賽門鐵克安全摘要--2021年10月

BlackMatter、Conti 和 Harvester 集團

貝絲・斯塔克波爾
記者

2021 年 10 月 27 日發布｜專題報導

勒索軟體仍然是一個持續的企業禍害。賽門鐵克威脅獵手團隊的一份新研究報告發現，在過去 18 個月裡，有針對性的勒索軟體活動呈上升趨勢，這是由於新參與者的激增和勒索軟體即服務 (RaaS) 市場的日益複雜化。根據研究，在該時間段內，組織報告的已確認攻擊數量增加了 83%，從 2020 年 1 月的 81 次增加到 2021 年 6 月的 148 次。調查結果顯示，該時期依企業組織分類的報告其攻擊確認件數從 2020 年 1 月的 81 件增加到 2021 年 6 月的 148 件，增加了83%。賽門鐵克研究人員認為，實際攻擊次數可能還要更高，因為有許多針對性攻擊在有效載荷部署之前就被阻止了，因此它們不會被辨識為實際的勒索軟體。

問題變得如此嚴重，引起了白宮的注意。拜登總統宣布，美國將與包括北約盟國和七大工業國夥伴等 30 個國家的代表會面，合作打擊網路犯罪，特別是勒索軟體。如新聞稿中所述，合作夥伴將共同努力改善執法合作，阻止加密貨幣的非法使用，並以外交方式解決這些問題。新聞稿稱：「我們正在建立一個國家聯盟，以倡導和投資可信賴的 5G 技術，並更好地保護我們的供應鏈。」「我們正在充分發揮我們的能力來打擊惡意網路活動，包括量子運算和人工智慧等新興科技的風險和機遇。」

> 拜登總統宣布，美國將與包括北約盟國和七大工業國夥伴等30個國家的代表會面，合作打擊網路犯罪，特別是勒索軟體。

繼續以勒索軟體為主題：聯邦網路安全和基礎設施安全局 (CISA)、聯邦調查局 (FBI) 以及美國國家安全局 (NSA) 發布了關於 BlackMatter 勒索軟體的聯合網路安全公告。自 2021 年 7 月以來，惡意網路攻擊者已使用 BlackMatter 勒索軟體針對多個美國關鍵基礎設施企業，包括美國食品和農業部門組織。Broadcom Software 博通軟體部門 (Symantec) 被聯邦網路安全和基礎設施安全局 (CISA)命為對分析有助益的貢獻者。

Conti 惡意軟體是所有勒索軟體相關新聞的焦點。使用此類勒索軟體的攻擊者正利用一種新戰術，並將目標對準 Veeam 備份解決方案的用戶，以刪除受害者內部網路上的備份。Advanced Intel 進階的情資研究發現，攻擊者正在尋找擁有高權限的 Veeam 用戶並竊取他們的憑證，以便他們可以冒充他們使用 rclone 竊取備份，然後再將其從受害者的網路中刪除。在一份聲明中，Veeam 官方建議用戶維護一個單獨的網域，以便在主網域遭到破壞時運行備份軟體。

Conti 勒索軟體（也稱為 Miner 或 Wizard Spider）的運營商還威脅說，如果公開分享勒索內容或螢幕快照，將洩露受害者資料。原因是：越來越多的媒體報導記錄了贖金談判的細節，這

使得他們的利用變得更加難以實現。

加密貨幣也遭魚池之殃。Coinbase 的簡訊 (SMS) 雙因素身份驗證系統中的一個錯誤，使攻擊者能夠從加密貨幣交易所的 6,000 多個客戶那裡竊取資金。這些漏洞發生在 2021 年 3 月至 2021 年 5 月之間，由於攻擊者取得了與該帳戶關聯的客戶電子郵件地址、密碼和電話號碼的存取權限，使得他們能夠利用雙因素認證機制 (2FA) 的失效而得手。Coinbase 表示將補償在這些交易中丟失資金的用戶，並更新其簡訊 (SMS) 帳號復原 (Account Recovery) 協議以防止發生進一步的事件。

> “ Conti 勒索軟體（也稱為 Miner 或 Wizard Spider）的運營商也威脅說，如果公開分享勒索內容或螢幕快照，將洩露受害者資料。

與此同時，司法部採取措施加強加密貨幣的**安全性**。美國副總檢察長麗莎・摩納哥宣布成立國家加密貨幣執法團隊，該團隊將包括反洗錢和網路安全專家，他們的任務是強化司法部根除這些平台在金融市場被濫用的能力，以遏止網路犯罪分子囂張的行徑。 這項任務並以減少勒索軟體的增加為主旨，勒索軟體通常要求以加密貨幣支付。

「加密貨幣交易所希望成為未來的銀行」，摩納哥在最近的阿斯彭網路峰會上的一次線上演講中說。「我們需要確保人們在使用這些系統時有信心，我們需要準備好根除濫用行為。」

Harvester 團體是勒索軟體領域的新手。一個以前沒沒無聞的參與者，可能背後有國家的支持，正在瞄準南亞的組織，重點是阿富汗，正在以阿富汗為焦點的南亞組織為目標，這似乎是一場使用新工具集的資訊竊取行動。

據博通軟體 (Symantec) 的威脅情報團隊稱，Harvester 組織在其攻擊中使用了自定義惡意軟體和公開可用的工具，攻擊始於 2021 年 6 月，最近一次活動發生在 2021 年 10 月。目標行業包括電信、政府和資訊科技 (IT)。這些工具的功能、自制開發以及目標受害者都顯示出 Harvester 是一個由國家級支持的參與者。

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-october-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