賽門鐵克安全摘要--2021年5月

貝絲・斯塔克波爾
記者

勒索軟體、新的行政命令和太陽風 (Solar Winds)「供應鏈攻擊」的影響

殺氣騰騰的勒索軟體。網路犯罪集團策劃發動了最近對一家美國管道營運商的攻擊，致其關閉了運營並再一次引起對關鍵基礎設施脆弱性的擔憂之後，勒索軟體再次躍上國際舞台。將汽油和航空燃油從德克薩斯州運輸到紐約的殖民管道 (Colonial Pipeline) 表示，它關閉了 5,500 英里的管道，以抑制這次駭客同時也竊取近 100GB 資料的入侵攻擊活動。雖然公司高層表示駭客入侵了其業務系統(IT)，而不是控制實體管道基礎設施的系統(OT)，但基於保險起見，他們還是關閉了網路和管道。攻擊對燃油氣泵產生了直接影響，鑑於關鍵的基礎設施漏洞，行業專家擔心接續的蝴蝶效應。交通部發布了一項緊急聲明，旨在增加石油和天然氣的替代運輸路線。

> 將汽油和航空燃油從德克薩斯州運輸到紐約的 殖民管道(Colonial Pipeline) 表示，它關閉了 5,500 英里的管道，以遏制這次駭客同時也竊取近 100GB 資料的入侵攻擊活動。

美國聯邦調查局證實，這次攻擊的起源是一個名為 DarkSide 的勒索軟體，據信它與俄羅斯網路犯罪集團有關。駭客組織在暗網上發布通知反駁稱，他們正在尋找賺錢的機會，而不是代表外國政府進行攻擊。據彭博社文章的消息來源稱，在此期間，一群私營公司在美國機構的幫助下，中斷了正在進行的攻擊，並幫助殖民管道(Colonial)恢復了一些被盜資料。

政府加大應對力道。由於最近這起事件，讓加密勒索攻擊的威脅推升至國安層級，美國司法部官員就勒索軟體攻擊日益嚴重的威脅發出警告，並成立了一個新的任務小組，致力於根除和應對勒索軟體日益增長的威脅。根據 CNN 獲得的一份備忘錄，2020 年是勒索軟體攻擊有記錄以來最糟糕的一年，包括針對華盛頓警察局、治療 COVID-19 患者的醫院及越來越多的製造業。

拜登政府還推出了一項為期 100 天的計劃，以加強國家電網的網路安全。 該計劃的目標之一是鼓勵發電廠的所有者和運營商加強安全事件檢測、緩解和回應； 部署防護技術以確保工業控制系統 (ICS) 和運營網路 (OT) 內的即時態勢感知； 並加強設施內使用的 IT 網路和基礎設施。拜登政府還發布了一項行政命令 (EO)，為與政府有業務往來的公司制定了一系列新的網路安全要求，以期推動變革和改進，並逐漸擴大到私營企業。

SolarWinds 攻擊活動比我們想像的要大。說到俄羅斯駭客攻擊，看起來由國家支持的俄

羅斯駭客組織 APT29（又名 Fritillary，Cozy Bear）精心策劃的 2020 年 SolarWinds 「供應鏈攻擊」事件，遠比最初預期的更為普遍。 對「供應鏈攻擊」的新分析發現，該活動中使用了 18 個額外的命令和控制 (C&C) 服務器，估計有 18,000 家公司因收到 SolarWinds 惡意更新而允許駭客於系統上植入後門，進而危害受害者網路並存取資料。RiskIQ 的研究人員表示，新發現的服務器代表「攻擊者已知的命令和控制足蹟的規模增加了 56%」，並且可能會導致新的可識別目標。

> 對「供應鏈攻擊」的新分析發現，該活動中使用了 18 個額外的命令和控制 (C&C) 伺服主機，估計有 18,000 家公司因收到 SolarWinds 惡意更新而暴險。

在其他與 SolarWinds 相關的新聞中，據信總部位於中國的 Spiral 進階持續威脅 (APT) 組織是一項長達一年的攻擊幕後黑手，該攻擊在 SolarWinds Orion 服務器上植入了 Supernova 後門，以便進行偵察、域映射(domain mapping)和資料竊取。

在所有這些引人注目的事件之後，美國國土安全部網路安全暨基礎設施安全局(CISA)、聯邦調查局和國家安全局以及英國國家網路安全中心，推出了聯合諮詢告警組織，以因應最近俄羅斯駭客組織採用最新的技術，用作其不斷升級的網路攻擊活動的一部分。該公告引用了一些新策略，例如：利用 Microsoft Exchange 零時差漏洞等等的漏洞，並利用 Silver 開源工具作為不斷發展的俄羅斯劇本的一部分來滲透網路，因此公司更應提高危機意識並加強防禦以妥善應對。

當然也少不了中國。不僅僅是俄羅斯在擴大資訊戰。疑似與中國有關連的駭客利用 Pulse Secure VPN 的漏洞，攻擊了數十個組織，包括政府機構、國防公司和金融機構。Pulse Secure 的零時差漏洞被多個威脅行為者在真實情境中所利用，在目標組織的網路上安裝惡意程式。Mandiant 發布的研究發現了 12 個與 Pulse Secure VPN 漏洞利用相關的惡意軟體家族。該漏洞的修補程式將於本月發布，在此之前，Pulse Secure 已發布緩解措施以遏止攻擊企圖。

即使是高科技巨擘也不能倖免。有報導稱 REvil 勒索軟體集團試圖勒索製造 iPhone、iPad 的蘋果公司「買回」被盜的產品詳細設計圖，以避免在本月初，該公司的大型春季活動之前洩露。 犯罪分子要求蘋果在 5 月 1 日之前支付 5,000 萬美元的門羅幣加密貨幣(Monero cryptocurrency)，以避免洩露其台灣合作夥伴廣達電腦的機密資料。一些文件在網上洩露，但該組織最終從其暗網部落格中刪除了所有提及企圖敲詐勒索事件的內容，蘋果公司沒有發表評論。

銀行被鎖定為待宰肥羊，一點也不奇怪。越來越多的證據證實遠端工作成為常態，導致針對銀行和保險公司的網路攻擊大幅增加。2021 年 COVID 犯罪指數報告發現，近四分之三 (74%) 的銀行和保險公司的犯罪活動有所增加，包括：殭屍網路攻擊的增加 (35%)、勒索軟體 (35%)、網路釣魚 (35%)、行動惡意軟體 (32%) 和 COVID 相關惡意軟體 (30%)。有 29% 的受訪者表示，內部威脅仍然是一個大問題。

歸根結底：似乎組織的安全性較低，客戶所面臨網路犯罪和欺詐的風險就更大。那就該好好加油了，朋友們。

原廠網址：https://symantec-enterprise-blogs.security.com/blogs/feature-stories/symantec-security-summary-may-2021

關於作者

貝絲・斯塔克波爾
記者

貝絲・斯塔克波爾是一位在商業與技術交叉領域擁有 20 多年經驗的資深記者。她為大多數領先的 IT 行業出版物和網站撰寫文章，並為一系列領先的技術提供商製作定制內容。

更多資訊 請造訪我們的網站 http://www.SaveTime.com.tw
(好記：幫您節省時間.的公司.在台灣)

關於保安資訊：

從協助顧客簡單使用賽門鐵克方案開始，到滿足顧客需求更超越顧客期望的價值。

- 保安資訊被業界公認為最專業的賽門鐵克解決方案的專家。
- 保安資訊的團隊自 1995 年起就專注於賽門鐵克資訊安全解決方案的銷售、規劃與整合、技術支援、教育訓練、顧問服務，特別是提供企業 IT 專業人員的技能傳承(Knowledge Transfer)的效益上，以及比原廠更快速的技術支援回應，深獲許多中大型企業與組織的青睞(特別是有 IT Team 的組織)，長期合作的意願與滿意度極高。
- 與許多系統整合或服務公司不同的是，我們不吝惜分享我們的專業技能與經驗給顧客的 IT Team，經由常態性的教育訓練、精簡的快速手冊、標準 SOP 文件的提供，以及基於比原廠更孰悉顧客的使用環境與現況的快速回應的品質，在業界建立扎實的口碑。
- 保安資訊一直專注於賽門鐵克領先業界的資訊系統基礎架構上的安全性與可用性的解決方案。進而累積了許多與基礎架構整合的成功經驗，讓導入 Symantec 解決方方案的成效非常卓越。我們的顧客都能免除Try & Error 的時間浪費及不確定的投入或自行摸索的運作風險。
- 關於我們：

保安資訊有限公司
http://www.savetime.com.tw
0800-381500、0936-285588