賽門鐵克安全摘要--2021年2月

國家級攻擊、工業物聯網和更多勒索軟體

貝絲・斯塔克波爾
記者

國家級攻擊再升級。隨著新年的開始，與國家層級有關的網路攻擊的消息也隨之而來。根據一份聯合國機密報告，北韓駭客被指控在 2019 年至 2020 年 11 月期間竊取了價值 3.164 億美元的虛擬資產。美國有線電視新聞網(CNN)獲得這份報告指責朝鮮政權「針對金融機構和虛擬貨幣交易所開展行動」，為其核計劃和導彈計劃提供資金，並維持該國陷入困境的經濟。

北韓駭客與加密貨幣交易所之間的聯繫已經確立：2019 年的一份報告稱，這個受到嚴厲制裁的民族國家，在過去五年中通過滲透加密貨幣交易所籌集了約 20 億美元。正如博通的企業安全部門--賽門鐵克研究指出的那樣，最近比特幣價格的上漲意味著，如果這種特定的加密貨幣是搶劫的一部分，那麼今天的非法賞金比被盜時的價值要高得多。

另一個國家級駭客在正在進行的 SolarWinds 網路安全傳奇中首次亮相。據稱，俄羅斯是去年 12 月大規模供應鏈駭客攻擊的幕後黑手，該駭客攻擊目標是美國商務部、財政部、國土安全部和能源部門及私營公司等備受矚目的目標。但現在路透社報導說，中國駭客也加入了這場遊戲，選擇了不同的攻擊路線。在俄羅斯支持的駭客透過在 Orion 網路監控工具的軟體更新中植入惡意程式精心策劃了此次非法攻擊活動，影響了多達18,000名客戶。然而，疑似中國駭客利用 SolarWinds 平台中的另一個軟體缺陷入侵其他政府機構，可能會洩露數千名政府僱員的資料。

隨著 SolarWinds 攻擊的影響仍在繼續，由於擔心其係統受到損害，美國法院系統已放棄在敏感案件中以電子方式提交法律文件。聯邦法院發布了一項命令，規定任何「包含外國政府情報部門可能感興趣的資訊」的文件現在都必須重新列印出來並以實物形式交付。

> 據報導，所謂「家貓」組織在過去四年中一直在對大約1,200人的目標名單進行廣泛監視，使用名為 Furball 的行動惡意軟體進行間諜活動。

根據 Check Point 和 SafeBreach Labs 的研究，**除了這些引人注目的例子外，伊朗國家駭客組織**也受備受關注，被指控對全球伊朗公民進行間諜活動。據報導，所謂的「家貓」組織在過去四年中一直在對大約 1,200 人的目標名單進行廣泛監視，使用名為 Furball 的行動惡意軟體進行間諜活動。然後，惡意軟體會使用網路釣魚、伊朗網站、Telegram 頻道和惡意 簡訊訊息進行傳播，並且可以擷取通話記錄、記錄通信，甚至竊取檔案。同一個研究小組強調了另一個與伊朗有關的組織，稱為 Infy，該組織參與了類似的間諜活動，但目標要少得多。

為了應對加劇的攻擊活動，拜登政府正在採取改善網路安全的措施。拜登總統最近在國務

院的一次國家安全演講中表示，他們「提升了我們政府內部網路安全問題的地位」，並「正在啟動一項緊急倡議，以提高我們在網路空間的量能、應變速度和韌性。」作為該計劃的一部分，政府聘請了國家安全局 (NSA) 官員 Anne Neuberger 擔任網路和新興技術副國家安全顧問的新職位。此前，紐伯格領導 NSA 網路安全防禦行動，並支持負責保護 2018 年中期選舉免受俄羅斯干擾的機構小組。

工業物聯網網路安全噩夢。隨著越來越多的設備和關鍵的民用基礎設施連接到網際網路，2 月初的事件代表了未來網路安全災難的趨勢。一名不知名的駭客經紀人闖入佛羅里達州奧茲馬的一家水處理廠，並接管了控制系統，將水中鹼液的含量提高到危險水平。幸運的是，一位機警的工廠操作員即時看到了異常狀況，馬上關閉了滲透並進行系統補救，及時化解了可能造成大眾傷亡的與基礎設施癱瘓的危機。

入侵事件發生的時間也令人震驚--它發生在周五的超級盃週末，在坦帕(Tampa)附近舉行。該工廠目前已停用其係統的遠端存取功能，並正在與 FBI 和特勤局合作進行調查。

網路犯罪分子大賺不義之財。所有這些勒索軟體活動似乎都有所斬獲。儘管網路犯罪活動整體數量下降，但 2020 年向勒索軟體集團支付的款項激增。根據區塊鏈分析公司 Chainalysis 的研究，使用加密貨幣的勒索軟體支付在 2020 年飆升了 311%，總額達到 3.5 億美元。研究發現，利潤似乎集中在攻擊者的核心集團中--從勒索軟體攻擊中收集到的資金中有 80% 可追溯到不到 200 個加密貨幣錢包。

從好的方面來說，Chainalysis 發現數位貨幣交易與網路犯罪之間存在的占比有下降的跡象。雖然勒索軟體已成為一個更大的問題，但加密貨幣仍在繼續擴大其市場。雖然透過加密貨幣進行的勒索軟體支付暴增，但總體而言，網路犯罪導致的數位貨幣交易量減少了。使用加密貨幣的網路犯罪交易下降了一半以上，達到 100 億美元，但由於整體加密貨幣交易量增加，網路犯罪的占比從 2019 年的超過 2% 下降到 2020 年僅佔所有加密貨幣交易的 0.34% 。

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-february-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

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