DEVCORE
SECURITY
CONSULTING

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

DEVCORE SECURITY CONSULTING


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
DETERMINATION
PROXY
LOGON
HACKER MINDSET
PENETRATION
TEST
MAN IN THE MIDDLE
LATERAL MOVEMENT
STACK SMASHING
INJECTION
USE AFTER FREE
BUG BOUNTY
META-PROGRAMMING
CROSS-SITE SCRIPTING
PASS THE TICKET
PRIVILEGE ESCALATION
XXE
CREDENTIAL STUFFING
DEVCORE

DEVCORE
SECURITY
CONSULTING

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

DEVCORE SECURITY CONSULTING

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

https://www.securityweek.com/national-cybersecurity-agencies-list-most-exploited-vulnerabilities-2021

2021 年最常被利用的15 個漏洞








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**

DEVCORE SECURITY CONSULTING

https://www.securityweek.com/national-cybersecurity-agencies-list-most-exploited-vulnerabilities-2021

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

如何正確使用紅隊演練

DEVCORE SECURITY CONSULTING

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

MITRE ATT&CK™ Enterprise Framework

attack.mitre.org

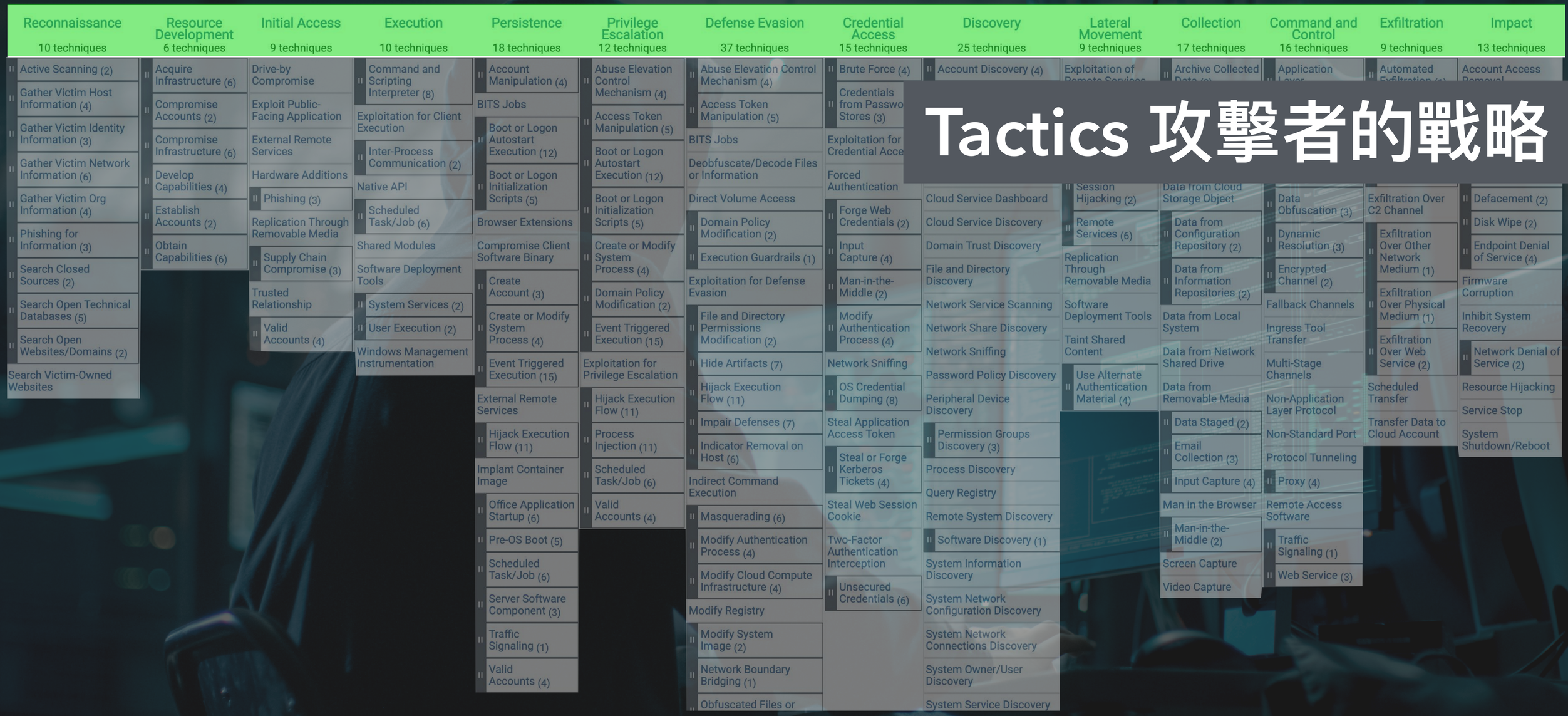
MITRE


MITRE
ATT&CK®
Adversarial Tactics, Techniques, and Common Knowledge
https://attack.mitre.org/

MITRE | ATT&CK® Matrix for Enterprise

https://attack.mitre.org/matrices/enterprise/

MITRE | ATT&CK® Matrix for Enterprise



Tactics 攻擊者的戰略

https://attack.mitre.org/matrices/enterprise/

MITRE | ATT&CK®

Matrix for Enterprise

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

https://attack.mitre.org/matrices/enterprise/

MITRE | ATT&CK® Matrix for Enterprise

Tactics 攻擊者的戰略

Techniques 攻擊者的技術

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

https://attack.mitre.org/matrices/enterprise/

MITRE | ATT&CK® Matrix for Enterprise

https://attack.mitre.org/matrices/enterprise/

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.

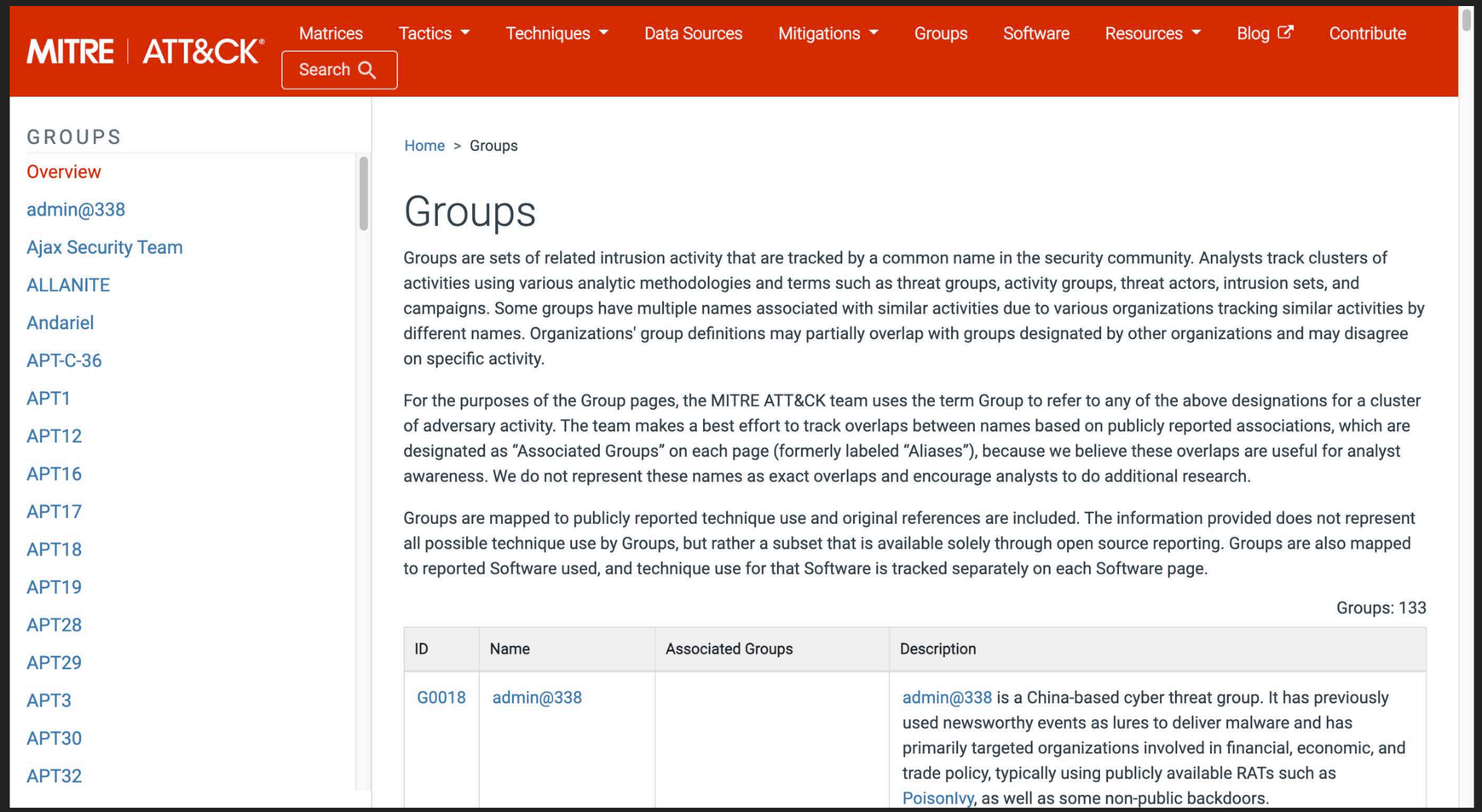
Enterprise Tactics

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

menuPass
Moafee
Mofang
Molerats
MuddyWater
Mustang Panda
Naikon
NEODYMIUM
Night Dragon
Nomadic Octopus
OilRig
Operation Wocao
Orangeworm
Patchwork
PittyTiger
PLATINUM
Poseidon 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 2014 and 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]

ID: G0045

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

Contributors: Edward Millington; Wyatt Roux

Version: 2.1

Created: 31 May 2017

Last Modified: 11 October 2021

Version Permalink

Associated Group Descriptions

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

APT 10 分析

APT組織分析，包含攻擊手法、戰略、工具方式。

APT10 (menuPass)

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

DEVCORE SECURITY CONSULTING

APT10
(menuPass)

https://mitre-attack.github.io/attack-navigator//#layerURL=https%3A%25%2Fattack.mitre.org%2FGroups%2FG0045%2FG0045-enterprise-layer.json

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					

DEVCORE SECURITY CONSULTING

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		
				Valid Accounts		Modify Authentication Process		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」🤣

DEVCORE SECURITY CONSULTING

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		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					

DEVCORE SECURITY CONSULTING

DEVCORE

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					

DEVCORE SECURITY CONSULTING

APT38

APT10

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					

DEVCORE SECURITY CONSULTING

DEVCORE

Recon.	Resource Dev.	Initial Access	Execution	Persistence	Privilege	Defense Evasion	Credential	Discovery	Lateral Movem	Collecti on	Comma nd and	Exfiltrati on	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 Deploy Container	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 Identity Information	Compromise Infrastructure	External Remote Services	Exploitation for Client Execution	Boot or Logon Autostart Execution	BITS Jobs	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	Inter-Process Communication	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	Native API	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	Scheduled Task/Job	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	Shared Modules	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	Software Deployment Tools	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	System Services	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			User Execution	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
			Windows Management Instrumentation	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
				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					

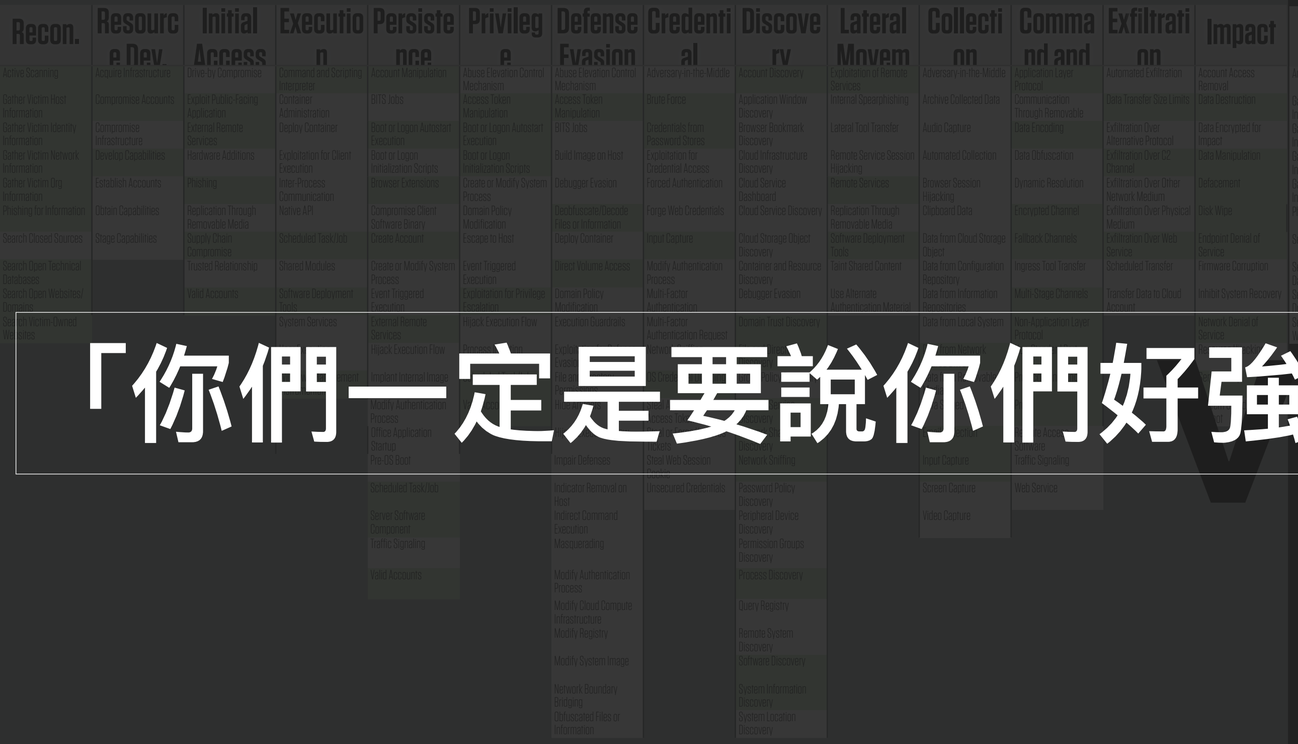
VS

APT10

Recon.	Resource Dev.	Initial Access	Execution	Persistence	Privilege	Defense Evasion	Credential	Discovery	Lateral Movem	Collecti on	Comma nd and	Exfiltrati on	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 Deploy Container	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 Identity Information	Compromise Infrastructure	External Remote Services	Exploitation for Client Execution	Boot or Logon Autostart Execution	BITS Jobs	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	Inter-Process Communication	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	Native API	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	Scheduled Task/Job	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	Shared Modules	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	Software Deployment Tools	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	System Services	External Remote Services	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			User Execution	Hijack Execution Flow	Hijack Execution Flow	Execution Guardrails	Multi-Factor Authentication Request	Domain Trust Discovery		Data from Local System	Non-Application Layer Protocol		Network Denial of Service
			Windows Management Instrumentation	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
				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					

DEVCORE

APT10



VS

「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！」

VS

『不是！！是你們進入了 ATT&CK 的誤區。』

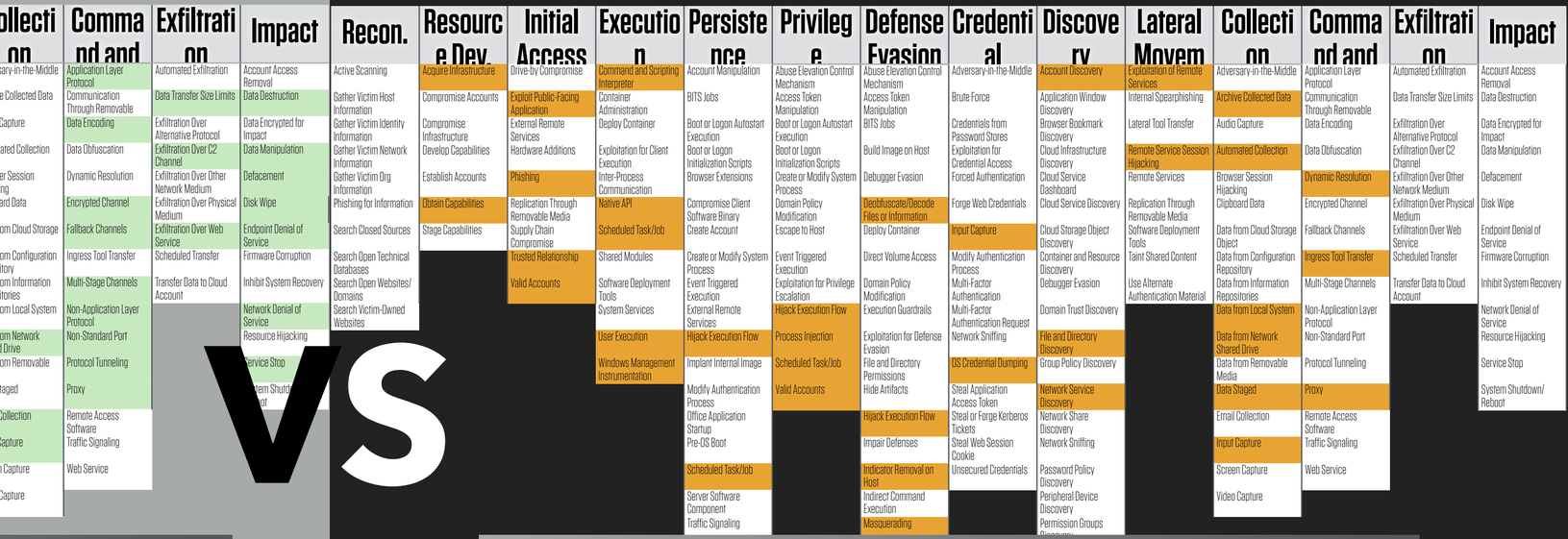
DEVCORE

演練後提供整理的結果

完整、正確性極高

VS

APT10

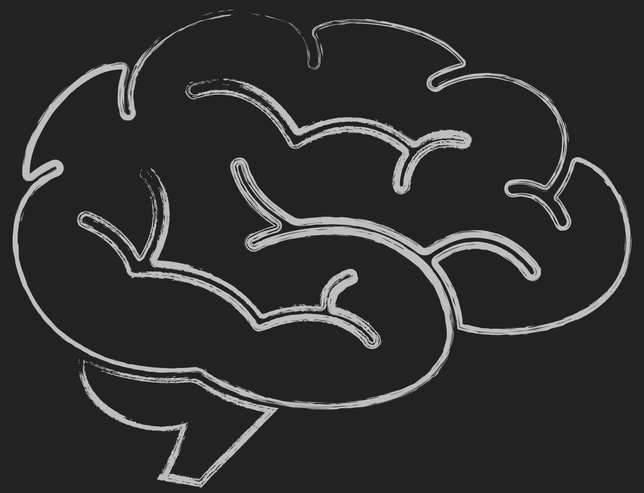


根據事件分析的結果

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

DEVCORE SECURITY CONSULTING

「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：

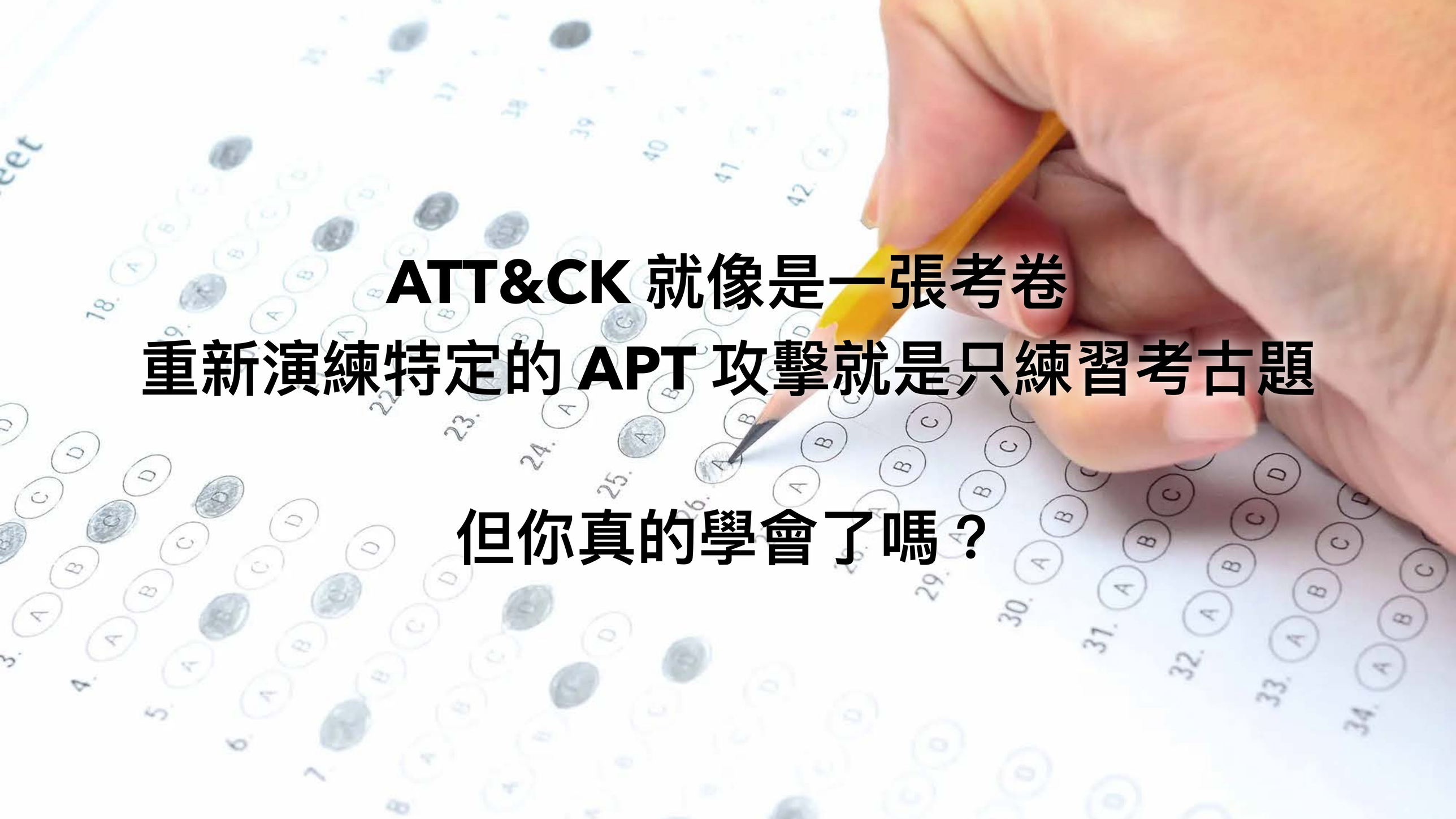
1. 以特定族群的 Tactics, Techniques, Procedures (TTPs) 來驗證產業的安全

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


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

https://www.csoonline.com/article/3153707/top-cybersecurity-facts-figures-and-statistics.html

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		
								t Capture	Traffic Signaling		
								en Capture	Web Service		
								o 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™

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					

DEVCORE SECURITY CONSULTING

APT38

APT10

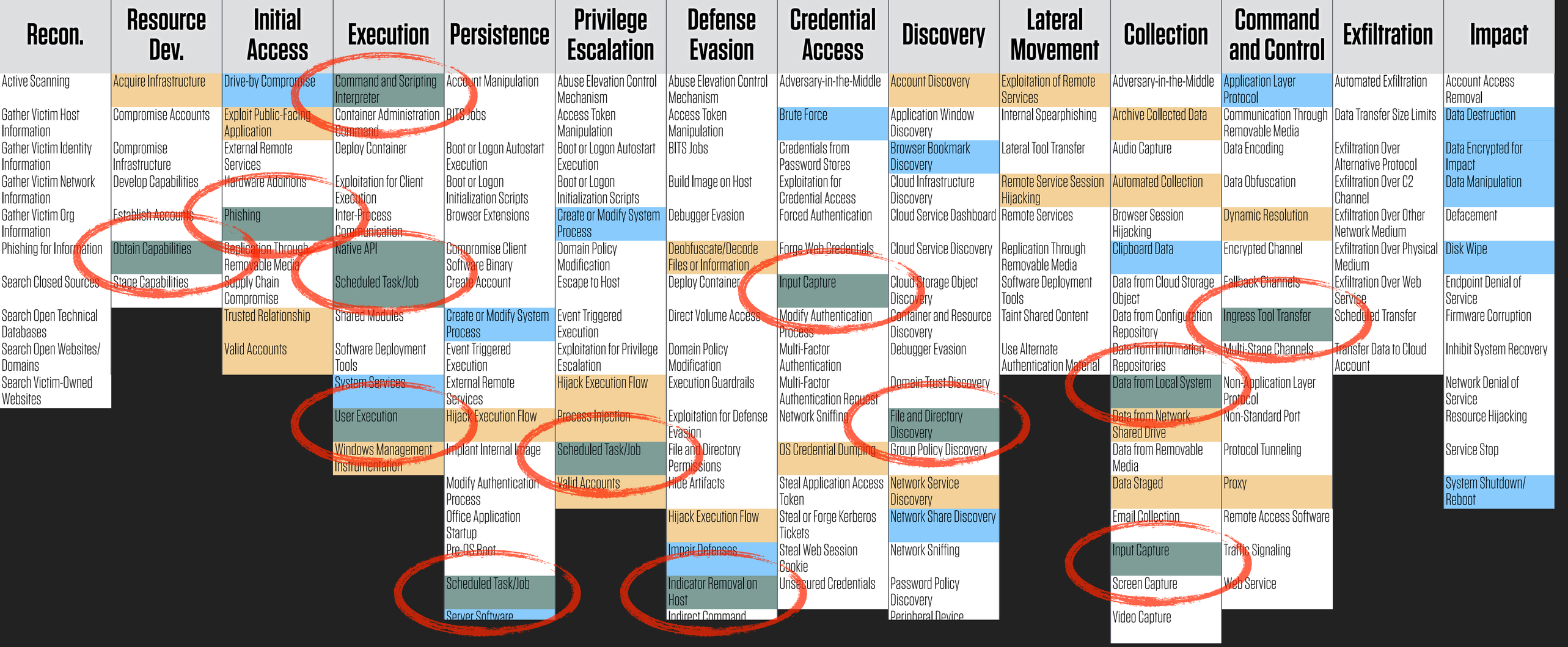
Recon.	Resource Dev.	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Active Scanning	Acquire Infrastructure	Drive-by Compromise	Command and Scripting Interpreter	Account Manipulation	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					

DEVCORE SECURITY CONSULTING

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

DEVCORE SECURITY CONSULTING

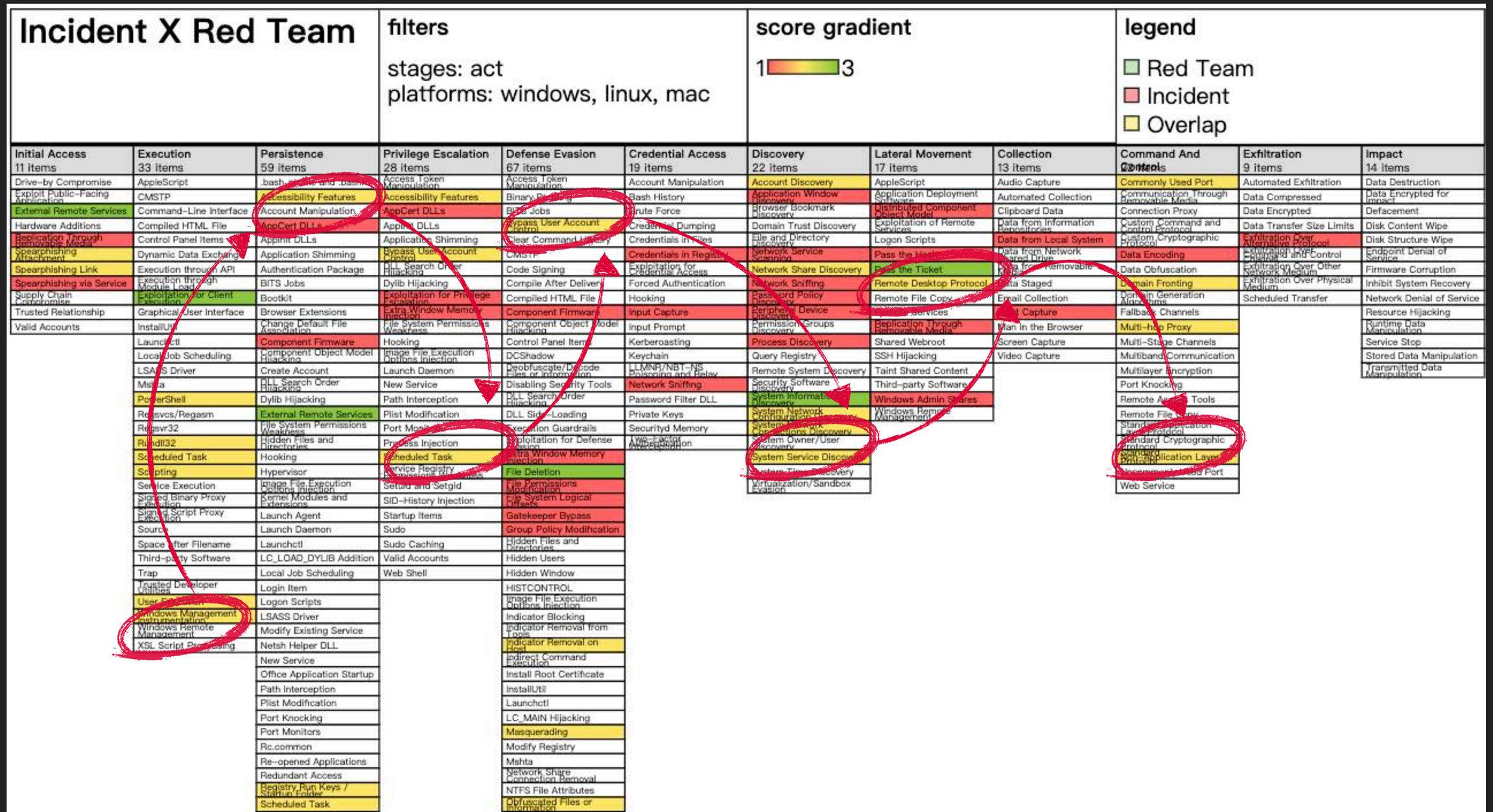


- 需要注意在不同組織的相同手法，
  是不能出錯的基本必考題（常見手法）

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



紅隊演練搭配 ATT&CK 檢視防禦狀態

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

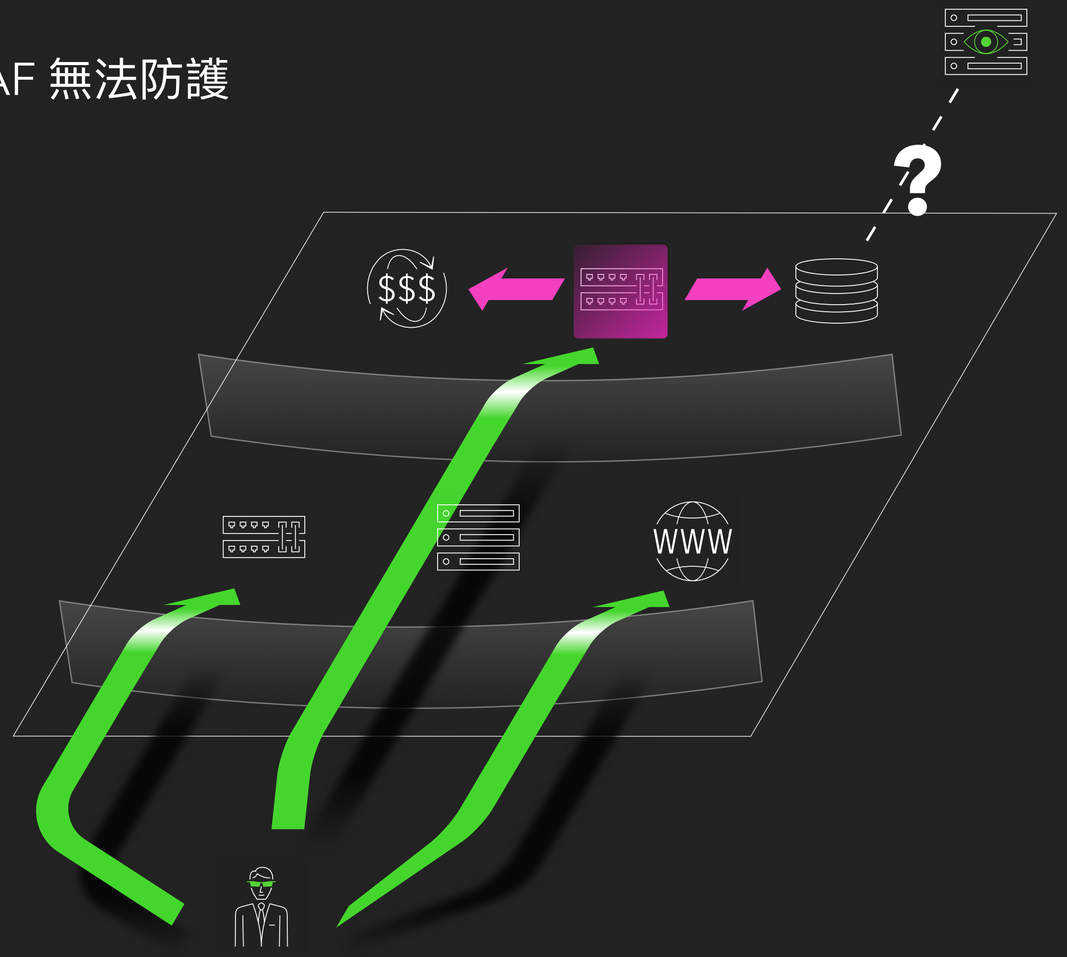
合法連線行為、網段區隔不良、ACL 不完善

#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



DEVCORE SECURITY CONSULTING

Takeaways

馬上進行：

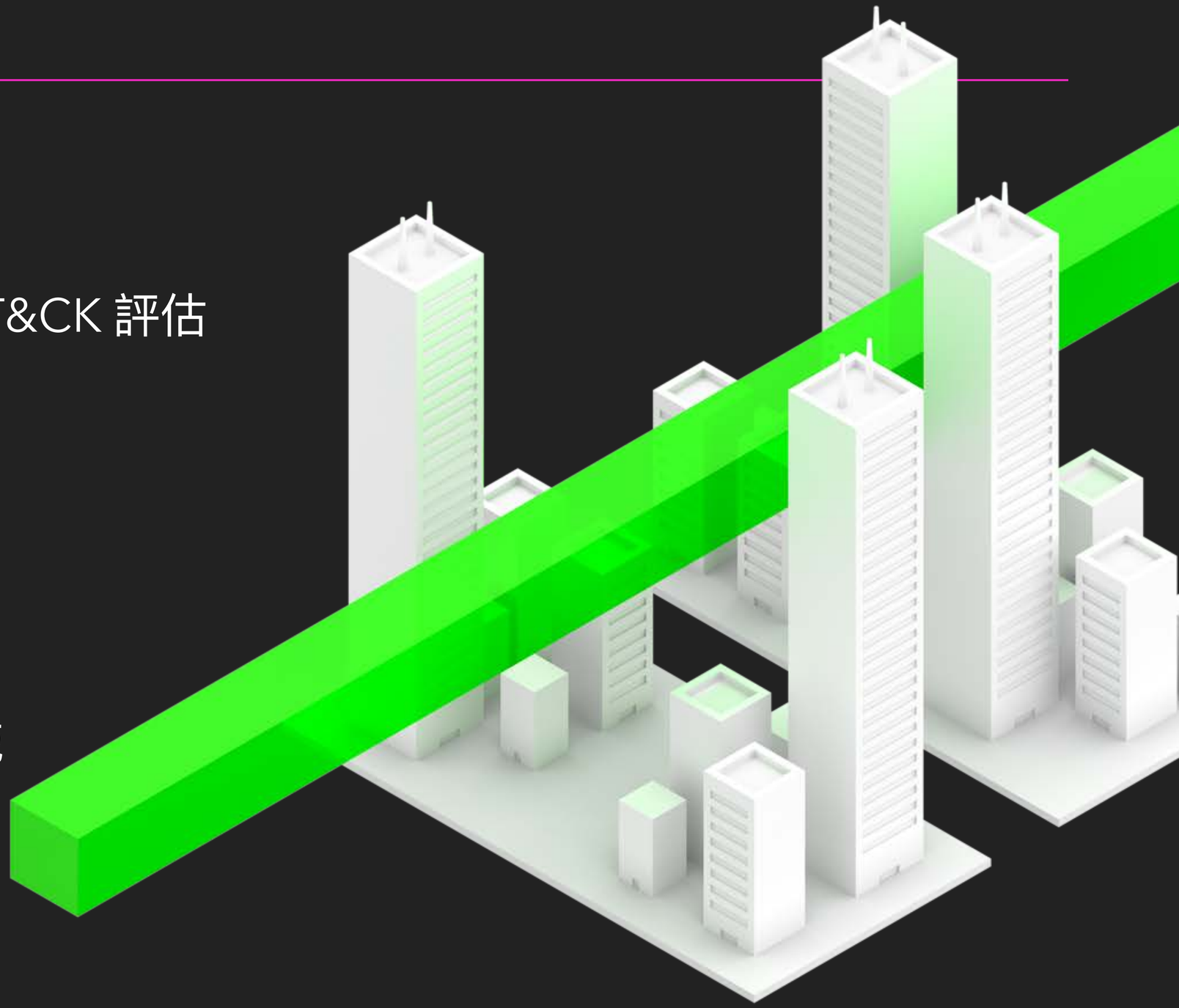
- 用正確的方式回顧過往 ATT&CK 評估

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



DEVCORE SECURITY CONSULTING

DEVCORE
SECURITY
CONSULTING

透過 ATT&CK 讓攻與防共創成果

Q&A

戴夫寇爾股份有限公司

contact@devco.re