賽門鐵克安全摘要--2021年11月

供應鏈攻擊、勒索軟體和政府提出的相關倡議

貝絲・斯塔克波爾
記者

2021 年 11 月 18 日發布｜專題報導

美國政府在主動積極的網路安全策略中，集中火力全面反制。拜登政府採取雙管齊下的方法，認真努力使政府的網路安全機構井然有序，同時採取積極措施打擊正在進行的國內外網路安全攻擊。

在國內，拜登政府推出了一項漏洞修復任務，給予聯邦民事機構六個月的時間來修補 2017 年至 2020 年間發現的網路安全威脅。美國國土安全部網路安全及基礎架構安全署（CISA）的首個指令涵蓋了專家在此期間發現的 200 個已知威脅及 2021 年發現的 90 個額外缺陷。報告稱，目標是迫使機構修復所有潛在威脅，無論是否嚴重，並為私人和公共組織建立可遵循的基本清單。

在國務院，網路安全已被確定為該機構現代化工作的五個支柱之一。國務卿安東尼・布林肯 (Antony Blinken) 加緊努力招聘更多 STEM 員工並提升該部門遠端工作的量能，其目標是建立一個專責於網路空間和數位政策的新局處，將美國外交帶入 21 世紀。邁向目標努力的一部分，該機構計劃增聘 500 個新的職員，並將其 IT 預算增加 50%。

還對不斷加劇的網路攻擊進行反擊。司法部承諾逮捕和採取其他行動，作為打擊勒索軟體和其他網路犯罪的持續努力的一部分。在最近採訪中，司法部副部長麗莎・摩納哥 (Lisa Monaco) 承諾將在「未來幾天和幾週內」逮捕更多人，扣押向駭客支付的贖金，並開展新的執法行動。該部門兌現了這一承諾，在 7 月份對軟體公司 Kaseya 進行 REvil 勒索軟體攻擊中，對烏克蘭的一名嫌犯提出了新的指控，據報導，該公司感染了 1,500 家企業。作為行動的一部分，政府還扣押了大約 600 萬美元的贖金。

此外，司法部宣布了民事網路欺詐倡議，該倡議將追查使用《虛假申報法》隱匿或未將網路安全漏洞通報政府的承包商。

> 司法部承諾逮捕和採取其他行動，作為打擊勒索軟體和其他網路犯罪持續努力的一部分。

勒索軟體再次成為人們關注的焦點。美國政府上個月召開了一次重要的全球勒索軟體峰會，有 30 多個國家參加。為期兩天的線上峰會活動旨在提高全球網路韌性，解決非法加密貨幣使用問題，並提升執法合作和外交努力。雖然俄羅斯和中國沒有被邀請參加這次峰會，但官員們不排除將它們包括在未來的會議中。

最近幾週，一項目標在扭轉勒索軟體組織 REvil（又名 Leafroller、Sodinokibi）局勢的**多國行**

動，對其採用反駭客攻擊並迫使其下線。路透社的一份報告稱，聯邦調查局與網路司令部、特勤局和志同道合的國家一起，對 REvil 和其他網路犯罪集團採取協同一致的反制行動。接近調查的消息人士告訴路透社，該計劃已成功破壞了 REvil 電腦網路基礎設施，並獲得對其部分伺服器的控制權。據報導，REvil 對 5 月美國最大燃油供應業者 Colonial Pipeline 和肉類加工商 JBS 的網路攻擊負責，在 Kaseya 遭受勒索軟體的供應鏈攻擊嚴重破壞後，於 7 月暫時關閉，以避風頭。

Darkside 勒索軟體集團也是美國政府的目標。美國國務院表示，將懸賞 1,000 萬美元，獎勵任何可以識別該集團成員身份的線索，該集團與賽門鐵克追踪的 Coreid 集團有關聯。根據政府發布的新聞稿，任何密謀參與 DarkSide 變種勒索軟體事件的個人在任何國家／地區被逮捕和／或定罪，將可獲得 500 萬美元的獎勵。

秉持保護關鍵基礎設施的精神，FBI、NSA、CISA 和 EPA 就針對供水設施的威脅發布了聯合網路安全諮詢。該公告警告稱，已知和未知的威脅媒介對美國水和廢物系統設施進行“持續的惡意網路活動”，這可能會阻礙提供乾淨飲用水以及廢水處理的能力。

俄羅斯的故伎重施。儘管拜登政府早些時候針對其中一些網路行動進行制裁，但根據微軟和網路安全專家的警告，俄羅斯情報機構 (SVR) 發起了一項滲透數以千計的美國政府、企業和智庫電腦網路的新行動。據報導，這項工作被一位微軟資訊安全部門高層歸類為“大型且持續的”，其目標是儲存在雲端的資料。微軟強調成功入侵的機率很低，但它最近通知了 600 多個組織，他們已成為大約 23,000 次入侵系統的目標。

金融部門的員工請注意：名為 MirrorBlast 網路釣魚詐騙，目的在誘使員工下載能用來當作網路攻擊武器的 Excel 檔案，以進行詐騙和滲透到公司網路。發現該行動的網路安全公司 ET Labs 認為，武器化的 Excel 檔案可以輕鬆繞過惡意軟體檢測系統，因為它伴隨著極其輕量級的嵌入式巨集。

根據美國身份竊盜資源中心 (ITRC) 最新資料外洩露報告顯示，**供應鏈攻擊**正在大幅增加。今年迄今為止，共有 793,000 人受到供應鏈攻擊的影響，比 2020 年一整年還多。根據卡巴斯基最新研究，北韓駭客組織 Lazarus (又名 Appleworm) 最新也加入了軟體供應鏈攻擊的行列。他們聲稱， Lazarus 集團正在使用 DeathNote 木馬集群和 BLINDINGCAN 遠端存取木馬 (RAT) 惡意軟體的最新變種，來構建供應鏈攻擊能力，最近的攻擊專門針對南韓智庫和 IT 資產監控解決方案供應商。

根據 Check Point 的新分析，**總體而言**，自 COVID-19 新冠疫情爆發以來，**全球網路攻擊順勢而起。**Check Points 報告稱，與去年相比，今年每週針對組織的攻擊增加了 40%，而美國的平均增幅甚至更高，達到 53%。研究發現，教育／研究部門遭受的攻擊最多，其次是政府／軍隊，然後是醫療保健行業。VirusTotal 報告說，目前已有 130 多個不同的勒索軟體家族在真實的攻擊活動中亮相。

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