賽門鐵克安全摘要--2021年12月

從全球網路態勢看到網路攻擊增加

貝絲・斯塔克波爾
記者

2021 年 12 月 16 日發布｜專題報導

國家支持的網路安全攻擊似乎是正在增加，**讓原本已令人擔憂的全球局勢更加複雜**。在發現 SolarWinds 供應鏈攻擊一周年之際，Mandiant 的一份報告發現，與俄羅斯有關聯的攻擊者仍在科技業多個組織中練兵。該組織被微軟標識為「Nobelium」，現在正在使用一個名為 Ceeloader 定制下載器，它可以解密 shellcode 有效籌載，以便在受感染設備的記憶體內執行。Mandiant 報告發現：「威脅行為者不斷創新和識別新技術及間諜情報技術，以保持對受害者環境的持續造訪、阻礙安全軟體偵測和混淆其來源。」

舉個例子：法國國家網路安全局 (ANSSI) 警告說，自 2021 年 2 月以來，同樣的攻擊者對法國組織發起多起網路釣魚行動。當攻擊者入侵法國組織轄下的電子郵件帳戶時，他們經常使用它們發送「武器化」的電子郵件給外國機構。

俄羅斯讓位--與伊朗有關連的駭客活動現在正在上升。微軟威脅情報中心 (Microsoft Threat Intelligence Center，MSTIC) 發布一份詳細報告，記錄了六名伊朗威脅行動者的演變，並突顯這些團體日益複雜的攻擊。微軟揭示三個值得注意的趨勢：這些團體越來越多使用勒索軟體來籌募基金或癱瘓他們的目標；他們表現出更有耐心和持續的行為；他們正在對預定目標進行激進的蠻力攻擊。微軟的報告得出結論，伊朗組織已經發展成為更有能力的威脅行動者，能夠進行全方位的攻擊行動，包括勒索軟體和磁碟刪除器、行動惡意軟體、網路釣魚攻擊、密碼潑灑 (Password Spraying)，甚至供應鏈攻擊。

> 微軟向 40 家 IT 公司發送了 1,600 多則通知，提醒他們注意由伊朗 APT 組織策劃的駭客攻擊。微軟表示，2020 年只有 48 則此類通知。

後續行動中，MSTIC 和微軟數位安全部門 (DSU) 報告說，伊朗威脅行動者正在加強對 IT 服務公司的攻擊，以此作為攻擊其客戶網路的一種跳板--即讓人想起 SolarWinds 供應鏈攻擊。合作夥伴評估說，這一系列活動是更廣泛的間諜目標之一部分，目的在損害伊朗政權的利益組織。「這項活動值得注意，因為針對第三方有可能透過利用供應鏈中的信任和存取，來開拓更敏感的組織」微軟表示。就在今年，微軟向 40 家 IT 公司發送了 1,600 多則通知，提醒他們注意由伊朗 APT 組織策劃的駭客攻擊。微軟表示，2020 年只有 48 則此類通知。

伊朗國家支持的活動加劇促使美國、英國和澳大利亞的網路安全機構**發出聯合安全警報**。該警報由美國網路安全和基礎設施安全局 (CISA)、聯邦調查局 (FBI)、澳大利亞網路安全中心 (ACSC) 和英國國家網路安全中心 (NCSC) 編寫。它警告伊朗國家資助的行為者積極利用 Fortinet

和 Microsoft Exchange ProxyShell 漏洞來獲得對易受攻擊系統的初始存取權限，以進行後續活動，包括資料外洩和勒索軟體。

伊朗是另一股操縱選舉的外國勢力。美國司法部最近起訴兩名伊朗公民，因為他們在 2020 年美國總統競選期間，從事「親近並影響」美國選民為目的的網路活動。對伊朗公民提出指控包括入侵美國 11 個州的選民登記網站、入侵一家美國媒體公司，以及向共和黨議員發送民主黨選舉舞弊的偽造影片。

另一方面，據路透社**報導，由以色列 NSO 集團開發的 Pegasus 間諜軟體，已在至少 9 名美國國務院轄下僱員 iPhone 上被發現**。雖然這次資安危害事件幕後的背景尚不清楚，但駭客攻擊發生在過去幾個月，目標是烏干達的官員或正在處理與該國相關的問題。NSO Group 表示它不相信它的工具被使用，但無論如何都計劃進行調查。

儘管國際間和民族國家的網路犯罪節節上升，但資安保險方面卻傳來壞消息。英國保險公司 Lloyd's of London (*倫敦勞合社) 宣布，其保險理賠將不再涵蓋與民族國家相關攻擊相關的費用。其新的「網路戰爭和網路攻擊行動排除條款」將排除與作為戰爭一部分進行的網路行動、特定國家之間的任何報復性攻擊或「對國家運作產生重大不利影響的網路行動」相關損失。根據新條款，該公司還可以拒絕支付民族國家支持的襲擊金融機構、金融市場基礎設施、醫療服務和其他公用事業等民生必要服務的費用。

> 一場被認為是勒索軟體的網路攻擊，已迫使英格蘭北部 300 多家超市暫時關閉並改用現金支付。

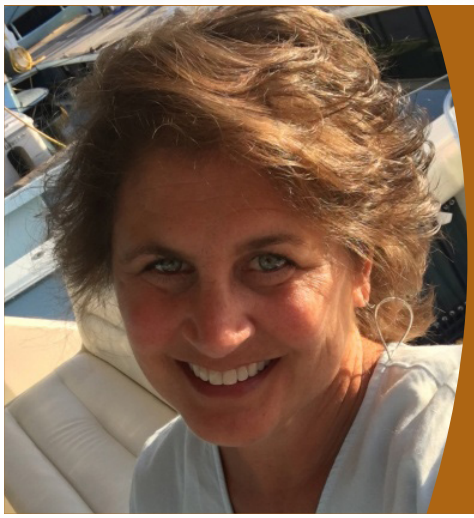
勒索軟體仍然是今年最大的網路禍害。根據威脅情報公司 ProDaft 的報告，自 2021 年 7 月以來，使用 Conti 勒索軟體的攻擊者已經爽收贖金至少 2,550 萬美元。現在也鎖定酒店為攻擊目標。最近披露 Conti 勒索軟體攻擊影響客人訂房和房卡系統。該連鎖酒店表示，似乎沒有洩露任何客人個資，也沒有提出贖金要求。一場被認為是勒索軟體的網路攻擊，已迫使英格蘭北部的 300 多家超市暫時關閉並改用現金支付。

一份新報告還發現，勒索軟體攻擊中採用「雙重勒索戰術」正在急速攀升。Group-IB 的《2021/2022 年高科技犯罪趨勢報告》發現，受到急速攀升「雙重勒索」攻擊的組織數量激增 935%，並在資料外洩網站上暴露他們盜來的資料。在復原方面，Sophos 一份新報告顯示，與其他行業相比，教育行業的目標從勒索軟體攻擊中復原回來的成本更高。除了支付贖金外，教育組織還需要支付約 273 萬美元的費用，來支付停機時間、資料復原、設備和網路維修以及安全更新費用，這比所有行業的全球平均水平高出 48%。

根據趨勢科技最新的研究調查，儘管如此，90% 的 IT 決策者承認他們願意在網路安全計劃上做出妥協，以實現其他數位轉型目標，並且只有一半的受訪者相信最高管理階層完全了解網路風險。

繫好安全帶--這將是一段顛簸的旅程。

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