MITRE ATT&CK

권민준

목차

MITRE ATT&CK 프레임워크 이해

MITRE ATT&CK란?

등장 배경

탐지의 중요성

IOC 기반 탐지 VS TTP 기반 탐지

MITRE ATT&CK 구성

MITRE ATT&CK 프레임워크 이해

MITRE ATT&CK

공개된 자료를 기반으로 공격자들의 TTPs를 집대성하고 체계적으로 정리한 지식 베이스

공격자들의 TTPs들을 탐지하기 위해 필요한 데이터 소스와 데이터 컴포넌트 및 탐지 전략, 보완 방법 등으로 구성

MITRE ATT&CK 프레임워크 이해

등장 배경

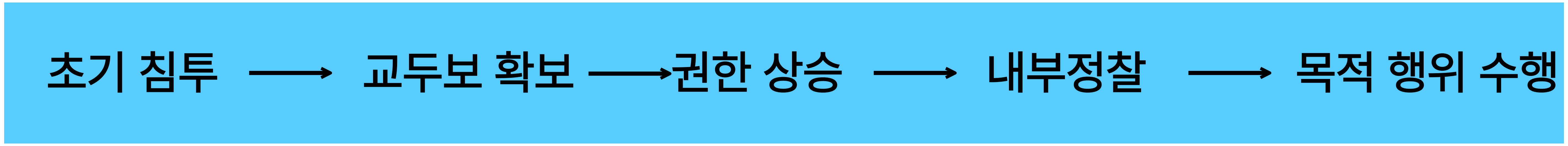
차단 및 보호 중심의 방어 전략이 탐지 중심으로 이동

TTPs를 체계적으로 정리한 지식 베이스 필요

MITRE ATT&CK 프레임워크 이해

탐지의 중요성

내부망 침투 차단에 실패해도 실질적인 피해가 발생하기 전에 위협을 찾아 제거할 수 있는 기회 존재



초기 침투 → 교두보 확보 → 권한 상승 → 내부정찰 → 목적 행위 수행

IOC 기반 탐지 VS TTP 기반 탐지

TTP(Tactics Techniques Procedures)

Tactics은 위협 행위의 목적을 나타냄

Techniques은 위협 행위의 목적을 달성하기 위해 사용하는 테크닉을 의미함

Procedures는 테크닉을 구현하기 위한 구체적인 절차와 방법을 의미함

IOC(indicator of compromise)

시스템이 악의적인 활동에 의해 침해되었을 가능성이 높음을 보여주는 운영체제 또는 네트워크 아티팩트

IOC로 주로 사용되는 정보 : 해시 값, 파일 이름 및 경로, C2 도메인, IP 어드레스 등

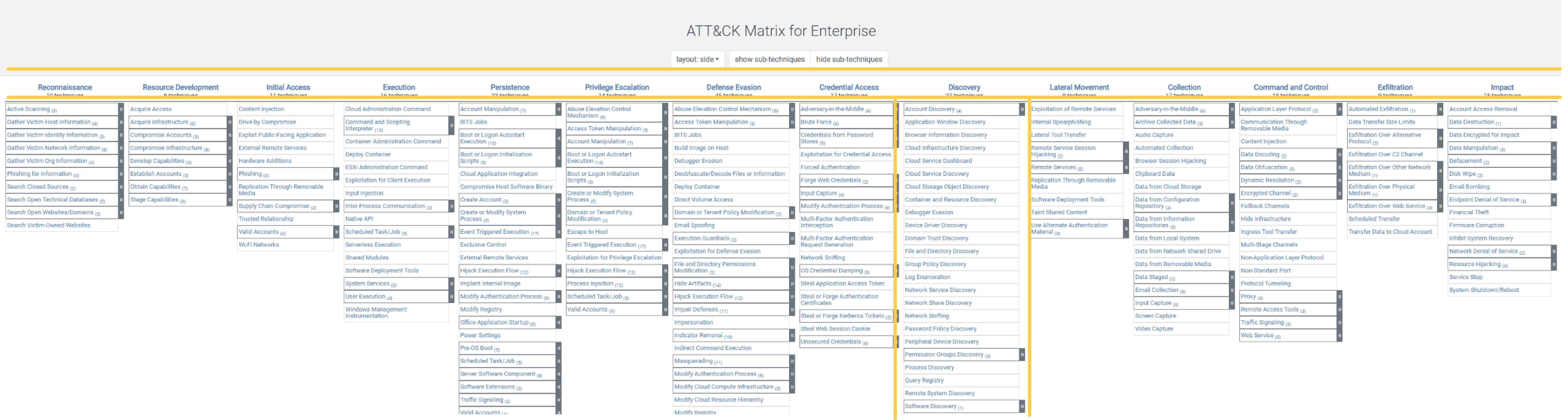
IOC 기반 탐지 한계점 : 반응성있음, 유효 기간이 짧음, 시간이 지날 수록 IOC 수가 과도하게 많아져 관리가 어렵고 탐지에도 많은 시간이 소요

IOC 기반 탐지 VS TTP 기반 탐지

공격범위	IOC 기반 탐지(예)	TTP 기반 탐지(예)
내부 시스템에 감염된 악성코드와 C&C간 커뮤니케이션(HTTP 활용)	C&C의 IP 어드레스, URL, User-Agent 문자열을 이용하여 탐지	주기성을 가진 아웃바운드 커넥션 최근에 등록한 도메인에 속한 시스템과의 통신 랜덤하게 생성된 도메인에 속한 시스템과 통신

MITRE ATT&CK 프레임워크 이해

MITRE ATT&CK 구성

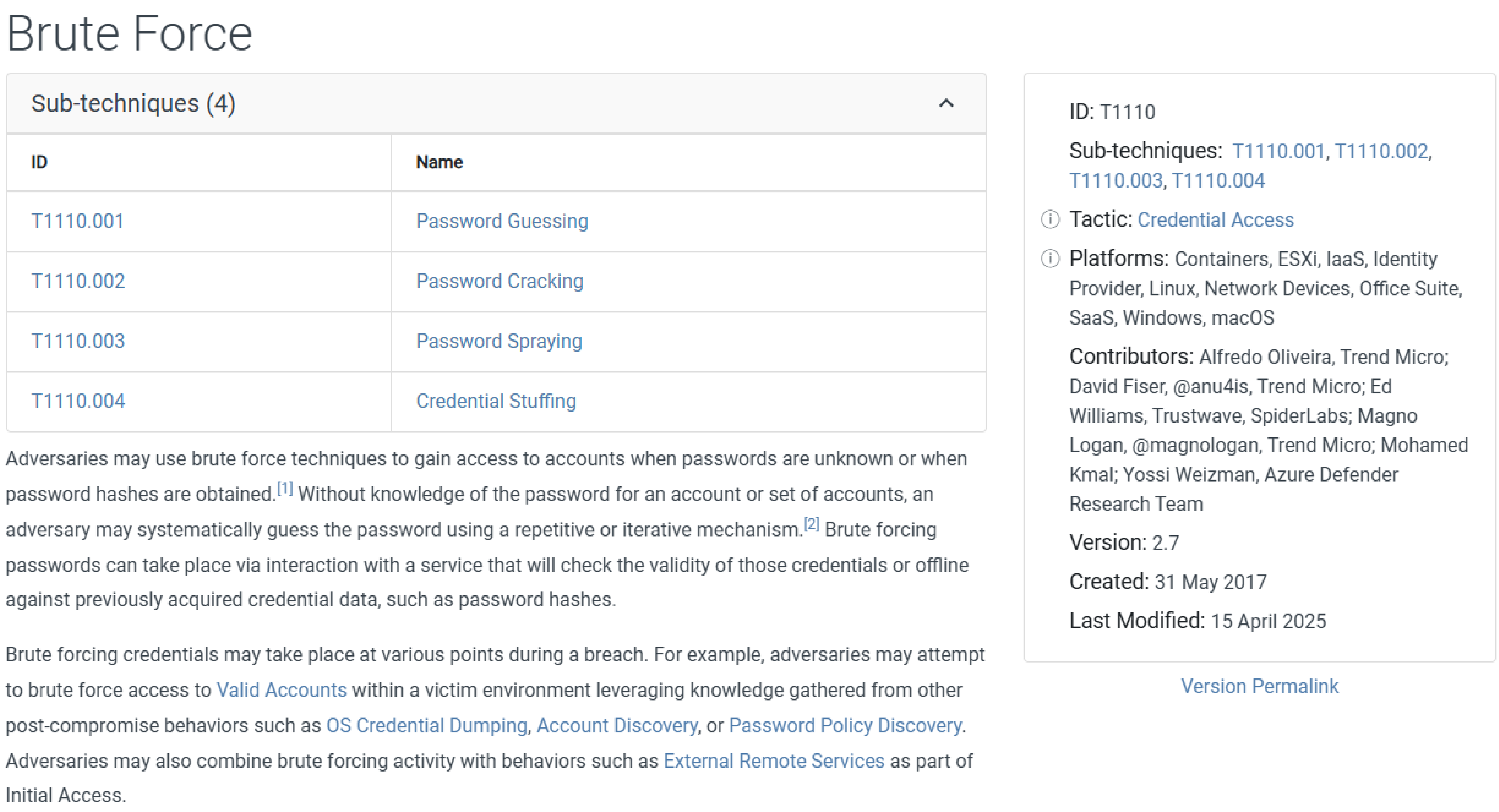


ATT&CK Matrix for Enterprise

layout: side ▾ | show sub-techniques | hide sub-techniques

Reconnaissance 10 techniques	Resource Development 8 techniques	Initial Access 11 techniques	Execution 16 techniques	Persistence 23 techniques	Privilege Escalation 14 techniques	Defense Evasion 45 techniques	Credential Access 17 techniques	Discovery 33 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 18 techniques	Exfiltration 9 techniques	Impact 15 techniques
Active Scanning (3)	Acquire Access	Content Injection	Cloud Administration Command	Account Manipulation (7)	Abuse Elevation Control Mechanism (6)	Abuse Elevation Control Mechanism (6)	Adversary-in-the-Middle (4)	Account Discovery (4)	Exploitation of Remote Services	Adversary-in-the-Middle (4)	Application Layer Protocol (5)	Automated Exfiltration (1)	Account Access Removal
Gather Victim Host Information (4)	Acquire Infrastructure (8)	Drive-by Compromise	Command and Scripting Interpreter (12)	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Brute Force (4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (3)	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction (1)
Gather Victim Identity Information (3)	Compromise Accounts (3)	Exploit Public-Facing Application	Container Administration Command	Boot or Logon Autostart Execution (14)	Account Manipulation (7)	BITS Jobs	Credentials from Password Stores (6)	Browser Information Discovery	Lateral Tool Transfer	Audio Capture	Content Injection	Exfiltration Over Alternative Protocol (3)	Data Encrypted for Impact
Gather Victim Network Information (6)	Compromise Infrastructure (8)	External Remote Services	Deploy Container	Boot or Logon Initialization Scripts (5)	Boot or Logon Autostart Execution (14)	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Automated Collection	Data Encoding (2)	Exfiltration Over C2 Channel	Data Manipulation (3)
Gather Victim Org Information (4)	Develop Capabilities (4)	Hardware Additions	ESXi Administration Command	Cloud Application Integration	Boot or Logon Initialization Scripts (5)	Debugger Evasion	Forced Authentication	Cloud Service Dashboard	Remote Services (8)	Browser Session Hijacking	Data Obfuscation (3)	Exfiltration Over Other Network Medium (1)	Defacement (2)
Phishing for Information (4)	Establish Accounts (3)	Phishing (4)	Exploitation for Client Execution	Compromise Host Software Binary	Create or Modify System Process (5)	Deobfuscate/Decode Files or Information	Forge Web Credentials (2)	Cloud Service Discovery	Replication Through Removable Media	Clipboard Data	Dynamic Resolution (3)	Exfiltration Over Physical Medium (1)	Disk Wipe (2)
Search Closed Sources (2)	Obtain Capabilities (7)	Replication Through Removable Media	Input Injection	Create Account (3)	Domain or Tenant Policy Modification (2)	Deploy Container	Input Capture (4)	Cloud Storage Object Discovery	Software Deployment Tools	Data from Cloud Storage	Encrypted Channel (2)	Exfiltration Over Web Service (4)	Email Bombing
Search Open Technical Databases (5)	Stage Capabilities (6)	Supply Chain Compromise (3)	Inter-Process Communication (3)	Create or Modify System Process (5)	Escape to Host	Direct Volume Access	Modify Authentication Process (9)	Container and Resource Discovery	Taint Shared Content	Data from Configuration Repository (2)	Fallback Channels	Scheduled Transfer	Endpoint Denial of Service (4)
Search Open Websites/Domains (3)		Trusted Relationship	Native API	Event Triggered Execution (17)	Event Triggered Execution (17)	Domain or Tenant Policy Modification (2)	Multi-Factor Authentication Interception	Debugger Evasion	Use Alternate Authentication Material (4)	Data from Information Repositories (5)	Hide Infrastructure	Transfer Data to Cloud Account	Financial Theft
Search Victim-Owned Websites		Valid Accounts (4)	Scheduled Task/Job (5)	Exclusive Control	Exploitation for Privilege Escalation	Email Spoofing	Multi-Factor Authentication Request Generation	Device Driver Discovery		Data from Local System	Ingress Tool Transfer		Firmware Corruption
		Wi-Fi Networks	Serverless Execution	External Remote Services	Hijack Execution Flow (12)	Execution Guardrails (2)	Network Sniffing	Domain Trust Discovery		Data from Network Shared Drive	Multi-Stage Channels		Inhibit System Recovery
			Shared Modules	Hijack Execution Flow (12)	Process Injection (12)	Exploitation for Defense Evasion	OS Credential Dumping (8)	File and Directory Discovery		Data from Removable Media	Non-Application Layer Protocol		Network Denial of Service (2)
			Software Deployment Tools	Implant Internal Image	Scheduled Task/Job (5)	File and Directory Permissions Modification (2)	Steal Application Access Token	Group Policy Discovery		Data Staged (2)	Non-Standard Port		Resource Hijacking (4)
			System Services (3)	Modify Authentication Process (9)	Valid Accounts (4)	Hide Artifacts (14)	Steal or Forge Authentication Certificates	Log Enumeration		Email Collection (3)	Protocol Tunneling		Service Stop
			User Execution (4)	Modify Registry		Hijack Execution Flow (12)	Steal or Forge Kerberos Tickets (5)	Network Service Discovery		Input Capture (4)	Proxy (4)		System Shutdown/Reboot
			Windows Management Instrumentation	Office Application Startup (6)		Impair Defenses (11)	Steal Web Session Cookie	Network Share Discovery		Screen Capture	Remote Access Tools (3)		
				Power Settings		Impersonation	Unsecured Credentials (8)	Network Sniffing		Video Capture	Traffic Signaling (2)		
				Pre-OS Boot (5)		Indicator Removal (10)		Password Policy Discovery			Web Service (3)		
				Scheduled Task/Job (5)		Indirect Command Execution		Peripheral Device Discovery					
				Server Software Component (6)		Masquerading (11)		Permission Groups Discovery (3)					
				Software Extensions (2)		Modify Authentication Process (9)		Process Discovery					
				Traffic Signaling (2)		Modify Cloud Compute Infrastructure (5)		Query Registry					
				Valid Accounts (4)		Modify Cloud Resource Hierarchy		Remote System Discovery					
						Modify Registry		Software Discovery (1)					

MITRE ATT&CK 구성



Brute Force

Sub-techniques (4)

ID	Name
T1110.001	Password Guessing
T1110.002	Password Cracking
T1110.003	Password Spraying
T1110.004	Credential Stuffing

Adversaries may use brute force techniques to gain access to accounts when passwords are unknown or when password hashes are obtained.[1] Without knowledge of the password for an account or set of accounts, an adversary may systematically guess the password using a repetitive or iterative mechanism.[2] Brute forcing passwords can take place via interaction with a service that will check the validity of those credentials or offline against previously acquired credential data, such as password hashes.

Brute forcing credentials may take place at various points during a breach. For example, adversaries may attempt to brute force access to Valid Accounts within a victim environment leveraging knowledge gathered from other post-compromise behaviors such as OS Credential Dumping, Account Discovery, or Password Policy Discovery. Adversaries may also combine brute forcing activity with behaviors such as External Remote Services as part of Initial Access.

ID: T1110

Sub-techniques: T1110.001, T1110.002, T1110.003, T1110.004

ⓘ Tactic: Credential Access

ⓘ Platforms: Containers, ESXi, IaaS, Identity Provider, Linux, Network Devices, Office Suite, SaaS, Windows, macOS

Contributors: Alfredo Oliveira, Trend Micro; David Fiser, @anu4is, Trend Micro; Ed Williams, Trustwave, SpiderLabs; Magno Logan, @magnologan, Trend Micro; Mohamed Kmal; Yossi Weizman, Azure Defender Research Team

Version: 2.7

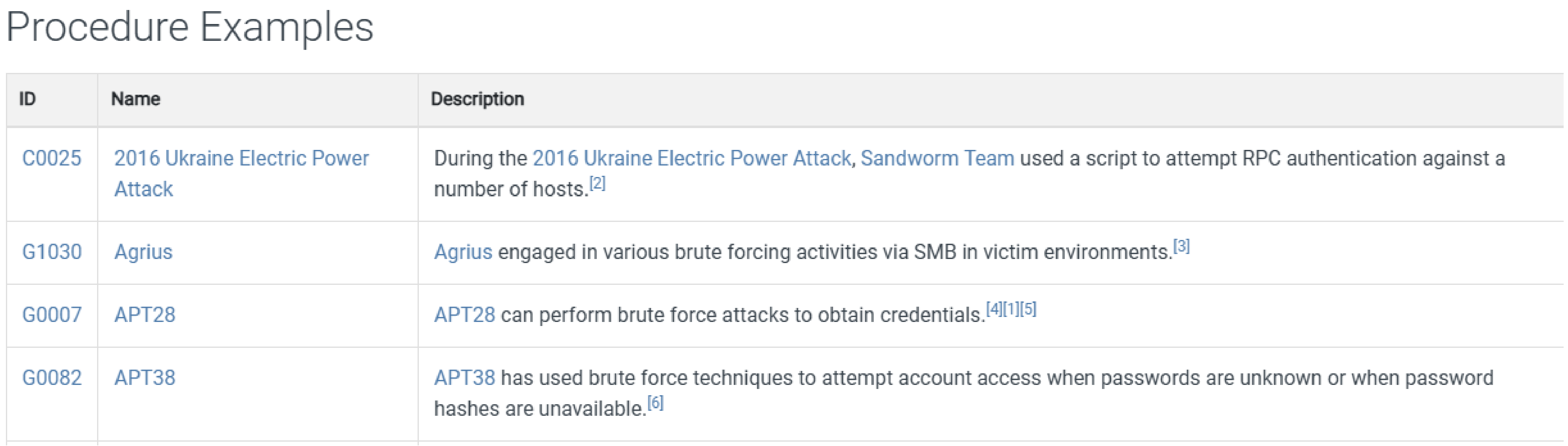
Created: 31 May 2017

Last Modified: 15 April 2025

Version Permalink

MITRE ATT&CK 프레임워크 이해

MITRE ATT&CK 구성

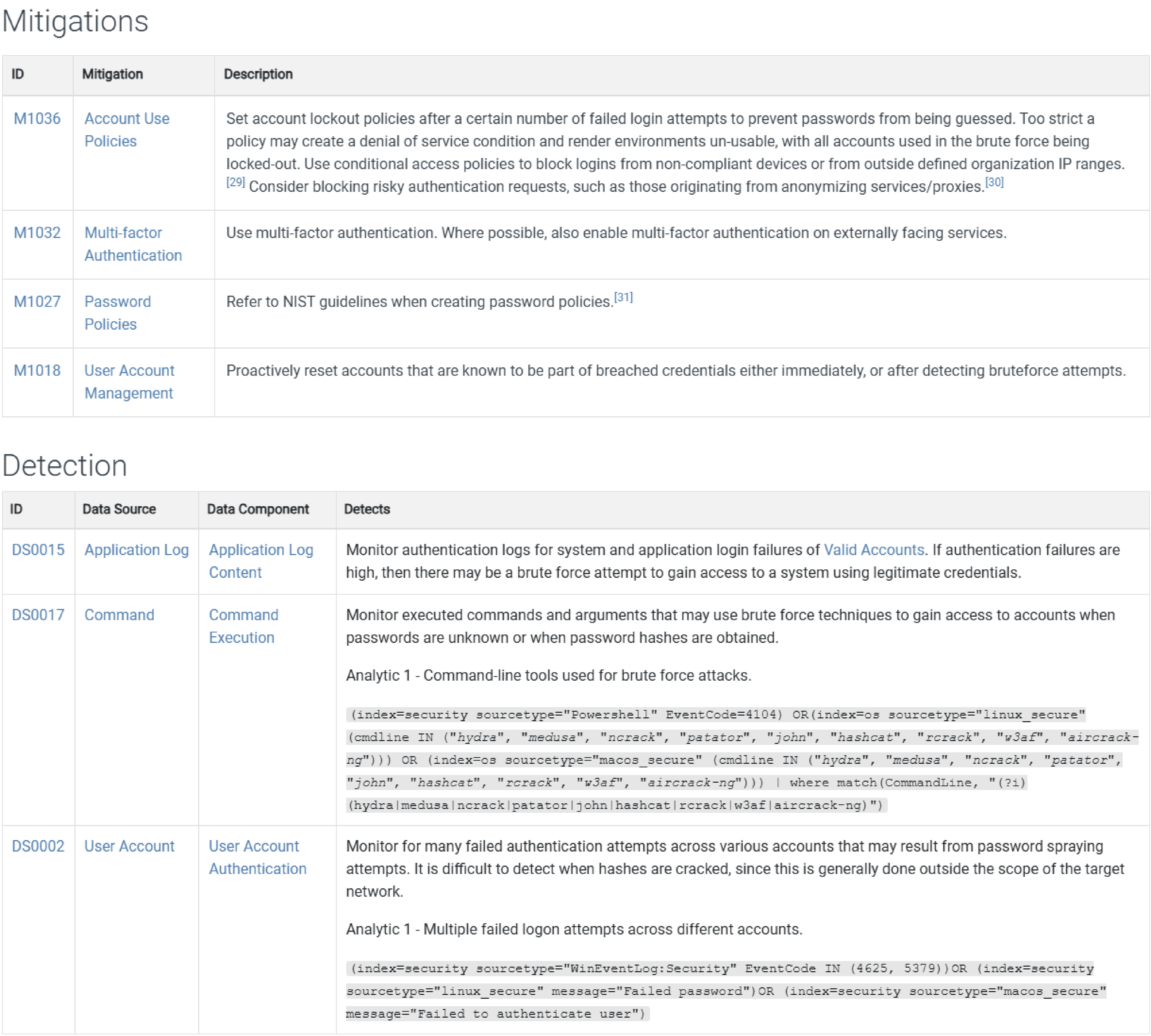


Procedure Examples

ID	Name	Description
C0025	2016 Ukraine Electric Power Attack	During the 2016 Ukraine Electric Power Attack, Sandworm Team used a script to attempt RPC authentication against a number of hosts.[2]
G1030	Agrius	Agrius engaged in various brute forcing activities via SMB in victim environments.[3]
G0007	APT28	APT28 can perform brute force attacks to obtain credentials.[4][1][5]
G0082	APT38	APT38 has used brute force techniques to attempt account access when passwords are unknown or when password hashes are unavailable.[6]

MITRE ATT&CK 프레임워크 이해

MITRE ATT&CK 구성



Mitigations

ID	Mitigation	Description
M1036	Account Use Policies	Set account lockout policies after a certain number of failed login attempts to prevent passwords from being guessed. Too strict a policy may create a denial of service condition and render environments un-usable, with all accounts used in the brute force being locked-out. Use conditional access policies to block logins from non-compliant devices or from outside defined organization IP ranges.[29] Consider blocking risky authentication requests, such as those originating from anonymizing services/proxies.[30]
M1032	Multi-factor Authentication	Use multi-factor authentication. Where possible, also enable multi-factor authentication on externally facing services.
M1027	Password Policies	Refer to NIST guidelines when creating password policies.[31]
M1018	User Account Management	Proactively reset accounts that are known to be part of breached credentials either immediately, or after detecting bruteforce attempts.

Detection

ID	Data Source	Data Component	Detects
DS0015	Application Log	Application Log Content	Monitor authentication logs for system and application login failures of Valid Accounts. If authentication failures are high, then there may be a brute force attempt to gain access to a system using legitimate credentials.
DS0017	Command	Command Execution	Monitor executed commands and arguments that may use brute force techniques to gain access to accounts when passwords are unknown or when password hashes are obtained. Analytic 1 - Command-line tools used for brute force attacks. `(index=security sourcetype="Powershell" EventCode=4104) OR(index=os sourcetype="linux_secure" (cmdline IN ("hydra", "medusa", "ncrack", "patator", "john", "hashcat", "rcrack", "w3af", "aircrack-ng"))) OR (index=os sourcetype="macos_secure" (cmdline IN ("hydra", "medusa", "ncrack", "patator", "john", "hashcat", "rcrack", "w3af", "aircrack-ng"))) | where match(CommandLine, "(?i)(hydra|medusa|ncrack|patator|john|hashcat|rcrack|w3af|aircrack-ng)")`
DS0002	User Account	User Account Authentication	Monitor for many failed authentication attempts across various accounts that may result from password spraying attempts. It is difficult to detect when hashes are cracked, since this is generally done outside the scope of the target network. Analytic 1 - Multiple failed logon attempts across different accounts. `(index=security sourcetype="WinEventLog:Security" EventCode IN (4625, 5379))OR (index=security sourcetype="linux_secure" message="Failed password")OR (index=security sourcetype="macos_secure" message="Failed to authenticate user")`