網路與系統安全 - 期中報告

資財三乙 108AB0726 李昕翰

1. 事件說明

在 2020 年底，美國政府機構與企業遭遇有史以來最大的資安威脅，這場風暴的核心，是網路監控產品 SolarWinds Orion 平臺遭入侵，駭客透過這種方式間接攻入鎖定的目標對象，由於這套產品廣為美國政府機構與企業使用，隨著事件的揭露，已有越來越多受駭者，事件也持續蔓延，甚至還發現又有另一後門程式。

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。

2. 事件剖析

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。

而且，由於攻擊者已經非常熟悉開發環境與流程，因此當惡意程式處於開發者環境時，並不會執行任何惡意的動作，而是等到軟體更新部署於客戶端時，才會進行下一步，載入其他惡意程式。

而隱藏在 Orion Platform 的惡意程式，使用了一個名為 FNV-1A HASH 來加密一系列字串，當執行 Sunburst 後門時，會先檢查 AD 網域是否屬於 SolarWinds，如果與清單符合，就不會執行，同時也會針對很多防毒驅動程式、處理程序與服務去進行檢查，並且都會經過該 HASH 來保護，而不被企業防護偵測。

特別的是，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。