ANKARA YILDIRIM BEYAZIT UNIVERSITY

FACULTY OF MANAGEMENT

CYBER KILL CHAIN AND MITRE ATT&CK FRAMEWORK

FINAL PROJECT REPORT

16030211014 – DERYA SAHA

15030461001 – HATİCE ARSLANHAN

17030411048 – MEHMET SAİT ALTINTAŞ

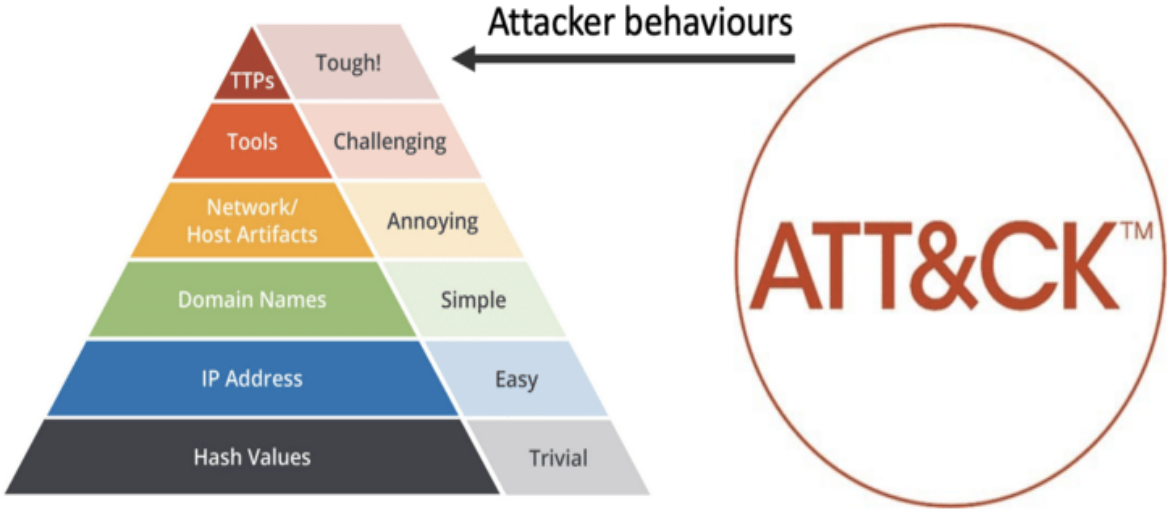
INTRODUCTION

Cyber attacks today have become as sophisticated as can be. Taking necessary precautions against these attacks is an important element for corporate security. There are many attack methodologies to predict the attacker's behavior during defense.

Cyber attacks, which have become widespread in the current period, have been going on for years. Various threat modeling studies are carried out against these attacks.

Skilled and motivated cyber attackers undergo thorough preparation before a cyberattack. After choosing a goal for their motivation, they begin to gather information about their goals. They aim to increase the probability of success of the cyber attack by acting systematically and organized. This situation forces us, who are on the defense side of cyber attacks, to understand the working methods of cyber attackers and to be prepared for these attacks.

This report will examine the ATT&CK knowledge base offered by MITER, which can be used to develop threat modeling and defense methodology, and the Cyber Kill Chain model, an intelligence-driven defense model.



A) Cyber Kill Chain

Intelligence guided defense model. In this article, we will talk about what the cyber kill chain is and what its steps are. Cyber attacks are the worst nightmare for most of us. That's why many cyber security experts and developers offer unique solutions for identifying and preventing cyber attack activities. One of these developers, Lockheed Martin, introduced Cyber Kill Chain into our lives. We continue to use it today.

What is the Cyber Kill Chain?

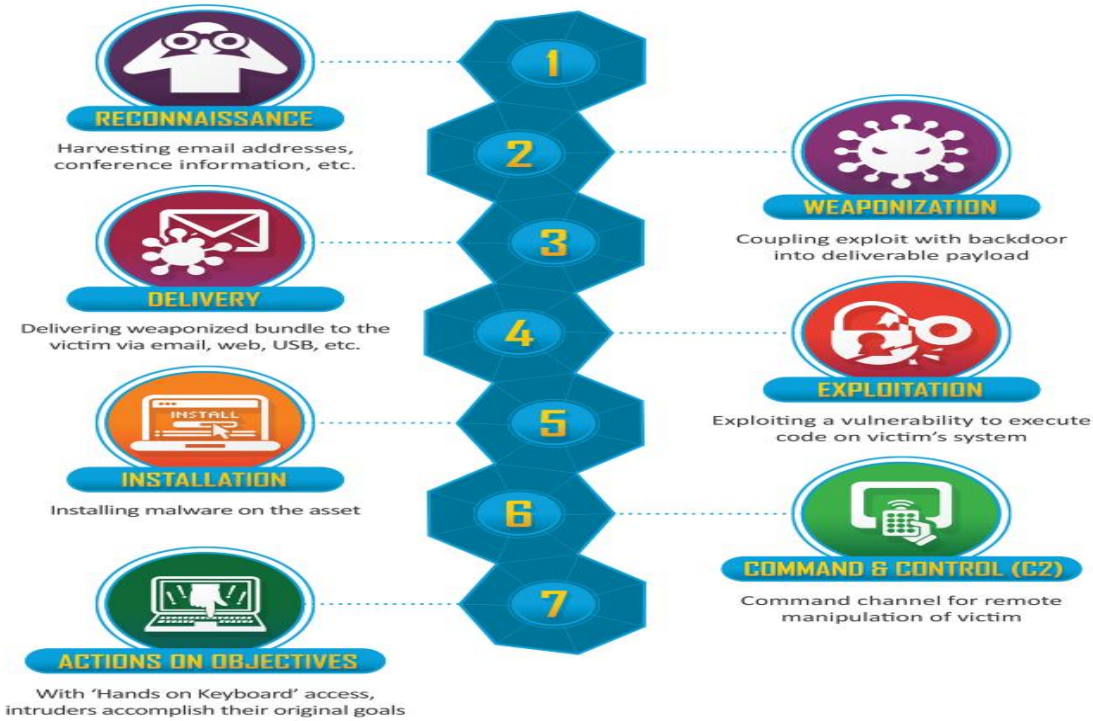
The term "**kill chain**" was first used as a military concept that defines the structure of an attack that covers:

- The identification of the target
- The force dispatch towards the target
- The decision and order to attack the target
- The destruction of the target

The idea of interrupting the opponent's kill chain activity is often employed as a defence. Inspired by the whole kill chain concept, Lockheed Martin (an aerospace, security, arms, defence and advanced technologies company based in the United States of America) created the Cyber Kill Chain. It is a cyber security framework that offers a method to deal with the intrusions on a computer network.

Since it first emerged, the Cyber Kill Chain has evolved significantly in order to anticipate and recognize insider threats much better, detect various other attack techniques like advanced ransomware and social engineering.

The Cyber Kill Chain consists of seven steps that aim to offer a better attack visibility while supporting the cyberattack / cybersecurity analyst to get a better understanding of the adversary's tactics, procedures and techniques. The seven steps of the Cyber Kill Chain illustrates the different phases of a cyberattack starting from reconnaissance, reaching to the exfiltration.



The Cyber Kill Chain consists of 7 steps: Reconnaissance, weaponization, delivery, exploitation, installation, command and control, and finally, actions on objectives. Below you can find detailed information on each.

1. Reconnaissance: In this step, the attacker / intruder chooses their target. Then they conduct an in-depth research on this target to identify its vulnerabilities that can be exploited.

2. Weaponization: In this step, the intruder creates a **malware weapon** like a virus, worm or such in order to exploit the vulnerabilities of the target. Depending on the target and the purpose of the attacker, this malware can exploit new, **undetected vulnerabilities** (also known as the **zero-day exploits**) or it can focus on a combination of different vulnerabilities.

3. Delivery: This step involves transmitting the weapon to the target. The intruder / attacker can employ different methods like USB drives, e-mail attachments and websites for this purpose.

4. Exploitation: In this step, the malware starts the action. The program code of the malware is triggered to exploit the target's vulnerability/vulnerabilities.

5. Installation: In this step, the malware installs an access point for the intruder / attacker. This access point is also known as the backdoor.

6. Command and Control: The malware gives the intruder / attacker access in the network/system.

7. Actions on Objective: Once the attacker / intruder gains persistent access, they finally take action to fullfil their purpose, such as **encryption** for ransom, **data exfiltration** or even **data destruction**.

Each of the steps we mentioned above is connected to each other like a chain. The success of each stage will directly affect another stage. For example, an attack without good reconnaissance is very likely to fail in the forwarding phase.

EXAMPLE:

PHASE	**EXPLANATION**
Reconnaissance	The e-mail addresses of the target are detected.
Weaponization	Harmful doc file is prepared.
Delivery	The malicious doc file is sent to the destination via e-mail.
Exploitation	The CVE-2017-8570 vulnerability is exploited.
Installation	HKEY_CURRENT_USER\Software\Microsoft\Current Version\Run
Command and Control	It communicates via HTTPS with xx.77.87.
Actions on Objective	It sends files containing corporate data to the command center.

In our example, the cyber attacker targets an institution named y in order to obtain files containing corporate data. After determining his motivation, he starts the exploration work about the institution. It detects that the employees of the target institution use their corporate e-mail addresses in their social media accounts and creates an e-mail pool. After this stage, it moves on to the stage of determining the attack vector to be used in the social engineering attack. Since they have detected that the target institution is using a Windows operating system during the discovery phase, they think that it would be a correct method to use the Microsoft Office remote code execution vulnerability with the code CVE-2017–8570. At this stage, it creates a macro code that can exploit the security vulnerability and prepares the attack vector with the extension ".doc". The attacker who prepared the attack vector sends the malware to the user via e-mail and waits for the user to open the file. Employees of the target institution open the malicious file in the e-mail and from this stage on, the malicious file is infected with the target systems. The malicious file exploits the vulnerability in the target system and installs itself at the start of the operating system, making it permanent. After this stage, the malware communicates with the domain address of xx.77.87 (which is an invalid domain address) and opens the way for the cyber attacker to remotely control the target system. The attacker, who has taken over the system, looks for corporate documents that provide motivation and manages to extract them to the command control server.

Why Do We Need It?

In order to take precautions against cyber attacks, it is necessary to know the attack methodologies well. Thanks to models such as Cyber Kill Chain, missing points can be detected before a cyber attack, the intervention method can be decided according to the stage of the attack at the time of the attack, and a risk analysis can be made after the attack to what extent the institution is affected by this attack.

The ATT&CK Framework is an information resource describing the tactics, techniques, and procedures used by attackers and is shaped in the last four steps of the Cyber Kill Chain.

Unlike the Cyber Kill Chain, the ATT&CK Framework does not follow a linear order. It is thought that the attacker can use any technique he wants to achieve his goal. In summary, the ATT&CK Framework has emerged with the aim of classifying the aggressive behaviors and making sense of the aggressive actions.

B) MITRE ve ATT&CK Framework

MITRE; is a non-profit organization supported by federal governments, working in many fields such as defense, intelligence, aviation, private sector, homeland security, judiciary, health, and doing many federal research and development.

ATT&CK Framework (Adversarial Tactics, Techniques, and Common Knowledge), launched by MITER for free in 2013, is a knowledge base that models aggressive behavior in known (almost all) cyber-attacks. The following concepts are grouped and associated with the ATT&CK Framework.

• **Groups:** These are the groups that carry out the attacks. Sample; Like APT41, Lazarus, Carbanak,….

• **Industries:** The organizations targeted by the attackers are the sectors. Sample; finance, government, health, etc.

• **Tactics:** The technique used by the attackers is the target. That is, the focus is on the "why" of the attack and "what purpose does the attacker have?" question is answered. Sample; such as first access (TA0001), entitlement upgrade (TA0004),…. Also, there is no order of importance among tactics.

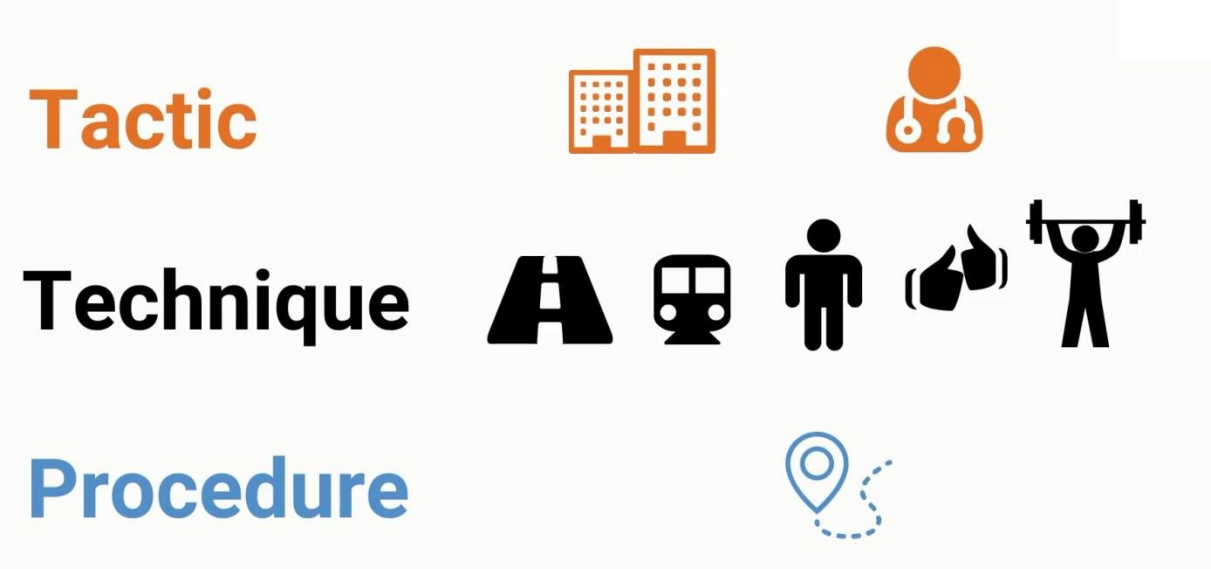
• **Techniques:** How (by which method) the objectives specified in the tactics will be achieved. Sample; phishing (T1566), recording keyboard movements (T1056.001),… etc.

• **Procedures:** It is the specialized application of techniques. Sample; such as downloading and running the powershell file, group APT39 creating scheduled task for persistence….

• **Tools / Software:** Applications or malicious software used. Sample; Like Mimikatz, Empire, Cobalt Strike, Duqu,…

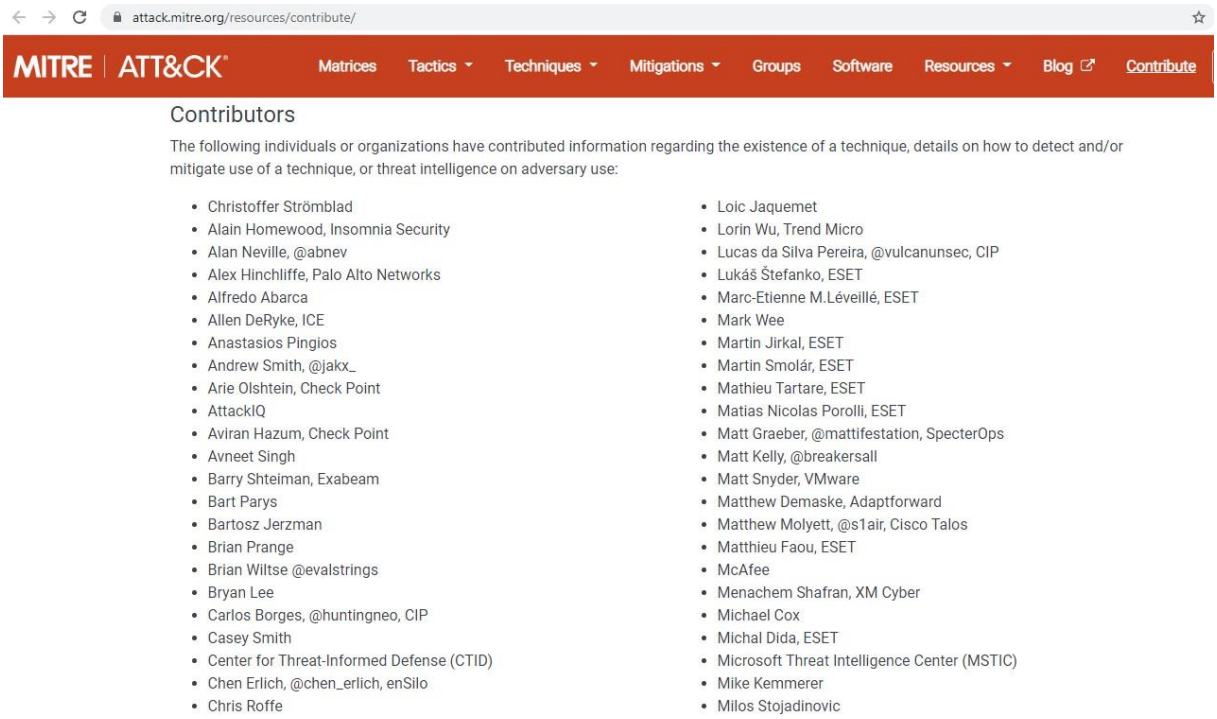
• **Detections:** These are the methods that can be used to detect attacks. Sample; monitoring network anomalies, generating alarms for changes in group memberships,… etc.

• **Precautions:** These are the precautions that can be taken against attacks. Sample; such as code signing, data backup, antivirus usage….



Note: During an attack, the attacker does not use all of these tactics and techniques. He/she can choose a method suitable for the environment and himself/herself.

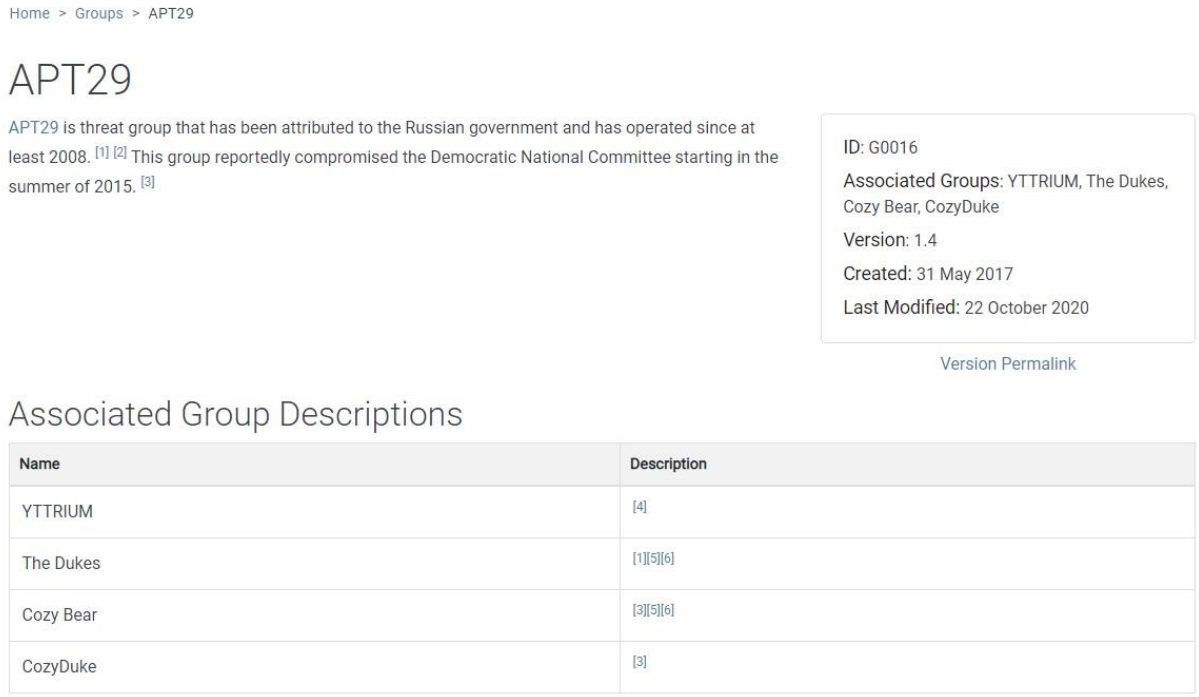
The ATT&CK Framework provides a constantly updated platform. There are many people and institutions that support these updates.



C) Application

The following information can be obtained with the ATT&CK Framework.

Which country the APT29 group is close to, which groups it is associated with, which sectors they attack, the techniques and software it uses



Home > Groups > APT29

APT29

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

ID: G0016
Associated Groups: YTTRIUM, The Dukes, Cozy Bear, CozyDuke
Version: 1.4
Created: 31 May 2017
Last Modified: 22 October 2020

Version Permalink

Associated Group Descriptions

Name	Description
YTTRIUM	[4]
The Dukes	[1][5][6]
Cozy Bear	[3][5][6]
CozyDuke	[3]

Software

ID	Name	References	Techniques
S0054	CloudDuke	[1]	Application Layer Protocol: Web Protocols, Ingress Tool Transfer, Web Service: Bidirectional Communication
S0154	Cobalt Strike	[9]	Abuse Elevation Control Mechanism: Bypass User Account Control, Access Token Manipulation: Token Impersonation/Theft, Access Token Manipulation: Parent PID Spoofing, Access Token Manipulation: Make and Impersonate Token, Account Discovery: Domain Account, Application Layer Protocol, Application Layer Protocol: DNS, Application Layer Protocol: Web Protocols, BITS Jobs, Command and Scripting Interpreter: Windows Command Shell, Command and Scripting Interpreter: PowerShell, Command and Scripting Interpreter: Visual Basic, Command and Scripting Interpreter: Python, Commonly Used Port, Create or Modify System Process: Windows Service, Data from Local System, Exploitation for Privilege Escalation, Indicator Removal on Host: Timestomp, Input Capture: Keylogging, Man in the Browser, Multiband Communication, Native API, Network Service Scanning, Network Share Discovery, Obfuscated Files or Information: Indicator Removal from Tools, OS Credential Dumping: Security Account Manager, Process Discovery, Process Injection, Process Injection: Process Hollowing, Protocol Tunneling, Proxy: Internal Proxy, Remote Services: SMB/Windows Admin Shares, Remote Services: Windows Remote Management, Remote Services: SSH, Remote Services: Remote Desktop Protocol, Remote Services: Distributed Component Object Model, Remote System Discovery, Scheduled Transfer, Screen Capture, System Network Configuration Discovery, System Services: Service Execution, Use Alternate Authentication Material: Pass the Hash, Valid Accounts: Local Accounts, Valid Accounts: Domain Accounts, Windows Management Instrumentation
S0050	CosmicDuke	[1]	Application Layer Protocol: Web Protocols, Automated Exfiltration, Clipboard Data, Create or Modify System Process: Windows Service, Credentials from Password Stores, Credentials from Password Stores: Credentials from Web Browsers, Data from Local System, Data from Network Shared Drive, Data from Removable Media, Email Collection: Local Email Collection, Encrypted Channel: Symmetric Cryptography, Exfiltration Over Alternative Protocol: Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol, Exploitation for Privilege Escalation, File and Directory Discovery, Input Capture: Keylogging, OS Credential Dumping: LSA Secrets, OS Credential Dumping: Security Account Manager, Scheduled Task/Job: Scheduled Task, Screen Capture

Techniques Used

ATT&CK® Navigator Layers

Domain	ID		Name	Use
Enterprise	T1548	.002	Abuse Elevation Control Mechanism: Bypass User Account Control	APT29 has bypassed UAC.[7]
Enterprise	T1583	.006	Acquire Infrastructure: Web Services	APT29 has registered algorithmically generated Twitter handles that are used for C2 by malware, such as HAMMERTOSS.[8]
Enterprise	T1547	.001	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	APT29 added Registry Run keys to establish persistence.[7]
		.009	Boot or Logon Autostart Execution: Shortcut Modification	APT29 drops a Windows shortcut file for execution.[9]
Enterprise	T1059	.001	Command and Scripting Interpreter: PowerShell	APT29 has used encoded PowerShell scripts uploaded to CozyCar installations to download and install SeaDuke. APT29 also used PowerShell scripts to evade defenses.[10][7][9]

Techniques that can be used for the tactic of stealing identity data from a mobile device .

Home > Tactics > Mobile > Credential Access

Credential Access

The adversary is trying to steal account names, passwords, or other secrets that enable access to resources.

Credential access represents techniques that can be used by adversaries to obtain access to or control over passwords, tokens, cryptographic keys, or other values that could be used by an adversary to gain unauthorized access to resources. Credential access allows the adversary to assume the identity of an account, with all of that account's permissions on the system and network, and makes it harder for defenders to detect the adversary. With sufficient access within a network, an adversary can create accounts for later use within the environment.

ID: TA0031
Created: 17 October 2018
Last Modified: 27 January 2020

Version Permalink

Techniques

Techniques: 11

ID	Name	Description
T1517	Access Notifications	A malicious application can read notifications sent by the operating system or other applications, which may contain sensitive data such as one-time authentication codes sent over SMS, email, or other mediums. A malicious application can also dismiss notifications to prevent the user from noticing that the notifications arrived and can trigger action buttons contained within notifications.
T1413	Access Sensitive Data in Device Logs	On versions of Android prior to 4.1, an adversary may use a malicious application that holds the READ_LOGS permission to obtain private keys, passwords, other credentials, or other sensitive data stored in the device's system log. On Android 4.1 and later, an adversary would need to attempt to perform an operating system privilege escalation attack to be able to access the log.
T1409	Access Stored Application Data	Adversaries may access and collect application data resident on the device. Adversaries often target popular applications such as Facebook, WeChat, and Gmail.
T1414	Capture Clipboard Data	Adversaries may abuse Clipboard Manager APIs to obtain sensitive information copied to the global clipboard. For example, passwords being copy-and-pasted from a password manager app could be captured by another application installed on the device.

Tactics using the Powershell attack technique, the platforms it works on, the necessary authorizations, the usage procedures of this technique, which groups it is used by, the detection of these attacks and the measures that can be taken against these attacks .

Home > Techniques > Enterprise > Command and Scripting Interpreter > PowerShell

Command and Scripting Interpreter: PowerShell

Other sub-techniques of Command and Scripting Interpreter (8)

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. Examples include the `Start-Process` cmdlet which can be used to run an executable and the `Invoke-Command` cmdlet which runs a command locally or on a remote computer (though administrator permissions are required to use PowerShell to connect to remote systems).

PowerShell may also be used to download and run executables from the Internet, which can be executed from disk or in memory without touching disk.

A number of PowerShell-based offensive testing tools are available, including Empire, PowerSploit, PoshC2, and PSAttack.[2]

PowerShell commands/scripts can also be executed without directly invoking the `powershell.exe` binary through interfaces to PowerShell's underlying `System.Management.Automation` assembly DLL exposed through the .NET framework and Windows Common Language Interface (CLI). [3][4][5]

ID: T1059.001
Sub-technique of: T1059
Tactic: Execution
Platforms: Windows
Permissions Required: Administrator, User
Data Sources: DLL monitoring, File monitoring, Loaded DLLs, PowerShell logs, Process command-line parameters, Process monitoring, Windows event logs
Supports Remote: Yes
Contributors: Praetorian
Version: 1.0
Created: 09 March 2020
Last Modified: 24 June 2020

Version Permalink

Procedure Examples

Name	Description
APT19	APT19 used PowerShell commands to execute payloads.[6]
APT28	APT28 downloads and executes PowerShell scripts.[7]
APT29	APT29 has used encoded PowerShell scripts uploaded to CozyCar installations to download and install SeaDuke. APT29 also used PowerShell scripts to evade defenses.[8][9][10]

Mitigations

Mitigation	Description
Antivirus/Antimalware	Anti-virus can be used to automatically quarantine suspicious files.
Code Signing	Set PowerShell execution policy to execute only signed scripts.
Disable or Remove Feature or Program	It may be possible to remove PowerShell from systems when not needed, but a review should be performed to assess the impact to an environment, since it could be in use for many legitimate purposes and administrative functions. Disable/restrict the WinRM Service to help prevent uses of PowerShell for remote execution.
Privileged Account Management	When PowerShell is necessary, restrict PowerShell execution policy to administrators. Be aware that there are methods of bypassing the PowerShell execution policy, depending on environment configuration.[151]

Detection

If proper execution policy is set, adversaries will likely be able to define their own execution policy if they obtain administrator or system access, either through the Registry or at the command line. This change in policy on a system may be a way to detect malicious use of PowerShell. If PowerShell is not used in an environment, then simply looking for PowerShell execution may detect malicious activity.

Monitor for loading and/or execution of artifacts associated with PowerShell specific assemblies, such as System.Management.Automation.dll (especially to unusual process names/locations).[3][4]

It is also beneficial to turn on PowerShell logging to gain increased fidelity in what occurs during execution (which is applied to .NET invocations). [152] PowerShell 5.0 introduced enhanced logging capabilities, and some of those features have since been added to PowerShell 4.0. Earlier versions of PowerShell do not have many logging features.[153] An organization can gather PowerShell execution details in a data analytic platform to supplement it with other data.

Attack techniques that multiple authentication protects.

Multi-factor Authentication

Use two or more pieces of evidence to authenticate to a system; such as username and password in addition to a token from a physical smart card or token generator.

ID: M1032
Version: 1.0
Created: 10 June 2019
Last Modified: 10 June 2019

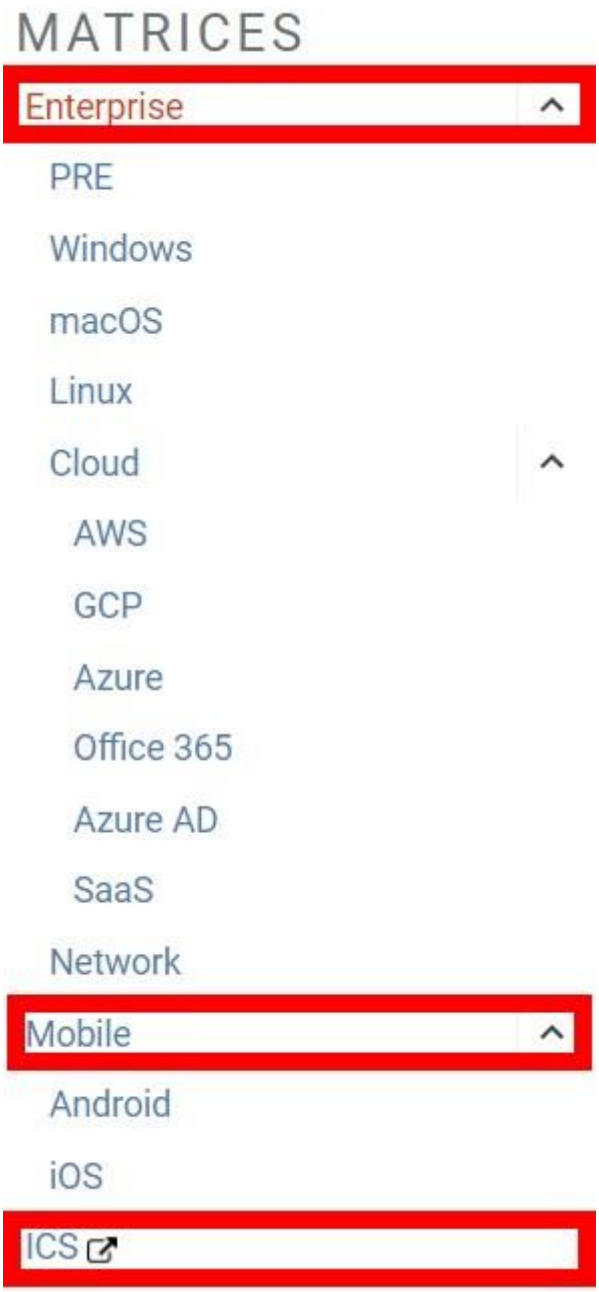
Version Permalink

Techniques Addressed by Mitigation

Domain	ID	Name	Use
Enterprise	T1098	Account Manipulation	Use multi-factor authentication for user and privileged accounts.
	.001	Additional Cloud Credentials	Use multi-factor authentication for user and privileged accounts. Consider enforcing multi-factor authentication for the `CreateKeyPair` and `ImportKeyPair` API calls through IAM policies.[1]
	.002	Exchange Email Delegate Permissions	Use multi-factor authentication for user and privileged accounts.
	.003	Add Office 365 Global Administrator Role	Use multi-factor authentication for user and privileged accounts.
Enterprise	T1110	Brute Force	Use multi-factor authentication. Where possible, also enable multi-factor authentication on externally facing services.
	.001	Password Guessing	Use multi-factor authentication. Where possible, also enable multi-factor authentication on externally facing services.
	.002	Password Cracking	Use multi-factor authentication. Where possible, also enable multi-factor authentication on externally facing services.
	.003	Password Spraying	Use multi-factor authentication. Where possible, also enable multi-factor authentication on externally facing services.
	.004	Credential Stuffing	Use multi-factor authentication. Where possible, also enable multi-factor authentication on externally facing services.

D) Matrices (Domains)

ATT&CK Framework offers 3 domains and sub-domains under them.



D.1) Enterprise ATT&CK

It consists of techniques and tactics for platforms such as Windows, macOS, Linux, PRE, AWS, GCP, Azure, Azure AD, Office 365, SaaS and Network. As of mid-December 2020, it

consists of tactics,117 main techniques and 348 sub-techniques.

For detailed information about the tactics used, the links to Netsmart, Medium [ii] and CyberKavram can be examined.

Reconnaisance

Resource Development (Supportive resource collection)

Initial Access

Execution (Local or remote execution of malicious code/command)

Persistence

Privilege Escalation (Horizontal or vertical authorization/right escalation)

Defense Evasion (Bypass defense systems)

Credential Access (credential collection)

Discovery (Discovery on the network/system being accessed)

Lateral Movement

Collection (Critical data collection)

Command And Control

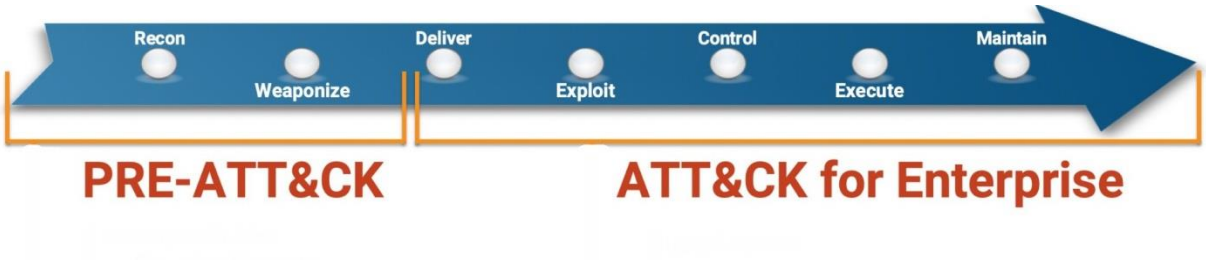
Exfiltration (Missing collected data)

Impact (Preventing availability of existing system/data)

For detailed information about each of these tactics, the Tripwire link in the resources can also be examined. There are also some sub-matrices under the Enterprise ATT&CK matrix. These can be listed as follows.

Pre-ATT&CK Matrix: Covers the attackers' preliminary preparation techniques (intelligence-based), which are the first 2 steps of the Enterprise ATT&CK matrix.

Each of the tactics has different techniques under it. There may be sub-techniques under some techniques. For example, as can be seen from the matrix, there are 19 techniques, 9 of which are original, under the "Initial Access" tactic.

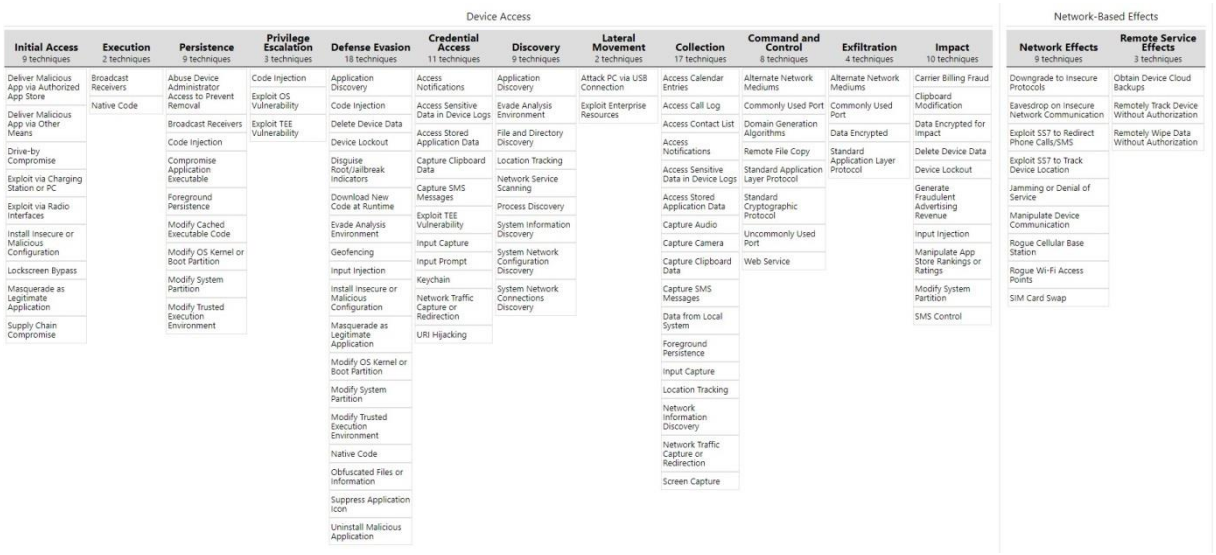


- **• Windows:** Includes attack tactics and techniques for Windows platforms.
- **• macOS:** Includes attack tactics and techniques for macOS platforms.
- **• Linux:** Includes attack tactics and techniques for Linux platforms.
- **• Cloud:** Includes attack tactics and techniques for cloud-based platforms.
- AWS
- GCPAzure
- Office 365
- Azure AD
- SaaS

• Network: Includes attack tactics and techniques for network infrastructure.

D.2) Mobile ATT&CK

It includes attack tactics and techniques for physical (Device Access) or remote (Network-Based Effects) hijacking of mobile devices. As of mid-December 2020, it consists of 14 tactics and 86 main techniques.



For detailed information about the tactics used, the Cyber Concept link in the resources can be examined. Device Access tactics in the Mobile ATT&CK matrix are similar in nomenclature to those in the Enterprise ATT&CK matrix (although they differ in technique).

- **Initial Access**
- **Execution (executing malicious code/command locally or remotely)**
- **Persistence**
- **Privilege Escalation (Horizontal or vertical authorization/right escalation)**
- **Defense Evasion (Bypass defense systems)**
- **Credential Access (credential collection)**
- **Discovery (Discovery in the accessed network / system)**
- **Lateral Movement (Spread over the network)**
- **Collection (Critical data collection)**
- **Command And Control (Commanding and managing victim systems)**
- **Exfiltration (Missing collected data)**
- **Impact (Preventing availability of existing system/data)**

In addition, the two attack tactics under Network-Based Effects, which are carried out remotely to the mobile device, differ.

Network Effects (Monitoring or modifying network traffic)

Remote Service Effects (attacks on external services such as Google Drive, Apple iCloud, MDM)

D.3) ICS ATT&CK

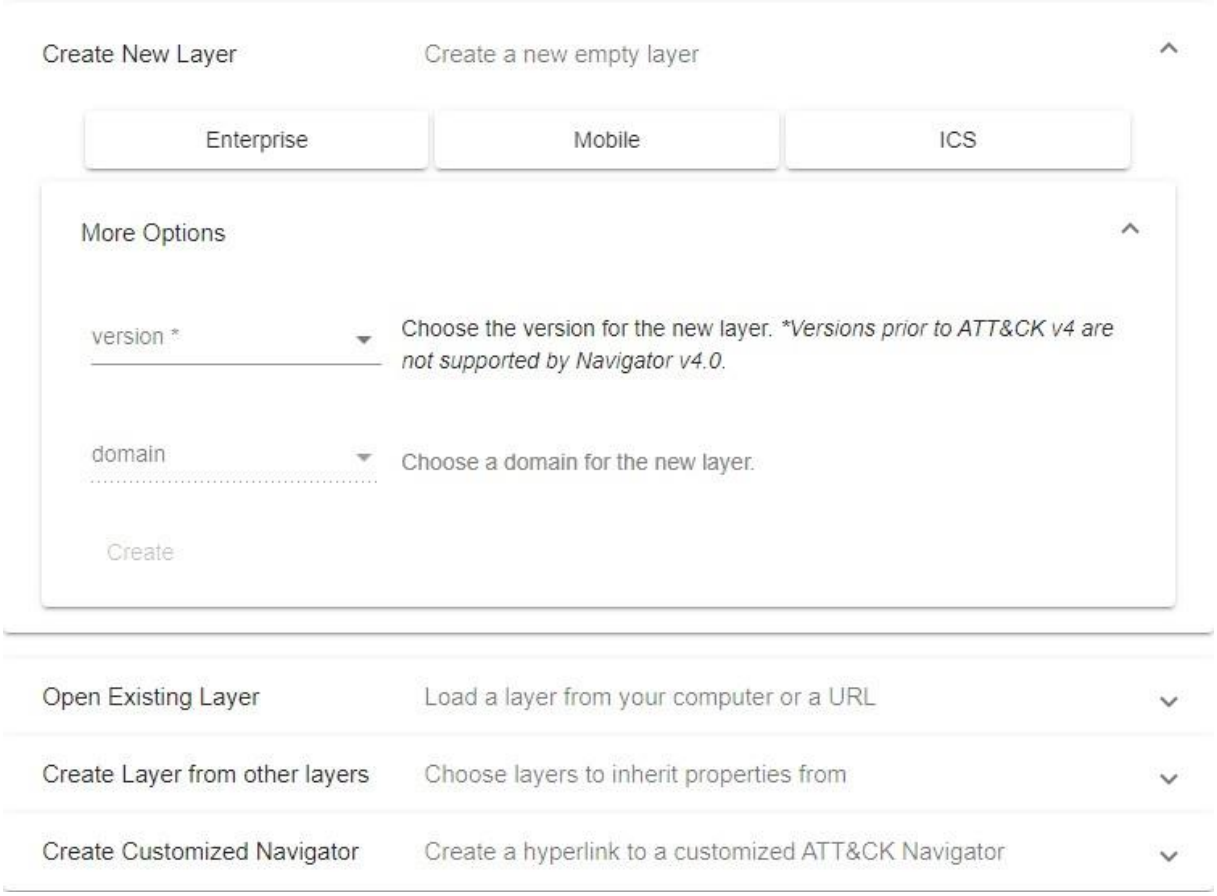
It includes attack tactics and techniques to take over the ICS / EKS (Industrial Control System) environment.

This domain is still under development.

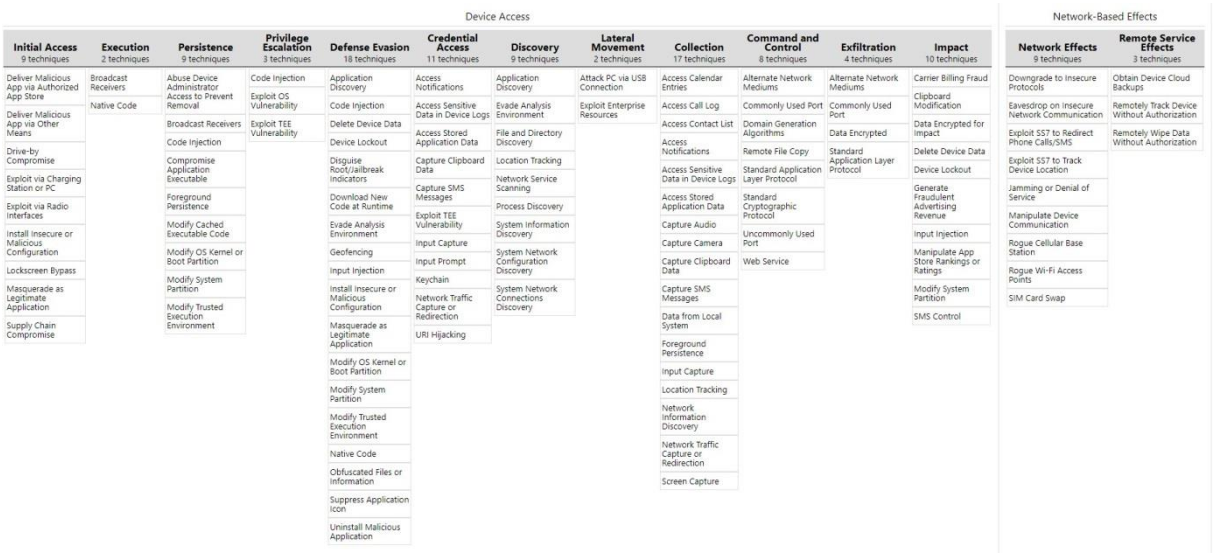
Initial Access 10 techniques	Execution 9 techniques	Persistence 6 techniques	Evasion 7 techniques	Discovery 7 techniques	Lateral Movement 6 techniques	Collection 11 techniques	Command and Control 3 techniques	Inhibit Response Function 15 techniques	Impair Process Control 11 techniques	Impact 11 techniques
Data Historian Compromise	Change Program State	Hooking	Exploitation for Evasion	Control Device Identification	Default Credentials	Automated Collection	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O	Damage to Property
Drive-by Compromise	Command-Line Interface	Module Firmware	Indicator Removal on Host	I/O Module Discovery	Exploitation of Remote Services	Data from Information Repositories	Connection Proxy	Alarm Suppression	Change Program State	Denial of Control
Engineering Workstation Compromise	Execution through API	Program Download	Masquerading	Network Connection Enumeration	External Remote Services	Detect Operating Mode	Standard Application Layer Protocol	Block Command Message	Masquerading	Denial of View
Exploit Public-Facing Application	Graphical User Interface	Project File Infection	Rogue Master Device	Network Service Scanning	Program Organization Units	Detect Program State		Block Reporting Message	Modify Control Logic	Loss of Availability
External Remote Services	Man in the Middle	System Firmware	Rootkit	Network Sniffing	Remote File Copy	I/O Image		Block Serial COM	Modify Parameter	Loss of Control
Internet Accessible Device	Program Organization Units	Valid Accounts	Spoof Reporting Message	Remote System Discovery	Valid Accounts	Location Identification		Data Destruction	Module Firmware	Loss of Productivity and Revenue
Replication Through Removable Media	Project File Infection		Utilize/Change Operating Mode	Serial Connection Enumeration		Monitor Process State		Denial of Service	Program Download	Loss of Safety
Spearphishing Attachment	Scripting					Point & Tag Identification		Device Restart/Shutdown	Rogue Master Device	Loss of View
Supply Chain Compromise	User Execution					Program Upload		Manipulate I/O Image	Service Stop	Manipulation of Control
Wireless Compromise						Role Identification		Modify Alarm Settings	Spoof Reporting Message	Manipulation of View
						Screen Capture		Modify Control Logic	Unauthorized Command Message	Theft of Operational Information
								Program Download		
								Rootkit		
								System Firmware		
								Utilize/Change Operating Mode		

E) ATT&CK Navigator

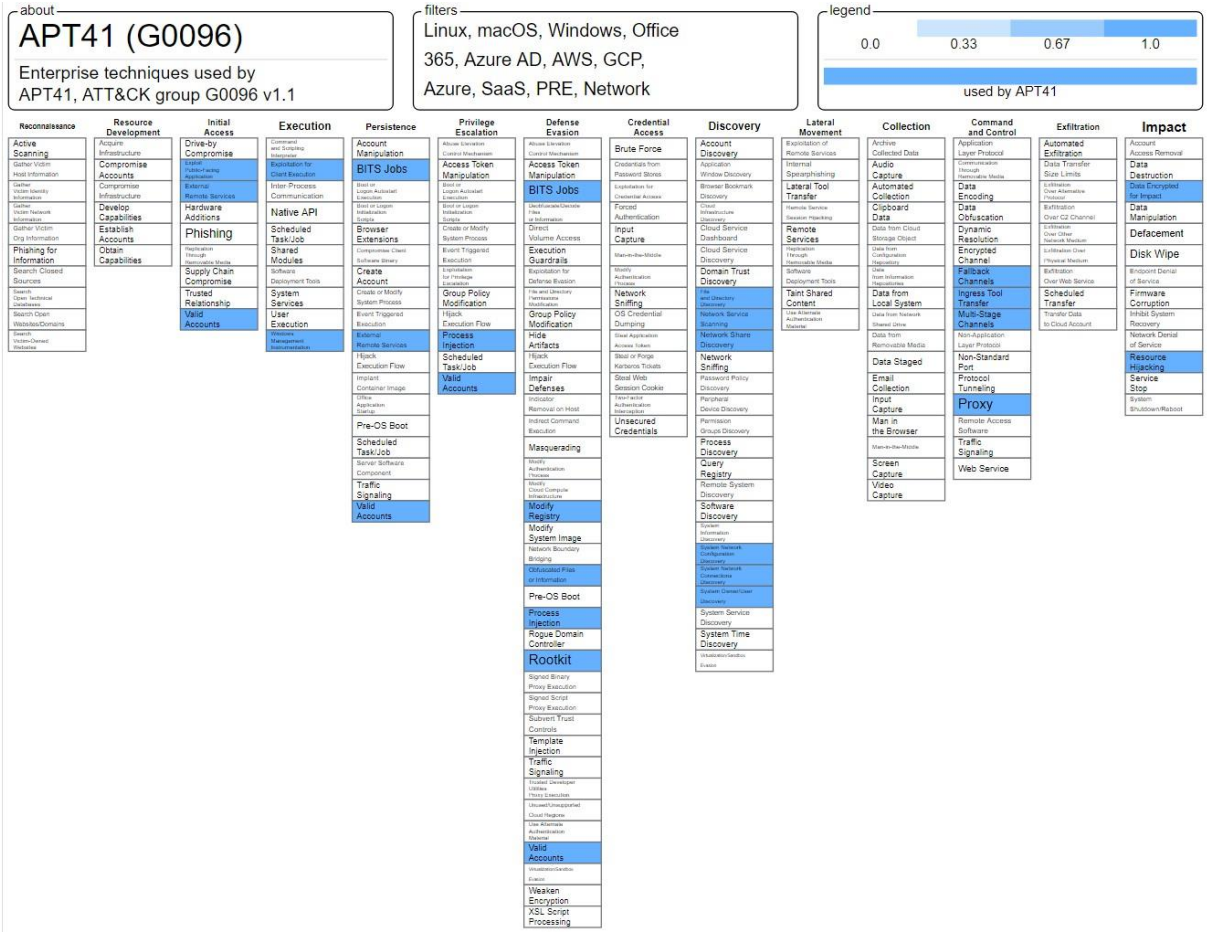
It is the structure that provides the matrix view for all techniques.



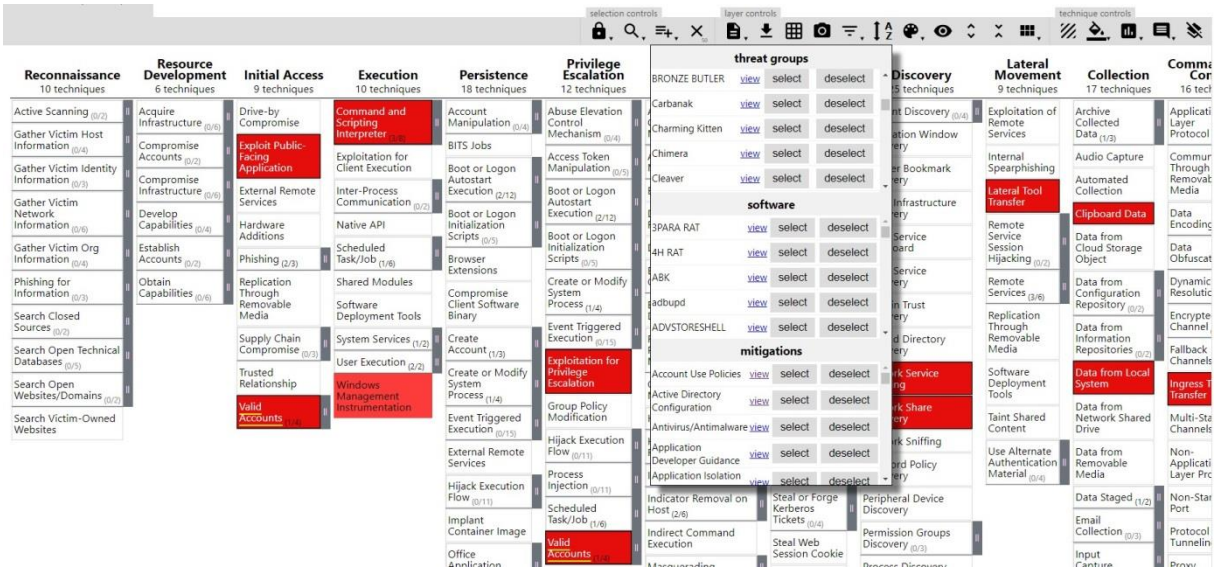
ATT&CK Navigator can be used for visualization of matrices.



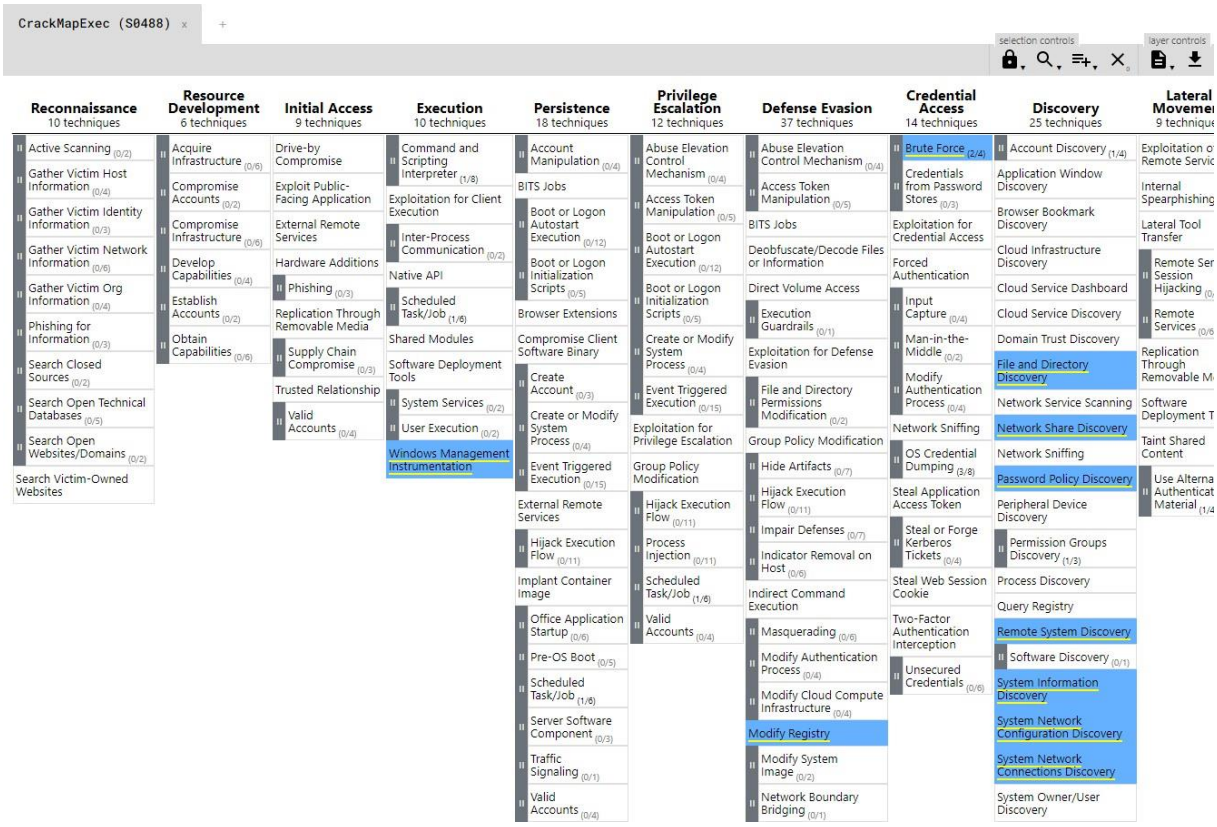
It can also be used to visualize the tactics and techniques used by a group by being directed from the page where the attack groups are located.



By selecting more than one group, the attack tactics and techniques they use can be seen from the interface.



Similarly, it can be used to visualize the tactics and techniques in which a tool is used, by being directed from the page where the tools / software are located.



Data displayed with ATT&CK Navigator can also be downloaded in formats such as JSON, XLSX.

F) Benefits

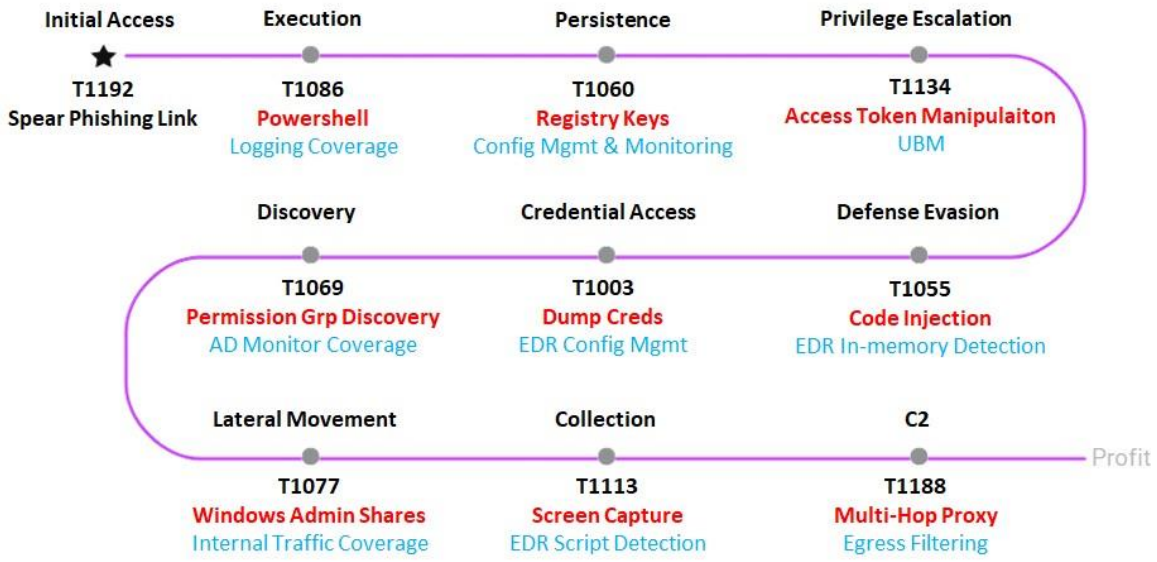
Miter ATT&CK Framework provides a library that includes attacker groups, attack tactics, techniques and precautions. The benefits of this library can be listed as follows:

It provides a source of information for those who will take a new step towards cybersecurity.

It helps security teams in corporate environments to improve their security perspective, especially attack and defense.

With the attacker group profiling, the purpose of the attack can be discovered.

Attack teams (red team members) in corporate environments can test their assets (network, system, user, defense mechanisms…).



Defense teams (blue team members) in corporate environments can understand their offensive behavior and use it as a reference for strengthening their defense systems.

Risk teams in enterprise environments can see threats, prioritize them according to their risks, and as a result, effectively perform threat modeling.

Information security teams in corporate environments can determine the cyber security maturity level of the institution.

It can give an idea for the scope of the benefit it provides in the purchase of purchased products (SIEM products, attack simulation products, exploit tools, …) and helps in product reviews and evaluations.

G) Challenges & Shortcomings

There are many tactics and techniques for different domains on the ATT&CK Framework. However, this framework is not always easy to use. For example,

Some activities such as file deletion (T1070.004) in daily life are also included as an attack technique on ATT&CK Framework.

Some attacks, such as DNS tunneling (T1048), are difficult to detect and require the use of appropriate technologies.

REFERANCES

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

[ii] https://attack.mitre.org/resources/working-with-attack/

[i] https://www.siberportal.org/red-team/cyber-attacks/siber-saldirilarin-evrimi-1986-2017/

[ii] https://www.siberportal.org/blue-team/governance/bilgi-guvenligi-bakis-acisiyla-tehdit-modelleme/

[i] https://medium.com/mitre-attack/attack-with-sub-techniques-is-now-just-attack-8fc20997d8de

[ii] https://medium.com/@ncepki/the-mitre-att-ck-framework-cc85f1c07b58

https://academy.attackiq.com/learn/course/foundations-of-purple-teaming