賽門鐵克安全摘要--2021年9月

勒索軟體、加密和區塊鏈的最新狀態

貝絲・斯塔克波爾
記者

2021 年 9 月27 日發布｜專題報導

勒索軟體繼續在網路安全頭條新聞中**獨佔鰲頭**，由於不斷出現新的變種，有跡象顯示駭客正在精進其戰術並越來越有意識地選擇目標。

FBI 首次發布警報對名為 OnePercent 的勒索軟體分紅附屬運營商發出警告，該運營商自 2020 年 11 月以來，一直使用一套一致的駭客攻擊戰術流程(TTP；工具、策略和程序)來瞄準美國組織。該網路犯罪集團使用惡意釣魚電子郵件附件來散布 IcedID 銀行木馬感染媒介，然後在受感染的端點上使用原用於滲透測試的工具--Cobalt Strike，在受害者的網路中橫向移動以竊取敏感資料，最後一步是部署勒索軟體籌載，並附上一則鏈接到該集團 .Onion 存在暗網上的網站說明。 FBI 警報將 OnePercent Group 與惡名昭彰的 REvil (Sodinokibi) 勒索軟體集團聯繫起來，該犯罪集團是最近許多備受矚目的攻擊的幕後黑手。根據報導，今年初夏，在多起網路攻擊引起了全世界的撻伐之後，包括拜登總統對與俄羅斯總理普丁的強硬談話，REvil 銷聲匿跡了一陣子，但最近有跡象顯示他又捲土重來了。

作為加強勒索軟體監管的一部分，聯邦調查局還針對農業食品行業所面臨的新攻擊提出示警。該示警稱，對智能科技、工業控制系統 (ICS) 和依賴網際網路連線的自動化系統的依賴性增加，使該行業成為更具吸引力的目標。該示警稱，可能的後果是經濟損失、食品價格飆升以及食品供應鏈中斷。該示警鼓勵該行業的公司採取措施保護其 IT 網路，包括強化 RDP 端點的安全性和修補面向網際網路的設備以防止漏洞。

勒索軟體感染也蔓延到大學和城鎮。據《華盛頓郵報》報導，近年來，近 400 個城鎮成為勒索軟體攻擊的受害者，導致阻礙了緊急救援、核心系統癱瘓、報稅延宕等。就在本月稍早學生返校時，霍華德大學(HBCU) 遭受了勒索軟體攻擊。HBCU 網路遭到攻擊後，被迫取消所有線上和混合教學課程。

勒索軟體希望名單。威脅情報公司 KILA 分析了勒索軟體參與者尋找合作者的地下論壇帖文，並為偏好的受害者提出了各種希望名單。勒索軟體犯罪集團主要針對美國、加拿大、歐洲和澳洲收入超過 1 億美元的組織。醫療保健和教育部門對許多攻擊者來說有所顧忌，而其他人則避開政府和非營利組織。研究人員得出的結論是，避開這些部門與利他主義或社會責任無關，更有可能是為了避免爭議和避免執法部門的關注。

加密貨幣這個炙手可熱的領域看起來像是網路安全攻擊的下一個重點。處理跨區塊鏈平台加密貨幣交易的中國公司-- Poly Network 透露，其平台上有超過 6.11 億美元的加密貨幣被盜。Poly Network 將此次網路攻擊歸咎於駭客利用「合同請求」漏洞--這意味著在區塊鏈上自動執行交易的兩個程式同時運行，駭客發現了漏洞，並建議其客戶（包括全球最大加密貨幣交易所幣

安 (Binance) 和 Coinbase Pro 等加密貨幣交易所）停止來自特定錢包地址的交易，以避開竊賊。幾天後，威脅行為者返還了價值近 2.6 億美元的資金被盜的加密貨幣。所謂的小偷聲稱搶劫不是為了偷錢，而是要經由暴露他們的弱點來給 Poly Networks 一個教訓。更有可能的轉變，應該是由於區塊鏈安全公司--Slowmist 聲稱其擁有攻擊者身份的證據。

網路犯罪分子開發了一種區塊鏈分析工具來協助洗錢。根據 Elliptic 的說法，Antilysis 區塊鏈分析工具已在暗網上啟動--其任務是檢查比特幣地址以查找與犯罪活動的鏈接。根據 Elliptic 的聯合創始人兼首席執行官的說法，這意味著犯罪分子可以「測試他們的資金是否會被受監管的交易所認定為犯罪所得」，這是隱藏他們活動的關鍵技術。

網路安全百戰百勝的傑出律師。根據美國司法部的新聞稿，為持續擴大打擊網路犯罪和不斷升級的威脅，司法部 (DOJ) 宣布了一項新的獎助計畫，其任務是培訓新一代檢察官和律師了解網路安全問題。選定的律師將通過多個部門參與為期三年的輪調，並專責「起訴國家支持的網路威脅、跨國犯罪集團、勒索軟體攻擊以及使用加密貨幣洗錢以幫網路犯罪集團提供資金和圖利自己」的案件。

如果本月的網路威脅活動有任何風吹草動，那麼他們將有得忙了。

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-september-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。2021/9

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