Understanding MITRE ATT&CK Framework

01. Overview

Even now, attacks to threaten cyberspace continue. Cyber attacks such as DDoS and Ransomware are becoming more intelligent and sophisticated, and therefore many people are still exposed to continuous threats.

MITRE, a non-profit research and development organization that originally performed national security-related tasks with support from the U.S. federal government, naturally started researching on that area as the influence of cyber attacks and damage increased among countries. This is the ATT&CK (Attack) Framework.

02. Cyber Kill Chain

1) What is the Cyber Kill Chain?

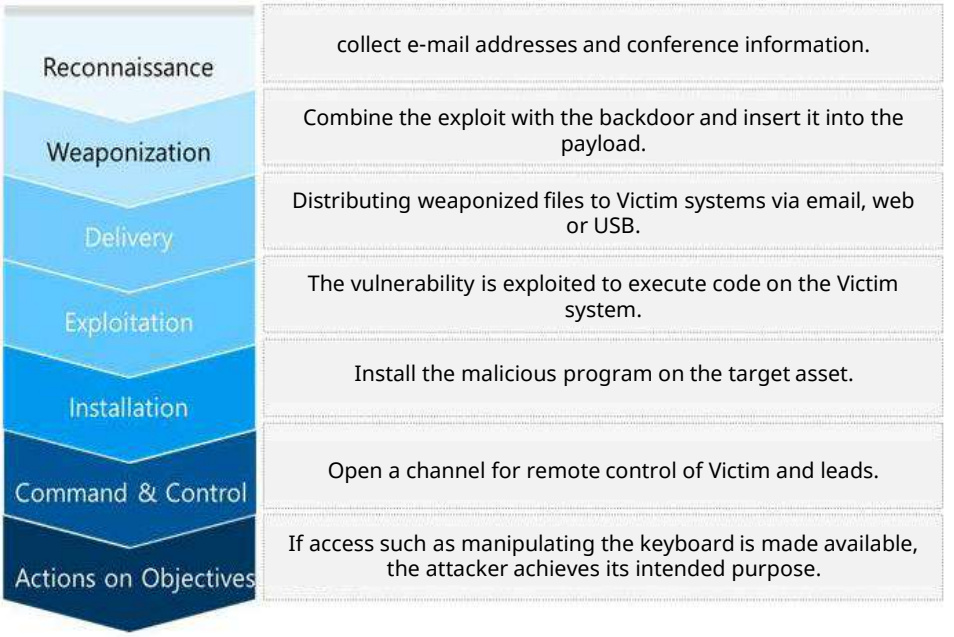
The ATT&CK Framework developed and summarized the stages of the Cyber Kill Chain on the basis of actual attack cases in MITRE, and it is necessary to understand the cyber kill chain first. The cyber kill chain is the most widely known model for analyzing cyber attacks, and it is derived from the existing military term kill chain (strike cycle system). Instead of intercepting the launched missile, it prevents the missile launch itself through a preemptive attack. The concept was brought to cyberspace and applied.

When analyzing various cyber attacks, it usually goes through the following five steps. Since the cyber kill chain is a series of activities to remove threats at each stage and cannot block all attacks, it is important to minimize damage by breaking the chain in advance through attack analysis from the attacker's point of view. This can be considered as the goal of the strategy.

Step 1	Reconnaissance	Penetrate the target infrastructure to secure a base and conduct reconnaissance for a long time
Step 2	Weaponization and delivery	Gather information and gain privileges to achieve attack goals
Step 3	Exploit and installation	Create and install public malware
Step 4	Command and Control, C&C	Execute commands remotely
Step 5	Action and Exfiltration	After information leakage or system destruction, the attacker deletes evidence

2) Lockheed Martin's Cyber Kill Chain

The first use of the term “kill chain” in the cybersecurity field was the US military company Lockheed Martin Corporation. In the method suggested to respond to APT, the process that an attacker must go through when attacking a target is divided into 7 stages: reconnaissance, weaponization, delivery, exploitation, installation, command & control, and action on objectives. It is a defense strategy that detects, blocks, and responds. A cyber attack shows an integrated process that shows the characteristics of a cyber attack that can only achieve its end goal when all steps from the beginning to the end are successful.



3) Limitations of Cyber Kill Chain

The cyber kill chain is a listing of the attacker's actions according to each stage according to the passage of time, and there is a limitation in that there is no link with information about which technologies are used for each stage and related attack tools or hacking groups. In other words, the attacker's actions are not effective in expressing and communicating the link between the tactical attack objective and each action. In addition, since it is a strategy focused on defense against external intruders, there is no strategy for internal security such as an attack by an attacker or an insider. This means that the cyber kill chain requires additional application of new strategies or steps.

03. MITRE ATT&CK Framework

1) What is the MITRE ATT&CK ?

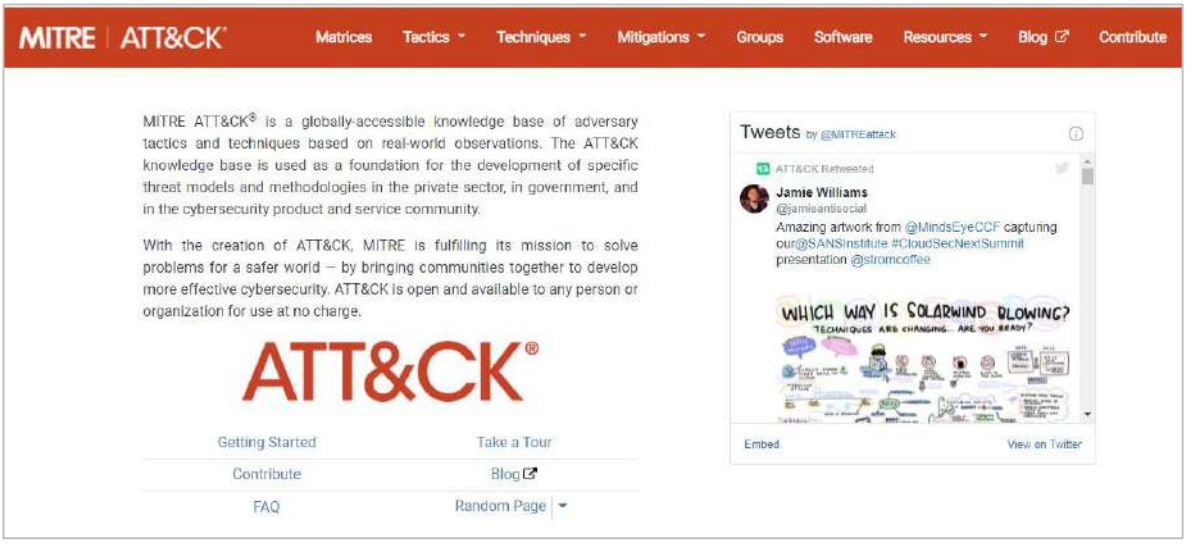
MITRE ATT&CK is a repository of the latest attack technology information of attackers.

MITRE ATT&CK is an abbreviation of Adversarial Tactics, Techniques, and Common Knowledge. After observing actual cyber attack cases, adversary behaviors used by attackers are analyzed from the perspective of Tactics and Techniques to classify information on attack techniques of various attack groups. These are standard data that have been cataloged.

It is a systematization (patterning) of threatening tactics and techniques to improve the detection of intelligent attacks by slightly different from the concept of the traditional cyber kill chain. Originally, ATT&CK was a hacking attack used in the Windows corporate network environment in MITRE. It started with documenting TTPs such as Tactics, Techniques, Procedures, etc., and has since developed into a framework that can identify attacker behavior by mapping TTPs information based on analysis of consistent attack behavior patterns generated by attackers.

First of all, we will visit the website and take a closer look at the information on the MITRE ATT&CK Framework.

✓ MITRE ATT&CK web page : https://attack.mitre.org



2) MITRE ATT&CK Framework

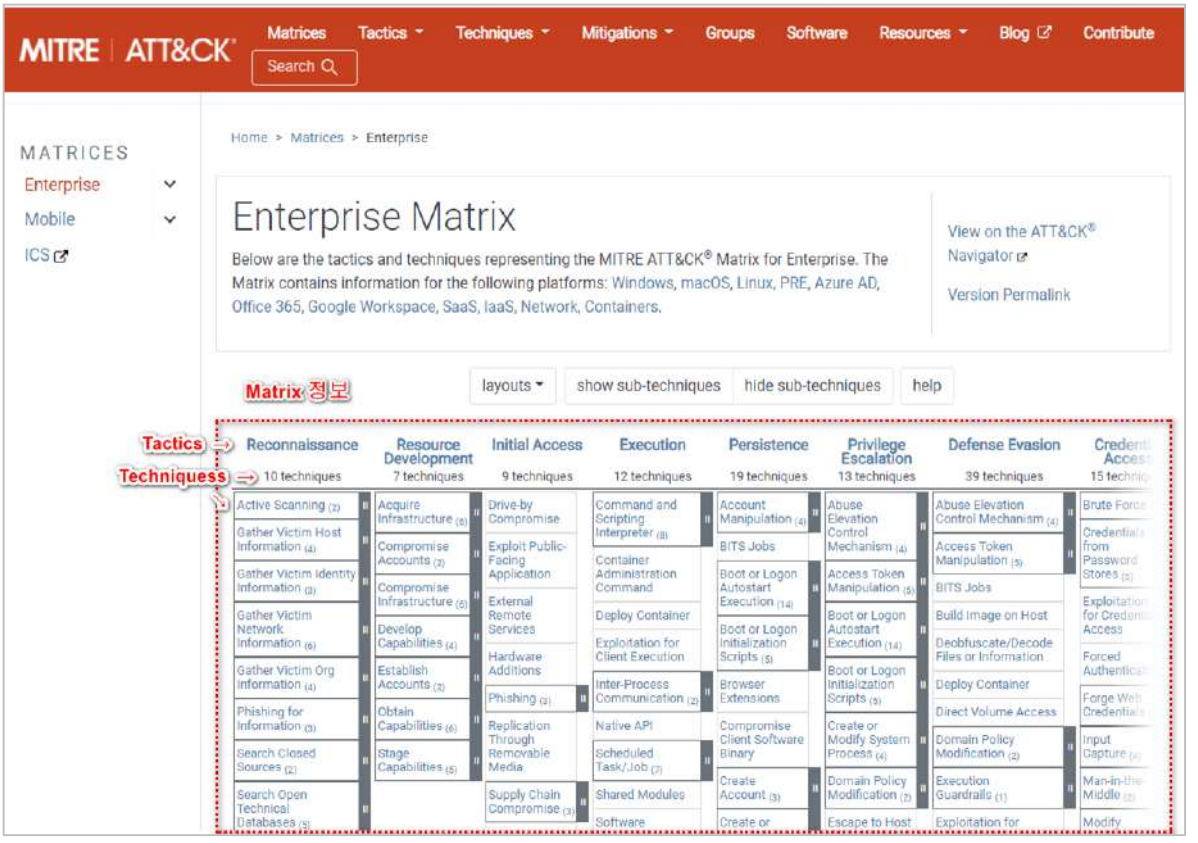
The MITRE ATT&CK website provides information in various categories such as Matrices Mitigations, Groups, and Software, and through this, we can check attack information and countermeasures related to Tactics and Techniques of the system.

✓ **ATT&CK v1 was first announced in January 2018, and ATT&CK v9 was recently updated in April 2021.**

Matrices

- Visualization of the concept and relationship of Tactic, Technique, which is an attack technique
- Tactic includes various Techniques
- Each Tactic is used in various ways depending on the attack target.

✓ MITRE ATT&CK Matrix is provided in **Enterprise, Mobile, ICS versions**



Tactics

- Tactics represent actions according to the attacker's attack target.
- Categorical role for each Techniques according to the situation
- Various classifications such as persistence, information search, execution, and file extraction according to the purpose of the attack

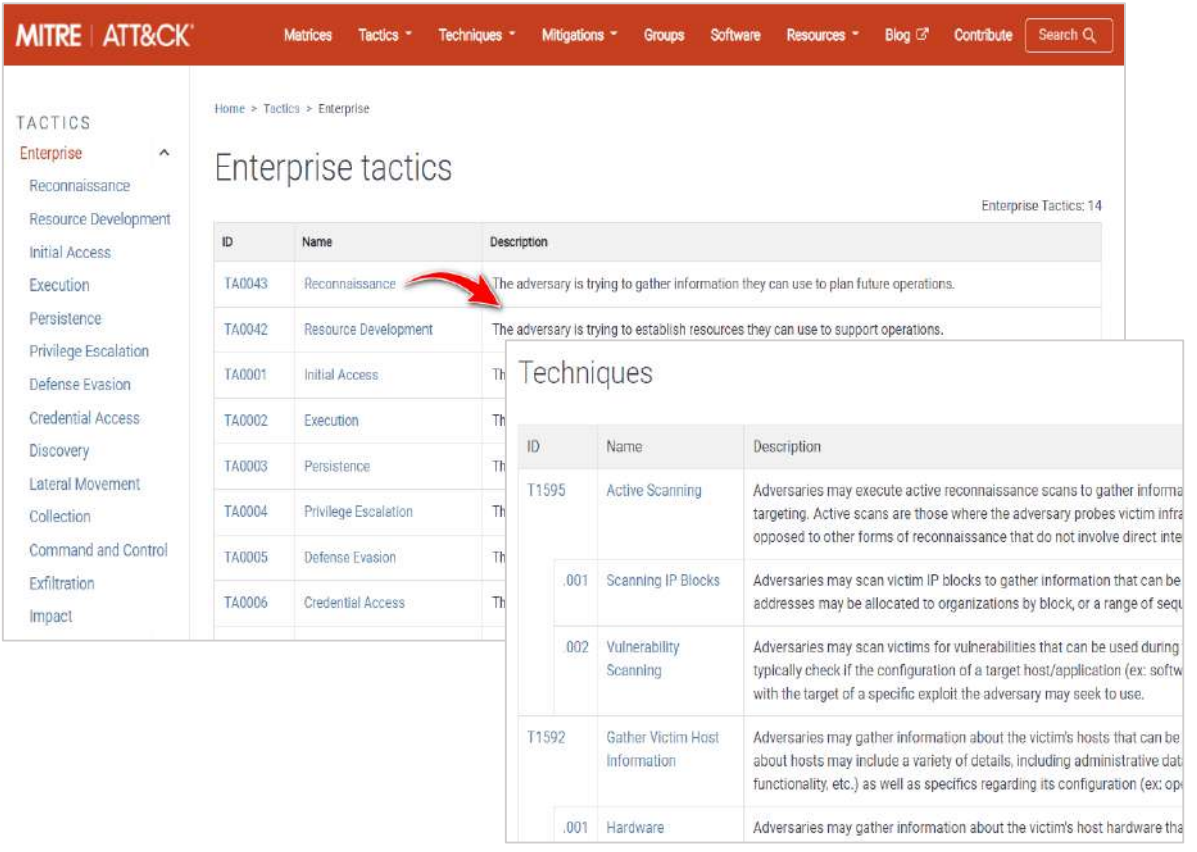
❖ **Provide total 40 Tactics (Enterprise : 14, Mobile : 14, ICS : 12)**

Techniques

- Indicate how an attacker will achieve tactics for a goal
- Specify the result (damage) that occurs through the attacker's attack (Technique)
- Various Techniques may exist according to the previously classified Tactics.

❖ **Provide total 392 Techniques (Enterprise : 185(Sub-Tech : 367), Mobile : 118, ICS : 89)**

✓ The attacker's target tactics are listed, and if we select them, we can check the detailed techniques used in the actual attack



Mitigations

- Techniques that defenders (administrators) can take to prevent and detect attacks
- Acts as a category for multiple Techniques and can be applied redundantly depending on the security purpose and system situation
- Using countermeasure information from similar cases in the past, it is possible to suggest solutions to newly detected attacks

❖ **Provide total 106 Mitigations (Enterprise : 42, Mobile : 13, ICS : 51)**

Mitigations: 42

ID	Name	Description
M1036	Account Use Policies	Configure features related to account use like login attempt lockouts, specific login times, etc.
M1015	Active Directory Configuration	Configure Active Directory to prevent use of certain techniques; use SID Filtering, etc.
M1049	Antivirus/Antimalware	Use signatures or heuristics to detect malicious software.

Groups

- Analyze and organize information on publicly named hacking groups and attack techniques
- Specify and define hacking organizations based on mainly used attack methods, activity analysis, and official documents
- It contains a list of techniques and software used in the attack and maps it to provide the attack types that hacking groups use most → When a new attack occurs, it is possible to utilize and compare the existing matrix
- Another group related to each group is displayed together and the target and characteristics of the attack are explained together → It is possible to guess the hacking group that uses the detected attack or the reason/purpose of the attack, etc.

❖ **Provide total 131 Groups information (Enterprise/Mobile : 122, ICS : 9)**

Groups: 122

ID	Name	Associated Groups	Description
G0018	admin@338		admin@338 is a China-based cyber threat group. It has previously used newsworthy events as lures to deliver malware and has primarily targeted organizations involved in financial, economic, and trade policy, typically using publicly available RATs such as Poisonlvy, as well as some non-public backdoors.
G0130	Ajax Security Team	Operation Woolen-Goldfish, AjaxTM, Rocket Kitten, Flying Kitten, Operation Saffron Rose	Ajax Security Team is a group that has been active since at least 2010 and believed to be operating out of Iran. By 2014 Ajax Security Team transitioned from website defacement operations to malware-based cyber espionage campaigns targeting the US defense industrial base and Iranian users of anti-censorship technologies.
G0099	APT-C-36	Blind Eagle	APT-C-36 is a suspected South America espionage group that has been active since at least 2018. The group mainly targets Colombian government institutions as well as important corporations in the financial sector, petroleum industry, and professional manufacturing.

Software

- The attack code used when the attacker attacks the target, the basic tools included in the operating system (OS), or publicly available tools (Open-Source S/W) are listed and organized
- It is a collectively organized “collection of various tools” used in attacks. It is a collection of the same tools, but it can be used under different names for different hacking organizations, so some of the tools may have different names

*** Provide total 604 software information (Enterprise/Mobile : 585, ICS 19)**

Software: 585

ID	Name	Associated Software	Description
S0066	3PARA RAT		3PARA RAT is a remote access tool (RAT) programmed in C++ that has been used by Putter Panda.
S0065	4H RAT		4H RAT is malware that has been used by Putter Panda since at least 2007.
S0469	ABK		ABK is a downloader that has been used by BRONZE BUTLER since at least 2019.
S0202	adbupd		adbupd is a backdoor used by PLATINUM that is similar to Dipsind.
S0552	AdFind		AdFind is a free command-line query tool that can be used for gathering information from Active Directory.
S0309	Adups		Adups is software that was pre-installed onto Android devices, including those made by BLU Products. The software was reportedly designed to help a Chinese phone manufacturer monitor user behavior, transferring sensitive data to a Chinese server.
S0045	ADVSTORESHELL	AZZY, EVILTOSS, NETUI, Sedreco	ADVSTORESHELL is a spying backdoor that has been used by APT28 from at least 2012 to 2016. It is generally used for long-term espionage and is deployed on targets deemed interesting after a reconnaissance phase.

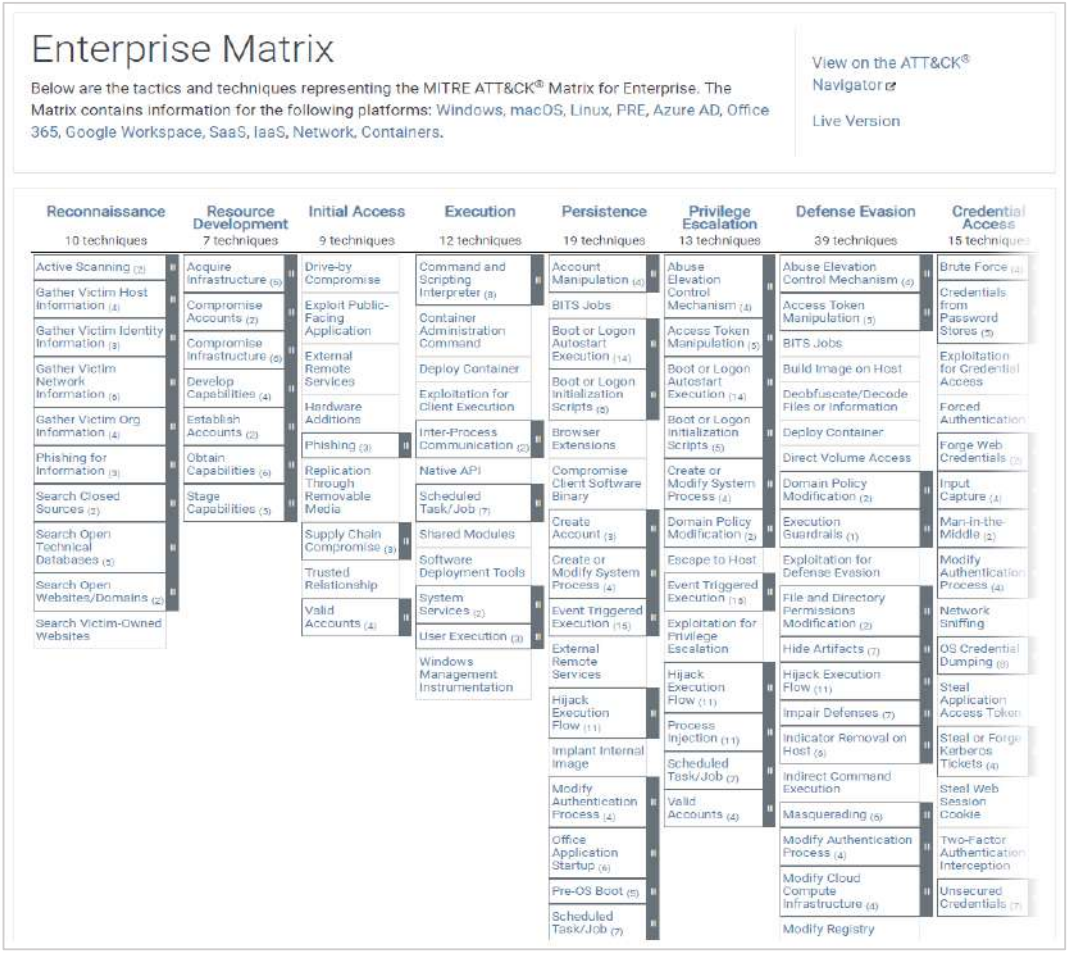
3) Explore the MITRE ATT&CK Matrix

MITRE ATT&CK Matrix is produced in **Enterprise, Mobile, and ICS** versions, and provides information on the attacker's actions in an intuitive **tabular structure (Matrix).** Among them, ATT&CK for Enterprise and ATT&CK for ICS will be examined.

ATT&CK for Enterprise

Enterprise version is a framework created in September 2013 to model corporate system breaches in detail for networks and various OSs and platforms applied to general-purpose corporate environments.

It is a step-by-step reconfiguration of the existing cyber kill chain based on the attacker's TTP and network attack activity characteristics, and can comprehensively evaluate network intrusion defense (CND) technology, processes, and policies.



ATT&CK for Enterprise version provides 14 Tactics, 185 Techniques, and 367 Sub-Techniques (as of April 2021).

- In July 2020, the existing 266 Techniques were merged into 256, and 272 new sub-techniques were added that did not exist before.
- In the case of the existing technology, there was a disadvantage that the scope of the definition was unbalanced because it could be described only with one broad action.
- As a result, the specificity of the threat information within the framework has been improved overall, and when the final result is derived, it is possible to define more detailed attack techniques.

ID	Name	Description
TA0043	Reconnaissance	Exploring to move to other systems in the internal reconnaissance phase
TA0042	Resource Development	Steps to secure an account, etc. with information for moving to another system
TA0001	Initial Access	The purpose of acquiring information about the user environment for network entry
TA0002	Execution	Actions by an attacker to execute malicious code through a local or remote system
TA0003	Persistence	Actions to maintain an attack base and gain continuous access to the system
TA0004	Privilege Escalation	Actions by an attacker to gain elevated privileges on a system or network
TA0005	Defense Evasion	Actions to avoid being detected during the attacker's intrusion time
TA0006	Credential Access	Actions to access or control systems, domain services, credentials, etc.
TA0007	Discovery	Actions to obtain information about systems and internal networks
TA0008	Lateral Movement	Actions to control a remote system on the network after accessing it
TA0009	Collection	Actions for the purpose of an attack or to collect data containing relevant information
TA0011	Command And Control	Actions taken by an attacker to communicate with and control systems inside the target network
TA0010	Exfiltration	Actions by attackers to steal data from the network
TA0040	Impact	Actions intended to compromise the availability and integrity of the attack target

ATT&CK for ICS

The ATT&CK for ICS version contains 12 Tactics and 89 Techniques information (as of April 2021), and for ICS, information is provided through a separate website.

✓ URL : https://collaborate.mitre.org/attackics/index.php/Main_Page

The model applied to the industrial control system (ICS) includes information such as the attack type and process targeting the system that controls and manages the operation of facilities in the related network and industrial production area. It was first published in January 2020 and is currently being continuously updated as a standardized version of Tactics and Techniques of industrial control systems based on papers or actual security incidents of intelligence agencies.

ATT&CK® for Industrial Control Systems

ATT&CK for ICS is a knowledge base useful for describing the actions an adversary may take while operating within an ICS network. The knowledge base can be used to better characterize and describe post-compromise adversary behavior. Please see the overview page for more information about ATT&CK for ICS.

You may start with the following links to become more familiar with ATT&CK for ICS:

- ATT&CK for ICS - Philosophy Paper
- Full list of ATT&CK for ICS techniques
- Software used by ICS threats
- Adversary groups from ICS related incidents
- Assets present in ICS
- Contribute or contact us

The MITRE ATT&CK for ICS Matrix is an overview of the tactics and techniques described in the ATT&CK for ICS knowledge base. It visually aligns individual techniques under the tactics in which they can be applied. Some techniques span more than one tactic because they can be used for different purposes.

Initial Access	Execution	Persistence	Privilege Escalation	Evasion	Discovery	Lateral Movement	Collection	Command and Control	Inhibit Response Function	Impair Process Control	Impact
Data Historian Compromise	Change Operating Mode	Modify Program	Exploitation for Privilege Escalation	Change Operating Mode	Network Connection Enumeration	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	Hooking	Exploitation for Evasion	Network Sniffing	Exploitation of Remote Services	Data from Information Repositories	Connection Proxy	Alarm Suppression	Modify Parameter	Denial of Control
Engineering Workstation Compromise	Execution through API	Project File Infection		Indicator Removal on Host	Remote System Discovery	Lateral Tool Transfer	Detect Operating Mode	Standard Application Layer Protocol	Block Command Message	Module Firmware	Denial of View
Exploit Public-Facing Application	Graphical User Interface	System Firmware		Masquerading	Remote System Information Discovery	Program Download	I/O Image		Block Reporting Message	Spoof Reporting Message	Loss of Availability
Exploitation of Remote Services	Hooking	Valid Accounts		Rootkit	Wireless Sniffing	Remote Services	Man in the Middle		Block Serial COM	Unauthorized Command Message	Loss of Control
External Remote	Modify Controller			Spoof Reporting		Valid Accounts	Monitor Process		Data Destruction		Loss of Productivity

Based on the Purdue Model used in the industrial control system, the area of OT (Operation Technology) was divided into Level 0~2, and assets were classified into systems suitable for each level.

Classification	Description
Level 0 – I/O Network	Consists of sensors and actuators connected to physical equipment and processes
Level 1 – Control	Composed of process detection and control, PLC, RTU, and safety instrumentation/distributed control system
Level 2 – Monitoring/Control LAN	Configuration including monitoring and control, HMI and console, etc.

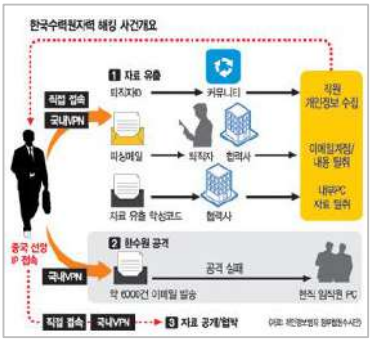
[Table 4-1-2] ATT&CK for ICS Level

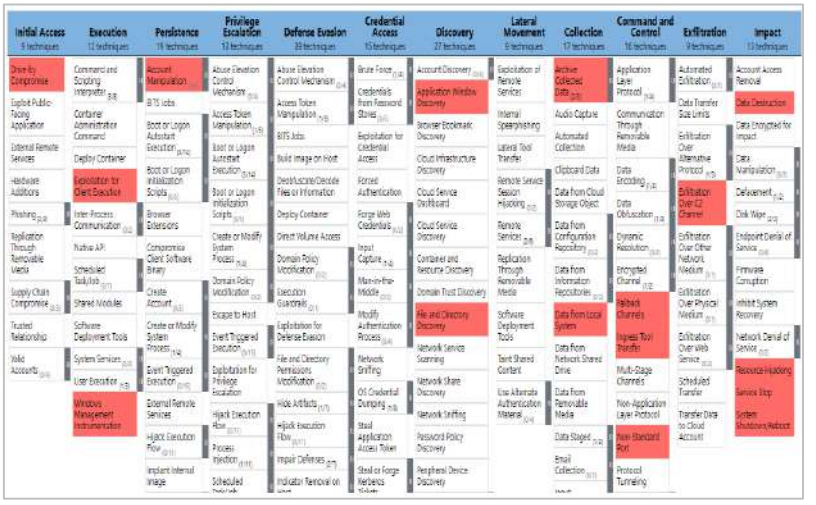
It is composed of threat information focusing on heterogeneous devices and networks (protocol), control systems, sensors, and units. Property and human damage that may occur due to the characteristics of industrial control systems is considered, and it is written focusing on availability. In addition, compared to ATT&CK for Enterprise, the steps related to system control suitable for the industrial control system environment have been added, and the tactics for data leakage, authority, and authentication have been reduced. Techniques aimed at stopping and destroying are included.

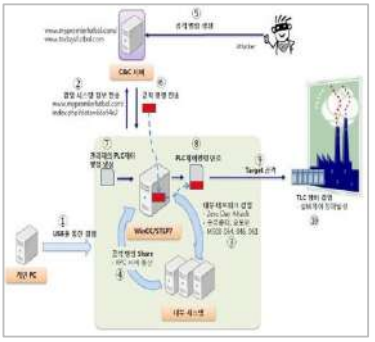
Name	Description
Collection	Tactics for gathering information about target data and systems
Command and Control	Tactics to communicate and control the systems, controllers, and platforms that have invaded and seized the ICS environment
Discovery	Tactics used to access and control the remote system of the ICS
Evasion	Tactics used by an attacker to avoid being detected during the break-in period
Execution	Random execution of malicious code or programs
Impact	Tactics to manipulate data, disrupt and destroy systems against ICS
Impair Process Control	Tactics to disable or compromise physical control procedures
Inhibit Response Function	Tactics to prevent you from responding to safety-related functions
Initial Access	Tactics for accessing the ICS environment
Lateral Movement	Tactics used to access and control ICS' remote systems
Persistence	Tactics for maintaining low-speed connection to the intruded ICS network environment
Privilege Escalation	Tactics to break into the ICS environment and gain high privileges in the system or network

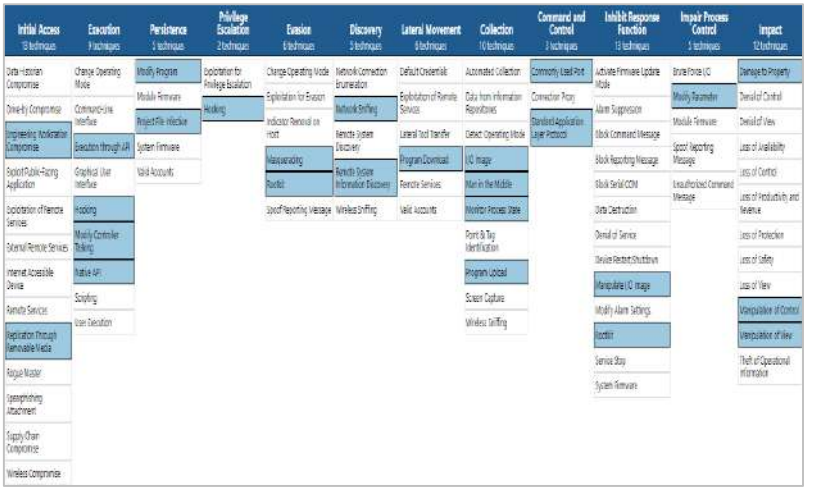
4) MITRE ATT&CK use cases

You can use the MITRE ATT&CK Framework by mapping (substituting) it to specific security events. For example, it is possible to map the incident that attacked the Korea Hydro & Nuclear Power Plant, or the hacking incident of the Iranian nuclear power plant using Stuxnet.





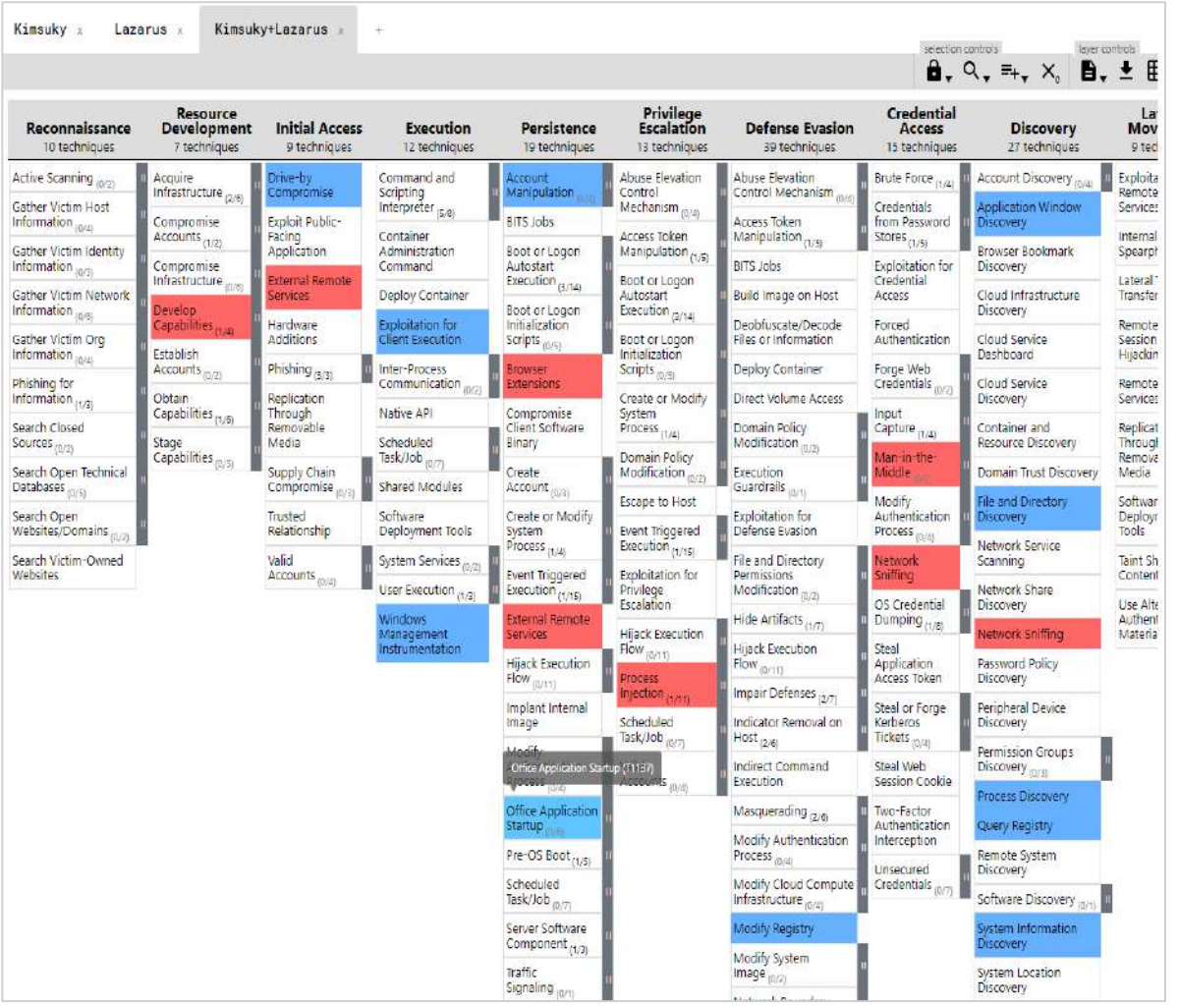




it is possible to visualize and compare in various ways using the Navigator function provided separately on the MITRE ATT&CK website.

✓ ATT&CK® Navigator : https://mitre-attack.github.io/attack-navigator/

The following diagram compares the Tactics and Techniques used by Kimsuky and Lazarus groups, known as North Korean hacking organizations.

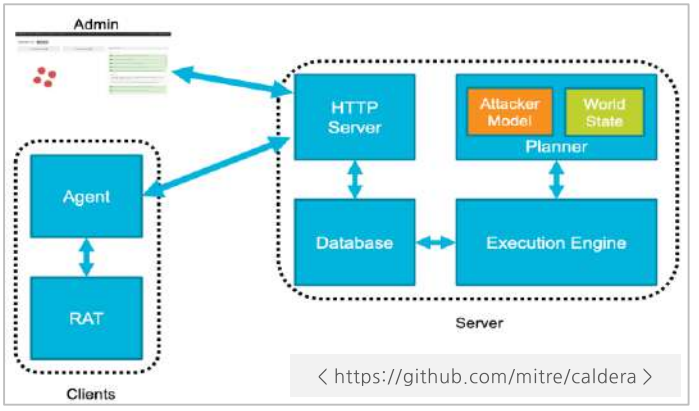


5) MITRE ATT&CK related projects

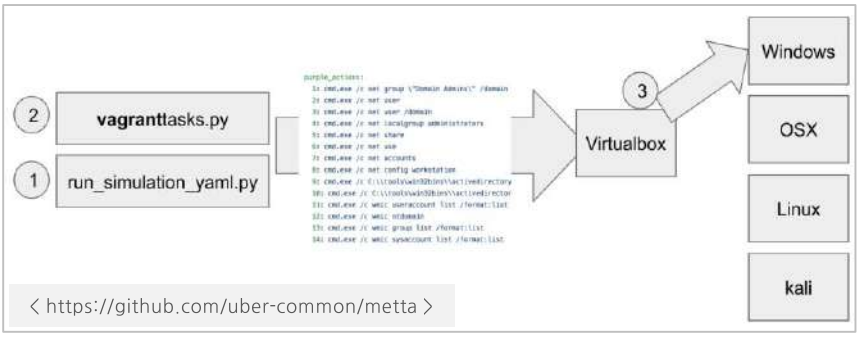
In addition to MITRE's ATT&CK, a number of related projects are in progress, and adversary emulation tools such as CALDERA, METTA, and Atomic Red Team are representative. It aims to derive the current security level and countermeasures with tools (Framework) created to reproduce and test the attack technology of the hacking group, and automatically plan an attack using the information (Tactics, Techniques) of the MITRE ATT&CK Framework. It has been continuously developed to establish and implement methods to carry out attacks.

✓ Gartner defines it as a new security suite called Breach and Attack Simulation (BAS), and various commercial solutions and open source tools are already being developed.

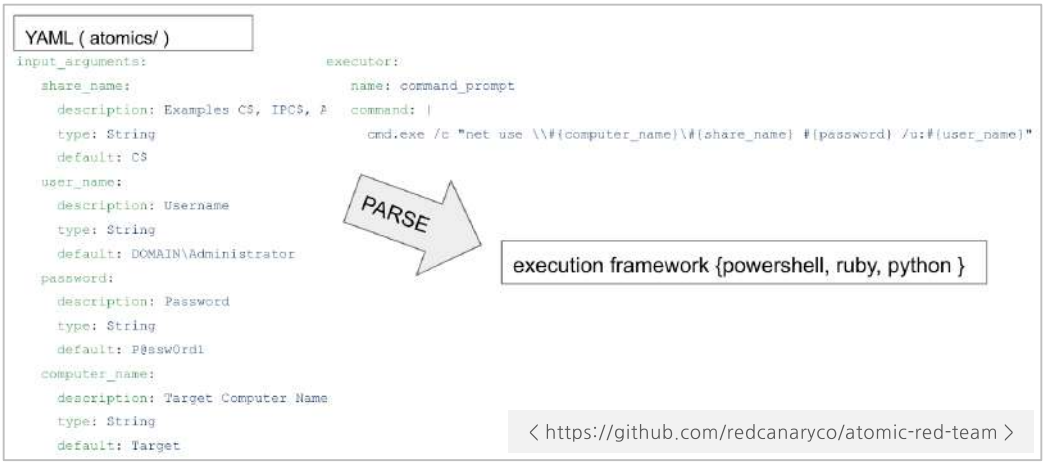
❖ **CALDERA** : Developed by MITRE, it is a project that started in 2016 and can simulate attack behavior through various plug-ins.



❖ **METTA** : It is an open source tool released by the Uber taxi service, which reads the YAML file, configures the necessary virtual machine environment, performs attack actions, and can simulate multiple attack techniques.



❖ **Atomic Red Team** : It is the most actively developed tool, and the attack data is composed based on MITRE ATT&CK, and the attack technique file data is also the most.



04. Conclusion

As security technology develops, defense techniques are also strengthened, and attackers are constantly developing their own attack techniques. Attackers are trying to infiltrate using very covert and various methods, and are incapacitating the existing security system.
In this situation, in order to protect the organization's security and respond to various security threats, it is necessary to understand their attack technology and attack process in advance, and through this, it is necessary to always acquire and reflect the latest technologies.

The MITRE ATT&CK Framework enhances the practicality of the part that was described only as a conceptual stage from the point of view of the flow and process of the attack in the existing model such as the Cyber Kill Chain to TTP, and provides actual attack cases and is applied to the current incident response. It has developed into an easy-to-use model and is an excellent reference material that has taken the information from the existing abstract concepts to the next level into realistic cyber threat information based on real cases.

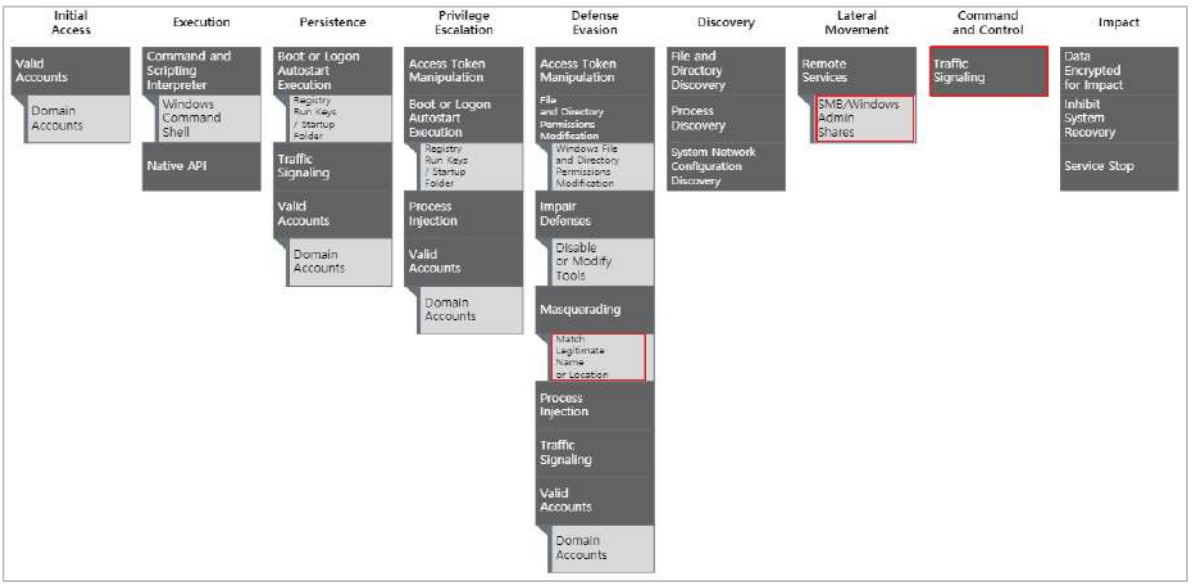
Security officers who defend against cyberattacks should use the information provided by the MITRE ATT&CK Framework to actively detect and respond based on the facts that occurred in real situations to prevent them from launching further attack tactics.

EXAMPLES

1) Ryuk

Classification	Contents
Country	U.S, England, Canada
Business	Energy, Medical, Government, etc.
Additional Info.	- Attempts to spread using phishing and spear-phishing - File encryption possible using remote encryption and Wake-On-LAN function - Using DaaS (Download as a Service), hackers with deployment skills can perform proxy attacks - Download Ryuk and tools used for attack using BazarLoader and BazarBackdoor

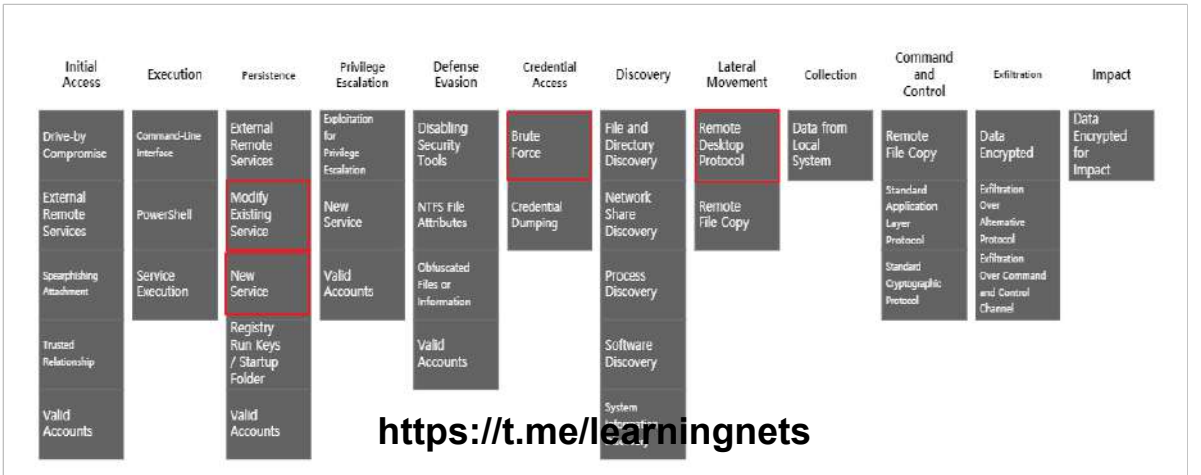
- MITRE ATT&CK Matrix (v9)



2) Maze (ChaCha)

Country	U.S., England, Canada, France, Swiss, etc.
Business	Finance, Transportation, Logistics, Energy, Medical, Government, etc.
Additional Info.	- At the end of 2020, an attempt to encrypt files using VirtualBox images on infected targets to bypass antivirus detection - Use Cobalt Strike, Mimikatz, PowerSploit, ProcDump and other tools to aid infiltration - Leaking the stolen data to a site that can only be accessed from the Tor browser and demanding ransom through threats - In November 2020, the Maze ransomware developer officially declared the end of the project on their site

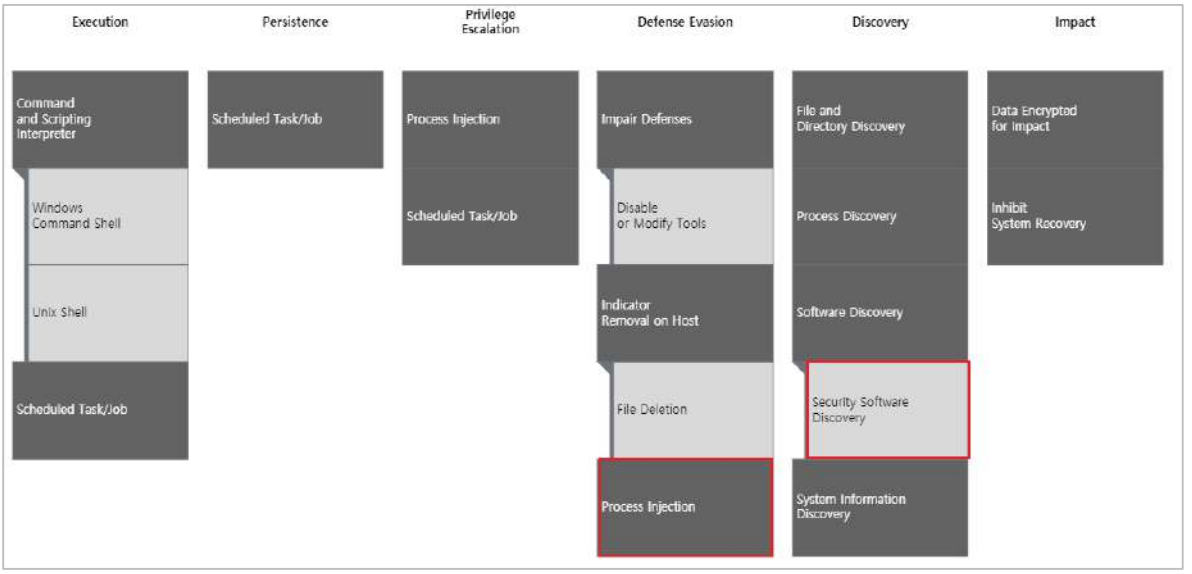
- MITRE ATT&CK Matrix (v6)



3) Defray777 (RansomEXX, Target777)

Classification	Contents
Country	U.S., England, Canada, Australia, Japan, France, Brazil, etc.
Business	Medical, Education, Government, Energy, etc.
Additional Info.	- Use of Vatet loader, PyXie RAT, and Cobalt Strike and other tools to aid penetration - Can run independently on Windows and Linux, and can run on VMWare ESXI servers that can run ELF binaries

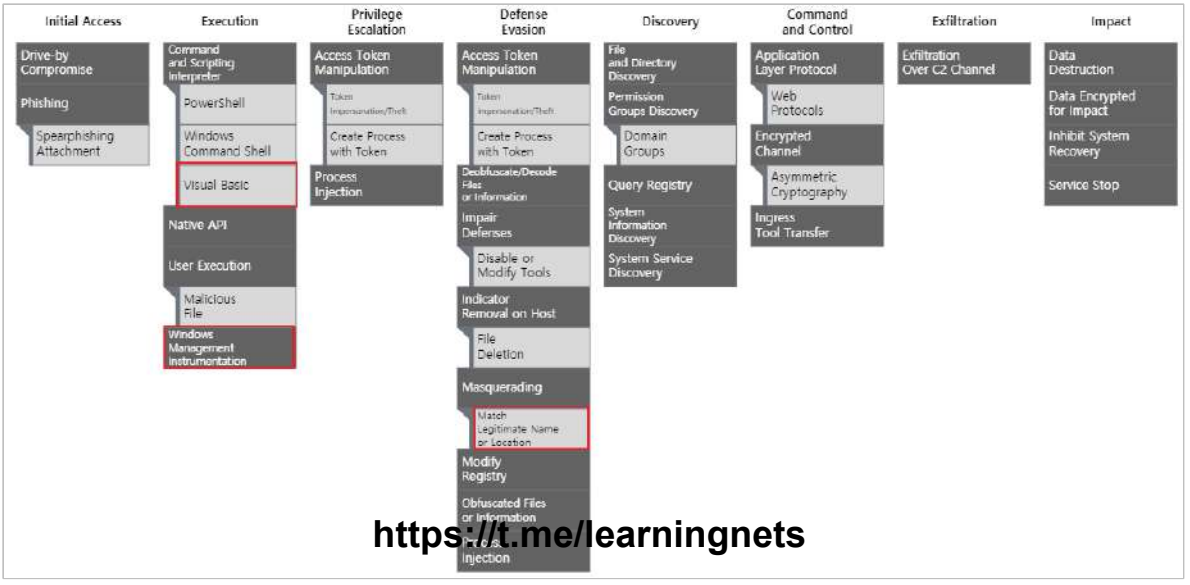
- MITRE ATT&CK Matrix (v7)



4) GandCrab + REvil (Sodinokibi)

Country	U.S., Australia, Canada, Hongkong, etc.
Business	Media, Energy, Laws, Manufacture, Construction, etc.
Additional Info.	- Attack attempt using drive-by download technique - Attack attempts mainly using Rig and Grandsoft Exploit tools - Ransomware does not work when using Russian layout after checking keyboard layout - In the case of GandCrab, additional development was announced in May 2019 - In April 2019, Revil (Sodinokibi) ransomware was discovered and found many similarities to GandCrab ransomware

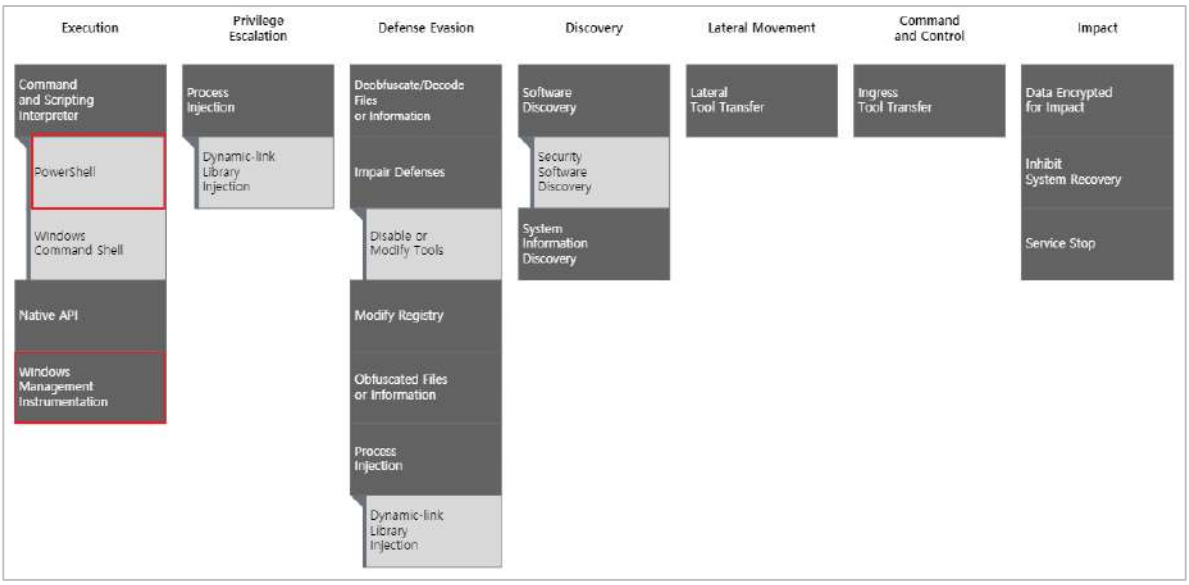
- MITRE ATT&CK Matrix (v9)



5) NetWalker (Mailto)

Classification	Contents
Country	U.S., Canada, France, Germany, Australia, etc.
Business	Government, Medical, Manufacture, Logistics, Energy, etc.
Additional Info.	- Attempts to spread using phishing and spear-phishing - Unauthorized access attempts using externally exposed vulnerabilities or vulnerable RDP services - Fileless attack technique using VBScript and Powershell - Salsa20 encryption, using Reflective DLL Loading technique

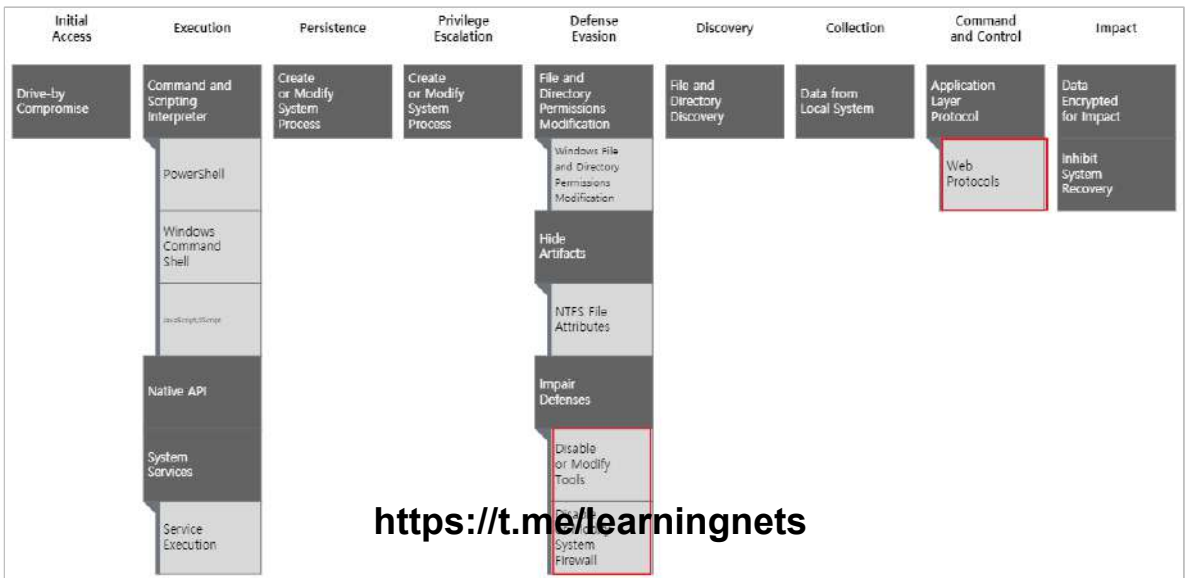
- MITRE ATT&CK Matrix (v7)



6) WasteLocker

Country	U.S., England, etc.
Business	Pharmaceuticals, Transportation, Logistics, Medical, Government, etc.
Additional Info.	- Perform APT attacks targeting specific companies - File server, database service, virtual machine and cloud environment are the main goals - Part of the attack method is phishing attempts using fake browser updates - The attack tool used for this phishing is SocGholish, a JavaScript-based attack framework.

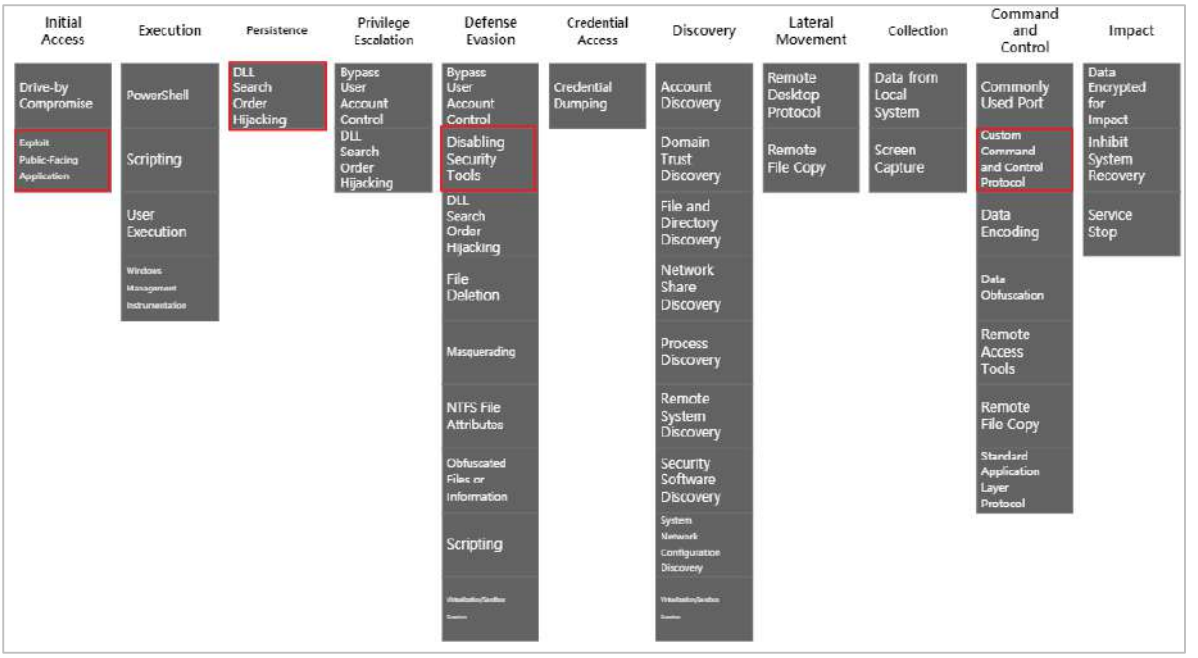
- MITRE ATT&CK Matrix (v9)



7) DoppelPaymer (BitPaymer)

Classification	Contents
Country	U.S., Mexico, Canada, Italy, Norway, Germany, etc.
Business	Government, Logistics, Finance, Transportation, Medical, etc.
Additional Info.	- Attempts to spread fake updates using phishing and spear-phishing - Download DoppelPaymer and tools used for attack using Emotet, Dridex - Use of Cobalt Strike, Mimikatz, PSExec and other tools to aid infiltration - Change the password of the current user account before rebooting into safe mode

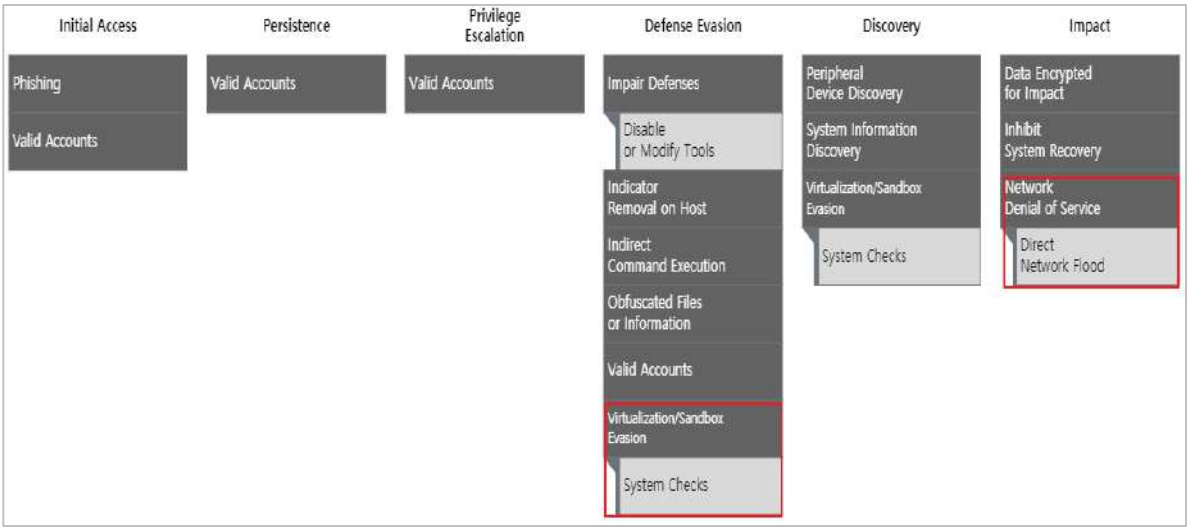
- MITRE ATT&CK Matrix (v6)



8) Avaddon

Classification	Contents
Country	Australia, Brazil, China, Germany, Indonesia, Spain, England, France, India, Italy, U.S., etc.
Business	Manufacture, Energy, Aviation, Medical, Marketing, Distribution, Finance, Government, etc.
Additional Info.	- Phishing, spear-phishing, and attempts to spread by exploiting vulnerabilities - Attached files mainly use compressed files containing JavaScript (.js) files. - Unauthorized access attempts using externally exposed vulnerabilities or vulnerable RDP services - For users of certain languages (Russia, Tatar, Ukraine, Yakut), exit without file encryption - Using a triple threat strategy that combines file encryption + confidentiality leak threat + DDoS attack

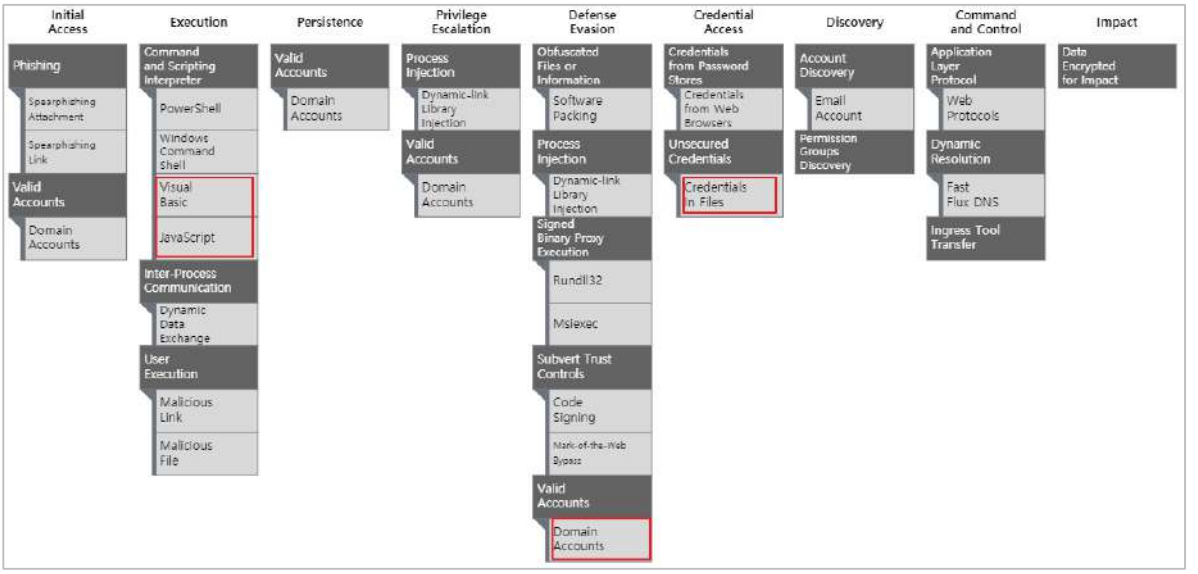
- MITRE ATT&CK Matrix (v7)



9) Clop

Classification	Contents
Country	Swiss, England, U.S., Netherlands, Croatia, etc.
Business	Government, Finance, Manufacture, Distribution, Education, etc.
Additional Info.	- Attempts to spread spear-phishing and exploit vulnerabilities - Attach documents, HTML, LNK files containing malicious macro code or Excel 4.0 macros - Use of Cobalt Strike, Mimikatz, FlawedAmmyy and other tools to aid penetration - Check AD (Active Directory) environment and install Beacon if it is correct - Distribute and run ransomware after registering itself as a service

- MITRE ATT&CK Matrix (v9)



10) Zeppelin (Buran / VegaLocker)

Classification	Contents
Country	U.S., Canada, Bulgaria, Japan, Korea, France, Taiwan, etc.
Business	Real estate, Manufacture, Health, Medical, Tech., etc.
Additional Info.	- Phishing, spear-phishing, and attempts to spread by exploiting vulnerabilities - Check the country code and exit without file encryption if it is a specific country (Russia, Ukraine, Belarus, Kazakhstan) - When running for the first time, file encryption is executed after waiting for about 26 seconds to bypass the vaccine and sandbox - Utilize Rex3Packer, a Packer-as-a-service (PaaS) to use Cobalt Strike and its own framework

- MITRE ATT&CK Matrix (v6)