資財三乙 108AB0738 徐偉翔

網路與系統安全期中報告

近年來供應鏈攻擊儼然已經成為資安界的頭號大敵，2020 美國 SolarWinds 公司被攻擊的事件更是讓這個議題受到更高度的關注。

2020 年的人們在為了突如其來的 covid-19 疫情被迫改變生活習慣忙得不可開交之時，各路的駭客也沒有閒著，當眼看 2020 就要過去時，12 月初 Fireeye 公司卻揭露了一場外媒比喻是近年最大的資安攻擊事件----「SolarWinds 資安攻擊事件」。

SolarWinds 是一間發展企業管理網路系統、資訊基礎設施的資源監控起家的公司，世界財富 500 強的企業中就有 425 間企業使用 SolarWinds 的產品。其中包含電信商、國防單位、軍火商、國務院、政府機關、大學院校都是它的客戶，從北美、歐洲，一直到亞洲的印度、中國大陸、日本與台灣都有企業採用它們旗下產品。2020 年 12 月美國的 FirEeye 公司被入侵，被竊取資安演練中扮演進攻角色紅隊的駭客分析工具。而後 FirEeye 資安公司揭露 SolarWinds Orion 網管監控軟體被置換植入含有惡意程式，卻同時具有 SolarWinds 公司數位簽章，並將此次攻擊命名為「Sunburst 旭日攻擊」。

而事情並沒有這麼簡單就落幕，很快的更多間的資安業者也指出駭客發動了第二波「Supernova 超新星」攻擊，不同於 Sunburst 攻擊手法，採用 Webshell 方式進行入侵。

2020年12月9日	FireEye紅隊測試工具外流
2020年12月13日	CISA針對SolarWinds Orion發布緊急指令，FireEye揭露發現Sunburst惡意程式
2020年12月13-14日	路透社與華爾街日報披露美國財政部與商務部遭供應鏈攻擊
2020年12月15-18日	第二支惡意程式Supernova被揭露
2020年12月17日	微軟、FireEye與GoDaddy聯手打造該攻擊的銷毀開關
2020年12月17日	微軟揭露潛在受害者
2020年12月31日	微軟證實SolarWinds駭客存取其原始碼
2021年1月5日	美國CISA、DNI與NSA調查報告猜測攻擊者來自俄羅斯
2021年1月6日	美國司法部證實遭駭
2021年1月11日	SolarWinds調查報告公布指出攻擊源頭為Sunspot
2021年1月13日	CISA指出繞過雲端服務多因素驗證的攻擊案例
2021年1月19日	FireEye釋出針對Microsoft 365補救措施
2021年1月19日	Malwarebytes表示自己也遭駭
2021年1月22日	微軟揭露攻擊者在第二階段所採取的攻擊行動
2021年2月18日	微軟內部調查最後更新揭露
2021年3月4日	FireEye、微軟揭露新發現的惡意程式Sunshuttle後門

以 SolarWinds 委由 CrowdStrike 調查的報告內容來看，有三個關鍵的時間點。首先，攻擊者在 2019 年 9 月 4 日，就已經入侵了 SolarWinds 的內網；第二，到了 2020 年 2 月 20 日，攻擊者正式將 Sunburst 後門部署到該公司系統環境；第三，直到 2020 年 12 月 12 日，SolarWinds 才知道有這個後門的存在。顯然，攻擊者入侵後在內網已經做了很多探查，當了解夠深透後才將後門 Sunburst 植入，而且，從 SolarWinds 知道被入侵，回推到最早被入侵的時間點，這段期間長達 1

年 3 個月之久。

為何駭客可以在軟體開發流程被滲透，而且不被發現呢?我們可以參考 Fox-IT 威脅分析師吳宗育的說法:「以軟體開發流程而言，這裡簡單分成提交（Commit）、編譯（Build）、測試（Test）與部署（Deploy），攻擊者先是打造了一個名為 Sunspot 的惡意程式，這是用於植入惡意程式的程序（Injector），在軟體開發提交階段，可將一段 Sunburst 後門與 Beacon 的程式碼，注入到 Orion Platform 的程式碼。因此，之後軟體經過編譯、簽章後，就會變成帶有惡意程式的軟體產品。」

在躲避偵測與偽裝融入環境上，SolarWinds 攻擊者注入在 Orion Platform 的惡意程式會有一份檢查清單，這些都是屬於 SolarWinds 的網域，目的是當惡意程式處於開發者環境時先不要動作，等到軟體更新部署到客戶端時，才會進一步載入其他惡意程式。而且，這些惡意程式碼的撰寫與程式原本的架構很相像。例如一行程式碼中寫著看似檢查時間戳記的 assemblyTimestamps，但其實攻擊者是用 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。

個人看完之後都驚呆了，連 FirEeye 這種做資安的大公司都會被入侵了，更何況是小公司、政府機關與一般民眾，不過我覺得 FirEeye 的處理很棒，他們是第一個能夠發現此威脅的受害者。在他們發現問題後，馬上進行調查，並將結果盡快與社群、產業分享，避免事件擴大，也縮短應對攻擊時間。否則，其他受害者可能到現在還是不知情，並有更多受駭可能。或許駭客有無數種入侵方式，也許我們還未知的漏洞有無數個，但我相信資安界是有著很強的實力的，在使用著望路帶來便利的同時，也該好好感謝資安人員為我們打造安全的環境。