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 SCANNIG、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]

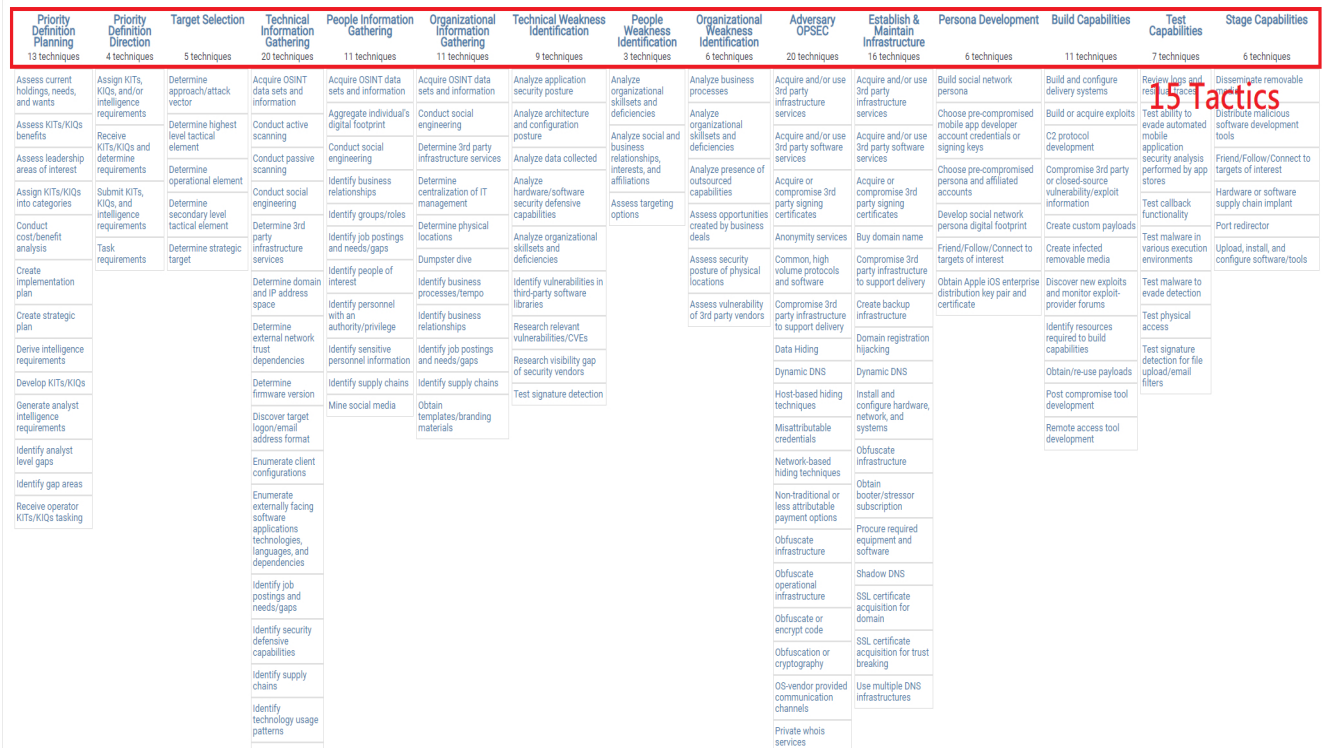
[3] Cyber Kill Chain, https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html.

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



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

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

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。