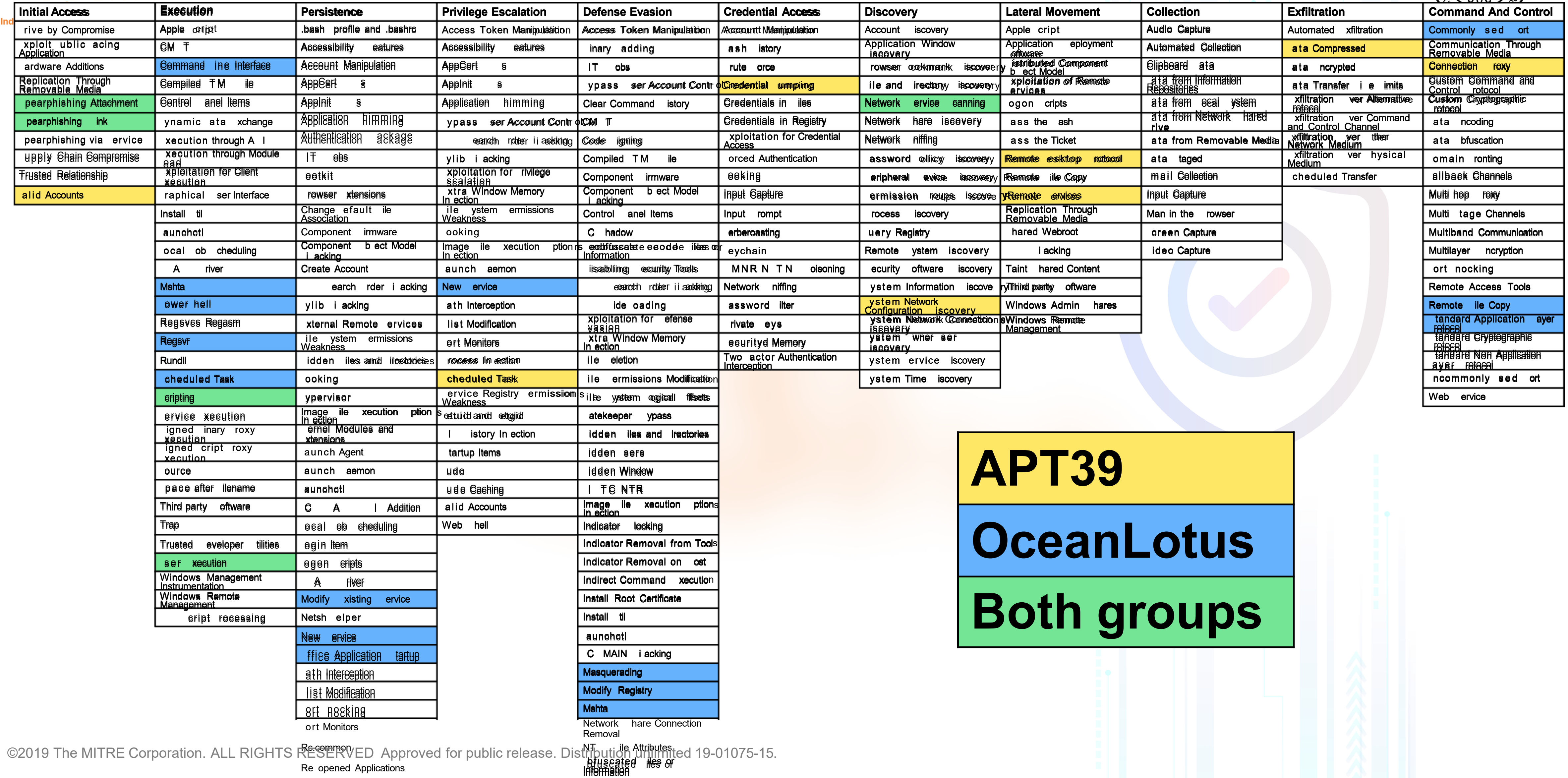
ATT&CK Navigator Demo

Exercise : 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 ayers in Navigator”
  - Techniques are listed in the “A T 9 and Cobalt itty techniques”

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**

Exercise: Comparing Layers in ATT&CK Navigator



Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command And Control
rive by Compromise	Apple cript	.bash profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account iscovery	Apple cript	Audio Capture	Automated xfiltration	🟦 Commonly sed ort
xploit ublic acing Application	CM T	Accessibility eatures	Accessibility eatures	inary adding	ash istory	Application Window iscovery	Application eployment oftware	Automated Collection	🟨 ata Compressed	Communication Through Removable Media
ardware Additions	🟦 Command ine Interface	Account Manipulation	AppCert s	IT obs	rute orce	rowser ookmark iscovery	istributed Component b ect Model	Clipboard ata	ata ncrypted	🟨 Connection roxy
Replication Through Removable Media	Compiled T M ile	AppCert s	AppInit s	ypass ser Account Contr ol	🟨 Credential umping	ile and irectory iscovery	xploitation of Remote ervices	ata from Information Repositories	ata Transfer i e imits	Custom Command and Control rotocol
🟩 pearphishing Attachment	Control anel Items	AppInit s	Application himming	Clear Command istory	Credentials in iles	🟩 Network ervice canning	ogon cripts	ata from ocal ystem	xfiltration ver Alternative rotocol	Custom Cryptographic rotocol
🟩 pearphishing ink	ynamic ata xchange	Application himming	ypass ser Account Contr ol	CM T	Credentials in Registry	Network hare iscovery	ass the ash	ata from Network hared rive	xfiltration ver Command and Control Channel	ata ncoding
pearphishing via ervice	xecution through A I	Authentication ackage	earch rder i acking	Code igning	xploitation for Credential Access	Network niffing	ass the Ticket	ata from Removable Media	xfiltration ver ther Network Medium	ata bfuscation
upply Chain Compromise	xecution through Module oad	IT obs	ylib i acking	Compiled T M ile	orced Authentication	assword olicy iscovery	🟨 Remote esktop rotocol	ata taged	xfiltration ver hysical Medium	omain ronting
Trusted Relationship	xploitation for Client xecution	ootkit	xploitation for rivilege scalation	Component irmware	ooking	eripheral evice iscovery	Remote ile Copy	mail Collection	cheduled Transfer	allback Channels
🟨 alid Accounts	raphical ser Interface	rowser xtensions	xtra Window Memory In ection	Component b ect Model i acking	Input Capture	ermission roups iscovery	🟨 Remote ervices	Input Capture		Multi hop roxy
	Install til	Change efault ile Association	ile ystem ermissions Weakness	Control anel Items	Input rompt	rocess iscovery	Replication Through Removable Media	Man in the rowser		Multi tage Channels
	aunchctl	Component irmware	ooking	C hadow	erberoasting	uery Registry	hared Webroot	creen Capture		Multiband Communication
	ocal ob cheduling	Component b ect Model i acking	Image ile xecution ption s In ection	eobfuscate ecode iles or Information	eychain	Remote ystem iscovery	i acking	ideo Capture		Multilayer ncryption
	A river	Create Account	aunch aemon	isabling ecurity Tools	MNR N T N oisoning	ecurity oftware iscovery	Taint hared Content			ort nocking
	🟦 Mshta	earch rder i acking	🟦 New ervice	earch rder i acking	Network niffing	ystem Information iscovery	Third party oftware			Remote Access Tools
	🟦 ower hell	ylib i acking	ath Interception	ide oading	assword ilter	🟨 ystem Network Configuration iscovery	Windows Admin hares			🟦 Remote ile Copy
	Regsves Regasm	xternal Remote ervices	list Modification	xploitation for efense vasion	rivate eys	ystem Network Connections iscovery	Windows Remote Management			🟦 tandard Application ayer rotocol
	🟦 Regsvr	ile ystem ermissions Weakness	ort Monitors	xtra Window Memory In ection	ecurityd Memory	ystem wner ser iscovery				tandard Cryptographic rotocol
	Rundll	idden iles and irectories	rocess In ection	ile eletion	Two actor Authentication Interception	ystem ervice iscovery				tandard Non Application ayer rotocol
	🟦 cheduled Task	ooking	🟨 cheduled Task	ile ermissions Modification		ystem Time iscovery				ncommonly sed ort
	🟩 cripting	ypervisor	ervice Registry ermission s Weakness	ile ystem ogical ffsets						Web ervice
	ervice xecution	Image ile xecution ption s In ection	etuid and etgid	atekeeper ypass						
	igned inary roxy xecution	ernel Modules and xtensions	I istory In ection	idden iles and irectories						
	igned cript roxy xecution	aunch Agent	tartup Items	idden sers						
	ource	aunch aemon	udo	idden Window						
	pace after ilename	aunchctl	udo Caching	I TC NTR						
	Third party oftware	C A I Addition	alid Accounts	Image ile xecution ptions In ection						
	Trap	ocal ob cheduling	Web hell	Indicator locking						
	Trusted eveloper tilities	ogin Item		Indicator Removal from Tools						
	🟩 ser xecution	ogon cripts		Indicator Removal on ost						
	Windows Management Instrumentation	A river		Indirect Command xecution						
	Windows Remote Management	🟦 Modify xisting ervice		Install Root Certificate						
	cript rocessing	Netsh elper		Install til						
		🟦 New ervice		aunchctl						
		🟦 ffice Application tartup		C MAIN i acking						
		ath Interception		🟦 Masquerading						
		list Modification		🟦 Modify Registry						
		ort nocking		🟦 Mshta						
		ort Monitors		Network hare Connection Removal						
		Re common		NT ile Attributes						
		Re opened Applications		bfuscated iles or Information						

🟨 APT39

🟦 OceanLotus

🟩 Both groups

Exercise: 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

C3iHub
भारतीय प्रौद्योगिकी संस्थान कानपुर
Indian Institute of Technology Kanpur

End of Module 3.4