****

**ANKARA YILDIRIM BEYAZIT UNIVERSITY**

**FACULTY OF MANAGEMENT**

**CYBER KILL CHAIN AND MITRE ATT&CK FRAMEWORK**

**FINAL PROJECT REPORT**

**16030211014 – DERYA SAHA**

**15030461001 – HATİCE ARSLANHAN**

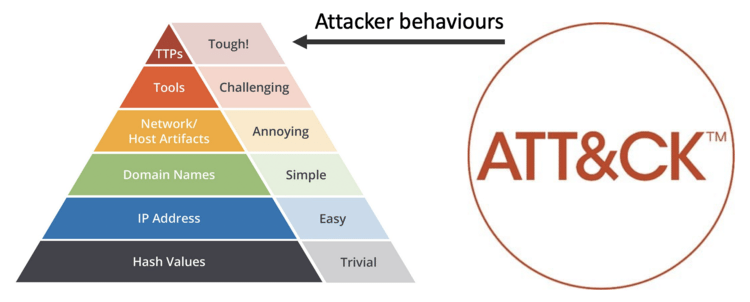
**17030411048 – MEHMET SAİT ALTINTAŞ**

**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?**

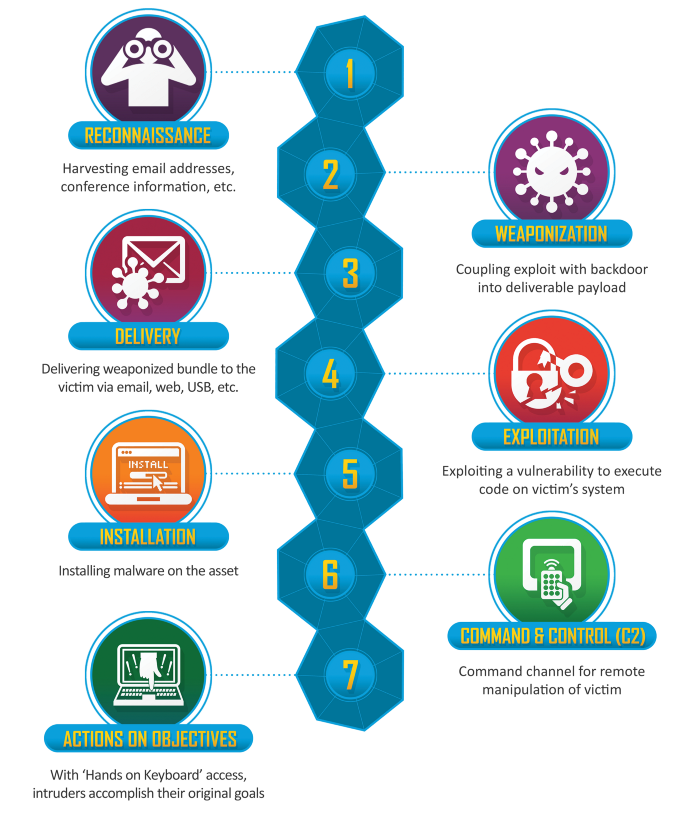
The term “**kill chain**” was first used as a military concept that defines the structure of an attack that covers:

* 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.

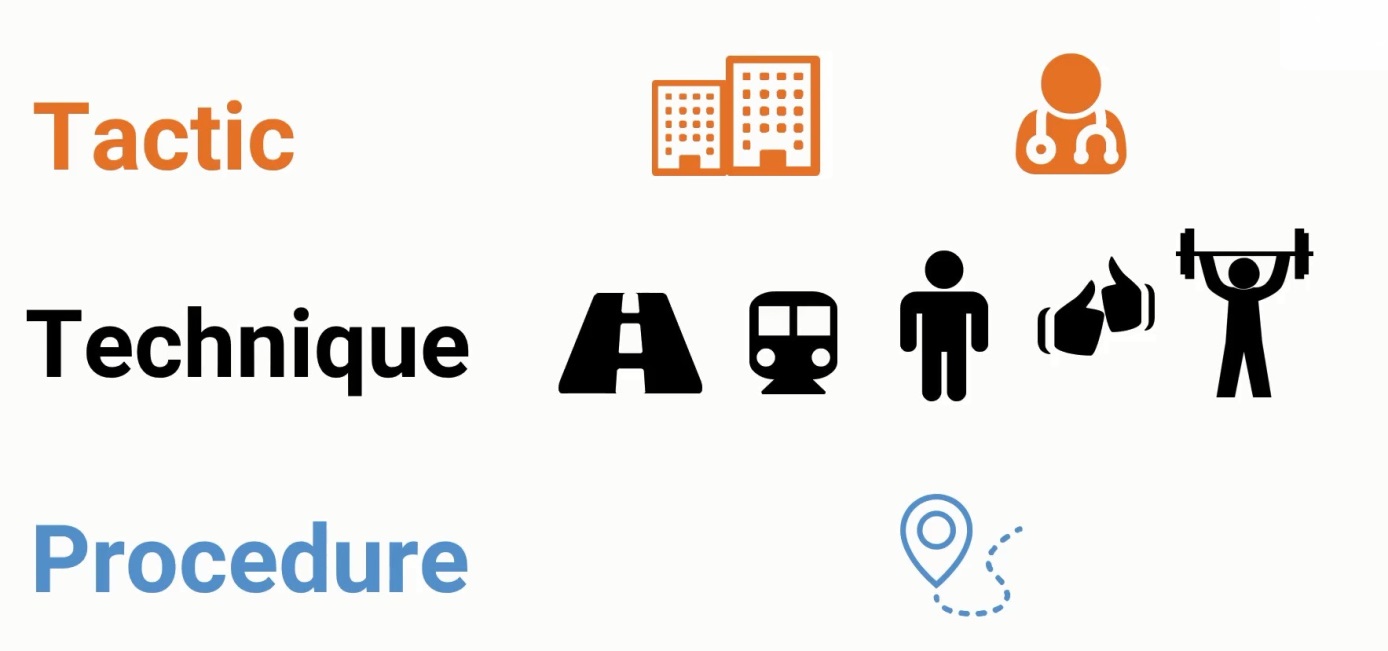
**• Tactics:** The technique used by the attackers is the target. That is, the focus is on the "why" of the attack and "what purpose does the attacker have?" question is answered. Sample; such as first access (TA0001), entitlement upgrade (TA0004),…. Also, there is no order of importance among tactics.

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

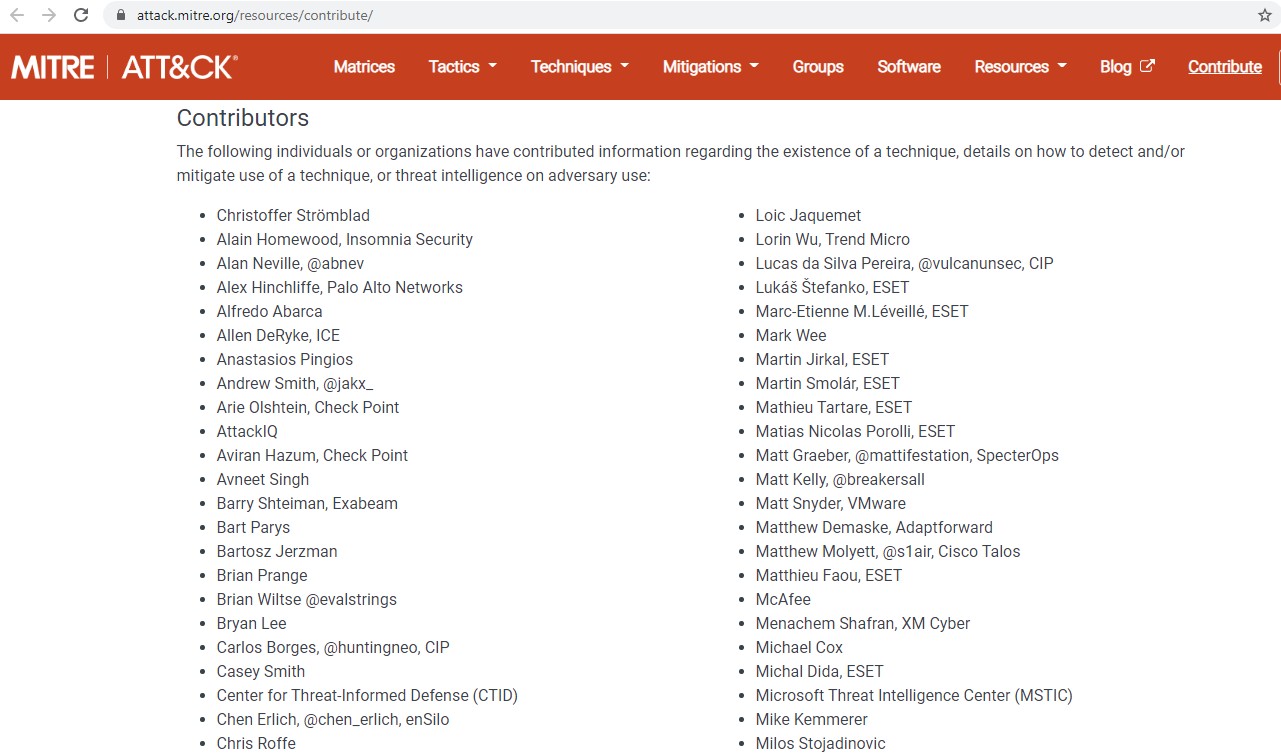
• **Procedures:** It is the specialized application of techniques. Sample; such as downloading and running the powershell file, group APT39 creating scheduled task for persistence….

**• 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.

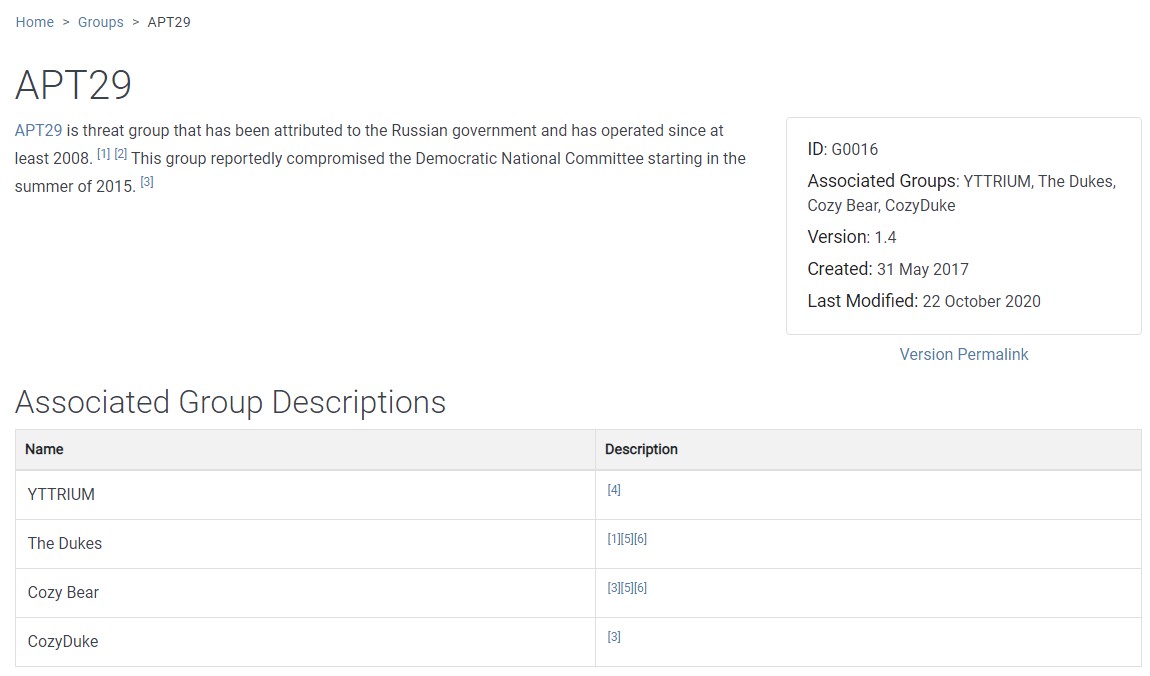
**• Precautions:** These are the precautions that can be taken against attacks. Sample; such as code signing, data backup, antivirus usage…. **Note:** During an attack, the attacker does not use all of these tactics and techniques. He/she can choose a method suitable for the environment and himself/herself.

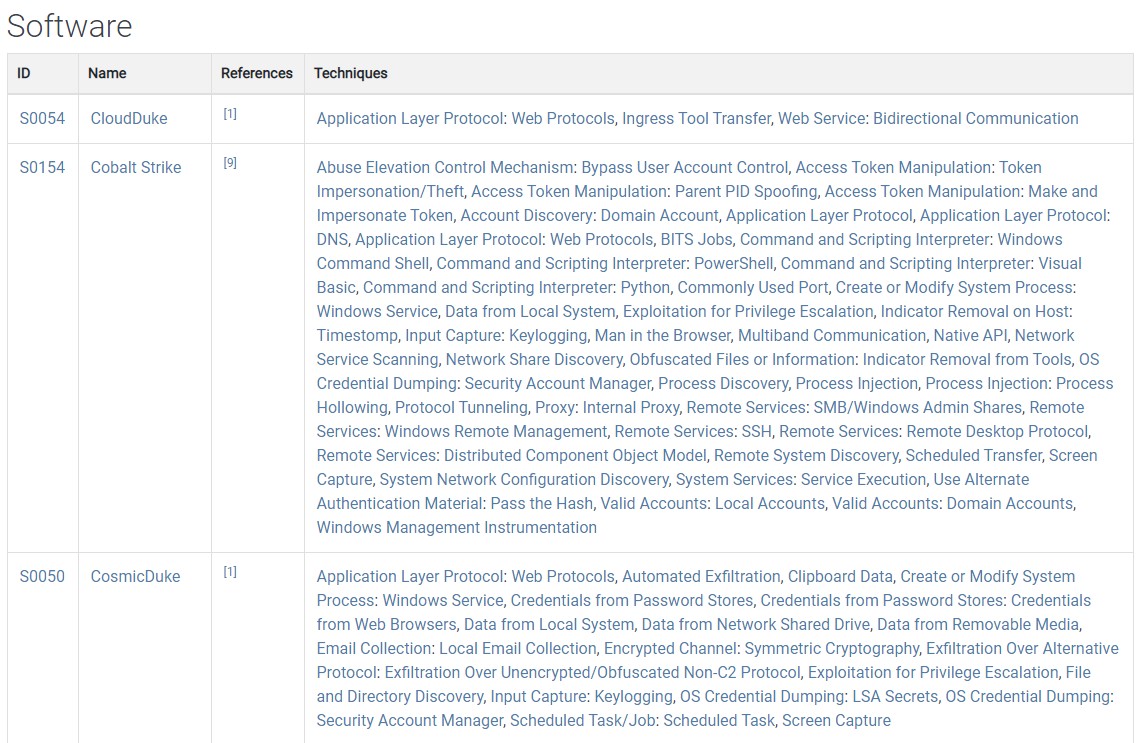
The ATT&CK Framework provides a constantly updated platform. There are many people and institutions that support theseupdates.

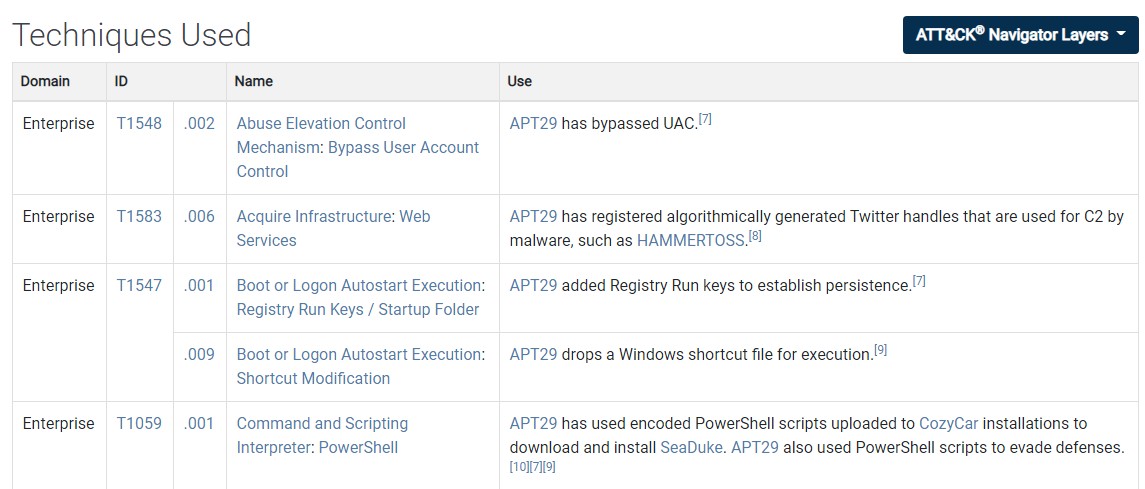


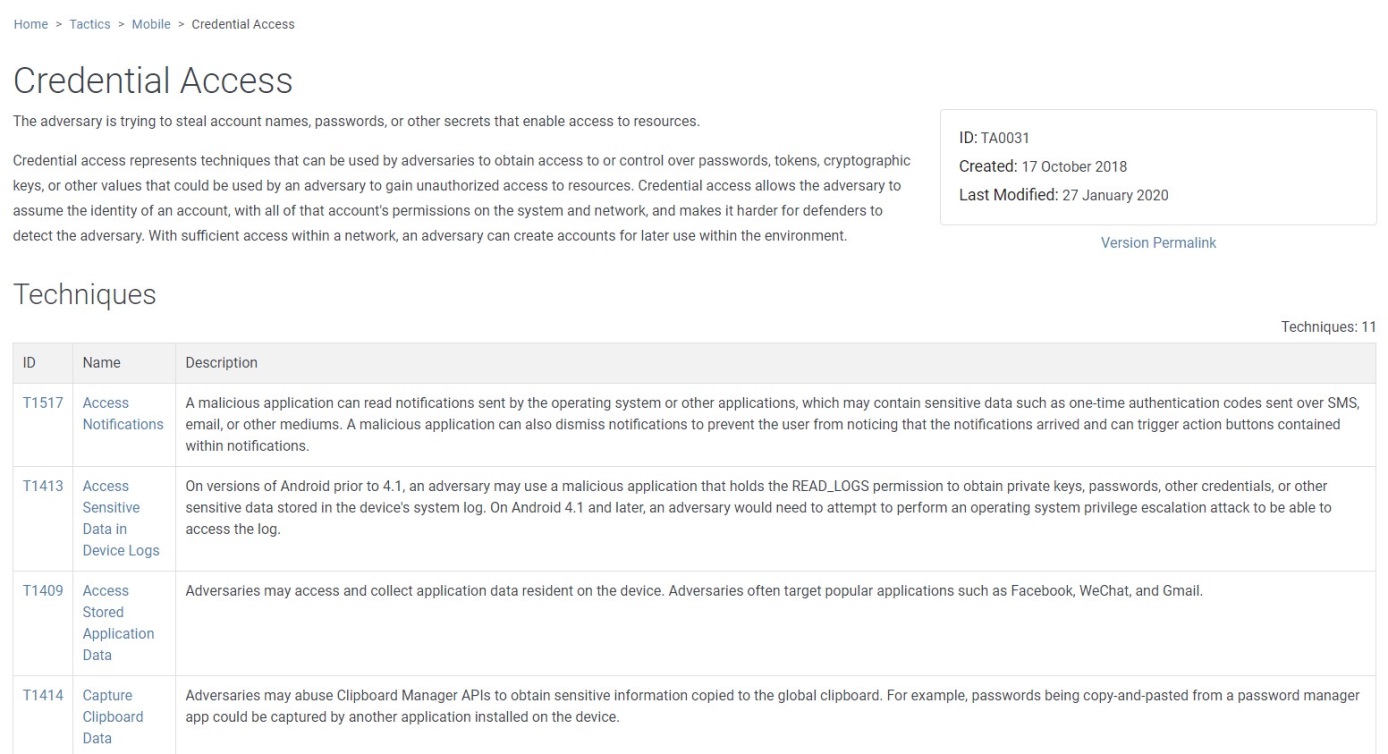
**C) Application**

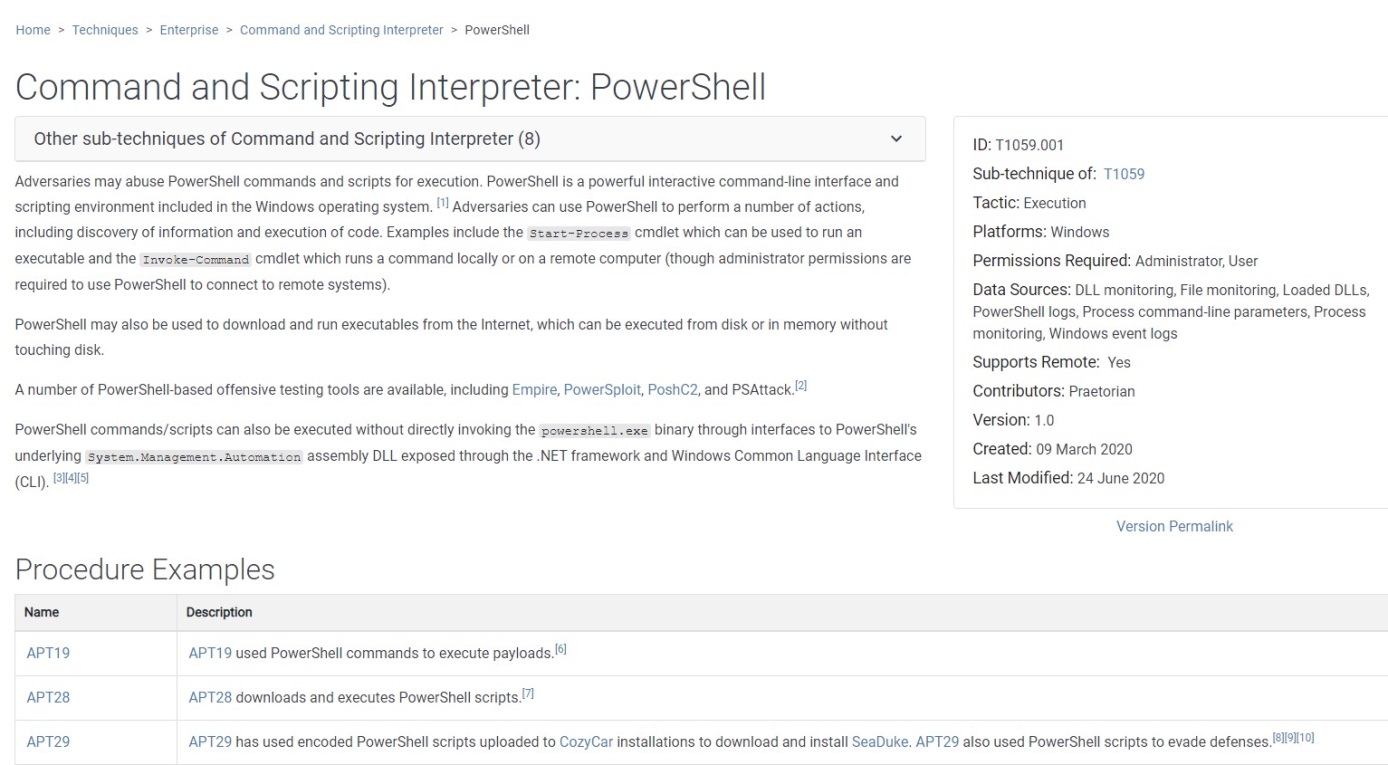
The following information can be obtained with the ATT&CK Framework.

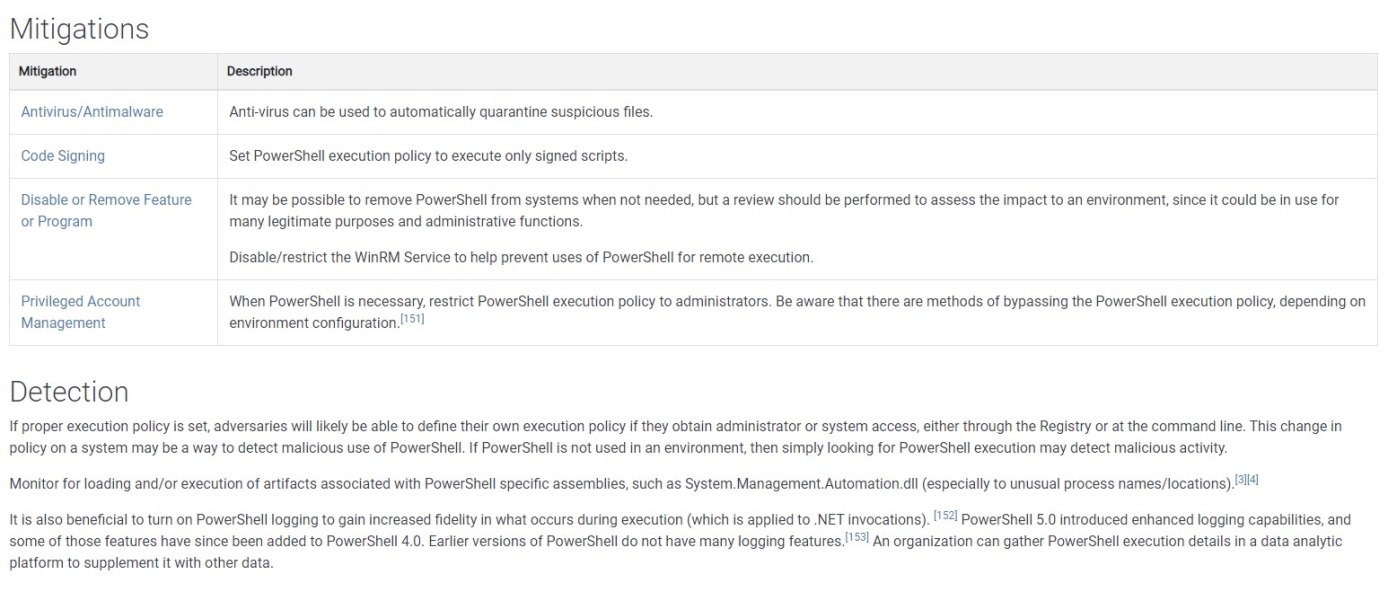
Which country the APT29 group is close to, which groups it is associated with, which sectors they attack, the techniques and software it uses 

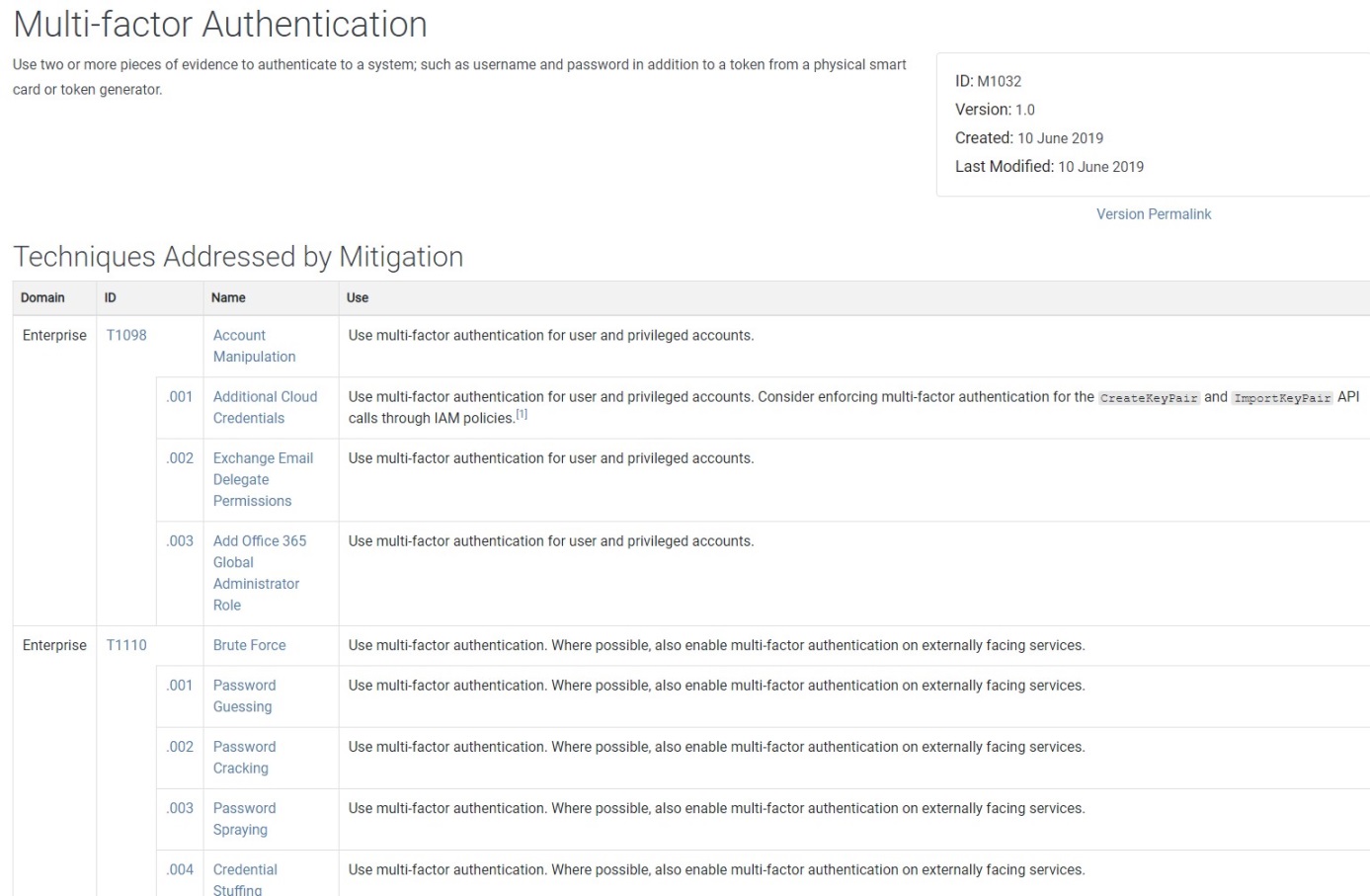




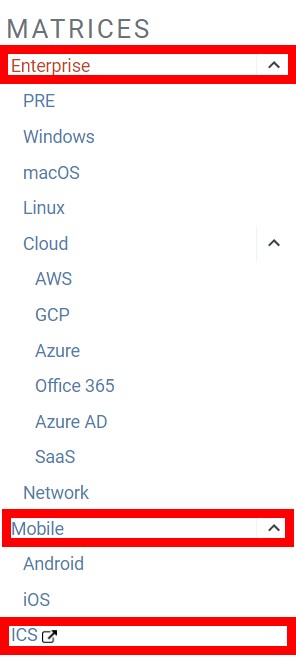
Techniques that can be used for the tactic of stealing identity data from a mobile device .

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 .



Attack techniques that multiple authentication protects.

**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)**

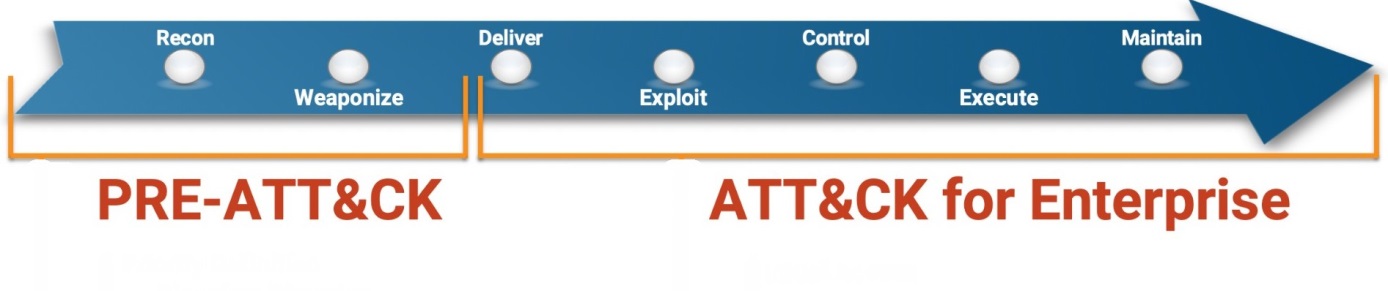
**Impact (Preventing availability of existing system/data)**



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.

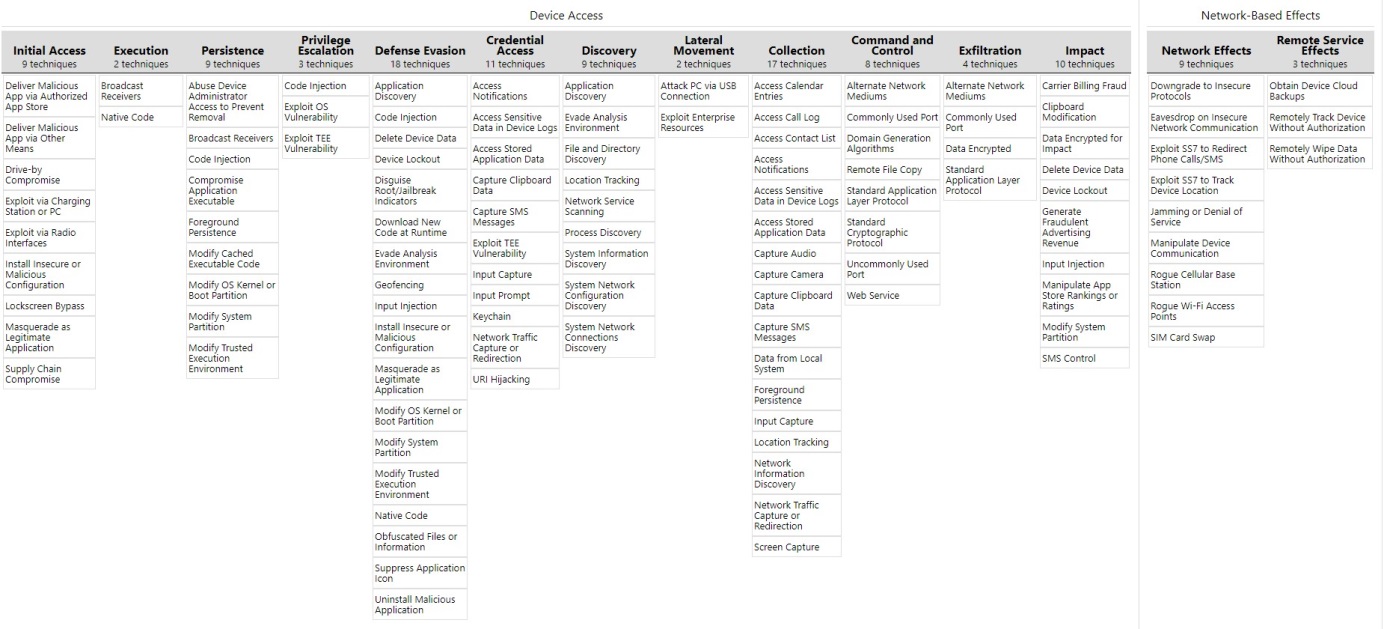


* + **• Windows:** Includes attack tactics and techniques for Windows platforms.
  + **• macOS:** Includes attack tactics and techniques for macOS platforms.
  + **• Linux:** Includes attack tactics and techniques for Linux platforms.
  + **• Cloud:** Includes attack tactics and techniques for cloud-based 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.

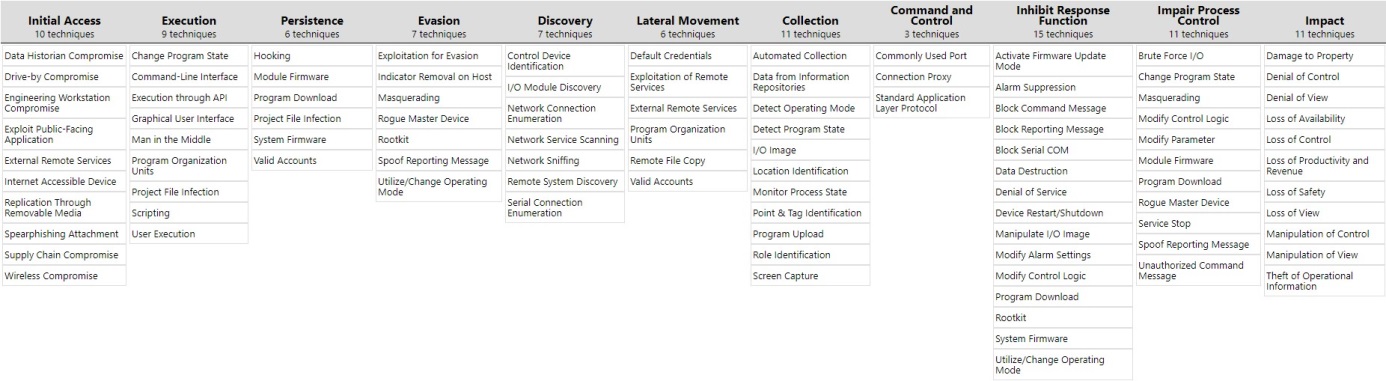
**Network Effects (Monitoring or modifying network traffic)**

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

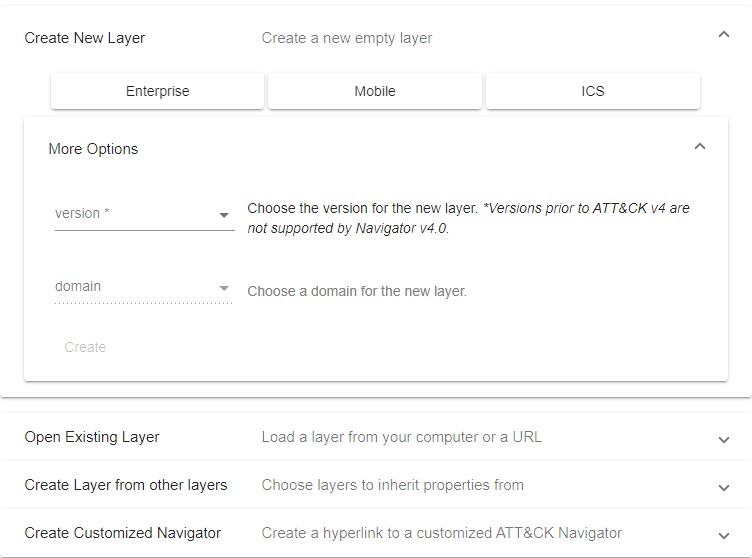
**D.3) ICS ATT&CK**

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

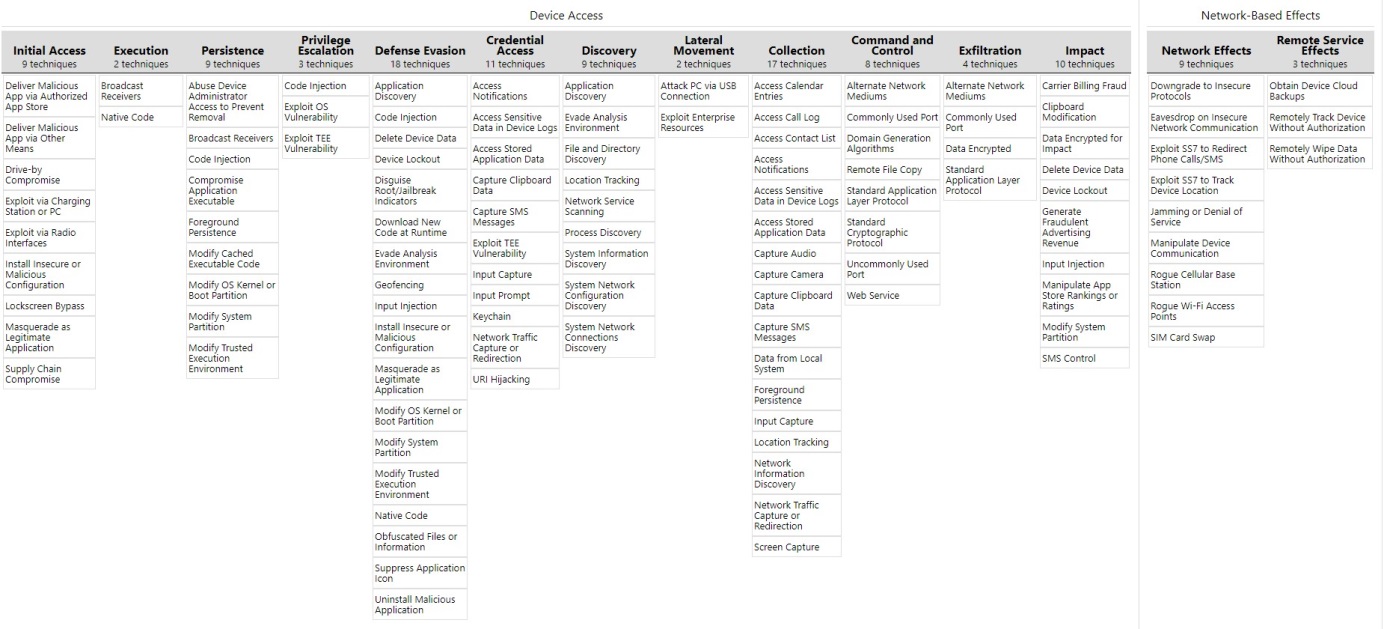
This domain is still under development.



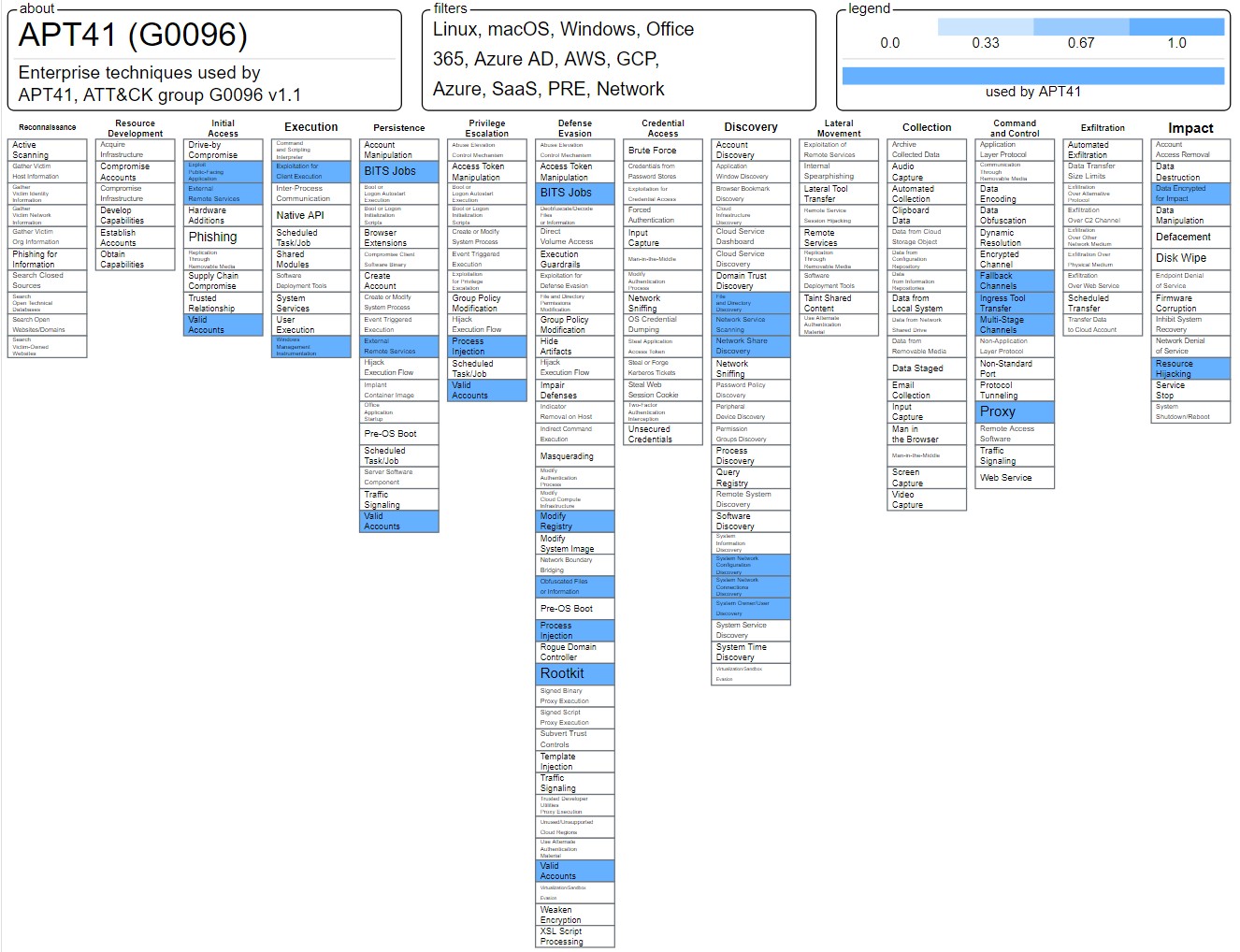
**E) ATT&CK Navigator**

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

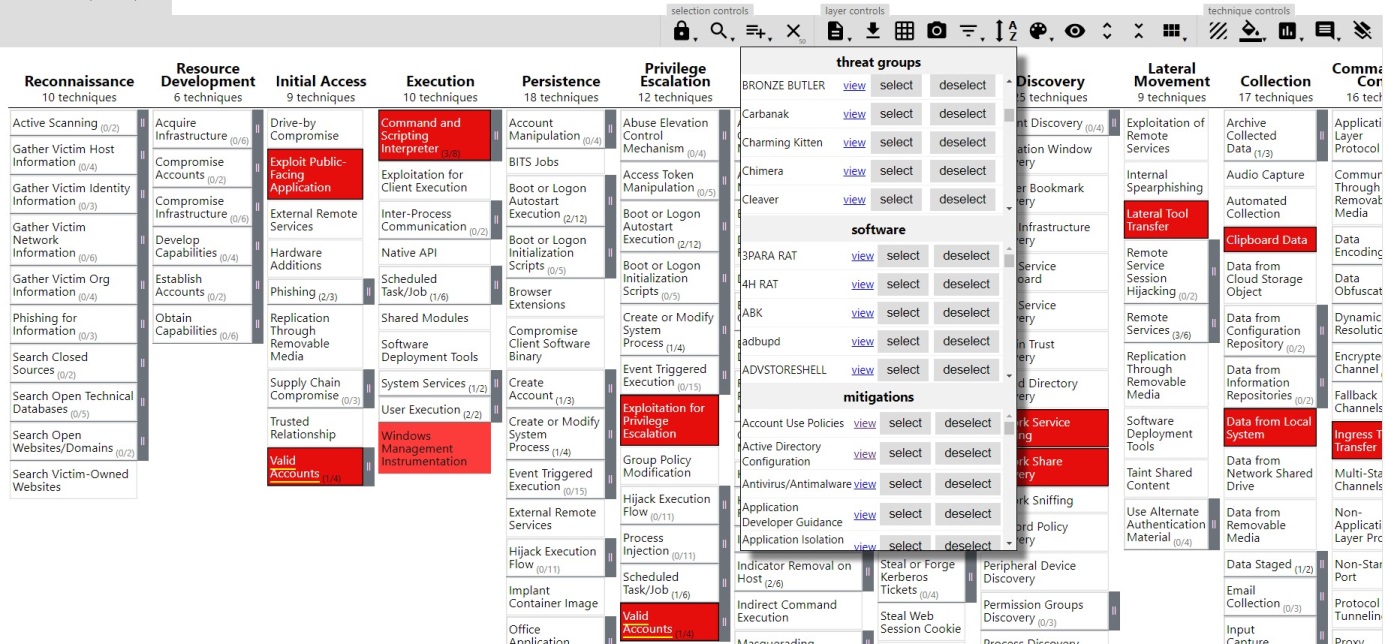
ATT&CK Navigator can be used for visualization of matrices.



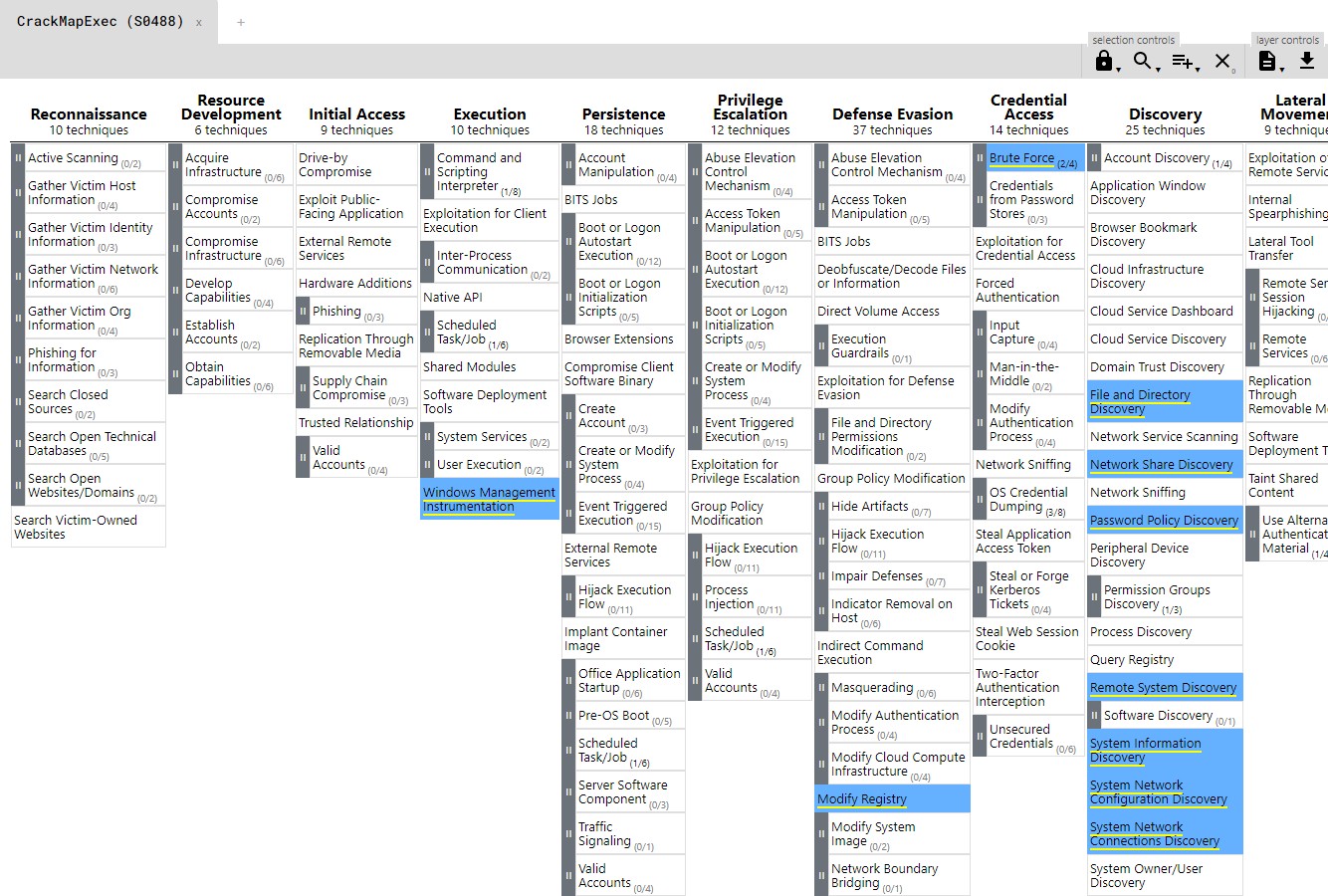
It can also be used to visualize the tactics and techniques used by a group by being directed from the page where the attack groups are located.



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**

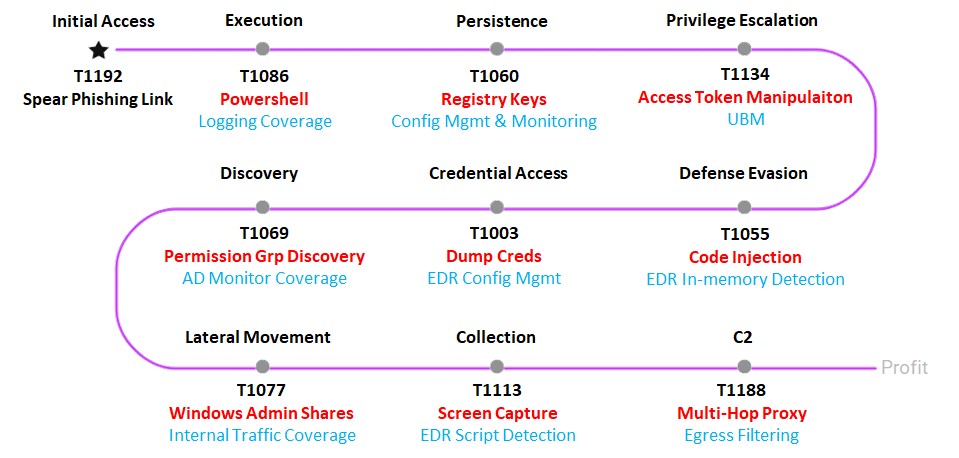
Miter ATT&CK Framework provides a library that includes attacker groups, attack tactics, techniques and precautions. The benefits of this library can be listed as follows:

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