

真實風險與 ATT&CK 的鴻溝

翁浩正 (Allen Own)

戴夫寇爾股份有限公司

allenown@devco.re

2022.09.22 iThome CYBERSEC

講者簡介

翁浩正 (Allen Own)

戴夫寇爾 DEVCORE 執行長

台灣駭客協會 HITCON 理事長

TiEA 協會理事及資安小組負責人

allenown@devco.re

專長：駭客攻擊手法分析、紅隊演練



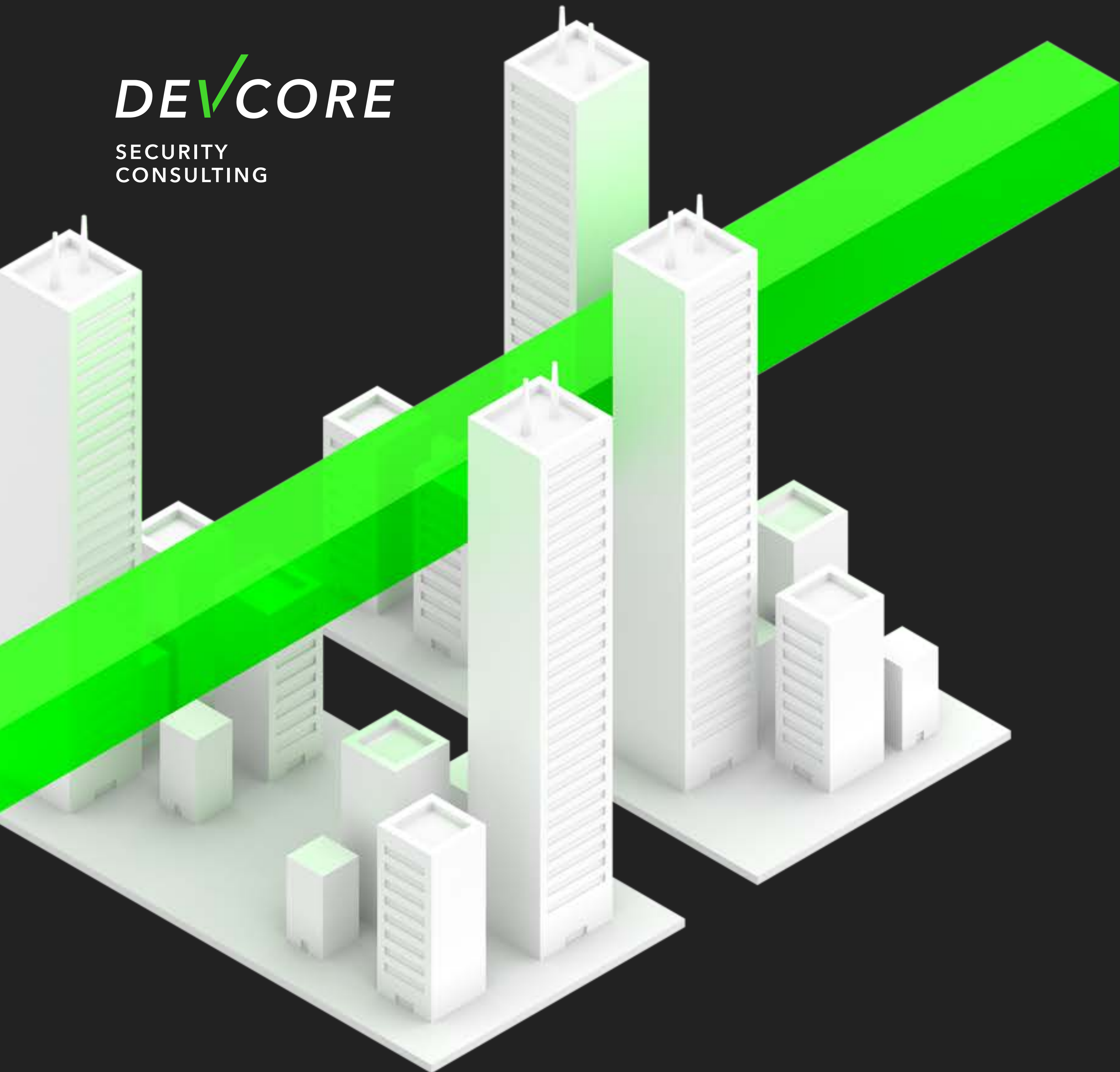
你面對的是駭客，我們也是

主動出擊、知己知彼
聚焦威脅、防範未然

RED TEAM ASSESSMENT
BROKEN ACCESS CONTROL
SECURITY MISCONFIGURATION
OPERATION PROXY LOGON
HACKER MINDSET
PENETRATION (TEST)
MAN IN THE MIDDLE
LATERAL MOVEMENT
STACK SMASHING
PROCESS INJECTION
BUFFER OVERFLOW
USE AFTER FREE
BUG BOUNTY
HEAD SPRAY
INJECTION
META-PROGRAMMING
CROSS-SITE SCRIPTING
PAST THE TICKET
PRIVILEGE ESCALATION
XXE
CREDENTIAL STUFFING

DEV✓CORE





DEVCORE 成立於 2012 年，團隊由**具備駭客思維及技巧的專家組成**。專注於**世界級攻擊手法研究**，具豐富的檢測及真實資安風險評估經驗。以對資安的熱情與專業，為企業建立堅強的資安後盾。

- 國內紅隊演練及滲透測試領導廠商
- 客製化攻擊工具的能力
- 發現世界級產品 0-day 漏洞能力
- 熟悉最新的攻擊技巧

獎項與研究成果

10 項 國際肯定

2021 Pwn2Own Austin 亞軍
2021 Pwnie Award (Best Server-side Bug)
2021 Pwn2Own Vancouver 冠軍
2021 Top 10 Web Hacking Techniques #3
2020 Pwn2Own Tokyo 亞軍
2020 Top 10 Web Hacking Techniques #7
2019 Pwnie Awards (Best Server-side Bug)
2019 Top 10 Web Hacking Techniques #4 & #8
2018 Top 10 Web Hacking Techniques #1
2017 Top 10 Web Hacking Techniques #1

130+ 個 漏洞揭露

超過 30 種產品類型，
包含最企業常使用的
Microsoft Exchange、
Pulse Secure、Fortinet、
Palo Alto、Jenkins、
Mail2000、Synology、
HiNet GPON 數據機

30+ 場 國際研討會

Black Hat USA
DEF CON
Black Hat Asia
Red Team Summit
CODE BLUE
HITB
HITCON

25+ 次 漏洞獎金計畫

Amazon
Facebook
Microsoft
GitHub
Google
LINE
Twitter
Uber

2021 年最常被利用的15 個漏洞



Communications Security Establishment
Canadian Centre for Cyber Security

Centre de la sécurité des télécommunications
Centre canadien pour la cybersécurité



GOVERNMENT COMMUNICATIONS SECURITY BUREAU
TE TIRA TIAKI



National Cyber Security Centre
a part of GCHQ

CVE	Vulnerability Name	Vendor and Product	Type
CVE-2021-44228	Log4Shell	Apache Log4j	Remote code execution (RCE)
CVE-2021-40539		Zoho ManageEngine AD SelfService Plus	RCE
CVE-2021-34523	ProxyShell	Microsoft Exchange Server	Elevation of privilege
CVE-2021-34473	ProxyShell	Microsoft Exchange Server	RCE
CVE-2021-31207	ProxyShell	Microsoft Exchange Server	Security feature bypass
CVE-2021-27065	ProxyLogon	Microsoft Exchange Server	RCE
CVE-2021-26858	ProxyLogon	Microsoft Exchange Server	RCE
CVE-2021-26857	ProxyLogon	Microsoft Exchange Server	RCE
CVE-2021-26855	ProxyLogon	Microsoft Exchange Server	RCE
CVE-2021-26084		Atlassian Confluence Server and Data Center	Arbitrary code execution
CVE-2021-21972		VMware vSphere Client	RCE
CVE-2020-1472	ZeroLogon	Microsoft Netlogon Remote Protocol (MS-NRPC)	Elevation of privilege
CVE-2020-0688		Microsoft Exchange Server	RCE
CVE-2019-11510		Pulse Secure Pulse Connect Secure	Arbitrary file reading
CVE-2018-13379		Fortinet FortiOS and FortiProxy	Path traversal

2021 年最常被利用的15 個漏洞



Communications Security Establishment
Canadian Centre for Cyber Security

Centre de la sécurité des télécommunications
Centre canadien pour la cybersécurité



GOVERNMENT COMMUNICATIONS SECURITY BUREAU
TE TIRA TIAKI



National Cyber Security Centre
a part of GCHQ

CVE	Vulnerability Name	Vendor and Product	Type
CVE-2021-44228	Log4Shell	Apache Log4j	Remote code execution (RCE)
CVE-2021-40539		Zoho ManageEngine AD SelfService Plus	RCE
CVE-2021-34523	ProxyShell	Microsoft Exchange Server	Elevation of privilege
CVE-2021-34473	ProxyShell	Microsoft Exchange Server	RCE
CVE-2021-31207	ProxyShell	Microsoft Exchange Server	Security feature bypass
CVE-2021-27065	ProxyLogon	Microsoft Exchange Server	RCE
CVE-2021-26858	ProxyLogon	Microsoft Exchange Server	RCE
CVE-2021-26857	ProxyLogon	Microsoft Exchange Server	RCE
CVE-2021-26855	ProxyLogon	Microsoft Exchange Server	RCE
CVE-2021-26084		Atlassian Confluence Server and Data Center	Arbitrary code execution
CVE-2021-21972		VMware vSphere Client	RCE
CVE-2020-1472	ZeroLogon	Microsoft Netlogon Remote Protocol (MS-NRPC)	Elevation of privilege
CVE-2020-0688		Microsoft Exchange Server	RCE
CVE-2019-11510		Pulse Secure Pulse Connect Secure	Arbitrary file reading
CVE-2018-13379		Fortinet FortiOS and FortiProxy	Path traversal

客戶實績

高科技製造業

全球前五大半導體製造廠
全球前五大半導體設計廠
全球前五大半導體封測廠
電腦及週邊設備業

政府機關

總統府
衛生福利部
交通部
中央健康保險署
台北市政府

金融服務業

兆豐國際商業銀行
臺灣證券交易所
國泰世華商業銀行
國泰人壽保險
臺灣證券交易所

重要產業

交通運輸
電子商務
醫療衛生
新創產業

如何正確使用紅隊演練

ATT&CK 簡述

怎麼使用 ATT&CK

ATT&CK 的誤區

Case Studies

如何正確使用紅隊演練

ATT&CK 簡述

怎麼使用 ATT&CK

ATT&CK 的誤區

Case Studies

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact	
Drive-by Compromise	Scheduled Task		Binary Padding		Network Sniffing		AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Data Destruction	
Exploit Public-Facing Application	Launchctl	Access Token Manipulation		Account Manipulation	Account Discovery	Application Window Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed	Data Encrypted for Impact	
	Local Job Scheduling		Bypass User Account Control	Bash History	Brute Force		Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Connection Proxy	Data Encrypted	Defacement
External Remote Services	LSASS Driver		Extra Window Memory Injection			Credential Dumping			Credentials in Files		Exploitation of Remote Services	Data from Information Repositories
Hardware Additions	Trap		Process Injection		Credentials in Registry	Domain Trust Discovery	File and Directory Discovery	Data from Local System	Custom Cryptographic Protocol	Exfiltration Over Other Network Medium		Disk Structure Wipe
Replication Through Removable Media	AppleScript	DLL Search Order Hijacking		Image File Execution Options Injection		Exploitation for Credential Access		Logon Scripts	Data from Network Shared Drive	Exfiltration Over Command and Control Channel	Exfiltration Over Command and Control Channel	Endpoint Denial of Service
Spearphishing Attachment	Command-Line Interface	Plist Modification		Valid Accounts		Forced Authentication	Network Service Scanning	Data from Removable Media	Data Encoding		Exfiltration Over Alternative Protocol	Network Denial of Service
Spearphishing Link	Compiled HTML File	Accessibility Features		BITS Jobs		Hooking	Network Share Discovery	Data Staged	Data Obfuscation	Exfiltration Over Physical Medium	Resource Hijacking	
Spearphishing via Service	Control Panel Items	AppCert DLLs		Clear Command History	CMSTP	Input Capture	Password Policy Discovery	Email Collection	Domain Fronting		Exfiltration Over Physical Medium	Runtime Data Manipulation
Supply Chain Compromise	Dynamic Data Exchange	AppInit DLLs		Code Signing		Input Prompt	Peripheral Device Discovery	Input Capture	Domain Generation Algorithms	Scheduled Transfer	Service Stop	
Trusted Relationship	Execution through API	Application Shimming		Compiled HTML File	Component Firmware	Kerberoasting	Process Discovery	Man in the Browser	Fallback Channels		Stored Data Manipulation	Transmitted Data Manipulation
Valid Accounts	Execution through Module Load	Dylib Hijacking		Component Object Model Hijacking		Keychain	Query Registry	Screen Capture	Multiband Communication	Multi-hop Proxy		Multilayer Encryption
		File System Permissions Weakness		Control Panel Items		LLMNR/NBT-NS Poisoning and Relay	Remote System Discovery	SSH Hijacking	Video Capture		Multi-Stage Channels	
Graphical User Interface	Launch Daemon	Hooking		DCShadow		Private Keys	Security Software Discovery	Taint Shared Content	Port Knocking	Remote Access Tools	Remote File Copy	
		New Service		Deobfuscate/Decode Files or Information		Two-Factor Authentication Interception	System Information Discovery	Third-party Software	Remote File Copy	Standard Application Layer Protocol	Standard Cryptographic Protocol	Standard Non-Application Layer Protocol
Mshta	Path Interception		Disabling Security Tools		Securityd Memory		System Network Configuration Discovery	Windows Admin Shares	Standard Application Layer Protocol	Uncommonly Used Port	Web Service	
PowerShell	Port Monitors		DLL Side-Loading		Two-Factor Authentication Interception		System Network Connections Discovery	Windows Remote Management	Standard Application Layer Protocol	Uncommonly Used Port	Web Service	
Regsvcs/Regasm	Service Registry Permissions Weakness		Execution Guardrails		Two-Factor Authentication Interception		System Owner/User Discovery	Windows Remote Management	Standard Application Layer Protocol	Uncommonly Used Port	Web Service	
Regsvr32	Setuid and Setgid		Exploitation for Privilege Escalation		Two-Factor Authentication Interception		System Service Discovery	Windows Remote Management	Standard Application Layer Protocol	Uncommonly Used Port	Web Service	
Rundll32	Startup Items		File Deletion		Two-Factor Authentication Interception		System Time Discovery	Windows Remote Management	Standard Application Layer Protocol	Uncommonly Used Port	Web Service	
Scripting	Web Shell		File Permissions Modification		Two-Factor Authentication Interception		Virtualization/Sandbox Evasion	Windows Remote Management	Standard Application Layer Protocol	Uncommonly Used Port	Web Service	
Service Execution	.bash_profile and .bashrc	Sudo		File System Logical Offsets		Two-Factor Authentication Interception		Windows Remote Management	Standard Application Layer Protocol	Uncommonly Used Port	Web Service	
Signed Binary Proxy Execution	Account Manipulation	Sudo Caching		Gatekeeper Bypass		Two-Factor Authentication Interception		Windows Remote Management	Standard Application Layer Protocol	Uncommonly Used Port	Web Service	
Signed Script Proxy Execution	Authentication Package	Sudo Caching		Group Policy Modification		Two-Factor Authentication Interception		Windows Remote Management	Standard Application Layer Protocol	Uncommonly Used Port	Web Service	
Source	BITS Jobs		Hidden Files and Directories		Hidden Users		Two-Factor Authentication Interception		Windows Remote Management	Standard Application Layer Protocol	Uncommonly Used Port	Web Service
	Bootkit		Hidden Window		HISTCONTROL		Two-Factor Authentication Interception		Windows Remote Management	Standard Application Layer Protocol	Uncommonly Used Port	Web Service
Space after Filename	Browser Extensions		Indicator Removal from Tools		Indicator Removal on Host		Two-Factor Authentication Interception		Windows Remote Management	Standard Application Layer Protocol	Uncommonly Used Port	Web Service
Third-party Software	Change Default File Association		Indirect Command Execution		Install Root Certificate		Two-Factor Authentication Interception		Windows Remote Management	Standard Application Layer Protocol	Uncommonly Used Port	Web Service
Trusted Developer Utilities	Component Firmware		Install Root Certificate		InstallUtil		Two-Factor Authentication Interception		Windows Remote Management	Standard Application Layer Protocol	Uncommonly Used Port	Web Service
User Execution	Component Object Model Hijacking		InstallUtil		Launchctl		Two-Factor Authentication Interception		Windows Remote Management	Standard Application Layer Protocol	Uncommonly Used Port	Web Service
Windows Management Instrumentation	Create Account		Launchctl		LC_MAIN Hijacking		Two-Factor Authentication Interception		Windows Remote Management	Standard Application Layer Protocol	Uncommonly Used Port	Web Service
Windows Remote Management	External Remote Services		LC_MAIN Hijacking		Masquerading		Two-Factor Authentication Interception		Windows Remote Management	Standard Application Layer Protocol	Uncommonly Used Port	Web Service
XSL Script Processing	Hidden Files and Directories		Masquerading		Modify Registry		Two-Factor Authentication Interception		Windows Remote Management	Standard Application Layer Protocol	Uncommonly Used Port	Web Service
	Hypervisor		Modify Registry		Mshta		Two-Factor Authentication Interception		Windows Remote Management	Standard Application Layer Protocol	Uncommonly Used Port	Web Service
	Kernel Modules and Extensions		Network Share Connection Removal		NTFS File Attributes		Two-Factor Authentication Interception		Windows Remote Management	Standard Application Layer Protocol	Uncommonly Used Port	Web Service
	Launch Agent		Obfuscated Files or Information		Obfuscated Files or Information		Two-Factor Authentication Interception		Windows Remote Management	Standard Application Layer Protocol	Uncommonly Used Port	Web Service
	LC_LOAD_DYLIB Addition		Port Knocking		Port Knocking		Two-Factor Authentication Interception		Windows Remote Management	Standard Application Layer Protocol	Uncommonly Used Port	Web Service
	Login Item		Process Doppelgänger		Process Doppelgänger		Two-Factor Authentication Interception		Windows Remote Management	Standard Application Layer Protocol	Uncommonly Used Port	Web Service
	Logon Scripts		Process Hollowing		Process Hollowing		Two-Factor Authentication Interception		Windows Remote Management	Standard Application Layer Protocol	Uncommonly Used Port	Web Service
	Modify Existing Service		Redundant Access		Redundant Access		Two-Factor Authentication Interception		Windows Remote Management	Standard Application Layer Protocol	Uncommonly Used Port	Web Service
	Netsh Helper DLL		Regsvcs/Regasm		Regsvcs/Regasm		Two-Factor Authentication Interception		Windows Remote Management	Standard Application Layer Protocol	Uncommonly Used Port	Web Service
	Office Application Startup		Regsvr32		Regsvr32		Two-Factor Authentication Interception		Windows Remote Management	Standard Application Layer Protocol	Uncommonly Used Port	Web Service
	Port Knocking		Rootkit		Rootkit		Two-Factor Authentication Interception		Windows Remote Management	Standard Application Layer Protocol	Uncommonly Used Port	Web Service
	Rc.common		Rundll32		Rundll32		Two-Factor Authentication Interception		Windows Remote Management	Standard Application Layer Protocol	Uncommonly Used Port	Web Service
	Redundant Access		Scripting		Scripting		Two-Factor Authentication Interception		Windows Remote Management	Standard Application Layer Protocol	Uncommonly Used Port	Web Service
	Registry Run Keys / Startup Folder		Signed Binary Proxy Execution		Signed Binary Proxy Execution		Two-Factor Authentication Interception		Windows Remote Management	Standard Application Layer Protocol	Uncommonly Used Port	Web Service
	Re-opened Applications		Signed Script Proxy Execution		Signed Script Proxy Execution		Two-Factor Authentication Interception		Windows Remote Management	Standard Application Layer Protocol	Uncommonly Used Port	Web Service
	Screensaver		SIP and Trust Provider Hijacking		SIP and Trust Provider Hijacking		Two-Factor Authentication Interception		Windows Remote Management	Standard Application Layer Protocol	Uncommonly Used Port	Web Service
	Security Support Provider		Software Packing		Software Packing		Two-Factor Authentication Interception		Windows Remote Management	Standard Application Layer Protocol	Uncommonly Used Port	Web Service
	Shortcut Modification		Space after Filename		Space after Filename		Two-Factor Authentication Interception		Windows Remote Management	Standard Application Layer Protocol	Uncommonly Used Port	Web Service
	SIP and Trust Provider Hijacking		Template Injection		Template Injection		Two-Factor Authentication Interception		Windows Remote Management	Standard Application Layer Protocol	Uncommonly Used Port	Web Service
	System Firmware		Timestamp		Timestamp		Two-Factor Authentication Interception		Windows Remote Management	Standard Application Layer Protocol	Uncommonly Used Port	Web Service
	Systemd Service		Trusted Developer Utilities		Trusted Developer Utilities		Two-Factor Authentication Interception		Windows Remote Management	Standard Application Layer Protocol	Uncommonly Used Port	Web Service
	Time Providers		Virtualization/Sandbox Evasion		Virtualization/Sandbox Evasion		Two-Factor Authentication Interception		Windows Remote Management	Standard Application Layer Protocol	Uncommonly Used Port	Web Service
	Windows Management Instrumentation Event Subscription		Web Service		Web Service		Two-Factor Authentication Interception		Windows Remote Management	Standard Application Layer Protocol	Uncommonly Used Port	Web Service
	Winlogon Helper DLL		XSL Script Processing		XSL Script Processing		Two-Factor Authentication Interception		Windows Remote Management	Standard Application Layer Protocol	Uncommonly Used Port	Web Service

MITRE ATT&CK™ Enterprise Framework

attack.mitre.org

MITRE

ATT&CK[®]

Adversarial Tactics, Techniques, and Common Knowledge

<https://attack.mitre.org/>

Reconnaissance 10 techniques	Resource Development 6 techniques	Initial Access 9 techniques	Execution 10 techniques	Persistence 18 techniques	Privilege Escalation 12 techniques	Defense Evasion 37 techniques	Credential Access 15 techniques	Discovery 25 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 16 techniques	Exfiltration 9 techniques	Impact 13 techniques
Active Scanning (2)	Acquire Infrastructure (6)	Drive-by Compromise	Command and Scripting Interpreter (8)	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 (1)	Account Access Removal
Gather Victim Host Information (4)	Compromise Accounts (2)	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
Gather Victim Identity Information (3)	Compromise Infrastructure (6)	External Remote Services	Inter-Process Communication (2)	Boot or Logon Autostart Execution (12)	Boot or Logon Autostart Execution (12)	BITS Jobs	Exploitation for Credential Access	Browser Bookmark Discovery	Lateral Tool Transfer	Automated Collection	Data Encoded (2)	Exfiltration Over Alternative Protocol (3)	Data Encrypted for Impact
Gather Victim Network Information (6)	Develop Capabilities (4)	Hardware Additions	Native API	Boot or Logon Initialization Scripts (5)	Boot or Logon Autostart Execution (12)	Deobfuscate/Decode Files or Information	Forced Authentication	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Clipboard Data	Data from Cloud Storage Object	Exfiltration Over C2 Channel	Data Manipulation (3)
Gather Victim Org Information (4)	Establish Accounts (2)	Phishing (3)	Scheduled Task/Job (6)	Browser Extensions	Boot or Logon Initialization Scripts (5)	Direct Volume Access	Forge Web Credentials (2)	Cloud Service Dashboard	Remote Services (6)	Data from Configuration Repository (2)	Data Obfuscation (3)	Exfiltration Over Other Network Medium (1)	Defacement (2)
Phishing for Information (3)	Obtain Capabilities (6)	Replication Through Removable Media	Shared Modules	Compromise Client Software Binary	Create or Modify System Process (4)	Domain Policy Modification (2)	Input Capture (4)	Cloud Service Discovery	Replication Through Removable Media	Data from Information Repositories (2)	Dynamic Resolution (3)	Exfiltration Over Physical Medium (1)	Disk Wipe (2)
Search Closed Sources (2)		Supply Chain Compromise (3)	Software Deployment Tools	Event Triggered Execution (15)	Domain Policy Modification (2)	Execution Guardrails (1)	Man-in-the-Middle (2)	Cloud Service Discovery	Software Deployment Tools	Data from Local System	Encrypted Channel (2)	Exfiltration Over Web Service (2)	Endpoint Denial of Service (4)
Search Open Technical Databases (5)		Trusted Relationship	System Services (2)	Create Account (3)	Event Triggered Execution (15)	Exploitation for Defense Evasion	Modify Authentication Process (4)	Domain Trust Discovery	Taint Shared Content	Data from Network Shared Drive	Fallback Channels	Firmware Corruption	Inhibit System Recovery
Search Open Websites/Domains (2)		Valid Accounts (4)	User Execution (2)	Create or Modify System Process (4)	Event Triggered Execution (15)	File and Directory Permissions Modification (2)	Network Sniffing	File and Directory Discovery	Use Alternate Authentication Material (4)	Data from Removable Media	Ingress Tool Transfer	Network Denial of Service (2)	Resource Hijacking
Search Victim-Owned Websites			Windows Management Instrumentation	Event Triggered Execution (15)	Exploitation for Privilege Escalation	Hide Artifacts (7)	OS Credential Dumping (8)	Network Service Scanning		Data from Removable Media	Multi-Stage Channels	Scheduled Transfer	Service Stop
				External Remote Services	Hijack Execution Flow (11)	Hijack Execution Flow (11)	Steal Application Access Token	Network Share Discovery		Data from Removable Media	Non-Application Layer Protocol	Transfer Data to Cloud Account	System Shutdown/Reboot
				Hijack Execution Flow (11)	Process Injection (11)	Hijack Execution Flow (11)	Steal or Forge Kerberos Tickets (4)	Network Sniffing		Data Staged (2)	Non-Standard Port		
				Implant Container Image	Scheduled Task/Job (6)	Impair Defenses (7)	Two-Factor Authentication Interception	Peripheral Device Discovery		Email Collection (3)	Protocol Tunneling		
				Office Application Startup (6)	Valid Accounts (4)	Indicator Removal on Host (6)	Unsecured Credentials (6)	Permission Groups Discovery (3)		Input Capture (4)	Proxy (4)		
				Pre-OS Boot (5)		Indirect Command Execution		Process Discovery		Man in the Browser	Remote Access Software		
				Scheduled Task/Job (6)		Masquerading (6)		Query Registry		Man-in-the-Middle (2)	Traffic Signaling (1)		
				Server Software Component (3)		Modify Authentication Process (4)		Remote System Discovery		Screen Capture	Web Service (3)		
				Traffic Signaling (1)		Modify Cloud Compute Infrastructure (4)		Software Discovery (1)		Video Capture			
				Valid Accounts (4)		Modify Registry		System Information Discovery					
						Modify System Image (2)		System Network Configuration Discovery					
						Network Boundary Bridging (1)		System Network Connections Discovery					
						Obfuscated Files or		System Owner/User Discovery					
								System Service Discovery					

Reconnaissance 10 techniques	Resource Development 6 techniques	Initial Access 9 techniques	Execution 10 techniques	Persistence 18 techniques	Privilege Escalation 12 techniques	Defense Evasion 37 techniques	Credential Access 15 techniques	Discovery 25 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 16 techniques	Exfiltration 9 techniques	Impact 13 techniques
Active Scanning (2)	Acquire Infrastructure (6)	Drive-by Compromise	Command and Scripting Interpreter (8)	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 (2)	Application Layer	Automated Exfiltration (2)	Account Access Removal
Gather Victim Host Information (4)	Compromise Accounts (2)	Exploit Public-Facing Application	Exploitation for Client Execution	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Credentials from Password Stores (3)	Exploitation for Credential Access					
Gather Victim Identity Information (3)	Compromise Infrastructure (6)	External Remote Services	Inter-Process Communication (2)	Boot or Logon Autostart Execution (12)	Boot or Logon Autostart Execution (12)	BITS Jobs	Exploitation for Credential Access	Forced Authentication					
Gather Victim Network Information (6)	Develop Capabilities (4)	Hardware Additions	Native API	Boot or Logon Initialization Scripts (5)	Boot or Logon Initialization Scripts (5)	Deobfuscate/Decode Files or Information	Forge Web Credentials (2)	Cloud Service Dashboard	Session Hijacking (2)	Data from Cloud Storage Object	Data Obfuscation (3)	Exfiltration Over C2 Channel	Defacement (2)
Gather Victim Org Information (4)	Establish Accounts (2)	Phishing (3)	Scheduled Task/Job (6)	Browser Extensions	Create or Modify System Process (4)	Domain Policy Modification (2)	Input Capture (4)	Cloud Service Discovery	Remote Services (6)	Data from Configuration Repository (2)	Dynamic Resolution (3)	Exfiltration Over Other Network Medium (1)	Disk Wipe (2)
Phishing for Information (3)	Obtain Capabilities (6)	Replication Through Removable Media	Shared Modules	Compromise Client Software Binary	Domain Policy Modification (2)	Execution Guardrails (1)	Man-in-the-Middle (2)	Domain Trust Discovery	Replication Through Removable Media	Data from Information Repositories (2)	Encrypted Channel (2)	Exfiltration Over Physical Medium (1)	Endpoint Denial of Service (4)
Search Closed Sources (2)		Supply Chain Compromise (3)	Software Deployment Tools	Create Account (3)	Event Triggered Execution (15)	Exploitation for Defense Evasion	Modify Authentication Process (4)	File and Directory Discovery	Software Deployment Tools	Data from Local System	Fallback Channels	Exfiltration Over Web Service (2)	Firmware Corruption
Search Open Technical Databases (5)		Trusted Relationship	System Services (2)	Create or Modify System Process (4)	File and Directory Permissions Modification (2)	File and Directory Permissions Modification (2)	Network Sniffing	Network Service Scanning	Taint Shared Content	Data from Network Shared Drive	Ingress Tool Transfer	Exfiltration Over Web Service (2)	Inhibit System Recovery
Search Open Websites/Domains (2)		Valid Accounts (4)	User Execution (2)	Event Triggered Execution (15)	Hijack Execution Flow (11)	Hide Artifacts (7)	OS Credential Dumping (8)	Network Share Discovery	Use Alternate Authentication Material (4)	Data from Removable Media	Multi-Stage Channels	Scheduled Transfer	Network Denial of Service (2)
Search Victim-Owned Websites			Windows Management Instrumentation	External Remote Services	Hijack Execution Flow (11)	Hijack Execution Flow (11)	Steal Application Access Token	Password Policy Discovery		Data from Removable Media	Non-Application Layer Protocol	Transfer Data to Cloud Account	Resource Hijacking
				Hijack Execution Flow (11)	Process Injection (11)	Impair Defenses (7)	Steal or Forge Kerberos Tickets (4)	Peripheral Device Discovery		Data Staged (2)	Non-Standard Port	Service Stop	System Shutdown/Reboot
				Implant Container Image	Scheduled Task/Job (6)	Indicator Removal on Host (6)	Steal Web Session Cookie	Permission Groups Discovery (3)		Email Collection (3)	Protocol Tunneling		
				Office Application Startup (6)	Valid Accounts (4)	Indirect Command Execution	Two-Factor Authentication Interception	Process Discovery		Input Capture (4)	Proxy (4)		
				Pre-OS Boot (5)		Masquerading (6)	Unsecured Credentials (6)	Query Registry		Man in the Browser	Remote Access Software		
				Scheduled Task/Job (6)		Modify Authentication Process (4)		Remote System Discovery		Man-in-the-Middle (2)	Traffic Signaling (1)		
				Server Software Component (3)		Modify Cloud Compute Infrastructure (4)		Software Discovery (1)		Screen Capture	Web Service (3)		
				Traffic Signaling (1)		Modify Registry		System Information Discovery		Video Capture			
				Valid Accounts (4)		Modify System Image (2)		System Network Configuration Discovery					
						Network Boundary Bridging (1)		System Network Connections Discovery					
						Obfuscated Files or		System Owner/User Discovery					
								System Service Discovery					

Tactics 攻擊者的戰略

Reconnaissance 10 techniques	Resource Development 6 techniques	Initial Access 9 techniques	Execution 10 techniques	Persistence 18 techniques	Privilege Escalation 12 techniques	Defense Evasion 37 techniques	Credential Access 15 techniques	Discovery 25 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 16 techniques	Exfiltration 9 techniques	Impact 13 techniques
Active Scanning (2)	Acquire Infrastructure (6)	Drive-by Compromise	Command and Scripting Interpreter (8)	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 (1)	Account Access Removal
Gather Victim Host Information (4)	Compromise Accounts (2)	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
Gather Victim Identity Information (3)	Compromise Infrastructure (6)	External Remote Services	Inter-Process Communication (2)	Boot or Logon Autostart Execution (12)	Boot or Logon Autostart Execution (12)	BITS Jobs	Exploitation for Credential Access	Browser Bookmark Discovery	Lateral Tool Transfer	Automated Collection	Clipboard Data	Exfiltration Over Alternative Protocol (3)	Data Encrypted for Impact
Gather Victim Network Information (6)	Develop Capabilities (4)	Hardware Additions	Native API	Boot or Logon Initialization Scripts (5)	Boot or Logon Initialization Scripts (5)	Deobfuscate/Decode Files or Information	Forced Authentication	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Data from Cloud Storage Object	Data Encoding (2)	Data Manipulation (3)	
Gather Victim Org Information (4)	Establish Accounts (2)	Phishing (3)	Scheduled Task/Job (6)	Browser Extensions	Domain Policy Modification (2)	Direct Volume Access	Forge Web Credentials (2)	Cloud Service Dashboard	Remote Services (6)	Data from Configuration Repository (2)	Data Obfuscation (3)	Exfiltration Over C2 Channel	Defacement (2)
Phishing for Information (3)	Obtain Capabilities (6)	Replication Through Removable Media	Shared Modules	Compromise Client Software Binary	Create or Modify System Process (4)	Execution Guardrails (1)	Input Capture (4)	Cloud Service Discovery	Replication Through Removable Media	Data from Information Repositories (2)	Dynamic Resolution (3)	Exfiltration Over Other Network Medium (1)	Disk Wipe (2)
Search Closed Sources (2)		Supply Chain Compromise (3)	Software Deployment Tools	Event Triggered Execution (15)	Domain Policy Modification (2)	Exploitation for Defense Evasion	Man-in-the-Middle (2)	Domain Trust Discovery	Software Deployment Tools	Data from Local System	Encrypted Channel (2)	Exfiltration Over Physical Medium (1)	Endpoint Denial of Service (4)
Search Open Technical Databases (5)		Trusted Relationship	System Services (2)	Create Account (3)	Event Triggered Execution (15)	File and Directory Permissions Modification (2)	Modify Authentication Process (4)	File and Directory Discovery	Taint Shared Content	Data from Network Shared Drive	Fallback Channels	Exfiltration Over Web Service (2)	Firmware Corruption
Search Open Websites/Domains (2)		Valid Accounts (4)	User Execution (2)	Create or Modify System Process (4)	Exploitation for Privilege Escalation	Hide Artifacts (7)	Network Sniffing	Network Service Scanning	Use Alternate Authentication Material (4)	Data from Removable Media	Ingress Tool Transfer	Exfiltration Over Web Service (2)	Inhibit System Recovery
Search Victim-Owned Websites		Windows Management Instrumentation	Windows Management Instrumentation	Event Triggered Execution (15)	Hijack Execution Flow (11)	Hijack Execution Flow (11)	OS Credential Dumping (8)	Network Share Discovery		Data from Removable Media	Multi-Stage Channels	Scheduled Transfer	Network Denial of Service (2)
				Event Triggered Execution (15)	Hijack Execution Flow (11)	Impair Defenses (7)	Steal Application Access Token	Network Sniffing		Data from Removable Media	Non-Application Layer Protocol	Transfer Data to Cloud Account	Resource Hijacking
				External Remote Services	Hijack Execution Flow (11)	Indicator Removal on Process (4)	Steal or Forge Kerberos Tickets (4)	Password Policy Discovery		Data Staged (2)	Non-Standard Port	Service Stop	System Shutdown/Reboot
				Hijack Execution Flow (11)	Process Injection (11)	Modify Cloud Compute Infrastructure (4)	Steal Web Session Cookie	Peripheral Device Discovery		Email Collection (3)	Protocol Tunneling		
						Modify Registry	Two-Factor Authentication Interception	Permission Groups Discovery (3)		Input Capture (4)	Proxy (4)		
						Modify System Image (2)	Unsecured Credentials (6)	Process Discovery		Man in the Browser	Remote Access Software		
						Network Boundary Bridging (1)		Query Registry		Man-in-the-Middle (2)	Traffic Signaling (1)		
						Obfuscated Files or		Remote System Discovery		Screen Capture	Web Service (3)		
								Software Discovery (1)		Video Capture			
								System Information Discovery					
								System Network Configuration Discovery					
								System Network Connections Discovery					
								System Owner/User Discovery					
								System Service Discovery					

Techniques 攻擊者的技術

Reconnaissance 10 techniques	Resource Development 6 techniques	Initial Access 9 techniques	Execution 10 techniques	Persistence 18 techniques	Privilege Escalation 12 techniques	Defense Evasion 37 techniques	Credential Access 15 techniques	Discovery 25 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 16 techniques	Exfiltration 9 techniques	Impact 13 techniques
Active Scanning (2) 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	Acquire Infrastructure (6) Compromise Accounts (2) Compromise Infrastructure (6) Develop Capabilities (4) Establish Accounts (2) Obtain Capabilities (6)	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)	Command and Scripting Interpreter (8) Exploitation for Client Execution Inter-Process Communication (2) Native API Scheduled Task/Job (6) Shared Modules Software Deployment Tools System Services (2) User Execution (2) Windows Management Instrumentation	Account Manipulation (4) BITS Jobs Boot or Logon Autostart Execution (12) 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 (11)	Abuse Elevation Control Mechanism (4) Access Token Manipulation (5) Boot or Logon Autostart Execution (12) Boot or Logon Initialization Scripts (5) Create or Modify System Process (4) Domain Policy Modification (2) Event Triggered Execution (15) Exploitation for Privilege Escalation Hijack Execution Flow (11) Process Injection (11)	Abuse Elevation Control Mechanism (4) Access Token Manipulation (5) BITS Jobs Deobfuscate/Decode Files or Information Direct Volume Access Domain Policy Modification (2) Execution Guardrails (1) Exploitation for Defense Evasion File and Directory Permissions Modification (2) Hide Artifacts (7) Hijack Execution Flow (11) Impair Defenses (7) Indicator Removal on Process (4) Modify Cloud Compute Infrastructure (4) Modify Registry Modify System Image (2) Network Boundary Bridging (1) Obfuscated Files or	Brute Force (4) Credentials from Password Stores (3) Exploitation for Credential Access Forced Authentication Forge Web Credentials (2) Input Capture (4) Man-in-the-Middle (2) Modify Authentication Process (4) Network Sniffing OS Credential Dumping (8) Steal Application Access Token Steal or Forge Kerberos Tickets (4) Steal Web Session Cookie Two-Factor Authentication Interception Unsecured Credentials (6)	Account Discovery (4) Cloud Service Dashboard Cloud Service Discovery Domain Trust Discovery File and Directory Discovery Network Service Scanning Network Share Discovery Network Sniffing Password Policy Discovery Peripheral Device Discovery Permission Groups Discovery (3) Process Discovery Query Registry Remote System Discovery Software Discovery (1) System Information Discovery System Network Configuration Discovery System Network Connections Discovery System Owner/User Discovery System Service Discovery	Exploitation of Remote Services Session Hijacking (2) Remote Services (6) Replication Through Removable Media Software Deployment Tools Taint Shared Content Use Alternate Authentication Material (4)	Archive Collected Data (6) Data from Cloud Storage Object Data from Configuration Repository (2) Data from Information Repositories (2) Data from Local System Data from Network Shared Drive Data from Removable Media Data Staged (2) Email Collection (3) Input Capture (4) Man in the Browser Man-in-the-Middle (2) Screen Capture Video Capture	Application Layer Data Obfuscation (3) Dynamic Resolution (3) Encrypted Channel (2) Fallback Channels Ingress Tool Transfer Multi-Stage Channels Non-Application Layer Protocol Non-Standard Port Protocol Tunneling Proxy (4) Remote Access Software Traffic Signaling (1) Web Service (3)	Automated Exfiltration (6) 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	Account Access Removal 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

Tactics 攻擊者的戰略

Techniques 攻擊者的技術

Reconnaissance 10 techniques	Resource Development 6 techniques	Initial Access 9 techniques	Execution 10 techniques	Persistence 18 techniques	Privilege Escalation 12 techniques	Defense Evasion 37 techniques	Credential Access 15 techniques	Discovery 25 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 16 techniques	Exfiltration 9 techniques	Impact 13 techniques
Active Scanning (2)	Acquire Infrastructure (6)	Drive-by Compromise	Command and Scripting Interpreter (8)	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 (1)	Account Access Removal
Gather Victim Host Information (4)	Compromise Accounts (2)	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
Gather Victim Identity Information (3)	Compromise Infrastructure (6)	External Remote Services	Inter-Process Communication (2)	Boot or Logon Autostart Execution (12)	Boot or Logon Autostart Execution (12)	BITS Jobs	Exploitation for Credential Access	Browser Bookmark Discovery	Lateral Tool Transfer	Automated Collection	Clipboard Data	Exfiltration Over Alternative Protocol (3)	Data Encrypted for Impact
Gather Victim Network Information (6)	Develop Capabilities (4)	Hardware Additions	Native API	Boot or Logon Initialization Scripts (5)	Boot or Logon Initialization Scripts (5)	Deobfuscate/Decode Files or Information	Forced Authentication	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Data from Cloud Storage Object	Data Encoding (2)	Exfiltration Over C2 Channel	Data Manipulation (3)
Gather Victim Org Information (4)	Establish Accounts (2)	Phishing (3)	Scheduled Task/Job (6)	Browser Extensions	Boot or Logon Initialization Scripts (5)	Direct Volume Access	Forge Web Credentials (2)	Cloud Service Dashboard	Remote Services (6)	Data from Configuration Repository (2)	Data Obfuscation (3)	Exfiltration Over Other Network Medium (1)	Defacement (2)
Phishing for Credentials		Replication Through Removable Media	Shared Modules	Compromise Client Software Binary	Create or Modify System Process (4)	Domain Policy Modification (2)	Execute	Cloud Service Discovery	Replication Through Removable Media	Data from Information Repositories (2)	Dynamic Resolution (3)	Exfiltration Over Physical Medium (1)	Disk Wipe (2)
Search Open Websites/Domains (2)		Supply Chain Compromise (3)	Software Deployment Tools	Create Account (3)	Domain Policy Modification (2)	Exploitation Evasion	File and Directory Permissions Modification (2)	Content Discovery	Software Deployment Tools	Data from Local System	Encrypted Channel (2)	Inhibit System Recovery	
Search Victim-Owned Websites		Trusted Relationship	User Execution (2)	Create or Modify System Process (4)	Event Triggered Execution (15)	Hide Artifacts (7)	Hijack Execution Flow (11)	Network Share Discovery	Taint Shared Content	Data from Network Shared Drive	Fallback Channels	Exfiltration Over Web Service (2)	Network Denial of Service (2)
		Valid Accounts (4)	Windows Management Instrumentation	Event Triggered Execution (15)	Exploitation for Privilege Escalation	Hijack Execution Flow (11)	Impair Defenses (7)	Network Sniffing	Use Alternate Authentication Material (4)	Data from Removable Media	Ingress Tool Transfer	Scheduled Transfer	Resource Hijacking
				External Remote Services	Hijack Execution Flow (11)	Indicator Removal on Host (6)	Indirect Command Execution	Password Policy Discovery		Data Staged (2)	Multi-Stage Channels	Transfer Data to Cloud Account	Service Stop
				Hijack Execution Flow (11)	Process Injection (11)	Indirect Command Execution	Masquerading (6)	Peripheral Device Discovery		Email Collection (3)	Non-Application Layer Protocol		System Shutdown/Reboot
				Implant Container Image	Scheduled Task/Job (6)	Modify Authentication Process (4)	Modify Cloud Compute Infrastructure (4)	Permission Groups Discovery (3)		Input Capture (4)	Non-Standard Port		
				Office Application Startup (6)	Valid Accounts (4)	Modify Cloud Compute Infrastructure (4)	Modify Registry	Process Discovery		Man in the Browser	Protocol Tunneling		
				Pre-OS Boot (5)		Modify Registry	Modify System Image (2)	Query Registry		Man-in-the-Middle (2)	Proxy (4)		
				Scheduled Task/Job (6)		Modify System Image (2)	Network Boundary Bridging (1)	Remote System Discovery		Screen Capture	Remote Access Software		
				Server Software Component (3)		Obfuscated Files or		Remote System Discovery		Video Capture	Traffic Signaling (1)		
				Traffic Signaling (1)				System Information Discovery			Web Service (3)		
				Valid Accounts (4)				System Network Configuration Discovery					
								System Network Connections Discovery					
								System Owner/User Discovery					
								System Service Discovery					

準備階段

入侵階段

影響

Enterprise Tactics

ID	Name	Description
TA004	Reconnaissance	Gather information they can use to plan future operations.
TA004	Resource Development	Establish resources they can use to support operations.
TA000	Initial Access	Get into your network.
TA000	Execution	Run malicious code.
TA000	Persistence	Maintain their foothold.
TA000	Privilege Escalation	Gain higher-level permissions.
TA000	Defense Evasion	Avoid being detected.
TA000	Credential Access	Steal account names and passwords.
TA000	Discovery	Figure out your environment.
TA000	Lateral Movement	Move through your environment.
TA000	Collection	Gather data of interest to their goal.
TA001	Command and Control	Communicate with compromised systems to control them.
TA001	Exfiltration	Steal data.
TA004	Impact	Manipulate, interrupt, or destroy your systems and data.

Enterprise Tactics

ID	Name	Description
TA004	Reconnaissance	Gather information they can use to plan future operations.
TA004	Resource Development	Establish resources they can use to support operations.
TA000	Initial Access	Get into your network .
TA000	Execution	Run malicious code .
TA000	Persistence	Maintain their foothold.
TA000	Privilege Escalation	Gain higher-level permissions .
TA000	Defense Evasion	Avoid being detected.
TA000	Credential Access	Steal account names and passwords.
TA000	Discovery	Figure out your environment .
TA000	Lateral Movement	Move through your environment.
TA000	Collection	Gather data of interest to their goal.
TA001	Command and Control	Communicate with compromised systems to control them.
TA001	Exfiltration	Steal data .
TA004	Impact	Manipulate, interrupt, or destroy your systems and data.

APT Groups

133 個 APT 組織的分析

<https://attack.mitre.org/groups/>

MITRE | ATT&CK®

Matrices Tactics Techniques Data Sources Mitigations Groups Software Resources Blog Contribute

Search

GROUPS

[Overview](#)

[admin@338](#)

[Ajax Security Team](#)

[ALLANITE](#)

[Andariel](#)

[APT-C-36](#)

[APT1](#)

[APT12](#)

[APT16](#)

[APT17](#)

[APT18](#)

[APT19](#)

[APT28](#)

[APT29](#)

[APT3](#)

[APT30](#)

[APT32](#)

Home > Groups

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.

GROUPS

- menuPass
- Moafee
- Mofang
- Molerats
- MuddyWater
- Mustang Panda
- Naikon
- NEODYMIUM
- Night Dragon
- Nomadic Octopus
- OilRig
- Operation Wocao
- Orangeworm
- Patchwork
- PittyTiger
- PLATINUM
- Recon Group

Home > Groups > menuPass

menuPass

menuPass is a threat group that has been active since at least 2006. Individual members of menuPass are known to have acted in association with the Chinese Ministry of State Security's (MSS) Tianjin State Security Bureau and worked for the Huaying Haitai Science and Technology Development Company.^{[1][2]}

menuPass has targeted healthcare, defense, aerospace, finance, maritime, biotechnology, energy, and government sectors globally, with an emphasis on Japanese organizations. In 2017, the group is known to have targeted managed IT service providers (MSPs), manufacturing and mining companies, and a university.^{[3][4][5][6][7][1][2]}

APT 10 分析

ID: G0045
 ⓘ Associated Groups: Cicada, POTASSIUM, Stone Panda, APT10, Red Apollo, CVNX, HOGFISH

APT 組織分析，包含攻擊手法、戰略、工具方式。

Contributors: Edward Millington, Michael Cox
 Version: 2.1
 Created: 31 May 2017
 Last Modified: 11 October 2021

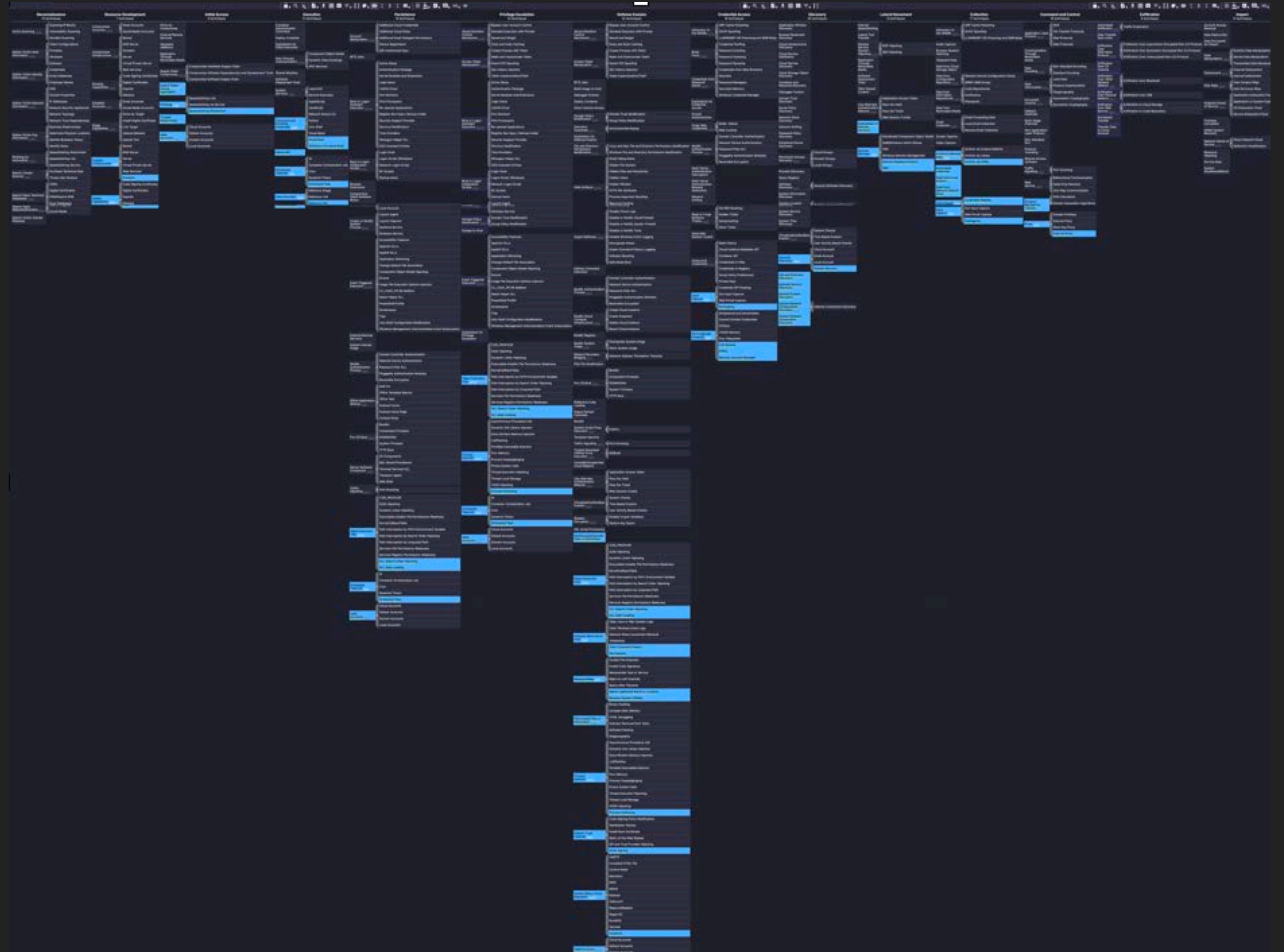
[Version Permalink](#)

Associated Group Descriptions

Name	Description
Cicada	[8]
POTASSIUM	[1][2]

APT10 (menuPass)

<https://mitre-attack.github.io/attack-navigator/#layerURL=https%3A%2F%2Fattack.mitre.org%2Fgroups%2FG0045%2FG0045-enterprise-layer.json>



APT10
(menuPass)

先等等！

你們應該看過很多 APT 組織 ATT&CK 了。

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



請問，這個是哪一個 APT Group 的 ATT&CK 圖？

Recon.	Resource Dev.	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Active Scanning	Acquire Infrastructure	Drive-by Compromise	Command and Scripting Interpreter	Account Manipulation	Abuse Elevation Control Mechanism	Abuse Elevation Control Mechanism	Adversary-in-the-Middle	Account Discovery	Exploitation of Remote Services	Adversary-in-the-Middle	Application Layer Protocol	Automated Exfiltration	Account Access Removal
Gather Victim Host Information	Compromise Accounts	Exploit Public-Facing Application	Container Administration Command	BITS Jobs	Access Token Manipulation	Access Token Manipulation	Brute Force	Application Window Discovery	Internal Spearphishing	Archive Collected Data	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information	Compromise Infrastructure	External Remote Services	Deploy Container	Boot or Logon Autostart Execution	Boot or Logon Autostart Execution	BITS Jobs	Credentials from Password Stores	Browser Bookmark Discovery	Lateral Tool Transfer	Audio Capture	Data Encoding	Exfiltration Over Alternative Protocol	Data Encrypted for Impact
Gather Victim Network Information	Develop Capabilities	Hardware Additions	Exploitation for Client Execution	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking	Automated Collection	Data Obfuscation	Exfiltration Over C2 Channel	Data Manipulation
Gather Victim Org Information	Establish Accounts	Phishing	Inter-Process Communication	Browser Extensions	Create or Modify System Process	Debugger Evasion	Forced Authentication	Cloud Service Dashboard	Remote Services	Browser Session Hijacking	Dynamic Resolution	Exfiltration Over Other Network Medium	Defacement
Phishing for Information	Obtain Capabilities	Replication Through Removable Media	Native API	Compromise Client Software Binary	Domain Policy Modification	Deobfuscate/Decode Files or Information	Forge Web Credentials	Cloud Service Discovery	Replication Through Removable Media	Clipboard Data	Encrypted Channel	Exfiltration Over Physical Medium	Disk Wipe
Search Closed Sources	Stage Capabilities	Supply Chain Compromise	Scheduled Task/Job	Create Account	Escape to Host	Deploy Container	Input Capture	Cloud Storage Object Discovery	Software Deployment Tools	Data from Cloud Storage Object	Fallback Channels	Exfiltration Over Web Service	Endpoint Denial of Service
Search Open Technical Databases		Trusted Relationship	Shared Modules	Create or Modify System Process	Event Triggered Execution	Direct Volume Access	Modify Authentication Process	Container and Resource Discovery	Taint Shared Content	Data from Configuration Repository	Ingress Tool Transfer	Scheduled Transfer	Firmware Corruption
Search Open Websites/ Domains		Valid Accounts	Software Deployment Tools	Event Triggered Execution	Exploitation for Privilege Escalation	Domain Policy Modification	Multi-Factor Authentication	Debugger Evasion	Use Alternate Authentication Material	Data from Information Repositories	Multi-Stage Channels	Transfer Data to Cloud Account	Inhibit System Recovery
Search Victim-Owned Websites			System Services	External Remote Services	Hijack Execution Flow	Execution Guardrails	Multi-Factor Authentication Request	Domain Trust Discovery		Data from Local System	Non-Application Layer Protocol		Network Denial of Service
			User Execution	Hijack Execution Flow	Process Injection	Exploitation for Defense Evasion	Network Sniffing	File and Directory Discovery		Data from Network Shared Drive	Non-Standard Port		Resource Hijacking
			Windows Management Instrumentation	Implant Internal Image	Scheduled Task/Job	File and Directory Permissions	OS Credential Dumping	Group Policy Discovery		Data from Removable Media	Protocol Tunneling		Service Stop
				Modify Authentication Process	Valid Accounts	Hide Artifacts	Steal Application Access Token	Network Service Discovery		Data Staged	Proxy		System Shutdown/ Reboot
				Office Application Startup		Hijack Execution Flow	Steal or Forge Kerberos Tickets	Network Share Discovery		Email Collection	Remote Access Software		
				Pre-OS Boot		Impair Defenses	Steal Web Session Cookie	Network Sniffing		Input Capture	Traffic Signaling		
				Scheduled Task/Job		Indicator Removal on Host	Unsecured Credentials	Password Policy Discovery		Screen Capture	Web Service		
				Service Binary Execution		Direct Command Execution	Unsecured Credentials	Service Discovery		Video Capture			
				Traffic Manipulation		Modify Authentication Process	Valid Accounts	Process Discovery					
						Modify Cloud Compute Infrastructure		Query Registry					
						Modify System Image		Software Discovery					
						Network Boundary Bridging		System Information Discovery					
						Obfuscated Files or Information		System Location Discovery					

這是 DEVCORE 某一隊近 20 次紅隊演練 ATT&CK Matrix

沒錯，我們在一些資安產品中被定義為「APT Group」🤔

比較看看各 APT 組織的 ATT&CK Matrix

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

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

APT38

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

APT10

DEVCORE

APT10

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

VS

DEVCORE

APT10

Recon.	Resource Dev.	Initial Access	Execution	Persistence	Privilege	Defense Evasion	Credential	Discovery	Lateral Movem	Collection	Command and	Exfiltration	Impact	Recon.	Resource Dev.	Initial Access	Execution	Persistence	Privilege	Defense Evasion	Credential	Discovery	Lateral Movem	Collection	Command and	Exfiltration	Impact
Active Scanning	Acquire Infrastructure	Drive-by Compromise	Command and Scripting Interpreter	Account Manipulation	Abuse Elevation Control Mechanism	Abuse Elevation Control Mechanism	Adversary in-the-Middle	Account Discovery	Exploitation of Remote Services	Adversary in-the-Middle	Application Layer Protocol	Automated Exfiltration	Account Access Removal	Active Scanning	Acquire Infrastructure	Drive-by Compromise	Command and Scripting Interpreter	Account Manipulation	Abuse Elevation Control Mechanism	Abuse Elevation Control Mechanism	Adversary in-the-Middle	Account Discovery	Exploitation of Remote Services	Adversary in-the-Middle	Application Layer Protocol	Automated Exfiltration	Account Access Removal
Gather Victim Host Information	Compromise Accounts	Exploit Public-Facing Application	Container Administration	BITS Jobs	Access Token Manipulation	Access Token Manipulation	Brute Force	Application Window Discovery	Internal Spearphishing	Archive Collected Data	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction	Gather Victim Host Information	Compromise Accounts	Exploit Public-Facing Application	Container Administration	Deployment Container	BITS Jobs	Access Token Manipulation	Access Token Manipulation	Brute Force	Application Window Discovery	Internal Spearphishing	Archive Collected Data	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information	Compromise Infrastructure	External Remote Services	Deploy Container	Boot or Logon Autostart Execution	Boot or Logon Autostart Execution	Boot or Logon Autostart Execution	Credentials from Password Stores	Browser Bookmark Discovery	Lateral Tool Transfer	Audio Capture	Data Encapsulation	Exfiltration Over Alternative Protocol	Data Encrypted for Impact	Gather Victim Identity Information	Compromise Infrastructure	External Remote Services	Hardware Additions	Execution for Client Execution	Inter-Process Communication	Boot or Logon Autostart Execution	Boot or Logon Autostart Execution	Credentials from Password Stores	Browser Bookmark Discovery	Lateral Tool Transfer	Audio Capture	Exfiltration Over Alternative Protocol	Data Encrypted for Impact
Gather Victim Network Information	Develop Capabilities	Hardware Additions	Exploitation for Client Execution	Inter-Process Communication	Inter-Process Communication	Inter-Process Communication	Build Image on Host	Cloud Infrastructure Discovery	Remote Service Session Hijacking	Automated Collection	Data Obfuscation	Exfiltration Over C2 Channel	Data Manipulation	Gather Victim Network Information	Develop Capabilities	Hardware Additions	Exploitation for Client Execution	Inter-Process Communication	Boot or Logon Autostart Execution	Boot or Logon Autostart Execution	Credentials from Password Stores	Browser Bookmark Discovery	Lateral Tool Transfer	Automated Collection	Data Obfuscation	Exfiltration Over C2 Channel	
Gather Victim Org Information	Establish Accounts	Phishing	Exploitation for Client Execution	Inter-Process Communication	Inter-Process Communication	Inter-Process Communication	Create or Modify System Process	Cloud Service Dashboard	Remote Services	Browser Session Hijacking	Dynamic Resolution	Exfiltration Over Other Network Medium	Detachment	Gather Victim Org Information	Establish Accounts	Phishing	Exploitation for Client Execution	Inter-Process Communication	Boot or Logon Autostart Execution	Boot or Logon Autostart Execution	Credentials from Password Stores	Browser Bookmark Discovery	Lateral Tool Transfer	Remote Services	Automated Collection	Data Obfuscation	
Phishing for Information	Obtain Capabilities	Replication Through Removable Media	Native API	Compromise Client Software Binary	Domain Policy Modification	Domain Policy Modification	Debugger Evasion	Cloud Service Dashboard	Replication Through Removable Media	Browser Session Hijacking	Encrypted Channel	Exfiltration Over Physical Medium	Detachment	Phishing for Information	Obtain Capabilities	Replication Through Removable Media	Native API	Compromise Client Software Binary	Domain Policy Modification	Domain Policy Modification	Debugger Evasion	Cloud Service Dashboard	Replication Through Removable Media	Browser Session Hijacking	Encrypted Channel	Exfiltration Over Physical Medium	
Search Closed Sources	Stage Capabilities	Supply Chain Compromise	Scheduled Task/job	Create Account	Escape to Host	Escape to Host	Direct Volume Access	Cloud Storage Object Discovery	Software Deployment Tools	Data from Cloud Storage Object	Fallback Channels	Exfiltration Over Web Service	Endpoint Denial of Service	Search Closed Sources	Stage Capabilities	Supply Chain Compromise	Scheduled Task/job	Create Account	Escape to Host	Escape to Host	Debugger Evasion	Cloud Storage Object Discovery	Software Deployment Tools	Data from Cloud Storage Object	Fallback Channels	Exfiltration Over Web Service	
Search Open Technical Databases		Trusted Relationship	Shared Modules	Create or Modify System Process	Event Triggered Execution	Event Triggered Execution	Direct Volume Access	Container and Resource Discovery	Taint Shared Content	Data from Configuration Repository	Ingress Tool Transfer	Scheduled Transfer	Firmware Corruption	Search Open Technical Databases		Trusted Relationship	Shared Modules	Create or Modify System Process	Event Triggered Execution	Event Triggered Execution	Exploitation for Privilege Escalation	Domain Policy Modification	Debugger Evasion	Container and Resource Discovery	Taint Shared Content	Scheduled Transfer	
Search Open Websites/ Domains		Valid Accounts	Software Deployment Tools	Event Triggered Execution	Exploitation for Privilege Escalation	Exploitation for Privilege Escalation	Domain Policy Modification	Debugger Evasion	Use Alternate Authentication Material	Data from Information Repositories	Multi-Stage Channels	Transfer Data to Cloud Account	Inhibit System Recovery	Search Open Websites/ Domains		Valid Accounts	Software Deployment Tools	Event Triggered Execution	Exploitation for Privilege Escalation	Exploitation for Privilege Escalation	Domain Policy Modification	Debugger Evasion	Container and Resource Discovery	Taint Shared Content	Use Alternate Authentication Material	Inhibit System Recovery	
Search Victim Owned Files		System Services	External Remote Services	Hack Execution Flow	Execution Guardrails	Execution Guardrails	Multi-Factor Authentication Request	Domain Trust Discovery	Non-Application Layer Protocol	Data from Local System	Non-Application Layer Protocol	Network Denial of Service	Network Denial of Service	Search Victim Owned Files		System Services	External Remote Services	Hack Execution Flow	Execution Guardrails	Execution Guardrails	Multi-Factor Authentication Request	Domain Trust Discovery	Non-Application Layer Protocol	Non-Application Layer Protocol	Network Denial of Service	Network Denial of Service	
		Implant Internal Image	Process	Exploit Execution Flow	Exploit Execution Flow	Exploit Execution Flow	Multi-Factor Authentication Request	Domain Trust Discovery	Non-Application Layer Protocol	Data from Local System	Non-Application Layer Protocol	Network Denial of Service	Network Denial of Service	Search Victim Owned Files		System Services	External Remote Services	Hack Execution Flow	Execution Guardrails	Execution Guardrails	Multi-Factor Authentication Request	Domain Trust Discovery	Non-Application Layer Protocol	Non-Application Layer Protocol	Network Denial of Service	Network Denial of Service	
		Office Application Startup	Pre-OS Boot	Impair Defenses	Impair Defenses	Impair Defenses	Multi-Factor Authentication Request	Domain Trust Discovery	Non-Application Layer Protocol	Data from Local System	Non-Application Layer Protocol	Network Denial of Service	Network Denial of Service	Search Victim Owned Files		System Services	External Remote Services	Hack Execution Flow	Execution Guardrails	Execution Guardrails	Multi-Factor Authentication Request	Domain Trust Discovery	Non-Application Layer Protocol	Non-Application Layer Protocol	Network Denial of Service	Network Denial of Service	
		Scheduled Task/job	Indicator Removal on Host	Unsecured Credentials	Unsecured Credentials	Unsecured Credentials	Multi-Factor Authentication Request	Domain Trust Discovery	Non-Application Layer Protocol	Data from Local System	Non-Application Layer Protocol	Network Denial of Service	Network Denial of Service	Search Victim Owned Files		System Services	External Remote Services	Hack Execution Flow	Execution Guardrails	Execution Guardrails	Multi-Factor Authentication Request	Domain Trust Discovery	Non-Application Layer Protocol	Non-Application Layer Protocol	Network Denial of Service	Network Denial of Service	
		Server Software Component	Indirect Command Execution	Peripheral Device Discovery	Peripheral Device Discovery	Peripheral Device Discovery	Multi-Factor Authentication Request	Domain Trust Discovery	Non-Application Layer Protocol	Data from Local System	Non-Application Layer Protocol	Network Denial of Service	Network Denial of Service	Search Victim Owned Files		System Services	External Remote Services	Hack Execution Flow	Execution Guardrails	Execution Guardrails	Multi-Factor Authentication Request	Domain Trust Discovery	Non-Application Layer Protocol	Non-Application Layer Protocol	Network Denial of Service	Network Denial of Service	
		Traffic Signaling	Masquerading	Masquerading	Masquerading	Masquerading	Multi-Factor Authentication Request	Domain Trust Discovery	Non-Application Layer Protocol	Data from Local System	Non-Application Layer Protocol	Network Denial of Service	Network Denial of Service	Search Victim Owned Files		System Services	External Remote Services	Hack Execution Flow	Execution Guardrails	Execution Guardrails	Multi-Factor Authentication Request	Domain Trust Discovery	Non-Application Layer Protocol	Non-Application Layer Protocol	Network Denial of Service	Network Denial of Service	
		Valid Accounts	Modify Authentication Process	Process Discovery	Process Discovery	Process Discovery	Multi-Factor Authentication Request	Domain Trust Discovery	Non-Application Layer Protocol	Data from Local System	Non-Application Layer Protocol	Network Denial of Service	Network Denial of Service	Search Victim Owned Files		System Services	External Remote Services	Hack Execution Flow	Execution Guardrails	Execution Guardrails	Multi-Factor Authentication Request	Domain Trust Discovery	Non-Application Layer Protocol	Non-Application Layer Protocol	Network Denial of Service	Network Denial of Service	
			Modify Cloud Compute Infrastructure	Query Registry	Query Registry	Query Registry	Multi-Factor Authentication Request	Domain Trust Discovery	Non-Application Layer Protocol	Data from Local System	Non-Application Layer Protocol	Network Denial of Service	Network Denial of Service	Search Victim Owned Files		System Services	External Remote Services	Hack Execution Flow	Execution Guardrails	Execution Guardrails	Multi-Factor Authentication Request	Domain Trust Discovery	Non-Application Layer Protocol	Non-Application Layer Protocol	Network Denial of Service	Network Denial of Service	
			Modify Registry	Remote System Discovery	Remote System Discovery	Remote System Discovery	Multi-Factor Authentication Request	Domain Trust Discovery	Non-Application Layer Protocol	Data from Local System	Non-Application Layer Protocol	Network Denial of Service	Network Denial of Service	Search Victim Owned Files		System Services	External Remote Services	Hack Execution Flow	Execution Guardrails	Execution Guardrails	Multi-Factor Authentication Request	Domain Trust Discovery	Non-Application Layer Protocol	Non-Application Layer Protocol	Network Denial of Service	Network Denial of Service	
			Modify System Image	System Information Discovery	System Information Discovery	System Information Discovery	Multi-Factor Authentication Request	Domain Trust Discovery	Non-Application Layer Protocol	Data from Local System	Non-Application Layer Protocol	Network Denial of Service	Network Denial of Service	Search Victim Owned Files		System Services	External Remote Services	Hack Execution Flow	Execution Guardrails	Execution Guardrails	Multi-Factor Authentication Request	Domain Trust Discovery	Non-Application Layer Protocol	Non-Application Layer Protocol	Network Denial of Service	Network Denial of Service	
			Network Boundary Bridging	System Location Discovery	System Location Discovery	System Location Discovery	Multi-Factor Authentication Request	Domain Trust Discovery	Non-Application Layer Protocol	Data from Local System	Non-Application Layer Protocol	Network Denial of Service	Network Denial of Service	Search Victim Owned Files		System Services	External Remote Services	Hack Execution Flow	Execution Guardrails	Execution Guardrails	Multi-Factor Authentication Request	Domain Trust Discovery	Non-Application Layer Protocol	Non-Application Layer Protocol	Network Denial of Service	Network Denial of Service	
			Obfuscated Files or Information	System Location Discovery	System Location Discovery	System Location Discovery	Multi-Factor Authentication Request	Domain Trust Discovery	Non-Application Layer Protocol	Data from Local System	Non-Application Layer Protocol	Network Denial of Service	Network Denial of Service	Search Victim Owned Files		System Services	External Remote Services	Hack Execution Flow	Execution Guardrails	Execution Guardrails	Multi-Factor Authentication Request	Domain Trust Discovery	Non-Application Layer Protocol	Non-Application Layer Protocol	Network Denial of Service	Network Denial of Service	

「你們一定是要說你們好強啦！比 APT 組織還強！」

DEVCORE

APT10

「你們一定是要說你們好強啦！比 APT 組織還強！」

『不是！！是你們進入了 ATT&CK 的誤區。』

VS

DEVCORE

APT10

Recon.	Resource Dev.	Initial Access	Execution	Persistence	Privilege	Defense Evasion	Credential	Discovery	Lateral Movem.	Collection	Command and	Exfiltration	Impact	Recon.	Resource Dev.	Initial Access	Execution	Persistence	Privilege	Defense Evasion	Credential	Discovery	Lateral Movem.	Collection	Command and	Exfiltration	Impact	
Active Scanning	Acquire Infrastructure	Drive-by Compromise	Command and Scripting Interpreter	Account Manipulation	Abuse Elevation Control Mechanism	Abuse Elevation Control Mechanism	Adversary-in-the-Middle	Account Discovery	Exploitation of Remote Services	Adversary-in-the-Middle	Application Layer Protocol	Automated Exfiltration	Account Access Removal	Active Scanning	Acquire Infrastructure	Drive-by Compromise	Command and Scripting Interpreter	Account Manipulation	Abuse Elevation Control Mechanism	Abuse Elevation Control Mechanism	Adversary-in-the-Middle	Account Discovery	Exploitation of Remote Services	Adversary-in-the-Middle	Application Layer Protocol	Automated Exfiltration	Account Access Removal	
Gather Victim Host Information	Compromise Accounts	Exploit Public-Facing Application	Container Administration	BITS Jobs	Access Token Manipulation	Access Token Manipulation	Brute Force	Application Window Discovery	Internal Spearphishing	Archive Collected Data	Communication Through Removable	Data Transfer Size Limits	Data Destruction	Gather Victim Host Information	Compromise Accounts	Exploit Public-Facing Application	Container Administration	BITS Jobs	Abuse Elevation Control Mechanism	Access Token Manipulation	Brute Force	Application Window Discovery	Internal Spearphishing	Archive Collected Data	Communication Through Removable	Data Transfer Size Limits	Data Destruction	
Gather Victim Identity Information	Compromise Infrastructure	External Remote Services	Deploy Container	Boot or Logon Autostart Execution	Boot or Logon Autostart Execution	BITS Jobs	Credentials from Password Stores	Browser Bookmark Discovery	Lateral Tool Transfer	Audio Capture	Data Encoding	Exfiltration Over Alternative Protocol	Data Encrypted for Impact	Gather Victim Network Information	Compromise Infrastructure	External Remote Services	Deploy Container	Boot or Logon Autostart Execution	Abuse Elevation Control Mechanism	Access Token Manipulation	Credentials from Password Stores	Browser Bookmark Discovery	Lateral Tool Transfer	Audio Capture	Data Encoding	Exfiltration Over Alternative Protocol	Data Encrypted for Impact	
Gather Victim Network Information	Develop Capabilities	Hardware Additions	Exploitation for Client Execution	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Build Image on Host	Cloud Infrastructure Discovery	Cloud Infrastructure Discovery	Remote Service Session Hijacking	Automated Collection	Data Obfuscation	Exfiltration Over C2 Channel	Data Manipulation	Gather Victim Org Information	Develop Capabilities	Hardware Additions	Exploitation for Client Execution	Boot or Logon Initialization Scripts	Abuse Elevation Control Mechanism	Access Token Manipulation	Cloud Infrastructure Discovery	Cloud Infrastructure Discovery	Remote Service Session Hijacking	Automated Collection	Data Obfuscation	Exfiltration Over C2 Channel	Data Manipulation	
Gather Victim Org Information	Establish Accounts	Phishing	Inter-Process Communication	Browser Extensions	Create or Modify System Process	Debugger Evasion	Cloud Service Dashboard	Cloud Service Dashboard	Remote Services	Browser Session Hijacking	Dynamic Resolution	Exfiltration Over Other Network Medium	Defacement	Gather Victim Org Information	Establish Accounts	Phishing	Inter-Process Communication	Browser Extensions	Abuse Elevation Control Mechanism	Access Token Manipulation	Cloud Service Dashboard	Cloud Service Dashboard	Remote Services	Browser Session Hijacking	Dynamic Resolution	Exfiltration Over Other Network Medium	Defacement	
Phishing for Information	Obtain Capabilities	Replication Through Removable Media	Native API	Compromise Client Software Binary	Create or Modify System Process	Deobfuscate/Decode Files or Information	Cloud Service Discovery	Cloud Service Discovery	Replication Through Removable Media	Browser Session Hijacking	Encrypted Channel	Exfiltration Over Physical Medium	Disk Wipe	Phishing for Information	Obtain Capabilities	Replication Through Removable Media	Native API	Compromise Client Software Binary	Abuse Elevation Control Mechanism	Access Token Manipulation	Debugger Evasion	Cloud Service Dashboard	Cloud Service Dashboard	Remote Services	Browser Session Hijacking	Dynamic Resolution	Exfiltration Over Physical Medium	Disk Wipe
Search Closed Sources	Stage Capabilities	Supply Chain Compromise	Scheduled Task/Job	Create Account	Escape to Host	Deploy Container	Cloud Storage Object Discovery	Cloud Storage Object Discovery	Software Deployment Tools	Data from Cloud Storage Object	Fallback Channels	Exfiltration Over Web Service	Endpoint Denial of Service	Search Closed Sources	Stage Capabilities	Supply Chain Compromise	Scheduled Task/Job	Create Account	Domain Policy Modification	Deobfuscate/Decode Files or Information	Input Capture	Cloud Storage Object Discovery	Cloud Storage Object Discovery	Software Deployment Tools	Data from Cloud Storage Object	Fallback Channels	Exfiltration Over Web Service	Endpoint Denial of Service
Search Open Technical Databases		Trusted Relationship	Shared Modules	Create or Modify System Process	Event Triggered Execution	Direct Volume Access	Container and Resource Discovery	Container and Resource Discovery	Taint Shared Content	Data from Configuration Repository	Ingress Tool Transfer	Scheduled Transfer	Firmware Corruption	Search Open Technical Databases		Trusted Relationship	Shared Modules	Create or Modify System Process	Event Triggered Execution	Domain Policy Modification	Direct Volume Access	Container and Resource Discovery	Container and Resource Discovery	Software Deployment Tools	Data from Configuration Repository	Ingress Tool Transfer	Scheduled Transfer	Firmware Corruption
Search Open Websites/ Domains		Valid Accounts	Software Deployment Tools	Event Triggered Execution	Exploitation for Privilege Escalation	Domain Policy Modification	Debugger Evasion	Debugger Evasion	Use Alternate Authentication Material	Data from Information Repositories	Multi-Stage Channels	Transfer Data to Cloud Account	Inhibit System Recovery	Search Open Websites/ Domains		Valid Accounts	Software Deployment Tools	Event Triggered Execution	Exploitation for Privilege Escalation	Domain Policy Modification	Multi-Factor Authentication	File and Directory Discovery	Debugger Evasion	Data from Information Repositories	Multi-Stage Channels	Transfer Data to Cloud Account	Inhibit System Recovery	
Search Victim-Owned Websites			System Services	External Remote Services	Hijack Execution Flow	Execution Guardrails	Domain Trust Discovery	Domain Trust Discovery		Data from Local System	Non-Application Layer Protocol	Network Denial of Service	Search Victim-Owned Websites			System Services	External Remote Services	Hijack Execution Flow	Exploitation for Defense Evasion	Multi-Factor Authentication	File and Directory Discovery	Debugger Evasion	Data from Local System	Non-Application Layer Protocol	Network Denial of Service	Resource Hijacking		
			User Execution	Hijack Execution Flow	Process Injection	Exploitation for Defense Evasion	File and Directory Discovery	File and Directory Discovery		Data from Network Shared Drive	Non-Standard Port					User Execution	Hijack Execution Flow	Process Injection	Exploitation for Defense Evasion	Multi-Factor Authentication	File and Directory Discovery	Debugger Evasion	Data from Network Shared Drive	Non-Standard Port				
			Windows Management Instrumentation	Implant Internal Image	Scheduled Task/Job	Hide Artifacts	Group Policy Discovery	Group Policy Discovery		Data from Removable Media	Protocol Tunneling					Windows Management Instrumentation	Implant Internal Image	Scheduled Task/Job	Exploitation for Defense Evasion	OS Credential Dumping	File and Directory Discovery	Debugger Evasion	Data from Removable Media	Protocol Tunneling				
				Modify Authentication Process	Office Application Startup	Pre-OS Boot	Hijack Execution Flow	Network Service Discovery		Data Staged	Proxy						Modify Authentication Process	Office Application Startup	Exploitation for Defense Evasion	Steal Application Access Token	File and Directory Discovery	Debugger Evasion	Data from Removable Media	Proxy				
				Scheduled Task/Job		Impair Defenses	Unsecured Credentials	Network Share Discovery			Remote Access Software	Traffic Signaling					Scheduled Task/Job		Exploitation for Defense Evasion	Steal Web Session Cookie	Network Share Discovery	Debugger Evasion			Remote Access Software	Traffic Signaling		
				Server Software Component	Traffic Signaling	Indicator Removal on Host	Peripheral Device Discovery	Peripheral Device Discovery			Web Service						Server Software Component	Traffic Signaling	Exploitation for Defense Evasion	Unsecured Credentials	Password Policy Discovery	Peripheral Device Discovery			Web Service			
						Masquerading	Permission Groups	Permission Groups											Masquerading			Permission Groups						

VS

演練後提供整理的結果
完整、正確性極高

根據事件分析的結果
不完整、正確性低

攻擊者怎麼看待 ATT&CK

- 攻擊者創造 Techniques 及 Tools 進行攻擊。防守方根據結果，歸納 Tactics，整理 Techniques 及 Tools
- **但分析結果是死的，駭客是活的，重點在心法。**



如何正確使用紅隊演練



「我們想做 APT 10 的演練。」

『好。但你們真的確定你們要的是什麼嗎？』

ATT&CK 常見的誤區：

1. 以特定族群的 **Tactics, Techniques, Procedures (TTPs)** 來驗證產業的安全
2. 指定模擬特定/已發生的 **TTPs** 來確保防禦的有效性

ATT&CK 的常見誤區

- 攻擊者是誰：我們面對的攻擊者真的只有這個組織嗎？
- 攻擊者的手法：
 - 只要針對 APT 組織的 ATT&CK 手法來防禦就好了嗎？
 - APT 組織的能力真的只有這樣嗎？如果你是攻擊者，你只會嘗試那些手法嗎？
 - 沒有盤點自己的核心目標，跟攻擊事件絕對不同，手法當然也不一樣
- ATT&CK 分析
 - APT 組織的準備階段是無法觀測的
 - ATT&CK Matrix 是「事後」整理，並非 APT 組織真實現況



ATT&CK 就像是一張考卷

重新演練特定的 APT 攻擊就是只練習考古題

A close-up photograph of a hand holding a yellow pencil, pointing at a multiple-choice test paper. The paper is filled with numbered questions and circular bubbles containing letters A, B, C, and D. The background is slightly blurred, focusing attention on the hand and the pencil tip.

ATT&CK 就像是一張考卷
重新演練特定的 APT 攻擊就是只練習考古題

但你真的學會了嗎？

ATT&CK 的正確用法

- 規劃策略：哪些該優先處理、用什麼方式處理 (CSF 5 個 functions)
- 盤點攻擊鏈需要阻斷處：用自己有的優勢優先阻斷攻擊鏈
- 永遠要把「範圍」列入模擬攻擊的重要評估因素：子公司 A & 子公司 B 會面對不同的 TTPs

九大網路安全統計數字速覽

94% 的惡意軟體透過**電子郵件**傳送

在被報導的資安事件中，超過 80% 的成因來自**釣魚攻擊**

釣魚攻擊每分鐘造成 17,700 美元的損失

無檔案攻擊在 2019 上半年成長 256%

60% 的外洩事件所利用的**漏洞**已經有修補程式，但卻沒有套用所致

針對**物聯網設備的攻擊**在 2019 上半年增加了兩倍

63% 的企業認為他們的資料在近 12 個月內可能因為**硬體或晶片的漏洞**遭到感染

資料外洩平均耗費企業 392 萬美元

有 40% 的 IT 主管認為**網路安全的工作最難補足人力**

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

94% 的惡意軟體透過電子郵件傳送

- 電子郵件只是媒介，但不是最終目標
- 數據趨勢只在 ATT&CK 中的 Initial Access。而 Initial Access 只是起點。

ATT&CK™

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

?????



94% 的惡意軟體透過電子郵件傳送

- 電子郵件只是媒介，但不是最終目標
- 數據趨勢只在 ATT&CK 中的 Initial Access。而 Initial Access 只是起點。

ATT&CK™

我們真正該談的是什麼

- 不同組織的相同手法
- 如何在攻擊階段中阻斷攻擊鍊
- 如何有足夠的觀測點來及時發現攻擊行為



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

APT38

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

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

APT10+APT38

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

• 需要注意在不同組織的相同手法，
是不能出錯的基本必考題（常見手法）

APT10+APT38

如何正確使用紅隊演練



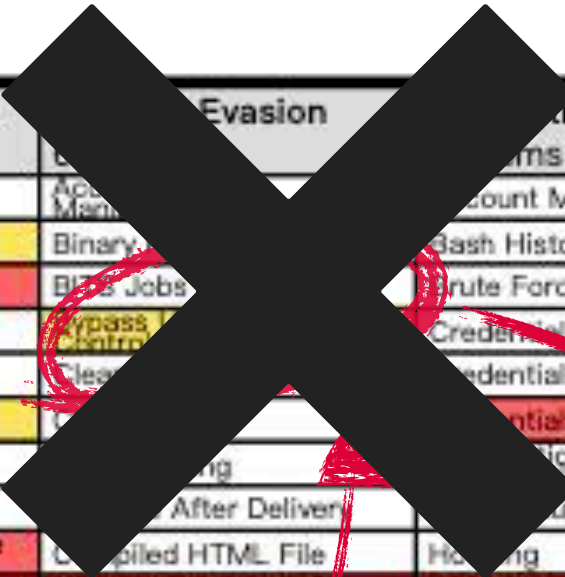
紅隊演練搭配 ATT&CK 檢視防禦狀態

Incident X Red Team		filters	score gradient	legend							
		stages: act platforms: windows, linux, mac	1 3	<div style="display: flex; gap: 10px;"> ■ Red Team ■ Incident ■ Overlap </div>							
Initial Access 11 items	Execution 33 items	Persistence 59 items	Privilege Escalation 28 items	Defense Evasion 67 items	Credential Access 19 items	Discovery 22 items	Lateral Movement 17 items	Collection 13 items	Command And Controls	Exfiltration 9 items	Impact 14 items
Drive-by Compromise	AppleScript	bash, perl and python	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Data Destruction
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Patching	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed	Data Encrypted for Impact
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	Bits Jobs	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Connection Proxy	Data Encrypted	Defacement
Hardware Additions	Compiled HTML File	AppCert DLLs	Appint DLLs	Bypass User Account Control	Credential Dumping	Domain Trust Discovery	Exploitation of Remote Services	Data from Information Repositories	Custom Command and Control Protocol	Data Transfer Size Limits	Disk Content Wipe
Replication Through Removable Media	Control Panel Items	Appint DLLs	Application Shimming	Clear Command History	Credentials in Files	File and Directory Discovery	Logon Scripts	Data from Local System	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Structure Wipe
Spearphishing Attachment	Dynamic Data Exchange	Application Shimming	Bypass User Account Control	CMSH	Credentials in Registry	Network Service Discovery	Pass the Hash	Data from Network Shared Drive	Data Encoding	Exfiltration Over Command and Control	Endpoint Denial of Service
Spearphishing Link	Execution through API	Authentication Package	DLL Search Order Hijacking	Code Signing	Exploitation for Credential Access	Network Share Discovery	Pass the Ticket	Data from Removable Media	Data Obfuscation	Exfiltration Over Other Network Medium	Firmware Corruption
Spearphishing via Service	Execution through Module Load	BITS Jobs	Dylib Hijacking	Compile After Delivery	Forced Authentication	Network Sniffing	Remote Desktop Protocol	Data Staged	Domain Fronting	Exfiltration Over Physical Medium	Inhibit System Recovery
Supply Chain Compromise	Exploitation for Client Execution	Bootkit	Exploitation for Privilege Escalation	Compiled HTML File	Hooking	Password Policy Discovery	Remote File Copy	Email Collection	Domain Generation Algorithms	Scheduled Transfer	Network Denial of Service
Trusted Relationship	Graphical User Interface	Browser Extensions	Extra Window Memory Injection	Component Firmware Hijacking	Input Capture	Peripheral Device Discovery	Remote Services	File Capture	Fallback Channels		Resource Hijacking
Valid Accounts	InstallUtil	Change Default File Association	File System Permissions Weakness	Component Object Model Hijacking	Input Prompt	Permission Groups Discovery	Replication Through Removable Media	Man in the Browser	Multi-hop Proxy		Runtime Data Manipulation
	Launchctl	Component Firmware Hijacking	Hooking	Control Panel Item Hijacking	Kerberoasting	Process Discovery	Shared Webroot	Screen Capture	Multi-Stage Channels		Service Stop
	Local Job Scheduling	Component Object Model Hijacking	Image File Execution Options Injection	DCShadow	Keychain	Query Registry	SSH Hijacking	Video Capture	Multiband Communication		Stored Data Manipulation
	LSASS Driver	Create Account	Launch Daemon	Deobfuscate/Decode Files or Information	LLMNR/NBT-NS Poisoning and Relay	Remote System Discovery	Taint Shared Content		Multilayer Encryption		Transmitted Data Manipulation
	Msihta	DLL Search Order Hijacking	New Service	Disabling Security Tools	Network Sniffing	Security Software Discovery	Third-party Software		Port Knocking		
	PowerShell	Dylib Hijacking	Path Interception	DLL Search Order Hijacking	Password Filter DLL	System Information Discovery	Windows Admin Shares		Remote Access Tools		
	Revsrv/Regasm	External Remote Services	Plist Modification	DLL Side-Loading	Private Keys	System Network Configuration Discovery	Windows Remote Management		Remote File Copy		
	Revsrv32	File System Permissions Weakness	Port Monitors	Execution Guardrails	Securityd Memory	System Work Configuration Discovery			Standard Application Layer Protocol		
	Rundll32	Hidden Files and Directories	Process Injection	Exploitation for Defense Evasion	Vis-Exploit Mitigation	System Owner/User Discovery			Standard Cryptographic Protocol		
	Scheduled Task	Hooking	Scheduled Task Hijacking	Extra Window Memory Injection		System Service Discovery			Standard Application Layer Protocol		
	Scripting	Hypervisor	Service Registry Hijacking	File Deletion		System Time Discovery			Uncommonly Used Port		
	Service Execution	Image File Execution Options Injection	Setuid and Setgid	File Permissions Modification		Virtualization/Sandbox Evasion			Web Service		
	Signed Binary Proxy Execution	Kernel Modules and Extensions	SID-History Injection	File System Logical Offsets							
	Signed Script Proxy Execution	Launch Agent	Startup Items	Gatekeeper Bypass							
	Source	Launch Daemon	Sudo	Group Policy Modification							
	Space after Filename	Launchctl	Sudo Caching	Hidden Files and Directories							
	Third-party Software	LC_LOAD_DYLIB Addition	Valid Accounts	Hidden Users							
	Trap	Local Job Scheduling	Web Shell	Hidden Window							
	Trusted Developer Utilities	Login Item		HISTCONTROL							
	User Execution	Logon Scripts		Image File Execution Options Injection							
	Windows Management Instrumentation	LSASS Driver		Indicator Blocking							
	Windows Remote Management	Modify Existing Service		Indicator Removal from Tools							
	XSL Script Processing	Netsh Helper DLL		Indicator Removal on Host							
		New Service		Indirect Command Execution							
		Office Application Startup		Install Root Certificate							
		Path Interception		InstallUtil							
		Plist Modification		Launchctl							
		Port Knocking		LC_MAIN Hijacking							
		Port Monitors		Masquerading							
		Rc.common		Modify Registry							
		Re-opened Applications		Msihta							
		Redundant Access		Network Share Connection Removal							
		Registry Run Keys / Startup Folder		NTFS File Attributes							
		Scheduled Task		Obfuscated Files or Information							

紅隊演練搭配 ATT&CK 檢視防禦狀態

Incident X Red Team		filters	score gradient	legend							
		stages: act	1 3	Red Team							
		platforms: windows, linux, m									
Initial Access 11 items	Execution 33 items	Persistence 59 items	Privilege Escalation 28 items	Evasion 11 items	Impact 14 items						
Drive-by Compromise	AppleScript	bash, perl, and python	Account Manipulation	Account Discovery	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Data Destruction
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Patching	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed	Data Encrypted for Impact
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	Bits Jobs	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Connection Proxy	Data Encrypted	Defacement
Hardware Additions	Compiled HTML File	AppCert DLLs	Applet DLLs	Bypass Controls	Credential Dumping	Domain Trust Discovery	Exploitation of Remote Services	Data from Information Repositories	Custom Command and Control Protocol	Data Transfer Size Limits	Disk Content Wipe
Replication Through Removable Media	Control Panel Items	Appint DLLs	Application Shimming	Clear Credentials in Files	Credentials in Files	File and Directory Discovery	Logon Scripts	Data from Local System	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Structure Wipe
Spearphishing Attachment	Dynamic Data Exchange	Application Shimming	Bypass User Account Control	Credentials in Registry	Exploitation for Privilege Escalation	Network Service Discovery	Pass the Hash	Data from Network	Data Encoding	Exfiltration Over Command and Control	Endpoint Denial of Service
Spearphishing Link	Execution through API	Authentication Package	DLL Search Order Hijacking	Exploitation for Access	Exploitation for Privilege Escalation	Network Share Discovery	Pass the Ticket	Data from Removable Media	Data Obfuscation	Exfiltration Over Other Network Medium	Firmware Corruption
Spearphishing via Service	Execution through Module Load	BITS Jobs	Dylib Hijacking	After Delivery	Hooking	Network Sniffing	Remote Desktop Protocol	Data Staged	Domain Fronting	Exfiltration Over Physical Medium	Inhibit System Recovery
Supply Chain Compromise	Exploitation for Client Execution	Bootkit	Exploitation for Privilege Escalation	Compiled HTML File	Input Capture	Password Policy Discovery	Remote File Copy	Email Collection	Domain Generation Algorithms	Scheduled Transfer	Network Denial of Service
Trusted Relationship	Graphical User Interface	Browser Extensions	Extra Window Memory Injection	Component Firmware Hijacking	Input Prompt	Peripheral Device Discovery	Replication Through Removable Media	Event Capture	Fallback Channels		Resource Hijacking
Valid Accounts	InstallUtil	Change Default File Association	File System Permissions Weakness	Component Object Model Hijacking	Kerberoasting	Permission Groups Discovery	Shared Webroot	Man in the Browser	Multi-hop Proxy		Runtime Data Manipulation
	Launchctl	Component Firmware	Hooking	Control Panel Item Hijacking	Keychain	Process Discovery	SSH Hijacking	Screen Capture	Multi-Stage Channels		Service Stop
	Local Job Scheduling	Component Object Model Hijacking	Image File Execution Options Injection	DCShadow	LLMNR/NBT-NS Poisoning and Relay	Query Registry	SSH Hijacking	Video Capture	Multiband Communication		Stored Data Manipulation
	LSASS Driver	Create Account	Launch Daemon	Deobfuscate/Decode Files or Information	Network Sniffing	Remote System Discovery	Taint Shared Content		Multilayer Encryption		Transmitted Data Manipulation
	Msihta	DLL Search Order Hijacking	New Service	Disabling Security Tools	Network Sniffing	Security Software Discovery	Third-party Software		Port Knocking		
	PowerShell	Dylib Hijacking	Path Interception	DLL Search Order Hijacking	Password Filter DLL	System Information Discovery	Windows Admin Shares		Remote Access Tools		
	Revsrv/Regasm	External Remote Services	Plist Modification	DLL Side-Loading	Private Keys	System Network Configuration Discovery	Windows Remote Management		Remote File Copy		
	Revsrv32	File System Permissions Weakness	Port Monitors	Execution Guardrails	Securityd Memory	System Work Configuration Discovery			Remote File Copy		
	Rundll32	Hidden Files and Directories	Process Injection	Exploitation for Defense Evasion	Virtualization	System Owner/User Discovery			Standard Application Layer Protocol		
	Scheduled Task	Hooking	Scheduled Task	Extra Window Memory Injection	Virtualization	System Service Discovery			Standard Cryptographic Protocol		
	Scripting	Hypervisor	Service Registry Manipulation	File Deletion	Virtualization	System Time Discovery			Standard Application Layer Protocol		
	Service Execution	Image File Execution Options Injection	Setuid and Setgid	File Permissions Modification	Virtualization/Sandbox Evasion				Web Service		
	Signed Binary Proxy Execution	Kernel Modules and Extensions	SID-History Injection	File System Logical Offsets							
	Signed Script Proxy Execution	Launch Agent	Startup Items	Gatekeeper Bypass							
	Source	Launch Daemon	Sudo	Group Policy Modification							
	Space After Filename	Launchctl	Sudo Caching	Hidden Files and Directories							
	Third-party Software	LC_LOAD_DYLIB Addition	Valid Accounts	Hidden Users							
	Trap	Local Job Scheduling	Web Shell	Hidden Window							
	Trusted Developer Utilities	Login Item		HISTCONTROL							
	User Execution	Logon Scripts		Image File Execution Options Injection							
	Windows Management Instrumentation	LSASS Driver		Indicator Blocking							
	Windows Remote Management	Modify Existing Service		Indicator Removal from Tools							
	XSL Script Processing	Netsh Helper DLL		Indicator Removal on Host							
		New Service		Indirect Command Execution							
		Office Application Startup		Install Root Certificate							
		Path Interception		InstallUtil							
		Plist Modification		Launchctl							
		Port Knocking		LC_MAIN Hijacking							
		Port Monitors		Masquerading							
		Rc.common		Modify Registry							
		Re-opened Applications		Msihta							
		Redundant Access		Network Share Connection Removal							
		Registry Run Keys / Startup Folder		NTFS File Attributes							
		Scheduled Task		Obfuscated Files or Information							

如果在這裡可以阻斷



金融業常見的 ATT&CK 手法

- **T1078** Valid Accounts
- **T1003** OS Credential Dumping
- **T1550** Use Alternate Authentication Material
- **T1059** Command and Scripting Interpreter
- **T1071** Application Layer Protocol
- **T1110** Brute Force
- **T1016** System Network Configuration Discovery

- **T1021** Remote Services
- **T1087** Account Discovery
- **T1090** Proxy

Impact

- T1491 Defacement
- T1561 Disk Wipe
- T1565 Data Manipulation

DEVCORE's Top 5: 最常見的五種攻擊樣態

#1 外部服務存在漏洞

可利用資訊已外洩、未執行滲透測試、已知弱點未修補、WAF 無法防護

#2 第三方服務存在高風險漏洞

存在 0-Day、使用原廠預設密碼、使用弱密碼

#3 網路區隔存在利用機會

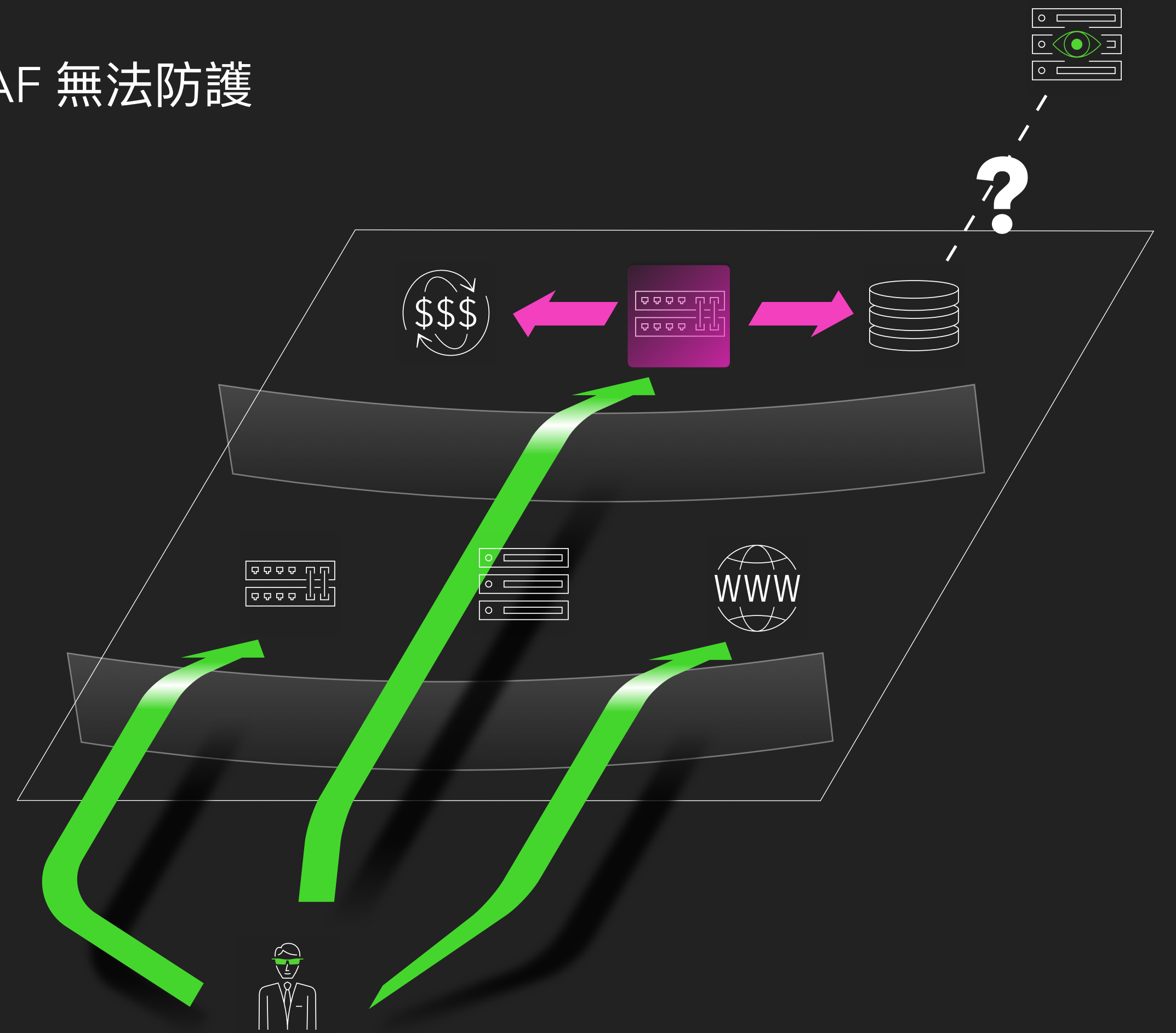
合法連線行為、網段區隔不良、ACL 不完善

#4 帳號權限保護不足

系統共用特權帳號、合法特權帳號活動、使用弱密碼

#5 監控回應不如預期

告警誤判、人員回應不即時、無法確認告警正確性



Takeaways

馬上進行：

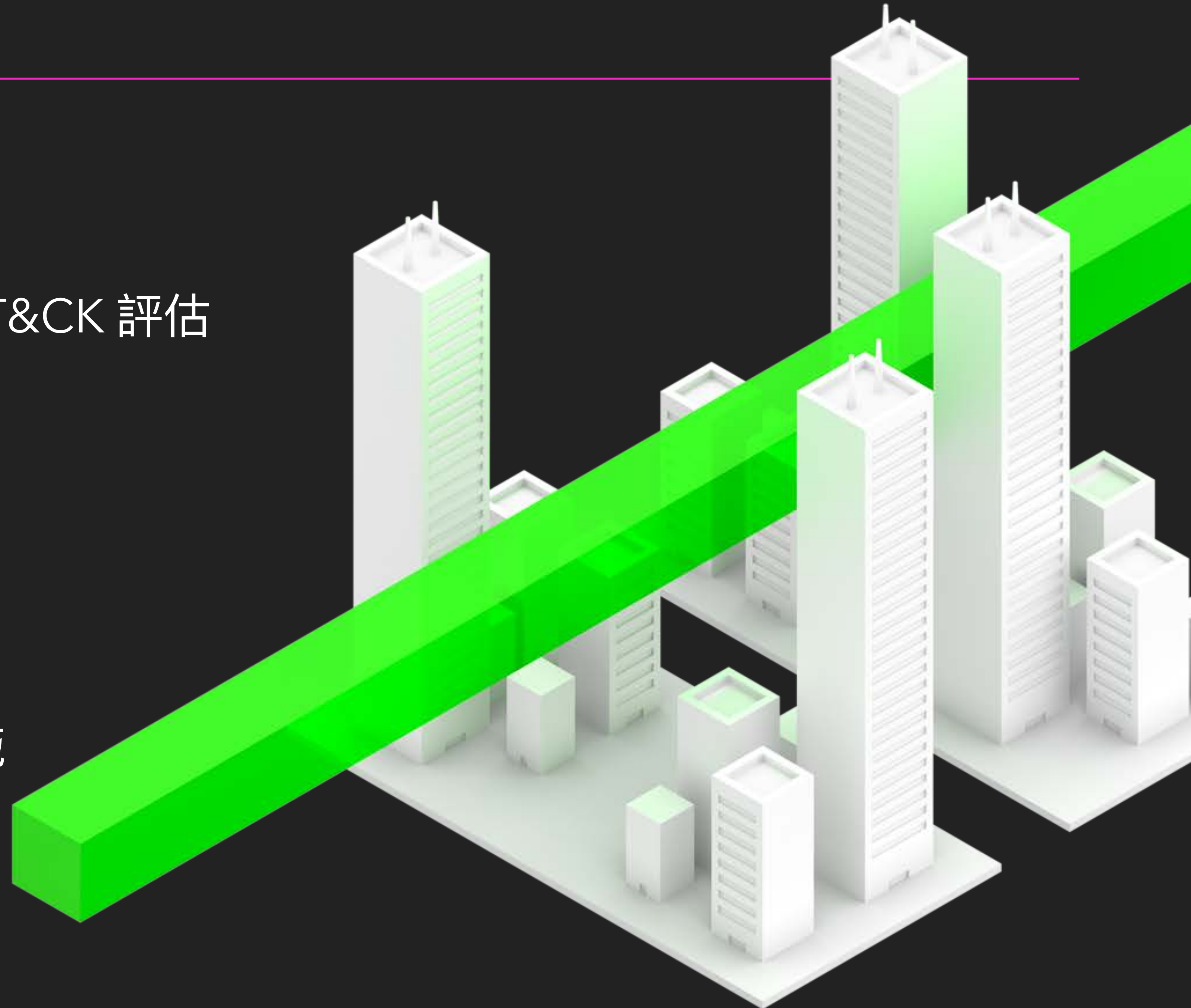
- 用正確的方式回顧過往 ATT&CK 評估

今年底嘗試：

- 盤點防禦機制的 ATT&CK，
並與資安事件核對

明年開始：

- 逐步強化阻斷攻擊鍊的措施



透過 ATT&CK 讓攻與防共創成果

戴夫寇爾股份有限公司

contact@devco.re

Q&A