kaspersky

國際重大資安情資分享

近期關於大量報導關於 Solarwind 被利用的攻應鏈攻擊事件。在威脅第一時間公佈後，我們對事件開始進行了調查，並確保卡巴斯基的用戶已可偵測到相關的惡意程式及連結的 C2 位置。在此調查過程中，我們找到了一些非常有趣及特別的資訊。可參考以下連結，有相關詳細的描述：
https://securelist.com/sunburst-connecting-the-dots-in-the-dns-requests/99862/

節錄上述相關報導幾個重要部份及常問問題：

此為一 APT 利用供應鏈攻擊的實際案例，在此案例中，所有的調查都還在進行中。包含 Fireeye 及其他友商都在持續協助進行。在這個階段我們發現到。

一、 此案例使用的手法非常專業。譬如：此惡意程式會休眠超過 2 個星期，用來躲避偵測。此為常見專業手法之一。

二、 從不同案件回報及透過 SolarWinds Orion IT 所被感染的感染者至少約有 18,000 名客戶。若攻擊組織要手動對這些客戶進行進一步完整的攻擊，從攻擊者所需要的資源要對這 18,000 用戶同時進行下一階段的攻擊應該不太可能，所以應該會對目標對象進行優先順序的管理。所以如果這 18,000 誰收到更多的惡意程式或是其他持續性的特徵...等，都可用來辨識出那些用戶是被標識為更高優先攻擊對象的條件。

三、 另從初步的分析，發現惡意程式會連上 C2 使用加密過的 DNS CNAME 來查詢，如果該用戶端的電腦資料為攻擊者有興趣的對像目標時，會回傳 level2 的 CNAME 主機。透過 Fireeyes 及 John Bambenek 的資訊。卡巴斯基從 1722 DNS 中找出 1026 目標名稱及 964 UID。關於解碼的工具已共享至 (https://github.com/2igosha/sunburst_dga) 方便找出其他攻擊者有興趣的攻擊目標方式。

常見問題：

1、 誰發起的攻擊，是跟俄羅斯駭客組織 APT29/Dukes 有關聯嗎？

就現在知道的相關訊息及分析過程中的資訊，還沒有任何與此組織有關聯的情報。這起攻擊事件的來源組織，現在依最早協助調查的人員命名為”DarkHalo”及依 Fireeyes 命名為”UNC2452”，但實際還是為”Unknown actor”。只從媒體上的轉述，看不出有 TTP 與 APT29/Dukes 有所關聯。

2、 用戶也在使用 Orion IT。是否就是攻擊目標對像。

建議立即掃描檢查您的環境，是否有更新為最新修正後的版本，已確保沒有使用到是被感染後的 Solarwinds 版本(https://www.solarwinds.com/securityadvisory)。同時可以確認您的網路流量中是否有連線至已知的 IoC 位置 IP。(https://github.com/fireeye/sunburst_countermeasures)。注意，即使您下載了含有木馬被感染的版本，但不代表您就是被選中的攻擊目標。

3、 這只是間諜活動或是破壞活動，會類似勒索病毒事件？

雖然大部份新聞及用戶都只在意被攻擊破壞的事件，譬如：勒索病毒...等，但此事件有的資訊來看來主要目的還是間諜活動為主。該攻擊組織表現出對 Office365、Azure、Exchange、Poweshell 都有非常深入的研究，並創造不同的方式來進行監視及提取受害者中的相關系統資訊。

4、 知道有多少受害者嗎？

透過 John Bambenek 發現的 DNS 資訊。比對後超過 100K 的卡巴斯基使用者有下載含有感染樣本的程序。實際的受害者人數應該更多。注意：此為 APT 攻擊階段一的事件，有下載該樣本，不代表就是被標註為有興趣的會進一步進行攻擊的對象目標。

5、 影響最嚴重的國家為？

我們觀察到有超過 17 個國家有下載被感染的 Orion IT 套件。但實際的數量還需要參考 SolarWinds 提供的資料。

6、 為何稱為這個為攻擊事件，即時這只是初步階段？

在技術上而言，我們統稱為”供應鏈攻擊(Supply Chain Attack)”，比較好辨識。若在每一個階段中提供一種不同的名稱，也不方便辨識攻擊事件的嚴重性。譬如：供應鏈曝露利用?

7、 超過 18,000 個第一階段的受害者，有多少是真正被感興趣的目標對象？

這個很難去評估計算。在缺少可視性資料及攻擊者特別小心預防被追蹤的條件下。從被公開的 CNAME 中，我們發現了二個可能的對象。一是 US 政治機關、另一是大型電信公司。這些目標被使用了專用的 C2 回應及有進一步的攻擊利用動作。

8、 為什麼不能在第一時間就抓到攻擊者？

這是非常好的問題。在這個案例，有二個技術導致攻擊者非常安靜。第一：此惡意程式處於休眠期長達二個星期以上。第二：此惡意程式注入攻擊是利用.Net 注入模組，在很有限制的檔案大小變更小達成惡意程式的注入。卡巴斯基在 2019 年發現 2 個可疑模組，大小會從 500k 到 900k，被注入檔案為”SolarWinds.Orion.Core.BusinessLayer.dll”。但今年 2 月起，檔案大小並未有明顯的更改。如果攻擊者使用的是這種方式來規避偵測，那是一件很了不起的技術。

9、 什麼是”Teardrop”

根據 Fireeyes 的說明，此惡意樣本為攻擊者針對受害者電腦提供的未知記憶體的 dropper 程式。用來提供客制化的偵測程式。譬如：”CobaltStrike BEACON”。到現在我們並未收集到任何 Teardrop 攻擊樣本。

10、 為什麼這樣的攻擊可以這麼成功？

可能有多種原因，但綜合來說就是”攻應鏈攻擊”的模式。非常仔細嚴謹的第一階段導入。小心的選擇要攻擊的目標，不使用已知的可疑連線行為或是已知的 TTPs 進行滲透。

註 1:Fireeye 提供的資訊參考位置：
(https://github.com/fireeye/sunburst_countermeasures/blob/main/indicator_release/Indicator_Release_NBIs.csv)

註 2:最先進行調查此事件的研究人員 John Bambene 所提供 IoC 相關資訊位置：
(https://github.com/bambenek/research/blob/main/sunburst/uniq-hostnames.txt)

註 3:卡巴斯基提供解碼 DNS CNAME 的相關工具連結：
(https://github.com/2igosha/sunburst_dga)