賽門鐵克安全摘要--2021年8月

LockBit、BlackMatter 以及對抗網路威脅的重要進展

貝絲・斯塔克波爾
記者

網路安全等級不及格。在美國國會參議院國土安全委員會發布的一份政府報告發現關鍵的聯邦機構仍然缺乏基本的網路安全防護之後，美國政府本月再收到了一個重大警鐘。該報告於 8 月 3 日通過兩黨國會調查發布，稱國家、教育、農業、衛生和公共服務部門等關鍵機構沒有建立有效的網路安全計劃，也沒有充分遵守聯邦資訊安全標準。**結果：此一缺失已造成國家安全和敏感的個人資訊，輕易遭受日益老練的駭客竊取和破壞。**

這份題為「聯邦網路安全：美國的數據仍然處於危險之中」的報告的主要調查結果是，七個機構未能遵守奧巴馬總統於 2014 年簽署成為法律的《聯邦資訊安全現代化法案》。這些機構因未達到聯邦規定的標準而獲得平均 C 級。在眾多違規行為中，國務院在員工離職後，在其機密和非機密網路上留下了數千個帳戶以及教育部門，在那裡稽核人員能夠洩露數百個包含敏感的、個人可識別資訊的檔案。

> 在參議院國土安全委員會發布的一份政府報告，發現關鍵的聯邦機構仍然缺乏基本的網路安全防護之後，美國政府本月收到了一個敲醒「**國家面臨的核心安全挑戰**」的重大警鐘。

總共有六個機構未能安裝用於修補潛在漏洞的安全修補和其他控制措施，而少數其他機構仍然依賴供應商已經公示不再支援及更新的舊版作業系統及應用程式。參議院報告得出結論，政府需要更新聯邦機構的旗艦網路安全計劃 EINSTEIN。

「從 SolarWinds 到最近針對關鍵基礎設施的勒索軟體攻擊，很明顯，網路攻擊將繼續發生，我們自己的聯邦機構沒有盡一切可能保護美國的數據是不可接受的」， 也是委員會主席之一的共和黨參議員 (俄亥俄州)羅伯波特曼說，同時在一份準備好的聲明中發布了報告。在一個日益被網路安全風險定義的時代，對於政府來說絕對不是一份令人滿意的成績單。

隨著新威脅的出現，勒索軟體繼續肆虐。以 BlackMatter 為例，這是一個新的勒索軟體集團，藉由從惡名昭彰的 REvil 和 DarkSide 組織的錯誤中吸取教訓，制定了自己的路線。在接受 Recorded Future 採訪時，BlackMatter 表示它有興趣瞄準超過 1 億美元的大公司，但聲稱將會排除某些特定領域的公司或組織，包括醫療保健、政府和關鍵基礎設施等。

在採訪中，BlackMatter 開發人員否認了先前有關該新組織的背後是 Darkside 勒索軟體的報導，該軟體自從成為殖民管道公司(Colonial Pipeline) 等備受矚目的攻擊事件的核心後就消失了。勒索軟體專家將兩者聯繫起來，因為他們被認為使用相同的加密程序。BlackMatter 則聲稱是利用了 REvil、Darkside 和 LockBit 的部分劇本。

說到 LockBit，與該組織相關的勒索軟體攻擊活動如雨後春筍般激增--有人說，這表示他

們正試圖填補 Sodinokibi 勒索軟體留下的空缺。賽門鐵克威脅獵手團隊的一項調查發現，至少有一個前 Sodinokibi 相關的「攻擊發動分紅組織」，現在使用 LockBit--攻擊始於一個名為 mimi.exe 的檔案，該檔案是一個安裝程式，可以投放許多密碼傾印工具。威脅獵手團隊還在與 LockBit 攻擊相關的許多主機上發現了名為 Neshta 的惡意軟體。瀏覽賽門鐵克威脅獵手團隊的部落格，可以獲得與此議題更深入資訊。

> 另一方面，1 月份的 SolarWinds 供應鏈攻擊仍在繼續。

徵人廣告。LockBit 勒索軟體集團在攻擊方面養精蓄銳，蓄勢待發的另一個徵兆是：該組織現在正試圖招募企業內部人員來幫助入侵和加密該企業的網路，向成功入侵的人提供數百萬美元的報酬。今年 6 月，這個新組織更名為 LockBit 2.0 勒索軟體即服務，正試圖跳過中間人，直接招募擁有開啟該企業網路「鑰匙」的內部人員。LockBit 2.0 表示他們專門尋找 RDP、VPN 和企業電子郵件憑證，以利他們可以獲得網路存取權限，做進一步的網路攻擊。

另一方面，在 1 月份登上新聞頭條的 SolarWinds 供應鏈攻擊仍在繼續。負責的俄羅斯駭客已經轉向美國司法部。根據政府官方聲明，2020 年 5 月 7 日至 12 月 27 日期間，27 個美國檢察官辦公室員工的 Microsoft Office 365 電子郵件帳戶遭到入侵。

在一系列壞消息中，網路威脅戰爭取得了一些關鍵進展。最有希望的一個是新的「聯合網路防禦合作組織」（JCDC），它由美國網路安全暨基礎設施安全局（CISA），建立政府和私營部門的網絡安全專家的合作夥伴關係，以制定和實施更好的網路安全計劃。博通的軟體部門(Broadcom Software；賽門鐵克現為博通企業安全部門)也將於 8 月 23 日星期一參加 JCDC 的第一次會議。該合作夥伴關係目標在追求：

- 設計和實施全面的、全國性的網路防禦計劃，以應對風險並促進協調行動
- 分享洞見以形成對網路防禦的挑戰及機會的共同理解
- 實施協調的防禦性網路行動，以防止和減少網路入侵的影響
- 支持聯合演習，以改善網路防禦行動

拜登政府還採取措施改善關鍵基礎設施控制系統的網路安全--這是在備受矚目的殖民管道攻擊後日益受到關注的問題，對國家傷害也被視為等同「真槍實彈的戰爭」。該行政命令要求採取諸如加密和雙因素身份驗證等自願措施，作為推動公司制定網路安全績效目標的一部分。

還提出了將勒索軟體定位為恐怖主義的立法提案。參議員馬可・魯比歐(共和黨--佛羅里達)和黛安・范士丹(民主黨--加利福尼亞)，提出的制裁和阻止勒索軟體法案將制裁支持網路攻擊者的國家，該法案還呼籲制定加密貨幣交易法規。

隨機新聞。對於那些對漏洞回報獎勵計畫（Bug Bounty Program）感興趣的朋友，這裡有一個機會。Twitter 推出了由其機器學習、道德、透明度和問責制 (META) 團隊贊助的第一個人工智慧項目，挑戰人們在其圖像裁剪算法中發現偏見，以及政治意識型態內容建議等機器學習演算法，對用戶帶來的影響，並將這些影響回饋到系統中，避免演算法對用戶造成傷害，並為獲勝者提供現金---一等獎：3,500 美元。

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