【2020/12/16 重要資安事件回應】

華爾街日報/路透社報導：美國國土安全部發布緊急指令，要聯邦機構立即關閉被植入木馬的 SolarWinds 系統

經濟部工業局新興資安產業生態系推動計畫整理

www.acw.org.tw

www.secpaas.org.tw

一、 媒體描述與摘要

（一）國家級駭客透過供應鏈攻擊美國財政部與商務部

路透社與華爾街日報本周日(12/13)引述消息來源報導，美國的財政部與商務部近日遭到駭客攻擊，美國國土安全部所屬的網路安全與基礎設施安全局 CISA 要求所有聯邦機構網站關閉 SolarWinds Orion 這款 IT 監管平臺。SolarWinds 為美國系統/網路/IT 設施管理軟體的業者，全球客戶數達 30 萬家，包括全美五百大企業中的 425 家、前十大電信業者、美國軍方、美國國防部、國務院、NSAS、國安局、郵政服務、司法部，以及美國總統辦公室等。

（二）駭客開採 SolarWinds Orion 漏洞植入後門，已滲透數個月

12 月 14 日 SolarWinds 坦承，從今年 3 月到 6 月間釋出的 SolarWinds Orion Platform 2019.4 HF 5 至 2020.2.1 版本遭到駭客攻擊，目前安裝含漏洞 Orion Platform 版本的客戶數接近 1.8 萬家。儘管尚未確定攻擊來源，但部份參與調查的人士透露，他們相信是源自於俄羅斯所支持的駭客集團，且攻擊手法與 FireEye 被駭事件如出一轍。

（三）FireEye 坦承遭駭客攻擊，造成該公司提供安全測試工具外洩

全球最大安全軟體公司之一 FireEye 12 月 8 日公布，近日遭到疑似國家支持的駭客攻擊，造成該公司提供安全測試的紅隊工具外洩。該公司表示，他們已於 GitHub 提供相關的入侵指標（IoC）、Snort 與 Yara 特徵碼等資訊，並強調他們提供的工具都是利用已知漏洞。思科威脅情報單位於 9 日整理了一份指南，列出遭外洩的工具裡，所採用的漏洞 CVE 編號清單與 Snort 特徵編號對照表，以供企業進行因應。

二、新聞內容分析

（一）國際資安大廠陸續中招，企業機構應盤點數位資產，加強更新

SolarWinds 與 FireEye 均為國際知名系統管理與資安防護大廠，此次事件突顯駭客攻擊對供應鏈的深遠影響，因為攻擊者可以通過一個供應鏈進入點擊中多個目標。目前調查顯示應是 SolarWinds 在春季開始的例行更新遭駭客中間人攻擊，被植入惡意軟體，進而利用 SolarWinds 的市場滲透率攻擊相關機構的網路設備與竊取資料。因此建議公司機構盡可能限制供應商的資料數據存取權限，並為第三方供應商可能存在的違規行為做好心理準備或資料備份。

（二）企業對於系統已知漏洞要即時更新解決

針對 FireEye 這次遭外洩的紅隊演練工具，思科列出了當中利用的 16 個漏洞 CVE 編號與 Snort 特徵碼，呼籲企業進行更新防範。其中這些漏洞分佈在 Windows 作業系統、網路安全設備、電子郵件系統、協作平臺、身分驗證管理系統及 IT 管理工具等。而值得留意的是，上述演練工具利用的漏洞，已有不少出現在今年的駭客攻擊行動中。駭客為何會如此食髓之味，不斷利用這種已知漏洞發動攻擊，很可能和許多企業尚未即時修補漏洞有關。例如，今年 4 月資安業者 Rapid7 發現，微軟在 2 月修補的 CVE-2020-0688 漏洞，仍有 35 萬臺 Exchange 伺服器未修補，微軟也再次於 6 月提出警告，表示他們發現有越來越多駭客濫用這項漏洞來攻擊 Exchange 伺服器。同樣在去年已經發佈更新的 CVE-2018-13379 SSL VPN 漏洞，在今年 11 月下旬，仍有駭客在論壇張貼近 5 萬個未修補漏洞的 Fortinet SSL VPN 設備名單。這也代表著企業面對這種重大漏洞，應該需要採取更為快速的策略，以避免在尚未修補的空窗期成為駭客下手攻擊的對象。

三、 企業因應作為建議

（一） 檢視公司是否有使用 SolarWinds 相關上下游解決方案

檢視企業轄屬主機、伺服器、網通裝置是否使用 SolarWind 相關網路管理、系統管理、資安監管、資料庫管理、應用程式管理與服務託管等服務，包含相關服務模組 (如網路監管服務系統會建置 Microsoft SQL Server 2017 Express Edition (SOLARWINDS_ORION)，於程式移除時不會查找到相關模組)，已確實盤點所使用之 SolarWind 相關解決方案。

已知漏洞影響服務包含應用中心監控器(ACM)、資料庫性能分析器模組(DPAIM)、企業控制台(EOC)、IP 地址管理器(IPAM)、日誌分析器(LA)、網路自動化管理器(NAM)、網路配置管理器(NCM)、網路運營管理器(NOM)、網路性能監管(NPM)、NetFlow 流量分析器(NTA)、服務和應用程式監管(SAM)、服務配置監管(SCM)、存儲資源監管(SRM)、用戶設備跟踪器(UDT)、虛擬化管理器(VMAN)、VoIP 和網路品質管理(VNQM)、Web 效能監管(WPM)等系統。

（二） 若有使用需先進行日誌清查，掌握漏洞是否已被利用，並進行修復排除

根據盤點結果如有使用上述系統模組時，可視影響範圍與部屬設備之重要性判定是否需要資安服務單位協處，若判定為高重要性時可視為資安事件處理，應立即聯繫轄屬廠商以及進行資安事件通報，並視事件影響範圍關閉相關服務，處理原則應先保存設備與系統完整性(包含系統狀態、資料庫、日誌)，若重要性較低可保存相關日誌檔即可，透過後續日誌清查掌握漏洞是否已被利用，並進行修復排除。

（三） 聯絡原廠或代理商進行漏洞修補與更新

目前 SolarWind 原廠已中止含有漏洞版本之軟體下載，並提供 SolarWind Orion Platform 2020.2.1 HF2 之更新版本協助用戶進行更新，相關更新內容除提換含有漏洞模組外，亦增加額外安全防護功能。若無法更新者，SolarWind 原廠亦提供相關緩解措施包含建置防火牆規則以及限制 Orion Platform 對外之網路連線，企業可聯絡原廠或代理商進行漏洞修補與更新，建議後續導入 Secuirty OTA (安全線上更新) 機制，並確認相關資安解決與事件處理流程符合企業災損防禦預期目標，若相關事件處理流程需要調整，則提出後續改善機制擬定，以滾動式調整完備資安事件因應作為。

（四） 訂閱公司重要軟體資產相關弱點情資，持續追蹤管理

目前初步分析結果該 SUNBURST 惡意軟體為針對性攻擊，受感染主機如果非主要攻擊標的，即使連線控制中心亦不會下載攻擊程式，但仍須確實盤點相關軟體安裝，或透過訂閱安全管理工具以持續盤點公司軟體資產之相關弱點情資，於相關重要漏洞遭揭露時第一時間收到相關情資，儘速施行相關災損控制與修補更新作業。