資財四乙_107AB0730_賴奕辰_網路與系統安全期中報告

何謂供應鏈攻擊？
一起供應鏈攻擊是由至少兩起攻擊結合而成的。第一起攻擊對象是供應商，並用於獲取目標的資產，而目標可以是最末端的客戶或是其他的供應商。因此若要定義一次攻擊為供應鏈攻擊，其中供應商和客戶都必須成為攻擊對象。

供應鏈攻擊的生命週期可以看作是兩起APT攻擊（高級長期威脅）的結合，第一起攻擊目標為一或多個供應商，第二起攻擊目標為客戶。這些攻擊都需要縝密的計畫和執行。

其中APT攻擊具備幾個要點：具有針對性、獲得對組織機構越權訪問權限（通常是代碼執行）、持續很長時間以及最終目的和目標具有特定關係（和密幣挖掘不同）。

報告整理了近期供應商和客戶遭攻擊的手法和遭盜取的資產，以及報告的要點有說明：

- 約62%的針對客戶的攻擊利用的是客戶對供應商的信任。
- 在62%的攻擊中，攻擊手法為使用惡意軟體。
- 在目標資產方面，在66%的安全事件中攻擊者通過供應商代碼進一步攻陷目標客戶。
- 約58%的供應鏈攻擊旨在獲得數據（主要是客戶數據，包括個人數據和知識財產）的訪問權限，約16%的攻擊為了訪問人員。

由以上的要點，我想要以SolarWinds Orion案例進行分享。因為此案例除了有名之外，供應商和客戶遭攻擊的手法和被盜取的資產都是在供應鏈攻擊中佔大多數的。

SolarWinds Orion案例中：
對供應鏈的攻擊手法：利用軟體漏洞、暴力攻擊、社交工程。
對客戶端的攻擊手法：利用對供應商的信任、惡意感染。
對供應商的目標：進程、代碼。
對客戶端的目標：數據。

SolarWinds是一個管理和監控軟體的供應商，Orion則是該供應商的網管產品，駭客先用了名為Sunspot的惡意程式，在軟體開發的階段中在Orion程式碼注入Sunburst後門和Beacon程序，軟體經過編譯、簽章後就變成具有惡意程式的產品，

Sunburst啟動後會檢查AD網域是否在SolarWinds中，若在清單之中才會執行。這樣能判斷自身是否在開發環境中，以在程式發布後才執行惡意程式。攻擊者注入在Orion Platform的程式碼，撰寫方式都與原本程式非常相像，包括變數、函式（Function）的命名，以及程式的結構。例如一行程式碼中寫著 assemblyTimestamps ，看似檢查時間戳記，但這是用前面所提的HASH加解密隱藏起來，實際作用是惡意程式要檢查的防毒驅動程式與處理程序等。

當帶有Sunburst後門的Orion Platform被部署到客戶端時，該後門內建主動通知能力的Beacon這時才會啟動，連回C&C中繼站通知攻擊者，而不是由中繼站主動去連線。

Sunburst有兩個階段，第一階段是Beacon使用DNS通訊協定回傳資訊，第二階段是後門使用HTPP通訊協定。因此，他們從Passive DNS找出曾經進入第二階段，也就是可以讓攻擊者操作後門的階段，以及其所對應的AD網域名稱，便可找出哪些是攻擊者感興趣的目標。