2021 年的全球網路威脅態勢回顧

2022 年 1 月 20 日發布｜威脅情報

威脅獵手團隊
賽門鐵克

賽門鐵克深入探討影響這一年的網路安全趨勢

從不斷演變的勒索軟體生態系統到針對關鍵基礎設施的攻擊，賽門鐵克回顧了影響及形成 2021 年的網路安全趨勢。

博通 (Broadcom) 的企業安全部門--賽門鐵克一份最新白皮書，回顧 2021 年期間形成威脅格局的一些主要威脅。

勒索軟體可以說是 2021 年組織面臨的最重大威脅，一些勒索軟體運營商退出，新的運營商進入，並且改進商業模式和戰術，在在顯示目標式勒索軟體已進入完全競爭並且比以往任何時候都更有利可圖。

然而，勒索軟體並不是唯一的威脅，供應鏈攻擊、利用服務公眾之公開應用程式漏洞的攻擊者增加，以及對關鍵基礎設施的攻擊，也影響 2021 年威脅態勢的發展。

勒索軟體

勒索軟體，或者更精確來說，目標式勒索軟體，是整個 2021 年成為頭條新聞的最主要威脅。勒索軟體集團開始瞄準擁有為數眾多下游用戶的企業。這些上游企業包括關鍵基礎設施營運商或大型軟體開發商和組織，如 Kaseya 軟體公司和 Colonial Pipeline (殖民地管道公司) 所遭受的攻擊所示。以管理服務提供商 (MSP) 為目標，還讓攻擊者有機會透過僅攻擊一個受害者來感染潛在的數千名受害者。

儘管與往年一樣，賽門鐵克在 2021 年偵測和攔截的勒索軟體攻擊總數繼續呈下降趨勢，但這並不意味著勒索軟體活動的威脅正在減弱。這種下降趨勢是由於相對簡單、亂槍打鳥的隨機式分的勒索軟體攻擊顯著減少，並且威脅參與者將注意力轉移到大型組織，在那裡他們可能造成更多破壞並要求更高的贖金。這些有針對性的目標式勒索軟體攻擊的數量從 2020 年 1 月的約 80 起上升到 2021 年 9 月的 200 多起。

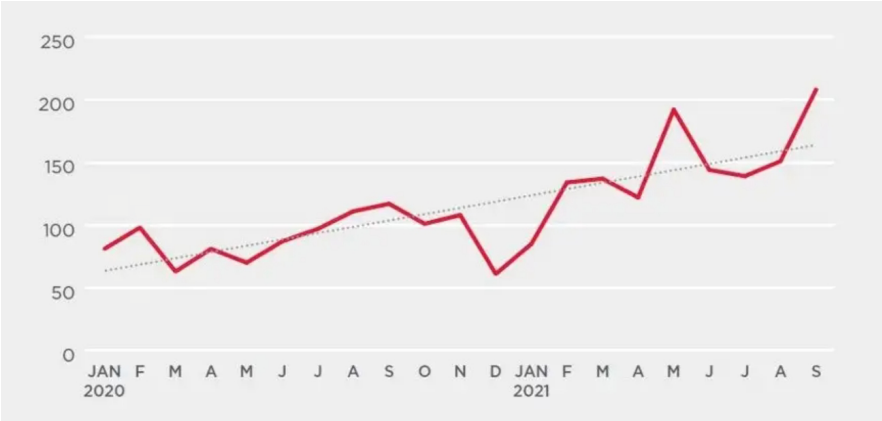


圖 1. 2020 年 1 月至 2021 年 9 月有目標式勒索軟體攻擊數量

這種有針對性的目標式勒索軟體攻擊的增加，有部分是由兩個相對較新的發展所推波助瀾下：其一是所謂的初始存取代理 (IABs：initial access brokers) 的興起，威脅攻擊發動者將已入侵網路的存取權，出售給願意出高價的人，最近已升格成為目標式勒索軟體集團；再來是勒索軟體即服務 (RaaS) 的興起，這是一種訂閱制的商業性質網路攻擊服務，允許被稱為聯盟夥伴的個人或集團，在攻擊中使用已經開發的勒索軟體威脅。

RaaS 模型大大增加組織面臨的對手數量，現在有多個攻擊者試圖提供相同的勒索軟體，但使用不同手法、技術與過程 (Tactics, Techniques, and Procedures，簡稱 TTPs)。

由於 RaaS 市場的增長，如果當前的勒索軟體關閉，聯盟夥伴公司現在可以選擇遷移到另一種勒索軟體。此外，賽門鐵克還觀察到聯盟夥伴公司在很短的時間內，使用兩種不同的勒索軟體，在某些情況下，在同一次攻擊中。這表明一些聯盟夥伴公司有足夠的聲譽，不會被鎖定在與固定一個勒索軟體運營商的獨家協議中。

> 儘管與往年一樣，賽門鐵克在 2021 年檢測和阻止的勒索軟體攻擊總數繼續呈下降趨勢，但這並不意味著勒索軟體活動的威脅正在減弱。

殭屍網路現在也在勒索軟體攻擊中扮演著重要的角色，許多舊的金融欺詐殭屍網路已被重新用於傳播勒索軟體。在某些情況下，它是勒索軟體和殭屍網路幕後相同的主使者。例如：Trickbot 被認為由 Miner 集團 (又名 Wizard Spider) 所控制，該集團也與 Ryuk 和 Conti 勒索軟體有關。

去年與勒索軟體有關的另一個要點，包括針對受 COVID-19 新冠疫情打擊最嚴重的行業的運營商。一個典型的例子是 Conti (又名 Miner，Wizard Spider) 勒索軟體運營商對愛爾蘭國家衛生服務機構 Health Service Executive 的攻擊。

去年還看到 REvil (又名 Leafroller，Sodinokibi) 勒索軟體營運商的基礎設施遭到執法部門的破壞，至少控制一些 REvil 的伺服器。然而，與之前打擊該集團活動的努力一樣，REvil 很可能在最近拆除行動之後，以某種形式借屍還魂再重出江湖。

2021 年，有目標式勒索軟體集團也開始威脅受害者，以防止他們與媒體或勒索軟體談判公司分享攻擊細節。Conti 和 Grief 勒索軟體集團都表示，如果公開分享贖金談判的交談紀錄或螢幕截圖，他們將公佈被盜的受害者資料或刪除解密密鑰。這一聲明很可能是由越來越多的媒體報導中包含贖金談判的細節而引起。其他威脅集團也採用類似的戰術，包括 Ragnar Locker 和賽門鐵克威脅獵手團隊發現一種名為 Yanluowang (*閻羅王) 全新勒索軟體威脅。

供應鏈攻擊

由於軟體供應鏈攻擊有可能嚴重擾亂社會和商業很大部分，仍然是世界各地政府和企業關注的問題。去年成為頭條新聞的兩起重大供應鏈攻擊事件，包括 SolarWinds 駭客事件和 Kaseya

攻擊事件。

雖然 SolarWinds 攻擊發生在 2020 年底，但它繼續在 2021 年掀起波瀾。負責這次的攻擊者，就是由俄羅斯所支持並一直活躍於駭客圈的 Nobelium (又名Hagensia) 國家級駭客集團。一個可能由 Nobelium 開發的新後門威脅 (Tomiris) 在 9 月被發現。該惡意軟體與 Nobelium 在 SolarWinds 攻擊中使用的 SUNSHUTTLE 第二階段惡意軟體有相似之處。而另一個後攻擊 (post-exploitation) 的後門 (FoggyWeb) 也與 Nobelium 有關。該惡意軟體是設計來從被攻擊的活動目錄聯盟服務 (AD FS：Active Directory Federation Services) 伺服器中竊取敏感性資料。

由 REvil 勒索軟體運營商發動針對 IT 管理軟體設計商：Kaseya 的攻擊，影響使用該公司軟體多個管理服務提供商 (MSPs：managed service providers)。雖然 Kaseya 報告說，他們的客戶中大約有 60 人受到攻擊的影響，但這些客戶都是本身擁有眾多客戶的 MSP。據估計，因供應鏈攻擊而受到影響的組織數量高達 1,500 家。這次攻擊是在美國 7 月 4 日的長假週末進行，可能是讓攻擊盡可能長時間地不被注意，因為許多員工正在休假。這是威脅者越來越多採用的一種策略。

雖然 Kaseya 和 SolarWinds 攻擊是最重要的，但絕不是近期僅有的兩個供應鏈攻擊。根據美國身份竊盜資源中心 (Identity Theft Resource Center，ITRC) 一份報告，供應鏈攻擊正在增加，與 2020 年整個年度的 12 個月相比，2021 年前三個季度遭受此類攻擊影響的人數增加 793,000 人。

新的攻擊途徑

去年攻擊者利用服務公眾的公開應用程式漏洞，來獲取對組織網路的存取權限的攻擊有所增加。雖然在某些案例中，攻擊者專注於零時差漏洞，但更多時候，他們會關注最近釋放出修補程式的漏洞並積極尋找尚未在第一時間修補的系統。

這方面一個著名例子是微軟 Exchange Server 伺服器的重大漏洞，統稱為 ProxyLogon。這些漏洞在 2021 年 3 月初被修補，微軟當時說，這些漏洞被一個稱為 Hafnium 的進階持續性威脅 (APT) 組織 (賽門鐵克稱這個組織為 Ant 並持續追蹤中) 在目標攻擊中利用。然而，在 ProxyLogon 漏洞被披露後不久，其他威脅者也開始運用這些漏洞。

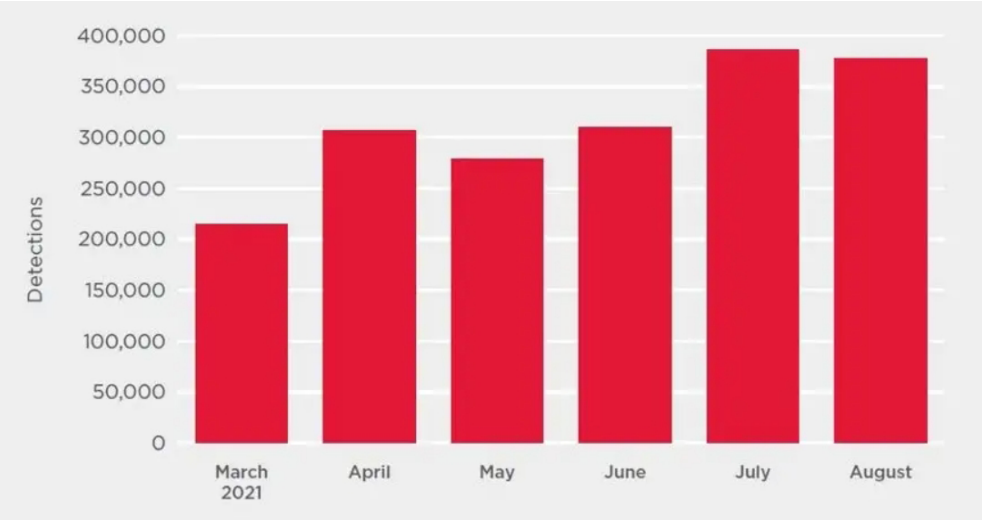


圖2. 2021年3月至8月針對微軟 Exchange Server 伺服器漏洞的刺探攻擊次數

2021 年 8 月，微軟 Exchange Server 伺服器另一系列，被統稱為 ProxyShell 的漏洞一被公開披露，馬上就有大量針對這些漏洞的刺探攻擊湧現，也凸顯公開披露的漏洞必須馬上修補的急迫性。賽門鐵克的資料顯示，僅在 2021 年 8 月就有超過 20 萬次針對這一系列漏洞的刺探攻擊。

2021 年經常被威脅者利用的服務公眾的公開應用程式的其他漏洞還包括 Pulse Secure (CVE 2019-11510)、Fortinet (CVE-2018-13379) 和SonicWall (CVE-2021-20016）的 VPN 產品的缺陷，以及 Accellion 的檔案傳輸設備 (FTA) 軟體的漏洞 (CVE-2021-27101、CVE-2021-27102 和 CVE-2021-27104)。

關鍵基礎設施

針對關鍵國家基礎設施 (CNI) 的網路攻擊可能是最具影響力，因為可能會影響社會大眾。這在 2021 年 5 月感受特別深刻，當時美國最大的石油管道公司--殖民地管道--Colonial Pipeline 遭受勒索軟體攻擊，影響了管道的營運設備。

這次攻擊是由總部位於俄羅斯的 DarkSide 勒索軟體集團發動。雖然在攻擊發生幾小時後支付贖金，但解密速度很慢，管道的運作也停止，導致美國多個州出現燃料短缺、價格上漲和恐慌性搶購。

殖民地管道的攻擊不是一個個別事件，2021 年 7 月也有消息指出，中國支持的國家級駭客組織在 2011 年至 2013 年的攻擊活動中，針對 23 個美國石油和天然氣管道運營商。美國官員宣佈，這些攻擊幕後的主使者目的是“宣示中國有能力發展針對美國管道的網路攻擊，以物理破壞管道或擾亂管道運營”。

針對 CNI 的攻擊沒有停止的跡象，可由與針對 CNI 相關攻擊的基於網路偵測數量呈上升趨勢 (圖 3) 得到驗證。賽門鐵克的入侵防禦系統 (IPS) 技術可以阻止這些攻擊。在網路上阻止的惡意活動在 2021 年 7 月達到高峰後出現了下降，但總體而言，數字呈上升趨勢。

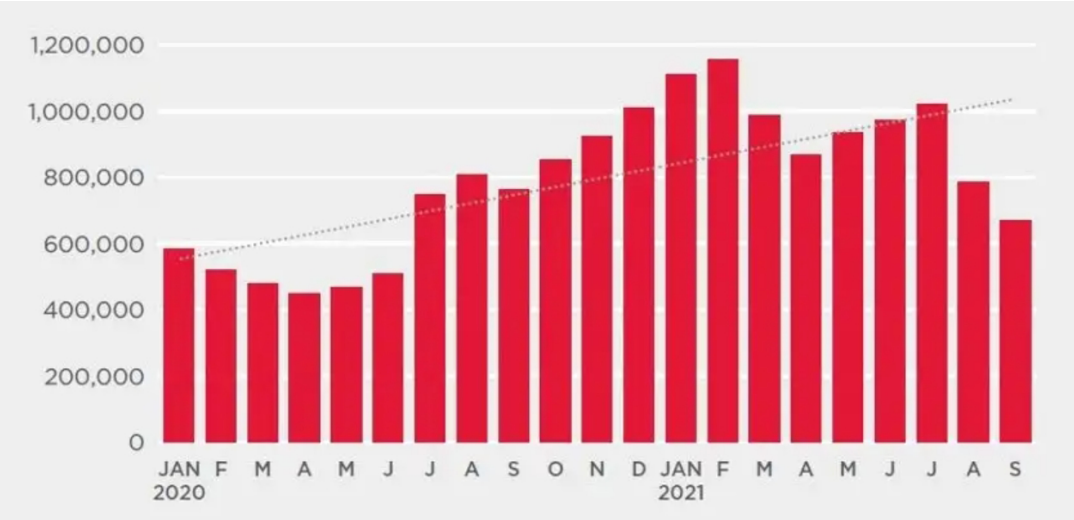


圖 3. 針對 CNI 相關的攻擊次數--基於網路檢測技術的方法

在針對 CNI 組織網路的攻擊活動最多的地區方面，美國遙遙領先，佔所有活動的 69%。

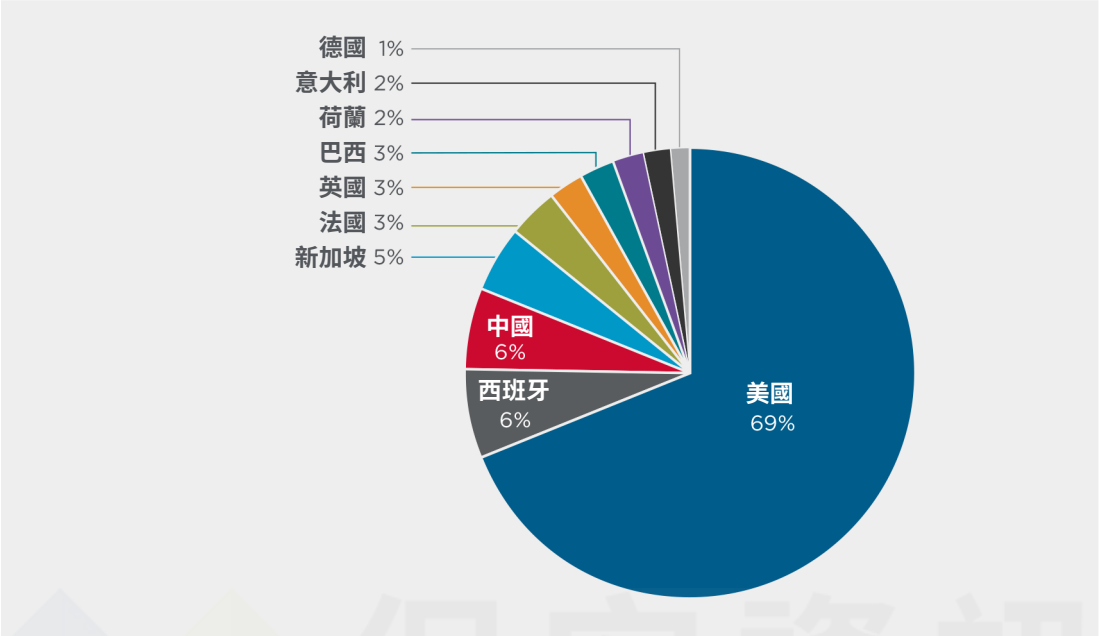
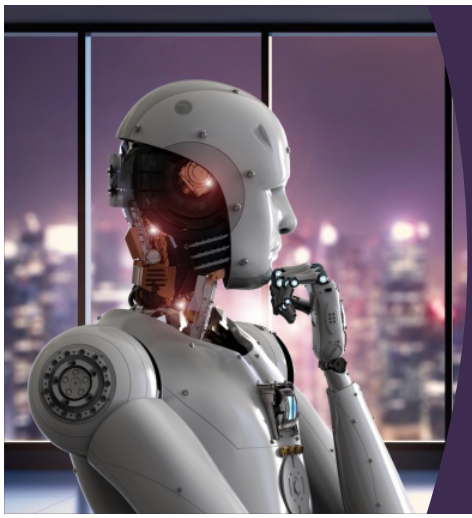


圖 4. 針對 CNI 組織的網路攻擊活動最多的地區

這只是我們最新白皮書中的部分內容樣本。閱讀全文，瞭解 2021 年威脅態勢的更多見解。



關於作者

威脅獵手團隊

賽門鐵克

威脅獵手 (Threat Hunter) 團隊是賽門鐵克內部的一群安全專家，其任務是調查有針對性的攻擊，推動賽門鐵克產品的增強保護，並提供分析以幫助客戶應對攻擊。

原廠網址：https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/threat-landscape-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