Cyber Kill Chain

2021. 11. 11

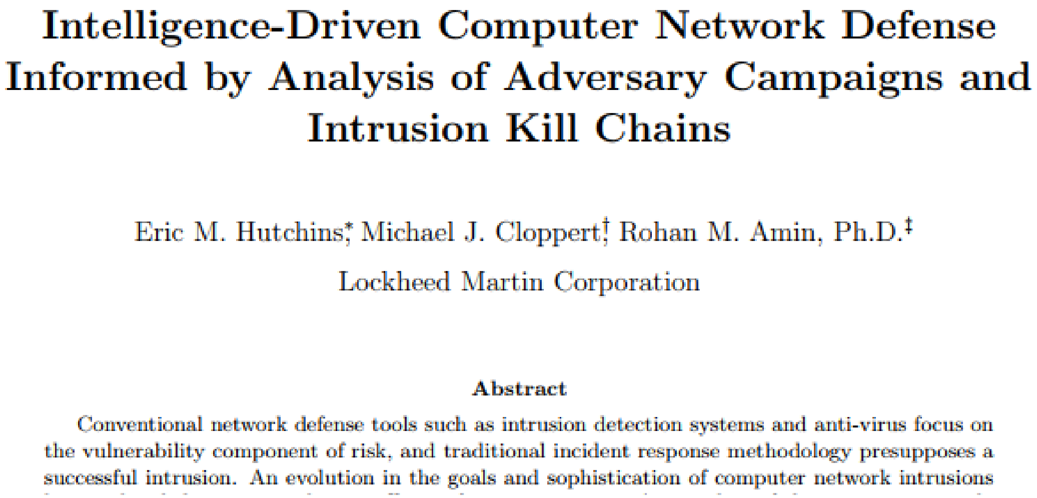
정보보호연구실
이주현

Introduction

- Cyber Kill Chain : 2009년 록히드 마틴사에서 수많은 해킹 공격을 분석하고 대응전략을 수립해 발표한 논문에서 Intrusion Kill Chain으로 소개되었다가, 이후 Cyber Kill Chain으로 변경해 사용되고 있음

  Kill Chain : 군사용어로 미사일을 방어하기 위해 선제 공격으로 미사일을 무력화 시키는 전략

- 사이버 공격 프로세스를 분석하여 각 공격 단계에서 조직에 가해지는 위협 요소 및 공격자의 목적, 활동 등을 분석하여 위협요소를 완화, 제거하는 선제적 방어 기법



Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains

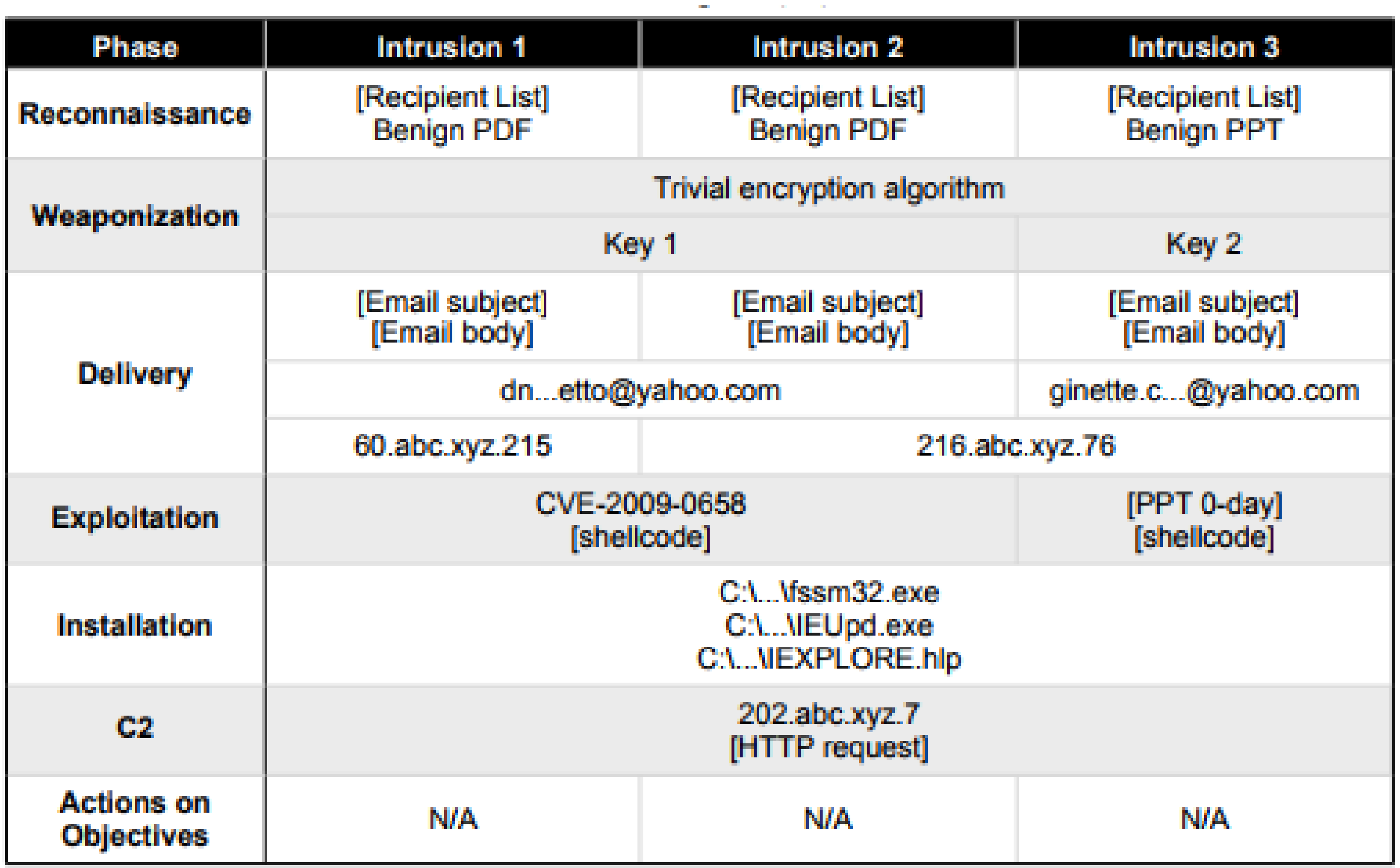
Eric M. Hutchins[*] Michael J. Cloppert[†] Rohan M. Amin, Ph.D.[‡]

Lockheed Martin Corporation

Abstract

Conventional network defense tools such as intrusion detection systems and anti-virus focus on the vulnerability component of risk, and traditional incident response methodology presupposes a successful intrusion. An evolution in the goals and sophistication of computer network intrusions

Cyber Kill Chain



Phase	Intrusion 1	Intrusion 2	Intrusion 3
Reconnaissance	[Recipient List] Benign PDF	[Recipient List] Benign PDF	[Recipient List] Benign PPT
Weaponization	Trivial encryption algorithm		
	Key 1		Key 2
Delivery	[Email subject] [Email body]	[Email subject] [Email body]	[Email subject] [Email body]
	dn...etto@yahoo.com		ginette.c...@yahoo.com
	60.abc.xyz.215	216.abc.xyz.76	
Exploitation	CVE-2009-0658 [shellcode]		[PPT 0-day] [shellcode]
Installation	C:\...\fssm32.exe C:\...\IEUpd.exe C:\...\IEXPLORE.hlp		
C2	202.abc.xyz.7 [HTTP request]		
Actions on Objectives	N/A	N/A	N/A

Intrusion Attempts 1, 2, and 3 Indicators

Cyber Kill Chain

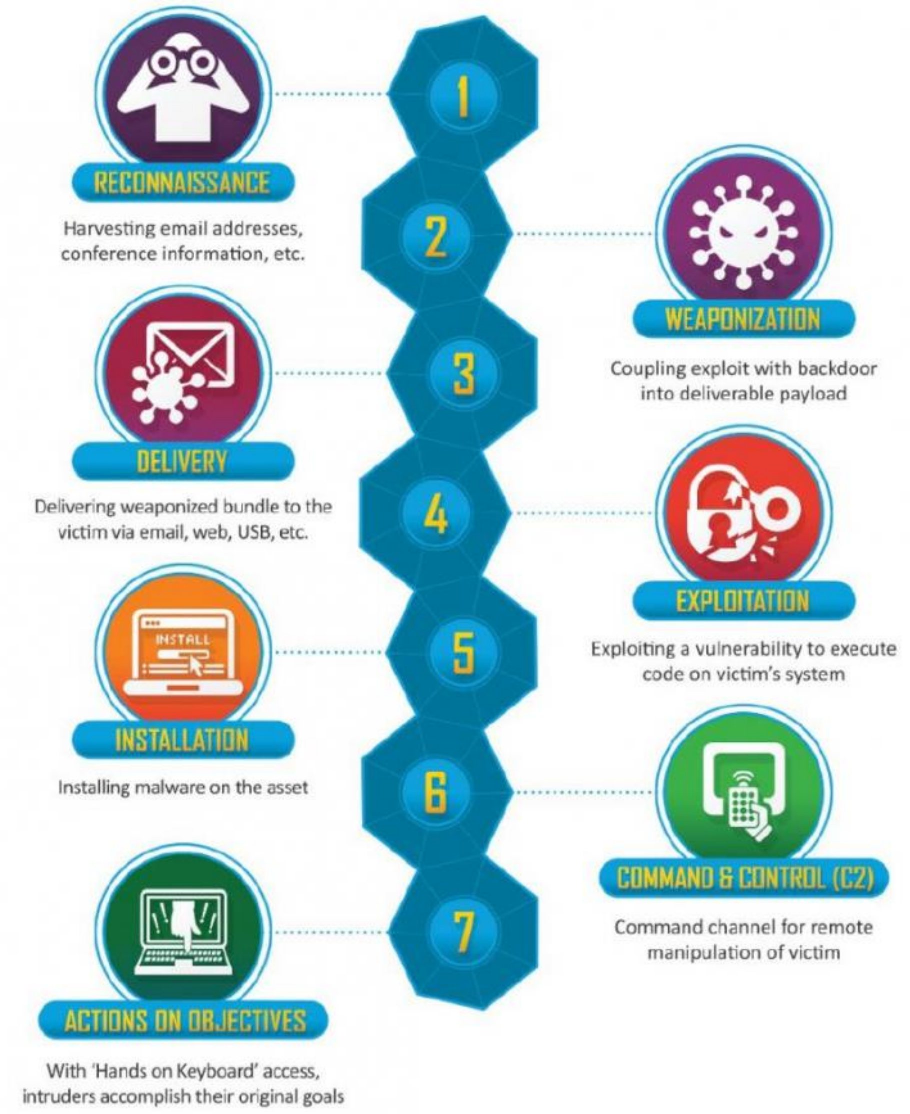
Cyber Kill Chain 7단계

타깃 분석을 위한 정찰(Reconnaissance)

- 목표물을 정하고 대상을 식별
- 목표물 공격에 활용할 수 있는 이메일 주소 등의 정보 수집

타깃 공격을 위한 무기작성(Weaponization)

- Exploit과 백도어를 결합하여 악성코드 생성
- 앞서 파악한 공격 대상 정보에 따라
  알려진 취약점 또는 제로데이 취약점을 활용


1
RECONNAISSANCE
Harvesting email addresses, conference information, etc.
2
WEAPONIZATION
Coupling exploit with backdoor into deliverable payload
3
DELIVERY
Delivering weaponized bundle to the victim via email, web, USB, etc.
4
EXPLOITATION
Exploiting a vulnerability to execute code on victim's system
5
INSTALLATION
INSTALL
Installing malware on the asset
6
COMMAND & CONTROL (C2)
Command channel for remote manipulation of victim
7
ACTIONS ON OBJECTIVES
With 'Hands on Keyboard' access, intruders accomplish their original goals

Cyber Kill Chain

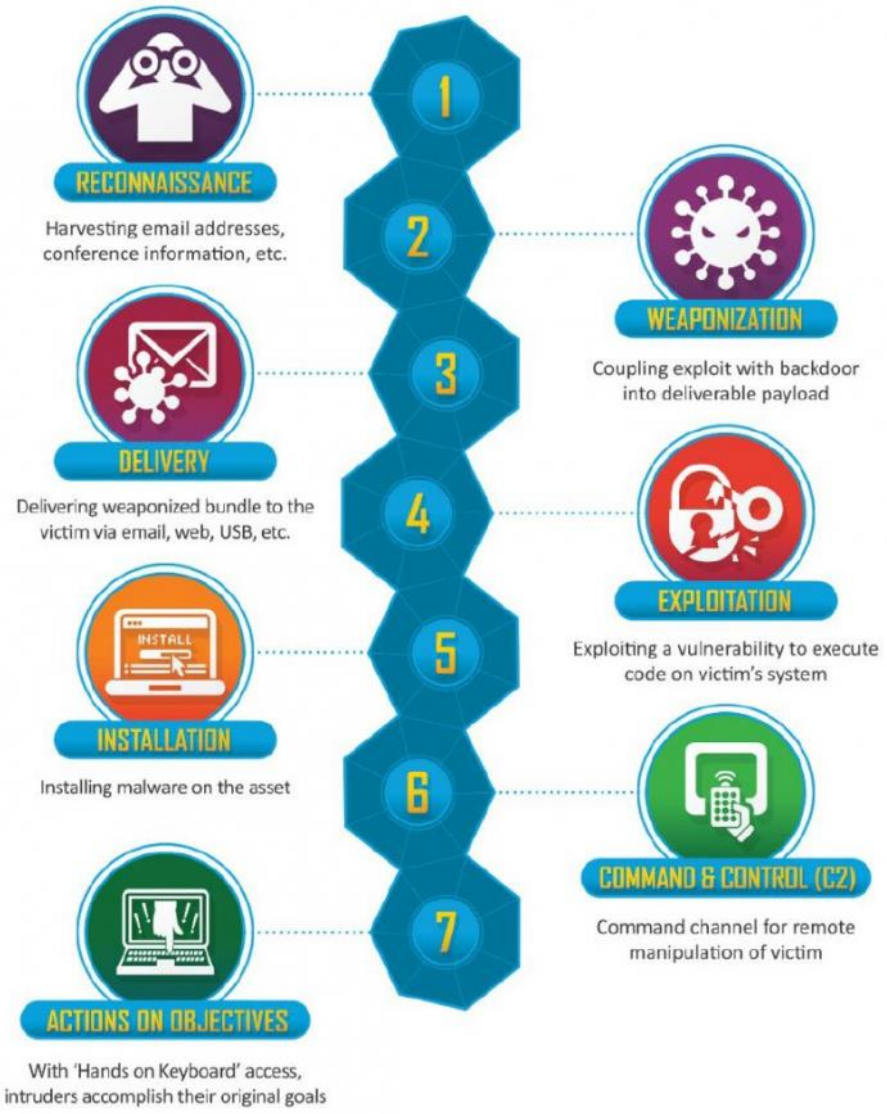
Cyber Kill Chain 7단계

타깃에 전달(Delivery)

- 목표 대상에게 이메일에 파일 첨부, 웹사이트 링크, USB 등의 다양한 방식으로 악성코드를 유포한다.

권한탈취(Exploitation)

- 대상 목표에 전달된 악성코드가 활성화되면서 공격자가 의도한 악의적 행위가 실행된다.


1
RECONNAISSANCE
Harvesting email addresses, conference information, etc.
2
WEAPONIZATION
Coupling exploit with backdoor into deliverable payload
3
DELIVERY
Delivering weaponized bundle to the victim via email, web, USB, etc.
4
EXPLOITATION
Exploiting a vulnerability to execute code on victim's system
5
INSTALL
INSTALLATION
Installing malware on the asset
6
COMMAND & CONTROL (C2)
Command channel for remote manipulation of victim
7
ACTIONS ON OBJECTIVES
With 'Hands on Keyboard' access, intruders accomplish their original goals

Cyber Kill Chain

Cyber Kill Chain 7단계

악성코드 설치(Installation)

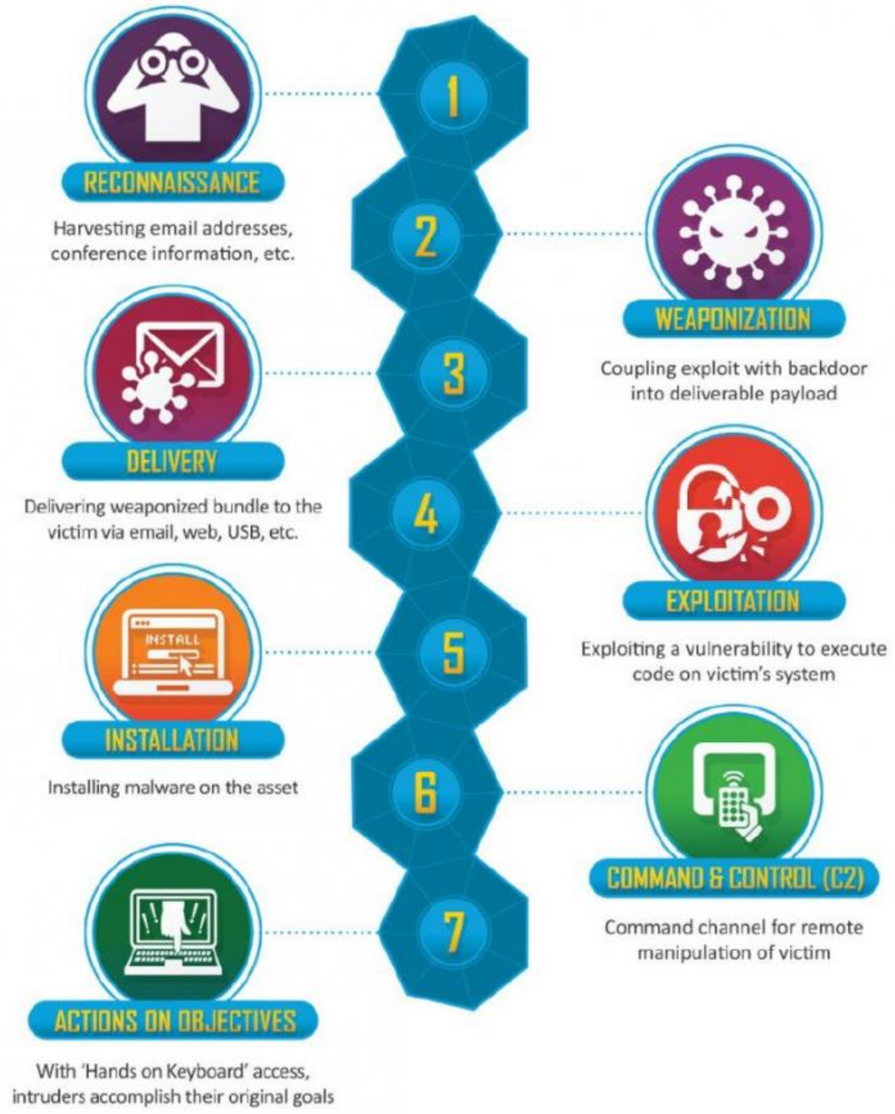
- 공격자가 지속적으로 대상에 접근할 수 있도록
  백도어나 원격제어가 가능한 악성 프로그램을 설치한다.

원격제어(Command & Control)

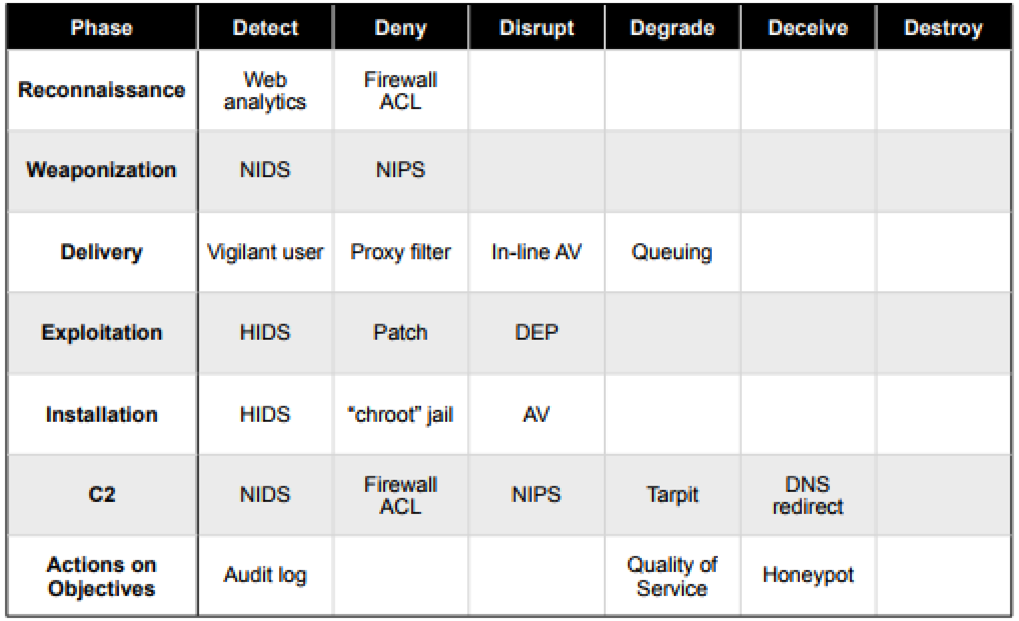
- 공격자가 대상물을 제어할 수 있는 통신 채널을 통해
  대상을 수동조작 및 내부 목표물에 접근하도록 활용

정보유출, 시스템파괴 등의 목적수행(Actions on objectives)

- 공격자가 목표한 데이터 수집에 성공하여 결과물 획득

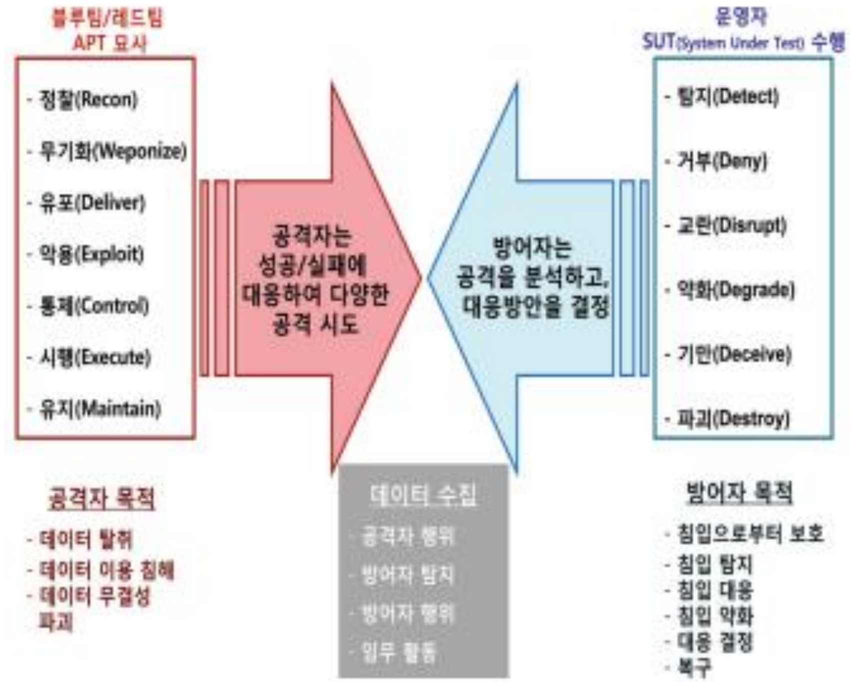

1
RECONNAISSANCE
Harvesting email addresses, conference information, etc.
2
WEAPONIZATION
Coupling exploit with backdoor into deliverable payload
3
DELIVERY
Delivering weaponized bundle to the victim via email, web, USB, etc.
4
EXPLOITATION
Exploiting a vulnerability to execute code on victim's system
5
INSTALL
INSTALLATION
Installing malware on the asset
6
COMMAND & CONTROL (C2)
Command channel for remote manipulation of victim
7
ACTIONS ON OBJECTIVES
With 'Hands on Keyboard' access, intruders accomplish their original goals

Cyber Kill Chain



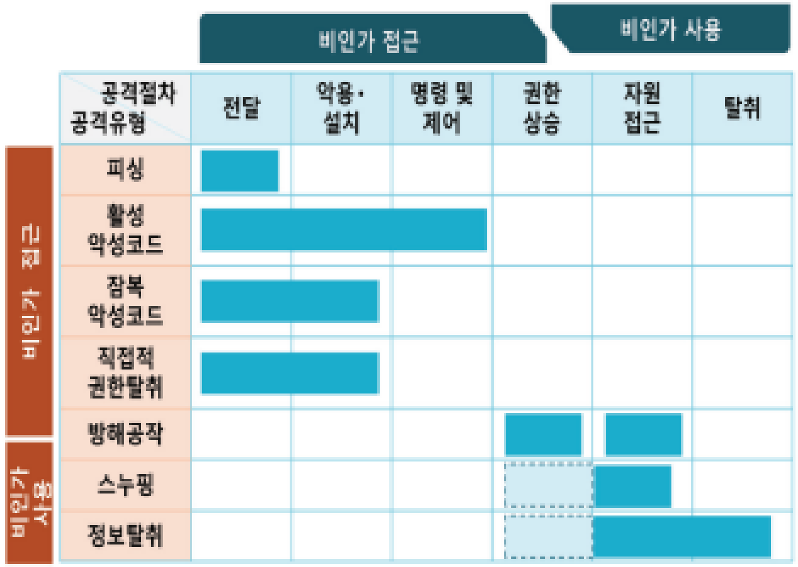
Phase	Detect	Deny	Disrupt	Degrade	Deceive	Destroy
Reconnaissance	Web analytics	Firewall ACL				
Weaponization	NIDS	NIPS				
Delivery	Vigilant user	Proxy filter	In-line AV	Queuing		
Exploitation	HIDS	Patch	DEP			
Installation	HIDS	"chroot" jail	AV			
C2	NIDS	Firewall ACL	NIPS	Tarpit	DNS redirect	
Actions on Objectives	Audit log			Quality of Service	Honeypot	

사이버킬체인 공격 절차에 따른 단계별 대응 유형



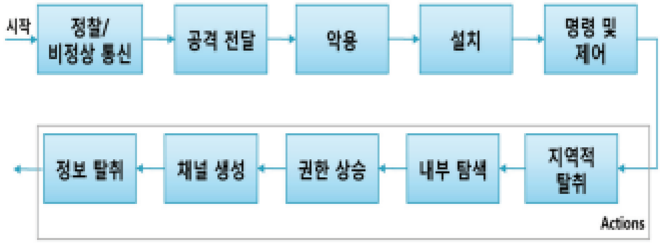
미 국방부의 사이버안보킬체인

Cyber Kill Chain

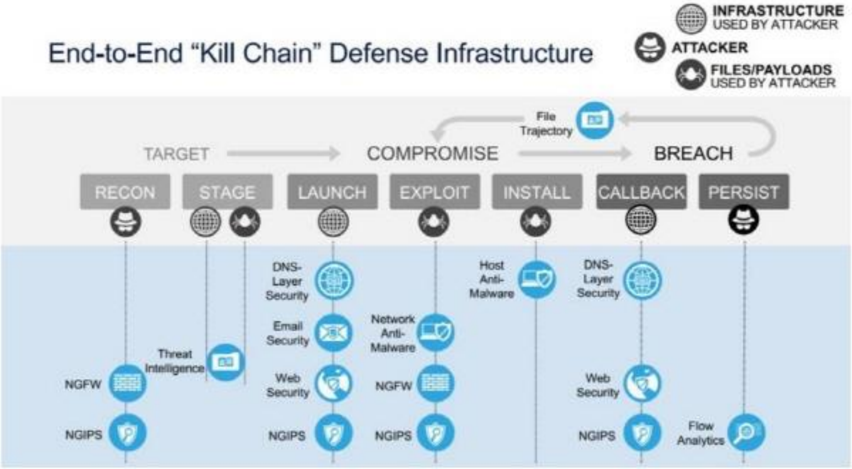


		비인가 접근			비인가 사용		
	공격절차 공격유형	전달	악용·설치	명령 및 제어	권한 상승	자원 접근	탈취
비인가 접근	피싱	■					
	활성 악성코드	■	■	■			
	잠복 악성코드	■	■				
	직접적 권한탈취	■	■				
비인가 사용	방해공작				■	■	
	스누핑				⬚	■	
	정보탈취				⬚	■	■

가트너의 공격체인모델



휴렛패커드의 공격라이프사이클

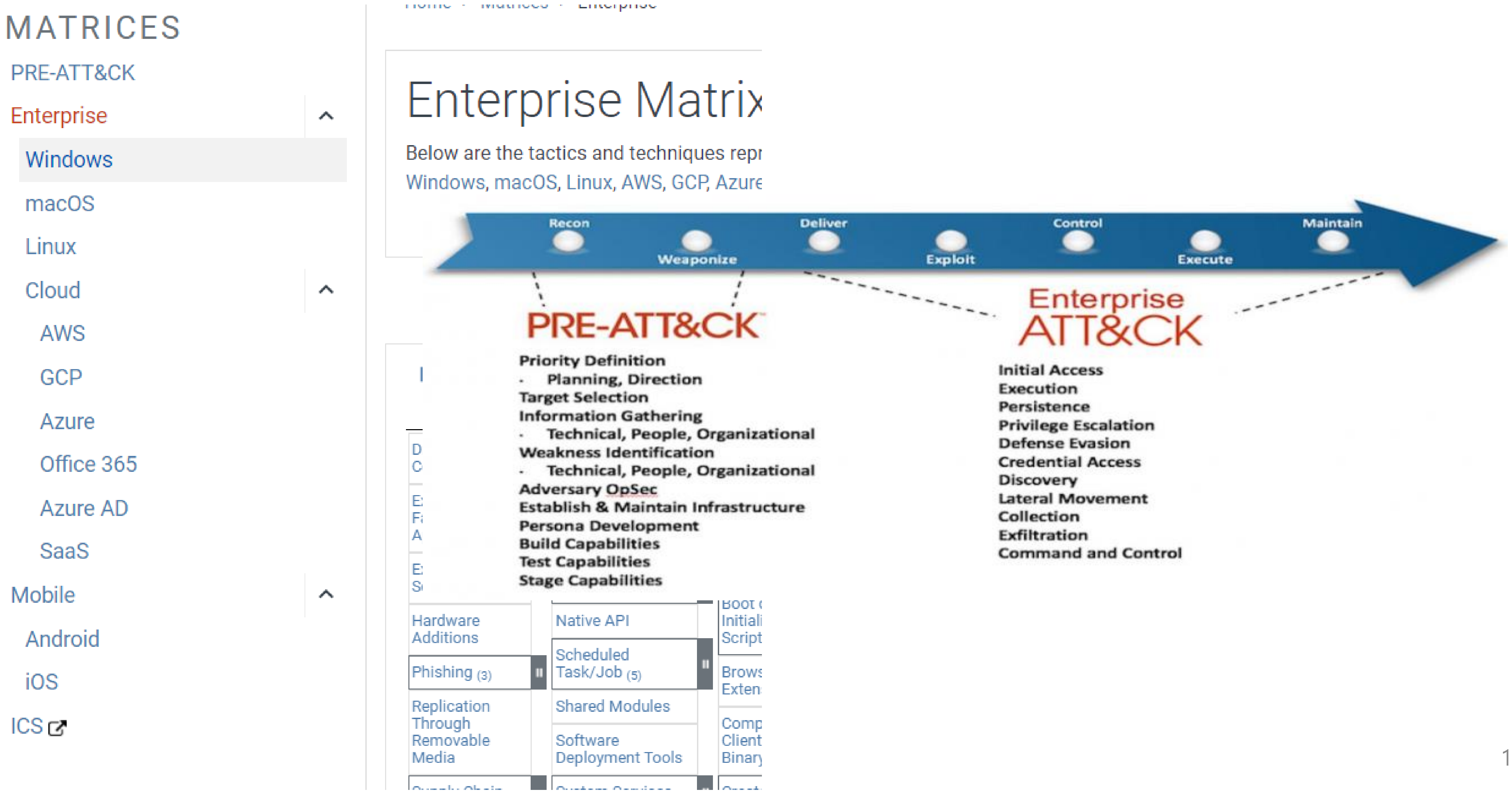


kill chain with Cisco Security

ATT&CK

- MITRE에서 윈도우 네트워크에 실제 사용되는 해킹 기술에 대해서 TTPs(Tactics, Techniques, and Procedures)를 문서화하는 것으로 시작되었다.
- 이후, TTPs에 대해 사용된 것을 식별할 수 있도록 해주는 프레임워크로 개발되었음
- 2013년 9월에 처음 완성되었고, 이후 보다 많은 곳에 도움이 되고자 2015년 5월에 최초 공개
- 사이버 공격에 대한 분석 및 탐지 역량 강화에 초점이 맞춰져 있음
- 공격자가 실제 사용하는 기술들을 세분화하여 이를 단위 기술로 재연할 수 있도록 돕기위함
- Tactics : 통산 전술이라고 번역을 하는데, 이 부분은 "Why"에 맵핑된다. 현재 엔터프라이즈에는 12개의 전술이 존재하는데, 세부기술들의 목적(이유) 등을 설명하고 있다.
- Techniques : 기술이라고 통상 번역되며, "How"로 맵핑된다. 실제 해커가 어떤 기술을 이용했는지를 설명하는 것으로 엔터프라이즈에는 현재 중복되지 않는 244개의 세부 기술을 설명하고 있다.
- Procedure : 공격 기술(Techniques) 진행을 위해 시도한 실제 상세 공격 방법이다.

ATT&CK



MATRICES

- PRE-ATT&CK
- Enterprise
  - Windows
  - macOS
  - Linux
  - Cloud
    - AWS
    - GCP
    - Azure
    - Office 365
    - Azure AD
    - SaaS
- Mobile
  - Android
  - iOS
- ICS

Home · Matrices · Enterprise

Enterprise Matrix

Below are the tactics and techniques repr

Windows, macOS, Linux, AWS, GCP, Azure

Hardware Additions	Native API	Boot or Initiali Script
Phishing (3)	Scheduled Task/Job (5)	Brows Exten
Replication Through Removable Media	Shared Modules	Comp Client Binary
	Software Deployment Tools	

PRE-ATT&CK

Priority Definition
- Planning, Direction

Target Selection

Information Gathering
- Technical, People, Organizational

Weakness Identification
- Technical, People, Organizational

Adversary OpSec

Establish & Maintain Infrastructure

Persona Development

Build Capabilities

Test Capabilities

Stage Capabilities

Enterprise ATT&CK

Initial Access

Execution

Persistence

Privilege Escalation

Defense Evasion

Credential Access

Discovery

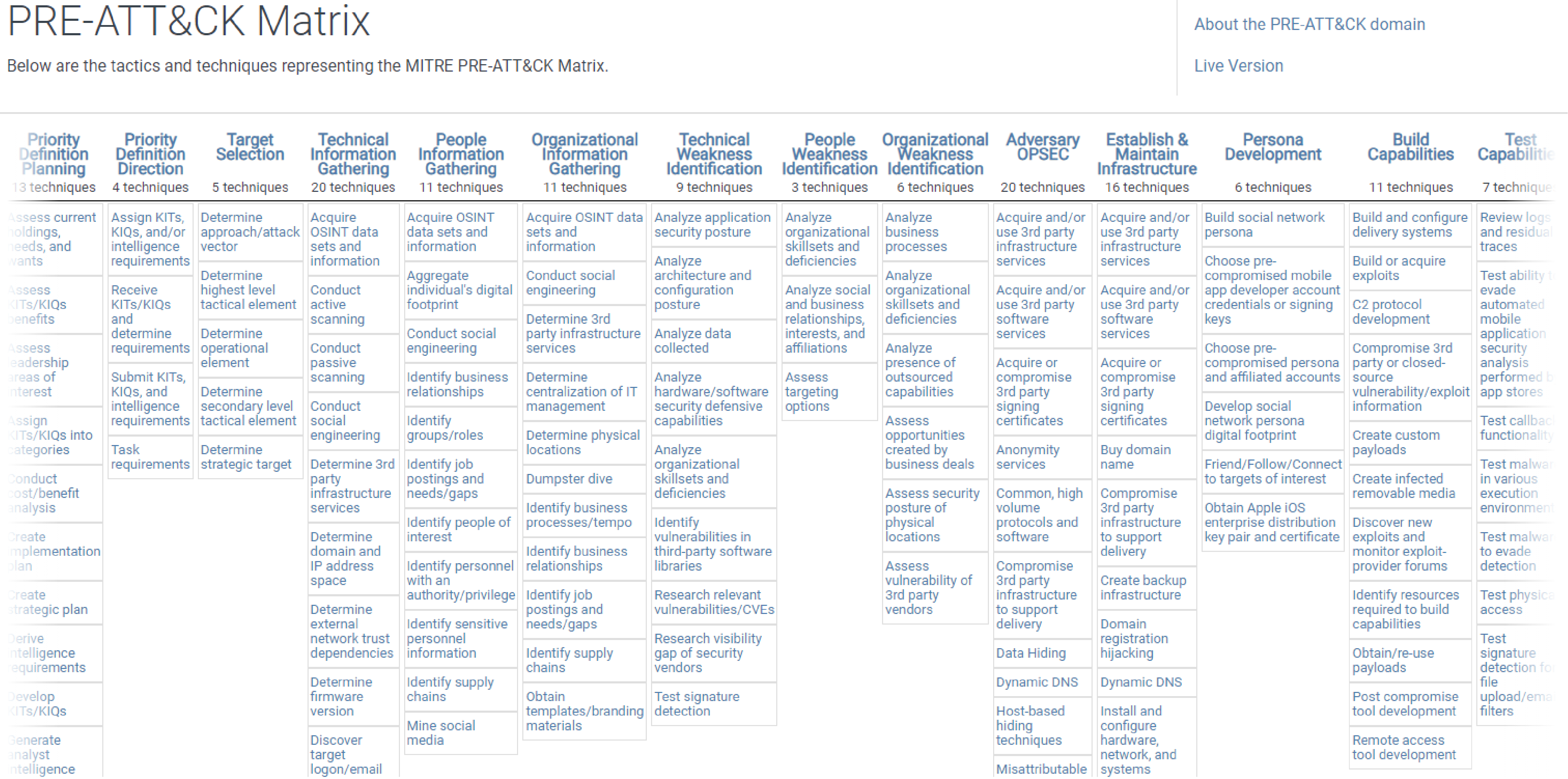
Lateral Movement

Collection

Exfiltration

Command and Control

ATT&CK



PRE-ATT&CK Matrix

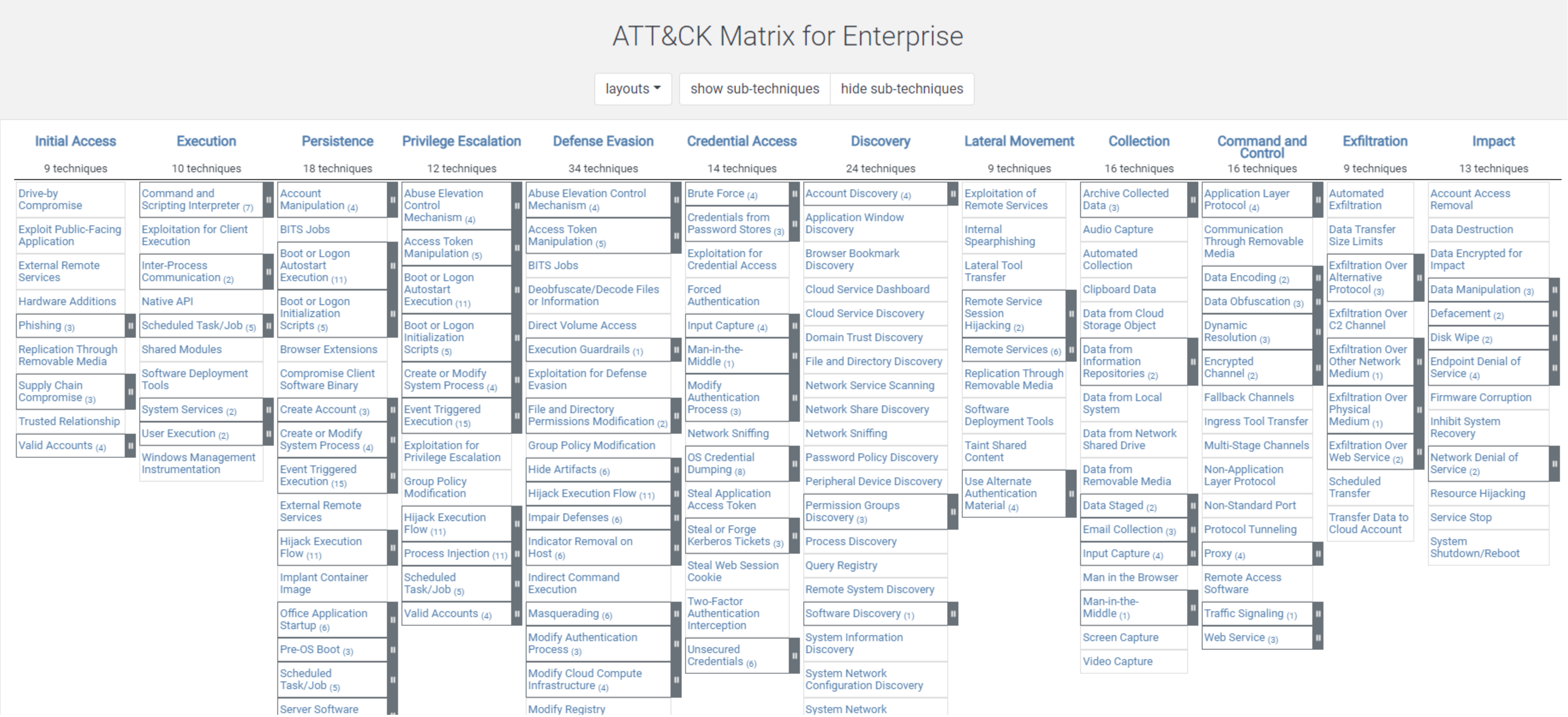
Below are the tactics and techniques representing the MITRE PRE-ATT&CK Matrix.

About the PRE-ATT&CK domain

Live Version

Priority Definition Planning	Priority Definition Direction	Target Selection	Technical Information Gathering	People Information Gathering	Organizational Information Gathering	Technical Weakness Identification	People Weakness Identification	Organizational Weakness Identification	Adversary OPSEC	Establish & Maintain Infrastructure	Persona Development	Build Capabilities	Test Capabilities
13 techniques	4 techniques	5 techniques	20 techniques	11 techniques	11 techniques	9 techniques	3 techniques	6 techniques	20 techniques	16 techniques	6 techniques	11 techniques	7 techniques
Assess current holdings, needs, and wants	Assign KITs, KIQs, and/or intelligence requirements	Determine approach/attack vector	Acquire OSINT data sets and information	Acquire OSINT data sets and information	Acquire OSINT data sets and information	Analyze application security posture	Analyze organizational skillsets and deficiencies	Analyze business processes	Acquire and/or use 3rd party infrastructure services	Acquire and/or use 3rd party infrastructure services	Build social network persona	Build and configure delivery systems	Review logs and residual traces
Assess KITs/KIQs benefits	Receive KITs/KIQs and determine requirements	Determine highest level tactical element	Conduct active scanning	Aggregate individual's digital footprint	Conduct social engineering	Analyze architecture and configuration posture	Analyze social and business relationships, interests, and affiliations	Analyze organizational skillsets and deficiencies	Acquire and/or use 3rd party software services	Acquire and/or use 3rd party software services	Choose pre-compromised mobile app developer account credentials or signing keys	Build or acquire exploits	Test ability to evade automated mobile application security analysis performed by app stores
Assess leadership areas of interest	Submit KITs, KIQs, and intelligence requirements	Determine operational element	Conduct passive scanning	Conduct social engineering	Determine 3rd party infrastructure services	Analyze data collected	Assess targeting options	Analyze presence of outsourced capabilities	Acquire or compromise 3rd party signing certificates	Acquire or compromise 3rd party signing certificates	Choose pre-compromised persona and affiliated accounts	C2 protocol development	Test callback functionality
Assign KITs/KIQs into categories	Task requirements	Determine secondary level tactical element	Conduct social engineering	Identify business relationships	Determine centralization of IT management	Analyze hardware/software security defensive capabilities		Assess opportunities created by business deals	Anonymity services	Buy domain name	Develop social network persona digital footprint	Compromise 3rd party or closed-source vulnerability/exploit information	Test malware in various execution environments
Conduct cost/benefit analysis		Determine strategic target	Determine 3rd party infrastructure services	Identify groups/roles	Determine physical locations	Analyze organizational skillsets and deficiencies		Assess security posture of physical locations	Common, high volume protocols and software	Compromise 3rd party infrastructure to support delivery	Friend/Follow/Connect to targets of interest	Create custom payloads	Test malware to evade detection
Create implementation plan			Determine domain and IP address space	Identify job postings and needs/gaps	Dumpster dive	Identify vulnerabilities in third-party software libraries		Assess vulnerability of 3rd party vendors	Compromise 3rd party infrastructure to support delivery	Create backup infrastructure	Obtain Apple iOS enterprise distribution key pair and certificate	Create infected removable media	Test physical access
Create strategic plan			Determine external network trust dependencies	Identify people of interest	Identify business processes/tempo	Research relevant vulnerabilities/CVEs			Data Hiding	Domain registration hijacking		Discover new exploits and monitor exploit-provider forums	Test signature detection for file upload/email filters
Derive intelligence requirements			Determine firmware version	Identify personnel with an authority/privilege	Identify business relationships	Research visibility gap of security vendors			Dynamic DNS	Dynamic DNS		Identify resources required to build capabilities	
Develop KITs/KIQs			Discover target logon/email	Identify sensitive personnel information	Identify job postings and needs/gaps	Test signature detection			Host-based hiding techniques	Install and configure hardware, network, and systems		Obtain/re-use payloads	
Generate analyst intelligence				Identify supply chains	Identify supply chains				Misattributable			Post compromise tool development	
				Mine social media	Obtain templates/branding materials							Remote access tool development	

ATT&CK



ATT&CK Matrix for Enterprise

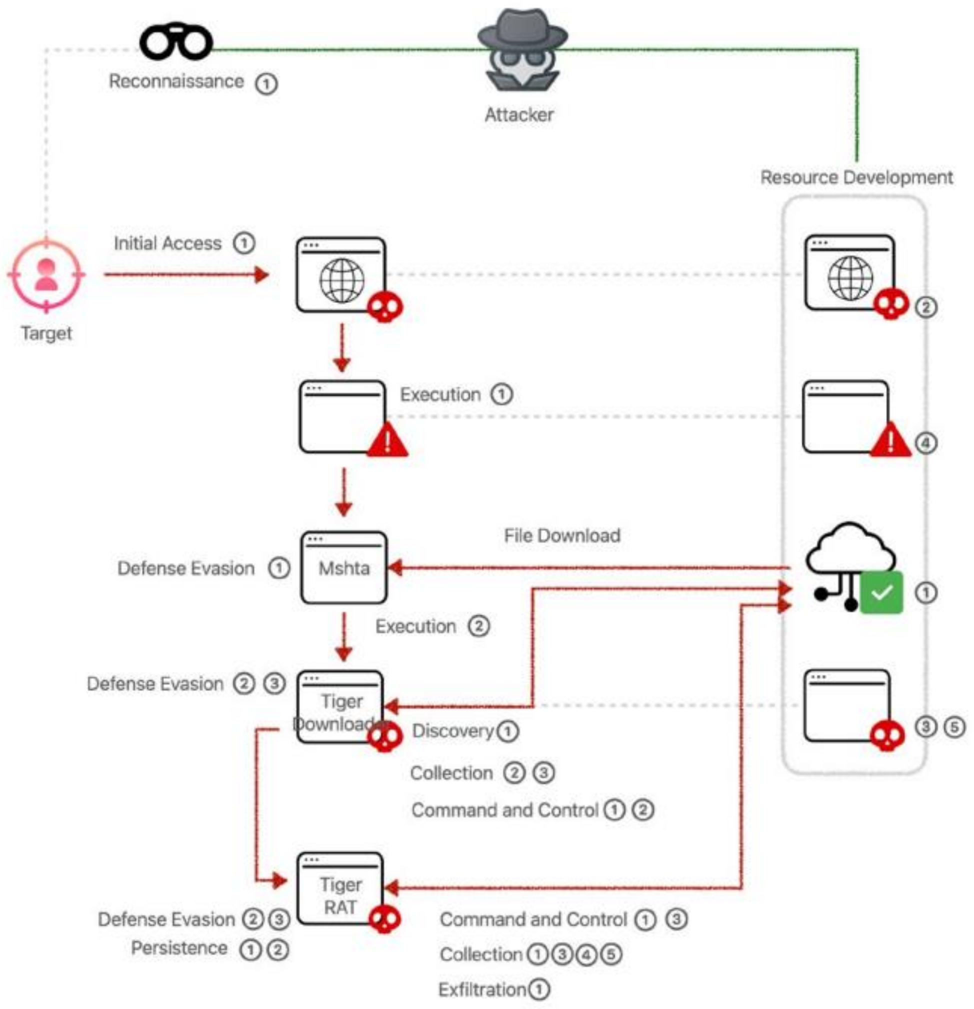
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
9 techniques	10 techniques	18 techniques	12 techniques	34 techniques	14 techniques	24 techniques	9 techniques	16 techniques	16 techniques	9 techniques	13 techniques
Drive-by Compromise	Command and Scripting Interpreter (7)	Account Manipulation (4)	Abuse Elevation Control Mechanism (4)	Abuse Elevation Control Mechanism (4)	Brute Force (4)	Account Discovery (4)	Exploitation of Remote Services	Archive Collected Data (3)	Application Layer Protocol (4)	Automated Exfiltration	Account Access Removal
Exploit Public-Facing Application	Exploitation for Client Execution	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Credentials from Password Stores (3)	Application Window Discovery	Internal Spearphishing	Audio Capture	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
External Remote Services	Inter-Process Communication (2)	Boot or Logon Autostart Execution (11)	Boot or Logon Autostart Execution (11)	BITS Jobs	Exploitation for Credential Access	Browser Bookmark Discovery	Lateral Tool Transfer	Automated Collection	Data Encoding (2)	Exfiltration Over Alternative Protocol (3)	Data Encrypted for Impact
Hardware Additions	Native API	Boot or Logon Initialization Scripts (5)	Boot or Logon Initialization Scripts (5)	Deobfuscate/Decode Files or Information	Forced Authentication	Cloud Service Dashboard	Remote Service Session Hijacking (2)	Clipboard Data	Data Obfuscation (3)	Exfiltration Over C2 Channel	Data Manipulation (3)
Phishing (3)	Scheduled Task/Job (5)	Browser Extensions	Create or Modify System Process (4)	Direct Volume Access	Input Capture (4)	Cloud Service Discovery	Remote Services (6)	Data from Cloud Storage Object	Dynamic Resolution (3)	Exfiltration Over Other Network Medium (1)	Defacement (2)
Replication Through Removable Media	Shared Modules	Compromise Client Software Binary	Event Triggered Execution (15)	Execution Guardrails (1)	Man-in-the-Middle (1)	Domain Trust Discovery	Replication Through Removable Media	Data from Information Repositories (2)	Encrypted Channel (2)	Exfiltration Over Physical Medium (1)	Disk Wipe (2)
Supply Chain Compromise (3)	Software Deployment Tools	Create Account (3)	Exploitation for Privilege Escalation	Exploitation for Defense Evasion	Modify Authentication Process (3)	File and Directory Discovery	Software Deployment Tools	Data from Local System	Fallback Channels	Exfiltration Over Web Service (2)	Endpoint Denial of Service (4)
Trusted Relationship	System Services (2)	Create or Modify System Process (4)	Group Policy Modification	File and Directory Permissions Modification (2)	Network Sniffing	Network Service Scanning	Taint Shared Content	Data from Network Shared Drive	Ingress Tool Transfer	Scheduled Transfer	Firmware Corruption
Valid Accounts (4)	User Execution (2)	Event Triggered Execution (15)	Hijack Execution Flow (11)	Group Policy Modification	OS Credential Dumping (8)	Network Share Discovery	Use Alternate Authentication Material (4)	Data from Removable Media	Multi-Stage Channels	Transfer Data to Cloud Account	Inhibit System Recovery
	Windows Management Instrumentation	External Remote Services	Process Injection (11)	Hide Artifacts (6)	Steal Application Access Token	Network Sniffing		Data Staged (2)	Non-Application Layer Protocol		Network Denial of Service (2)
		Hijack Execution Flow (11)	Scheduled Task/Job (5)	Hijack Execution Flow (11)	Steal or Forge Kerberos Tickets (3)	Password Policy Discovery		Email Collection (3)	Non-Standard Port		Resource Hijacking
		Implant Container Image	Valid Accounts (4)	Impair Defenses (6)	Steal Web Session Cookie	Peripheral Device Discovery		Input Capture (4)	Protocol Tunneling		Service Stop
		Office Application Startup (6)		Indicator Removal on Host (6)	Two-Factor Authentication Interception	Permission Groups Discovery (3)		Man in the Browser	Proxy (4)		System Shutdown/Reboot
		Pre-OS Boot (3)		Indirect Command Execution	Unsecured Credentials (6)	Process Discovery		Man-in-the-Middle (1)	Remote Access Software		
		Scheduled Task/Job (5)		Masquerading (6)		Query Registry		Screen Capture	Traffic Signaling (1)		
		Server Software		Modify Authentication Process (3)		Remote System Discovery		Video Capture	Web Service (3)		
				Modify Cloud Compute Infrastructure (4)		Software Discovery (1)					
				Modify Registry		System Information Discovery					
						System Network Configuration Discovery					
						System Network					

ATT&CK

ATT&CK 프레임워크 활용 기대 효과

1. 악의적 행위(Adversary behaviors) 분석 : 공격자의 활동과 관련 기술에 대해서 집중함으로써 실제 공격 탐지 가능성을 높이고자 함. 침해 탐지에 주로 사용되는 IOC 값인 도메인, IP, 파일해시 등은 우회 또는 위/변조 등이 가능해 이보다 어떤 부분이 더욱 탐지에 도움이 되는지를 설명하고자 함
2. 적절하지 않은 라이프사이클 모델(Lifecycle models that didn't fit) : Cyber Kill Chain은 실제 방어를 위한 행동 요령을 설명하기에는 너무 상위 레벨의 개념. 따라서 실제 행동 요령에 도움을 주고자 함
3. 실제 환경에 적용(Applicability to real environments) : 사고조사를 통해 확인된 TTPs를 실제 환경에 적용해 테스트할 수 있도록 하기 위함
4. 분류체계 (Common taxonomy) : TTPs에 대해 다른 공격 그룹이나 기술들에 대해 용어의 통일을 통해 비교를 용이하게 하기 위함

ATT&CK



공격 개요도

Reconnaissance

- T1590.005 Gather Victim Network Information

Resource Development

- T1583.003 Acquire Infrastructure
- T1584.004 Compromise Infrastructure
- T1587.001 Develop Capabilities
- T1608.004 Stage Capabilities

Initial Access

- T1189 Drive-by Compromise

Execution

- T1203 Exploitation for Client Execution
- T1059 Command and Scripting Interpreter

Persistence

- T1547.001 Boot or Logon Autostart Executio
- T1053.005 Scheduled Task/Job

Defense Evasion

- T1218.005 Signed Binary Proxy Execution
- T1036.005 Masquerading
- T1140 Deobfuscate/Decode Files or Information

Discovery

- T1033 System Owner/User Discovery

Collection

- T1560.002 Archive Collected Data
- T1119 Automated Collection
- T1005 Data from Local System
- T1056.001 Input Capture
- T1113 Screen Capture

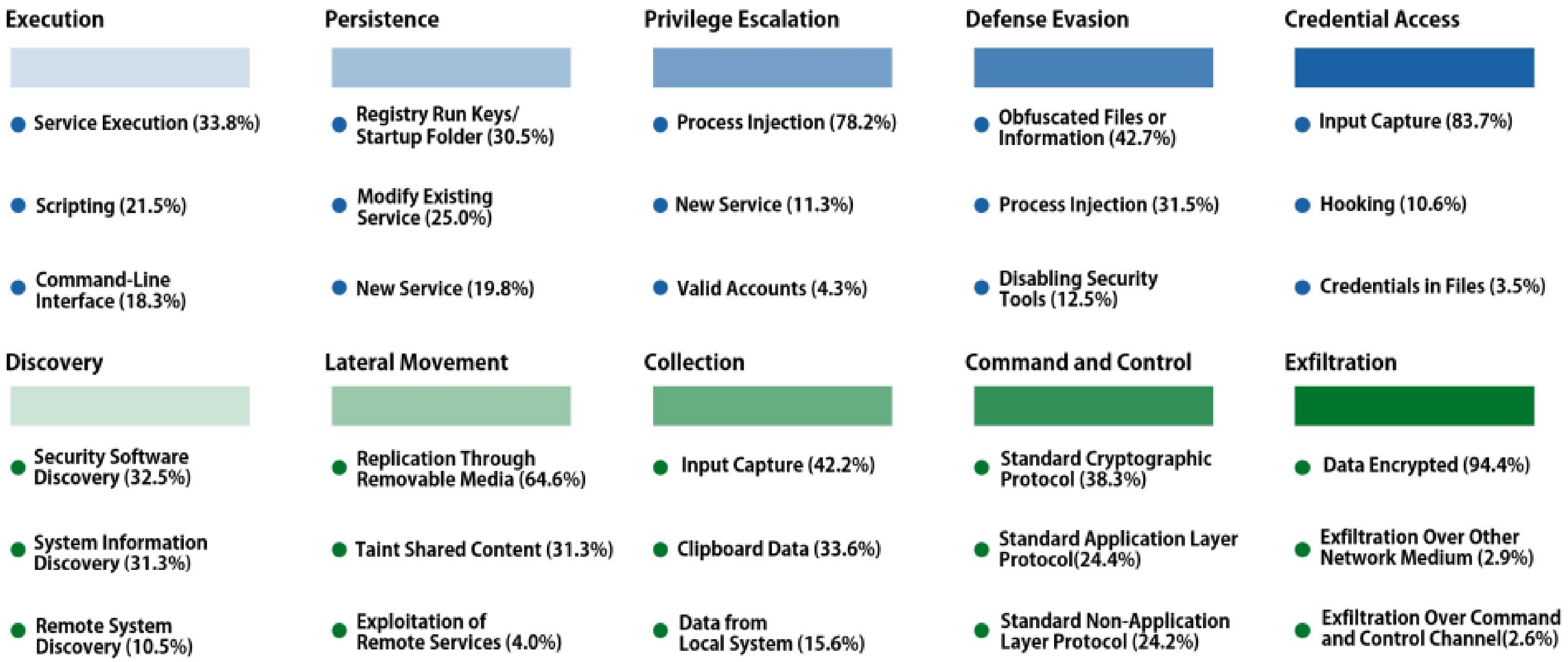
Command and Control

- T1071.001 Application Layer Protocol
- T1132.001 Data Encoding
- T1573.001 Encrypted channel

Exfiltration

- T1041 Exfiltration Over C2 Channel

ATT&CK



Execution

- Service Execution (33.8%)
- Scripting (21.5%)
- Command-Line Interface (18.3%)

Persistence

- Registry Run Keys/ Startup Folder (30.5%)
- Modify Existing Service (25.0%)
- New Service (19.8%)

Privilege Escalation

- Process Injection (78.2%)
- New Service (11.3%)
- Valid Accounts (4.3%)

Defense Evasion

- Obfuscated Files or Information (42.7%)
- Process Injection (31.5%)
- Disabling Security Tools (12.5%)

Credential Access

- Input Capture (83.7%)
- Hooking (10.6%)
- Credentials in Files (3.5%)

Discovery

- Security Software Discovery (32.5%)
- System Information Discovery (31.3%)
- Remote System Discovery (10.5%)

Lateral Movement

- Replication Through Removable Media (64.6%)
- Taint Shared Content (31.3%)
- Exploitation of Remote Services (4.0%)

Collection

- Input Capture (42.2%)
- Clipboard Data (33.6%)
- Data from Local System (15.6%)

Command and Control

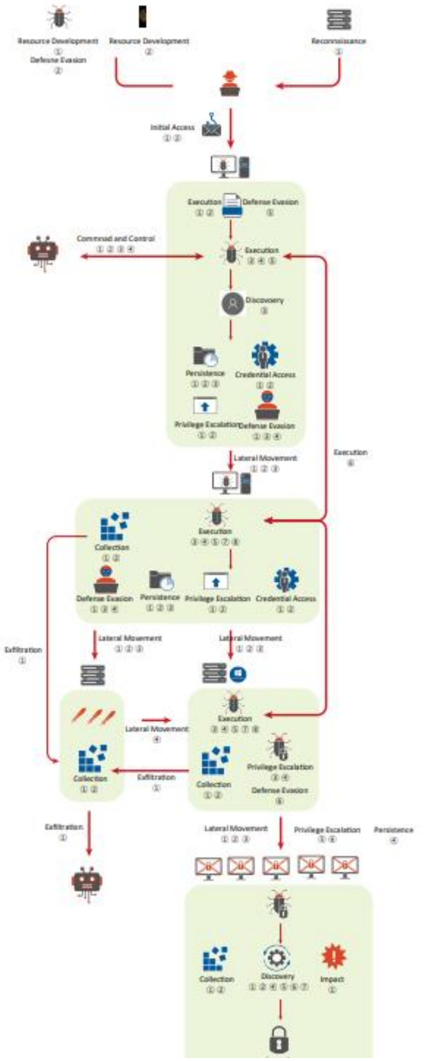
- Standard Cryptographic Protocol (38.3%)
- Standard Application Layer Protocol(24.4%)
- Standard Non-Application Layer Protocol (24.2%)

Exfiltration

- Data Encrypted (94.4%)
- Exfiltration Over Other Network Medium (2.9%)
- Exfiltration Over Command and Control Channel(2.6%)

* 각 기술 별 대응전략은 MITRE 홈페이지에서 제시한 내용을 반영

ATT&CK



Reconnaissance

- Gather Victim Identity Information

Persistence

- Create Account
- Create or Modify System Process
- Boot or Logon Autostart Execution
- Boot or Logon Initialization Scripts

Resource Development

- Obtain Capabilities
- Develop Capabilities
- Compromise Infrastructure

Privilege Escalation

- Valid Accounts
- Abuse Elevation Control Mechanism
- Account Token Manipulation
- Domain Policy Modification
- Boot or Logon Initialization Scripts

Initial Access

- Phishing

Credential Access

- OS Credential Dumping
- Create Account

Execution

- User Execution
- Command and Scripting Interpreter
- System Services
- Inter-Process Communication
- Scheduled Task
- Windows Management Instrumentation

Defense Evasion

- Masquerading
- Subvert Trust Controls
- Indicator Removal on Host
- Signed Binary Proxy Execution
- Deobfuscate/Decode Files or information

Discovery

- Software Discovery
- Process Discovery
- Account Discovery
- File and Directory Discovery
- Network Share Discovery
- System Information Discovery
- System Owner/User Discovery

Impact

- Service Stop
- Data Encrypted for Impact

Lateral Movement

- Remote Services
- Lateral Tool Transfer

Command and Control

- Remote Access Software
- Application Layer Protocol
- Ingress Tool Transfer
- Protocol Tunneling

Collection

- Data from Local System
- Archive Collected Data

Exfiltration

- Exfiltration Over C2 Channel

Q & A