駭客攻擊的防護機制

資料參考來源: ATT&CK 資訊安全知識庫

ATT&CK 資訊安全知識庫的起源

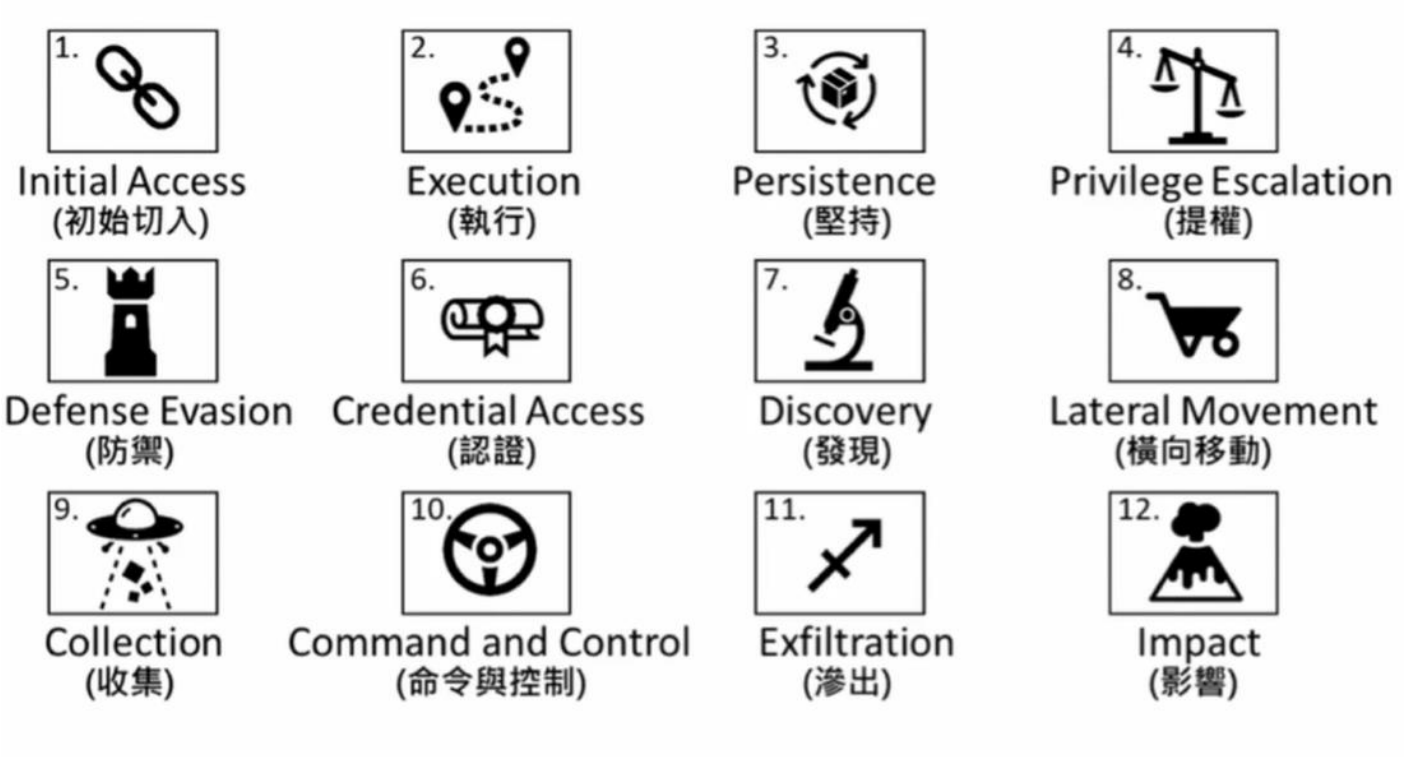
MITRE 是一家非營利組織，它和很多政府、非營利組織或一些技術專家配合，集結大家的 Knowhow 形成知識庫，免費提供 Solution 給其他企業使用，ATT&CK 就是其中針對資訊安全的知識庫，這裡面記錄了有哪些駭客組織，駭客組織用什麼樣的攻擊手法等等。

About TRS File Monitor

TRS File Monitor 是一套翊捷資訊(Team Rise System)研發的防勒索軟體(Anti-Ransomware) ，參考 ATT&CK 資訊安全知識庫，駭客攻擊的防護機制，實地驗證在許多方面是有效防止駭客攻擊的軟體工具。

駭客攻擊的 12 個階段

在 ATT&CK 資訊安全知識庫裡面，分析一個駭客入侵企業總共有 12 個階段。



1.初始切入

駭客攻擊企業，一定要有和企業接觸的管道，例如：打電話、Email、Web、Terminal、RDP 漏洞、甚至身體接觸。

2.執行

當駭客接觸到企業以後，就會有很多的攻擊或者誘騙手法，讓用戶不小心或是不經意間執行惡意程式。

3.堅持

惡意程式被執行了以後，駭客會留下後門，以便未來連線使用。例如：駭客可能會留下一些 Power Script 或者是.bat、Psexec、psexesvc 等程式，這些程式被啟動之後會自動運行，這樣在用戶下一次開機的時候，駭客就可以連線進來。

4.提權

當駭客已經可以連線進來以後，就會需要對連線的這台電腦具有一定的掌控權限，也就是提權。

5.防禦

惡意程式想要不被防毒軟體偵測到、被阻擋或清除，最簡單的做法就是停掉防毒軟體，這就是防禦。

6.認證

接下來，惡意程式就可以破解登入電腦的帳號密碼。

7.發現

惡意程式會做 Scan，去發現網路裡面還有哪些裝置、哪些電腦設備是存在漏洞可以被利用的。

8.橫向移動

當惡意程式找到目標物以後，就會從入侵的這台電腦橫向移動到目標電腦上。

9.收集

惡意程式透過目標電腦，進一步入侵資料庫，收集想要的資訊。

10.命令與控制

收集到足夠的資訊以後，惡意程式就可以掌控更多的電腦和設備。

11.滲出

惡意程式透過掌控的電腦竊取資料。

12.影響

惡意程式將資料庫主機加密，出售資料變現，甚至植入勒索病毒。

以上是駭客攻擊的 12 個階段，**當然因為情況的不同，不是一定完全按照這樣的步驟執行**。

各階段攻擊手法

在 ATT&CK 資訊安全知識庫裡面，提列了每個階段的攻擊手法，我們來說明幾個駭客攻擊的常用手法。

階段	手法
初始切入	攻擊Terminal主機、發送釣魚信件
執行	以釣魚信件為例，就是誘騙使用者點擊惡意程式
堅持	利用PowerShell執行連線，或在電腦中埋入安全後門
提權	關閉防毒軟體、防火牆
認證	暴力破解登錄密碼
發現	網路掃描，常用網路指令Ipconfig、nbtstat或Arp的Scan
橫向移動	透過Scp、rsync或者Sftp把惡意程式傳輸到目標電腦
滲出	竊取資料再透過合理的封包滲出，例如透過Web 80Port滲出
影響	加密入侵的系統

駭客攻擊的防護機制

這 12 個階段也可以劃分為 5 大程序，這五個程序都有相對應的防護機制。

1.侵入階段的防護機制

(1)防火牆

(2)防毒軟體及防勒索軟體(如 TRS File Monitor Anti-Ransomware)

(3)SPAM

(4)資訊安全意識提升教育訓練：教育員工不能隨意點擊 Mail。

2.固守階段的防護機制

(1)使用中央控管型防毒軟體及防勒索軟體：防毒或防勒索軟體被停用時會告警。(如 TRS File Monitor Anti-Ransomware)

(2)EDR(Endpoint Detection and Response)：端點異常入侵時可被偵測並告警。

(如 TRS File Monitor Anti-Ransomware)

3.擴大階段的防護機制

(1)EDR(Endpoint Detection and Response)：偵測外來攻擊。

(如 TRS File Monitor Anti-Ransomware)

(2)Log 收集器：收集每個 Server 跟 client 端的 Log。

(如 TRS File Monitor Anti-Ransomware)

4.掌握階段的防護機制

Log 收集器：偵測大量收集、異常收集行為。

(如 TRS File Monitor Anti-Ransomware)

5.收割階段的防護機制

(1)DLP(Data Loss Prevention) (如 TRS File Monitor Anti-Ransomware)

(2)不被惡意病毒及勒索軟體影響的備份機制

結語

藉由上述說明了解網路常見的攻擊，以實際了解駭客的行為，進而知道如何保護網路、制定策略、權限，防堵系統免受不法駭客的攻擊。

TRS File Monitor Anti-Ransomware 官網: https://www.teamrise.com.tw/trsfilemonitor_ch/