

MITRE ATT&CK 框架概述

蘇柏鳴 / 金融聯合徵信中心 資安部

一、Mitre Corporation介紹

Mitre Corporation是一家美國非營利組織，總部位於Massachusetts(馬薩塞州)，起源始於第二次世界大戰期間的麻省理工學院(MIT)的實驗室，並於1958年從MIT分離出來，除了協助進行多項資安相關研究，也是維運CVE(Common Vulnerabilities and Exposures)¹漏洞資料庫的組織，而ATT&CK框架的研究計畫，是該組織在2015年5月發起。

二、網路攻擊阻殺鏈(Cyber Kill Chain)

Kill Chain在軍事上指的是一種攻擊過程，具體是指識別所要打擊的目標、向目標派遣兵力、決定並下令攻擊目標、最後摧毀目標等一系列攻擊過程。而洛克希德·馬丁²(Lockheed Martin)公司將這一攻擊過程導入資訊安全領

域，設想駭客也會採取這種攻擊過程，並將其稱之為Cyber Kill Chain，共分成以下7個步驟：

1. 偵查 (Reconnaissance)

研究、識別及選擇目標，可以在網際網路上利用像是WHOIS、SHODAN、GOOGLE、COMPANY WEBSITE...等搜尋相關資訊，或是利用NMAP、PORT SCANNING、BANNER GRABBING、VULNERABILITY SCANNERS...等工具掃描或探測目標環境。

2. 武裝 (Weaponization)

在這階段入侵者會針對目標設計一些惡意軟件武器，例如使用SET(Social-Engineer Toolkit)來執行網路釣魚攻擊與SQLMap來發現並利用給定的URL的SQL Injection漏洞。

3. 傳遞 (Delivery)

駭客將攻擊武器傳輸到攻擊目標環境，目前最常用運送的方法是E-Mail附件、網站及USB儲存媒體。

¹ 是一個與資訊安全有關的資料庫，收集各種資安弱點及漏洞並給予編號以便於公眾查閱，此資料庫現由美國非營利組織MITRE所屬的National Cybersecurity FFRDC所營運維護。

² 是一家美國航空航太製造廠商，以開發、製造軍用飛機聞名世界。https://en.wikipedia.org/wiki/Lockheed_Martin

4. 弱點攻擊 (Exploitation)

駭客在系統中發現漏洞，他們便會利用該漏洞進入系統安裝允許駭客命令執行的惡意軟體，並在網路內部建立立足點後，透過Internet下載其他工具，並嘗試提升自身權限。

5. 安裝(Installation)

指駭客在目標環境中安裝木馬或後門程式。

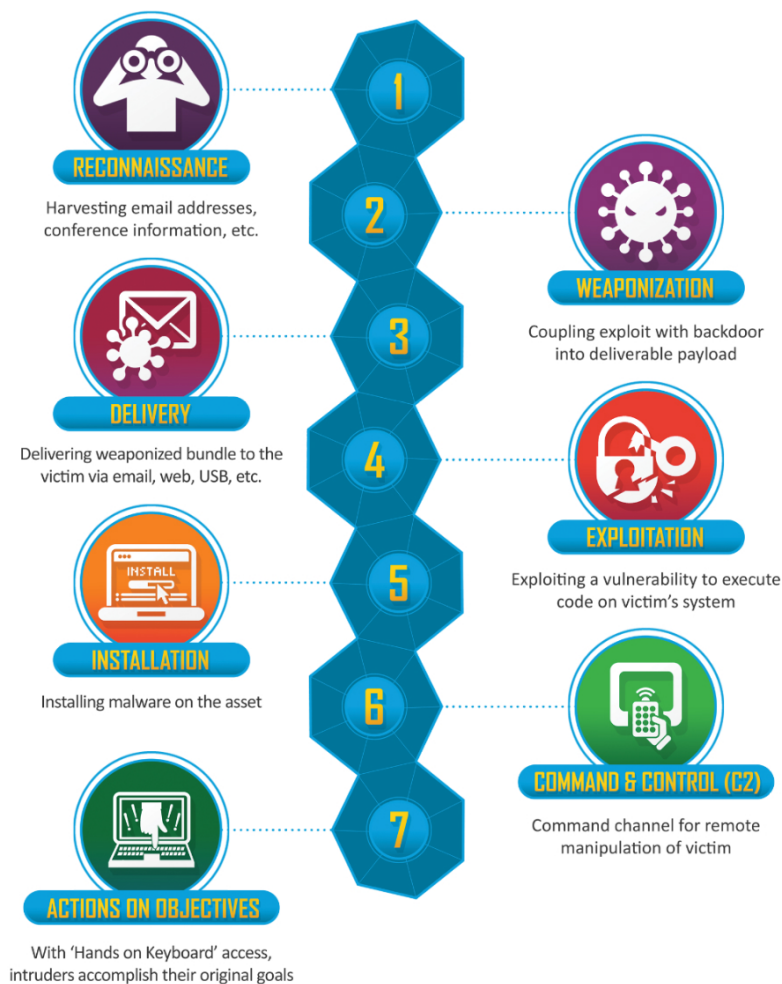
6. 命令與控制 (Command & Control)

在被駭系統上安裝可遠端存取的後門或木馬，讓駭客可以在目標環境中維持存在並執行遠端命令。

7. 採取行動 (Actions on Objectives)

是指駭客如何實現其最終目標，駭客最終目標可能用勒索軟體獲得贖金、中斷企業營運或竊取內部資料等。

圖1、Cyber Kill Chain 七步驟³



³ Cyber Kill Chain, <https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html>.

三、MITRE ATT&CK 框架

MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) 「戰術、技術和知識庫」，主要整合網路攻擊行為，反映了攻擊者生命週期的各個階段變化，可對於理解已知攻擊行為與手法，並可驗證既有防禦控管是否有效，在version 7前的版本主要分成PRE-ATT&CK、ATT&CK Enterprise與ATT&CK Mobile，PRE-ATT&CK定義了駭客攻擊前置作業，相當於Cyber Kill Chain的前兩個步驟(偵查與武裝)，而Enterprise與Mobile的戰術及技術基本上大同小異，對照了Cyber Kill Chain的後五個步驟(傳遞、弱點攻擊、安裝、命令與控制及採取行動)。

PRE-ATT&CK畫分為15個戰略階段與148個技術，15個戰略階段依序分為Priority Definition Planning、Priority Definition Direction、Target Selection、Technical Information Gathering、People Information Gathering、Organizational Information Gathering、Technical Weakness Identification、People Weakness Identification、Organizational Weakness Identification、Adversary OPSEC、Establish & Maintain Infrastructure、Persona Development、Build Capabilities、Test Capabilities、Stage Capabilities。

圖2、PRE-ATT&CK 戰略階段及技術

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

而ATT&CK Enterprise是指具體的攻擊入侵過程，也是現在各界最主要討論的項目，當中涵蓋Windows、Linux與macOS這三種系統平台，分為12個戰略階段，184個技術，12個Tactics依序包含了Initial Access、Execution Persistence、Privilege Escalation、Defense Evasion、Credential Access、Discovery、Lateral Movement、Collection、Command and Control、Exfiltration及Impact，像是Initial Access策略裡包含了9個技術(Techniques)：

1. Drive-by Compromise

2. Exploit Public-Facing Application

3. 外部遠端連線 (External Remote Services)

4. Hardware Additions

5. 網路釣魚 (Phishing)：可分為魚叉式附件、連結及服務。

6. Replication Through Removable Media

7. 供應鏈攻擊 (Supply Chain Compromise)：開發工具、軟體及硬體的供應鏈攻擊。

8. Trusted Relationship

9. 有效帳號 (Valid Accounts)：Domain帳號、Local帳號、預設帳號及雲端帳號。

圖3、ATT&CK Enterprise(version 7) 戰略階段及技術

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

12 Tactics

MITRE ATT&CK在2020年10月27日發布了version 8，此最新的版本將PRE-ATT&CK 濃縮成偵查（Reconnaissance）及

資源開發（Resource Development）後納入MITRE ATT&CK，變成了14個Tactics及184個Techniques。

圖4、MITRE ATT&CK 版本更新時間

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
Active Scanning (2)	Acquire Infrastructure (6)	Drive-by Compromise	Command and Scripting Interpreter (8)	Account Manipulation (4)	Abuse Elevation Control Mechanism (4)	Abuse Elevation Control Mechanism (4)
Gather Victim Host Information (4)	Compromise Accounts (2)	Exploit Public-Facing Application	Exploitation for Client Execution	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)
Gather Victim Identity Information (3)	Compromise Infrastructure (6)	External Remote Services	Inter-Process Communication (2)	Boot or Logon Autostart Execution (12)	Boot or Logon Autostart Execution (12)	BITS Jobs
Gather Victim Network Information (6)	Develop Capabilities (4)	Hardware Additions	Native API	Boot or Logon Initialization Scripts (5)	Boot or Logon Initialization Scripts (5)	Deobfuscate/Decode Files or Information
Gather Victim Org Information (4)	Establish Accounts (2)	Phishing (3)	Scheduled Task/Job (6)	Browser Extensions	Boot or Logon Initialization Scripts (5)	Direct Volume Access
Phishing for Information (3)	Obtain Capabilities (6)	Replication Through Removable Media	Shared Modules	Compromise Client Software Binary	Create or Modify System Process (4)	Execution Guardrails (1)
Search Closed Sources (2)		Supply Chain Compromise (3)	Software Deployment Tools	Create Account (3)	Event Triggered Execution (15)	Exploitation for Defense Evasion
Search Open Technical Databases (5)		Trusted Relationship	System Services (2)	Create or Modify System Process (4)	Exploitation for Privilege Escalation	File and Directory Permissions Modification (2)
Search Open Websites/Domains (2)		Valid Accounts (4)	User Execution (2)	Event Triggered Execution (15)	Group Policy Modification	Group Policy Modification
Search Victim-Owned Websites			Windows Management Instrumentation	External Remote Services	Group Policy Modification	Hide Artifacts (7)
				Hijack	Hijack Execution Flow (11)	Hijack Execution Flow (11)
					Impair Defenses (7)	Impair Defenses (7)
					Indicator Removal on Host (6)	Indicator Removal on Host (6)

圖5、PRE-ATT&CK 納入ATT&CK Enterprise

Below are a list of versions of the ATT&CK website preserved for posterity, including a permalink to the current version of the site:

Version	Start Date	End Date	Data	Release Notes
ATT&CK v8 (current version)	October 27, 2020	n/a	v8.1 on MITRE/CTI	Updates – October 2020
ATT&CK v7	July 8, 2020	October 26, 2020	v7.2 on MITRE/CTI	Updates – July 2020
ATT&CK v7-beta	March 31, 2020	July 7, 2020	v7.0-beta on MITRE/CTI	Updates – March 2020
ATT&CK v6	October 24, 2019	March 30, 2020	v6.3 on MITRE/CTI	Updates – October 2019
ATT&CK v5	July 31, 2019	October 23, 2019	v5.2 on MITRE/CTI	Updates – July 2019
ATT&CK v4	April 30, 2019	July 30, 2019	v4.0 on MITRE/CTI	Updates – April 2019
ATT&CK v3	October 23, 2018	April 29, 2019	v3.0 on MITRE/CTI	Updates – October 2018

Versions from before the migration from MediaWiki are not preserved on this site:

ATT&CK v2	April 13, 2018	October 22, 2018	v2.0 on MITRE/CTI	Updates – April 2018
ATT&CK v1	January 16, 2018	April 12, 2018	v1.0 on MITRE/CTI	Updates – January 2018

四、結論

根據相關權威資安公司這幾年的研究報告指出，進階持續性威脅（Advanced Persistent Threat, APT）被發現前的潛伏時間都非常久，代表這類攻擊非常難以被發現，而攻擊手法的隱匿性及多樣化，讓資安防護工作應對非常的吃力，而MITRE 提出的ATT&CK方法，藉由整

理所發現之駭客的攻擊手法，將其歸納為策略階段（Tactics），並將每個階段會使用之技術分類出來，讓資安防護工作可以「知己知彼，百戰不殆」，除此之外也可以拿來檢視目前防護工作的不足，及檢視相關資安產品防護能力的優劣。