Tower Federal Credit Union MITRE

ATT&CK Framework Analysis

Uche Obiora

2024 Summer Intern / uche.obiora@towerfcu.org

7/15/2024

Goal of Research

1) Identify APT groups that may pose risk to Tower Federal Credit Union

2) Focus on APT groups that fall under financial and government industry

3) Research the TTPs used by APT groups

4) Conduct analysis of Tower's capabilities to defend against APT group TTPs

Financial APT Group Analysis

Researching Financial APT Groups

We started our research off of the APT group database found on the MITRE ATT&CK navigator. From here, we started to filter the APT groups based on if they pose risk to the Financial sector. In order to be more efficient in the filtering process, we decided to only worry about APT groups that attacked/attacks the USA.

After this initial research/filter phase, we had 41 APT Groups that had a history of targeting the Financial sector.

With this narrowed down list of APT groups, we went through each one and researched things such as:

1) What type of attacks have they done in the past?
2) What specific type of financial institution did the APT group attack?
3) How sophisticated and capable are these APT groups?

Based on these questions, we assigned a "Danger Score" ranging from 1(No Risk) to 5(High Risk) to each of the APT groups. If an APT group specifically attacked banks or credit unions, they were granted a 5. We selected the top 7 APT groups that had the highest scores and posed the most risk to Tower based on their past attacks and sophistication.

The groups were**:**

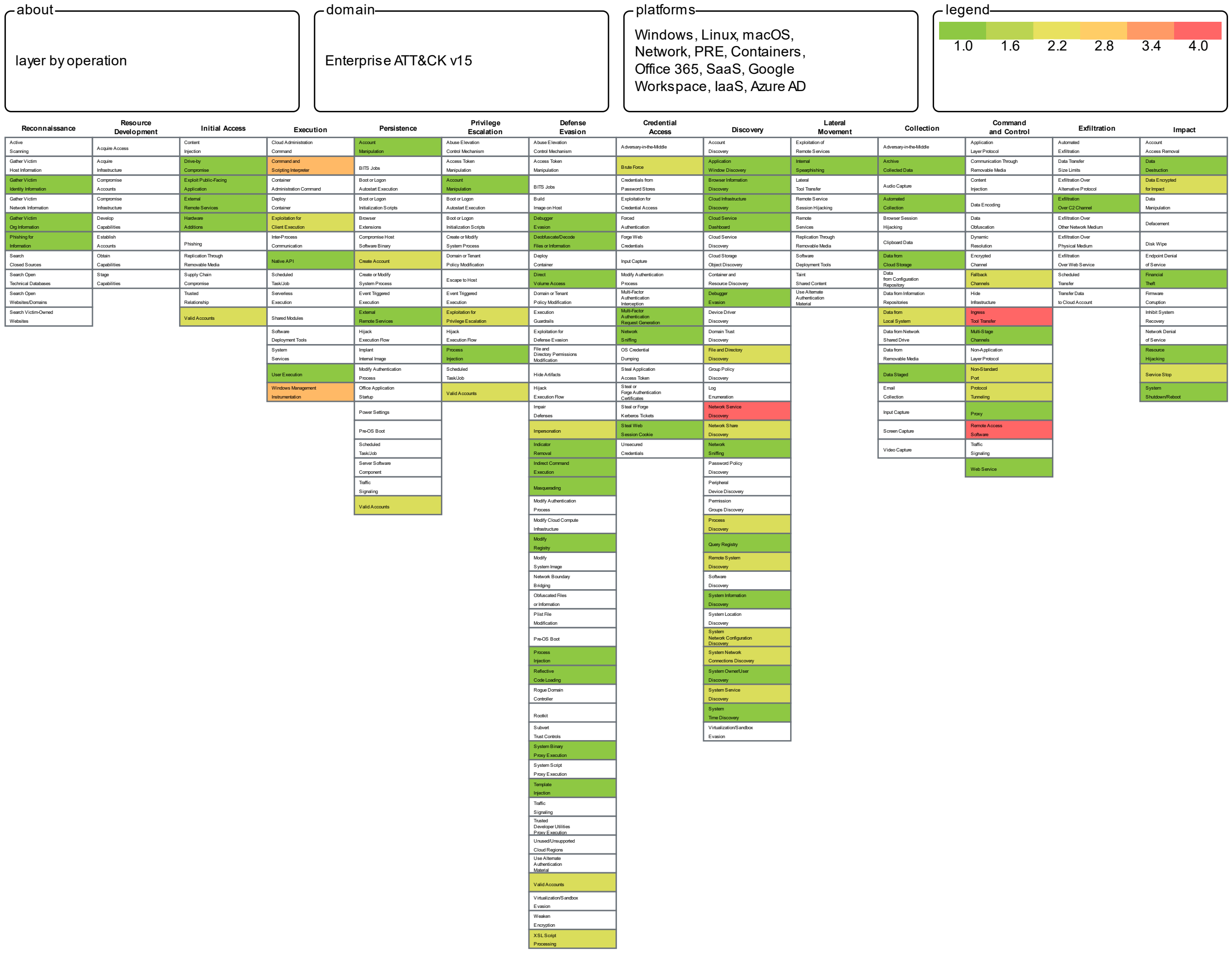
Scattered Spider, APT1, Indrik Spider, Carbanak, Cobalt Group, Dark Vishnya, Lazarus Group

Utilizing MITRE ATT&CK Navigator

Financial_APT_Groups.pdf Financial_APT_Groups_Expanded.pdf

After we had our 8 groups, we put those APT groups into the MITRE ATT&CK Navigator which shows a dashboard of all the TTPs that these APT groups use.

TTPs that are in a shade of red came up more than the TTPs that are in a shade of green. Therefore, red TTPs are those that should be of more concern.



about: layer by operation

domain: Enterprise ATT&CK v15

platforms: Windows, Linux, macOS, Network, PRE, Containers, Office 365, SaaS, Google Workspace, IaaS, Azure AD

legend: 🟩 1.0 🟩 1.6 🟨 2.2 🟧 2.8 🟧 3.4 🟥 4.0

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Active Scanning	Acquire Access	Content Injection	Cloud Administration Command	🟩 Account Manipulation	Abuse Elevation Control Mechanism	Abuse Elevation Control Mechanism	Adversary-in-the-Middle	Account Discovery	Exploitation of Remote Services	Adversary-in-the-Middle	Application Layer Protocol	Automated Exfiltration	Account Access Removal
Gather Victim Host Information	Acquire Infrastructure	🟩 Drive-by Compromise	🟧 Command and Scripting Interpreter	BITS Jobs	Access Token Manipulation	Access Token Manipulation	🟨 Brute Force	🟩 Application Window Discovery	🟩 Internal Spearphishing	🟩 Archive Collected Data	Communication Through Removable Media	Data Transfer Size Limits	🟩 Data Destruction
🟩 Gather Victim Identity Information	Compromise Accounts	🟩 Exploit Public-Facing Application	Container Administration Command	Boot or Logon Autostart Execution	🟩 Account Manipulation	BITS Jobs	Credentials from Password Stores	🟩 Browser Information Discovery	Lateral Tool Transfer	Audio Capture	Content Injection	Exfiltration Over Alternative Protocol	🟨 Data Encrypted for Impact
Gather Victim Network Information	Compromise Infrastructure	🟩 External Remote Services	Deploy Container	Boot or Logon Initialization Scripts	Boot or Logon Autostart Execution	Build Image on Host	Exploitation for Credential Access	🟩 Cloud Infrastructure Discovery	Remote Service Session Hijacking	🟩 Automated Collection	Data Encoding	🟩 Exfiltration Over C2 Channel	Data Manipulation
🟩 Gather Victim Org Information	Develop Capabilities	🟩 Hardware Additions	🟨 Exploitation for Client Execution	Browser Extensions	Boot or Logon Initialization Scripts	🟩 Debugger Evasion	Forced Authentication	🟩 Cloud Service Dashboard	Remote Services	Browser Session Hijacking	Data Obfuscation	Exfiltration Over Other Network Medium	Defacement
🟩 Phishing for Information	Establish Accounts	Phishing	Inter-Process Communication	Compromise Host Software Binary	Create or Modify System Process	🟩 Deobfuscate/Decode Files or Information	Forge Web Credentials	Cloud Service Discovery	Replication Through Removable Media	Clipboard Data	Dynamic Resolution	Exfiltration Over Physical Medium	Disk Wipe
Search Closed Sources	Obtain Capabilities	Replication Through Removable Media	🟩 Native API	🟨 Create Account	Domain or Tenant Policy Modification	Deploy Container	Input Capture	Cloud Storage Object Discovery	Software Deployment Tools	🟩 Data from Cloud Storage	Encrypted Channel	Exfiltration Over Web Service	Endpoint Denial of Service
Search Open Technical Databases	Stage Capabilities	Supply Chain Compromise	Scheduled Task/Job	Create or Modify System Process	Escape to Host	🟩 Direct Volume Access	Modify Authentication Process	Container and Resource Discovery	Taint Shared Content	Data from Configuration Repository	🟨 Fallback Channels	Scheduled Transfer	🟩 Financial Theft
Search Open Websites/Domains		Trusted Relationship	Serverless Execution	Event Triggered Execution	Event Triggered Execution	Domain or Tenant Policy Modification	Multi-Factor Authentication Interception	🟩 Debugger Evasion	Use Alternate Authentication Material	Data from Information Repositories	Hide Infrastructure	Transfer Data to Cloud Account	Firmware Corruption
Search Victim-Owned Websites		🟨 Valid Accounts	Shared Modules	🟩 External Remote Services	🟨 Exploitation for Privilege Escalation	Execution Guardrails	🟩 Multi-Factor Authentication Request Generation	Device Driver Discovery		🟨 Data from Local System	🟥 Ingress Tool Transfer		Inhibit System Recovery
			Software Deployment Tools	Hijack Execution Flow	Hijack Execution Flow	Exploitation for Defense Evasion	🟩 Network Sniffing	Domain Trust Discovery		Data from Network Shared Drive	🟩 Multi-Stage Channels		Network Denial of Service
			System Services	Implant Internal Image	🟩 Process Injection	File and Directory Permissions Modification	OS Credential Dumping	🟨 File and Directory Discovery		Data from Removable Media	Non-Application Layer Protocol		🟩 Resource Hijacking
			🟩 User Execution	Modify Authentication Process	Scheduled Task/Job	Hide Artifacts	Steal Application Access Token	Group Policy Discovery		🟩 Data Staged	🟨 Non-Standard Port		🟨 Service Stop
			🟧 Windows Management Instrumentation	Office Application Startup	🟨 Valid Accounts	Hijack Execution Flow	Steal or Forge Authentication Certificates	Log Enumeration		Email Collection	🟨 Protocol Tunneling		🟩 System Shutdown/Reboot
				Power Settings		Impair Defenses	Steal or Forge Kerberos Tickets	🟥 Network Service Discovery		Input Capture	🟩 Proxy		
				Pre-OS Boot		🟨 Impersonation	🟩 Steal Web Session Cookie	🟨 Network Share Discovery		Screen Capture	🟥 Remote Access Software		
				Scheduled Task/Job		🟩 Indicator Removal	Unsecured Credentials	🟩 Network Sniffing		Video Capture	Traffic Signaling		
				Server Software Component		🟩 Indirect Command Execution		Password Policy Discovery			🟩 Web Service		
				Traffic Signaling		🟩 Masquerading		Peripheral Device Discovery					
				🟨 Valid Accounts		Modify Authentication Process		Permission Groups Discovery					
						Modify Cloud Compute Infrastructure		🟨 Process Discovery					
						🟩 Modify Registry		🟩 Query Registry					
						Modify System Image		🟨 Remote System Discovery					
						Network Boundary Bridging		Software Discovery					
						Obfuscated Files or Information		🟩 System Information Discovery					
						Plist File Modification		System Location Discovery					
						Pre-OS Boot		🟨 System Network Configuration Discovery					
						🟩 Process Injection		🟨 System Network Connections Discovery					
						🟩 Reflective Code Loading		🟩 System Owner/User Discovery					
						Rogue Domain Controller		🟨 System Service Discovery					
						Rootkit		🟩 System Time Discovery					
						Subvert Trust Controls		Virtualization/Sandbox Evasion					
						🟩 System Binary Proxy Execution							
						System Script Proxy Execution							
						🟩 Template Injection							
						Traffic Signaling							
						Trusted Developer Utilities Proxy Execution							
						Unused/Unsupported Cloud Regions							
						Use Alternate Authentication Material							
						🟨 Valid Accounts							
						Virtualization/Sandbox Evasion							
						Weaken Encryption							
						🟨 XSL Script Processing							

Financial Critical TTPs

Resource Development / Obtain Capabilities / Tool

Execution / Command and Scripting Interpreter / PowerShell

Execution / Command and Scripting Interpreter / Windows Command Shell

Persistence / Create or Modify System Process / Windows Service

Privilege Escalation / Create or Modify System Process / Windows Service

Defense Evasion / Masquerading / Match legitimate name or location

Discovery / Network Service Discovery

Command and Control / Ingress Tool Transfer

Command and Control / Remote Access Software

Resource Development / Obtain Capabilities / Tool

APT Groups

Lazarus, Dark Vishnya, Cobalt Group, Carbanak, APT1, Scattered Spider

MITRE Description

Adversaries may buy, steal, or download software tools that can be used during targeting. Tools can be open or closed source, free or commercial. A tool can be used for malicious purposes by an adversary, but (unlike malware) were not intended to be used for those purposes

Dangers

Utilizing tools in order to carry out malicious attacks. Attackers who are not that sophisticated could cause damage due to these available tools

Tower's Capabilities Against TTP

Hard to mitigate the availability of tools as Tower has no control over that. Tower employs a layered defense system in order to defend against any tool or malicious attack.

Execution / Command and Scripting Interpreter / PowerShell

APT Groups

Lazarus, Indrik Spider, Cobalt Group, Dark Vishnya

MITRE Description

Adversaries may abuse PowerShell commands and scripts for execution. PowerShell is a powerful interactive command-line interface and scripting environment included in the Windows operating system.[1] Adversaries can use PowerShell to perform a number of actions, including discovery of information and execution of code.

Dangers

Utilizing PowerShell to execute harmful scripts/commands for data exfiltration, lateral movement, ransomware deployment, disabling security controls

Tower's Capabilities against TTP

- **Application whitelisting**: Allow only approved scripts and executables to run
- **Network Segmentation**: Isolate critical systems
- **Log scripts**: Constantly monitor for any suspicious activity
- **Least Privilege**: Assign minimal permissions to user accounts, avoid running PowerShell unless necessary

Execution / Command and Scripting Interpreter / Windows Command Shell

APT Groups

Lazarus, Cobalt Group, Indrik Spider, APT1

MITRE Definition

Adversaries may abuse the Windows command shell for execution. The Windows command shell (cmd) is the primary command prompt on Windows systems. The Windows command prompt can be used to control almost any aspect of a system, with various permission levels required for different subsets of commands.

Dangers

Utilizing Windows Command Shell to execute malicious code for lateral movement, data exfiltration, disabling security controls, ransomware deployment

Tower's Capabilities against TTP

- **Application Whitelisting:** Allow only approved scripts and executables to run
- **Network Segmentation**: Isolate critical systems
- **Log scripts**: Constantly monitor logs for any suspicious activity
- **Least Privilege**: Assign minimal permissions to user accounts, disable unused Windows CS features

Persistence / Create or Modify System Process / Windows Service

APT Groups

Lazarus, Dark Vishnya, Cobalt Group, Carbanak

MITRE Definition

Adversaries may create or modify Windows services to repeatedly execute malicious payloads as part of persistence. When Windows boots up, it starts programs or applications called services that perform background system functions.[1] Windows service configuration information, including the file path to the service's executable or recovery programs/commands, is stored in the Windows Registry.

Dangers

Create/modify Windows services to run in the background, masquerading as legitimate services

Tower's Capabilities against TTP

- **Application whitelisting:** Only allow approved services to run
- **Security Hardening:** Review and audit existing services
- **Patching:** Keep operating system and services up to date as vulnerabilities can lead to exploitation

Defense Evasion / Masquerading / Match legitimate name or location

APT Groups

Lazarus, Carbanak, Indrik Spider, APT1,

MITRE Definition

Adversaries may match or approximate the name or location of legitimate files or resources when naming/placing them. This is done for the sake of evading defenses and observation. This may be done by placing an executable in a commonly trusted directory (ex: under System32) or giving it the name of a legitimate, trusted program (ex: svchost.exe). In containerized environments, this may also be done by creating a resource in a namespace that matches the naming convention of a container pod or cluster. Alternatively, a file or container image name given may be a close approximation to legitimate programs/images or something innocuous.

Dangers

Evade defenses and detection by matching name/location of legitimate files/resources that can lead to undetected malware, execution of malware, and spread of malware

Tower's Capabilities against TTP

- **File Integrity Monitoring:** Monitor changes to critical system files and directories
- **Employee Training:** Train to verify file sources and avoid blindly executing files
- **Regular Audits:** Review directories and services, remove suspicious/unnecessary entries
- **Endpoint Detection:** Signature-based detection, behavioral analysis, and heuristic algorithms to protect against malicious files and executables

Discovery / Network Service Discovery

APT Groups

Scattered Spider, Cobalt Group, Dark Vishnya, Lazarus

MITRE Definition

Adversaries may attempt to get a listing of services running on remote hosts and local network infrastructure devices, including those that may be vulnerable to remote software exploitation. Common methods to acquire this information include port and/or vulnerability scans using tools that are brought onto a system.

Dangers

While devices perform network discovery, data can be intercepted by third parties, malicious software with network access can read all unencrypted traffic, and devices may have exploitable vulnerabilities

Tower's Capabilities against TTP

- **Network Segmentation:** Isolate critical systems to limit exposure during discovery
- **Firewalls:** Configure firewalls and rules to restrict unnecessary service discovery traffic
- **Encryption:** Encrypt traffic to prevent eavesdropping
- **Authentication and Authorization:** Authenticate and ensure only authorized devices are participating in network discovery

Command and Control / Ingress Tool Transfer

APT Groups

Scattered Spider, Indrik Spider, Cobalt Group, Lazarus

MITRE Definition:

Adversaries may transfer tools or other files from an external system into a compromised environment. Tools or files may be copied from an external adversary-controlled system to the victim network through the command and control channel or through alternate protocols such as ftp. Once present, adversaries may also transfer/spread tools between victim devices within a compromised environment

Dangers

Transfer tools/files to compromised environment in order to move laterally within network for malware delivery

Tower's Capabilities against TTP

- **Network Segmentation:** Isolate critical systems to prevent lateral movement
- **Firewall Rules:** Configure firewalls to restrict tool transfer traffic
- **Least Privilege:** Ensure only authorized users can transfer tools
- **Monitoring and Detection:** IDS and IPS to detect any suspicious tool transfers, utilizing signatures

Command and Control / Remote Access Software

APT Groups

Scattered Spider, Carbanak, Cobalt Group, Dark Vishnya

MITRE Definition:

An adversary may use legitimate desktop support and remote access software to establish an interactive command and control channel to target systems within networks. These services, such as VNC, Team Viewer, AnyDesk, ScreenConnect, LogMein, AmmyyAdmin, and other remote monitoring and management (RMM) tools, are commonly used as legitimate technical support software and may be allowed by application control within a target environment.

Dangers

Attackers may use command and control to remotely manage compromised systems, carrying out malicious activities undetected

Tower's Capabilities against TTP

- **Network Segmentation:** Isolate critical systems so they are not be access by lateral movement
- **Credentials:** Implement strong password policies, MFA, and regular password changes to prevent account access
- **Remote Access Control:** Restrict remote access to essential personnel, use secure VPNs
- **Logging:** Continuously monitor logs for any unauthorized behavior or suspicious activity

Government APT Group Analysis

Researching Government APT Groups

We started our research off of the APT group database found on the MITRE ATT&CK navigator. From here, we started to filter the APT groups based on if they pose risk to the Government sector. In order to be more efficient in the filtering process, we decided to only worry about APT groups that attacked/attacks the USA.

After this initial research/filter phase, we had 31 APT Groups that had a history of targeting the Government sector.

With this narrowed down list of APT groups, we went through each one and researched things such as:

1) What type of attacks have they done in the past
2) What specific type of US government body did they attack?
3) How sophisticated and capable are these APT groups?

Based on these questions, we assigned a “Danger Score” ranging from 1(No Risk) to 5(High Risk) to each of the APT groups. APT groups that attacked important government bodies (ex. Department of Defense, Pentagon, White House) were awarded a score of 5. We selected the top 6 APT groups that had the highest scores and posed the most risk to Tower based on their past attacks and sophistication.

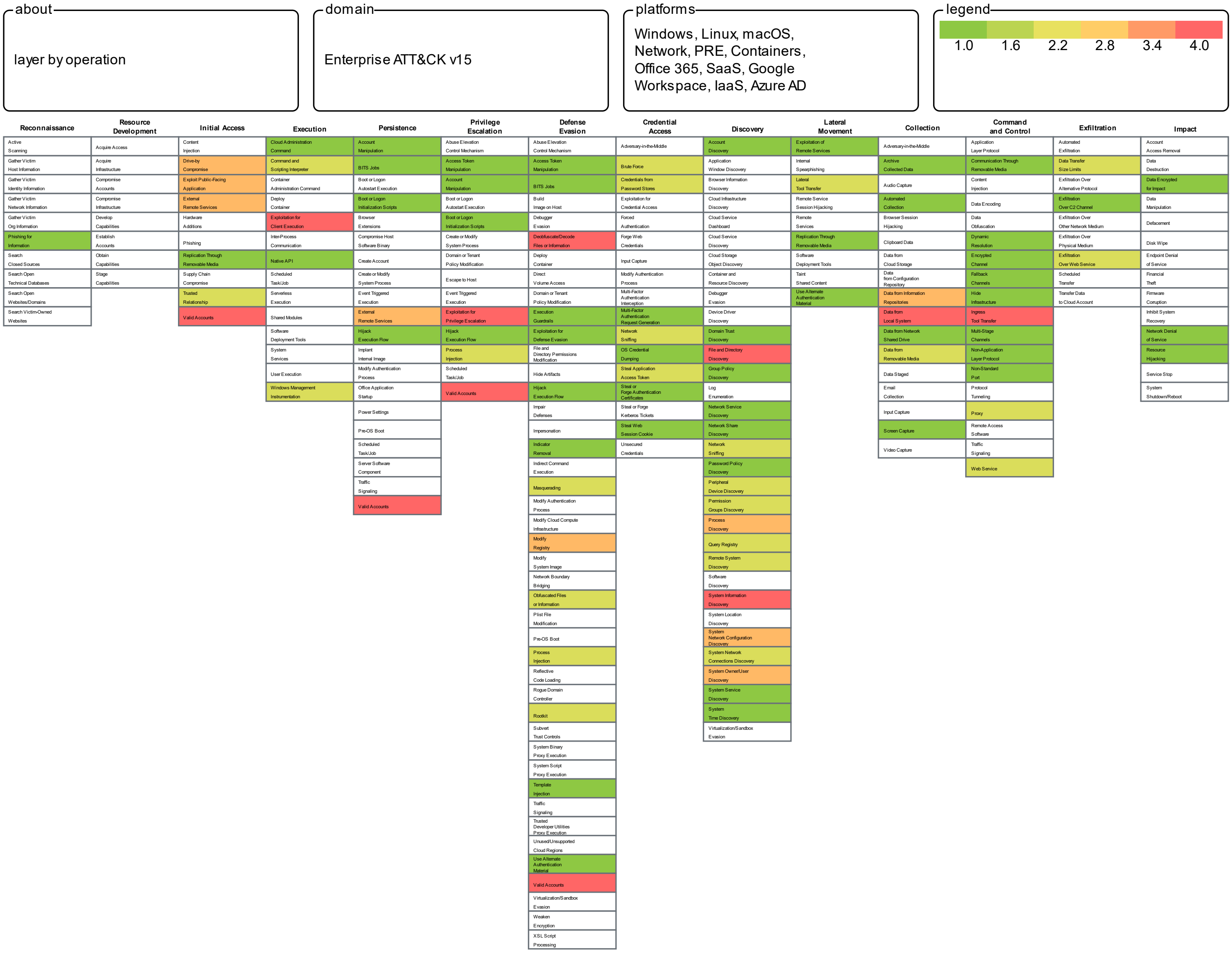
The groups were:

APT41, APT19, Sofacy, Turla, APT29, APT33

Utilizing MITRE ATT&CK Navigator

Government_APT_Groups.pdf   Government_APT_Groups_Expanded.pd

After we had our 6 groups, we put those APT groups into the MITRE ATT&CK Navigator which shows a dashboard of all the TTPs that these APT groups use. TTPs that are in a shade of red came up more than the TTPs that are in a shade of green. Therefore, red TTPs are those that should be of more concern.



about
layer by operation

domain
Enterprise ATT&CK v15

platforms
Windows, Linux, macOS, Network, PRE, Containers, Office 365, SaaS, Google Workspace, IaaS, Azure AD

legend
1.0 1.6 2.2 2.8 3.4 4.0

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Active Scanning	Acquire Access	Content Injection	Cloud Administration Command	Account Manipulation	Abuse Elevation Control Mechanism	Abuse Elevation Control Mechanism	Adversary-in-the-Middle	Account Discovery	Exploitation of Remote Services	Adversary-in-the-Middle	Application Layer Protocol	Automated Exfiltration	Account Access Removal
Gather Victim Host Information	Acquire Infrastructure	Drive-by Compromise	Command and Scripting Interpreter	BITS Jobs	Access Token Manipulation	Access Token Manipulation	Brute Force	Application Window Discovery	Internal Spearphishing	Archive Collected Data	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information	Compromise Accounts	Exploit Public-Facing Application	Container Administration Command	Boot or Logon Autostart Execution	Account Manipulation	BITS Jobs	Credentials from Password Stores	Browser Information Discovery	Lateral Tool Transfer	Audio Capture	Content Injection	Exfiltration Over Alternative Protocol	Data Encrypted for Impact
Gather Victim Network Information	Compromise Infrastructure	External Remote Services	Deploy Container	Boot or Logon Initialization Scripts	Boot or Logon Autostart Execution	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking	Automated Collection	Data Encoding	Exfiltration Over C2 Channel	Data Manipulation
Gather Victim Org Information	Develop Capabilities	Hardware Additions	Exploitation for Client Execution	Browser Extensions	Boot or Logon Initialization Scripts	Debugger Evasion	Forced Authentication	Cloud Service Dashboard	Remote Services	Browser Session Hijacking	Data Obfuscation	Exfiltration Over Other Network Medium	Defacement
Phishing for Information	Establish Accounts	Phishing	Inter-Process Communication	Compromise Host Software Binary	Create or Modify System Process	Deobfuscate/Decode Files or Information	Forge Web Credentials	Cloud Service Discovery	Replication Through Removable Media	Clipboard Data	Dynamic Resolution	Exfiltration Over Physical Medium	Disk Wipe
Search Closed Sources	Obtain Capabilities	Replication Through Removable Media	Native API	Create Account	Domain or Tenant Policy Modification	Deploy Container	Input Capture	Cloud Storage Object Discovery	Software Deployment Tools	Data from Cloud Storage	Encrypted Channel	Exfiltration Over Web Service	Endpoint Denial of Service
Search Open Technical Databases	Stage Capabilities	Supply Chain Compromise	Scheduled Task/Job	Create or Modify System Process	Escape to Host	Direct Volume Access	Modify Authentication Process	Container and Resource Discovery	Taint Shared Content	Data from Configuration Repository	Fallback Channels	Scheduled Transfer	Financial Theft
Search Open Websites/Domains		Trusted Relationship	Serverless Execution	Event Triggered Execution	Event Triggered Execution	Domain or Tenant Policy Modification	Multi-Factor Authentication Interception	Debugger Evasion	Use Alternate Authentication Material	Data from Information Repositories	Hide Infrastructure	Transfer Data to Cloud Account	Firmware Corruption
Search Victim-Owned Websites		Valid Accounts	Shared Modules	External Remote Services	Exploitation for Privilege Escalation	Execution Guardrails	Multi-Factor Authentication Request Generation	Device Driver Discovery		Data from Local System	Ingress Tool Transfer		Inhibit System Recovery
			Software Deployment Tools	Hijack Execution Flow	Hijack Execution Flow	Exploitation for Defense Evasion	Network Sniffing	Domain Trust Discovery		Data from Network Shared Drive	Multi-Stage Channels		Network Denial of Service
			System Services	Implant Internal Image	Process Injection	File and Directory Permissions Modification	OS Credential Dumping	File and Directory Discovery		Data from Removable Media	Non-Application Layer Protocol		Resource Hijacking
			User Execution	Modify Authentication Process	Scheduled Task/Job	Hide Artifacts	Steal Application Access Token	Group Policy Discovery		Data Staged	Non-Standard Port		Service Stop
			Windows Management Instrumentation	Office Application Startup	Valid Accounts	Hijack Execution Flow	Steal or Forge Authentication Certificates	Log Enumeration		Email Collection	Protocol Tunneling		System Shutdown/Reboot
				Power Settings		Impair Defenses	Steal or Forge Kerberos Tickets	Network Service Discovery		Input Capture	Proxy		
				Pre-OS Boot		Impersonation	Steal Web Session Cookie	Network Share Discovery		Screen Capture	Remote Access Software		
				Scheduled Task/Job		Indicator Removal	Unsecured Credentials	Network Sniffing		Video Capture	Traffic Signaling		
				Server Software Component		Indirect Command Execution		Password Policy Discovery			Web Service		
				Traffic Signaling		Masquerading		Peripheral Device Discovery					
				Valid Accounts		Modify Authentication Process		Permission Groups Discovery					
						Modify Cloud Compute Infrastructure		Process Discovery					
						Modify Registry		Query Registry					
						Modify System Image		Remote System Discovery					
						Network Boundary Bridging		Software Discovery					
						Obfuscated Files or Information		System Information Discovery					
						Plist File Modification		System Location Discovery					
						Pre-OS Boot		System Network Configuration Discovery					
						Process Injection		System Network Connections Discovery					
						Reflective Code Loading		System Owner/User Discovery					
						Rogue Domain Controller		System Service Discovery					
						Rootkit		System Time Discovery					
						Subvert Trust Controls		Virtualization/Sandbox Evasion					
						System Binary Proxy Execution							
						System Script Proxy Execution							
						Template Injection							
						Traffic Signaling							
						Trusted Developer Utilities Proxy Execution							
						Unused/Unsupported Cloud Regions							
						Use Alternate Authentication Material							
						Valid Accounts							
						Virtualization/Sandbox Evasion							
						Weaken Encryption							
						XSL Script Processing							

Government Critical TTPs

Resource Development / Obtain Capabilities / Tool

Initial Access / Phishing / Spear phishing Attachment

Execution / Command and Scripting Interpreter / PowerShell

Persistence / Boot or Logon AutoStart Execution / Registry Run Keys Startup Folder

Privilege Escalation / Exploitation for Privilege Escalation

Defense Evasion / Obfuscate or Decode Files of Information

Discovery / System Information Discovery

Collection / Archive Collected Data/ Archive via Utility

Command and Control / Application Layer Protocol / Web Protocols

Command and Control / Ingress Tool Transfer

Resource Development / Obtain Capabilities / Tool

APT Groups

APT41, APT19, Sofacy, Turla, APT29, APT33

MITRE Description

Adversaries may buy, steal, or download software tools that can be used during targeting. Tools can be open or closed source, free or commercial. A tool can be used for malicious purposes by an adversary, but (unlike malware) were not intended to be used for those purposes

Dangers

Utilizing tools in order to carry out malicious attacks. Attackers who are not that sophisticated could cause damage due to these available tools

Tower’s Capabilities Against TTP

Hard to mitigate the availability of tools as Tower has no control over that. Tower employs a layered defense system in order to defend against any tool or malicious attack.

Initial Access / Phishing / Spear phishing Attachment

APT Groups

APT41, APT19, Sofacy, Turla, APT29, APT33

MITRE Description

Adversaries may send spearphishing emails with a malicious attachment in an attempt to gain access to victim systems. Spearphishing attachment is a specific variant of spearphishing. Spearphishing attachment is different from other forms of spearphishing in that it employs the use of malware attached to an email. All forms of spearphishing are electronically delivered social engineering targeted at a specific individual, company, or industry. In this scenario, adversaries attach a file to the spearphishing email and usually rely upon User Execution to gain execution.[1] Spearphishing may also involve social engineering techniques, such as posing as a trusted source.

Dangers

Targeted attacks to deceive a particular individual with attachments that contain malware, disguised executables in order to commit malicious activities

Tower's Capabilities Against TTP

- **Employee Training:** PhishER used to train employees on social engineering attacks such as phishing
- **Network Intrusion Prevention:** Scan and remove malicious email attachments
- **Restricting Content:** Block risky attachments
- **Antivirus:** Scan for viruses

Execution / Command and Scripting Interpreter / PowerShell

APT Groups

APT33, APT29, Turla, Sofacy, APT19, APT41

MITRE Description

Adversaries may abuse PowerShell commands and scripts for execution. PowerShell is a powerful interactive command-line interface and scripting environment included in the Windows operating system.[1] Adversaries can use PowerShell to perform a number of actions, including discovery of information and execution of code.

Dangers

Utilizing PowerShell to execute harmful scripts/commands for data exfiltration, lateral movement, ransomware deployment, disabling security controls

Tower's Capabilities against TTP

- **Application whitelisting**: Allow only approved scripts and executables to run
- **Network Segmentation**: Isolate critical systems
- **Log scripts**: Constantly monitor for any suspicious activity
- **Least Privilege**: Assign minimal permissions to user accounts, avoid running PowerShell unless necessary

Persistence / Boot or Logon AutoStart Execution / Registry Run Keys Startup Folder

APT Groups

APT41, APT19, APT33, APT29, Turla, Sofacy

MITRE Description

Adversaries may achieve persistence by adding a program to a startup folder or referencing it with a Registry run key. Adding an entry to the "run keys" in the Registry or startup folder will cause the program referenced to be executed when a user logs in.[1] These programs will be executed under the context of the user and will have the account's associated permissions level.

Dangers

Executing programs unknown to user can lead to malware persistence, system performance impact, increased attack surface

Tower's Capabilities against TTP

- **Application whitelisting**: Allow only approved programs and executables to run
- **Monitor:** Monitor executed commands, start folder, newly created registry keys for any suspicious or unauthorized behavior

Privilege Escalation / Exploitation for Privilege Escalation

APT Groups

APT41, APT33, APT29, Turla, Sofacy

MITRE Description

Adversaries may exploit software vulnerabilities in an attempt to elevate privileges. Exploitation of a software vulnerability occurs when an adversary takes advantage of a programming error in a program, service, or within the operating system software or kernel itself to execute adversary-controlled code. Security constructs such as permission levels will often hinder access to information and use of certain techniques, so adversaries will likely need to perform privilege escalation to include use of software exploitation to circumvent those restrictions.

Dangers

With privilege escalation, attackers gain more access to critical systems and can cause great damage by installing malware, deleting databases, disabling crucial services, and stealing sensitive files

Tower’s Capabilities against TTP

- **Isolation and Sandboxing:** Make it difficult for attackers to advance their operation
- **Execution Prevention:** Block execution of known vulnerability drivers that attackers may exploit
- **Exploit Protection:** Security applications that analyze behavior during exploits can be used to mitigate
- **Updates:** Employ patches and updates to mitigate vulnerabilities

Defense Evasion / Obfuscate or Decode Files of Information

APT Groups

APT41, APT19, APT29, Turla, Sofacy

MITRE Description

Adversaries may use Obfuscated Files or Information to hide artifacts of an intrusion from analysis. They may require separate mechanisms to decode or deobfuscate that information depending on how they intend to use it. Methods for doing that include built-in functionality of malware or by using utilities present on the system.

Dangers

Obfuscating files to evade defenses could lead to attackers being in your system undetected

Tower's Capabilities against TTP

- **Monitor:** Monitor changes made to files, newly executed processes, and scripts as these changes may be used to hide artifacts
- **EDR:** Analyze and detect anomalies indicative of obfuscation techniques
- **Signature Based Detection and Heuristics:** Recognize patterns and behaviors of previous obfuscations and utilize heuristics to detect variations in methods

Discovery / System Information Discovery

APT Groups

APT41, APT19, APT29, Turla, Sofacy

MITRE Description

An adversary may attempt to get detailed information about the operating system and hardware, including version, patches, hotfixes, service packs, and architecture. Adversaries may use the information from System Information Discovery during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions.

Dangers

Attackers could gain detailed information about the security posture of an organization and develop specific attacks

Tower's Capabilities against TTP

- **Encryption:** Encrypt sensitive data to prevent attackers from gaining knowledge
- **Network Segmentation:** Isolate critical systems and sensitive data to reduce possible exposure
- **Monitor:** Review logs for any suspicious activity

Collection / Archive Collected Data/ Archive via Utility

APT Groups

APT41, APT33, APT29, Turla, Sofacy

MITRE Description

Adversaries may use utilities to compress and/or encrypt collected data prior to exfiltration. Many utilities include functionalities to compress, encrypt, or otherwise package data into a format that is easier/more secure to transport. Adversaries may abuse various utilities to compress or encrypt data before exfiltration. Some third party utilities may be preinstalled, such as tar on Linux and macOS or zip on Windows systems.

Dangers

By using utilities to encrypt data prior to exfiltration, attackers can go undetected and an organization may not even know data is being exfiltrated

Tower's Capabilities against TTP

- **Audit:** System scans can be performed to identify unauthorized archived utilities
- **Application Whitelisting:** restrict use of utilities to prevent unauthorized/unknown utilities from running
- **EDR:** Provide visibility into endpoint activities like data compression/encryption

Command and Control / Application Layer Protocol / Web Protocols

APT Groups

APT41, APT33, APT29, Turla, Sofacy, APT19

MITRE Description

Adversaries may communicate using application layer protocols associated with web traffic to avoid detection/network filtering by blending in with existing traffic. Commands to the remote system, and often the results of those commands, will be embedded within the protocol traffic between the client and server.

Dangers

Attackers can go undetected and perform malicious attacks from within

Tower's Capabilities against TTP

- **Packet Inspection:** Implementing DPI to analyze web traffic to look for anomalies
- **Network Segmentation and Access Control:** Isolating critical assets and ensure only authorized traffic and protocols are permitted, reducing attack surface
- **SSL/TLS Inspection:** Many communications may be encrypted with SSL/TLS, so inspecting may uncover malicious activities hidden within

Command and Control / Ingress Tool Transfer

APT Groups

APT41, APT33, APT29, Turla, Sofacy

MITRE Definition:

Adversaries may transfer tools or other files from an external system into a compromised environment. Tools or files may be copied from an external adversary-controlled system to the victim network through the command and control channel or through alternate protocols such as ftp. Once present, adversaries may also transfer/spread tools between victim devices within a compromised environment

Dangers

Transfer tools/files to compromised environment in order to move laterally within network for malware delivery

Tower’s Capabilities against TTP

- **Network Segmentation:** Isolate critical systems to prevent lateral movement
- **Firewall Rules:** Configure firewalls to restrict tool transfer traffic
- **Least Privilege:** Ensure only authorized users can transfer tools
- **Monitoring and Detection:** IDS and IPS to detect any suspicious tool transfers, utilizing signatures