4EC Ecuador

KARLA MORALES FOUNDATION

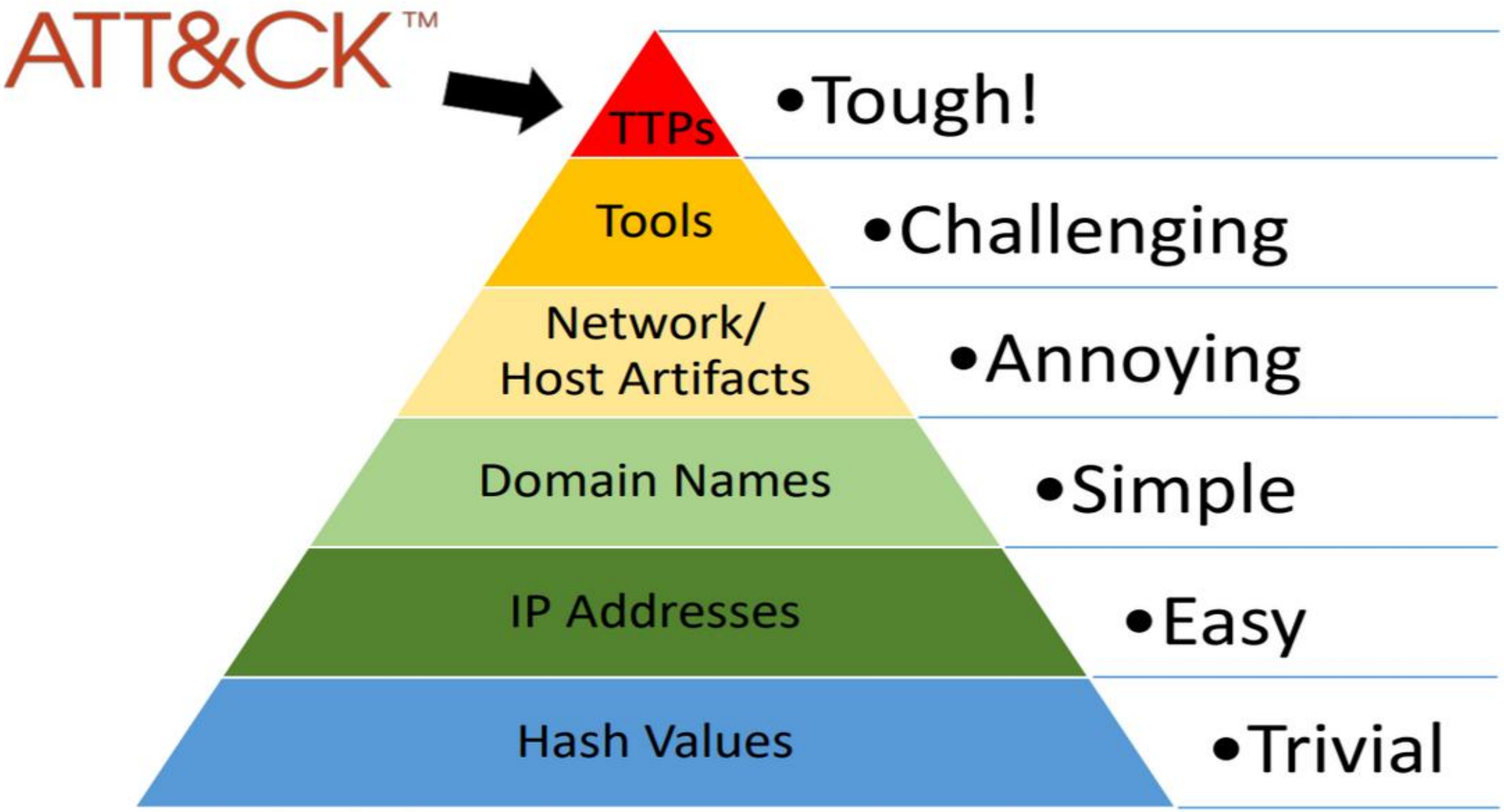
Cyber Threat Intelligence using MITRE ATT&CK™

LUIS SOLÍS

Términos

- Indicadores de Compromiso (IOC)
- Cyber Intelligence (CI)
- Cyber Threat Intelligence (CTI)

Pyrimed of Pain



ATT&CK™

TTPs – •Tough!

Tools – •Challenging

Network/ Host Artifacts – •Annoying

Domain Names – •Simple

IP Addresses – •Easy

Hash Values – •Trivial

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

MITRE ATT&CK

MITRE es una corporación no gubernamental fundada en 1958 cuya misión es intentar resolver problemas que contribuyan a un mundo más seguro.

MITTRE organiza y categoriza los distintos tipos de ciberataques, ciberamenazas y procedimientos realizados por los distintos grupos de atacantes en el ciberespacio.

ATT&CK?

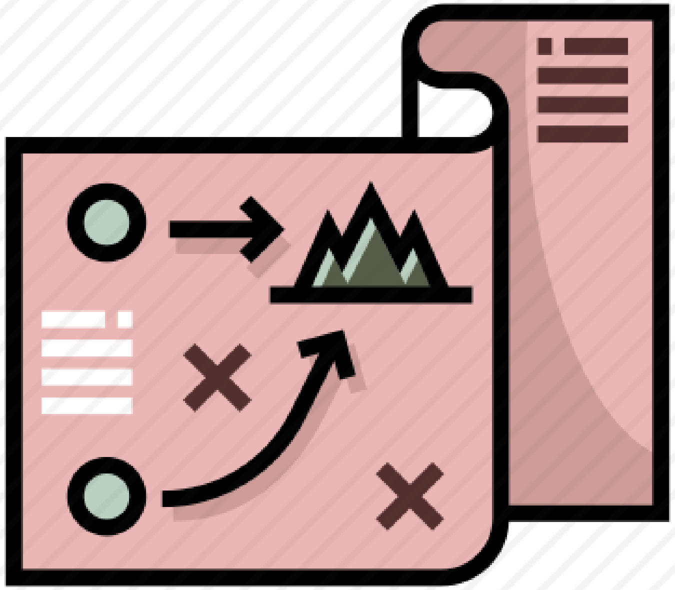
✓ Adversarial	Adversarios
✓ Tactics	Tácticas
✓ Techniques	Técnicas
✓ &	
✓ Common Knowledge	Conocimiento Común

El modelo ATT&CK

- Es un conjunto de procedimientos que representan acciones que puede realizar un adversario para cumplir sus objetivos. Estos objetivos son categorizados como tácticas, las cuales agrupan técnicas usadas por los adversarios.
- Es una base de conocimientos accesible a nivel mundial. Dicha base contiene información sobre técnicas adversas basadas en observaciones del mundo real.

MITRE - TTI

Tácticas



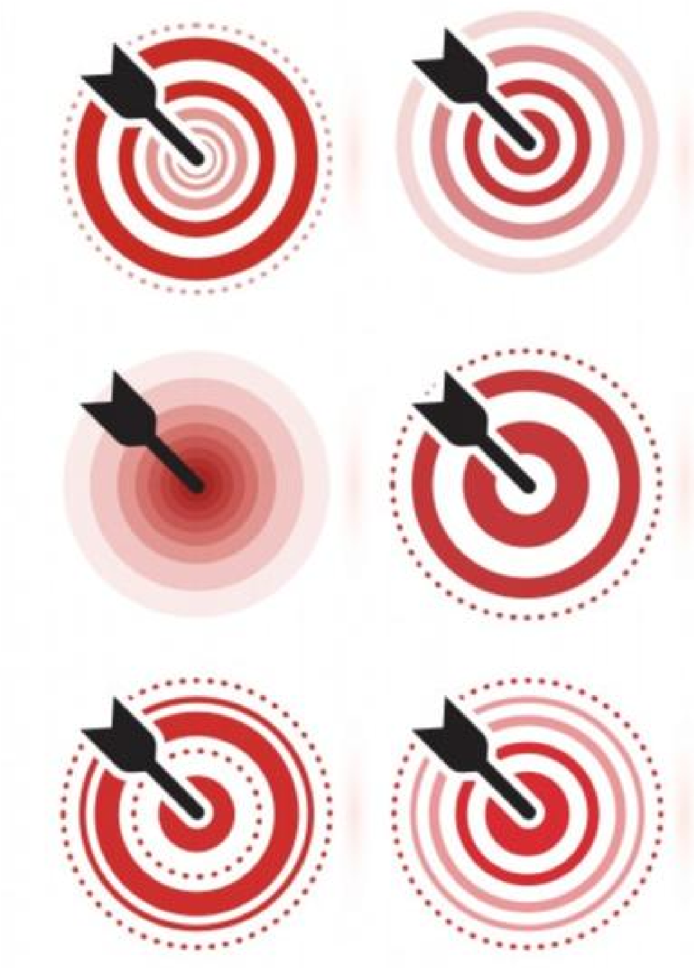
MITTRE - TTI

Técnicas

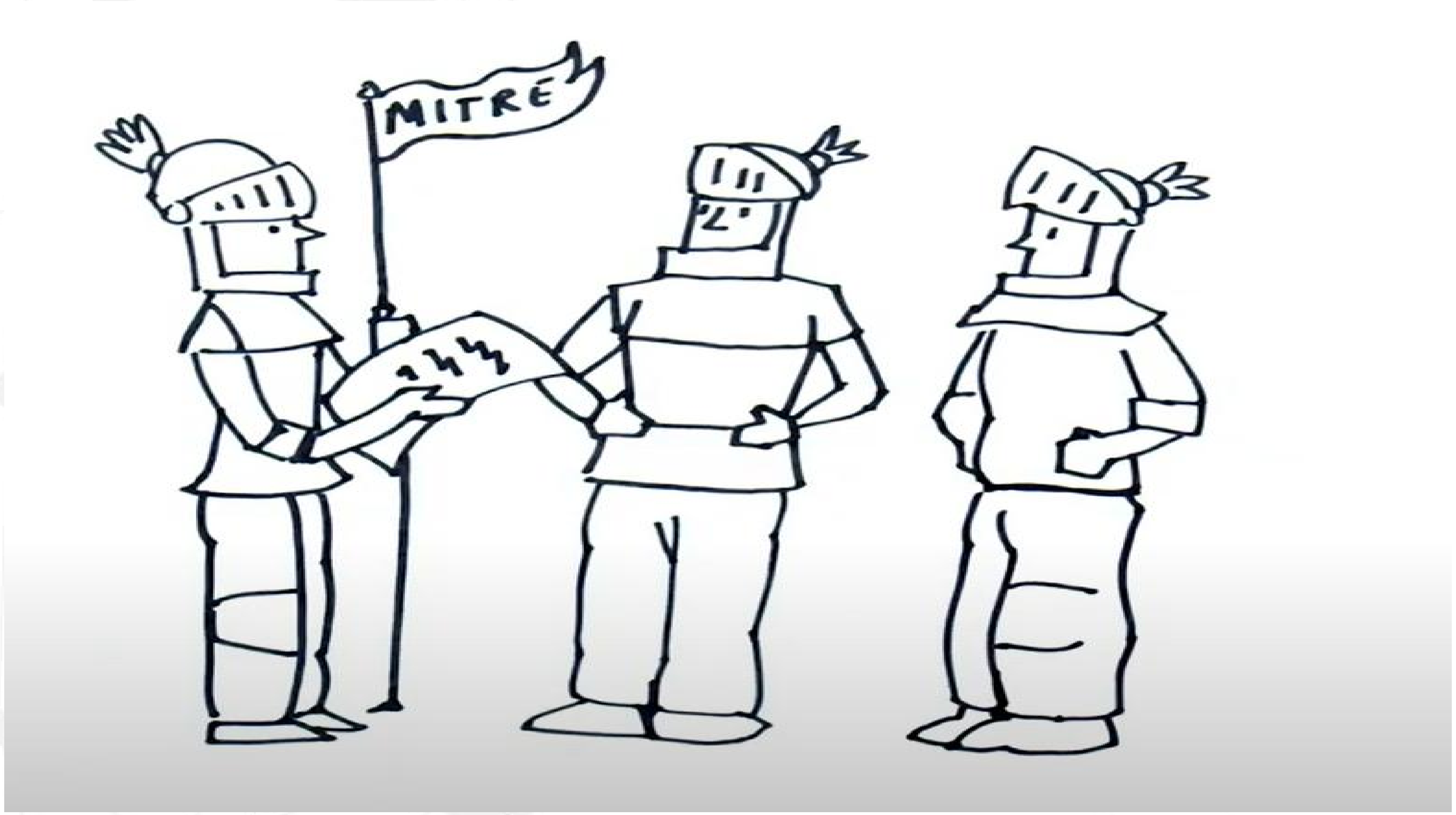
MITTRE - TTI

Procedimientos

MITTRE - TTI



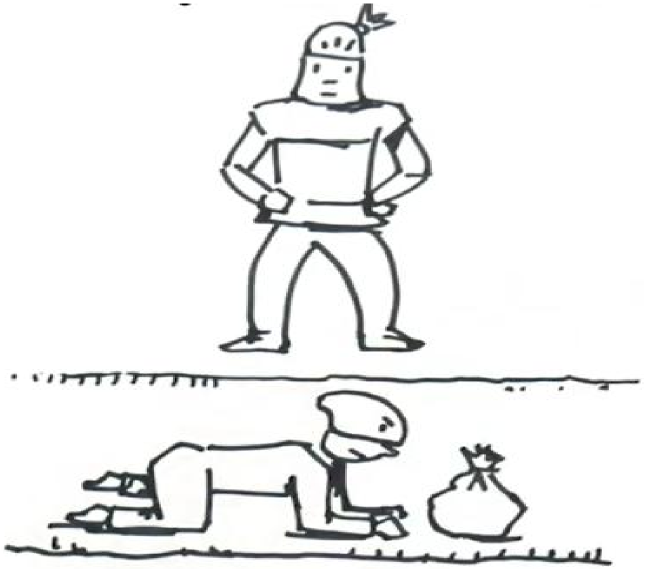
MITTRE - TTI



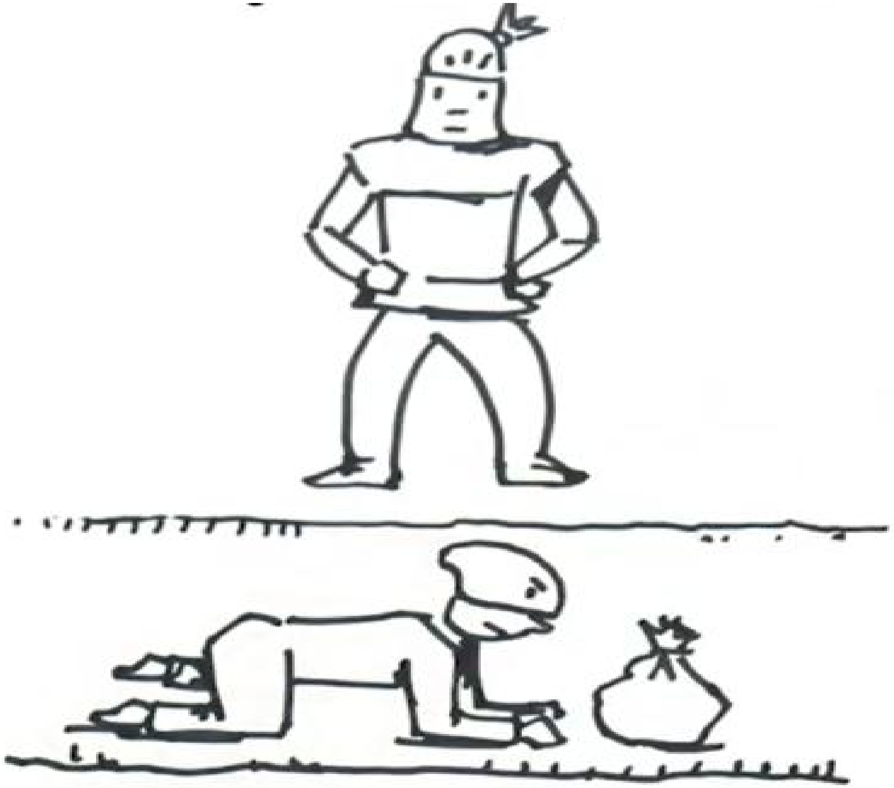
MITTRE - TTI

Defense Evasion

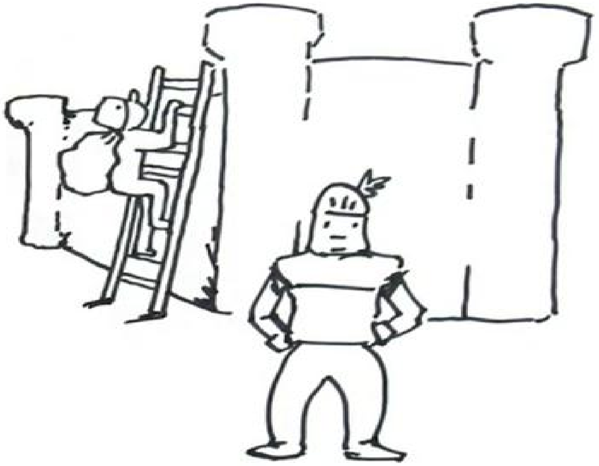
MITTRE - TTI



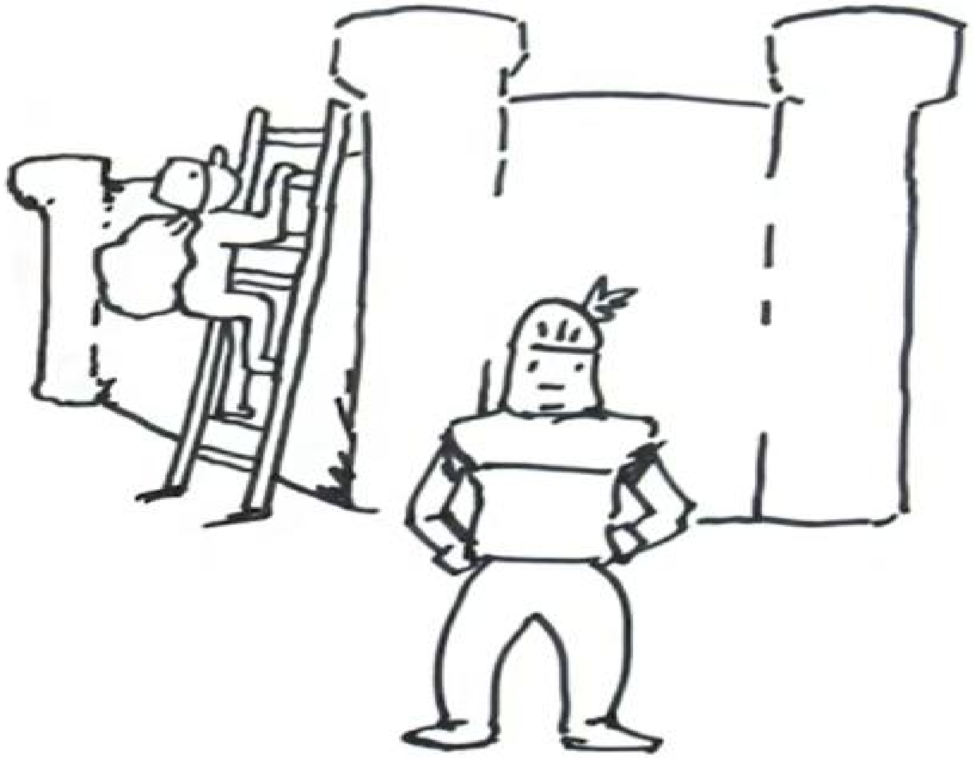
Lateral Movement



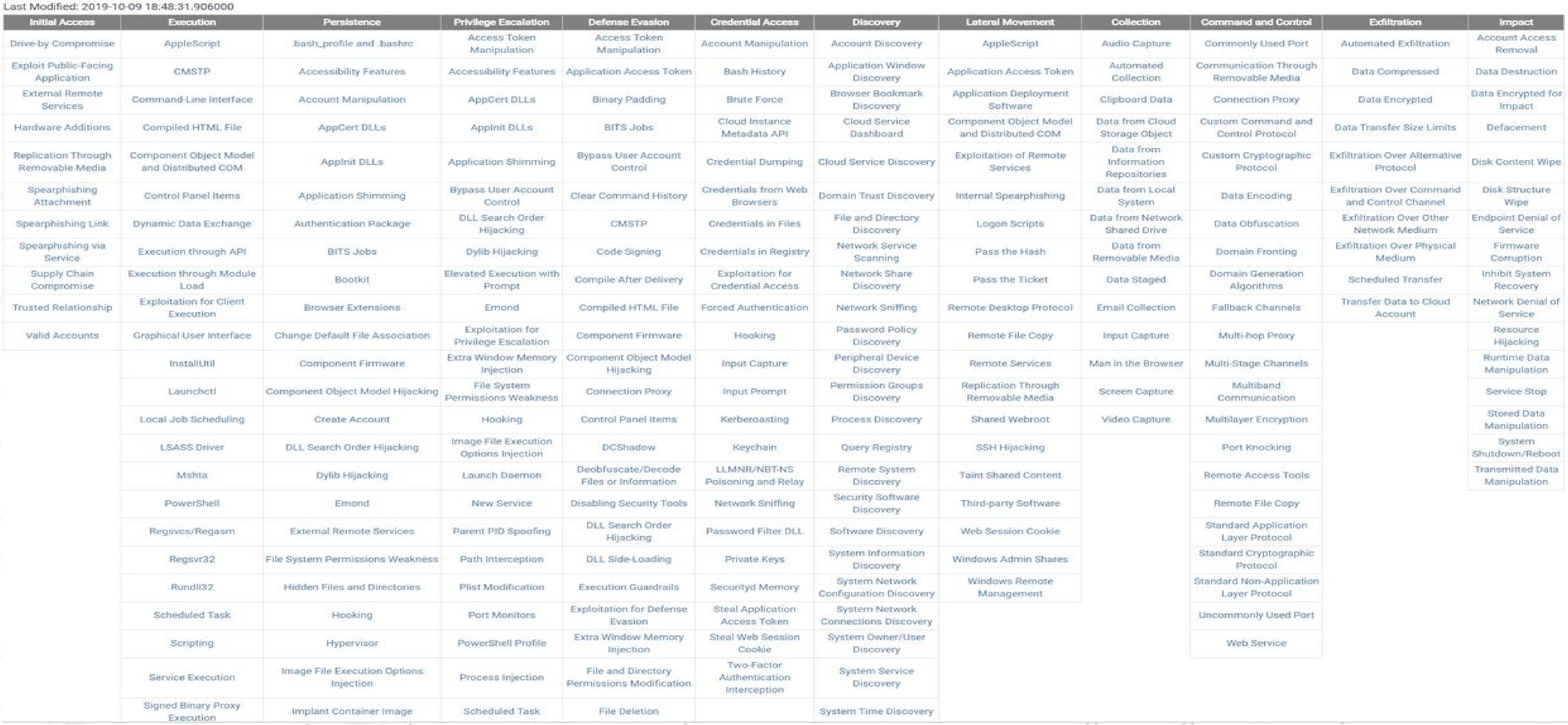
MITTRE - TTI



Exfiltration



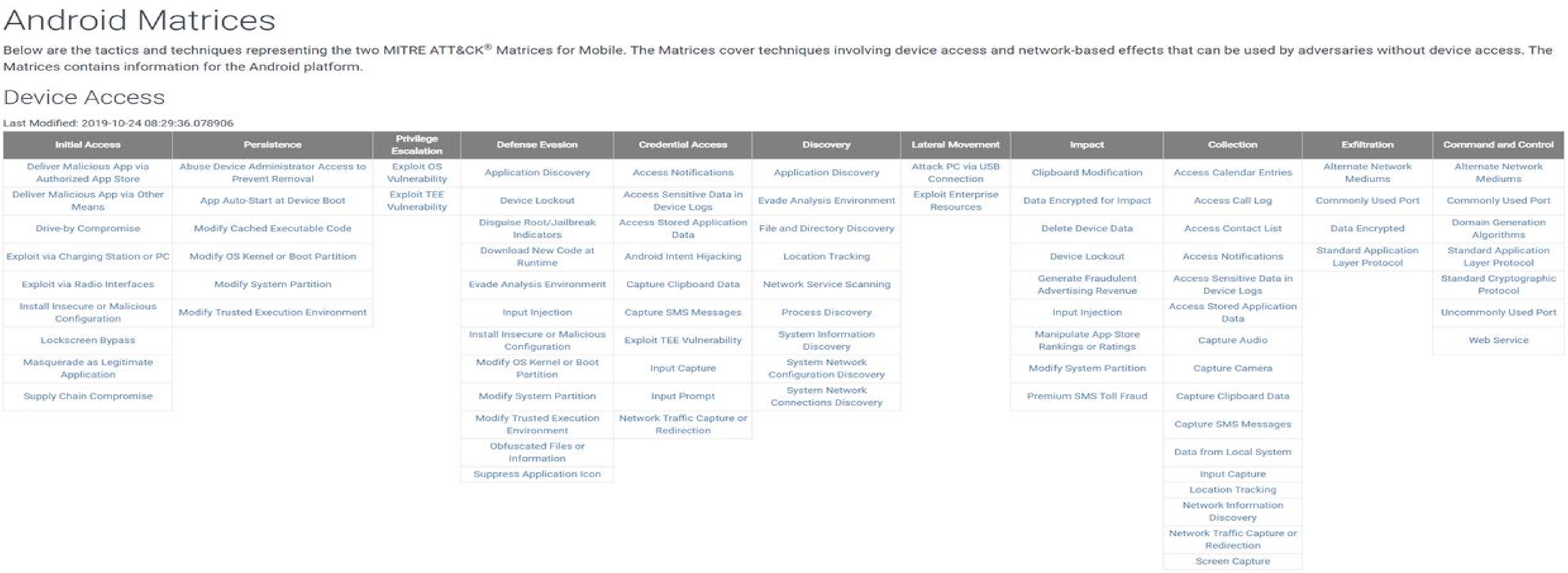
MITTRE - The Matrix



Last Modified: 2019-10-09 18:48:31.906000

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

Mobile / Android



Android Matrices

Below are the tactics and techniques representing the two MITRE ATT&CK® Matrices for Mobile. The Matrices cover techniques involving device access and network-based effects that can be used by adversaries without device access. The Matrices contains information for the Android platform.

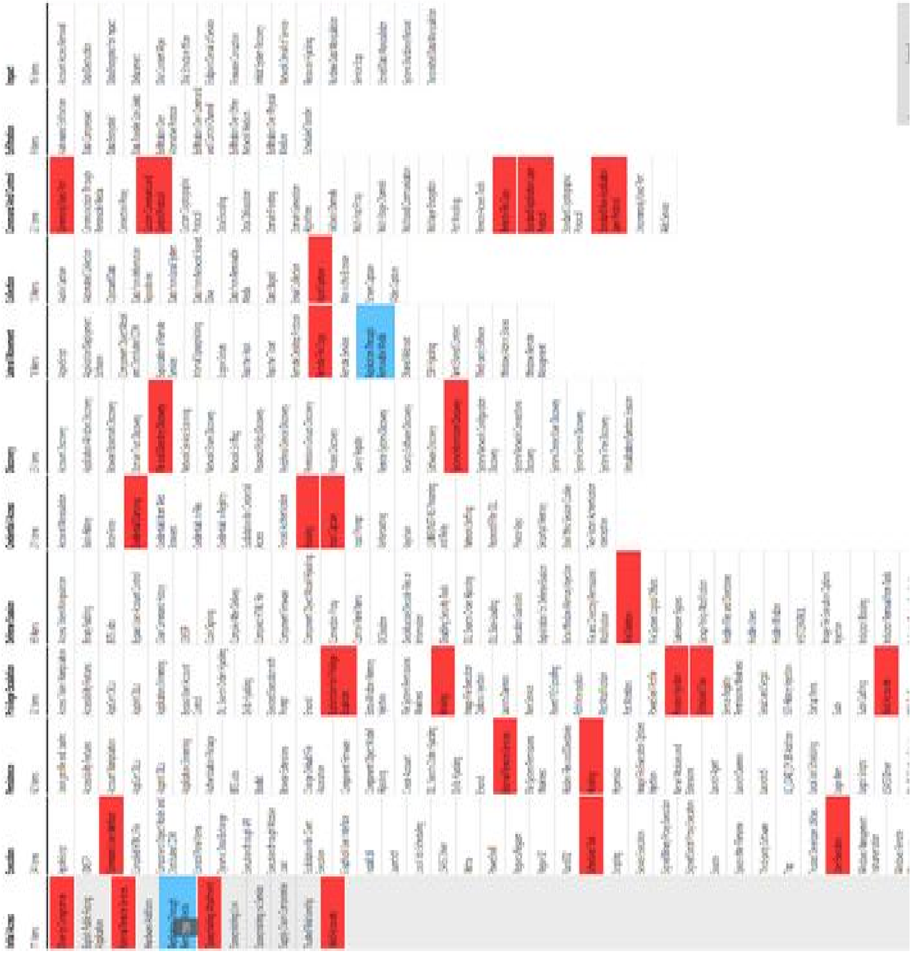
Device Access

Last Modified: 2019-10-24 08:29:36.078906

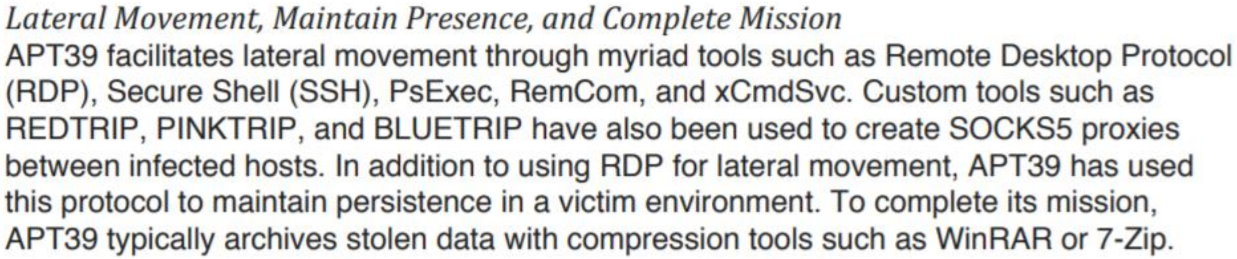
Initial Access	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Impact	Collection	Exfiltration	Command and Control
Deliver Malicious App via Authorized App Store	Abuse Device Administrator Access to Prevent Removal	Exploit OS Vulnerability	Application Discovery	Access Notifications	Application Discovery	Attack PC via USB Connection	Clipboard Modification	Access Calendar Entries	Alternate Network Mediums	Alternate Network Mediums
Deliver Malicious App via Other Means	App Auto-Start at Device Boot	Exploit TEE Vulnerability	Device Lockout	Access Sensitive Data in Device Logs	Evade Analysis Environment	Exploit Enterprise Resources	Data Encrypted for Impact	Access Call Log	Commonly Used Port	Commonly Used Port
Drive-by Compromise	Modify Cached Executable Code		Disguise Root/Jailbreak Indicators	Access Stored Application Data	File and Directory Discovery		Delete Device Data	Access Contact List	Data Encrypted	Domain Generation Algorithms
Exploit via Charging Station or PC	Modify OS Kernel or Boot Partition		Download New Code at Runtime	Android Intent Hijacking	Location Tracking		Device Lockout	Access Notifications	Standard Application Layer Protocol	Standard Application Layer Protocol
Exploit via Radio Interfaces	Modify System Partition		Evade Analysis Environment	Capture Clipboard Data	Network Service Scanning		Generate Fraudulent Advertising Revenue	Access Sensitive Data in Device Logs		Standard Cryptographic Protocol
Install Insecure or Malicious Configuration	Modify Trusted Execution Environment		Input Injection	Capture SMS Messages	Process Discovery		Input Injection	Access Stored Application Data		Uncommonly Used Port
Lockscreen Bypass			Install Insecure or Malicious Configuration	Exploit TEE Vulnerability	System Information Discovery		Manipulate App Store Rankings or Ratings	Capture Audio		Web Service
Masquerade as Legitimate Application			Modify OS Kernel or Boot Partition	Input Capture	System Network Configuration Discovery		Modify System Partition	Capture Camera		
Supply Chain Compromise			Modify System Partition	Input Prompt	System Network Connections Discovery		Premium SMS Toll Fraud	Capture Clipboard Data		
			Modify Trusted Execution Environment	Network Traffic Capture or Redirection				Capture SMS Messages		
			Obfuscated Files or Information					Data from Local System		
			Suppress Application Icon					Input Capture		
								Location Tracking		
								Network Information Discovery		
								Network Traffic Capture or Redirection		
								Screen Capture		

CATEGORÍAS DE LA MATRIZ

- ACCESO INICIAL
- EJECUCIÓN
- PERSISTENCIA
- ESCALADO DE PRIVILEGIOS
- EVASIÓN DE DEFENSAS
- ACCESO A CREDENCIALES
- IDENTIFICACIÓN
- MOVIMIENTO LATERAL
- RECOLECCIÓN
- CAMANDO Y CONTROL
- EXFILTRACIÓN
- IMPACTO

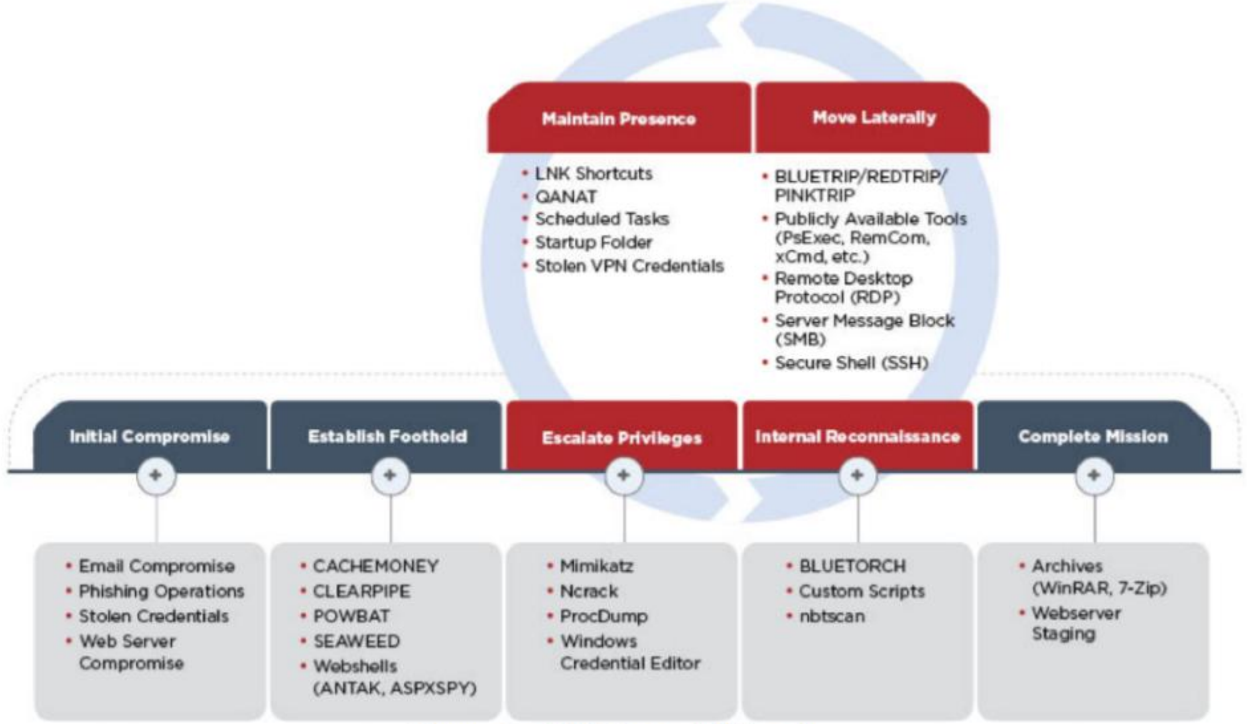


FireEye APT39 Report:



Lateral Movement, Maintain Presence, and Complete Mission

APT39 facilitates lateral movement through myriad tools such as Remote Desktop Protocol (RDP), Secure Shell (SSH), PsExec, RemCom, and xCmdSvc. Custom tools such as REDTRIP, PINKTRIP, and BLUETRIP have also been used to create SOCKS5 proxies between infected hosts. In addition to using RDP for lateral movement, APT39 has used this protocol to maintain persistence in a victim environment. To complete its mission, APT39 typically archives stolen data with compression tools such as WinRAR or 7-Zip.



Maintain Presence
- LNK Shortcuts
- QANAT
- Scheduled Tasks
- Startup Folder
- Stolen VPN Credentials

Move Laterally
- BLUETRIP/REDTRIP/PINKTRIP
- Publicly Available Tools (PsExec, RemCom, xCmd, etc.)
- Remote Desktop Protocol (RDP)
- Server Message Block (SMB)
- Secure Shell (SSH)

Initial Compromise
- Email Compromise
- Phishing Operations
- Stolen Credentials
- Web Server Compromise

Establish Foothold
- CACHEMONEY
- CLEARPIPE
- POWBAT
- SEAWEED
- Webshells (ANTAK, ASPXSPY)

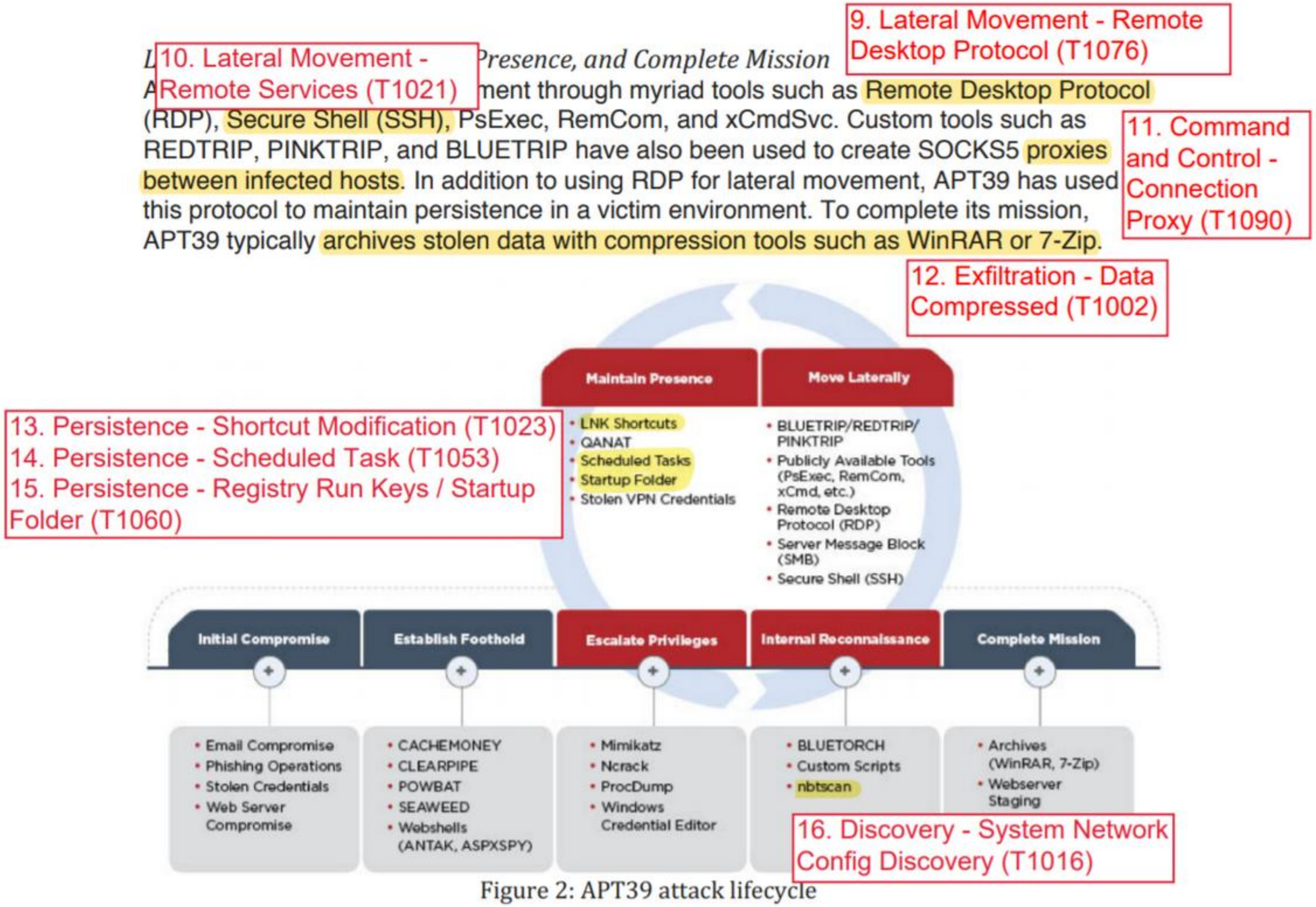
Escalate Privileges
- Mimikatz
- Ncrack
- ProcDump
- Windows Credential Editor

Internal Reconnaissance
- BLUETORCH
- Custom Scripts
- nbtscan

Complete Mission
- Archives (WinRAR, 7-Zip)
- Webserver Staging

Figure 2: APT39 attack lifecycle

FireEye APT39:



9. Lateral Movement - Remote Desktop Protocol (T1076)

L 10. Lateral Movement - Remote Services (T1021) *Presence, and Complete Mission*

A ment through myriad tools such as Remote Desktop Protocol (RDP), Secure Shell (SSH), PsExec, RemCom, and xCmdSvc. Custom tools such as REDTRIP, PINKTRIP, and BLUETRIP have also been used to create SOCKS5 proxies between infected hosts. In addition to using RDP for lateral movement, APT39 has used this protocol to maintain persistence in a victim environment. To complete its mission, APT39 typically archives stolen data with compression tools such as WinRAR or 7-Zip.

11. Command and Control - Connection Proxy (T1090)

12. Exfiltration - Data Compressed (T1002)

13. Persistence - Shortcut Modification (T1023)
14. Persistence - Scheduled Task (T1053)
15. Persistence - Registry Run Keys / Startup Folder (T1060)

Maintain Presence

- LNK Shortcuts
- QANAT
- Scheduled Tasks
- Startup Folder
- Stolen VPN Credentials

Move Laterally

- BLUETRIP/REDTRIP/PINKTRIP
- Publicly Available Tools (PsExec, RemCom, xCmd, etc.)
- Remote Desktop Protocol (RDP)
- Server Message Block (SMB)
- Secure Shell (SSH)

Initial Compromise

- Email Compromise
- Phishing Operations
- Stolen Credentials
- Web Server Compromise

Establish Foothold

- CACHEMONEY
- CLEARPIPE
- POWBAT
- SEAWEED
- Webshells (ANTAK, ASPXSPY)

Escalate Privileges

- Mimikatz
- Ncrack
- ProcDump
- Windows Credential Editor

Internal Reconnaissance

- BLUETORCH
- Custom Scripts
- nbtscan

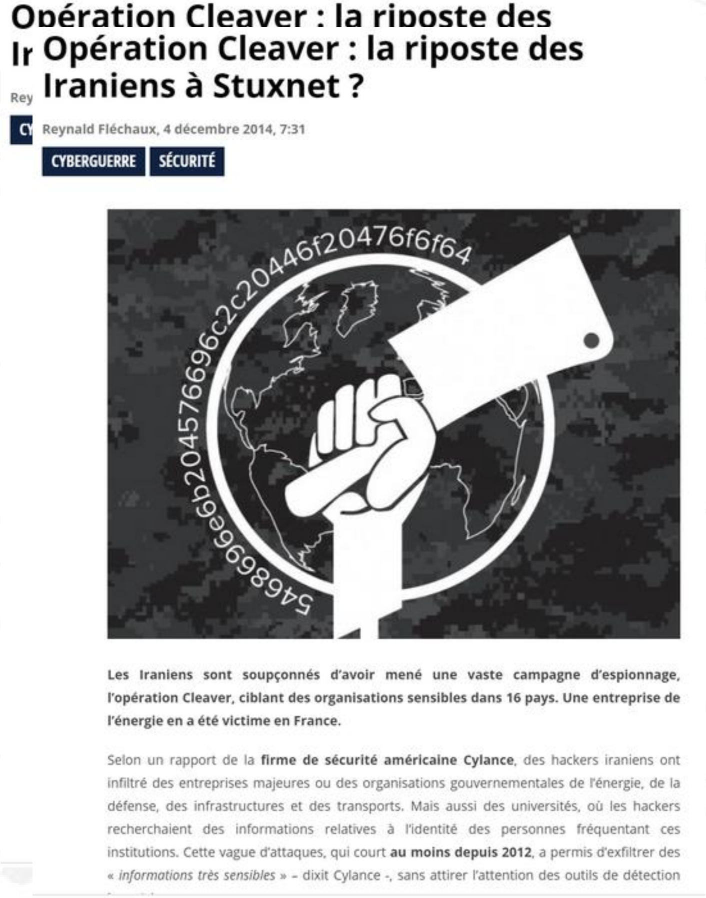
Complete Mission

- Archives (WinRAR, 7-Zip)
- Webserver Staging

16. Discovery - System Network Config Discovery (T1016)

Figure 2: APT39 attack lifecycle

Operation Cleaver



Opération Cleaver : la riposte des

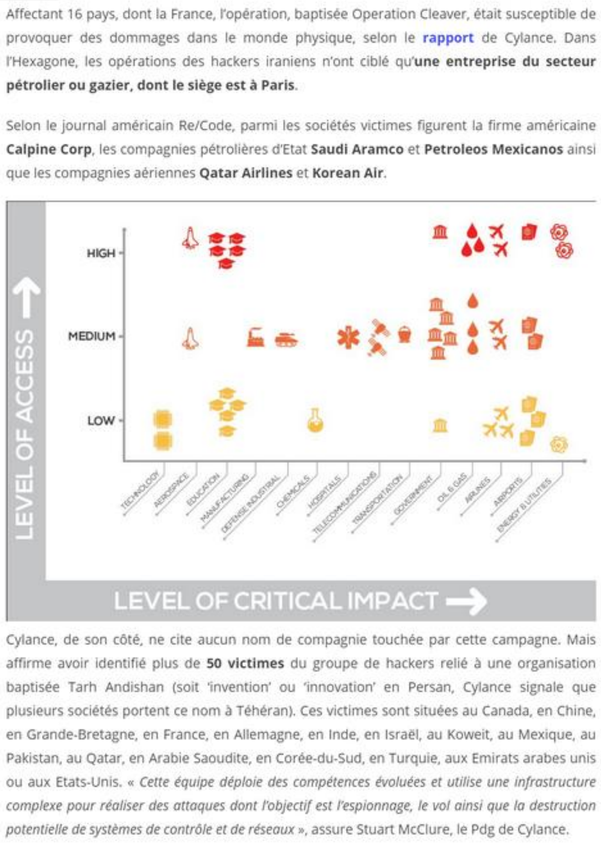
Opération Cleaver : la riposte des Iraniens à Stuxnet ?

Reynald Fléchaux, 4 décembre 2014, 7:31

CYBERGUERRE SÉCURITÉ

Les Iraniens sont soupçonnés d'avoir mené une vaste campagne d'espionnage, l'opération Cleaver, ciblant des organisations sensibles dans 16 pays. Une entreprise de l'énergie en a été victime en France.

Selon un rapport de la **firme de sécurité américaine Cylance**, des hackers iraniens ont infiltré des entreprises majeures ou des organisations gouvernementales de l'énergie, de la défense, des infrastructures et des transports. Mais aussi des universités, où les hackers recherchaient des informations relatives à l'identité des personnes fréquentant ces institutions. Cette vague d'attaques, qui court **au moins depuis 2012**, a permis d'exfiltrer des « *informations très sensibles* » – dixit Cylance -, sans attirer l'attention des outils de détection



Affectant 16 pays, dont la France, l'opération, baptisée Operation Cleaver, était susceptible de provoquer des dommages dans le monde physique, selon le **rapport** de Cylance. Dans l'Hexagone, les opérations des hackers iraniens n'ont ciblé qu'**une entreprise du secteur pétrolier ou gazier, dont le siège est à Paris**.

Selon le journal américain Re/Code, parmi les sociétés victimes figurent la firme américaine **Calpine Corp**, les compagnies pétrolières d'Etat **Saudi Aramco** et **Petroleos Mexicanos** ainsi que les compagnies aériennes **Qatar Airlines** et **Korean Air**.

Cylance, de son côté, ne cite aucun nom de compagnie touchée par cette campagne. Mais affirme avoir identifié plus de **50 victimes** du groupe de hackers relié à une organisation baptisée Tarh Andishan (soit 'invention' ou 'innovation' en Persan, Cylance signale que plusieurs sociétés portent ce nom à Téhéran). Ces victimes sont situées au Canada, en Chine, en Grande-Bretagne, en France, en Allemagne, en Inde, en Israël, au Koweit, au Mexique, au Pakistan, au Qatar, en Arabie Saoudite, en Corée-du-Sud, en Turquie, aux Emirats arabes unis ou aux Etats-Unis. « *Cette équipe déploie des compétences évoluées et utilise une infrastructure complexe pour réaliser des attaques dont l'objectif est l'espionnage, le vol ainsi que la destruction potentielle de systèmes de contrôle et de réseaux* », assure Stuart McClure, le Pdg de Cylance.

MITTRE - TTI

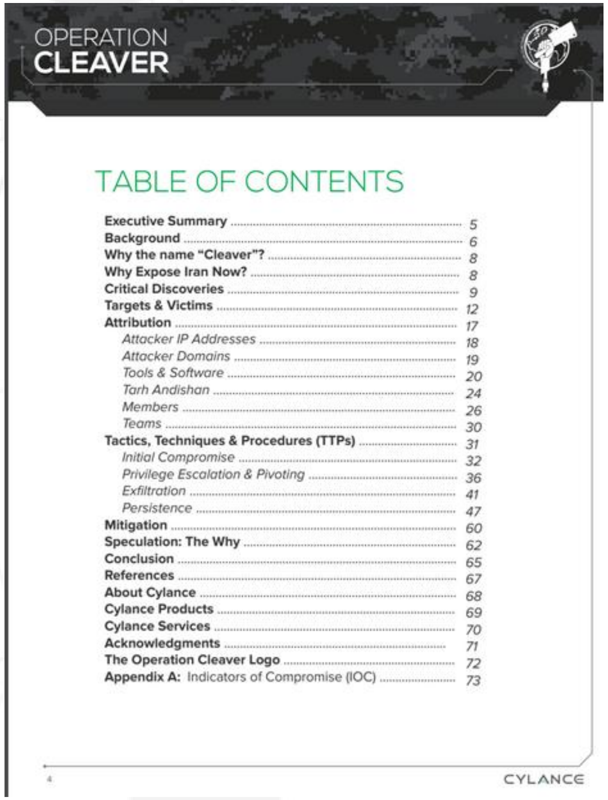
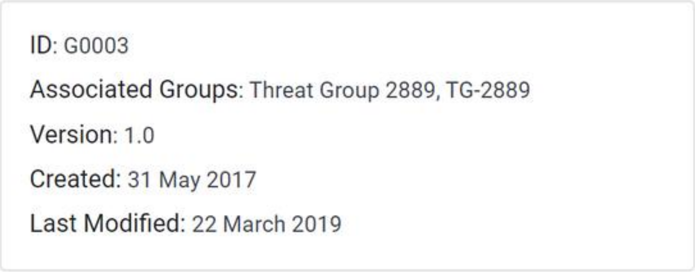

OPERATION
CLEAVER

TABLE OF CONTENTS

CYLANCE

Cleaver is a threat group that has been attributed to Iranian actors and is responsible for activity tracked as Operation Cleaver. [1] Strong circumstantial evidence suggests Cleaver is linked to Threat Group 2889 (TG-2889). [2]


ID: G0003

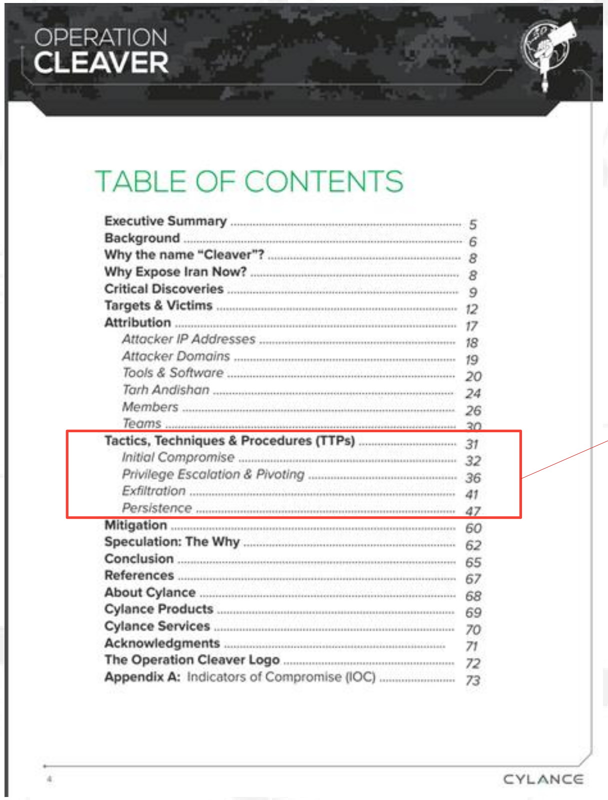
Associated Groups: Threat Group 2889, TG-2889

Version: 1.0

Created: 31 May 2017

Last Modified: 22 March 2019

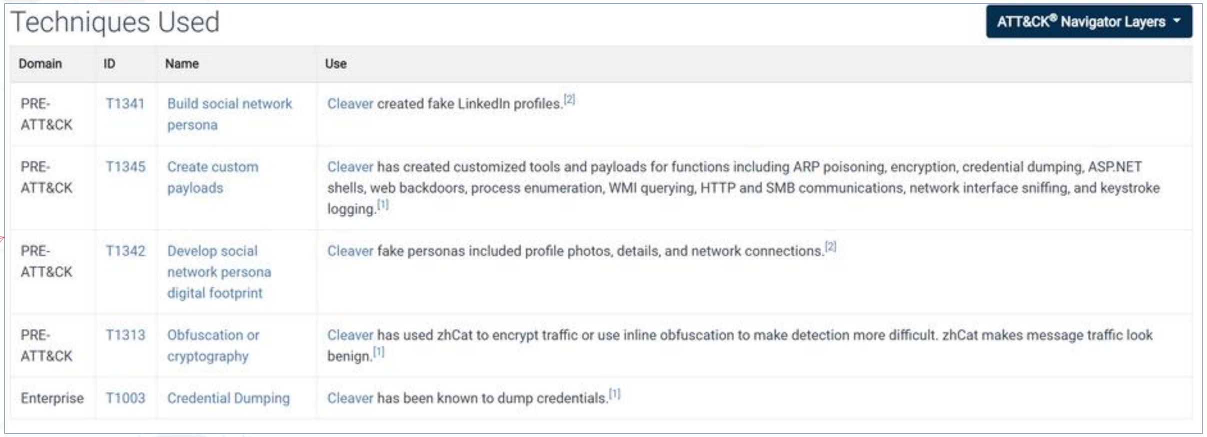
MITTRE - TTI



OPERATION
CLEAVER

TABLE OF CONTENTS

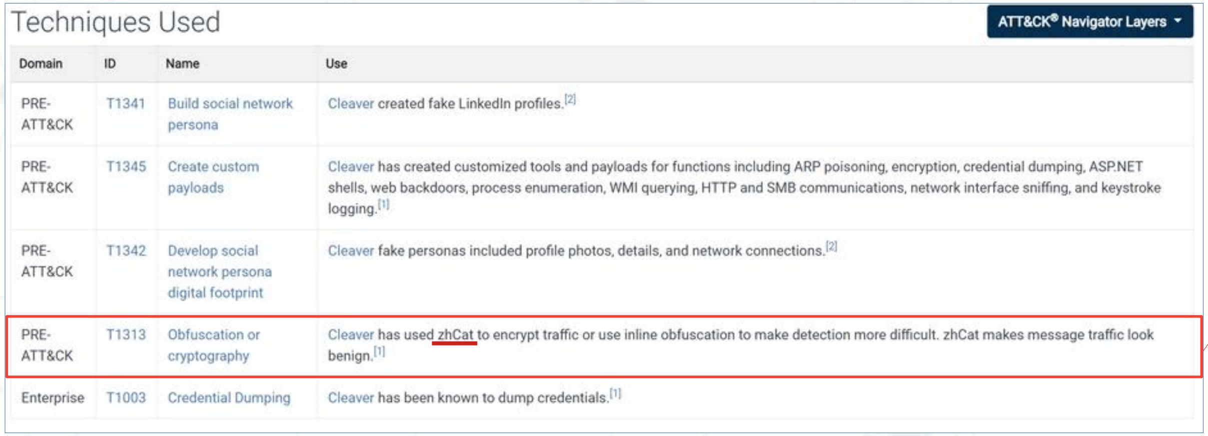
CYLANCE



Techniques Used

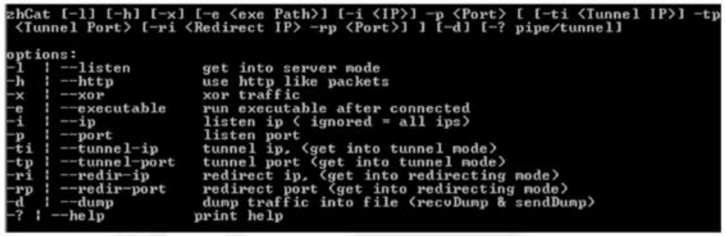
Domain	ID	Name	Use
PRE-ATT&CK	T1341	Build social network persona	Cleaver created fake LinkedIn profiles.[2]
PRE-ATT&CK	T1345	Create custom payloads	Cleaver has created customized tools and payloads for functions including ARP poisoning, encryption, credential dumping, ASP.NET shells, web backdoors, process enumeration, WMI querying, HTTP and SMB communications, network interface sniffing, and keystroke logging.[1]
PRE-ATT&CK	T1342	Develop social network persona digital footprint	Cleaver fake personas included profile photos, details, and network connections.[2]
PRE-ATT&CK	T1313	Obfuscation or cryptography	Cleaver has used zhCat to encrypt traffic or use inline obfuscation to make detection more difficult. zhCat makes message traffic look benign.[1]
Enterprise	T1003	Credential Dumping	Cleaver has been known to dump credentials.[1]

MITTRE - TTI



Techniques Used

Domain	ID	Name	Use
PRE-ATT&CK	T1341	Build social network persona	Cleaver created fake LinkedIn profiles.[2]
PRE-ATT&CK	T1345	Create custom payloads	Cleaver has created customized tools and payloads for functions including ARP poisoning, encryption, credential dumping, ASP.NET shells, web backdoors, process enumeration, WMI querying, HTTP and SMB communications, network interface sniffing, and keystroke logging.[1]
PRE-ATT&CK	T1342	Develop social network persona digital footprint	Cleaver fake personas included profile photos, details, and network connections.[2]
PRE-ATT&CK	T1313	Obfuscation or cryptography	Cleaver has used zhCat to encrypt traffic or use inline obfuscation to make detection more difficult. zhCat makes message traffic look benign.[1]
Enterprise	T1003	Credential Dumping	Cleaver has been known to dump credentials.[1]



```
zhCat [-l] [-h] [-x] [-e <exe Path>] [-i <IP>] -p <Port> [ [-ti <Tunnel IP>] -tp
 <Tunnel Port> [-ri <Redirect IP> -rp <Port>] ] [-d] [-? pipe/tunnel]

options:
-l  | --listen         get into server mode
-h  | --http           use http like packets
-x  | --xor            xor traffic
-e  | --executable     run executable after connected
-i  | --ip             listen ip ( ignored = all ips)
-p  | --port           listen port
-ti | --tunnel-ip      tunnel ip, (get into tunnel mode)
-tp | --tunnel-port    tunnel port (get into tunnel mode)
-ri | --redir-ip       redirect ip, (get into redirecting mode)
-rp | --redir-port     redirect port (get into redirecting mode)
-d  | --dump           dump traffic into file (recvDump & sendDump)
-? | --help           print help
```

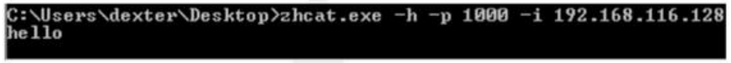
Multiple obfuscation/encryption methods are available. The `-h` argument enables HTTP mode. This makes the traffic between zhCat instances look like benign HTTP traffic. For instance, if the attackers set up a zhCat instance listening on port 1000 on `192.168.116.128` in HTTP mode, the client instance of zhCat would use the following command:

```
zhcat.exe -h -p 1000 -i 192.168.116.128
```

The server instance would use the following command:

```
zhcat.exe -l -h -p 1000
```

When we run both of these, we can send information just by typing it into the terminal of the running application. Information can be supplied by standard input.



```
C:\Users\dexter\Desktop>zhcat.exe -h -p 1000 -i 192.168.116.128
hello
```

MITTRE – Creación de TTI

```
ipconfig /all
sc.exe \\ln334656-pc create
.\recycler.exe a -hpfGzq5yKw C:\$Recycle.Bin\old
C:\$Recycle.Bin\Shockwave_network.vsdx
```

Commands captured by Sysmon being run interactively via cmd.exe

```
10.2.13.44:32123 -> 128.29.32.4:443
128.29.32.4:443 -> 10.2.13.44:32123
```

Flows from malware in a sandbox

```
HKLM\Software\Microsoft\Windows\CurrentVersion\Run
HKLM\Software\Microsoft\Netsh
```

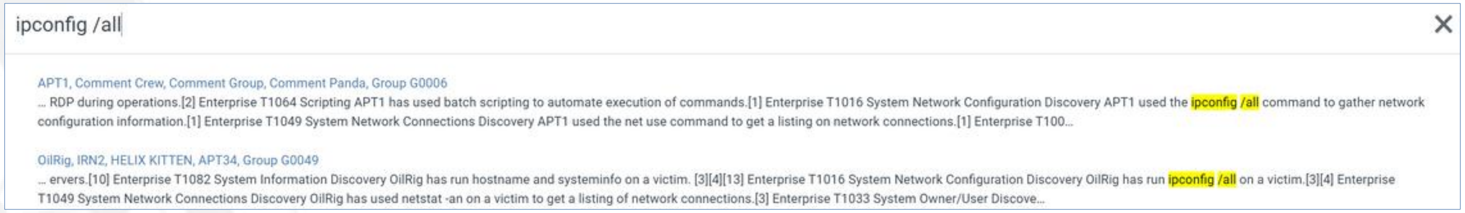
MITTRE - TTI

ipconfig /all

sc.exe \\ln334656-pc create

.\recycler.exe a -hpfGzq5yKw C:\$Recycle.Bin\old C:\$Recycle.Bin\Shockwave_network.vsdx

Commands captured by Sysmon being run interactively via cmd.exe



ipconfig /all

APT1, Comment Crew, Comment Group, Comment Panda, Group G0006

… RDP during operations.[2] Enterprise T1064 Scripting APT1 has used batch scripting to automate execution of commands.[1] Enterprise T1016 System Network Configuration Discovery APT1 used the ipconfig /all command to gather network configuration information.[1] Enterprise T1049 System Network Connections Discovery APT1 used the net use command to get a listing on network connections.[1] Enterprise T100…

OilRig, IRN2, HELIX KITTEN, APT34, Group G0049

… ervers.[10] Enterprise T1082 System Information Discovery OilRig has run hostname and systeminfo on a victim. [3][4][13] Enterprise T1016 System Network Configuration Discovery OilRig has run ipconfig /all on a victim.[3][4] Enterprise T1049 System Network Connections Discovery OilRig has used netstat -an on a victim to get a listing of network connections.[3] Enterprise T1033 System Owner/User Discove…

10.2.13.44:32123 -> 128.29.32.4:443

128.29.32.4:443 -> 10.2.13.44:32123

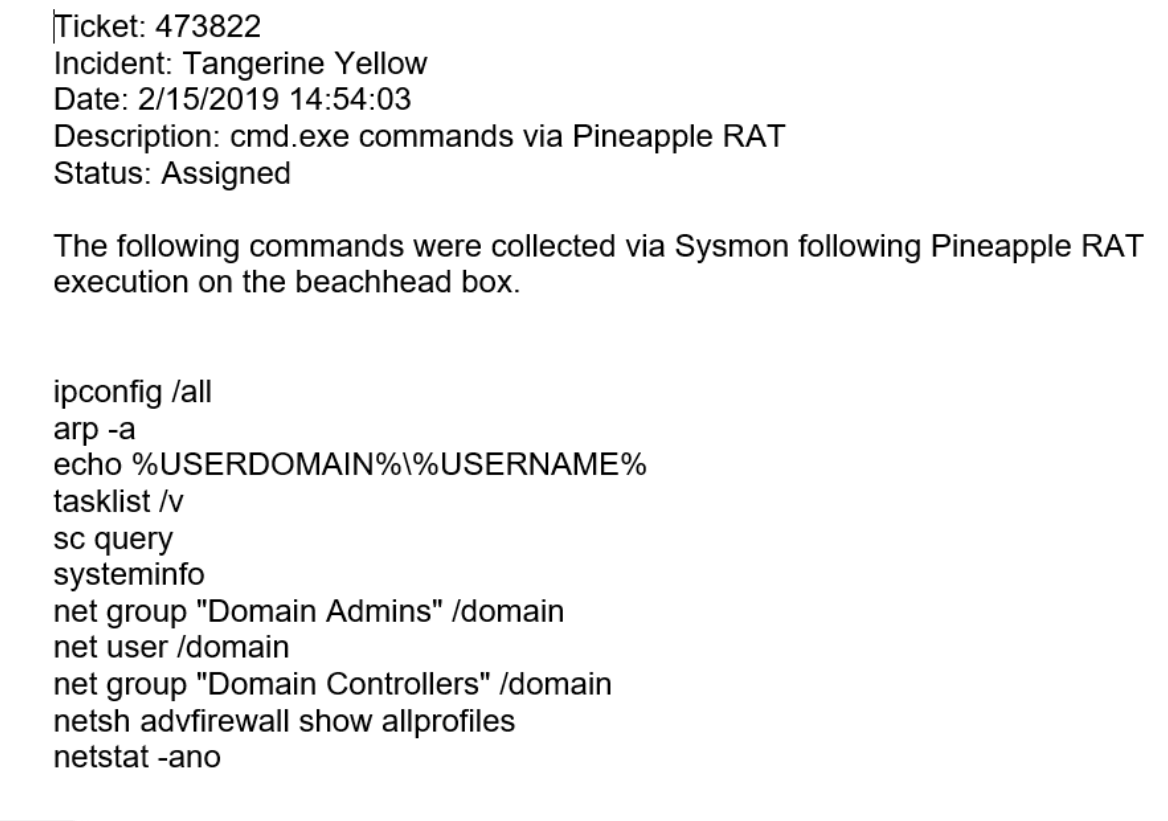
Flows from malware in a sandbox

HKLM\Software\Microsoft\Windows\CurrentVersion\Run

HKLM\Software\Microsoft\Netsh

https://attack.mitre.org/techniques/T1016/

MITTRE – de raw hacia TTI

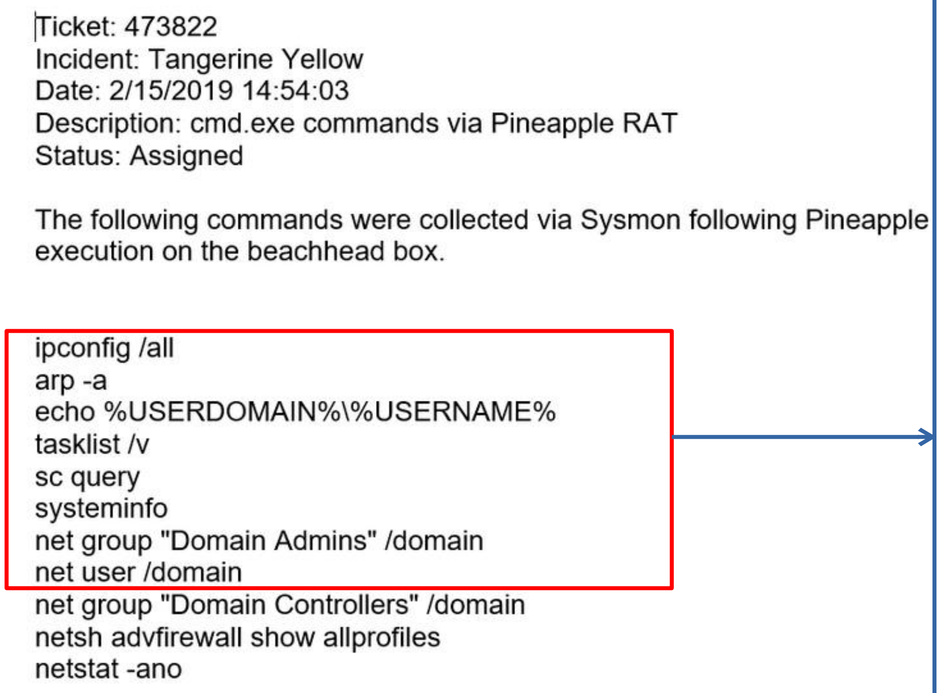


Ticket: 473822
Incident: Tangerine Yellow
Date: 2/15/2019 14:54:03
Description: cmd.exe commands via Pineapple RAT
Status: Assigned

The following commands were collected via Sysmon following Pineapple RAT execution on the beachhead box.

```
ipconfig /all
arp -a
echo %USERDOMAIN%\%USERNAME%
tasklist /v
sc query
systeminfo
net group "Domain Admins" /domain
net user /domain
net group "Domain Controllers" /domain
netsh advfirewall show allprofiles
netstat -ano
```

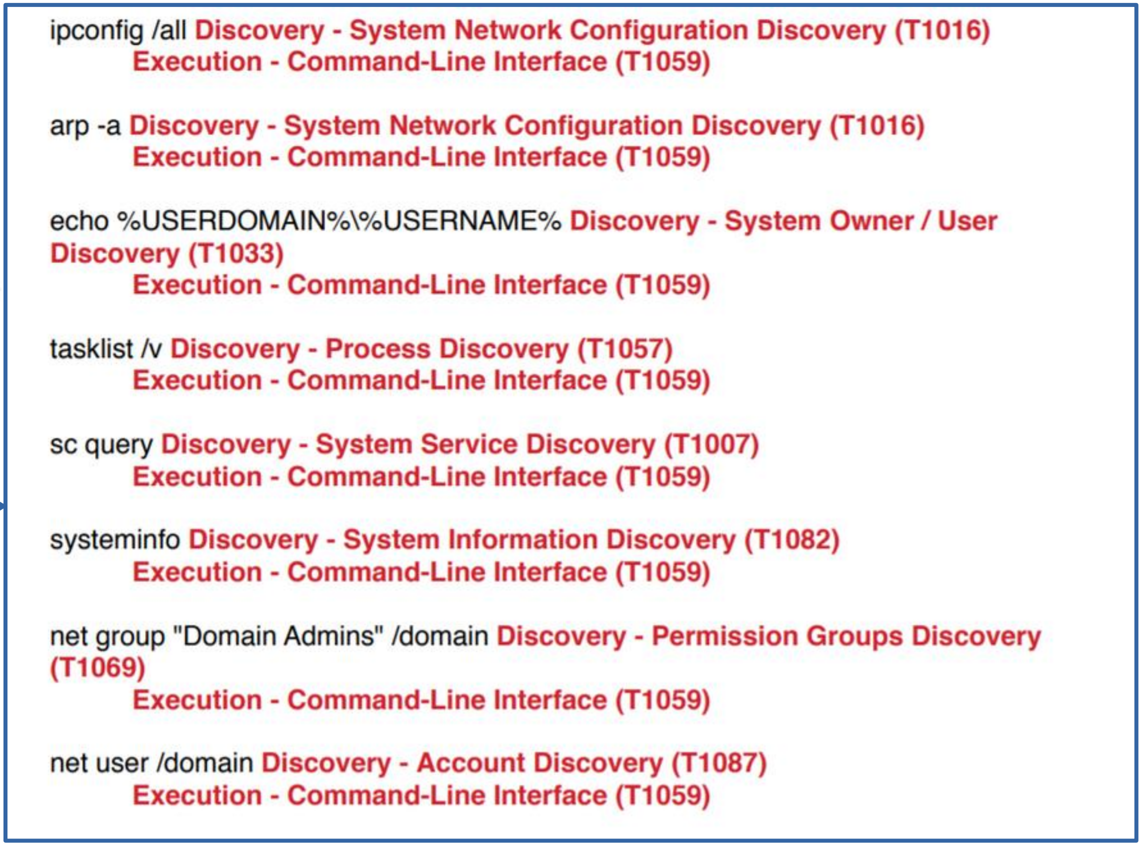
MITTRE – de Raw hacia TTI



Ticket: 473822
Incident: Tangerine Yellow
Date: 2/15/2019 14:54:03
Description: cmd.exe commands via Pineapple RAT
Status: Assigned

The following commands were collected via Sysmon following Pineapple execution on the beachhead box.

```
ipconfig /all
arp -a
echo %USERDOMAIN%\%USERNAME%
tasklist /v
sc query
systeminfo
net group "Domain Admins" /domain
net user /domain
net group "Domain Controllers" /domain
netsh advfirewall show allprofiles
netstat -ano
```



ipconfig /all **Discovery - System Network Configuration Discovery (T1016)**
Execution - Command-Line Interface (T1059)

arp -a **Discovery - System Network Configuration Discovery (T1016)**
Execution - Command-Line Interface (T1059)

echo %USERDOMAIN%\%USERNAME% **Discovery - System Owner / User Discovery (T1033)**
Execution - Command-Line Interface (T1059)

tasklist /v **Discovery - Process Discovery (T1057)**
Execution - Command-Line Interface (T1059)

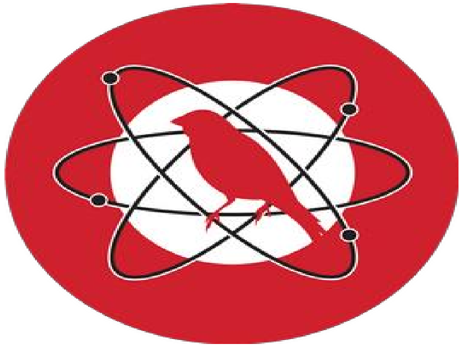
sc query **Discovery - System Service Discovery (T1007)**
Execution - Command-Line Interface (T1059)

systeminfo **Discovery - System Information Discovery (T1082)**
Execution - Command-Line Interface (T1059)

net group "Domain Admins" /domain **Discovery - Permission Groups Discovery (T1069)**
Execution - Command-Line Interface (T1059)

net user /domain **Discovery - Account Discovery (T1087)**
Execution - Command-Line Interface (T1059)

Casos de éxito



Atomic Red Team

Notas Finales

- No es sólo una herramienta de threat hunting
- Los CSIRTS deberían hacer uso o adaptarse a MITTRE ATT&CK
- Ayuda a crear un mapa del sistema de defensa de la empresa.
- Planificar los mecanismos de seguridad, teniendo en cuenta los posibles escenarios
- Puede ser usado en el sector privado, público, o implementarse en nuevas soluciones de seguridad
- Entrenamiento

Referencias

[1] Blake E., MITRE ATT&CK: Design and Philosophy, https://attack.mitre.org/docs/ATTACK_Design_and_Philosophy_March_2020.pdf

[2] https://attack.mitre.org/

[3] Mittre ATT&CK – Usage, https://github.com/mitre/cti/blob/master/USAGE.md

[4] Operation Cleaverhttps://www.cylance.com/content/dam/cylance/pages/operation-cleaver/Cylance_Operation_Cleaver_Report.pdf

Contactos

https://is3g.github.io/
https://www.linkedin.com/in/luisbetosolis/

Gracias