賽門鐵克安全摘要--2021年3月

太陽風 (SolarWinds)、阿貝耳 (Accellion) 漏洞和學校

貝絲・斯塔克波爾
記者

拜登政府對抗國家級網路攻擊。在拜登政府上任的頭幾個月裡，兩起備受矚目的國家級網路攻擊的衝擊，迴盪在各行各業和政府間，這似乎很明顯，網路安全已成為拜登政府執政的首要任務。

去年 12 月，俄羅斯駭客入侵了太陽風(SolarWinds) Orion 基礎設施監控和管理平台，利用這些公司的構建系統，將惡意更新推送到該公司的大約 18,000 名企業和政府客戶。後來，很明顯，中國還針對 SolarWinds 客戶進行了一項完全獨立的開採行動。

如果這還不足以敲響警鐘，在微軟報告其企業級電子郵件與行事曆應用系統伺服器Exchange Server，被為中國政府工作的駭客組織破壞後，美國官員本月發布了緊急警告。Microsoft 檢測到多個用於存取本地 Exchange 伺服器和電子郵件帳戶的零時差漏洞，可用於安裝其他惡意軟體以發動進一步的攻擊。

微軟威脅情報中心 (MSTIC) 將 HAFNIUM 列為攻擊對象，該組織被評估為在中國境外運營的國家贊助商，主要針對美國各行各業的實體，從高等教育到國防承包商和傳染病研究人員。報導稱，僅在美國，該漏洞就影響了至少 30,000 家公家和私營單位，儘管美國官員表示，沒有跡象表明聯邦機構或主要國防承包商受到影響。

> 在拜登政府上任的頭幾個月裡，兩起備受矚目的國家級網路攻擊的衝擊，迴盪在各行各業和政府間，這似乎很明顯，網路安全已成為拜登政府執政的首要任務。

網路安全暨基礎設施安全局(CISA)發布了一項罕見的緊急指令，要求所有政府網路升級到最新的 Exchange 軟體更新以抵禦駭客。在 3 月 3日更新的一篇部落格文章中，這家軟體巨擘表示，它繼續看到多個參與者利用未安裝修補程式的系統來攻擊具有本地 Exchange 服務器的組織。根據 Krebs on Security 報告，向美國國家安全顧問通報情況的兩名未透露姓名的網路安全專家認為，這次攻擊奪取了對全球「數十萬」Microsoft Exchange 服務器的控制權--每個系統代表一個依賴 Microsoft Exchange 獲取電子郵件的組織。

《紐約時報》的一篇報導稱，拜登政府已經在準備通過一系列制裁以及俄羅斯網路的進行一系列隱蔽的反擊行動來應對 SolarWinds 的攻擊，這對俄羅斯總統普丁(Vladimir Putin)及其情報和軍事機構來說是顯而易見的，但不展示給更廣泛的世界。在中國 Microsoft Exchange 攻擊之後，「整個政府的反應」已經提升並委託給由拜登政府任命的全新專責職位-網路和新興技術副國家安全顧問的紐伯格(Anne Neuberger)。

漏洞回報獎勵。一位獨立安全研究人員因發現一個漏洞而獲得了 50,000 美元的漏洞回報獎金，該漏洞可以讓任何人在用戶不知情或未經用戶同意的情況下接管任何 Microsoft 帳戶。Laxman Muthiyah 發現了微軟帳戶恢復過程中的一個缺陷，該漏洞使他能夠在重置密碼之前對發送到用戶電子郵件地址或手機的七位數安全代碼進行暴力破解，以恢復對其帳戶的存取權限。儘管微軟實施了速率限制、加密和其他檢查來防止此類暴力攻擊，但 Muthiyah 能夠「自動化整個過程，從加密代碼到發送多個並發請求」。

Muthiyah 向微軟報告了這個錯誤，隨後微軟並在去年 11 月發布了一個修補程式。他於 2 月 9 日通過 Hacker One 漏洞回報獎勵平台獲得了獎金。

受 Accellion 漏洞影響的公司數量繼續增加。Accellion 是一家為 3,000 多個客戶提供檔案傳輸解決方案的資訊服務商，它證實犯罪攻擊者 UNC3546 已利用其軟體中的多個漏洞安裝惡意軟體。當該漏洞於 12 月首次被發現時，多家媒體將此次攻擊與一個名為 Clop 的勒索軟體集團以及另一個名為 FIN11 的駭客組織聯繫起來。

最初，一家大型連鎖商店回報稱，其部分藥房服務客戶的個人資料可能已被盜，包括社會安全號碼和一些病歷。在那份報告之後，其他公司證實了類似的攻擊，包括著名的全球知名律師事務所--眾達(Jones Day)、一所大學和紐西蘭的銀行等。

> 據稱，Clop 勒索軟體集團的洩密網站上張貼了員工的社會安全號碼和家庭住址，目的是勒索銀行付款。

現在，美國第二大儲蓄銀行表示已受到影響並已開始通知客戶。據稱，Clop 勒索軟體集團的洩密網站上張貼了員工的社會安全號碼和家庭住址，目的是勒索銀行付款。

此外，另一家網路安全公司也被最新一波攻擊所席捲，據報導其檔案被洩露到 Clop 勒索軟體站點。洩露網站上發布的資料包括發票、採購訂單、稅務文件和掃描報告。目前尚不清楚 Clop 是否在洩露數據之前向該公司發送了贖金票據，但其他受害者過去曾收到過這些票據。

校舍也遭駭。不僅僅是企業正在經歷網路犯罪的增加--一項對美國 K-12 學校網路安全狀況的新分析發現，去年發生的事件數量創歷史新高。

在 K-12 網路安全領導研討會上發布的新研究記錄了過去一年公開揭露的 408 起學校事件，包括學生和教職員工資料外洩、勒索軟體爆發、網路釣魚和社交工程。該報告發現，「學區對 COVID-19 大流行的反應還揭示了 K-12 教育技術生態系統的韌性和安全性方面存在巨大落差和致命故障。」 學校網路事件的激增被歸咎於學校關閉、數百萬美元納稅人的錢被盜以及與身份盜用和欺詐相關的學生資料外洩。

原廠網址：https://symantec-enterprise-blogs.security.com/blogs/feature-stories/symantec-security-summary-march-2021
本文件由保安資訊有限公司專業細心整理後提供。如有遺誤、更新或異動均以上Symantec原廠公告為準，請知悉。2021/08

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