

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 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

130十個漏洞揭露

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

30十場 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





CVE	Vulnerability Name	Vendor and Product	Туре
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





CVE	Vulnerability Name	Vendor and Product	Туре
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



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

____object = mirror_ob

總統府衛生福利部交通部中央健康保險署台北市政府

object is not Mone

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



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	LAGCUNON	Scheduled Task	1 Hivnege Escalation	Binary Padding		k Sniffing	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Data Destruction
, ,	Laur	nchctl	Access Toke	n Manipulation	Account Manipulation	Account Discovery		Automated Collection	,	Data Compressed	Data Encrypted for Impact
Exploit Public-Facing Application		Scheduling		Account Control	Bash History		Application Deployment Software	Clipboard Data	Communication Through Removable Media	Data Encrypted	Defacement Defacement
External Remote Services		S Driver	71	Memory Injection	Brute Force	Application Window Discovery	Dietaih. de d Consonant	•	Connection Proxy	Data Transfer Size Limits	Disk Content Wipe
Hardware Additions		rap		s Injection	Credential Dumping	Browser Bookmark	Distributed Component Object Model	Data from Information Repositories	Custom Command and	Exfiltration Over Other	Disk Structure Wipe
Replication Through	AppleScript		DLL Search Order Hijacking	,	Credentials in Files	Discovery	Exploitation of	Data from Local System	Control Protocol	Network Medium	Endpoint Denial of Service
Removable Media	CMSTP	l	mage File Execution Options Inject	ion	Credentials in Registry	Domain Trust Discovery	Remote Services	Data from Network	Custom Cryptographic	Exfiltration Over Command	Firmware Corruption
Spearphishing Attachment	Command-Line Interface		Plist Modification		Exploitation for	File and Directory Discovery	Logon Scripts	Shared Drive	Protocol	and Control Channel	Inhibit System Recovery
Spearphishing Link	Compiled HTML File		Valid Accounts		Credential Access	Network Service Scanning	Pass the Hash	Data from Removable Media	Data Encoding	Exfiltration Over Alternative	Network Denial of Service
Spearphishing via Service	Control Panel Items	Accessibil	ity Features	BITS Jobs	Forced Authentication	Network Share Discovery	Pass the Ticket	Data Staged	Data Obfuscation	Protocol	Resource Hijacking
Supply Chain Compromise	Dynamic Data Exchange	AppCe	ert DLLs	Clear Command History	Hooking	Password Policy Discovery	Remote Desktop Protocol	Email Collection	Domain Fronting	Exfiltration Over	Runtime Data Manipulation
Trusted Relationship	Execution through API	Appln	it DLLs	CMSTP	Input Capture	Peripheral Device Discovery	Remote File Copy	Input Capture	Domain Generation	Physical Medium	Service Stop
Valid Accounts	Execution through	Application	n Shimming	Code Signing	Input Prompt	Permission Groups Discovery	Remote Services	Man in the Browser	Algorithms	Scheduled Transfer	Stored Data Manipulation
	Module Load	Dylib F	Hijacking	Compiled HTML File	Kerberoasting	Process Discovery	Replication Through	Screen Capture	Fallback Channels		Transmitted Data
	Exploitation for	File System Perm	nissions Weakness	ons Weakness Component Firmware		Query Registry	Removable Media	Video Capture	Multiband Communication		Manipulation
	Client Execution	Hooking		Component Object Model	LLMNR/NBT-NS Poisoning	Remote System Discovery	Shared Webroot		Multi-hop Proxy		
	Graphical User Interface	Launch	Daemon	Hijacking	and Relay	Security Software Discovery	SSH Hijacking		Multilayer Encryption		
	InstallUtil	New S	Service	Control Panel Items	Password Filter DLL	System Information	Taint Shared Content		Multi-Stage Channels		
	Mshta	Path Interception		DCShadow	Private Keys	Discovery	Third-party Software		Port Knocking		
	PowerShell	Port Monitors		Deobfuscate/Decode Files	Securityd Memory	System Network	Windows Admin Shares		Remote Access Tools		
	Regsvcs/Regasm	Service Registry Pe	ermissions Weakness	or Information	Two-Factor Authentication	Configuration Discovery	Windows Remote		Remote File Copy		
	Regsvr32	Setuid a	and Setgid	Disabling Security Tools	Interception	System Network	Management		Standard Application Layer		
	Rundll32	Startu	p Items	DLL Side-Loading		Connections Discovery			Protocol		
	Scripting	Web	Shell	Execution Guardrails		System Owner/User			Standard Cryptographic		
	Service Execution	.bash_profile and .bashrc	Exploitation for	Exploitation for		Discovery			Protocol		
	Signed Binary	Account Manipulation	Privilege Escalation	Defense Evasion		System Service Discovery			Standard Non-Application		
	Proxy Execution	Authentication Package	SID-History Injection	File Deletion		System Time Discovery			Layer Protocol		
	Signed Script Proxy Execution	BITS Jobs	Sudo	File Permissions Modification		Virtualization/Sandbox Evasion			Uncommonly Used Port		
	,	Bootkit	Sudo Caching			EVASION			Web Service		
	Source	Browser Extensions		File System Logical Offsets							
	Space after Filename	Change Default File Association		Gatekeeper Bypass							
	Third-party Software		_	Group Policy Modification Hidden Files and Directories							
	Trusted Developer Utilities User Execution	Component Firmware	_	Hidden Users							
		Component Object Model Hijacking		Hidden Window							
	Windows Management Instrumentation	Create Account	_	HISTCONTROL							
	Maria de la Companya de	External Remote Services		Indicator Blocking							
	Windows Remote Management	Hidden Files and Directories	-								
	XSL Script Processing	Hypervisor	-	Indicator Removal from Tools							
		Kernel Modules		Indicator Removal on Host							
		Kernel Modules and Extensions		Indirect Command Execution							
		Launch Agent		Install Root Certificate		AITP		TOO	I I I I I		
		LC_LOAD_DYLIB Addition		InstallUtil		\/ <i> </i>		IX/			
		Login Item		Launchctl		MITR		ICX			
		1	İ.								

LC_MAIN Hijacking

Masquerading

Modify Registry

Mshta

Network Share Connection Removal

NTFS File Attributes

Obfuscated Files or Information

Port Knocking

Process Doppelgänging

Process Hollowing

Redundant Access Regsvcs/Regasm

Rootkit

Rundll32

Scripting Signed Binary Proxy Execution

_Signed Script

SIP and Trust Provider Hijacking Software Packing Space after Filename Template Injection Timestomp

Trusted Developer Utilities

Virtualization/Sandbox

XSL Script Processing

Logon Scripts

Modify Existing Service

Netsh Helper DLL

Office Application Startup

Port Knocking

Rc.common

Redundant Access

Registry Run Keys / Startup Folder Re-opened Applications

Screensaver

Security Support Provider

Shortcut Modification

SIP and Trust Provider Hijacking System Firmware

Systemd Service

Time Providers

Windows Management Instrumentation Event Subscription

Winlogon Helper DLL

IVIIIIKL AI IQUI Enterprise Framework

attack.mitre.org





Matrix for Enterprise

System Service Discovery

				The same of the sa									
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	Account Manipulation (4)	Abuse Elevation Control	Abuse Elevation Control Mechanism (4)	II Brute Force (4)	Account Discovery (4)	Exploitation of Remote Services	Archive Collected Data (3)	Application II Layer	Automated Exfiltration (1)	Account Access Removal
Gather Victim Host Information (4)	Compromise	Exploit Public- Facing Application	Interpreter (8) Exploitation for Client	BITS Jobs	Mechanism (4) Access Token	Access Token Manipulation (5)	Credentials from Password	Application Window Discovery	Internal Spearphishing	Audio Capture	Protocol (4) Communication	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information (3)		External Remote	Execution	Boot or Logon II Autostart	Manipulation (5)	Manipulation (5) BITS Jobs	Stores (3) Exploitation for	Browser Bookmark Discovery	Lateral Tool	Automated Collection	Through Removable Media	Exfiltration	Data Encrypted for Impact
Gather Victim Network	Infrastructure (6)	Services	Inter-Process Communication (2)	Execution (12)	AND THE PERSON OF THE PERSON O	Deobfuscate/Decode Files	Credential Access	Cloud Infrastructure	Transfer	Clipboard Data	Data	Over Alternative	Data
Information (6)	Develop Capabilities (4)	Hardware Additions	Native API	Boot or Logon Initialization	Execution (12)	or Information	Forced Authentication	Discovery	Remote Service Session	Data from Cloud	Encoding (2)	Protocol (3)	Manipulation (3)
Gather Victim Org Information (4)	Establish	Phishing (3)	Scheduled	Scripts (5)	Boot or Logon Initialization	Direct Volume Access	Forge Web	Cloud Service Dashboard	Hijacking (2)	Storage Object	Data Obfuscation (3)	Exfiltration Over C2 Channel	Defacement (2)
Phishing for		Replication Through Removable Media	A A W-C - 1(0)	Browser Extensions	Scripts (5)	Domain Policy Modification (2)	Credentials (2)	Cloud Service Discovery	Remote Services (6)	Data from Configuration	Dynamic	Exfiltration	Disk Wipe (2)
Information (3)	Obtain Capabilities (6)	Supply Chain	A STATE OF THE PARTY OF THE PAR	Compromise Client Software Binary	Create or Modify System	II Execution Guardrails (1)	Input Capture (4)	Domain Trust Discovery	Replication	Repository (2)	Resolution (3)	Over Other Network	Endpoint Denial of Service (4)
Search Closed Sources (2)		" Compromise (3) Trusted	Software Deployment Tools	Create Account (3)	Process (4) Domain Policy	Exploitation for Defense Evasion	Man-in-the- Middle (2)	File and Directory Discovery	Through Removable Media	Data from Information Repositories (2)	Encrypted Channel (2)	Medium (1) Exfiltration	Firmware Corruption
Search Open Technical Databases (5)		Relationship	System Services (2)	Create or Modify	Modification (2)	File and Directory	Modify	Network Service Scanning	Software Deployment Tools	Data from Local	Fallback Channels	II Over Physical	Inhibit System
Search Open		Valid Accounts (4)	User Execution (2)	System Process (4)	Event Triggered Execution (15)	Permissions Modification (2)	Authentication Process (4)	Network Share Discovery	Taint Shared	System	Ingress Tool Transfer	Exfiltration	Recovery
Websites/Domains (2)		7.0000 (4)	Windows Management Instrumentation			Hide Artifacts (7)	Network Sniffing	Network Sniffing	Content	Data from Network Shared Drive		II Over Web	Network Denial of Service (2)
Search Victim-Owned Websites				Execution (15)	Privilege Escalation	Hijack Execution	OS Credential	Password Policy Discovery	Use Alternate Authentication	Data from	Channels	Scheduled	Resource Hijacking
				External Remote Services	Hijack Execution Flow (11)	Flow (11)	Dumping (8)	Peripheral Device Discovery	Material (4)	Removable Media	Non-Application Layer Protocol	Transfer	Service Stop
				Hijack Execution	Process	Impair Defenses (7)	Steal Application Access Token	Permission Groups		Data Staged (2)	Non-Standard Port	Transfer Data to Cloud Account	System
				Flow (11) Implant Container	Injection (11) Scheduled	Indicator Removal on Host (6)	Steal or Forge Kerberos	Discovery (3) Process Discovery	No. of Contract of	Email Collection (3)	Protocol Tunneling		Shutdown/Reboot
				Image	Task/Job (6)	Indirect Command Execution	Tickets (4)	Query Registry		II Input Capture (4)	II Proxy (4)		
				Office Application Startup (6)	Valid	II Masquerading (6)	Steal Web Session Cookie	Remote System Discovery	7		Remote Access Software		
				II Pre-OS Boot (5)		Modify Authentication	Two-Factor	Software Discovery (1)	Complete Applicate Application	Man-in-the- Middle (2)	Traffic		
				Scheduled Task (lab (s)		Process (4)	Authentication Interception	System Information		Screen Capture	Signaling (1)		
				Task/Job (6) Server Software		Modify Cloud Compute Infrastructure (4)	Unsecured Credentials (6)	Discovery System Network	TVI N	Video Capture	Web Service (3)		
				Component (3)	1	Modify Registry	Oredentials (6)	Configuration Discovery					
				Traffic Signaling (1)		Modify System Image (2)		System Network Connections Discovery					
				Valid Accounts (4)		Network Boundary Bridging (1)		System Owner/User Discovery	Marine III				

Obfuscated Files or

Matrix for Enterprise

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	Account Manipulation (4)	Abuse Elevation Control	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	Exploit Public-	Interpreter (8)	BITS Jobs	Mechanism (4)	Access Token	Credentials II from Passwo			_,,		, , , , , , , , , , , , , , , , , , ,	
Gather Victim Identity	Accounts (2)	Facing Application	Exploitation for Client Execution	Boot or Logon	Access Token Manipulation (5)	Manipulation (5)	Stores (3)	Tact					长四文
Information (3)	Compromise Infrastructure (6)	External Remote Services	Inter-Process	Autostart Execution (12)	Boot or Logon	BITS Jobs	Exploitation for Credential Acce	Tacti	(C)	以事		コリ異	人叫口
Gather Victim Network Information (6)	Develop	Hardware Additions	Communication (2)	Boot or Logon	Autostart Execution (12)	Deobfuscate/Decode Files or Information	Forced						
Gather Victim Org	Capabilities (4)	Phishing (3)	Native API	II Initialization Scripts (5)	Boot or Logon	Direct Volume Access	Authentication	Cloud Service Dashboard	Session Hijacking (2)	Storage Object	Data	Exfiltration Over	Defacement (2)
Information (4)	Establish Accounts (2)	Replication Through	Scheduled Task/Job (6)	Browser Extensions	Initialization Scripts (5)	Domain Policy	Forge Web Credentials (2)	Cloud Service Discovery	Remote	Data from	Obfuscation (3)	C2 Channel	Disk Wipe (2)
Phishing for Information (3)	Obtain Capabilities (6)	Removable Media Supply Chain	Shared Modules	Compromise Client Software Binary	Create or Modify System	Modification (2) Execution Guardrails (1)	Input Capture (4)	Domain Trust Discovery	Services (6) Replication	Configuration Repository (2)	Dynamic Resolution (3)	Exfiltration Over Other Network	Endpoint Denial of Service (4)
Search Closed Sources (2)	Capabilities (6)	Compromise (3)	Software Deployment Tools	Create	Process (4)	Exploitation for Defense	Man-in-the-	File and Directory Discovery	Through Removable Media	Data from II Information	Encrypted Channel (2)	Medium (1)	Firmware
Search Open Technical		Trusted Relationship	System Services (2)	Account (3)	Domain Policy Modification (2)	Evasion	Middle (2)	Network Service Scanning		Repositories (2)	Fallback Channels	Exfiltration Over Physical	Corruption
Databases (5)		, Valid	User Execution (2)	Create or Modify System	Event Triggered	File and Directory Permissions	Modify Authentication	Network Share Discovery	Deployment Tools	Data from Local System	Ingress Tool	Medium (1)	Inhibit System Recovery
Search Open Websites/Domains (2)		" Accounts (4)	Windows Management		Execution (15)	Modification (2)	Process (4)	Network Sniffing	Taint Shared Content	Data from Network	Transfer	Exfiltration Over Web	Network Denial of
Search Victim-Owned			Instrumentation		Exploitation for Privilege Escalation		Network Sniffing	Password Policy Discovery	Use Alternate	Shared Drive	Multi-Stage Channels	Service (2)	Service (2)
Websites				External Remote	Hijack Execution	Hijack Execution Flow (11)	OS Credential Dumping (8)	Peripheral Device	Authentication Material (4)	Data from Removable Media	Non-Application	Scheduled Transfer	Resource Hijacking
				Services Hijack Execution	Flow (11) Process	III Impair Defenses (7)	Steal Application Access Token	Discovery Permission Groups		II Data Staged (2)	Layer Protocol Non-Standard Port	Transfer Data to Cloud Account	Service Stop System
				Flow (11)	Injection (11)	Indicator Removal on Host (6)	Steal or Forge	Discovery (3)		Email Collection (3)	Protocol Tunneling	Cloud Account	Shutdown/Reboot
				Implant Container Image	Scheduled Task/Job (6)	Indirect Command	Kerberos Tickets (4)	Process Discovery	- 182	Input Capture (4)			
				,, Office Application		Execution	Steal Web Session	Query Registry	Carlot Arthur	Man in the Browser			
				Startup (6)	Accounts (4)	Masquerading (6)	Cookie	Remote System Discovery		Man-in-the-	Software		
				Pre-OS Boot (5)		Modify Authentication Process (4)	Two-Factor Authentication	Software Discovery (1)	Com Lambara Sant Sarva April 4	Middle (2)	Traffic Signaling (1)		
				Scheduled Task/Job (6)		Modify Cloud Compute	Interception	System Information Discovery		Screen Capture	Web Service (3)		
				Server Software		Infrastructure (4)	Unsecured Credentials (6)	System Network	'Y	Video Capture	Sell make 1		
				Component (3)		Modify Registry Modify System		Configuration Discovery System Network					
				Signaling (1)		Image (2)		Connections Discovery					
				Valid Accounts (4)		Network Boundary Bridging (1)		System Owner/User Discovery	Marie and				
						Obfuscated Files or		System Service Discovery					
						Allen	A		The state of the s	https://atta	ck.mitre.org	n/matrices	/enterprise/
										Tree on racea		<i>y- 11 13 61 13 3 3</i>	

Matrix for Enterprise

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

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	Account Manipulation (4)	Abuse Elevation Control	Abuse Elevation Control Mechanism (4)	Brute Force (4)	Account Discovery (4)	Exploitation of Remote Services	Archive Collected Data (3)	II Layer	Automated Exfiltration (1)	Account Access Removal
Gather Victim Host Information (4)	Compromise	Exploit Public-	Interpreter (8) Exploitation for Client	BITS Jobs	Mechanism (4) Access Token	Access Token Manipulation (5)	Credentials from Password	Application Window Discovery	Internal Spearphishing	Audio Capture	Protocol (4) Communication	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information (3)	Accounts (2) Compromise	Facing Application External Remote	Execution	Boot or Logon Autostart	Manipulation (5)	Manipulation (5) BITS Jobs	Stores (3) Exploitation for	Browser Bookmark Discovery	Lateral Tool	Automated Collection	Through Removable Media	Exfiltration	Data Encrypted for Impact
Gather Victim Network	Infrastructure (6)	Services	Inter-Process Communication (2)	Execution (12)	Boot or Logon Autostart	Deobfuscate/Decode Files	Credential Access	Cloud Infrastructure	Transfer	Clipboard Data	Data	Over Alternative	Data
Information (6) Gather Victim Org	Develop Capabilities (4)	Hardware Additions Phishing (3)	Native API	Boot or Logon Initialization	Execution (12) Boot or Logon	or Information Direct Volume Access	Forced Authentication	Discovery Cloud Service Dashboard	Remote Service Session Hijacking (2)	Data from Cloud	Encoding (2) Data	Protocol (3) Exfiltration Over	Manipulation (3) Defacement (2)
Information (4)	Establish Accounts (2)	Replication Through	Scheduled Task/Job (6)	Scripts (5) Browser Extensions	II Initialization Scripts (5)	Domain Policy	Forge Web Credentials (2)	Cloud Service Dashboard Cloud Service Discovery	Remote	Storage Object Data from	Obfuscation (3)	C2 Channel	Disk Wipe (2)
Phishing for Information (3)	Obtain	Removable Media	Shared Modules	Compromise Client	Create or Modify	Modification (2)	Input	Domain Trust Discovery	Services (6)	Configuration Repository (2)	Dynamic Resolution (3)	Exfiltration Over Other	Endpoint Denial
Search Closed	Capabilities (6)	Supply Chain Compromise (3)	Software Deployment Tools	Software Binary Create	System Process (4)	Exploitation for Defense	Capture (4) Man-in-the-	File and Directory Discovery	Replication Through Removable Media	Data from Information	Encrypted Channel (2)	Network Medium (1)	of Service (4) Firmware
Search Open Technical		Trusted Relationship	System Services (2)	Account (3)	Domain Policy Modification (2)	Evasion	Middle (2)	Network Service Scanning	Software	Repositories (2)	Fallback Channels	Exfiltration Over Physical	Corruption
Databases (5)		Valid	User Execution (2)	Create or Modify System	Event Triggered	File and Directory Permissions		Network Share Discovery	Deployment Tools		Ingress Tool	Medium (1)	Inhibit System Recovery
Websites/Domains (2)		Accounts (4)	Windows Management	Process (4) Event Triggered	Execution (15) Exploitation for	Modification (2) Hide Artifacts (7)	Process (4) Network Sniffing	Network Sniffing	Taint Shared Content	Data from Network Shared Drive	Transfer Multi-Stage	Exfiltration Over Web Service (2)	Network Denial of Service (2)
Search Victim-Owned				Execution (15)	Privilege Escalation		OS Credential	Password Policy Discovery	Use Alternate	Data from	Channels	Scheduled	Resource Hijacking
				External Remote Services	Hijack Execution Flow (11)	Flow (11)	Dumping (8)	Peripheral Device Discovery	Material (4)	Removable Media	Non-Application Layer Protocol	Transfer	Service Stop
				Hijack Execution	Process	Impair Defenses (7)	Steal Application Access Token	Permission Groups		Data Staged (2)	Non-Standard Port	Transfer Data to Cloud Account	System
				Flow (11)	Injection (11)	Indicator Removal on	Steal or Forge Kerberos	Discovery (3) Process Discovery		Email Collection (3)	Protocol Tunneling		Shutdown/Reboot
Too				製造	46/71		Tickets (4)	Query Registry		Input Capture (4)			
IEC		que	s 攻	第1		XIII	Steal Web Session Cookie	Remote System Discovery		Man in the Browser Man-in-the-	Remote Access Software		
						F100ess (4)	Two-Factor Authentication	Software Discovery (1)		Middle (2)	Traffic Signaling (1)		
				Scheduled Task/Job (6)		Modify Cloud Compute	Interception	System Information Discovery		Screen Capture	Web Service (3)		
				Server Software Component (3)		Infrastructure (4) Modify Registry	Unsecured Credentials (6)	System Network Configuration Discovery		Video Capture	4 60 1		
				Traffic		Modify System		System Network					
				" Signaling (1) Valid		Image (2) Network Boundary		Connections Discovery System Owner/User					
				Accounts (4)		Bridging (1)		Discovery					
						Obfuscated Files or		System Service Discovery					

Matrix for Enterprise



Matrix for Enterprise

Poconnoiscence	Panauras	Initial Access	Evecution	Persistence	Drivilogo	Defense Evenier	Cradontial	Discovery	Lotorol	Collection	Command and	Evfiltration	Import
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
II Active Scanning (2)	Acquire	Drive-by	Command and	Account	Abuse Elevation	Abuse Elevation Control	Brute Force (4)	Account Discovery (4)	Exploitation of	Archive Collected	Application	Automated	Account Access
Gather Victim Host	Infrastructure (6)	Compromise	Scripting Interpreter (8)	Manipulation (4)	Control Mechanism (4)	Mechanism (4)	Credentials	Application Window	Remote Services	Data (3)	Layer Protocol (4)	Exfiltration (1)	Removal
Information (4)	Compromise Accounts (2)	Exploit Public- Facing Application	Exploitation for Client	BITS Jobs	Access Token	Access Token Manipulation (5)	from Password Stores (3)		Internal Spearphishing		Communication	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information (3)	Compromise Infrastructure (6)	External Remote Services	Execution Inter-Process	Boot or Logon Autostart Execution (12)	Manipulation (5) Boot or Logon	BITS Jobs	Exploitation for Credential Access	Browser Bookmark Discovery	Lateral Tool Transfer	Automated Collection	Through Removable Media	Exfiltration	Data Encrypted for Impact
Gather Victim Network Information (6)	Develop	Hardware Additions	Communication (2)	Boot or Logon	II Autostart	Deobfuscate/Decode Files or Information		Cloud Infrastructure Discovery	Remote Service	Clipboard Data	Data Encoding (2)	Alternative Protocol (3)	Data Manipulation (3)
Gather Victim Org	Capabilities (4)	Phishing (3)	Native API	Initialization Scripts (5)	\ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \	Direct Volume Access	Authentication	Cloud Service Dashboard		Data from Cloud Storage Object	Data	Exfiltration Over	Defacement (2)
Information (4)	Establish Accounts (2)	Replication Through	Scheduled Task/Job (6)	Browser Extensions	Initialization Scripts (5)	Domain Policy	Forge Web Credentials (2)	Cloud Service Discovery	Remote	Data from	Obfuscation (3)	C2 Channel	Disk Wipe (2)
Phishing for		Removable Media		Compromise Client	Create or Modify	Modification (2)		ıst Discovery	Services (6)	Configuration Repository (2)	Dynamic Resolution (3)	Exfiltration Over Other	
门连有前		Supply Chain Compromise (3)	Software Deployment Tools	Software Binary Create	System Process (4)	Exploita:		ectory	Replication Through Removable Media	Data from Information	Encrypted Channel (2)	Medium (1)	音之學學
	PETX	usted Lelationship	System Services (2)	Account (3)	Domain Policy Modification (2)	Evasion	X PEI	ervice Scanning	Software	Repositories (2)	Fallback Channels	Exfiltration Over Physical	小
Databases (5)		, Valid	User Execution (2)	Create or Modify System	Event Triggered	File and Directory Permissions		Network Share Discovery	Deployment Tools		Ingress Tool	Medium (1)	Inhibit System Recovery
Search Open Websites/Domains (2)		Accounts (4)	Windows Management	Process (4)	Execution (15)	Modification (2)	Process (4)	Network Sniffing	Taint Shared Content	Data from Network	Transfer	Exfiltration Over Web	Network Denial of
Search Victim-Owned Websites			Instrumentation		Exploitation for Privilege Escalation	Hide Artifacts (7) Hijack Execution	Network Sniffing OS Credential	Password Policy Discovery	Use Alternate	Shared Drive Data from	Multi-Stage Channels	Service (2) Scheduled	Service (2) Resource Hijacking
Websites	_			External Remote Services	Hijack Execution Flow (11)	Flow (11)	Dumping (8)	Peripheral Device Discovery	Material (4)	Removable Media	Non-Application Layer Protocol	Transfer	Service Stop
				Hijack Execution	Process	Impair Defenses (7)	Steal Application Access Token	Permission Groups		Data Staged (2)		Transfer Data to Cloud Account	System
				Flow (11)	Injection (11)	Indicator Removal on Host (6)	Steal or Forge	Discovery (3)		Email Collection (3)	Protocol Tunneling		Shutdown/Reboot
				Implant Container Image		Indirect Command Execution	Tickets (4)	Process Discovery		Input Capture (4)	II Proxy (4)		
				Office Application Startup (6)	Valid	Masquerading (6)	Steal Web Session	Query Registry Remote System Discovery		Man in the Browser	Remote Access Software		
				II Pre-OS Boot (5)		Modify Authentication	Two-Factor	II Software Discovery (1)		Man-in-the- Middle (2)	Traffic		
				Scheduled		Process (4)	Authentication Interception	System Information		Screen Capture	Signaling (1)		
				Task/Job (6)		Modify Cloud Compute Infrastructure (4)	Unsecured Credentials (1)	Discovery		Video Capture	Web Service (3)		
				Server Software Component (3)	1	Modify Registry	Credentials (6)	System Network Configuration Discovery					
				Traffic Signaling (1)		Modify System Image (2)		System Network Connections Discovery					
				Valid Accounts (4)		Network Boundary Bridging (1)		System Owner/User Discovery					
				(1)		Obfuscated Files or		System Service Discovery					

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.



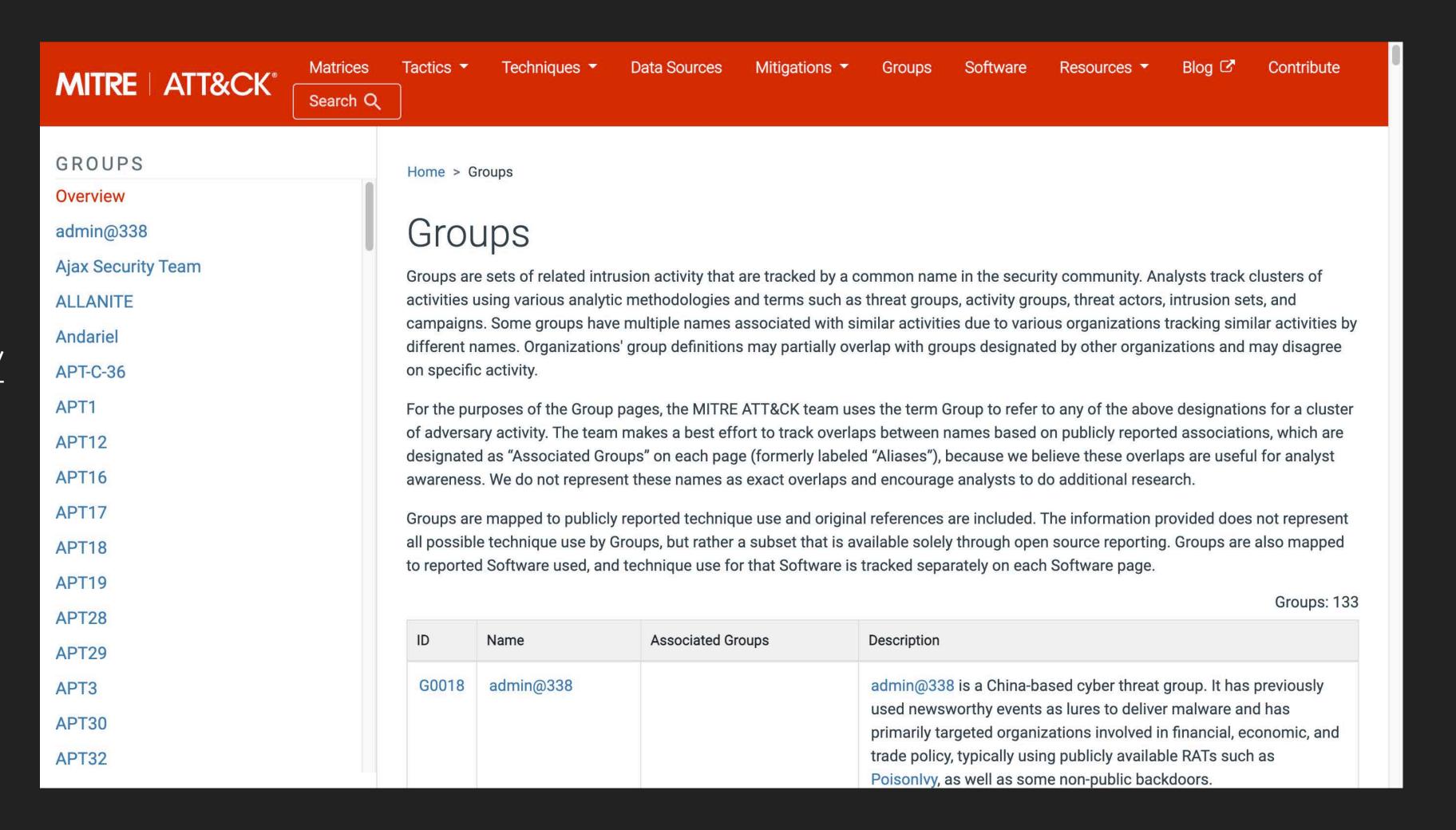
Enterprise Tactics

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/





Groups

GROUPS

menuPass

Moafee

Mofang

Molerats

MuddyWater

Mustang Panda

Naikon

NEODYMIUM

Night Dragon

Nomadic Octopus

OilRig

Operation Wocao

Orangeworm

Patchwork

PittyTiger

PLATINUM

B 11 - 8

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]

APT 10 分析

ID: G0045

Associated Groups: Cicada,
 POTASSIUM, Stone Panda, APT10, Red

Apollo, CVNX, HOGFISH

menuPass has targeted healthcare, defense, aerospace, finance, maritime, biotechnology and part and p

Version Permalink

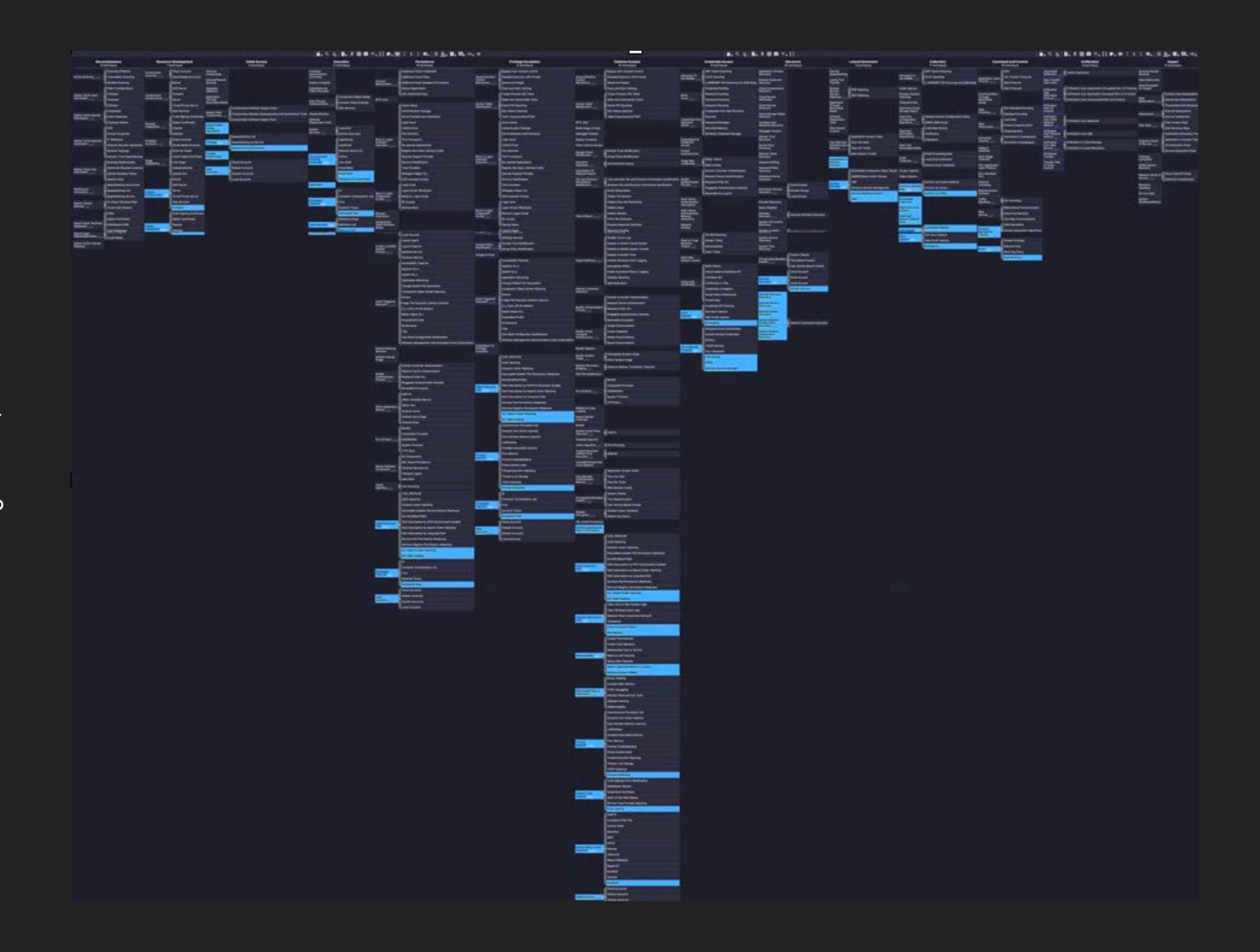
Associated Group Descriptions

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



APT10 (menuPass)

https://mitreattack.github.io/attacknavigator// #layerURL=https%3A% 2F%2Fattack.mitre.org %2Fgroups%2FG0045 %2FG0045-enterpriselayer.json





APT10 (menuPass)

先等等!

你們應該看過很多 APT組織 ATT&CK 了。

layer.json

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	Account Manipulation	Abuse Elevation Control	1	Adversary-in-the-Middle	Account Discovery	Exploitation of Remote	Adversary-in-the-Middle		Automated Exfiltration	Account Access
Gather Victim Host Information	Compromise Accounts	Exploit Public-Facing Application	Interpreter Container Administration Command	BITS Jobs	Mechanism Access Token Manipulation	Mechanism Access Token Manipulation	Brute Force	Application Window Discovery	Services Internal Spearphishing	Archive Collected Data	Protocol Communication Through Removable Media	Data Transfer Size Limits	Removal Data Destruction
	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
Information	Develop Capabilities	Hardware Additions	Exploitation for Client Execution		Initialization Scripts	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery	Hijacking	Automated Collection	Data Obfuscation	Exfiltration Over C2 Channel	Data Manipulation
Information	Establish Accounts	Phishing	Inter-Process Communication	Browser Extensions	Create or Modify System Process		Forced Authentication			Browser Session Hijacking	Dynamic Resolution	Exfiltration Over Other Network Medium	Defacement
Phishing for Information		Replication Through Removable Media	Native API	Compromise Client Software Binary	Modification	Deobfuscate/Decode Files or Information	Forge Web Credentials		Replication Through Removable Media	Clipboard Data	Encrypted Channel	Exfiltration Over Physical Medium	
	Stage Capabilities	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		Exfiltration Over Web Service	Endpoint Denial of Service
Search Open Technical Databases		Trusted Relationship	Shared Modules	Process	Execution	Direct Volume Access	Modify Authentication Process	Discovery		Data from Configuration Repository	Ingress Tool Transfer	Scheduled Transfer	Firmware Corruption
Search Open Websites/ Domains		Valid Accounts	Software Deployment Tools	Execution	Exploitation for Privilege Escalation	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	Services	Hijack Execution Flow		Multi-Factor Authentication Request	Domain Trust Discovery		Data from Local System Data from Notwork	Non-Application Layer Protocol Non-Standard Port		Network Denial of Service
			User Execution Windows Management	Hijack Execution Flow Implant Internal Image	Process Injection Scheduled Task/Job	Exploitation for Defense Evasion File and Directory		File and Directory Discovery Group Policy Discovery		Data from Network Shared Drive Data from Removable	Non-Standard Port Protocol Tunneling		Resource Hijacking Service Stop
			Instrumentation	Modify Authentication		Permissions	Steal Application Access			Media Data Staged	Proxy		System Shutdown/
				Process Office Application	Valia Accounts	Hijack Execution Flow	Token	Discovery Network Share Discovery		Email Collection	Remote Access Software		Reboot
				Startup Pre-OS Boot		,	Tickets Steal Web Session	Network Sniffing		Input Capture	Traffic Signaling		
				Scheduled Task/Job		Indicator Removal on Host	Cookie 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					

Modify System Image

Network Boundary Bridging Obfuscated Files or Information Discovery
Software Discovery

System Information
Discovery
System Location
Discovery





DE SEC

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	Account Manipulation	Abuse Elevation Control	Abuse Elevation Control	Adversary-in-the-Middle	Account Discovery	Exploitation of Remote	Adversary-in-the-Middle	Application Layer	Automated Exfiltration	Account Access
O a tha a Vi a tima I ha a t	0		Interpreter	DITO I ala a	Mechanism	Mechanism	Durita Farra	A a sali a a ti a sa NA/isa al a sus	Services	Aughius Oallastad Data	Protocol October 1 to 1 t	Data Tuanafan Olas Linsita	Removal
Gather Victim Host	Compromise Accounts		Container Administration	IRI12 1008		Access Token	Brute Force	_ ' '	Internal Spearphishing	Archive Collected Data	Communication Through	Dala Italisiel 2176 Fillills	Data Destruction
Information	Compromiso		Command Panloy Container	Doot or Logon Autostort		Manipulation	Orodontiala from	Discovery Drawper Dealtmark	Lateral Tool Transfer	1	Removable Media	Exfiltration Over	Data Engrupted for
Gather Victim Identity Information	Compromise Infrastructure	External Remote Services	Deploy Container	1_	Boot or Logon Autostart Execution	BITS Jobs	Credentials from Password Stores	Browser Bookmark	Lateral Tool Transfer	Audio Capture	_	Exfiltration Over Alternative Protocol	Data Encrypted for Impact
			Exploitation for Client	Execution Boot or Logon	Boot or Logon	 Build Image on Host		Discovery Cloud Infrastructure	 Remote Service Session	Automated Collection		Exfiltration Over C2	Data Manipulation
Information	ոշուլոի ոցիցոյյյյլու		Execution		Initialization Scripts	Dalla illiage oli fiosi	Credential Access	Discovery	Hijacking	Automaisu oonsonon		Channel	Data Manipulanon
	Establish Accounts			Browser Extensions	Create or Modify System	l Dehugger Evasion	Forced Authentication	Cloud Service Dashboard		Browser Session	Dynamic Resolution	Exfiltration Over Other	Defacement
Information	Lordonominio	_	Communication	Brownest Extremelers	Process	Donaggor Evacion	l orosa ramomicanom	ordad der vied Baeriseara		Hijacking		Network Medium	
Phishing for Information	Obtain Capabilities		Native API	Compromise Client	I	Deobfuscate/Decode	Forge Web Credentials	Cloud Service Discovery	Replication Through		Encrypted Channel	Exfiltration Over Physical	Disk Wipe
		Removable Media		Software Binary	Modification	Files or Information			Removable Media			Medium	
Search Closed Sources	Stage Capabilities	Supply Chain	Scheduled Task/Job	Create Account	Escape to Host	Deploy Container	Input Capture	Cloud Storage Object	Software Deployment	Data from Cloud Storage	Fallback Channels	Exfiltration Over Web	Endpoint Denial of
		Compromise						Discovery	Tools	Object		Service	Service
Search Open Technical		Trusted Relationship	Shared Modules	l_	l	Direct Volume Access	Modify Authentication	ls.	Taint Shared Content	l <u>_</u>	Ingress Tool Transfer	Scheduled Transfer	Firmware Corruption
Databases		W 10.1 A	0.6	Process	Execution		Process	Discovery		Repository		T. (D Ol	
Search Open Websites/			Software Deployment	_	Exploitation for Privilege	Domain Policy		Debugger Evasion	Use Alternate		Multi-Stage Channels	_	Inhibit System Recovery
Domains			Ouston Corvince	Execution Future I Demote		Modification	Authentication		Authentication Material	Repositories		Account	Natural Daniel of Carries
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
WODOIIOO			User Execution	Hijack Execution Flow	Process Injection	 Exploitation for Defense	Network Sniffing	File and Directory		Data from Network	Non-Standard Port		Resource Hijacking
			Coor Excounter	Trijadik Exteranti i Trioni	Trococo injection	Evasion	THO THE THIRTY	Discovery		Shared Drive	Thom standard r str		Thousands Injustating
			Windows Management	Implant Internal Image	Scheduled Task/Job	File and Directory	OS Credential Dumping	Group Policy Discovery		Data from Removable	Protocol Tunneling		Service Stop
			Instrumentation			Permissions				Media			
				Modify Authentication	Valid Accounts	Hide Artifacts	Steal Application Access	Network Service		Data Staged	Proxy		System Shutdown/
				Process			Token	Discovery					Reboot
				Office Application		Hijack Execution Flow		Network Share Discovery		Email Collection	Remote Access Software		
				Startup		lance of the De Constant	lickets Ottool Wala Consider	Natural Colffin		land to One to the	Traffic Oir all		
				Pre-OS Boot		Impair Defenses	0 11	Network Sniffing		Input Capture	Traffic Signaling		
				Scheduled Task/Job		Indicator Removal on	Uookie Unsecured Credentials	Password Policy		Screen Capture	 Web Service		

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	.	Account Manipulation	Abuse Elevation Control	Abuse Elevation Control	Adversary-in-the-Middle	'	Exploitation of Remote	Adversary-in-the-Middle		Automated Exfiltration	Account Access
Gather Victim Host	Compromise Accounts	Exploit Public-Facing	Interpreter Container Administration	RITS Inhs	Mechanism Access Token	Mechanism Access Token	Brute Force		Services Internal Spearphishing	Archive Collected Data	Protocol Communication Through	Nata Transfer Size Limits	Removal Nata Nestruction
Information		Application	Command	1	Manipulation	Manipulation		Discovery		Aronivo dollodioa bala	Removable Media	Dulu Hullolol 0120 Ellillio	Daid Dooridonon
Gather Victim Identity	Compromise	External Remote	Deploy Container		Boot or Logon Autostart	BITS Jobs	Credentials from		Lateral Tool Transfer	Audio Capture	I	Exfiltration Over	Data Encrypted for
	Infrastructure	Services		Execution	Execution		Password Stores	Discovery				Alternative Protocol	Impact
	Develop Capabilities	Hardware Additions	Exploitation for Client	_		Build Image on Host	1 ·		Remote Service Session	Automated Collection	Data Obfuscation		Data Manipulation
Information Cathor Viotim Org	Fotablish Assounts	Dhiohing	Execution Inter-Process	·	Initialization Scripts Create or Modify System	Dobugger Evenion	Credential Access	Discovery Cloud Service Dashboard	Hijacking	Drowoor Coopien	Dynamia Dagalutian	Channel Syfiltration Over Other	Nofocoment
Gather Victim Org Information	Establish Accounts	Phishing	Inter-Process Communication	Browser Extensions	Create or Modify System Process		Forced Authentication	PIONOR 261 AICE DAZIIDOGIA	HEILINIE PELVICES	Browser Session Hijacking	Dynamic Resolution	Exfiltration Over Other Network Medium	Defacement
Phishing for Information		Replication Through Removable Media	Native API	Compromise Client Software Binary		Deobfuscate/Decode Files or Information	Forge Web Credentials		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	·	Escape to Host	Deploy Container	Input Capture		Software Deployment Tools	Data from Cloud Storage Object	Fallback Channels		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		Taint Shared Content	Data from Configuration Repository	Ingress Tool Transfer	Scheduled Transfer	Firmware Corruption
Search Open Websites/ Domains		Valid Accounts	Software Deployment Tools	Execution	Exploitation for Privilege Escalation	Domain Policy Modification	Authentication	00	Use Alternate Authentication Material	Repositories	Multi-Stage Channels	Transfer Data to Cloud Account	Inhibit System Recovery
Search Victim-Owned Websites			System Services	Services	Hijack Execution Flow	Execution Guardrails	Multi-Factor Authentication Request	Domain Trust Discovery		Data from Local System	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		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	Network Service Discovery		Data Staged	Proxy		System Shutdown/ Reboot
				Office Application		Hijack Execution Flow	I	Network Share Discovery		Email Collection	Remote Access Software		1160001
				Startup Pre-OS Boot		Impair Defenses	Tickets 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			DEV		
						Modify System Image		Vottware Nicenvery					

Modify System Image

Network Boundary Bridging Obfuscated Files or

Information

Software Discovery

System Information
Discovery
System Location
Discovery



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	
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
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	Discovery	Remote Service Session Hijacking	Automated Collection		Exfiltration Over C2 Channel	Data Manipulation
Information	Establish Accounts	Phishing	Inter-Process Communication	Browser Extensions	Create or Modify System Process	Debugger Evasion	Forced Authentication	Cloud Service Dashboard		Browser Session Hijacking		Exfiltration Over Other Network Medium	Defacement
Phishing for Information		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		Exfiltration Over Physical Medium	
	Stage Capabilities	Supply Chain Compromise	Scheduled Task/Job	Create Account	Escape to Host	Deploy Container		Cloud Storage Object Discovery	Software Deployment Tools	Data from Cloud Storage Object			Endpoint Denial of Service
Search Open Technical Databases Coarch Open Websites /		Trusted Relationship	Shared Modules Coftwere Deployment	Process Front Triggered	Event Triggered Execution Evaluates for Privilege	Direct Volume Access	Modify Authentication Process Multi Footer	Container and Resource Discovery	Taint Shared Content	Data from Configuration Repository Data from Information		Scheduled Transfer Transfer Data to Cloud	Firmware Corruption
Search Open Websites/ Domains Search Victim-Owned		Valid Accounts	Software Deployment Tools	Execution	Exploitation for Privilege Escalation Hijack Execution Flow	Domain Policy Modification Execution Guardrails	Multi-Factor Authentication Multi-Factor	Debugger Evasion Domain Trust Discovery	Use Alternate Authentication Material	Data from Information Repositories Data from Local System	Multi-Stage Channels Non Application Layor	Account	Inhibit System Recovery Network Denial of
Websites			System Services User Execution	Services	Process Injection	Exploitation for Defense	Authentication Request Network Sniffing	File and Directory		Data from Network	Non-Application Layer Protocol Non-Standard Port		Service Resource Hijacking
			Windows Management	Implant Internal Image	Scheduled Task/Job	Evasion File and Directory	OS Credential Dumping	Discovery Group Policy Discovery		Shared Drive Data from Removable	Protocol Tunneling		Service Stop
			Instrumentation	Modify Authentication	Valid Accounts	Permissions Hide Artifacts	Steal Application Access			Media Data Staged	Proxy		System Shutdown/
				Process Office Application	runa rioccarno	Hijack Execution Flow	Token Steal or Forge Kerberos	Discovery Network Share Discovery		Email Collection	Remote Access Software		Reboot
				Startup Pre-OS Boot		Impair Defenses	Tickets Steal Web Session	Network Sniffing		Input Capture	Traffic Signaling		
				Scheduled Task/Job		Indicator Removal on	Cookie Unsecured Credentials	Password Policy		Screen Capture	Web Service		
				Server Software		Indirect Command		Discovery Peripheral Device		Video Capture			
				Component Traffic Signaling		Execution Masquerading		Discovery Permission Groups Discovery					
				Valid Accounts		Modify Authentication Process		Discovery Process Discovery					
						Modify Cloud Compute Infrastructure		Query Registry					

Modify System Image

Network Boundary Bridging

Obfuscated Files or Information

Remote System Discovery

Software Discovery

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
Information	Compromise Accounts	Exploit Public-Facing Application	Container Administration Command	BITS Jobs	Access Token Manipulation	Access Token Manipulation			Internal Spearphishing	Archive Collected Data	Communication Through Removable Media		
Information	Compromise Infrastructure	External Remote Services Hardware Additions	Deploy Container	Boot or Logon Autostart Execution	Boot or Logon Autostart Execution	BITS Jobs	Password Stores	Discovery	Lateral Tool Transfer	Audio Capture		Alternative Protocol	Data Encrypted for Impact
Information		Hardware Additions	I .	Initialization Scripts	Initialization Scripts	_	Credential Access	Cloud Infrastructure Discovery	Hijacking Description:	Automated Collection		Channel	Data Manipulation
Information	Establish Accounts	Phishing	Inter-Process Communication	1	Create or Modify System Process			Cloud Service Dashboard		Browser Session Hijacking		Exfiltration Over Other Network Medium	Defacement
Phishing for Information		Replication Through Removable Media		Software Binary	Domain Policy Modification	Files or Information			Replication Through Removable Media	Clipboard Data		Exfiltration Over Physical Medium	
		Supply Chain Compromise	Scheduled Task/Job		Escape to Host	Deploy Container		Discovery	Software Deployment Tools	Object			Endpoint Denial of Service
Search Open Technical Databases		Trusted Relationship	Shared Modules	Process	Event Triggered Execution	Direct Volume Access	Modify Authentication Process	Discovery		Data from Configuration Repository		Scheduled Transfer	Firmware Corruption
Search Open Websites/ Domains		Valid Accounts	Software Deployment Tools	Execution		Modification	Authentication		Use Alternate Authentication Material			Transfer Data to Cloud Account	Inhibit System Recovery
Search Victim-Owned Websites			System Services	External Remote Services	Hijack Execution Flow		Authentication Request	Domain Trust Discovery			Non-Application Layer Protocol		Network Denial of Service
			User Execution		·	Evasion	_	File and Directory Discovery		Data from Network Shared Drive	Non-Standard Port		Resource Hijacking
			Windows Management Instrumentation	Implant Internal Image		File and Directory Permissions		Group Policy Discovery		Data from Removable Media	Protocol Tunneling		Service Stop
				Modify Authentication Process	Valid Accounts		Steal Application Access Token	Discovery		Data Staged	Proxy		System Shutdown/ Reboot
				Office Application Startup			Tickets	Network Share Discovery		Email Collection	Remote Access Software		
				Pre-OS Boot			Cookie	Network Sniffing		Input Capture	Traffic Signaling		
				Scheduled Task/Job		Host		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				NPT1	

System Information

Discovery System Location

Network Boundary Bridging

Obfuscated Files or



AFIIU

Discovery
System Location
Discovery

Recon.	Resourc	Initial	Executio	Persiste	Privileg	Defense	Credenti	Discove	Lateral	Collecti	Comma	Exfiltrati	Impact	Recon.	Resourc	Initial	Executio	Persiste	Privileg	Defense	Credenti	Discove	
	e Dev	229111	<u> </u>	nce	<u>P</u>	Fvasinn	L Al	<u> </u>	Movem	Adversary-in-the-Middle	nd and	l nn l			e Dev	Access	n	nce	P	Fvasinn	al	rv	N
Active Scanning	Acquire Intrastructure	Drive-by Compromise	Command and Scripting	Account Manipulation	Abuse Elevation Control Mechanism	Abuse Elevation Control Mechanism	Adversary-in-the-Middle	Account Discovery	Exploitation of Kemote	Adversary-in-the-Middle	Application Layer Protocol	Automated Exfiltration	Account Access	Active Scanning	Acquire Infrastructure	Drive-by Compromise	Command and Scripting	Account Manipulation	Abuse Elevation Control Mechanism	Abuse Elevation Control	Adversary-in-the-Middle	Account Discovery E	ZXD
Gather Victim Host	Compromise Accounts	Exploit Public-Facing	Container	BITS Jobs		Access Token	Brute Force	Application Window	Internal Spearphishing	Archive Collected Data	Communication	Data Transfer Size Limits	Data Destruction	Gather Victim Host	Compromise Accounts	Exploit Public-Facing	Container	BITS Jobs	Access Token	Mechanism Access Token	Brute Force	Application Window Ir	Inte
Information	0	Application	Administration	Dankardana Astrobart	Manipulation	Manipulation	Out de salis la facesa	Discovery	Lateral Taul Transfer	A dia Oa to	Through Removable	F. Chartier Over	Data Francisco de la constante	Information		Application	Administration		Manipulation	Manipulation	[Discovery	
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 Identity Information		External Remote Services	Deploy Container	Boot or Logon Autostart Execution	Boot or Logon Autostart Execution		Credentials from E Password Stores E	Browser Bookmark La Discovery	_ate
Gather Victim Network	Develop Capabilities	Hardware Additions	Exploitation for Client	Boot or Logon	Boot or Logon	Build Image on Host	Exploitation for	Cloud Infrastructure	Remote Service Session	Automated Collection	Data Obfuscation	Exfiltration Over C2	Data Manipulation	Gather Victim Network		Hardware Additions	Exploitation for Client				Exploitation for (Cloud Infrastructure R	Rer
Information	Catablish Assounts	Dhighing	Execution Inter Process	Initialization Scripts	Initialization Scripts	Debugger Evenion	Credential Access	Discovery	Hijacking	Drawaar Cassian	Dunamia Decalution	Channel Systiltration Over Other	Defeasment	Information	Fatablish Assaults	Districts an	Execution	Boot or Logon Initialization Scripts	Initialization Scripts		Credential Access [Discovery H	Hija
Gather Victim Org Information	Establish Accounts	Phishing	Inter-Process Communication	Browser Extensions	Create or Modify System Process	Dennâdei Easioii	Forced Authentication	Cloud Service Dashhoard	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	Create or Modify System Process	Debugger Evasion	Forced Authentication (Cloud Service R Dashboard	.ter
Phishing for Information	Obtain Capabilities	Replication Through	Native API	Compromise Client	Domain Policy	Deobfuscate/Decode	Forge Web Credentials	Cloud Service Discovery	Replication Through	Clipboard Data	Encrypted Channel	Exfiltration Over Physical	Disk Wipe	Phishing for Information	Obtain Capabilities	Replication Through	Native API	Compromise Client	Domain Policy	Deobfuscate/Decode	Forge Web Credentials (Cloud Service Discovery R	Rep
Search Closed Sources	Stage Conshilition	Removable Media Supply Chain	Scheduled Task/Job	Software Binary Create Account	Modification Escape to Host	Files or Information Deploy Container	Input Capture	Cloud Storage Object	Removable Media Software Deployment	Data from Cloud Storage	Fallback Channala	Medium Exfiltration Over Web	Endpoint Nanial of	Coarob Closed Courses		Removable Media		Software Binary	Modification	Files or Information	Input Contura	Cloud Storage Object	yer
ocarcii diosen onnices	Staye Gapanillies	Compromise	OCHEUNIEN 192K/100	Gredie Account	ESCAPE IO HOSI	DehinA congulation	I IIIhai eahiais	Discovery	Tools	Object	Fallback Glidilliels	Service	Endpoint Denial of Service	Search Closed Sources		Supply Chain Compromise	Scheduled Task/Job	Create Account	Escape to Host	Deploy Container	Input Capture	Cloud Storage Object S Discovery Ti	IUc nnT
Search Open Technical		Trusted Relationship	Shared Modules	Create or Modify System		Direct Volume Access	Modify Authentication	Container and Resource	Taint Shared Content	Data from Configuration	Ingress Tool Transfer	Scheduled Transfer	Firmware Corruption	Search Open Technical		Trusted Relationship	Shared Modules	Create or Modify System		Direct Volume Access	Modify Authentication (Container and Resource Ta	Tair
Databases Search Open Websites/		Valid Accounts		Process Event Triggered	Execution Exploitation for Privilege	Domain Policy	Process Multi-Factor	Discovery Debugger Evasion	Use Alternate	Kepository Data from Information	Multi-Stage Channels	Transfer Data to Cloud	Inhibit System Recovery	Databases Search Open Websites/		Valid Accounts	Coftware Doployment	Process Event Triggered	Execution Exploitation for Privilege	Domain Daliay	Process [Multi-Factor [Discovery Debugger Evenion	Hor
Domains		Valla Apponilia	Tools	Execution		Modification	Authentication	nennââei raganii	Authentication Material	Repositories	Wulli-olaye ollalillelo	Account		Domains		Valid Accounts	Software Deployment Tools	Execution	Escalation	Domain Policy Modification	Authentication	Debugger Evasion U	Aut
Search Victim-Owned			System Services	External Remote		Execution Guardrails	Multi-Factor	Domain Trust Discovery		Data from Local System	Non-Application Layer		Network Denial of	Search Victim-Owned	'		System Services	External Remote		Execution Guardrails	Multi-Factor [Domain Trust Discovery	
Websites			User Execution	Services Hijack Execution Flow	Process Injection	Exploitation for Defense	Authentication Request Network Sniffing	File and Directory		Data from Network	Protocol Non-Standard Port		Service Resource Hijacking	Websites			User Execution	Services Hijack Execution Flow	Process Injection		Authentication Request Network Sniffing	File and Directory	
			USEI EXECUTION	TIIJAGK EXGGUIIOITTIOW	1100633 11116011011	Evasion	I NGI WOLK OHILINING	Discovery		Shared Drive	Noir ordinadra i ori		Hesource Hijacking				חספו דעפטמווטוו	HIJAGK EXECUTION HOW	FIUUGSS HIJGUHUH	Evasion	INCLIMOLK OUR THIRD	Discovery	
			Windows Management	Implant Internal Image	Scheduled Task/Job	File and Directory	OS Credential Dumping	Group Policy Discovery		Data from Removable	Protocol Tunneling		Service Stop					Implant Internal Image		File and Directory	OS Credential Dumping (Group Policy Discovery	
			Instrumentation	 Modify Authentication	Valid Accounts	Permissions Hide Artifacts	Steal Application	Network Service		Data Staged	Prnyv		tem Shutdr				Instrumentation	Modify Authentication		Permissions Hide Artifacts	Steal Application	Network Service	
				Process	Valia Adddanid		Access Token	Discovery			Τιολγ		1011 011414					Process	Vulla Accounts		Access Token [Discovery	
				Office Application		Hijack Execution Flow	Steal or Forge Kerberos	Network Share		Email Collection	Remote Access							Office Application		Hijack Execution Flow		Network Share	
			1	Startup Pre-OS Boot		I Impair Defenses	Steal Web Session	Network Sniffing		Input Capture	Software Traffic Signaling							Startup Pre-OS Boot		Impair Defenses	Tickets [1] Steal Web Session	Discovery Network Sniffing	
							Cookie													pa beleliese	Cookie		
				Scheduled Task/Job		Indicator Removal on Host	Unsecured Credentials	Password Policy Discovery		Screen Capture	Web Service							Scheduled Task/Job		Indicator Removal on	Unsecured Credentials F	Password Policy	
				Server Software		Indirect Command		Peripheral Device		Video Capture								Server Software		Indirect Command	·	Discovery Peripheral Device	
				Component		Execution		Discovery										Component		Execution	<u> </u>	Discovery	
				Traffic Signaling		Masquerading		Permission Groups Discovery										Traffic Signaling		Masquerading		Permission Groups Discovery	
				Valid Accounts		Modify Authentication		Process Discovery										Valid Accounts		Modify Authentication	·	Process Discovery	
				Tana Noodanii		Process		1.00000 01000001										Tunu Auduuniid		Process		100000 DIOUOVOI y	
						Modify Cloud Compute		Query Registry												Modify Cloud Compute	<u> </u>	Query Registry	
						Infrastructure Modify Registry		Remote System												Infrastructure Modify Registry		Domoto Svetem	
						IVIOUITY NEGISTRY		Discovery												IVIUUIIY NEYISIIY		Remote System Discovery	
						Modify System Image		Software Discovery												Modify System Image	(Software Discovery	
						Network Roundary		System Information												Network Roundary		System Information	

Initial	Executio	Persiste	Privileg	Defense	Credenti	Discove	Lateral	Collecti	Comma	Exfiltrati	Impact
Access	n	nce	P	Fvasinn	al	rv	Movem	nn	nd and	nn	iiiipuoi
rive-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
xploit Public-Facing pplication	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
xternal Remote ervices	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
ardware Additions	Exploitation for Client Execution		Boot or Logon Initialization Scripts	Build Image on Host	Exploitation for Credential Access	Discovery	Remote Service Session Hijacking	Automated Collection	Data Obfuscation	Channel	Data Manipulation
hishing	Inter-Process Communication	Browser Extensions	Process	Debugger Evasion	Forced Authentication	Dashboard	Remote Services	Browser Session Hijacking	Dynamic Resolution	Exfiltration Over Other Network Medium	Defacement
eplication Through emovable Media	Native API	Compromise Client Software Binary	Domain Policy Modification	Deobfuscate/Decode Files or Information	Forge Web Credentials	·	Replication Through Removable Media		Encrypted Channel	Exfiltration Over Physical Medium	Disk Wipe
upply Chain ompromise	Scheduled Task/Job	Create Account	Escape to Host	Deploy Container	Input Capture	Discovery	Software Deployment Tools	Object	Fallback Channels	Service	Endpoint Denial of Service
rusted Relationship	Shared Modules	Create or Modify System Process	Event Triggered Execution	Direct Volume Access	Modify Authentication Process	Discovery	Taint Shared Content	Data from Configuration Repository	Ingress Tool Transfer		Firmware Corruption
alid 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 Recover
	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 Traffic Signaling		Indirect Command Execution Masquerading		Peripheral Device Discovery Permission Groups		Video Capture			
		Matrid Digitality		Madifutuhantiaatian		Discovery					

	Alaitie	Farmeri	Paraiet	Divile		Annaday	4 Diagon		A Dellook	A Common of the	FuSiltro			Austrial		Increase	Debuiler		A Company	Al Discours		- Indian	40000	- Clave	
														ACCESS Drive by Compromis		nce Account Manipulation		FVASION Popular					nd and	Automated Exfiltration	
Search Closed Sources																									
Search Open Technical																									
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 Materi	Data from Information Repositories	Multi-Stage Channels	Transfer Data to Cloud Account	Inhibit System Recover	Search Open Websites/ Nomains	Valid Accounts	Software Deployment Tools	Event Triggered Execution	Exploitation for Privilege Escalation	Domain Policy Modification	Multi-Factor Authentication	Debugger Evasion	Use Alternate Authentication Mate	Data from Information Renositories	Multi-Stage Channels	Transfer Data to Cloud	Inhibit System Recovery
Sea ch Victim-Owned We sites		System Services	External Remote Services	Hijack Execution Flow	Execution Guardrails	Multi-Factor Authentication Reques	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	Execution Guardrails	Multi-Factor Authentication Reques	Domain Trust Discovery		Data from Local System	Non-Application Layer Protocol		Network Denial of Service
			Hijack Execution Flow	Process inn	Exploi	Netwo	A MANAGEMENT OF THE PARTY OF TH		from Network	/			ÈIL	1	A STATE OF THE PARTY OF THE PAR	A STATE OF	Process injection	Exploitation for Detense				1 -	an Clandard Port		
	AR'		Implant Internal mage		Parmiceinne	IS Urede			AK	/ "	112:	4	1115	1	In Phalon			e and Directory ermissions			74-	_ dia			Pervice Stop
		1 7	Process Office Application			CCess Tok	/ scovery						411	5	107	Pro Application	IU Abouthis	includers Flow	M=7	MU			AF		leboot
			Startup Pre-OS Root		Impair Defenses	Tickets Steal Web Session	Discovery Network Sniffing		Innut Capture	Sonware Traffic Signaling								Imnair Defenses	Tickets Steal Web Session	Discovery Network Sniffing		Innut Canture	Software Traffic Signaling		
			Scheduled Task/Job		Indicator Removal on	Cookie Unsecured Credentials	Password Policy		Screen Capture	Web Service						Scheduled Task/Job		Indicator Removal on	Cookie Unsecured Credential	Password Policy		Screen Capture	Web Service		



Recon.	Resourc	Initial	Executio	Persiste	Privileg	Defense	Credenti	Discove	Lateral	Collecti	Comma	Exfiltrati	Impact
11000111	e Nev	Access	n	nce	P.	Fvasinn	al	rv	Movem	nn	nd and	nn	Impuoi
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			Access Token Manipulation	Access Token Manipulation	Brute Force	Application Window Discovery	Internal Spearphishing	Archive Collected Data	Communication Through Removable	Data Transfer Size Limits	
Gather Victim Identity Information	Compromise Infrastructure	External Remote Services			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	Boot or Logon	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		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		Domain Policy Modification	Deobfuscate/Decode Files or Information	Forge Web Credentials	Cloud Service Discovery	Replication Through Removable Media	, ,	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		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		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 Recover
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		rtem Shutdr not
				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					

演練後提供整理的結果完整、正確性極高

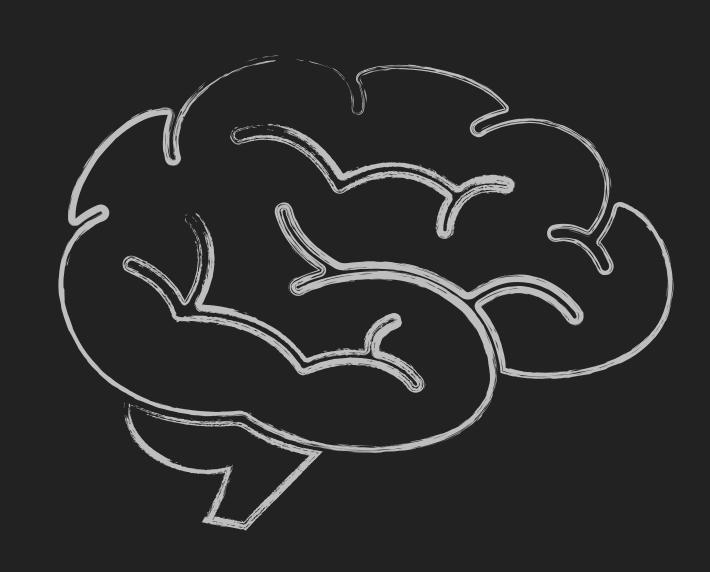
APT10

•	Recon.	Resourc	Initial	Executio	Persiste	Privileg		Credenti	Discove		Collecti	Comma	Exfiltrati	Impact
		e Dev.	Access	n	nce	P.	Fvasinn	al	l rv	Movem	nn	nd and	nn	•
	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	Compromise Accounts	Exploit Public-Facing	Container	BITS Jobs	Access Token	Access Token	Brute Force	Application Window	Internal Spearphishing	Archive Collected Data	Communication	Data Transfer Size Limits	Data Destruction
	Information		Application	Administration		Manipulation	Manipulation		Discovery			Through Removable		
	Gather Victim Identity	1 · · · · · · · · · · · · · · · · · · ·	External Remote	Deploy Container	Boot or Logon Autostart	Boot or Logon Autostart	BITS Jobs	Credentials from	Browser Bookmark	Lateral Tool Transfer	Audio Capture	Data Encoding	Exfiltration Over	Data Encrypted for
	Information Gather Victim Network		Services Hardware Additions	Exploitation for Client	Execution Boot or Logon	Execution Boot or Logon	Build Image on Host	Password Stores Exploitation for	Discovery Cloud Infrastructure	Remote Service Session	Automated Collection	Data Obfuscation	Alternative Protocol Exfiltration Over C2	Impact Data Manipulation
	Information	DEVELOP CAPADIIIIES	NATUWATE AUUITUTIS	Expluitation Glieni	Initialization Scripts	Initialization Scripts	Dullu IIIIdye UII NUSI	Credential Access	Discovery	Hiiacking	AUTOTTIATEU GOTTEGITOTT	Dala UDIUSCANUN	Channel	Dala Maliipulaliuli
	Gather Victim Org	Establish Accounts	Phishing	Inter-Process	Browser Extensions	Create or Modify System	Debugger Evasion	Forced Authentication	Cloud Service	Remote Services	Browser Session	Dynamic Resolution	Exfiltration Over Other	Defacement
	Information			Communication		Process			Dashboard		Hijacking		Network Medium	
	Phishing for Information		Replication Through	Native API	Compromise Client	Domain Policy	Deobfuscate/Decode	Forge Web Credentials	Cloud Service Discovery	Replication Through Removable Media	Clipboard Data	Encrypted Channel	Exfiltration Over Physical	Disk Wipe
	Search Closed Sources		Removable Media Supply Chain	Scheduled Task/Job	Software Binary Create Account	Modification Escape to Host	Files or Information Deploy Container	Input Capture	Cloud Storage Object	Software Deployment	Data from Cloud Storage	Fallback Channels	Medium Exfiltration Over Web	Endpoint Denial of
	ocaron olooca ocaroco		Compromise	Outleadion (dok/)OD	Olodic Addodili	Locape to floor	Doploy Cornainor	Input oupture	Discovery	Tools	Object	I dilbaok orialiriolo	Service	Service
	Search Open Technical		Trusted Relationship	Shared Modules		Event Triggered	Direct Volume Access	Modify Authentication		Taint Shared Content	Data from Configuration	Ingress Tool Transfer	Scheduled Transfer	Firmware Corruption
	Databases		W.B.LL	0 (1	Process	Execution		Process	Discovery	II. Ali	Repository	M In Or Ol	T (D 0)	
ery	Search Open Websites/ Domains		Valid Accounts	Software Deployment Tools		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	'		System Services	External Remote	Hijack Execution Flow	Execution Guardrails	Multi-Factor	Domain Trust Discovery	Aumeninganon watena	Data from Local System	Non-Application Layer	AGGOUIII	Network Denial of
	Websites			O yololii ool viooo	Services	Tiljaok Excoalion Flori	Exocution cadiatation	Authentication Request	Bernam Hadi Biodovery		Bala Holli Essai Gyololli	Protocol		Service
				User Execution	Hijack Execution Flow	Process Injection	Exploitation for Defense	Network Sniffing	File and Directory		Data from Network	Non-Standard Port		Resource Hijacking
				Windows Management	Implant Internal Image	Scheduled Task/Job	Evasion	Of Orodontial Dumping	Discovery Group Policy Discovery		Shared Drive Data from Removable	Dratagal Tunnaling		Convice Oten
				Windows Management Instrumentation	IIIIpidiii iiiieiiidi iiiidye	OCHEUNIEN 192K/JON	File and Directory Permissions	OS Credential Dumping	GLOUP LOUGH DISCOVELY		Media	Protocol Tunneling		Service Stop
		•		monument	Modify Authentication	Valid Accounts	Hide Artifacts	Steal Application	Network Service		Data Staged	Proxy		System Shutdown/
Ш					Process			Access Token	Discovery					Reboot
					Office Application		Hijack Execution Flow	Steal or Forge Kerberos	Network Share		Email Collection	Remote Access		
					Startup Pre-OS Boot		Impair Defenses	Tickets Steal Web Session	Discovery Network Sniffing		Input Capture	Software Traffic Signaling		
					1 10 00 0001		IIIIpuli Delelioeo	Cookie	NGIWOIK OIIIIIIII		піраї Офраїв	Trainic digitality		
					Scheduled Task/Job		Indicator Removal on	Unsecured Credentials	Password Policy		Screen Capture	Web Service		
					00		Host		Discovery		Wide a County was			
					Server Software		Indirect Command		Peripheral Device		Video Capture			

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

ATT&CK 簡述

怎麼使用 ATT&CK

ATT&CK的誤區

Case Studies



「我們想做APT 10的演練。」

了好。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

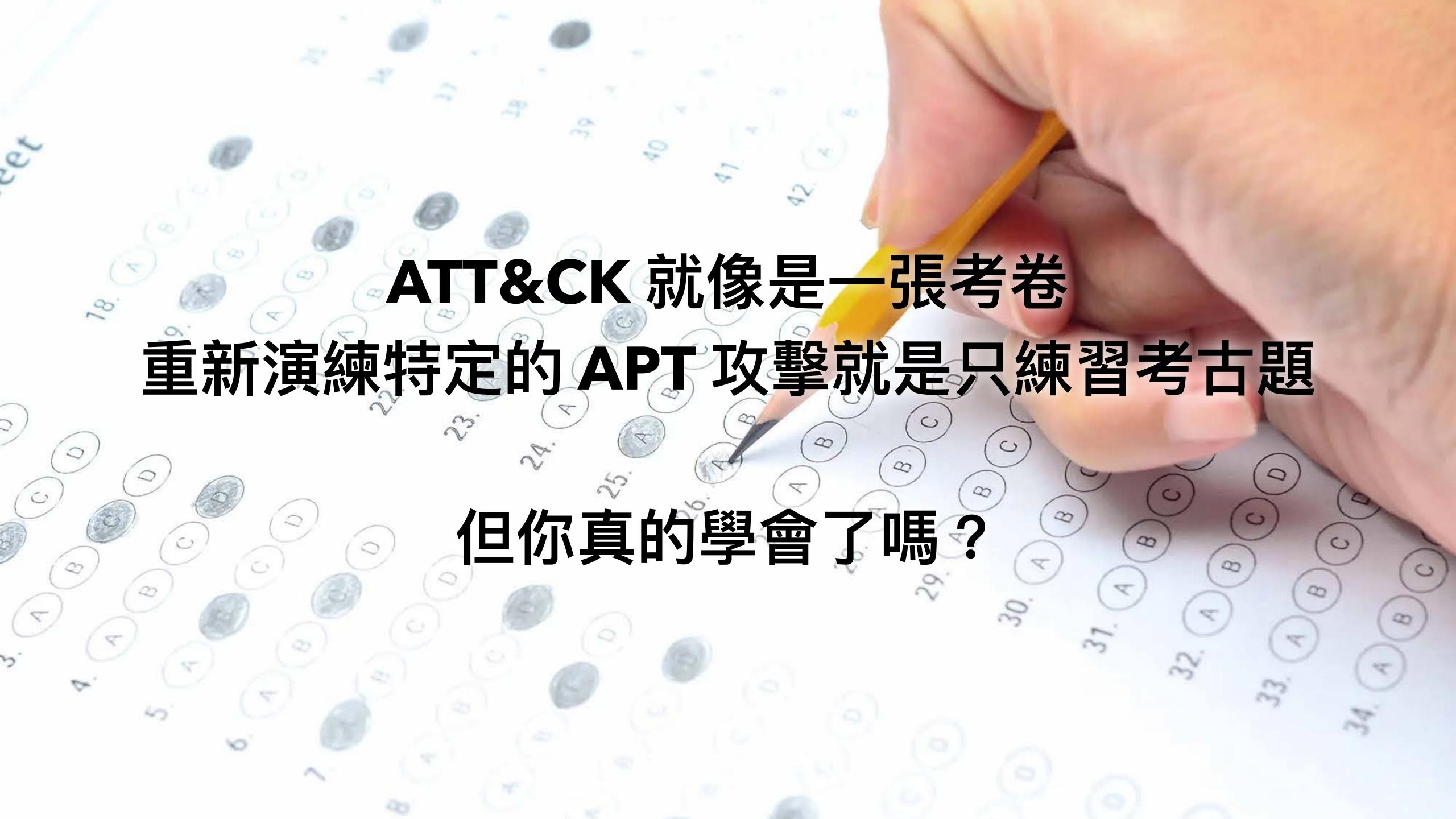


ATT&CK的常見誤區

- 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

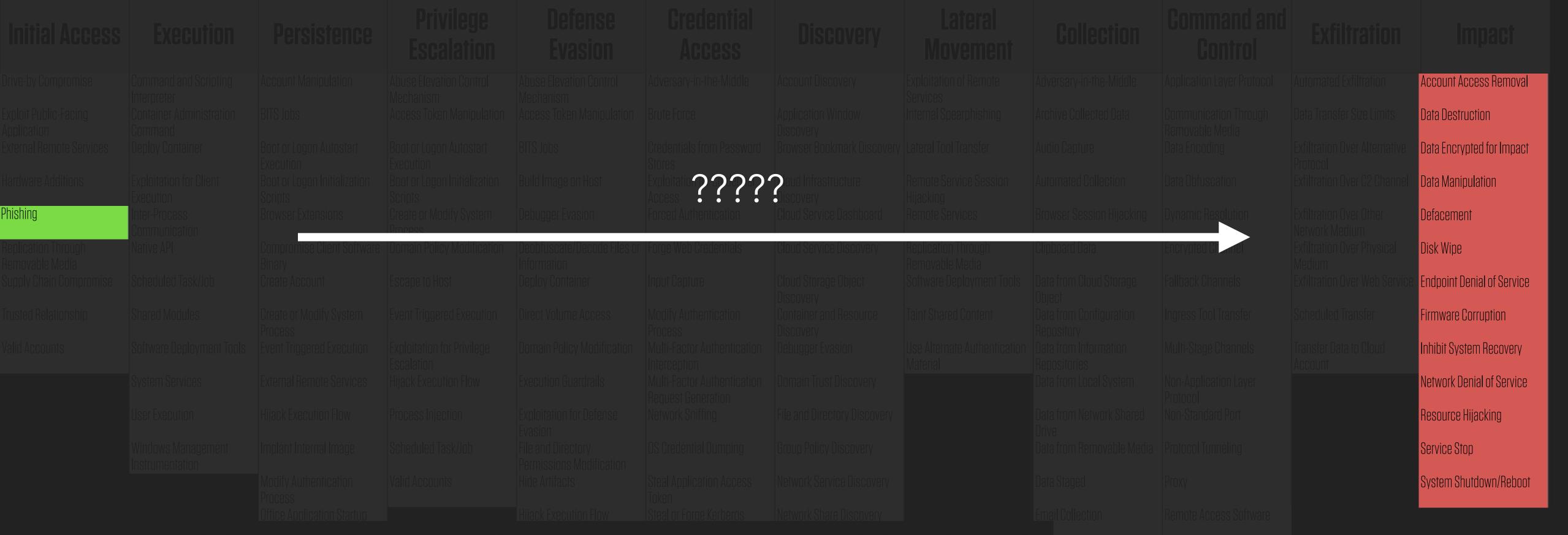


Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Drive-by Compromise	Command and Scripting Interpreter	Account Manipulation	Abuse Elevation Control Mechanism	Abuse Elevation Control 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		Create or Modify System Process		Forced Authentication	Cloud Service Dashboard	1	Browser Session Hijacking		Exfiltration Over Other Network Medium	Defacement
Replication Through Removable Media	Native API	·	1	Deobfuscate/Decode Files or Information	Forge Web Credentials		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		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		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		Multi-Factor Authentication Request Generation	Domain Trust Discovery			Non-Application Layer Protocol		Network Denial of Service
	User Execution	Hijack Execution Flow	Process Injection	Exploitation for Defense Evasion	· ·	File and Directory Discovery		Data from Network Shared Drive	Non-Standard Port		Resource Hijacking
	Windows Management Instrumentation	Implant Internal Image	Scheduled Task/Job		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		Network Share Discovery		Email Collection	Remote Access Software		
\bigcirc \bigcirc \bigcirc	/ 4/-	<u> 구도</u> 그는	末/7 屈曲	13年11日	一一 フ	壬7/4	/E5 > 4/	t Capture	Traffic Signaling		

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。





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。

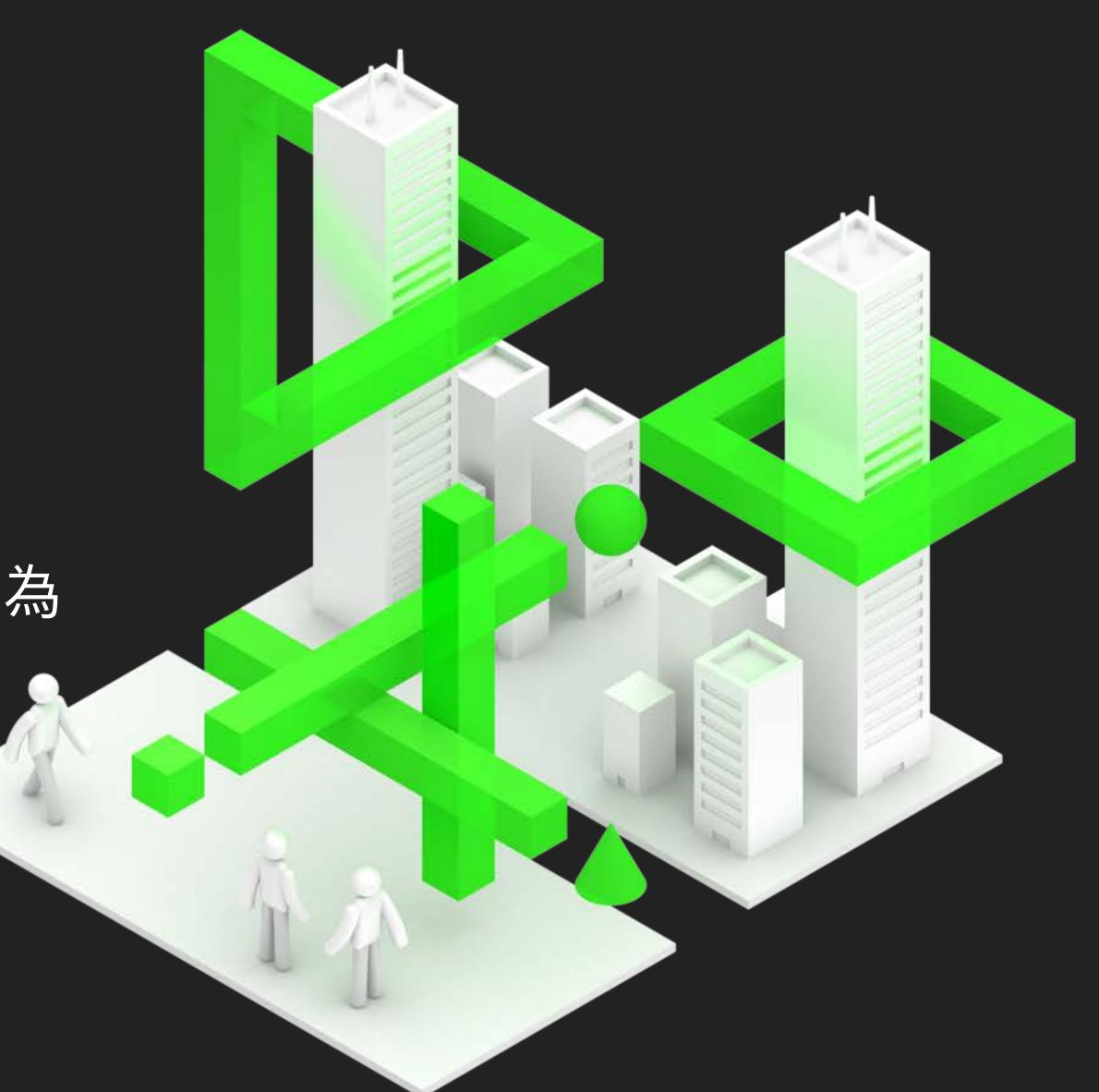


我們真正該談的是什麼

• 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	
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
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	Discovery	Remote Service Session Hijacking	Automated Collection		Exfiltration Over C2 Channel	Data Manipulation
Information	Establish Accounts	Phishing	Inter-Process Communication	Browser Extensions	Create or Modify System Process	Debugger Evasion	Forced Authentication	Cloud Service Dashboard		Browser Session Hijacking		Exfiltration Over Other Network Medium	Defacement
Phishing for Information		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		Exfiltration Over Physical Medium	
	Stage Capabilities	Supply Chain Compromise	Scheduled Task/Job	Create Account	Escape to Host	Deploy Container		Cloud Storage Object Discovery	Software Deployment Tools	Data from Cloud Storage Object			Endpoint Denial of Service
Search Open Technical Databases Coarch Open Websites		Trusted Relationship	Shared Modules Coftwere Deployment	Process Front Triggered	Event Triggered Execution Evaluates for Privilege	Direct Volume Access	Modify Authentication Process Multi Footer	Container and Resource Discovery	Taint Shared Content	Data from Configuration Repository Data from Information		Scheduled Transfer Transfer Data to Cloud	Firmware Corruption
Search Open Websites/ Domains Search Victim-Owned		Valid Accounts	Software Deployment Tools	Execution	Exploitation for Privilege Escalation Hijack Execution Flow	Domain Policy Modification Execution Guardrails	Multi-Factor Authentication Multi-Factor	Debugger Evasion Domain Trust Discovery	Use Alternate Authentication Material	Data from Information Repositories Data from Local System	Multi-Stage Channels Non Application Layor	Account	Inhibit System Recovery Network Denial of
Websites			System Services User Execution	Services	Process Injection	Exploitation for Defense	Authentication Request Network Sniffing	File and Directory		Data from Network	Non-Application Layer Protocol Non-Standard Port		Service Resource Hijacking
			Windows Management	Implant Internal Image	Scheduled Task/Job	Evasion File and Directory	OS Credential Dumping	Discovery Group Policy Discovery		Shared Drive Data from Removable	Protocol Tunneling		Service Stop
			Instrumentation	Modify Authentication	Valid Accounts	Permissions Hide Artifacts	Steal Application Access			Media Data Staged	Proxy		System Shutdown/
				Process Office Application	runa rioccarno	Hijack Execution Flow	Token Steal or Forge Kerberos	Discovery Network Share Discovery		Email Collection	Remote Access Software		Reboot
				Startup Pre-OS Boot		Impair Defenses	Tickets Steal Web Session	Network Sniffing		Input Capture	Traffic Signaling		
				Scheduled Task/Job		Indicator Removal on	Cookie Unsecured Credentials	Password Policy		Screen Capture	Web Service		
				Server Software		Indirect Command		Discovery Peripheral Device		Video Capture			
				Component Traffic Signaling		Execution Masquerading		Discovery Permission Groups Discovery					
				Valid Accounts		Modify Authentication Process		Discovery Process Discovery					
						Modify Cloud Compute Infrastructure		Query Registry					

Modify System Image

Network Boundary Bridging

Obfuscated Files or Information

Remote System Discovery

Software Discovery

System Information Discovery

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	1	Brute Force	Application Window Discovery	Internal Spearphishing	Archive Collected Data	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
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 Obtugaction	Exfiltration Over Alternative Protocol	Data Encrypted for Impact
Information	Develop Capabilities	Hardware Additions	Exploitation for Client Execution	Initialization Scripts	Boot or Logon Initialization Scripts	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking	Automated Collection		Exfiltration Over C2 Channel	Data Manipulation
Information	Establish Accounts	Phishing	Inter-Process Communication	Browser Extensions	Create or Modify System Process		Forced Authentication	Cloud Service Dashboard		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		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			A	NPT1	

System Information

System Location

Discovery

Network Boundary Bridging

Obfuscated Files or



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		Account Manipulation	Abuse Elevation Control	Abuse Elevation Control	Adversary-in-the-Middle	·	Exploitation of Remote	Adversary-in-the-Middle	Application Layer	Automated Exfiltration	Account Access
			Interpreter		Mechanism	Mechanism	D		Services		Protocol		Removal
	Compromise Accounts	Exploit Public-Facing	Container Administration	I .	Access Token	Access Token	Brute Force		Internal Spearphishing	Archive Collected Data	Communication Through	Data Transter Size Limits	Data Destruction
Information		Application	Command		l	Manipulation	Oue dentiele frame	Discovery	l ataval Ta al Transfer		Removable Media	Fufiltuation Over	Data Francistad for
	· ·	External Remote	Deploy Container	_	Boot or Logon Autostart	BITS Jobs	Credentials from		Lateral Tool Transfer	Audio Capture	Data Encoding		Data Encrypted for
	Infrastructure	Services Hardware Additions	 Exploitation for Client	Execution Post or Logon	Execution Root or Logon	Duild Image on Hoot	Password Stores	Discovery Cloud Infrastructure	Domoto Carvino Congion	Automated Collection	Data Obfuscation	Alternative Protocol	Impact Data Manipulation
Information	Develop Capabilities	Hardware Additions	Execution		Boot or Logon Initialization Scripts	Build Image on Host	Exploitation for Credential Access	Discovery	Remote Service Session Hijacking		Dala Uniustalluli	Exfiltration Over C2 Channel	Dala Malipulation
	 Establish Accounts	Phishing	Inter-Process	Browser Extensions	Create or Modify System	Nohunnor Evacion	Forced Authentication	Cloud Service Dashboard	, ,	Browser Session	Dynamic Resolution	Exfiltration Over Other	Defacement
Information	Lorabiloti Adddullio	Tillorining	Communication	DIOWOGI EXIGIISIONS	Process		Toroca Adminimidation	Oloud ool vloc Dashboard		Hijacking	Dynamio neodianon	Network Medium	Doladollidii
	Obtain Capabilities	Replication Through	Native API	Compromise Client		Deobfuscate/Decode	Forge Web Credentials	Cloud Service Discovery	Replication Through	Clipboard Data	Encrypted Channel	Exfiltration Over Physical	Disk Wine
,		Removable Media				Files or Information			Removable Media		2.76.7/6.65.2.3.3.3.3.	Medium	
Search Closed Sources	Stage Capabilities		Scheduled Task/Job		Escape to Host	Deploy Container	Input Capture	_	Software Deployment	Data from Cloud Storage	Fallback Channels	Exfiltration Over Web	Endpoint Denial of
		Compromise						Discovery	Tools	Object		Service	Service
Search Open Technical		Trusted Relationship	Shared Modules	Create or Modify System	Event Triggered	Direct Volume Access	Modify Authentication	Container and Resource	Taint Shared Content	Data from Configuration	Ingress Tool Transfer	Scheduled Transfer	Firmware Corruption
Databases					Execution		Process	Discovery		Repository			
Search Open Websites/		Valid Accounts	Software Deployment				Multi-Factor		Use Alternate	Data from Information	Multi-Stage Channels	Transfer Data to Cloud	Inhibit System Recovery
Domains			Tools	J.		Modification	Authentication		Authentication Material			Account	Nativaria Danial of
Search Victim-Owned			System Services	la .	Hijack Execution Flow	Execution Guardrails		Domain Trust Discovery		Data from Local System	Non-Application Layer		Network Denial of
Websites			User Execution	Services Hijook Evacution Flow	Drogge Injection	Evaluitation for Natanaa	Authentication Request Network Sniffing	Eila and Directory		Data from Network	Protocol Non Standard Port		Service Pagauras Hijaaking
			NOC EXECUIION	Hijack Execution Flow	Process Injection	Exploitation for Defense Evasion	INCIWOIK JIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII	File and Directory Discovery		Shared Drive	Non-Standard Port		Resource Hijacking
			Windows Management	Implant Internal Image	Scheduled Task/Job	File and Directory	OS Credential Dumping	Group Policy Discovery		Data from Removable	Protocol Tunneling		Service Stop
			Instrumentation		טטווטעווטע זעטאאָזטט	Permissions	oo orcaciilai barriping			Media	Troibboi fulfillolling		σοι νίου σιορ
			monamon	Modify Authentication	Valid Accounts	Hide Artifacts	Steal Application Access	Network Service			Proxy		System Shutdown/
				Process	Traina ricessarine		Token	Discovery					Reboot
				Office Application		Hijack Execution Flow	Steal or Forge Kerberos	Network Share Discovery		Email Collection	Remote Access Software		
				Startup			Tickets						
				Pre-OS Boot		Impair Defenses	Steal Web Session	Network Sniffing		Input Capture	Traffic Signaling		
							Cookie						
				Scheduled Task/Job		Indicator Removal on	Unsecured Credentials	Password Policy		Screen Capture	Web Service		
				0		Host		Discovery Device and Device		Walaa Oantuna			
				Server Software		Indirect Command		Peripheral Device		Video Capture			
				Component Troffic Cianolina		Execution Magazine		Discovery					
				Traffic Signaling		Masquerading		Permission Groups Discovery					
				Valid Accounts		Modify Authentication		Process Discovery					
				valiu Aobouillo		Process		1 100099 DI900AGI A					
						1 100000		0 0					

Query Registry

Remote System
Discovery
Software Discovery

System Information

System Location

Discovery

Modify Cloud Compute

Modify System Image

Network Boundary Bridging

Obfuscated Files or

Infrastructure Modify Registry



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	.	Account Manipulation	Abuse Elevation Control	Abuse Elevation Control	Adversary-in-the-Middle	Account Discovery	Exploitation of Remote	Adversary-in-the-Middle		Automated Exfiltration	Account Access
Pathar Viatim Haat	Compromise Accounts	Evaloit Dublic Focus	Interpreter Oenteiner Administration	DITOLOho	Mechanism	Mechanism	Druto Force	Application Window	Services Internal Concerniations	Archive Collected Date	Protocol Communication Through	Data Transfer Ciza Limita	Removal
Gather Victim Host nformation	Compromise Accounts	Exploit Public-Facing Application	Container Administration	RH93002	Access Token Manipulation	Access Token Manipulation	Brute Force	Application Window Discovery	Internal Spearphishing	Archive Collected Data	Communication Through Removable Media	ngig ilgilgibi qize filliliz	Data Destruction
Sather Victim Identity	Compromise	External Remote	Deploy Container	 Boot or Logon Autostart	Boot or Logon Autostart	BITS Jobs	Credentials from	Browser Bookmark	Lateral Tool Transfer	Audio Capture		Exfiltration Over	Data Encrypted for
nformation	· ·	Services	ן שלוטץ טטווומווופו וייס אוויס וויס וויס וויס וויס וויס וויס	Execution	Execution		Password Stores	Discovery	Laigiai iuui ilalisigi	Audio oapidio		Alternative Protocol	Imnact
Bather Victim Network	Develop Capabilities	and the same of th	Exploitation for Client	Boot or Logon	ı	1	Exploitation for	Cloud Infrastructure	Remote Service Session	Automated Collection		Exfiltration Over C2	Data Manipulation
nformation	Dovolop dupublililod	That a war o Maamono	Execution	Initialization Scripts	Initialization Scripts		Credential Access	Discovery	Hijacking	Transmarca consensiti	Bara obraodanon	Channel	
Gather Victim Org	Establish Accounts	Phishing		Browser Extensions	Create or Modify System		Forced Authentication	Cloud Service Dashboard	, ,	Browser Session	Dynamic Resolution		Defacement
nformation			Communication		Process				1	Hijacking	•	Network Medium	
Phishing for Information	Obtain Capabilities	Replication Through	Native API	Compromise Client		Deobfuscate/Decode	Forge Web Gredentials	Cloud Service Discovery	, ·	Clipboard Data	Encrypted Channel	Exfiltration Over Physical	Disk Wipe
		Removable Media		Software Binary	Modification	Files or Information			Removable Media			Medium	
Search Closed Sources	Stage Capabilities	Supply Chain	Scheduled Task/Job	Create Account	Escape to Host	Deploy Container	Input Capture	Cloud Storage Object	Software Deployment	Data from Cloud Storage	Fallback Channels	Exfiltration Over Web	Endpoint Denial of
		Compromise						Discovery	Tools	Object	l e	Service	Service
Search Open Technical		Trusted Relationship	Shared Modules		Event Triggered	Direct Volume Access	Modify Authentication	Confainer and Resource	1	Data from Configuration	Ingress Tool Transfer	Scheduled Transfer	Firmware Corruption
Databases		\/-!!-	0 - ft Dl t	Process	Execution	Davas in Dalian	PIOCESS	Discovery		Repository	Multi Otana Ohannala	Tan Data to Olavid	Indiana Oranga Danasana
Search Open Websites/		Valid Accounts	Software Deployment Tools	Event Triggered	Exploitation for Privilege	· · · · · · · · · · · · · · · · · · ·		Debugger Evasion		Data from Information Rennsitories	Multi-Stage Channels	Transfer Data to Cloud Account	Inhibit System Recovery
JUIIIdIIIS Soorah Viatim Nymad			System Services	Execution External Remote	Escalation	I'''Gailleanen	Authentication Multi-Factor	 Domain Trust Discovery	/ tarrior mountainon iva orial	1100001101100	Man Application Layer	AUGUUIII	Network Denial of
Search Victim-Owned Websites			PASIGHT DELAICES		Hijack Execution Flow		Authentication Request	THE HAIT HUST DISCOVERY		Data from Local System	Non-Application Layer		Service
พนทงแนง			User Execution	Services Hijack Execution Flow	Process Injection	Exploitation for Defense	Network Sniffing	File and Directory		Data from Network	Non-Standard Port		Resource Hijacking
			Oooi Excountri	Tilldok LAGoulloll Flow	TOUGOU-INJOUNUM	Evasion	INGIWORK OF HITTING	Discovery		Shared Drive	Non oranidara i on		Tiooduloc Hijaoking
			Windows Management	Implant Internal Image	Scheduled Task/Job		OS Credential Dumping	Group Policy Discovery		Data from Removable	Protocol Tunneling		Service Stop
			Instrumentation	implam imornal triago		Permissions	oo oroaormar barriping	droup I one y blood very		Media	Troided rainieming		001 1100 010p
				Modify Authentication	Valid Accounts	Hide Artifacts	Steal Application Access	Network Service		Data Staged	Proxy		System Shutdown/
				Process			Token	Discovery			·		Reboot
				Office Application		Hijack Execution Flow	Steal or Forge Kerberos	Network Share Discovery		Email Collection	Remote Access Software		
				Startup			Tickets						
				Pre-OS Boot		Impair Defenses	Steal Web Session	Network Sniffing		Input Capture	Traffic Signaling		
							Gookie			0 0			
				Scheduled Task/Job		Indicator Removal on	Unsecured Credentials	Password Policy		Screen Capture	Web Service		
				Carvor Coftware		HUSI		Discovery		Vidoo Conturo			
			The state of the s	Server Software		Indirect Command		Perinheral Nevice		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

ATT&CK 簡述

怎麼使用 ATT&CK

ATT&CK的誤區

Case Studies



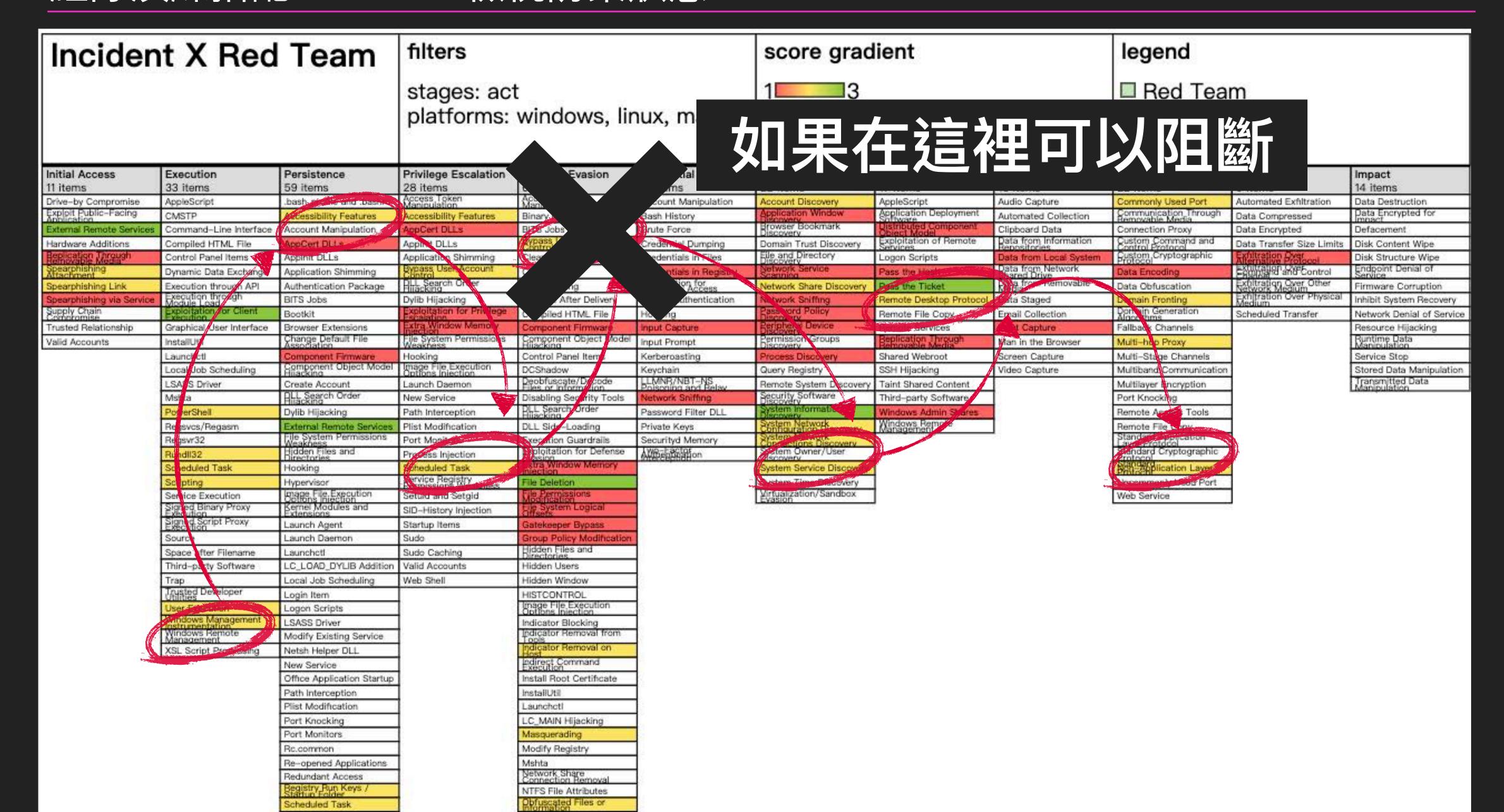
紅隊演練搭配 ATT&CK 檢視防禦狀態

Scheduled Task

Obfuscated Files or

Inciden	nt X Red	Team	filters			score grad	lient		legend			
			stages: act platforms: windows, linux, mac			1 3			□ Red Team□ Incident□ Overlap			
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	Exfiltration 9 items	Impact 14 items	
Drive-by Compromise	AppleScript		Access Token Manipulation		Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exhitration	Data Destruction	
Exploit Public-Facing	CMSTP	Accessibility Features	Accessibility Features	Binary Parting	Bash History	Application Window	Application Deployment	Automated Collection	Communication Through Removable Media	Data Compressed	Data Encrypted for	
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	Blas Jobs	rute Force	Browser Bookmark Discovery	Distributed Component	Clipboard Data	Connection Proxy	Data Encrypted	Defacement	
Hardware Additions	Compiled HTML File	VenCort DLIV	Applied DLLs	ypass User Account	Creden is Dumping	Domain Trust Discovery	Exploitation of Remote Services	Data from Information Repositories	Custom Command and	Data Transfer Size Limits	Disk Content Wipe	
Removable Media	Control Panel Items	Appinit OLLs	Application Shimming	Cear Command	Credentials in Files	Eile and Directory Discovery	Logen Scripts	Data from Local System	Custom Cryptographic Protocol	Exhitration Over Alternative Profocol	Disk Structure Wipe	
Spearphishing Attachment		Application Shimming	Bypass User Account Chotrol	CMSIE	Credenties in Registry	Network Service Scanning	Pass the Head	Data from Network Sared Drive	Data Encoding	CAMPAGE and Control	Endpoint Denial of Service	
Spearphishing Link	Execution through API		PIL Search Order		Exploitation for Credential Access	Network Share Discovery	Das the Ticket		Data Obfuscation	Exfiltration Over Other Network Medium	Firmware Corruption	
Spearphishing via Service	Execution through Module Load	BITS Jobs	Dylib Hijacking	Compile After Deliver	Forced Authentication	Ne twork Sniffing	Remate Desktop Protocol	nita Staged		Exhitration Over Physical Medium	Inhibit System Recovery	
Supply Chain Compromise	Exploitation or Client	Bootkit	Exploitation for Privilege escalation Extra Window Memory	Compiled HTML File	Hooking	Pass, ord Policy Disco. To Periphe. Device	Remote File Copy	Email Collection	Donwin Generation Algor times	Scheduled Transfer	Network Denial of Service	
Trusted Relationship	Graphical User Interface	Browser Extensions	Injection	Component Firmware	Input Capture	Discovery	Production Through	Capture Capture	Fallback Channels		Resource Hijacking	
Valid Accounts	InstallUV	Change Default File Association	File System Permissions Weakness	Component Object Model Hilacking	Input Prompt	Permission Groups Discovery	Bemovable Media	Man in the Browser	Multi-hop Proxy		Runtime Data Manipulation	
<u> </u>	Launchett	Component Firmware Component Object Model Hijacking	Hooking Image File Execution		Kerberoasting	Process Discovery	Shared Webroot	Screen Capture	Multi-Stage Channels	1	Service Stop	
)	Local Job Scheduling LSA S Driver	Hilacking Create Account	Image File Execution Options Injection Launch Daemon		Keychain LLMNR/NBT-NS Poisoning and Relay	Query Registry Remote System Discovery	SSH Hijacking	Video Capture	Multiband Communication Multilayer Encryption	1	Stored Data Manipulation Transmitted Data Manipulation	
1	Mst ta	DLL Search Order		Files or Information Disabling Security Tools	Poisoning and Relay Network Sniffing	Security Software	Third-party Software	1	Port Knocking	1	Manipulation	
	PowerShell	Dylib Hijacking		Mark Comments Manager	Password Filter DLL	System Information	Windows Admin Stares		Remote Apple Tools	1		
	Re svcs/Regasm	External Remote Services	Plist Modification		Drivata Keup	System Network	Windows Remote Wanagement	1	Remote File 4794	1		
1			Port Monit	Execution Guardrails	Securityd Memory	System System Corrections Discovery		t.	Stander Severation			
	Rundli32	Hidden Files and	Process Injection	ofgitation for Defense	AWGERENATION	tem Owner/User			Landard Cryptographic			
ř.	Scheduled Task	Hooking	pheduled Task	stra Window Memory	and September	System Service Discovery			philipplication Laver	ſ		
	Scipting	Hypervisor	Tylee Redshy	File Deletion		A STATE OF THE PARTY OF THE PAR	1		Port.	1		
	Service Execution	Image File Execution Cottons Injection	Setura and Setgid	Medification		Virtualization/Sandbox Evasion]		Web Service			
		Kernel Modules and Extensions	SID-History Injection	Offsets		Total Control Control						
	Sign d Script Proxy	Launch Agent	Startup Items	Gatekeeper Bypass	,							
3	Source	Launch Daemon	Sudo	Group Policy Modification	9							
Į.	Space ofter Filename	Launchott	Sudo Caching	Hidden Files and Directories								
Û	Third-party Software		Valid Accounts	Hidden Users								
	Trap	Local Job Scheduling	Web Shell	Hidden Window	8							
112	Trusted Developer	Login Item		HISTCONTROL Image File Execution								
	User-Editor Management	Logon Scripts		Image File Execution Options Injection	2							
		LSASS Driver		Indicator Blocking Indicator Removal from								
	What have all hall h	Modify Existing Service	113	Tools Indicator Removal on	7							
	XSL Script Purpositing	Netsh Helper DLL		Indirect Command								
		New Service Office Application Startup		Install Root Certificate	0							
		Path Interception		InstallUtil	G.							
		Plist Modification		Launchetl								
		Port Knocking	1	LC_MAIN Hijacking	8							
		Port Monitors		Masquerading	8							
		Rc.common		Modify Registry								
1		Re-opened Applications		Mshta								
		Redundant Access		Network Share Connection Removal	1/							
		Begistry Run Keys / Startun Folder	1	NTFS File Attributes	1							
		Schadulad Teek	10.00	Obfuscated Files or	1							

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

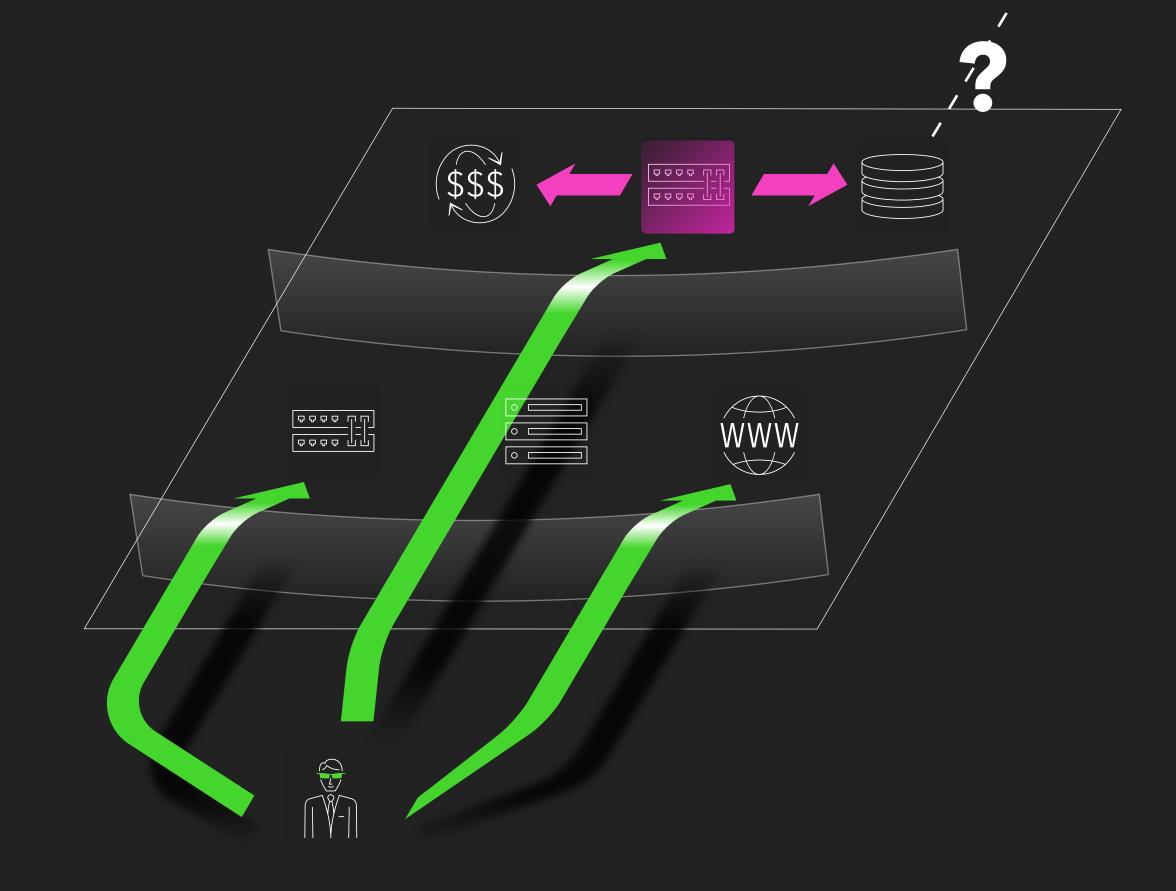
可利用資訊已外洩、未執行滲透測試、已知弱點未修補、WAF無法防護

#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





Takeaways

馬上進行:

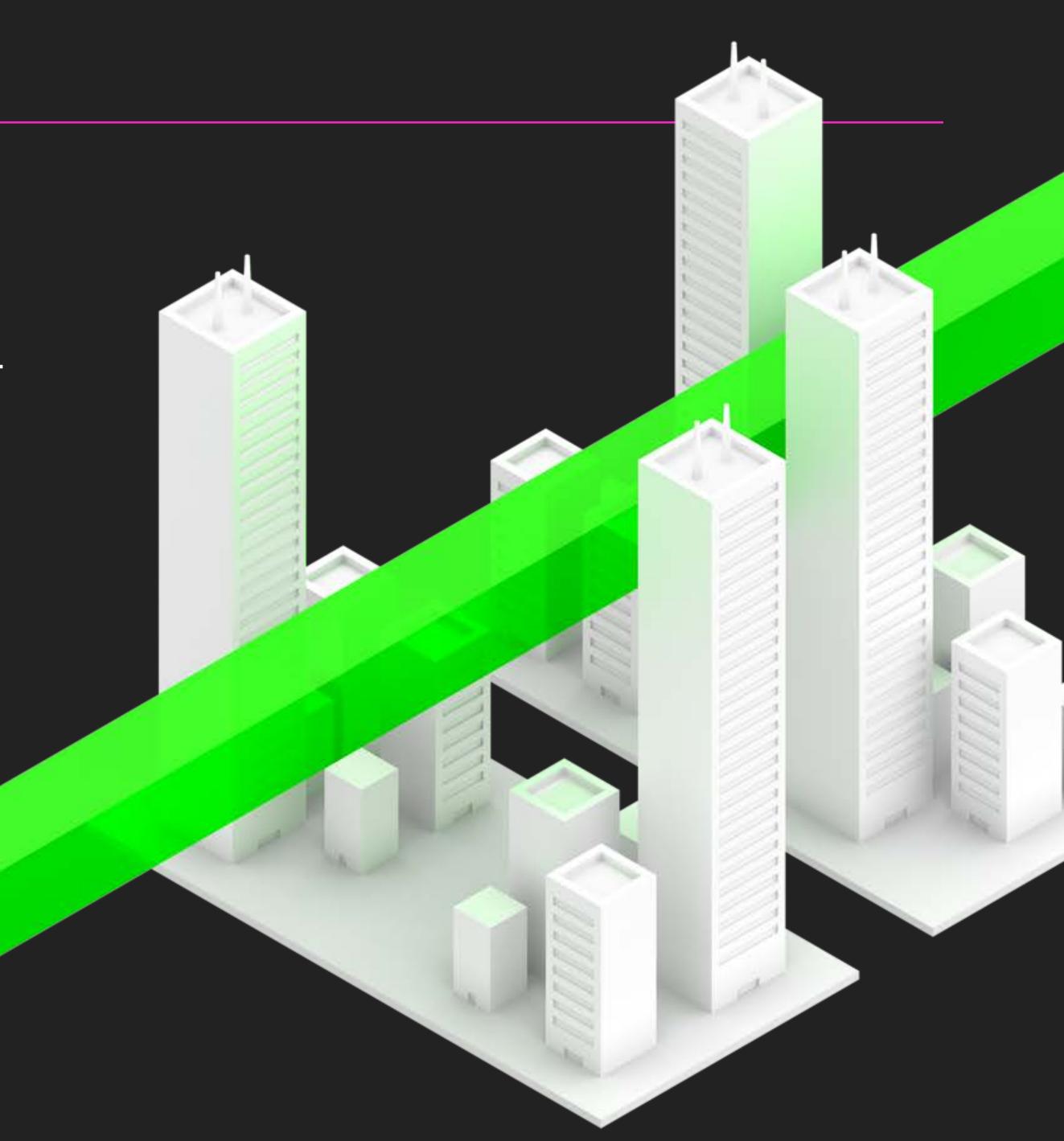
• 用正確的方式回顧過往 ATT&CK 評估

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

Q&A

戴夫寇爾股份有限公司

contact@devco.re