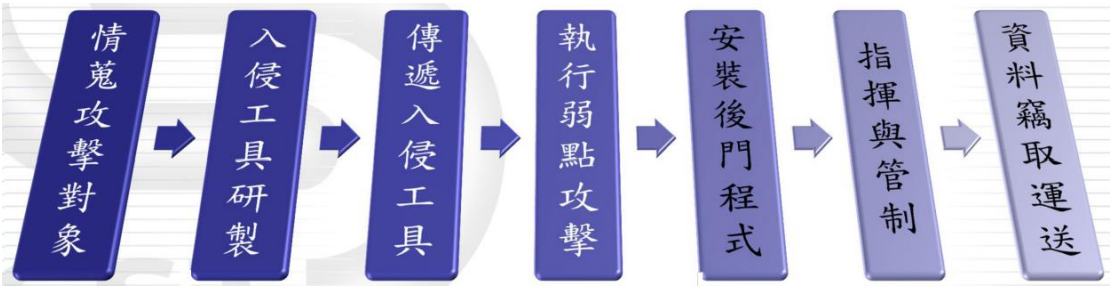
進階持續性攻擊 (Advanced Persistent Threat, APT)

“資安業者卡巴斯基實驗室表示，華碩筆電的更新伺服器遭駭客入侵，駭客透過偽裝成正常軟體更新的方式，藉此散布惡意後門,” [1] 上週驚傳國內筆電大廠華碩遭到 APT 攻擊, 自動更新程式(Asus Live Update)遭駭客植入惡意程式碼, 企圖去攻擊特定的對象, 更據卡巴斯基(Kaspersky)估計, 全球約有 100 萬人受到影響。而在去年 7 月時, 新加坡政府的保健服務集團系統遭受該國史上最大的駭客攻擊, 洩漏了包含總理李顯龍等 150 萬人的個人資料及處方資料, 也被認為和 APT 政擊有關[2]。

進階持續性攻擊(APT)是駭客組織針對特定政府, 企業或平台所進行的複雜且多方位的網路攻擊[3], 它是一個低調且緩慢的過程, 時間有可能長達數個月到數年，它利用了複雜的工具與手法接近目標對象引誘目標上當，進而竊取駭客鎖定的機密資料[4]。

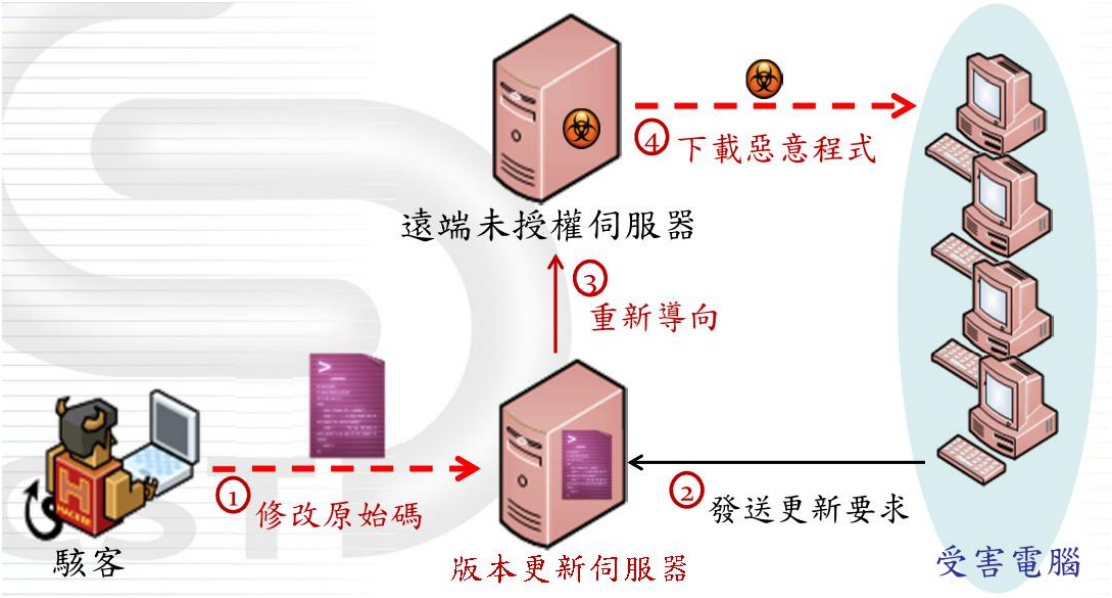
APT 通常是一個與國家掛勾的駭客集團組織所發動的攻擊, 它會先搜集所要攻擊目標對象的帳號、使用習性等資料, 並針對目標制定出不同的攻擊手法, 圖一為網際攻擊狙殺鍊(Cyber Kill Chain) [5]的流程圖, 其最終目的是取得機構內的機密資料, 並不聲不響地將資料透過網路加密送出。APT 會客製化攻擊目標專屬的入侵工具, 並利用社交程式、惡意郵件, 傳送能吸引目標目光的專屬文章或網站引誘目標將其打開, 甚至利用水坑式(Watering Hole)攻擊, 埋伏在攻擊目標常逛的網站中, 所謂水坑式攻擊是觀察攻擊目標瀏覽網站的習慣, 預先去攻擊

這些網站並植入零日漏洞的惡意程式。透過這些方式攻擊目標就在不知不覺中被安裝了惡意程式，以作為攻擊發動的進入點。一旦惡意程式被安裝，駭客即可在公司埋下了一個控制點，通常駭客會先在這台電腦上安裝遠程操控程式，以便從外網遠程操控這台被開了後門的電腦。一般而言，第一台被入侵的目標電腦並不是攻擊者感興趣的，它感興趣的是機構內保存重要資料的伺服器，被攻陷的電腦只是做為一個掃描系統漏洞的跳板，以便攻擊更多的電腦和伺服器。目前很多機構都會安裝單一登入系統(SSO)，一旦駭客取得了攻擊目標的帳號，就可以進入到內網中更多的系統當中，一步步地在內網中擴張直到入侵到擁有高權限的使用者帳戶，再透過這些高權限帳號取得機構內的機密資料。



圖一、網際攻擊狙殺鍊(Cyber Kill Chain)[5]

圖二是類似於這一次華碩攻擊的流程，透過軟體自動更新的功能，讓電腦自動下載並安裝惡意程式。其作法是駭客入侵軟體版本更新伺服器，更改了上面的程式碼讓使用者在下載更新程式時，自動轉向到駭客入侵或架設的伺服器上，然後下載並安裝已被駭客修改添加了惡意程式的更新程式。



圖二、應用程式軟體更新 [5]

參考資料:

1. "華碩更新伺服器驚傳遭駭，官方下午回應：鎖定特定機構用戶的攻擊" iThome, https://www.ithome.com.tw/news/129597
2. "星國史上最大網路攻擊，懷疑是政府駭客發動的 APT 攻擊," iThome, https://www.ithome.com.tw/news/125026
3. "什麼是 APT 進階持續性威脅 (Advanced Persistent Threat, APT)？," 資安趨勢部落格, https://blog.trendmicro.com.tw/?p=123
4. "淺談社交工程與 APT 攻擊," 陳淑萍, http://www.cc.ntu.edu.tw/chinese/epaper/0035/20151220_3504.html
5. "近期 APT 攻擊案例分享," 劉建良, http://download.icst.org.tw/attachfilenew/1.%E8%BF%91%E6%9C%9FAPT%E6%94%BB%E6%93%8A%E6%A1%88%E4%BE%8B%E5%88%86%E4%BA%AB.pdf