自動更新服務成了駭客攻擊跳板？！

賽門鐵克科普小教室

「供應鏈攻擊」

供應鏈攻擊是一項顯著的威脅態勢，2018 年的攻擊增加了 78%。供應鏈攻擊利用第三方服務和軟體來破壞最終目標，包括劫持軟體更新、將惡意程式碼植入合法軟體等。攻擊者的手法包括竊取版本控制工具憑證，或破壞較大軟體專案的第三方程式庫。攻擊者選擇劫持軟體更新的原因，就是越來越難找到可刺探利用的零時差漏洞。因此供應鏈攻擊是能達到目標且有效率的替代做法。

軟體更新供應鏈攻擊可定義如下：
在正當軟體套件的正常分佈位置植入惡意軟體，可能的情境包括在軟體廠商內生產期間、第三方儲存位置、透過重新導向而導致。典型的攻擊情境是攻擊者用惡意版本取代正當軟體更新，偷偷地將其迅速散佈給預期目標。凡是有使用者套用該軟體更新，他們的電腦就會自動受到感染，並且讓攻擊者在使用者的網路上得以取得立足之地。受害目標不僅限於桌上型電腦，也同樣適用於物聯網裝置和工業控制器元件。

攻擊者動機
軟體更新供應鏈之所以對攻擊者具有吸引力，有六個主要原因：
01 利用受信任的管道滲透受良好保護的組織
02 隨著使用者自動更新，感染數量迅速成長
03 以特定地區或部門為目標
04 滲透已隔離目標，如工業環境中的目標
05 受信任程序遭到濫用，很難識破攻擊
06 在安裝期間能為攻擊者提供更高的權限

資料來源：賽門鐵克ISTR第23、24期報告

賽門鐵克建議

企業用戶最佳實務

- 使用者上網安全管控，阻擋使用者連線至非業務需求之網站，並於使用者下載檔案時，透過沙箱系統進行檢測 。
- 針對未分類或風險級別高之網站，透過上網隔離系統進行風險隔離。
- 不要打開來路不明之郵件，部署郵件安全閘道，針對病毒及釣魚郵件進行過濾，並針對附件檔案進行沙箱檢測。
- 於對外服務之網頁伺服器進行白名單管控。
- 於端點電腦部署 EDR (Endpoint Detection and Response)系統，針對異常端點行為進行分析。

事中進階防護建議

- 進行防毒軟體更新及全系統掃描，鎖定存在該惡意更新程式之端點，檢視該端點近三個月之病毒及 EDR事件，確認是否隔離端點及啟動IR (Incident Response) 服務，以先控制損害並立即進行改善
- 針對該端點進行近三個月 NIPS、防火牆及 Proxy 事件檢視，確認是否連線至其他惡意網站或 C&C Server，統計有連線之網站或 IP，反向調查是否還有其他端點連線行為
- 於 SIEM 平台檢視該端點及有連線之網站及 IP 近三個月之關連事件，確認是否有其他異常行為

軟體開發商

- 需加強防護 APT 攻擊，進行使用者上網安全管控及郵件 APT 安全強化管控機制
- 針對未分類或風險級別高之網站，透過上網隔離系統進行風險隔離。
- 具備 SSDLC (安全的軟體發展生命週期)，軟體更新檔案上線前，需進行沙箱檢測
- 於軟體更新檔案上線之流程，需確認檔案之一致性。
- 於軟體更新檔案上傳於網站後，即時監控或鎖定該檔案之一致性。
- 針對開發相關伺服器及更新伺服器，採用白名單管控機制。

賽門鐵克建議解決方案

Symantec Web Isolation
Symantec Endpoint Detection and Response
Symantec Advanced Threat Protection
Symantec Data Center Security
Symantec Incident Response