賽門鐵克安全摘要--2021年7月

REvil 駭客組織、勒索軟體和「正義獎勵計畫」

貝絲・斯塔克波爾
記者

網路安全哀鴻遍野。在最新的大規模勒索軟體攻擊可能已經在世界各地造成 800 到 1500 家公司的影響。利用軟體開發商或服務提供商等受信賴的合作夥伴來找到並入侵新的受害者通常被稱為供應鏈攻擊，這在勒索軟體案件中並不常見。供應鏈攻擊始於針對 Kaseya 的供應鏈攻擊，Kaseya 是一家提供給企業 IT 團隊和託管服務供應商（MSPs）的 IT 管理軟體開發商。據報導，攻擊者是俄羅斯的 REvil 的駭客組織，該組織也發動最近其他備受矚目的攻擊，例如：針對肉類加工商 JBS 的攻擊。據我們目前所知，攻擊者利用了 Kaseya 的 VSA 端點管理、防護和網路監控平台中的漏洞。專家將此事件比作 SolarWinds 供應鏈勒索軟體襲擊事件，他將木馬軟體自動化派送並更新到整個公司的電腦系統。該公司督促 VSA 用戶關閉他們的 VSA 伺服器以防止它們受到威脅--這一動作最初影響了至少 36,000 家公司。

正如新趨勢所顯示的那樣，勒索軟體集團通常會在加密受害者的設備之前花時間竊取數據和刪除備份，從而強力迫使受害者支付贖金以確保資料能恢復。在 Kaseya 攻擊中，REvil 集團避開了這些做法，利用 VSA 伺服器中的零時差漏洞來自動化攻擊，而無需存取個別受害者的網路。因此，由於可以從備份中恢復網路，因此可能會有更少的公司感到支付壓力。科技網站 Bleeping Computer 推測，在估計的 1,500 名受害者中，只有兩家公司支付了贖金。

> 正如新趨勢所顯示的那樣，勒索軟體集團通常會在加密受害者的設備之前花時間竊取數據和刪除備份，從而強力迫使受害者支付贖金以確保資料能恢復。

與此同時，在 Kaseya 攻擊事件發生後不到兩週，REvil 集團就突然消聲匿跡了。雖然沒有明確的答案，但研究人員仔細探索了幾種可能的因素。一是克里姆林宮屈服於美國的壓力，迫使該駭客組織關門大吉。另一個是美國官員發起了自己的網路攻擊以進行報復，並使該組織下線。最後，REvil 的運營商也可能只是決定暫時低調。

在此期間，Kaseya 發布了緊急安全更新，以解決 REvil 利用的 VSA 中的關鍵漏洞。該公司還警告客戶有關針對 VSA 客戶的正在進行的網路釣魚活動，垃圾郵件發送者通過該活動利用有關事件更新的新聞發送帶有惡意鏈接和/或附件的電子郵件。

“抓襟見肘、疲於奔命” 毫無疑問勒索軟體今年已經成為主要的國家安全威脅，網路安全產業和網路安全高層正在努力尋找足夠的能力來應對戰線。Cyber Seek 是一個由美國國家標準與技術研究所（NIST）贊助的網路安全職缺供需狀態追蹤系統，報告顯示，儘管有需求且企業網

路安全預算充足，但仍有超過50萬個網路安全工作的職缺。

為解決這一差距而提出的一個想法是創建一個民用網路安全儲備團隊。美國國會的兩黨議員已提出立法，設計類似國民警衛隊的計劃，該計劃將存在於國土安全部和國防部之下，以應對美國政府面臨的日益增長的網路安全威脅。此外，美國國務院推出正義獎勵計畫（RFJ），提供一千萬美元的獎金，鼓勵各界提供攻擊美國關鍵基礎設施惡意網路攻擊的相關資訊，包括攻擊者身分和位址等，也提供 Tor 洋蔥瀏覽器的通報管道，獎金也會以加密貨幣提供。

反擊勒索軟體。今年這種攻擊尤其多，政府和網路安全業界也全力以赴對抗勒索軟體攻擊。美國網路安全和基礎設施安全局 (CISA) 發布了一種新的勒索軟體安全稽核自我評估功能，作為其網路安全評估工具 (CSET) 的一個模組。該工具稱為 RRA，目的在幫助組織發現他們在防禦 IT 或運營技術 (OT) 資產面對的勒索軟體攻擊和從復原方面的能力。

還有一個新的群眾外包專案以追蹤勒索軟體支付的贖金和金流。該網站被稱為 Ransomwhere，讓受害者和安全專業人員上傳贖金記錄和其他相關資訊的副本，以更深入了解攻擊者及其方法。該專案由史丹佛大學學生 Jack Cable 發起，他也是 Krebs Stamos Group 的研究員。

> 隨著勒索軟體今年明顯成為主要的國家安全威脅、網路安全產業和網路安全高層正在努力尋找足夠的能力來應對戰線。

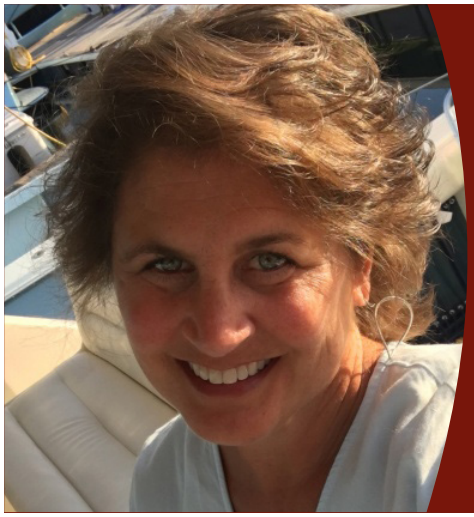
勒索軟體衍生的另一個茶壺風暴：根據國防智庫皇家聯合服務研究所(RUSI)的新研究，網路保險方面一定會發生一些變化。根據 RUSI 研究網路保險和網路安全挑戰的研究論文，這種做法不僅鼓勵網路罪犯，而且對網路保險行業也不可持續，它警告說勒索軟體已經成為一些保險公司的生存威脅。為應對激增的需求，保險公司也在推高成本和承保風險。例如：許多承保公司要求審查公司網路安全實踐的詳細證明，以確保保單的風險。

基礎設施攻擊比想像中更嚴重。最近一連串的網路攻擊也引發了對基礎設施漏洞的擔憂--有充分的證據顯示。本月稍早，伊朗國家鐵路的電腦系統遭到攻擊，導致客運和貨運列車延誤，伊朗的火車運輸系統的服務中斷。

在知名的攻擊活動中，一個遠端程式碼執行(RCE)漏洞已被揭露，它讓駭客更容易控制施耐德電氣 PLC，這些 PLC 廣泛用於工業設備，從製造車間設備到關鍵基礎設施。Armis 研究人員在 Modicon PLC 中發現一個缺陷，該 PLC 廣泛用於製造、自動化應用和能源公用事業。研究人員警告說，該漏洞可用於各種攻擊，從部署勒索軟體到更改機器命令。施耐德電氣正在開發補丁。

北韓駭客組織 Lazarus 瞄準工程師。一個著名的北韓駭客組織 Lazarus 在其最新的網路釣魚活動中瞄準了工程師。據 AT&T Alien Labs 稱，Lazarus(又名Appleworm)正使用虛假的工作機會作為一種手段，誘使工程職位求職者和擔任重要職務的員工點擊文件，然後將惡意軟體安裝到收件人的電腦上。該組織去年在一項名為 Dreamjob 國防承包商的活動中，首次使用了這種策略。

原廠網址:https://symantec-enterprise-blogs.security.com/blogs/feature-stories/symantec-security-summary-july-2021



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