賽門鐵克安全摘要--2021年1月

美國國會大廈、太陽風 (SolarWinds) 和 Babuk Locker

貝絲・斯塔克波爾
記者

煽動叛亂和網路風險。隨著更深入了解 1 月 6 日襲擊國會大廈期間所發生的事情，這次襲擊還打開了一個包含資料安全風險和資料隱私問題的潘多拉的盒子，也涉及從遺失的筆記型電腦到潛在的惡意軟體、其他國安以及情報威脅等問題。

當暴民衝進大樓時，暴民闖入國會辦公室，洗劫了文件，並有少數幾起筆記型電腦被偷的事件，其中包括來自俄勒岡州民主黨參議員傑夫默克利(Jeff Merkley)的筆記型電腦，以及從眾議院議長：南茜・佩洛西(Nancy Pelosi)辦公室偷走的另一部專用於開會簡報的筆記型電腦。

雖然沒有證據顯示同夥中有無技術嫻熟的駭客或間諜，但盜竊確實讓國會的整體安全態勢成為眾所矚目的焦點，並引發了人們對各別議員是否採取足夠的保護措施來保護他們的電腦設備和網路免受直接存取及滲透的擔憂。安全專家表示，操作實體設備可能比網路漏洞攻擊更危險，因為入侵者可以肆意破壞實體設備、不當存取或濫用資料。此外，暴露在議員辦公桌上的文件，只要用手機拍照就可以擷取機敏資訊。

當前的安全防護應對措施。專家認為，該事件必須被視為對真實 IT 資產的破壞，就像是掃描設備、監控網路流量以及採取監視對策以確保沒有被植入竊聽設備等措施。這也是參議院幾年前通過的規則要求所有新設備一律嚴格要求加密的效益彰顯。此外，立法機構的汰舊換新週期為兩到三年--這表示個人電腦的資料安全保護水準相對強固。

在其他與政府相關的網路安全新聞中，上個月披露正在進行的太陽風攻擊活動(SolarWinds)影響仍在持續。大規模、持續的入侵活動據稱是由俄羅斯駭客所發動，被鎖定的目標包含政府機構、私營公司和基礎設施實體，現在被認為包含許多未知的戰略--不僅僅是對 SolarWinds Orion 基礎設施監控和管理平台。

美國網路安全暨基礎設施安全局(CISA)發出警報警告稱，一些駭客攻擊的受害者在未使用 SolarWinds 平台的情況下也遭到入侵。警報顯示，駭客使用了「前所未見的策略、技術和程序」，正在進行的網路攻擊活動早在 2019 年 3 月就開始了--這是其廣泛影響的先兆。

駭客們轉而採用一種很少使用的技術來隱藏他們的命令和控制 (C&C) 連線--賽門鐵克威脅獵手團隊的一篇部落格文章中探討了這種策略。根據該篇文章，用於對 SolarWinds Orion 軟體進行木馬化的惡意軟體採用動態網域產生演算法(DGA，Domain Generation Algorithm)來混淆視聽以用於 C&C 目的。該 DGA 不是隨機生成字符，而是將訊息編碼到構成生成域名的文本中，這有助於它採取鴨子划水策略，不易被發現。一份獨立的報告認為，名為 Sunspot 的惡意軟體部署在 SolarWinds 構建環境中，並用於將 Sunburst 後門注入 Orion 軟體。

> 美國網路安全暨基礎設施安全局(CISA)發出警報警告稱，一些駭客攻擊的受害者在未使用 SolarWinds 平台的情況下也遭到入侵。

新的焦點。國務院的一個新辦公室，即網路空間安全和新興技術局 (CSET)，最近被批准處理網路安全和新興技術，包括努力防止與敵對國家的網路衝突。即將上任的拜登政府還宣布了由 Anne Neuberger擔任網路和新興技術國家安全首席顧問的計畫，她近期一直負責監督一個負責防止對敏感政府和軍事工業網路的數位威脅的組織。

追根究柢，明察秋毫。SolarWinds 的網路安全軟體處於國家安全漏洞的中心，正在採取持續措施減輕損失。該公司最近聘請了美國網路安全暨和基礎設施安全局 (CISA) 前任局長克里斯托弗・克雷布斯 (Christopher Krebs) 就此次入侵事件進行諮詢，並調查駭客如何使用惡意代碼侵入其 Orion 軟體。被川普政府解僱的克雷布斯與 Facebook 前首席安全官亞歷克斯・斯塔莫斯 (Alex Stamos) 共同創辦了一家網路安全諮詢公司。

買家提高警覺。PayPal 用戶應該提防簡訊(SMS) 網路釣魚（稱為 smishing）活動，該活動試圖誘騙人們交出帳戶憑證和其他敏感的個人資訊。簡訊內容聲稱收件人的 PayPal 帳戶由於可疑活動而受到「限制」，並要求收件人透過點擊鏈接來驗證其帳戶。如果他們上鉤，該鏈接會提供一個虛假的 PayPal 登錄畫面，將輸入的資訊（如：出生資料、銀行詳細訊息等）發送給攻擊者。Paypal 建議任何懷疑遭受攻擊的人，立即登入該網站並更改其密碼。

關於駭客組織：Babuk Locker？ 2021 年第一個新的鎖定企業組織為目標的勒索軟體，是由安全研究員 Chuong Dong 所發現的Babuk Locker。該勒索軟體以人為的操作方式發動攻擊，贖金要求以比特幣支付，從數萬美元不等。已經回報的受害者包括升降暨手扶電梯廠商、醫學檢測產品等各行各業公司。針對每個受害者進行不同的客製化攻擊，加密後會生成不同且極複雜的附檔名、勒索贖金通知和加密的 Tor 網頁鏈接(URL)。發現者說該編碼不是很先進，但 Babuk Locker 包括了安全加密，防止受害者可由免費的工具來復原他們的檔案。

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。

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

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