白皮書

2021年的全球網路威脅態勢回顧

由賽門鐵克威脅獵手 (Threat Hunter) 團隊撰寫

目錄

簡介

就安全領域而言，過去的一年 (2021) 是多事之秋，新的威脅不斷湧現，威脅者不斷發展他們的戰術，以保持或提高他們在威脅領域的地位。

2021 年期間，勒索軟體仍然是各種規模的組織所面臨的最嚴重威脅。目前的勒索軟體攻擊模型 -- 主要在癱瘓受害組織網路的目標式攻擊 -- 對網路犯罪分子來說是非常有利可圖。儘管出現一些可喜的發展，例如：幾個高度活躍的勒索軟體營運的退出，但不幸的是，這些都被新玩家的到來和策略的持續改進所抵消。

現在可以說是整個網路犯罪生態系統的關鍵，為越來越多的附屬攻擊小組提供資金，並為垃圾郵件發送者、金融木馬運營商和入侵專家等廣泛的攻擊者提供新的收入來源。

雖然勒索軟體仍是嚴重的問題，但在 2021 年還有其他一些值得注意的發展，特別是供應鏈攻擊的規模和企圖的顯著提升。雖然今年初主要受到 SolarWinds 攻擊影響，但緊隨其後是 7 月的 Kaseya 攻擊，勒索軟體運營商為其工具找到一個倍增助力的新戰力。這些攻擊不會被威脅者忽視，更多人可能會尋求將軟體供應鏈作為入侵高價值網路的一種手段。

也許 2021 年期間發生最出名的一次攻擊是對美國殖民地石油運輸管道公司 (Colonial Pipeline) 勒索軟體攻擊。作為該國能源供應的關鍵基礎設施，殖民地管道公司 (Colonial Pipeline) 攻擊具有高度破壞性，並就攻擊的潛在影響發出嚴重警告。出於經濟動機的勒索軟體集團並不是唯一的威脅。意圖造成破壞並在其對手中製造恐慌的民族國家，也是另一個令人擔憂的來源。

展望 2022 年時，各組織需要保持警惕，因為我們面對的是來自範圍越來越廣、動機強烈、資源越來越豐富的對手。

勒索軟體

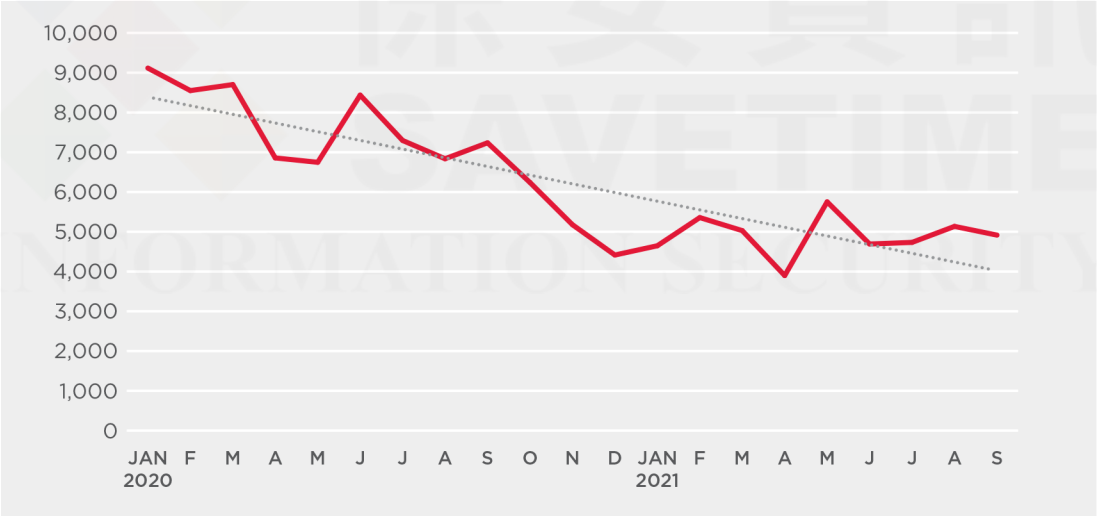
勒索軟體問題在 2021 年仍然是一個主要問題，最近的發展包括勒索軟體集團開始瞄準擁有為數眾多下游用戶的公司。這些上游企業包括關鍵基礎設施營運商或大型軟體開發商和組織，如 Kaseya 軟體公司和殖民地管道公司 (Colonial Pipeline) 所遭受的攻擊所示。此外，以管理服務提供商 (MSP) 為目標還讓攻擊者有機會透過僅攻擊一個受害者來感染潛在的數千名受害者。

這一年出現的另一個趨勢是勒索軟體集團瞄準受 COVID-19 新冠疫情打擊最嚴重的行業，即醫療保健行業。像是針對愛爾蘭健康服務管理署 (HSE) 的攻擊，是在醫院服務面臨巨大壓力的情況下進行，攻擊者可能認為這對他們有利，並迫使官員向他們的要求妥協。

對關鍵基礎設施的勒索軟體攻擊導致美國總統 -- 拜登 (Joe Biden) 呼籲俄羅斯總統 -- 普廷 (Vladimir Putin) 對俄羅斯的勒索軟體運營商採取行動。兩國的領導人同意，他們將召集兩國的網路安全專家，就網路活動的「禁區」以及美國和俄羅斯將如何「跟進」來自於「我們兩國中任何一國」的網路攻擊達成「具體理解」。然而，幾個月後，白宮國家安全委員會主辦一次國際反勒索軟體活動，有 30 多個國家參加，但俄羅斯卻顯然沒有參加。

勒索軟體的持續存在意味著賽門鐵克 (現為全球網通晶片巨擘 -- 博通 Broadcom，美國股市代號 AVGO 的企業安全部門，全世界網際網路流量有 99.9% 經過博通的網通晶片) 會定期發佈關於這個似乎永遠存在的威脅報告。我們最近的白皮書《勒索軟體的威脅》發現，與前幾年一樣，賽門鐵克檢測和阻止的勒索軟體攻擊總數繼續呈下降趨勢，然而，這並不一定意味著勒索軟體活動的威脅日益式微。該報告包括截至 2021 年 6 月的資料，顯示檢測和攔截的攻擊從 2020 年 1 月 9,116 次到 2021 年 6 月僅 4,692 次。雖然攻擊數量在 2021 年 9 月略微上升到 4,916 次，但數字總體上仍呈下降趨勢 (圖 1)。這是由於相對簡單、亂槍打鳥的隨機式勒索軟體攻擊明顯減少，及威脅者目標一直是針對大型組織，在那裡他們可以造成更大破壞並要求更高的贖金。

圖 1：2020 年 1 月至 2021 年 9 月的所有勒索軟體偵測呈下降趨勢

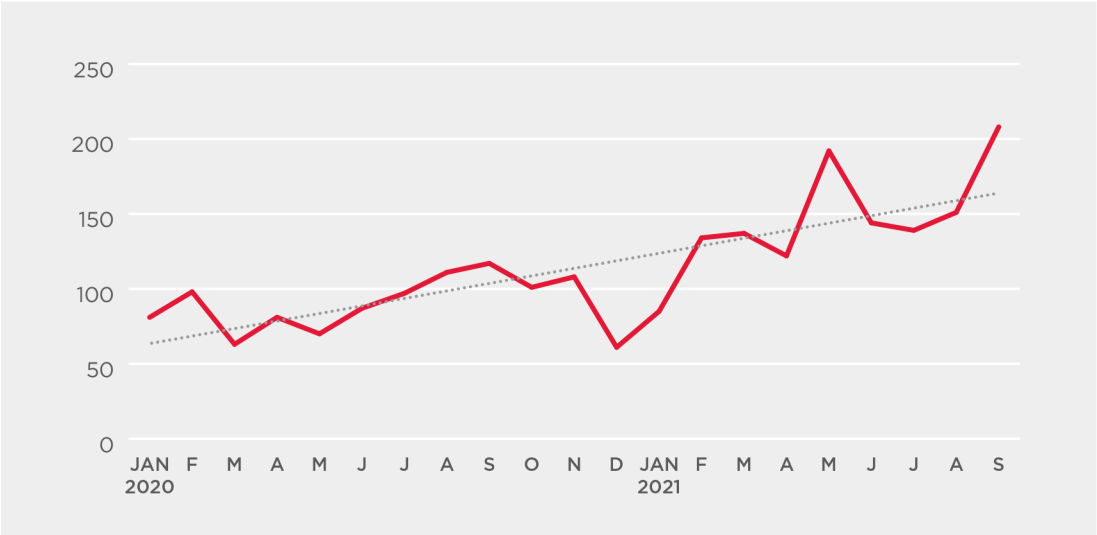


美國財政部的一份金融趨勢分析報告也強調這種有針對性的目標式勒索軟體威脅的增加，該報告將 2011 年以來超過 52 億美元的比特幣交易與勒索軟體集團關聯起來。該報告發現，僅在 2021 年的前六個月，這些類型的交易總額為 5.9 億美元，已經超過 2020 年一整年 12 個月中與勒索軟體相關的 4.16 億美元的比特幣交易。

儘管執法部門努力阻止有針對性的目標式勒索軟體的浪潮，例如：最近將 REvil(又名 Leafroller、Sodinokibi) 勒索軟體推下線的國際行動，所有這些都在發生。REvil 的基礎設施被美國聯邦調查局 (FBI)、美國網路司令部、特勤局和一些國際政府的特工破壞，他們至少控制 REvil 的一些伺服器。這是 REvil 第二次被關閉。該集團的活動在 2021 年 7 月 Kaseya 勒索軟體供應鏈攻擊後曾被停止，有傳言說執法部門當時也破壞它的運作。然而，REvil 在 9 月再次回歸，並且很可能在最近的拆除行動之後以某種形式借屍還魂再重出江湖。

雖然整體勒索軟體偵測數正在下降，但有針對性的目標式勒索軟體攻擊卻有上升的趨勢 (圖 2)。受目標式勒索軟體攻擊影響的組織數量從 2020 年 1 月約 80 個，上升到 2021 年 9 月的 200 多家。部分原因是勒索軟體即服務 (RaaS) 的興起，這是一種基於訂閱的商業模式，讓個人或被稱為聯盟夥伴公司的集團，在其勒索威脅攻擊中使用已經開發的勒索軟體。

圖 2：2020 年 1 月至 2021 年 9 月，受針對性目標式勒索軟體攻擊影響的組織數量



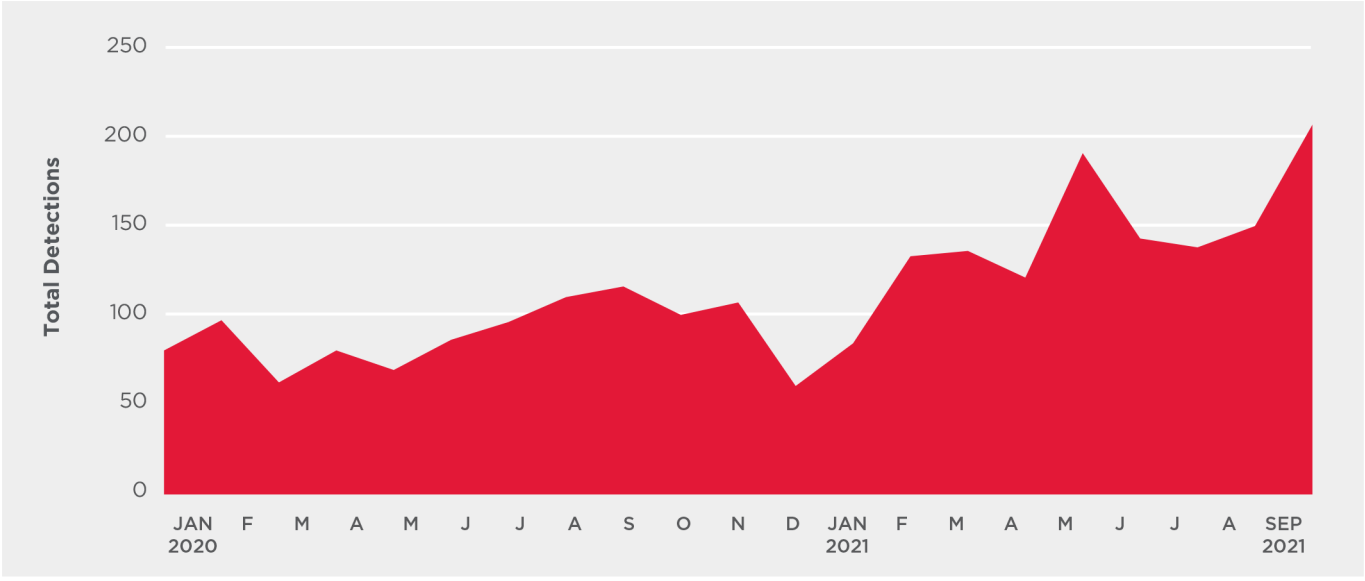
促成目標式勒索軟體攻擊增加的另一個趨勢是所謂初始存取代理 (IABs：initial access brokers) 的崛起。這些攻擊者已經獲得網路存取權，並將這種存取權賣給付錢給他們的人，最近一段時間，這種人越來越多是勒索軟體運營商。IABs 讓勒索軟體營運商省掉搜索與入侵組織漏洞的時間，使他們能夠集中精力敲詐他們的受害者。

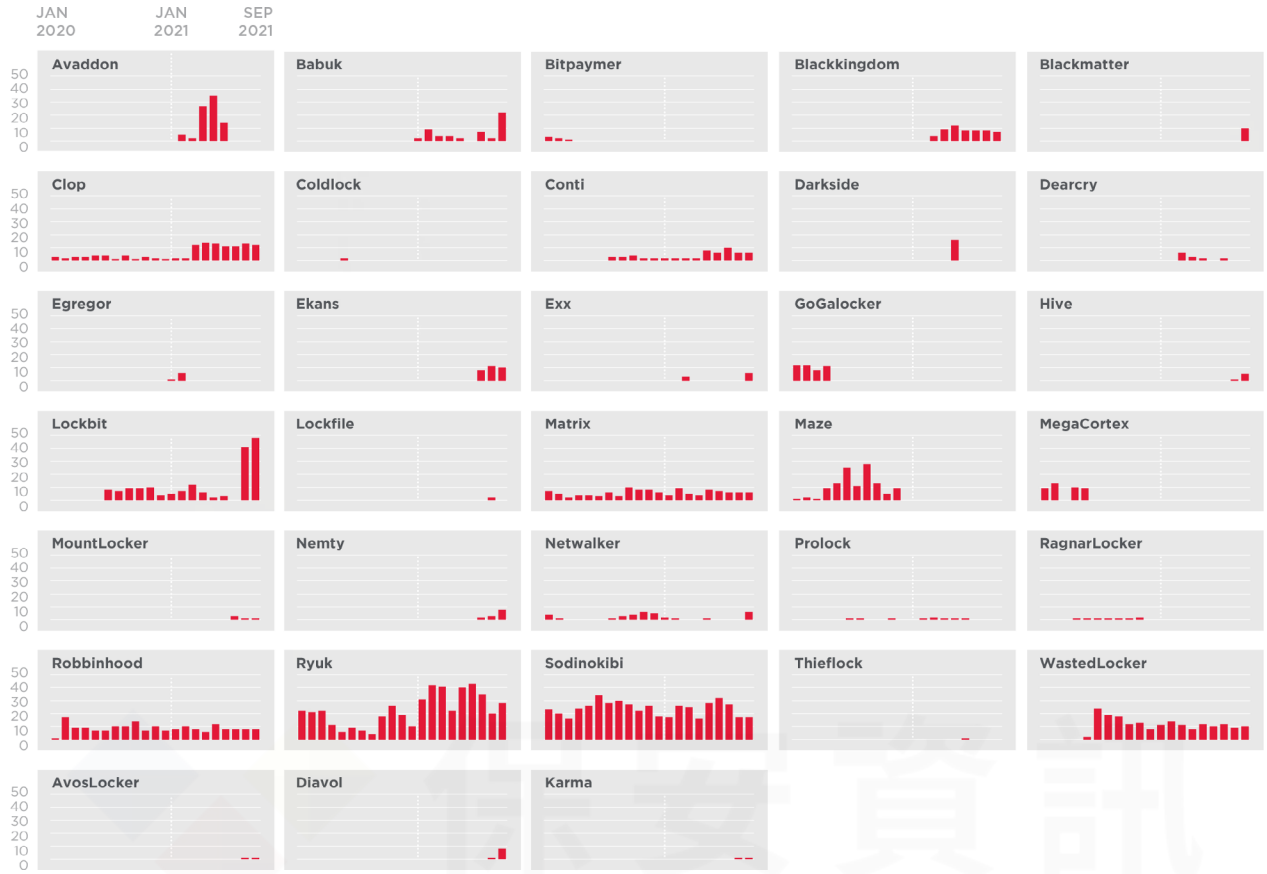
今年我們看到的另一個趨勢是，有針對性的目標式勒索軟體集團威脅受害者，要防止他們與媒體或勒索軟體談判公司分享攻擊的細節。

10 月，Conti 勒索軟體 (又名 Miner，Wizard Spider) 的運營商表示，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。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。

Grief 勒索軟體集團還警告受害者不要與談判公司聯繫，威脅說如果不按照他們的指示，將刪除受害者的解密金鑰。其他威脅集團也採用類似的戰術，包括 Ragnar Locker 和賽門鐵克的威脅獵手團隊發現的一種名為 Yanluowang(* 閻羅王) 新勒索軟體集團威脅。

圖 3：2020 年 1 月至 2021 年 9 月按針對性勒索軟體家族分類的受攻擊影響的組織數量





網路犯罪生態系統

勒索軟體對網路犯罪領域產生巨大影響，為胸懷壯志的攻擊者創造新契機，並帶來山頭林立的網路黑社會更大的合作空間。

變革的關鍵驅動力之一是勒索軟體即服務 (RaaS：ransomware-as-a-service) 的成熟。從勒索軟體發展者的角度來看，RaaS 是拼圖中缺少的一塊。有針對性的目標式勒索軟體攻擊是勞力密集型，對於任何勒索軟體運營商來說，他們的收入都受限於他們可以發動的攻擊數量。透過將他們的工具出租給其他攻擊者以換取分潤，勒索軟體運商便能盡其所能地提高他們的收入，並為那些可能沒有技能從頭開始建立自己勒索軟體運作的攻擊者，提供一個進入勒索軟體攻擊的捷徑。

對於企業來說，這使他們面臨的威脅數量倍增，因為現在的大多數勒索軟體威脅，多來自為數眾多的不同集團，多試圖提供相同的勒索軟體，但使用不同的戰術、技術和程序 (TTPs)。

今年，RaaS 市場的成熟程度與複雜度都在增加。聯盟夥伴成員現在流動性很高，如果一個勒索軟體運營商關閉了，許多人將容易地轉移到另一個勒索軟體集團，並開始使用他們的工具。

另有跡象表明，勒索軟體運營商和聯盟夥伴成員之間的權力平衡發生轉變，因為賽門鐵克已經觀察到聯盟夥伴成員在很短的時間內，某些情況下，在同一次攻擊中使用兩種不同的勒索軟體。這表明夠大牌的聯盟夥伴成員，不會被鎖定在與一個勒索軟體運營商的獨家協定中。

第二個值得注意的發展是僵屍網路現在在勒索軟體攻擊中發揮的作用，並為許多舊型態威脅提供新的生機。大多數僵屍網路最初是為了金融詐騙而建立，但許多僵屍網路已被重新利用，而有最多待價而沽的僵屍網路，即分布在許多企業內部殭屍電腦所組成的僵屍網路，正被賣給勒索軟體攻擊者。

在某些情況下，勒索軟體和僵屍網路幕後是同一個威脅集團。例如：Trickbot 被認為是由 Miner 集團 (又名 Wizard Spider) 控制，該集團也與 Ryuk 和 Conti 勒索軟體家族有關。IcedID 僵屍網路也被勒索軟體攻擊者大量使用，而其他僵屍網路，如 Qakbot、Emotet 和 Dridex 也有類似的特點。

這種程度的合作是一個不樂見的發展，因為這意味著任何在其網路上發現這種高度流行惡意軟體的組織，現在都必須考慮它是否被用作更強大威脅類型的工具。

供應鏈攻擊

我們於 2021 年 2 月發布的白皮書《供應鏈攻擊：網路犯罪分子瞄準最薄弱環節》中，我們討論這些類型的攻擊多年以來是如何發生，並在 2020 年底， SolarWinds 駭客事件發生時成為頭條新聞。

在 2020 年 12 月盡人皆知的一次供應鏈攻擊中，SolarWinds 的 Orion 軟體更新機制遭到破壞，一個被植入木馬的更新程式 (Backdoor.Sunburst) 被散佈給包括多個美國政府機構在內的數萬名 SolarWinds 客戶。

由俄羅斯支持的 Nobelium(又名 Hagensia) 駭客組織發起 SolarWinds 攻擊後，一直保持活躍。在 9 月發現一個可能由 Nobelium 開發的新後門威脅。該惡意軟體被稱為 Tomiris，與 Nobelium 在 SolarWinds 攻擊中使用的 SUNSHUTTLE 第二階段惡意軟體有相似之處。Tomiris 是透過 DNS 劫持攻擊部署，若不幸受駭，試圖存取公司電子郵件服務登錄頁面的目標，會被重導向到一個界面長得很像原公司的詐騙網域，以安全更新為幌子欺騙登錄者下載該惡意軟體。

另一個名為 FoggyWeb 的後門也與 Nobelium 有關。後攻擊 (post-exploitation) 的後門能夠從被入侵的活動目錄聯盟服務 (AD FS) 伺服器中竊取敏感性資料。

雖然 SolarWinds 的攻擊因公司客戶群的規模和構成而影響重大，但供應鏈攻擊絕非罕見。根據身份盜竊資源中心 (ITRC) 2021 年 10 月的一份報告，供應鏈攻擊正在增加，與 2020 年整個 12 個月相比，2021 年前三個季度受此類攻擊影響的人數增加 793,000 人。ITRC 記錄截至 2021 年 9 月 (包括 9 月) 期間，計有 60 個組織受到 23 次第三方或供應鏈攻擊的影響。

在供應鏈攻擊過程中被滲透的目標之一是 Kaseya，它是商業 IT 管理和遠端監控解決方 Kaseya Virtual System Administrator (VSA) 的製造商。該攻擊由 REvil(又名 Leafroller，Sodinokibi) 勒索軟體集團所發動，影響多個使用 Kaseya VSA 軟體的管理服務商 (MSPs：managed service providers)。

這次攻擊利用 VSA 中的一個漏洞，並且是在美國 7 月 4 日的週末假期中進行，可能是為了讓攻擊在達到目標之前不被察覺，因為許多員工可能已經下班了。攻擊被發現後，Kaseya 敦促 VSA 用戶關閉他們的 VSA 伺服器，以防止它們被入侵。雖然該公司表示，他們的客戶中只有“一小部分”受到攻擊的影響，但這些客戶都是本身擁有眾多客戶的 MSP。Kaseya 報告說，大約有 60 個客戶受到攻擊的影響；但是，由於供應鏈攻擊而受到影響的組織數量估計有 1,500 個。

7 月，Kaseya 宣布已獲得用於攻擊中使用 REvil 勒索軟體的通用解密工具。雖然 Kaseya 只說它從一個“受信任的第三方”獲得解密工具，但 REvil 集團後來透露，Kaseya 勒索軟體攻擊所有受害者的通用解密工具被其一名編碼員意外地發佈給受害者。REvil 最初要求 7,000 萬美元購買通用解密工具、500 萬美元購買單個 MSP 解密工具，或者每台電腦 4 萬美元解密。

軟體供應鏈攻擊，由於其有可能破壞社會和商業的大部分運作，仍然是世界各國政府和企業關注的問題。

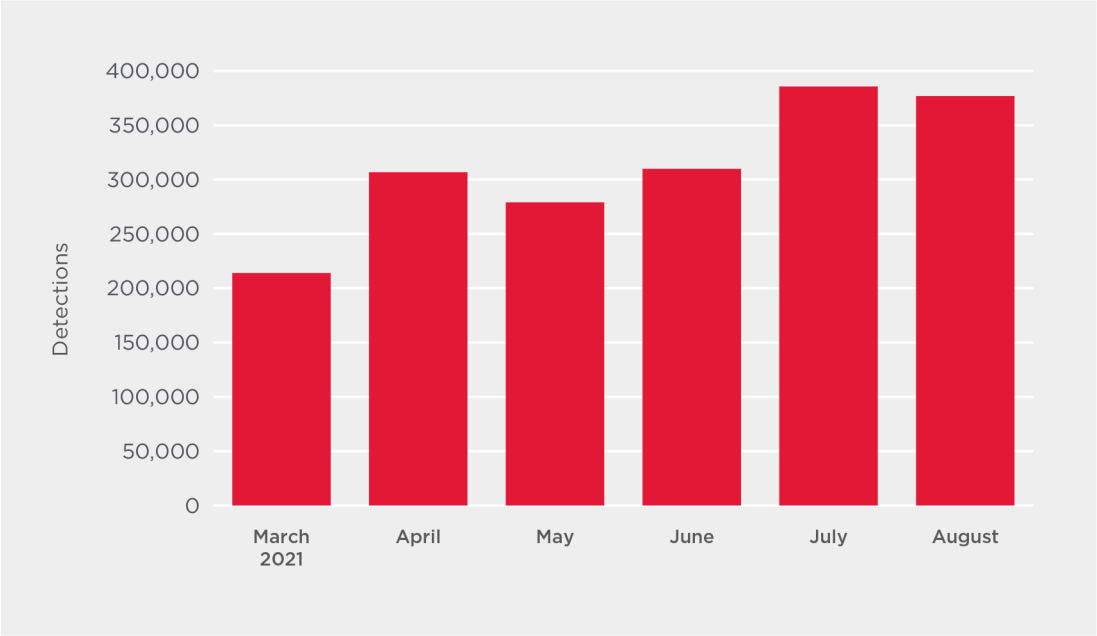
新的攻擊途徑

在過去的一年裡，攻擊者利用服務公眾的公開應用程式漏洞以獲取對組織網路存取權的數量激增。在某些情況下，它們是對零日漏洞的利用，但更多時候其關注為最近發布修補的漏洞和尋找未修補的系統。

最明顯的例子是在 Microsoft Exchange Server 中發現許多嚴重漏洞，通稱為 ProxyLogon。

微軟於 2021 年 3 月 2 日針對這些漏洞發布緊急修正程式。當時微軟表示，這些漏洞被一個稱為 Hafnium 高級持續性威脅 (APT) 組織 (賽門鐵克追蹤這個組織為 Ant) 在目標攻擊中利用。然而，當這些漏洞的存在成為公眾知識時，許多其他威脅者急於利用它們。這在當時的報告中可以看到，在我們的資料中也可以看到 (圖 4)，該資料顯示針對 Exchange 伺服器漏洞的刺探利用攻擊從 2021 年 3 月開始，此後一直處於高峰。

圖 4：利用微軟 Exchange 伺服器漏洞的刺探攻擊次數，區間：2021/03~2021/08



2021 年 8 月，微軟 Exchange 伺服器另一串漏洞，被稱為 ProxyShell，在黑帽技術大會被公開披露。這三個漏洞 (CVE-2021-34473、CVE-2021-34523 和 CVE-2021-31207) 串連這些漏洞將允許在微軟 Exchange 伺服器上，進行未經認證的遠端程式碼執行 (RCE)。針對這些漏洞的刺探利用攻擊迅速展開。賽門鐵克的資料顯示，僅在 2021 年 8 月就有超過 20 萬次針對這組漏洞的利用嘗試。

服務公眾的公開應用程式中經常被惡意行動者利用的其他漏洞包括：

- Pulse Secure(CVE2019-11510) 和 Fortinet(CVE-2018-13379) 的 VPN 漏洞。澳洲網路安全中心 (Australian Cyber Security Centre，ACSC) 在 2021 年中發布一份公告，警告 LockBit 2.0 勒索軟體攻擊者正在使用 CVE-2018-13379 獲取對受害者網路的初始存取權限。2021 年 9 月也有報導稱，這一漏洞被利用來竊取近 50 萬個 VPN 登錄帳密，並在一個駭客論壇上分享。這兩個漏洞也出現在美國網路安全暨基礎架構管理署 (CISA)2020 年被利用最多的漏洞名單中，儘管它們已經分別在 2019 年和 2018 年釋出修補。
- Sonicwall VPN 的一個零時差漏洞 (CVE-2021-20016)。在未修補之前，該漏洞被 Canthroid 網路犯罪集團利用，該集團負責 Thieflock 勒索軟體。該漏洞在 2021 年 2 月被修補，但 Canthroid 繼續透過利用未修補的軟體版本中的這個漏洞來攻擊組織。成功刺探利用後，攻擊者可以自建帳密並連入目標網路。
- Accellion 的檔案傳輸設備 (FTA) 軟體中的漏洞。攻擊者利用四個漏洞 (CVE-2021-27101、CVE-2021-27102、CVE-2021-27103 和 CVE-2021-27104) 攻擊 FTA 伺服器並安裝名為 DEWMODE 的 Web Shell。該漏洞與 FIN11 和 Clop 勒索軟體幫派有關，攻擊者可以獲得一些 Accellion 客戶的資料。

賽門鐵克的分析顯示，利用服務公眾之公開應用程式的漏洞出現一些明顯的趨勢：

- 攻擊者利用漏洞的速度非常之快。在大多數情況下，一旦漏洞為公眾所知，攻擊者就開始發動刺探利用攻擊。通常這是因為這些漏洞很快被整合到 Metasploit 等工具中，這可以讓相對不熟練的人有可能掃描和利用未修補的伺服器和產品上的這些漏洞。
- 一旦個漏洞被攻擊者盯上，它似乎會在很長一段時間內繼續被利用。刺探利用攻擊往往不會減弱。在大多數情況下，這可能是由於多個參與者和網路犯罪分子執行的大規模漏洞掃描。
- 服務公眾之公開應用程式的漏洞有可能讓惡意行動者能夠存取各種應用程式，並有可能為他們提供非常全面未經身份驗證的存取。

針對關鍵基礎設施的攻擊

賽門鐵克的白皮書《全球性的大問題：關鍵基礎設施攻擊》於 2021 年 6 月發表，重點關注針對關鍵國家基礎設施 (CNI) 的網路攻擊。這些攻擊可能是一些最具影響力的攻擊，因為它們有可能影響社會大眾。CNI 攻擊有可能破壞人們日常使用的公用事業，例如：電力、水、交通等。

我們對 CNI 的依賴和脆弱性在 2021 年 5 月 7 日凸顯出來，當時美國最大的石油運輸管道公司--殖民地 (Colonial Pipeline) 遭受勒索軟體攻擊，影響了管道控制設備。

總部位於俄羅斯的 DarkSide 勒索軟體幫派發動此次攻擊，並要求 75 比特幣 (當時為 440 萬美元) 解密 Colonial 的系統。該幫派還從該公司竊取 100 GB 的資料，以作為若該公司不願支付贖金情況下的籌碼。贖金在襲擊發生幾小時內支付；然而，解密過程緩慢，因管道運輸停止，導致美國多個州出現燃料短缺、價格上漲和恐慌性搶購。

由於攻擊者提供的解密軟體很差，Colonial 在 5 月 12 日用自己的備份回復並使系統重新上線。在這次攻擊給美國東南部帶來重大打擊之後，拜登總統簽署一項行政命令，以提高向政府銷售的軟體安全標準，並加強對現有系統的檢測和安全措施，改進資訊共享和訓練，建立網路安全審查委員會並增進事件反應。司法部還召集一個網路安全工作專案小組來增加起訴，努力阻止類似的攻擊。

不幸的是，殖民地石油運輸管道公司--Colonial Pipeline 攻擊並非單一事件。2021 年 7 月，據透露，中國政府支持的威脅行為者在 2011 年至 2013 年期間針對 23 家美國石油和天然氣管道營運廠商進行攻擊活動，成功破壞其中 13 家。該訊息在 7 月 20 日網路安全和基礎設施安全局 (CISA) 和聯邦調查局 (FBI) 發布的聯合報告中披露。報告稱「這些行為者專門針對美國管道基礎設施，目的是使美國管道基礎設施處於危險之中」，並且「這種活動最終是為了幫助中國發展針對美國管道的網路攻擊能力，以實際破壞管道或破壞管道的運作」。

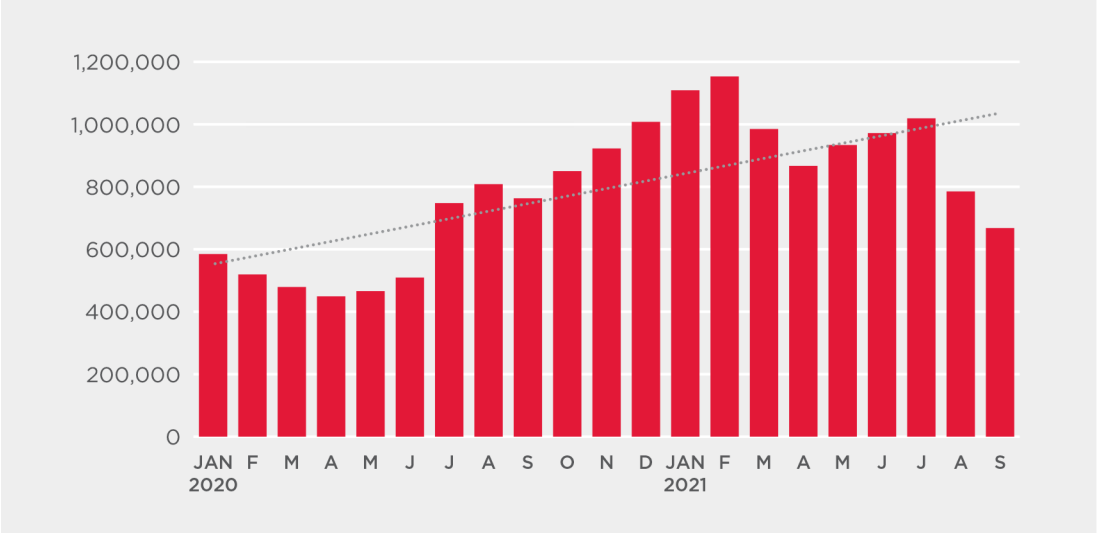
持續關注

如上所述，由於許多原因，針對 CNI 的攻擊令人擔憂，而且沒有停止的跡象。

雖然 CISA 列出總共 16 個屬於 CNI 的不同行業，但由於其中一些行業的規模，我們的 CNI 論文以及以下最新統計資料主要集中在這些行業類別，包括以下行業：

- 能源供應系統
- 水壩
- 化工產業
- 核能反應、材料、廢棄物系統
- 水資源與廢水處理
- 關鍵工業設施
- 運輸系統
- 商業設施

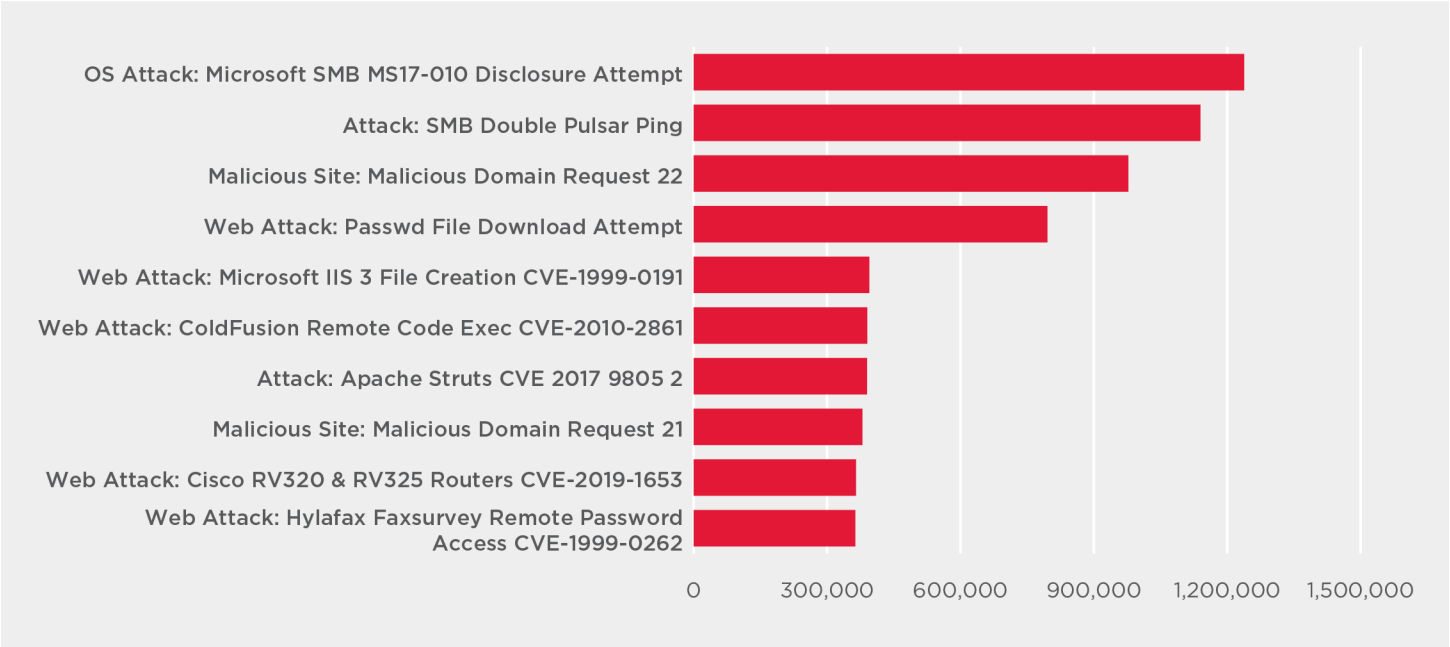
圖 5：2020 年 1 月至 2021 年 9 月， CNI 客戶在網路上攔截的惡意活動次數



針對 CNI 的攻擊相關之基於網路的偵測數量呈上升趨勢。賽門鐵克的入侵防禦系統 (IPS) 技術可以攔截這些攻擊。網路上攔截的惡意活動在 2021 年 7 月達到高峰後有所下降，但總體而言，數字依舊呈上升趨勢。

在關於 CNI 網路上攔截最多數量的 IPS 特徵檔時，結果與我們 CNI 白皮書中顯示的結果相當。大多數是攔截嘗試利用遠端程式碼執行 (RCE) 漏洞的特徵檔，攔截前四名的特徵檔排名不變。

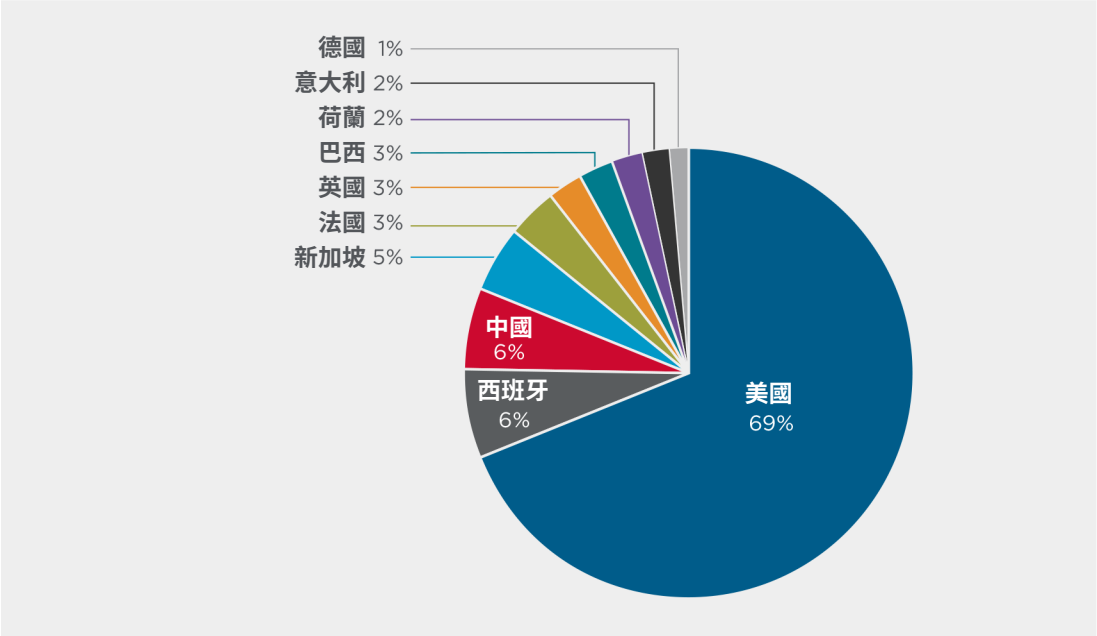
圖 6：2020 年 1 月至 2021 年 9 月 CNI 客戶網路上被攔截的排名前 10 個 IPS 特徵檔



在針對 CNI 組織遭受網路攻擊活動最多的地區排名方面，美國遙遙領先，佔所有活動的 69%。這與數據涵蓋從 2020 年 1 月至 2021 年 4 月的 CNI 白皮書中報告的活動百分比相同。

在我們的白皮書中列出下一個最受關注的地區是新加坡 (6%)，現在被西班牙 (6%) 和中國 (6%) 所取代。

圖 7：2020 年 1 月至 2021 年 9 月 CNI 客戶機器上網路塊排名前 10 的地區



「就地取材」攻擊

「就地取材」攻擊具有十分低調神祕並避免被發現的優勢，已經成為攻擊者日益喜愛的流行戰術。簡而言之，「就地取材」攻擊包括使用合法的工具或利用目標環境中已經存在的功能來達到惡意的目的。這可以幫助攻擊者保持不被發現，因為使用這些合法的工具和功能不可能引起任何懷疑。此外，由於這些工具和功能已經存在，攻擊者不需要花費時間和資源來開發他們自己的工具和功能，這使得「就地取材」成為一種更加誘人的戰術。

2020 年，賽門鐵克客戶環境中 22 種最常見的兩用工具執行次數增加 29.4%，從 2019 年 59 億次增加到 2020 年 76 億次。2021 年的數字已經超過 2020 年。到 2021 年 9 月底，已經比 2020 全年增加了 44.9%，到 2021 年迄今觀察到的執行次數為 109 億次，而 2020 年全年為 76 億次。

就客戶環境中最常見的兩用工具而言，PowerShell 仍然位居第一，其執行次數比第二名的 net.exe 高出 234%。

表 1：2019-2021 年前 26 種兩用工具的執行次數

Tool	2019	2020	2021 (Jan to Sep)
powershell.exe	5,680,737,655	7,248,945,270	7,956,724,935
net.exe	20,603,632	71,106,792	2,384,860,498
schtasks.exe	53,400,817	139,675,323	457,013,261
bitsadmin.exe	9,271,644	39,295,319	116,580,088
psexec.exe	21,061,886	19,000,752	67,091,362
wmic.exe	50,711,927	42,538,858	5,069,305
certutil.exe	16,306,248	19,785,607	2,627,475
sdelete.exe	211,417	248,111	1,258,608
tasklist.exe	925,812	687,823	1,187,194
teamviewer.exe	2,338,302	1,073,812	398,638
systeminfo.exe	365,362	273,187	174,686
wget.exe	455,273	250,821	136,140
gpresult.exe	1,428,498	674,506	91,127
curl.exe	468,414	195,474	81,694
ammyy.exe	123,066	56,086	11,634
rdpclip.exe	122,788	27,444	5,265
procdump.exe	6,603	3,924	3,202
nc.exe	8,309	3,276	2,234
vnc.exe	7,406	3,343	2,100
bloodhound.exe	7,318	1,095	264
wce.exe	338	179	130
nbtscan.exe	2,876	223	95
TOTAL:	**5,858,565,591**	**7,583,847,225**	**10,993,319,935**

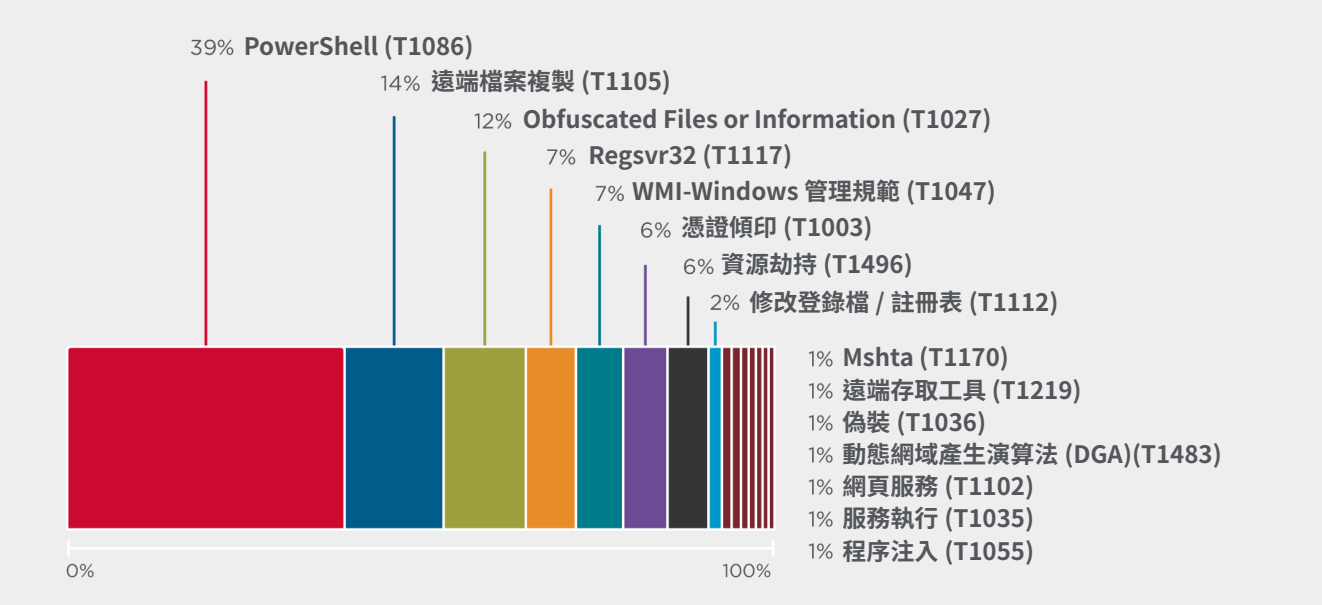
攻擊戰術、技術以及程序 (TTP)

MITRE ATT&CK® 矩陣對攻擊技術和戰術進行分類。它將攻擊戰術分為 12 個主要類別，它們映射到媒介和有效酬載執行之間的典型攻擊鏈：

- 初始存取
- 執行
- 持續
- 提升權限
- 防禦規避
- 憑證存取
- 發現環境資訊
- 橫向運動
- 收集
- 命令與控制
- 竊取資料
- 影響

在這些類別中，有 245 種不同的攻擊技術。有些可能用於攻擊鏈的多個階段，這意味著它們可以應用於上述 12 個類別中的多個類別。Symantec Cloud Analytics 使用 MITRE 技術名稱對所有事件進行分類。每年記錄數以百萬計的事件，因此可以對最常用的技術有些了解。雲分析利用分析師調查中收集的情報，並利用先進的機器學習來識別和阻止可疑活動的模式。因為它的目的是識別惡意活動，而不是惡意工具，所以產生的絕大多數事件都與「就地取材」的戰術有關。

圖 8：與雲分析事件相關的 MITRE 技術，2021 年 1 月至 9 月



惡意的 PowerShell 使用佔了事件的 39%。前五名的其他技術還包括：

- **遠端檔案複製**：經由從命令和控制 (C&C) 伺服器下載或採用其他方法 (例如：FTP) 將工具或檔案從外部來源傳輸到受感染網路。
- **混淆檔案或資訊**：試圖通過對惡意檔案進行編碼或以其他方式混淆其內容來使惡意檔案難以被發現。
- **Regsvr32**：Regsvr32.exe 是一個命令列程序，用於註冊和取消註冊物件鏈接並嵌入控制。攻擊者可能會濫用 Regsvr32.exe 代理執行惡意程式碼。
- **Windows Management Instrumentation (WMI) (WMI)**：Microsoft 命令列工具，可用在遠端電腦上執行命令。

結論

就威脅形勢而言，過去一年是多事之秋，所有指標都表明 2022 年將繼續這趨勢。雖然網路犯罪分子無疑會繼續利用本文討論的攻擊途徑，但他們也會發現新的攻擊機會。

網路安全威脅不會很快消失，組織應該保持對風險的認識，確保他們有適當的解決方案並積極主動，不要讓攻擊面的任何部分不受保護或不受監控。

保護方法

賽門鐵克解決方案如何提供幫助

賽門鐵克企業業務提供全面的安全解決方案組合，以應對當今的安全挑戰並保護資料和數位基礎架構免受多方面威脅。這些解決方案包括旨在幫助組織預防和檢測高級攻擊的核心功能。

賽門鐵克端點安全完整版 (Symantec Endpoint Security Complete：SESC)

專門用於幫助抵禦進階攻擊。雖然許多供應商提供 EDR 來幫助發現入侵，賽門鐵克也是如此，但存在差距。我們稱這些差距為盲點，SESC 有技術可以消除它們。

賽門鐵克建議客戶確保 IPS 技術在所有端點上運行，以針對基於網路的攻擊提供卓越的保護。此外，應實施自適應保護和先進的 TDAD 由端點面向防護 AD 技術，以加強系統抵禦就地取材攻擊並防止橫向移動。了解更多

高權限存取管理 (Privileged Access Management：PAM)

PAM 旨在通過保護機敏的管理憑證、控制高權限用戶存取、主動實施安全策略以及監控和記錄特權用戶活動來防止安全漏洞。了解更多

賽門鐵克網頁隔離 (Symantec Web Isolation)

Symantec Web Isolation 能透過在機構的企業系統和 Web 上的內容伺服器之建立建遠端執行環境 (遠端瀏覽技術)，隔離未分類及可能有風險的流量，以便在允許存取各種網頁的同時，防止惡意軟體和網路釣魚。了解更多

賽門鐵克安全網頁 (Web) 閘道 (SWG) -- SWG

提供高性能的本地或雲端安全服務的網頁 (Web) 安全閘道，組織可以利用這些閘道來控制或阻止對未知、未分類或高風險網站的瀏覽。強化雲端和網頁安全性和合規性，讓企業控制存取，協助使用者抵禦威脅並保護資料。了解更多

賽門鐵克情資服務 (Symantec Intelligence Services)

賽門鐵克情報服務利用賽門鐵克的全球情資網路為多個賽門鐵克網路安全解決方案提供即時威脅情資，包括賽門鐵克 Secure Web Gateway、賽門鐵克內容分析、賽門鐵克安全分析等。了解更多

賽門鐵克內容分析與進階沙箱 (Symantec Content Analysis with Advanced Sandboxing)

在賽門鐵克內容分析平台內，零日威脅會自動升級並通過動態沙箱代理到賽門鐵克惡意軟體分析，以對潛在的進階持續威脅 (APT) 檔案和工具包進行深度檢查和行為分析。了解更多

賽門鐵克安全分析 (Symantec Security Analytics)

賽門鐵克安全分析為完整網路流量分析、深入網路鑑識、異常檢測。為資安事端應變小組提供豐富的全封包擷取功能，以實現完整的安全性能見度、進階網路鑑識和即時威脅偵測。了解更多

緩解措施

賽門鐵克安全專家建議用戶遵循以下最佳實務來保護他們的網路。

當地環境：

- 監控內部網路兩用工具的使用情況。
- 確保您擁有最新版本的 PowerShell 並啟用日誌記錄。
- 限制僅允許來自特定已知 IP 位址的 RDP 來限制對遠程桌面協議 (RDP) 服務的存取，並確保您使用多重身份驗證 (MFA)。
- 對管理帳戶使用實施適當的審計和控制。您還可以為管理工作實施一次性憑證，以幫助防止盜竊和濫用管理憑證。
- 為系統管理工具建立使用配置文件 (profiles)。攻擊者使用其中許多工具在網路中橫向移動而未被發現。
- 在適用的情況下使用應用程式允許 (白) 名單。
- 鎖定 PowerShell 可以提高安全性，例如：使用受限語言模式。
- 使憑證傾印更加困難，例如：透過在 Windows 10 中啟用憑證保護或禁用 SeDebugPrivilege。
- 多因子驗證 (MFA) 可以幫助限制被入侵憑證的有效性。
- **建立計畫以考量外部方的通知**。若要確保正確地通知到必要組織 (例如：FBI 或其他法律執行機構／機關)，請務必制定驗證計畫。
- **建立一個仿效戰爭時「jump bag：跳袋」概念的機制，裡面同時存放所有關鍵管理資訊的紙本拷貝和電子檔備份**。為了防止這些關鍵資訊的可用性受到影響，將其與排除故障所需的硬體和軟體一起存放在一個跳袋中。當存放在網路的檔案被加密時，這些資訊也一樣化為烏有。「跳袋」一詞在第二次世界大戰期間一直用於傘兵。他們必須將任何落在敵後需要使用的東西塞進一個袋子裡。

保護電子郵件系統：

- 啟用雙重驗證 (2FA)，防止在網路釣魚攻擊期間危害憑證。
- 強化電子郵件系統周圍的安全架構，最大限度地減少到達一般使用者收件匣的垃圾郵件數量，並確保您遵循電子郵件系統的最佳實務準則，包括對網路釣魚攻擊使用 SPF 和其他防禦方法。

進行備份：

- **對備份複本實作異地儲存**。安排至少有四週異地儲存、每週完整和每日增量備份。
- **實作現場離線備份**。確保您的備份未連線至網路，以防止勒索軟體將它們進行加密。最好在系統關閉網路時進行移除，以防止任何潛在的威脅散佈。
- **確認並測試伺服器層級備份解決方案**。這應該已是災難復原程序的一部分。
- **提高備份檔和備份資料庫的檔案層級的安全等級**。可避免已被備份的檔案及資料庫被加密。
- **測試還原功能**。確保還原功能支援業務需求。