白皮書

勒索軟體威脅

由賽門鐵克威脅獵手 (Threat Hunter) 團隊撰寫

目錄

簡介

勒索軟體趨勢

加劇威脅：勒索軟體即服務

案例研究：周遊在不同聯盟之間的左右逢源營運模式

勒索軟體威脅集團

- Miner
- 案例研究：BazarLoader 攻擊中的社交工程要素
- Leafroller (* 壓葉機)
- Hispid (* 硬皮)
- Thysanura
- Syrphid
- Snakefly
- Coreid (* 核芯)
- Hornworm
- 案例研究：Hornworm 與 FIN8 的合作
- Leaftier
- Leaffolder
- Canthroid

工具、戰術及程序 (TTPs)

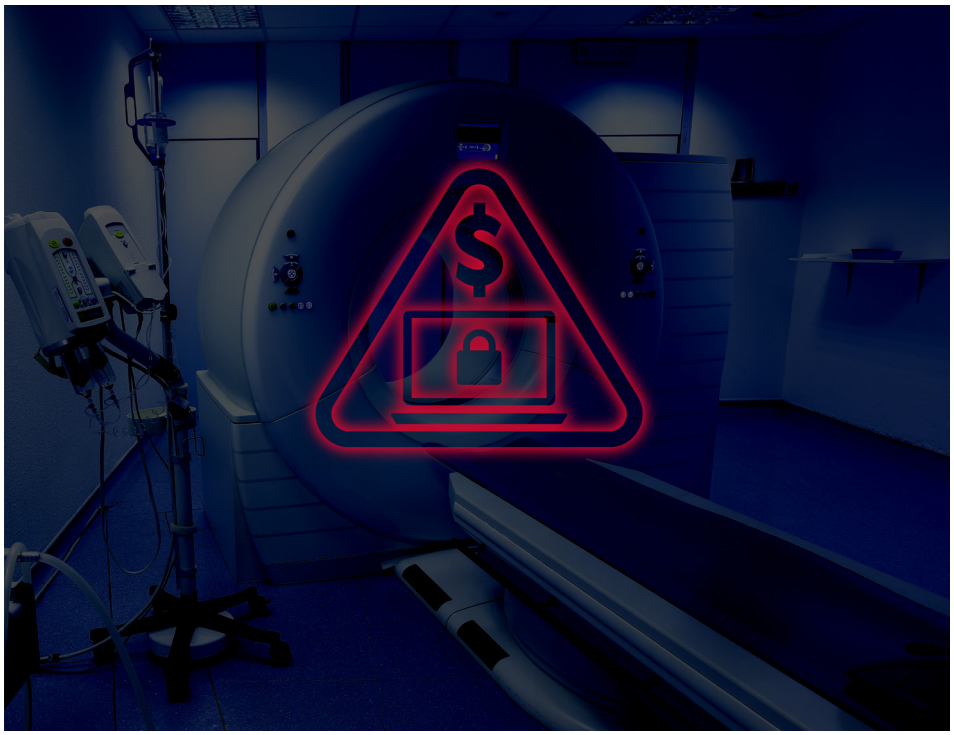
案例研究：勒索軟體供應鏈攻擊

感染媒介

- 二次感染
- 案例研究：IcedID 和 Conti 合作
- 網路釣魚
- 惡意廣告
- 漏洞利用
- 安全性不夠的服務

保護方法

緩解措施



簡介

勒索軟體仍對企業和其他大型組織構成重大威脅，特別是有針對性的目標式勒索軟體攻擊，被證明對網路犯罪分子來說利潤非常豐厚。導致數百萬美元贖金支出的重大勒索軟體攻擊，促使越來越多的惡意行動者加入勒索軟體領域。

在過去一年裡，勒索軟體攻擊者野心越來越大，並發起一系列備受矚目並極具破壞力的攻擊。2021 年 5 月對美國殖民管道的襲擊造成嚴重干擾，並引發對該國燃料供應的擔憂。同月，愛爾蘭國家衛生服務機構 Health Service Executive 遭到襲擊，迫使其取消數千個預約。在全球疫情大流行期間，工作人員不得不保留書面記錄，因為電腦一直處於離線狀態，直到網路被清理乾淨。

雖然這些攻擊描繪勒索軟體集團肆無忌憚的情況，但它們造成的破壞，確實產生了政治影響，美國總統拜登敦促俄羅斯總統普丁嚴加遏制勒索軟體攻擊集團，其中許多組織被公認設於俄羅斯。

據了解，一連串知名度很高的攻擊事件引發的公眾關注以及隨後的執法行動，肯定對一些較活躍的勒索軟體在 2021 年消失造成威脅，包括 Darkside、Sodinokibi（又名 REvil）和 Egregor 有實質的嚇阻作用。

雖然任何威脅的消失總是一個可喜的發展，但不應假設勒索軟體活動會減少。通常，已經退場的攻擊者會再帶著新的工具組重出江湖，而新的攻擊者會出現，虎視眈眈試圖接管退場黑幫所佔據的地盤。威脅形勢任何變化都意味著存在一段不確定性，網路防禦者不知道誰才是現在網路黑幫老大以及他們將採用什麼手段。

有兩個趨勢特別令人擔憂。首先，儘管勒索軟體即服務 (RaaS) 並不是新的現象，但作為檯面上主要勒索軟體開發商多元營運的一部分，它日益被採用，這導致有針對性的目標式勒索軟體攻擊激增。RaaS 不僅助長更多攻擊，而且發動勒索軟體攻擊所採用的工具、戰術和程序 (TTPs) 也不斷精進及增加。相同的勒索軟體都可以由多個不同的威脅參與者拿來發動攻擊，不同的人也將採用不同的 TTPs。RaaS 還降低參與者進入網路犯罪領域的技能門檻，增加攻擊者的數量。

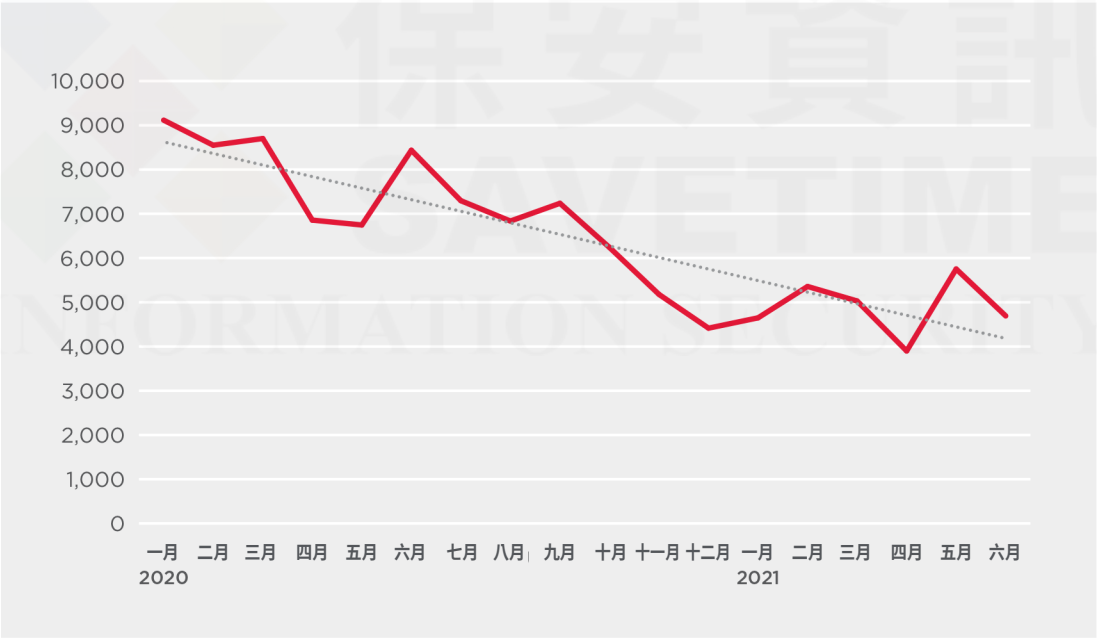
其次，越來越多的勒索軟體營運商正在與其他惡意軟體開發商合作，尤其是金融欺詐殭屍網路，以獲取受害者的存取權限。主要的殭屍網路通常具有廣泛影響力，並可能為勒索軟體集團提供大量潛在受害者，供他們從中進行網路釣魚。

勒索軟體集團現在是老練的威脅參與者，能夠與其他攻擊者建立關係以擴大其影響範圍，並採用一系列不斷發展的工具和戰術來提高他們的攻擊效率。成功防禦勒索軟體攻擊現在需要組織的深度防禦，以及對這些攻擊如何展開深入了解。

勒索軟體趨勢

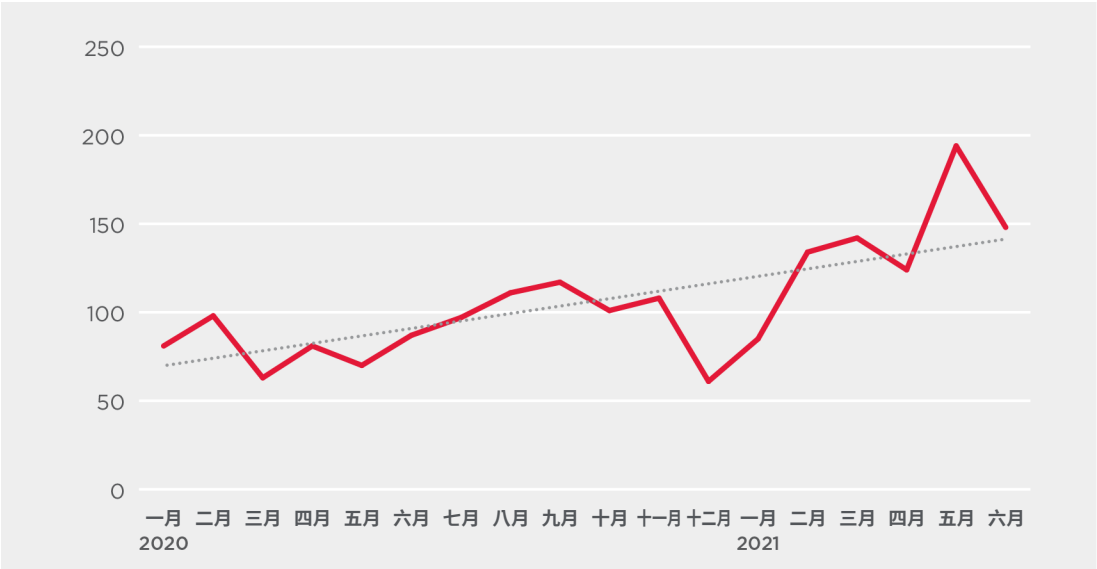
在過去的幾年中，勒索軟體威脅態勢發生顯著變化，並且這種趨勢在最近一直在持續。在過去 1 年半中，賽門鐵克檢測和阻止的勒索軟體攻擊總數幾乎減少一半，從 2020 年 1 月的 9,116 次減少到 2021 年 6 月的 4,692 次。

圖 1：2020 年 1 月至 2021 年 6 月的所有勒索軟體檢測



雖然勒索軟體活動任何減少都值得開心，但整體數量的下降是由於相對簡單、亂槍打鳥式的無差別攻擊持續下降所致。越來越多的威脅參與者現在專注於有針對性的目標式勒索軟體攻擊，其中一次攻擊一個組織，攻擊者試圖加密網路上盡可能多的電腦，以期提取高贖金。儘管數量相對較少，但這些攻擊對組織的破壞性遠大於亂槍打鳥式的攻擊，後者通常只有少數電腦可能受到影響。

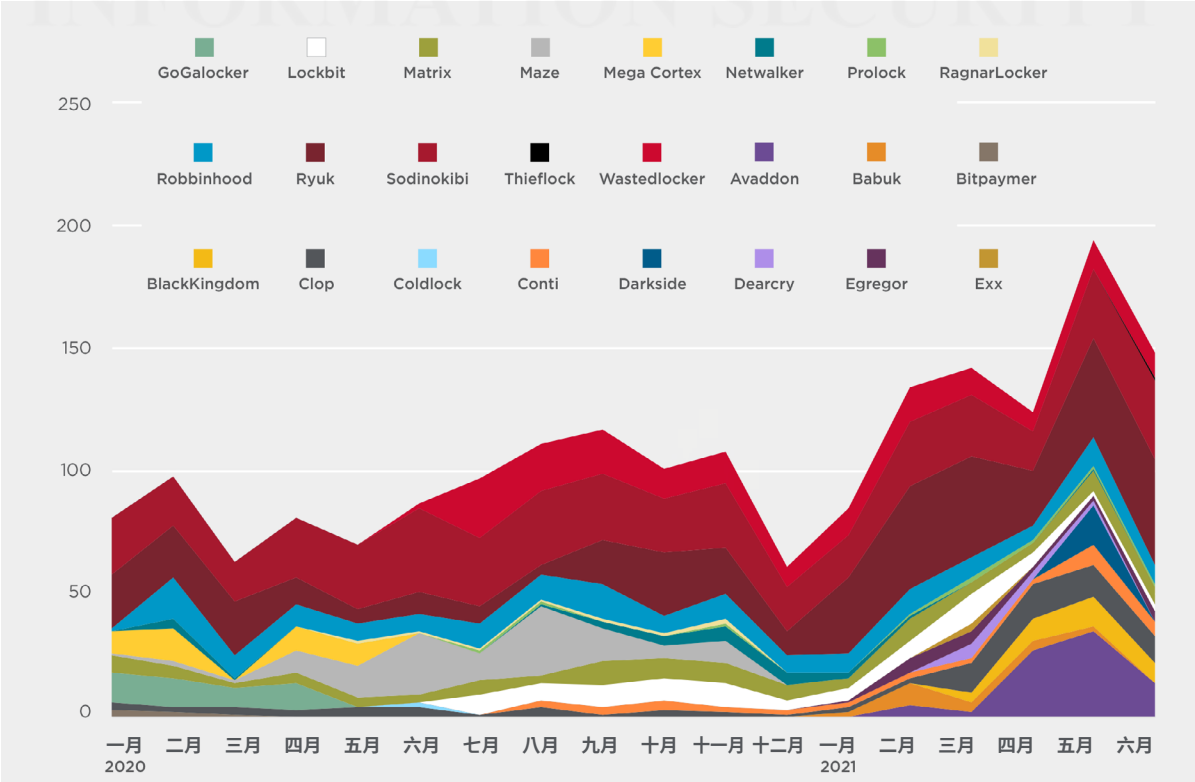
圖 2：受針對性目標式勒索軟體攻擊影響的組織數量，2020 年 1 月至 2021 年 6 月



目標式攻擊的統計數字則說明了不同的情況，在過去 18 個月中，遭受目標式勒索軟體攻擊影響的組織數量增加了 83%，從 2020 年 1 月的 81 家增加到 2021 年 6 月的 148 家。實際遭受目標式勒索軟體攻擊的數量遠遠高於此數字。除了用於目標式的攻擊外，一些勒索軟體家族還透過垃圾郵件行動進行散布。無法確定這些威脅的受害者有多少被目標式攻擊所感染，以及有多少是透過其他方式感染的，這意味著它們不能被計入目標式攻擊。

除此之外，來自已知目標式勒索軟體家族的已確認攻擊可能只是涉及這些威脅的攻擊總數的代表性樣本。許多目標式勒索軟體攻擊在有效酬載部署之前就已停止，這意味著它們可能不會被歸類為勒索軟體。此外，大多數目標式勒索軟體營運商都會為每次新的攻擊重新編譯他們的勒索軟體。這意味著攻擊中使用的勒索軟體變種可能會被通用或基於機器學習技術的特徵檔攔截，而不是歸類為與該勒索軟體家族相關的檢測。

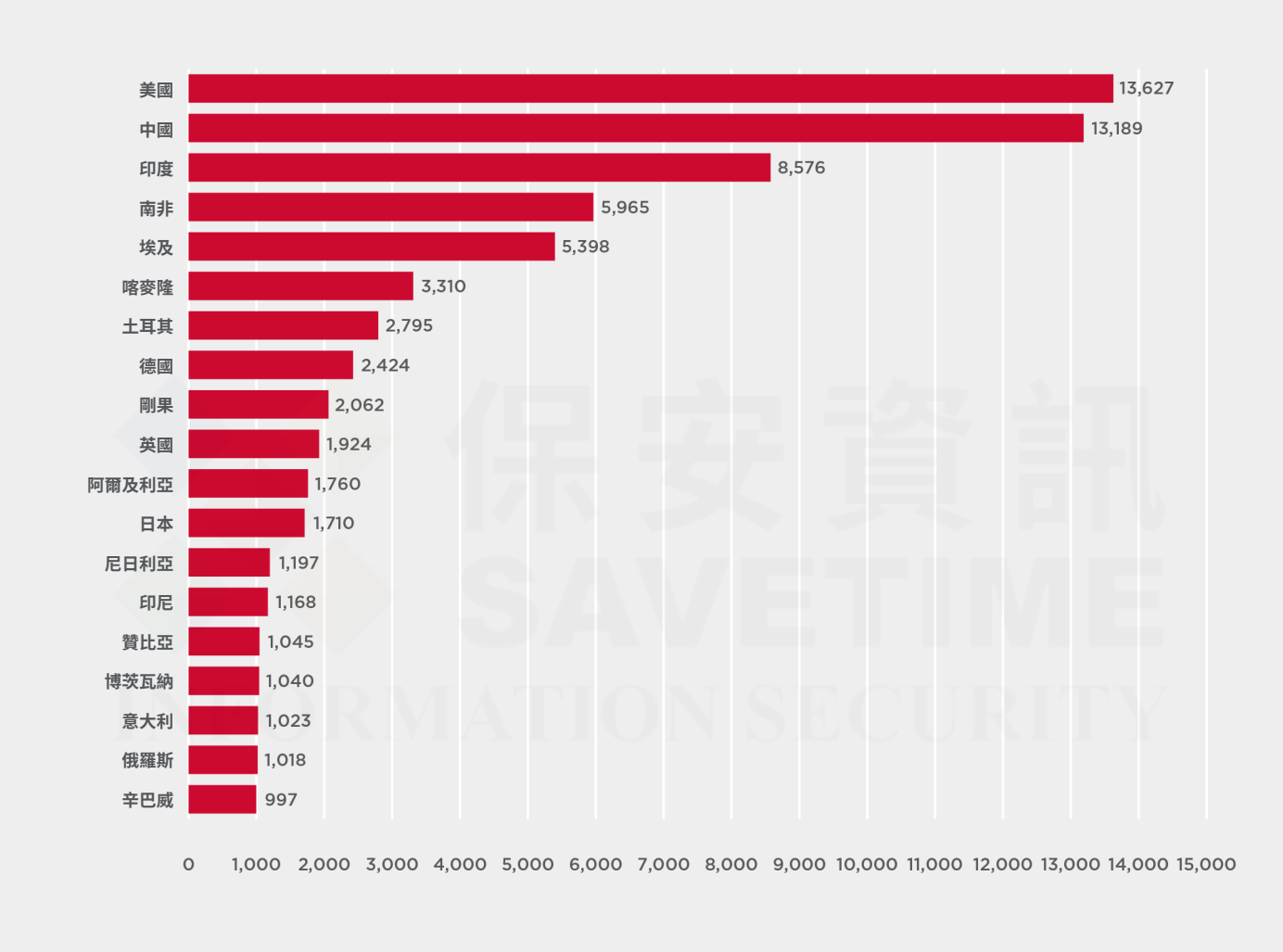
圖 3：2020 年 1 月至 2021 年 6 月按家族分列的遭受目標式勒索軟體攻擊影響的組織數量



當目標式勒索軟體攻擊以勒索軟體家族做區分時，兩種趨勢變得明顯。首先，新的威脅不斷湧現，並導致整體攻擊的增加。在分析的 24 個家族中，9 個在 2020 年 1 月活躍，然而在 2021 年 6 月活躍有 13 個。其次，少數前科累累的威脅攻擊者，如：Ryuk、Sodinokibi 和最近的 Avaddon，佔很大的攻擊比例。

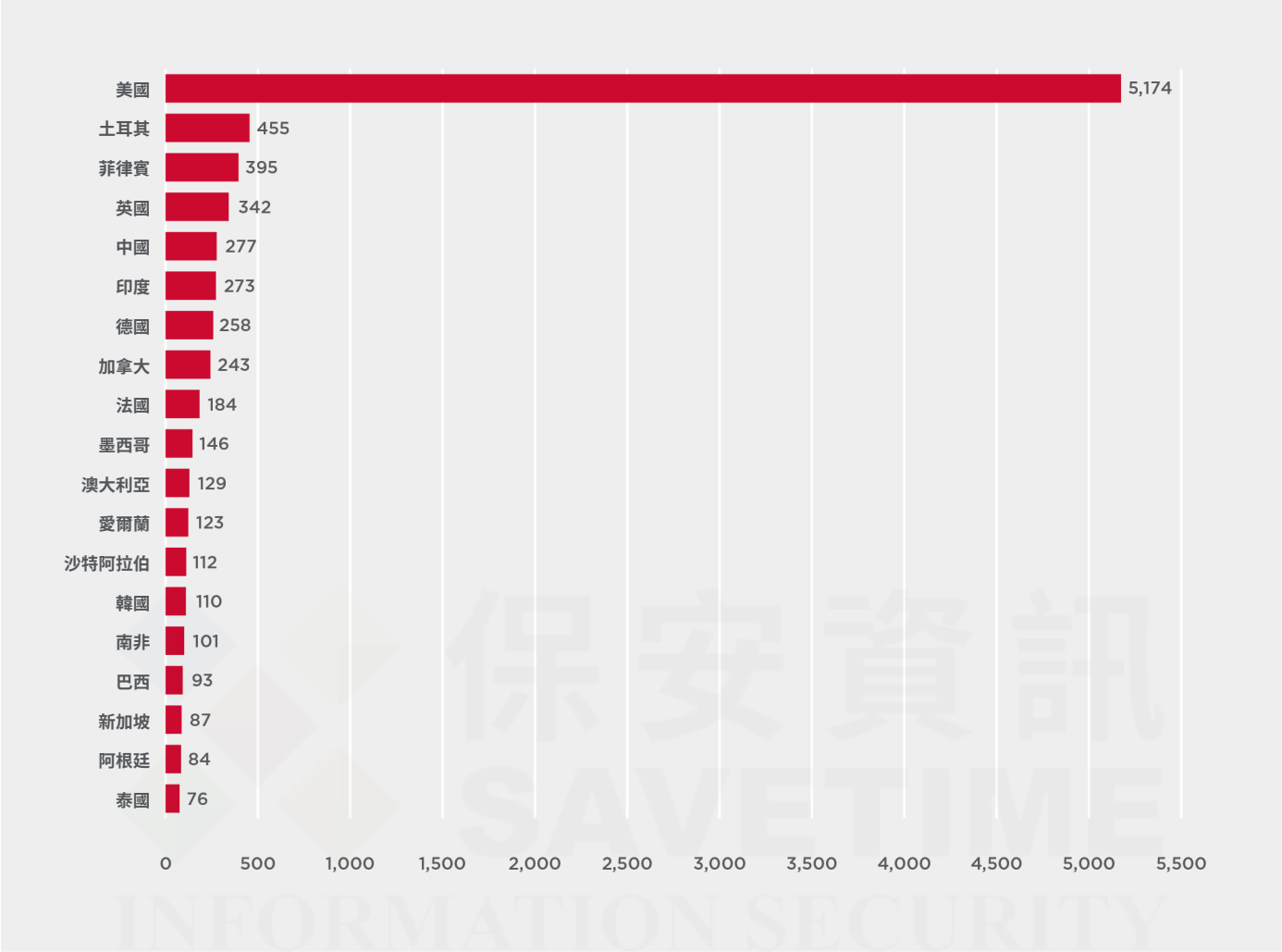
再次強調，這些統計數據應被視為賽門鐵克所阻止攻擊的代表性樣本。大多數攻擊很可能在勒索軟體部署前期，或在它們與任何特定的勒索軟體家族相關聯之前就被阻止。

圖 4：按國家／地區分列的勒索軟體檢測總數，2020 年 1 月至 2021 年 6 月



在檢視勒索軟體受害者排名時，會呈現另一個關鍵趨勢。雖然美國是受攻擊最頻繁的國家，但勒索軟體攻擊在全球範圍內普遍存在，過去 18 個月中，相當多的非洲國家出現在前 20 名中。非洲國家榜上有名在很大程度上是因為它似乎是攻擊者發起亂槍打鳥式之無差別勒索軟體攻擊的特別關注點，例如：透過垃圾郵件行動或利用已知漏洞。

圖 5：按國家 / 地區分列的目標勒索軟體檢測數量，2020 年 1 月至 2021 年 6 月



僅分析目標式勒索軟體攻擊時，會出現截然不同的情況。美國是迄今為止受影響最嚴重的國家，過去 18 個月遭攻擊次數是第二名國家（土耳其）的 11 倍之多。

受害者集中在美國並不奇怪。作為一個擁有商務高度發達的富裕大國，它自然是有針對性的勒索軟體攻擊之主要目標。記錄在案的幾個勒索軟體集團表示，他們主要（如果不是唯一）針對美國的組織。

雖然土耳其和菲律賓也佔據突出地位可能令人驚訝，但這與往年的統計數據一致，這兩個國家也都進入前五名。

應該注意的是，與前面列出計算組織數量的目標勒索軟體統計數據不同，該統計數據顯示檢測到目標勒索軟體家族的電腦數量。在按地理區域分析攻擊時，需要採用不同的方法，因為目標勒索軟體的許多受害者在多個國家／地區都用營運據點。

加劇威脅：勒索軟體即服務

勒索軟體構成威脅的一個關鍵因素是勒索軟體即服務 (RaaS) 出現。雖然成功的有針對性的目標式勒索軟體攻擊可能非常有效，但它對攻擊者缺點之一是它可能非常耗費人力。典型攻擊涉及各個步驟，包括憑證盜竊、特權提升、橫向移動、資料外洩、備份刪除和有效酬載部署，通常需要攻擊者的積極參與。因此，勒索軟體攻擊者可以執行的攻擊次數受到其可用人力的限制。

成功勒索軟體開發商意識到他們可透過招募其他攻擊者 (稱為聯盟合作機構) 來增加收入，並為他們提供攻擊軟體／工具的使用權限以換取分潤。這種營運模式現在已經高度發展，多數備受矚目的目標式勒索軟體開發商，都在營運某種形式的 RaaS 業務。

現有證據表明存在不同類型的聯盟合作關係，但目前的基本範本包含勒索軟體開發商提供對勒索軟體本身的使用權、代管洩露資料以及處理贖金談判。據報導，在某些情況下，勒索軟體開發商會為聯盟成員公司提供完整的營運手冊。然而，聯盟成員公司通常會使用他們自己的 TTPs。隨著時間的推移，賽門鐵克經常看到攻擊者使用相同的 TTPs，但不同的酬載。還有一些證據表明，攻擊者同時與多個勒索軟體開發商有聯盟合作關係（請參閱案例研究：周遊在不同聯盟之間的左右逢源營運模式）。

雖然一些勒索軟體開發商似乎只營運 RaaS 商業模式，但其他業者則更加親力親為，並將繼續自己發起攻擊。聯盟成員公司要求的性質也可能有所不同。已經觀察到有幾個為“存取代理”做的廣告，這表明他們只是在尋找一種進入潛在受害者網路的方法，並有意自己進行其餘的攻擊。

聯盟成員公司的出現，使得勒索軟體威脅態勢對於網路安全防護來說更加複雜，因為相同的勒索軟體都可以由多個不同的威脅參與者拿來發動攻擊，不同的攻擊者也將採用不同的 TTPs。

案例研究：周遊在不同聯盟之間的左右逢源營運模式

大多數勒索軟體聯盟成員公司似乎並不完全與單一個勒索軟體開發商結盟。當勒索軟體開發商下線或退休時，他們的許多聯盟成員將轉移到另一個 RaaS 營運商。

例如：當 Leafroller (又名 Revil) 集團在 2021 年 7 月上旬突然將其 Sodinokibi 勒索軟體營運下線時，似乎一些其聯盟成員公司轉而投向競爭對手轄下。在 Sodinokibi 失踪後，與 LockBit 有關聯的攻擊顯著增加，賽門鐵克發現證據表明，至少有一個前 Sodinokibi 聯盟成員現在正在使用 LockBit。以往該攻擊者使用一致的 TTPs 將 Sodinokibi 傳送給受害者，直到 2021 年 7 月才改採 LockBit 提供的有效酬載。

來自該攻擊者的攻擊始於一個名為 mimi.exe 檔案，該檔案是一個安裝程式，會植入許多密碼轉儲工具。在勒索軟體啟動之前，立即執行大量命令以停用各種服務、阻止對遠程桌面協議 (RDP) 的存取、刪除陰影複製……等。該攻擊者始終將其勒索軟體有效酬載命名為“svhost.exe”在他們過渡到 LockBit 後，這種做法一直保持不變。

勒索軟體威脅集團

Miner

別名：WizardSpider (* 巫師蜘蛛)

勒索軟體家族：Ryuk、Conti、GoGalocker (不活躍)、MegaCortex (不活躍)

開始活躍時間：2014

據判定 Miner 至少從 2014 年 6 月開始，在金融欺詐行動中使用 Dyre 銀行木馬開始活躍。2015 年 11 月 Dyre 變得不活躍，2016 年 9 月出現一種名為 Trickbot 新金融木馬。它隨後與 Miner 組織相關聯，因為 Trickbot 和 Dyr 似乎出於同一位作者。

Trickbot 最初開發目的是作為金融木馬，能夠在受害者使用網路銀行線上應用程式時，執行瀏覽器的中間人攻擊 (MitB) 以攔截線上交易。此後，它已被重新用作憑據竊取器並充當其他惡意軟體的散布通道。

Miner 還在 2020 年 4 月推出稱為 BazarLoader 和 BazarBackdoor 的新惡意軟體。與 Trickbot 一樣，BazarLoader 透過垃圾郵件行動傳播，並且可以傳遞第二階段 BazarBackdoor 有效酬載。與 Trickbot 不同的是，Bazar 系列似乎主要是為分發惡意軟體而開發。

2018 年，該集團使用 Ryuk 勒索軟體跨足到針對性的勒索軟體。Ryuk 是源於較舊 Hermes 勒索軟體家族，它似乎是從原始開發人員那裡獲得。

Ryuk 攻擊經常使用 Trickbot 和 Emotet 等殭屍網路作為感染媒介。然後使用諸如 CobaltStrike 和 Metasploit 等公開可用的惡意軟體來探索網路以進行橫向移動並增加權限。完成此步驟後，攻擊者將獲得對域控制器的管理權限。然後，攻擊者使用透過 PsExec 部署的批次檔，來停用和刪除整個環境中的備份／恢復功能和安全服務。

2019 年期間，Miner 開始使用兩個新的勒索軟體家族，GoGalocker（又名 LockerGoga）和 MegaCortex。兩者除與 Ryuk 共

享程式碼外，賽門鐵克的分析還發現，這三個勒索軟體家族使用的命令和控制 (C&C) 基礎架構存在重疊。涉及 GoGalocker 和 MegaCortex 的攻擊於 2020 年初停止。

Miner 隨後與 Conti 勒索軟體相關聯，該勒索軟體於 2019 年 12 月首次出現。有人猜測 Conti 是在 RaaS 營運模式下專門為聯盟成員公司特別開發，但這仍未得到證實。

Ryuk 和 Conti 都使用非常相似的 TTPs 進行分發。賽門鐵克 2021 年 5 月的一項調查發現，用於提交兩者的工具存在大量重疊。這些攻擊涉及廣泛使用 CobaltStrike 的變種。在某些情況下，感染媒介似乎是透過 IcedID 惡意軟體，該惡意軟體提供稱為 Longlist 惡意軟體，而該惡意軟體又用於安裝 CobaltStrike。

案例研究：BazarLoader 攻擊中的社交工程要素

最近一次與 Miner 集團有關的 BazarLoader 惡意軟體攻擊行動發現，攻擊者使用一定程度的社交工程手法，以便將惡意軟體推送到受害者網路上。該行動於 2021 年 7 月針對多個大型組織，從受害者網路上一台電腦上出現的惡意 Excel 檔案開始。

雖然最初的感染媒介並未在所有情況下都得到確認，但在一個已知的案例中，攻擊開始向員工發送魚叉式網路釣魚電子郵件。該電子郵件聲稱收件人正在處理最近一場車禍的汽車保險理賠。受害者被要求依指示的電話號碼回電客服電話，以提供更多資訊。這封電子郵件的說服力足以讓員工致電客服。電話交談後他們被欺騙指引至某一個網址，該網頁導致下載惡意的 Excel 檔案。

使用電話讓目標下載可疑檔案的手段是為了避免被發現。來自未知寄件者電子郵件中的可疑附件或鏈接，很可能會被安全軟體的自動過濾機制給攔截或引起收件人的懷疑。終端使用者手動輸入網址一般認為不太會是個惡意的網址，所以戒心就鬆懈了。

攻擊者在受感染的電腦上建立一個新目錄，並以新名稱將 Certutil 複製到該目錄：

CSIDL_COMMON_APPDATA\epvv2e\epvv2e.exe

這種偽裝技術以前在 Kaseya 攻擊中使用過，目的是隱藏對 Certutil 的惡意使用。

Certutil 用於下載惡意 DLL 檔案。這被確定為 BazarLoader。賽門鐵克沒有觀察到攻擊者成功部署有效載荷。然而，這些 TTPs 的關聯之前的勒索軟體攻擊，表明早期勒索軟體活動的可能性很大，很可能涉及 Ryuk。

Leafroller (* 壓葉機)

別名：REvil

勒索軟體家族：Sodinokibi (不活躍)、Gandcrab (不活躍)

開始活躍時間：2018

Leafroller 在 2019 年 4 月至 2021 年 7 月期間，使用 Sodinokibi 勒索軟體進行有針對性的目標式勒索軟體攻擊。眾所周知，該集團採用 RaaS 營運模式與聯盟成員公司合作。與許多勒索軟體集團一樣，Leafroller 及其聯盟成員公司通常會在加密之前竊取受害者資料，將樣本發佈到公開網站。然後攻擊者試圖透過威脅，如果不支付贖金就發布機敏資訊，施加更大的壓力敲詐受害者。

在開發 Sodinokibi 之前，該集團參與較舊的勒索軟體 Gandcrab 的攻擊，從原始開發人員那裡獲得其程式碼。當它過渡到 Sodinokibi 時，它與 Gandcrab 共享的一些聯盟成員公司繼續與該集團合作。

Leafroller 以針對知名組織而聞名，以最大限度提高他們可以勒索的贖金金額。其最著名的受害者之一是號稱全球最大外匯公司 Travelex，該公司於 2020 年 1 月遭到攻擊，並為勒索軟體營運商帶來 230 萬美元的贖金。

Leafroller 還因經常開展新的 TTPs 而聞名。在 2020 年期間，有人觀察到掃描受害者網路以查找信用卡或銷售點 (POS) 軟體。目前尚不清楚攻擊者是否將此軟體作為加密或資料竊取的目標。2021 年 7 月，Sodinokibi 被用於涉及 Kaseya 軟體的新型勒索軟體供應鏈攻擊（請參閱案例研究：勒索軟體供應鏈攻擊）。

在 Kaseya 攻擊後不到兩週，屬於 Leafroller 的基礎設施和網站就下線。與該組織相關的暗網和明網基礎設施均受到影響，包括贖金談判網站、數據洩露網站和 C&C 伺服器。該組織失踪的原因仍不清楚。然而，在撰寫本文時，還沒有證據證明新的 Sodinokibi 活動。

Hispid (* 硬皮)

別名：EvilCorp、Indrik Spider、TA505

勒索軟體家族：BitPaymer (已退休)、DoppelPaymer、WastedLocker、Hades、Phoenix Locker

開始活躍時間：2011

Hispid 是老牌的網路犯罪分子，自 2011 年左右開始活躍。該組織最初參與金融欺詐，曾負責開發 Dridex 銀行木馬。在鼎盛時期，Dridex 傳遞網路威脅前科累累，以大量垃圾郵件的形式分發到數百萬個電子郵件地址。Hispid 是一個成熟的網路犯罪集團，已經活躍大約 10 年。該組織最初與金融詐欺有關，Dridex 銀行木馬即為該組織所為，在 2017 年時，該組織將重心轉向勒索軟體。2019 年，美國財政部外國資產控制辦公室 (OFAC) 對 Hispid 實施制裁，禁止受害者向該集團付款。眾所周知，該組織經常重新命名其勒索軟體，可能為了規避這些制裁並從美國公司那裡獲得付款。

約在 2017 年左右，該組織將重心轉向目標式勒索軟體上，並推出 BitPaymer 勒索軟體家族。它後來推出第二個勒索軟體家族，稱為 DoppelPaymer，它基於相同的程式碼，儘管有一些細微的差別。據報導，DoppelPaymer 是為聯盟成員公司使用而開發的，但賽門鐵克尚未能夠證實這一點。

與 Miner 繼續使用 Trickbot 的方式類似，Hispid 在轉向勒索軟體後繼續使用 Dridex 一段時間，將惡意軟體重新改造成勒索軟體攻擊的前導工具。

2019 年 12 月，兩名俄羅斯國民在美國因與該集團活動有關的多項指控被起訴。並懸賞 500 萬美元以獲取致使他們被捕或定罪的線索。

2020 年 5 月，Hispid 隨即改弦易轍並推出一個名為 WastedLocker 新勒索軟體家族。攻擊始於一個名為 SocGholish 惡意基於 JavaScript 的框架，該框架偽裝成軟體更新。賽門鐵克在 2020 年 6 月一項調查發現，SocGholish 入侵超過 150 多個網站，其中並包括數十個美國新聞網站。

一旦攻擊者在受害者的網路上取得立足點後，就會使用 PowerShell 下載並執行載入器。該載入器包含一個 .NET 注入器以及一個用於 CobaltStrike 信標的載入器。

CobaltStrike 信標可用於執行命令、注入其他程序、提升當前程序或假冒其他進程，以及上傳和下載檔案。來自 PowerView 的 Get-NetComputer 命令被攻擊者重命名為隨機名稱。然後，此命令將搜索 ActiveDirectory 資料庫中的所有物件。

權限升級是使用被公開記錄的軟體授權使用者介面 (slui.exe) 工具的技術，這是一個負責啟動和更新 Windows 作業系統的 Windows 命令列公用程式。

攻擊者使用 Windows Management Instrumentation 命令列公用程式 (wmic.exe) 在遠端電腦上執行命令，例如：新增使用者或執行額外下載的 PowerShell 腳本。Cobalt Strike 還用於使用 ProcDump 執行憑證轉儲和清空日誌檔案。

為部署勒索軟體，攻擊者使用 Windows Sysinternals 工具 PsExec 啟動用於管理 Windows Defender (mpcmdrun.exe) 的合法命令列工具，以停用對所有下載檔案和附件的掃描，刪除所有已安裝的定義檔，並且在某些情況下停用即時監控。

然後使用 PsExec 啟動 PowerShell，它使用 win32_service WMI 類檢索服務並使用 net stop 命令停用這些服務。在 Windows Defender 被禁用並且整個組織服務停止後，PsExec 被用來啟動 Wast-edLocker 勒索軟體本身，然後開始加密檔案並刪除磁碟陰影副本。

2021 年 3 月，該組織推出一種名為 Hades 的勒索軟體新變種，該變種與 WastedLocker 存在明顯的程式碼重疊。Hispid 很可能開發 Hades 勒索軟體，以應對來自美國財政部外國資產控制辦公室 (OFAC) 於 2019 年實施的制裁，該制裁禁止受害者向該集團付款。

據報導，在撰寫本文時，該集團定期重新命名其勒索軟體，原因是擔心受害者不會支付贖金，以免他們違反美國的制裁。Hades 後來更名為 Phoenix Locker，截至 2021 年 6 月，它使用的新名稱為 PayloadBin 是早先 Babuk 集團已經使用過的名稱，這可能是為了愚弄受害者，讓他們誤認為是被另一個攻擊者所感染。

Thysanura

別名：Avaddon

勒索軟體家族：Avaddon

開始活躍時間：2019

至少從 2019 年開始，Thysanura 就以鎖定大型組織發起目標式勒索軟體行動而聞名。該集團經常使用遠端存取登錄憑據（例如：RDP 和虛擬私人網路 (VPN)）來攻擊受害者。

Thysanura 採用 RaaS 營運模式，並在俄語網路犯罪論壇上做廣告。該集團採用多種勒索手法迫使受害者付款。

除了加密檔案之外，它還威脅要洩露從受害者那裡竊取的資訊，並且在 2021 年 1 月，它開始告訴沒有支付贖金的受害者，它將透過分散式拒絕服務 (DDoS) 攻擊襲擊他們。迄今為止，尚未確認該組織是否曾經這樣做。

在攻擊者獲得對受害者網路的存取權限，他們會映射網路並識別備份以進行刪除和／或加密。使用 Avaddon 的攻擊者使用以下工具來入侵受害者：

- PowerShell
- WMIC.exe (WMI -Windows Management Instrumentation)
- Svchost.exe (Service host system process)
- Taskhost.exe (Host protocol)

2021 年 6 月 11 日，該組織宣布將關閉其業務並為受害者釋放解密密鑰。該駭客集團向新聞媒體 BleepingComputer 發送近三千個解密密鑰，之後安全公司 Emsisoft 製作一個免費的公開解密工具。在撰寫本文時，尚不清楚該組織的離開是否為永久性。

Syrphid

別名：LockBit

勒索軟體家族：LockBit

開始活躍時間：2019

LockBit 勒索軟體於 2019 年 9 月首次出現，由於被其加密過的檔案副檔名為 .ABCD，所以當時也被稱為 ABCD 勒索軟體。2020 年 1 月，Syrphid 透過建立聯屬成員營運的 RaaS 業務模式，擴大業務範圍。

眾所周知，使用 LockBit 的攻擊者會透過對運行過時 VPN 服務的 Web 伺服器，進行暴力攻擊來入侵組織。據報導，它還使用大規模漏洞掃描、網路釣魚和帳號填充（Credential Stuffing）作為攻擊媒介。據報導，它還購買地下論壇上已經被入侵伺服器的存取權限。

在某些情況下，攻擊者會暴力破解管理員憑證以貫穿整個網路。眾所周知，他們還使用後漏洞利用框架來進行特權提升和橫向移動。

在加密檔案之前，Syrphid 將嘗試識別目標網路上的機敏資料並將其匯出到外部代管主機。聯盟成員公司並為每個受害組織使用專用的獨特勒索軟體版本。

涉及 Lockbit 的攻擊在 2021 年 7 月顯著增加，並且有一些證據顯示 Syrphid 正試圖招募前 Sodinokibi 聯盟成員公司（參見案例研究：周遊在不同聯盟之間的左右逢源營運模式）。

Snakefly

別名：Clop

勒索軟體家族：Clop

開始活躍時間：2019

Snakefly 以開發 Clop 勒索軟體而聞名，並經常利用 Hispid（又名 EvilCorp）所營運的惡意軟體散布通路。該駭客集團與一些備受矚目的事件有關，包括 2019 年對馬斯特里赫特 (Maastricht) 大學的攻擊。

該集團的攻擊通常始於從先前被入侵的帳戶發送的惡意電子郵件，以使其更具說服力。此電子郵件包含一個 HTML 附件，該附件會重導向到一個受感染的網站，然後該網站會發送一個包含惡意巨集的檔案，該巨集會植入 Get2 載入器。然後，它會下載 SDBot 惡意軟體或其他遠端存取工具 (RAT)，以幫助攻擊者在網路中橫向移動、洩露資料並下載 Clop 勒索軟體。

一些勒索軟體有效酬載具有已簽章的憑證，可以讓它們看起來合法並可能繞過安全措施而得逞。執行 Clop 後，它會搜索要移除的安全軟體。第三方已經看到它移除或停止 Malwarebytes、ESET 和 Microsoft 的安全軟體。勒索軟體會加密檔案並為以加密檔案新增 .clop 的副檔名，然後在電腦上放置勒索信說明。

眾所周知，在加密之前從受害者那裡竊取檔案並威脅要公諸於世，除非支付贖金。與當今大多數勒索軟體集團一樣，該集團還營運著一個 Clop 資料洩露網站，該網站發布從拒絕支付贖金的受害者那裡竊取的機敏資訊。

Coreid（* 核芯)

別名：Darkside

勒索軟體家族：Darkside、BlackMatter (尚未證實)

開始活躍時間：2020

Coreid 在很短時間內就已經是前科累累的目標式勒索軟體集團之一，並被用於許多野心更大的攻擊，最引人注目的是 2021 年 5 月對美國殖民管道 (Colonial Pipeline) 的攻擊，該攻擊中斷對美國東海岸的燃料供應。

Coreid 在 RaaS 模式下營運，與聯盟成員機構合作進行勒索軟體攻擊並分潤。與大多數勒索軟體攻擊者一樣，與 Coreid 相關的攻擊會竊取受害者的資料，然後該集團威脅要公布這些資訊，以進一步迫使受害者支付贖金要求。

一旦進入受害者的網路，使用 Darkside 的攻擊者通常會開始竊取資料、憑證和其他機敏資訊。攻擊者還試圖透過網路橫向移動，以獲得對域控制器 (DC) 的存取權限。一旦進入 DC，他們就會洩露機敏資訊，並使用 PowerShell 下載 DarkSide 的二進位檔。

眾所周知，攻擊者會在 DC 上使用公司名稱建立一個共享資料夾，並將 Darkside 二進位檔案複製到其中。隨後，攻擊者使用 BITSAdmin 將勒索軟體二進位檔案從共享檔案夾散布到網路上的其他電腦。

Coreid 聯盟成員公司使用 TOR (洋蔥路由器-- The Onion Router) 與受害者聯繫並管理勒索軟體的運作。據報導，Coreid 鼓勵其聯盟成員公司在勒索軟體要求中請求門羅幣，這可能是由於該加密貨幣的高度匿名性。

Coreid 在殖民管道攻擊事件後，其一些基礎設施下線後似乎在變得不活躍。

2021 年 7 月下旬，媒體報導將 Coreid 與名為 BlackMatter 的新勒索軟體威脅關聯起來。該勒索軟體被認為使用與 Darkside 相同的慣用加密機制。在接受 Recorded Future 採訪時，BlackMatter 的開發人員否認這種關係，稱“我們過去曾與 Darkside 團隊合作過，但我們不是他們，儘管我們對他們很熟悉。”然而，區塊鏈分析公司 Chainalysis 也發現這兩種威脅之間的金流關聯性，並得出結論認為 BlackMatter 是由 Coreid 所開發。賽門鐵克的評估是，現在對 BlackMatter 做出明確的歸屬還為時過早。

Hornworm

別名：RagnarLocker、VikingSpider

勒索軟體家族：RagnarLocker

開始活躍時間：2020

Hornworm 與 RagnarLocker 勒索軟體有關。RagnarLocker 於 2020 年初首次出現，並於 2020 年 11 月成為 FBI 緊急警報的對象。FBI 報告稱，它對一家大型公司網路上的電腦進行加密，並要求支付 1,100 萬美元的贖金，並威脅如果不付贖金將要公布 10 TB 的被盜資料。從那時起，它對美國的多家其他組織發起勒索軟體攻擊。

據報導，為了避免被發現，RagnarLocker 在每台受感染的電腦上都部署完整的虛擬機。在某些情況下，有效酬載以 MSI 安裝套件的形式提供，其中包括舊版 Oracle VirtualBox (Sun xVM VirtualBox 版本 3.0.4) 的工作安裝和名為 micro.vdi 的虛擬磁碟映像檔 (VDI) -- Windows XP SP3 作業系統的精簡版映像，稱為 MicroXP v0.82。該映像檔包含一個 49KB 的勒索軟體有效酬載。雖然 Hornworm 可能率先採用這種戰術，但賽門鐵克此後觀察到使用其他有效酬載的攻擊者也試圖從虛擬機上運行它們。

RagnarLocker 為被其加密過的檔案，以 .RGNR_<ID> 附檔名來重新命名。其中 <ID> 是該電腦 NETBIOS 名稱的雜湊值 (Hash)。攻擊者自稱為 RAGNAR_LOCKER，在電腦上留下 .txt 勒索信／說明，說明如何支付贖金並接收解密密鑰。眾所周知，該組織經常更改混淆技術，並擁有 VMProtect、UPX 和自訂打包演算法。

據報導，Hornworm 在加密之前從受害者組織中竊取資料，並威脅要公開這些資料，除非支付贖金。為此，它使用一個代管在 Tor 上的專用資料洩露網站。

案例研究：Hornworm 與 FIN8 的合作

Hornworm 可能與 FIN8 網路犯罪集團建立合作關係。2021 年初，有人看到 FIIN8 將 RagnarLocker 勒索軟體部署到美國一家金融服務公司被入侵的電腦上，這是賽門鐵克第一次看到 FIN8 在被它入侵的電腦上安裝勒索軟體。

已知被 FIN8 組織使用的 BADHATCH 惡意軟體，於 2021 年 1 月透過 PowerShell 在該組織的電腦上啟動。從被濫用的合法 sslip[.]io 服務下載多個 PowerShell 腳本，已知該服務被 FIN8 所濫用。PowerShell 還用於從 WMI 物件下載未知內容。FIN8 也使用 PowerShell 將惡意工具部署到受害者電腦上。

還部署並執行一個鍵盤側錄軟體。2021 年 2 月，在網路上首次發現可疑活動的三個半星期後，開放原始碼工具 Rclone 被用於竊取資料。不到一個月後，也就是 3 月中旬，Ragnar Locker 勒索軟體被另一種稱為 Safebitsloader 工具植入到網路上。

雖然該網路上的 FIN8 和 RagnarLocker 活動可能是由兩個不同的攻擊者所發動，但有幾件事顯示情況並非如此。這包括 BADHATCH 和 Rclone 都是從同一 IP 位址下載，並且勒索軟體和 PowerShell 腳本都下載到受感染電腦上的同一目錄 (%WINDIR%\temp)。

Leaftier

別名：Babuk

勒索軟體家族：Babuk

開始活躍時間：2021

Leaftier 在 2021 年初試啼聲就一鳴驚人，以其對於資料洩露勒索的高度關注而著稱。該集團最初採用 RaaS 營運模式運作，並使用雙重勒索戰術，從受害者那裡竊取資料以及加密檔案。然而，Leaftier 後來宣布放棄加密，只關注資料竊取，以此作為向受害者勒索贖金的一種方式。

Babuk 被發現與另一個名為 Vasa Locker 的勒索軟體威脅具有高度相似性。McAfee 分析的 Vasa 樣本與 Babuk 共享大約 86% 相同程式庫，並且是在 Babuk 首次發布前一個月編譯。Babuk 和 VasaLocker 背後的參與者很可能是同一個人，或者彼此之間有有密切關聯。

2021 年 4 月下旬，Leaftier 宣布將終止其聯盟合作計劃，並轉向不依賴加密受害者電腦的勒索模式。該集團表示，它將專注於要求從受害者那裡竊取的資訊來索取贖金。

2021 年 5 月，Leaftier 宣布開發一個“獨立洩漏”平台，該平台將成為供其他參與者使用的資料洩密網站。與此同時，該集團更名，將其新洩密網站 (Payload.bin) 上的名稱從 Babuk 更改為 Payload Bin。

據報導，2021 年 7 月上旬，Leaftier 似乎又開始使用勒索軟體來攻擊企業網路。該駭客集團開始使用新版本的 Babuk 勒索軟體 (Babukv.2.0) 並轉移到一個新的資料洩露網站。

Leaffolder

別名：Maze、Egregor

勒索軟體家族：Maze、Egregor

開始活躍時間：2019

Leaffolder 活動的第一個證據可以追溯到 2019 年 5 月，當時出現 Maze 勒索軟體。Leaffolder 以率先在加密之前從受害者組織竊取資料的戰術而聞名，並威脅要公開這些資料，除非支付贖金。該戰術很快被多家其他有針對性的勒索軟體集團仿效。

Maze 主要散布媒介是 Fallout 和 Spelevo 漏洞利用工具包，受害者透過垃圾郵件行動被誘騙。一旦攻擊者獲得對網路上單台電腦的存取權限，他們就會下載商品化惡意軟體 CobaltStrike 和 Metasploit 框架，以便在網路中橫向移動並探索有機可趁的電腦。

2020 年 10 月，Leaffolder 宣布將關閉 Maze 勒索軟體運作。該集團隨後與名為 Egregor 的新勒索軟體業者相關聯，該業者在 Maze 退役後不久出現。許多以前的 Maze 聯盟成員移轉到 Egregor 旗下。

Egregor 的聯盟成員公司於 2021 年 2 月受到執法行動的制約。據了解 Egregor 自此事件發生以來已變得不活躍。

Canthroid

別名：UNC2447

勒索軟體家族：Thieflock

開始活躍時間：2021

Canthroid 於 2021 年初首次出現，當時它開始使用 Thieflock 發動目標式勒索軟體攻擊。它也是一個 RaaS 營運模式。

迄今為止，它以利用 SonicwallVPN (CVE-2021-20016) 中的零時差漏洞攻擊受害者而聞名。該漏洞已於 2021 年 2 月釋出修補，但 Canthroid 攻擊還再使用未修補版本之軟體的組織。成功利用該漏洞後，將允許攻擊者建立自己的憑證並加入目標網路。

發現到一旦成功入侵網路後，該集團就會使用 SoftPerfect Network Scanner，這是一種公開可用於探索主機名稱和網路服務的工具。還已知使用 SombRAT，這是一種自訂的遠端存取工具，允許攻擊者下載更多工具並保持與 C&C 伺服器的通信。

在加密之前，該組織會從目標網路中竊取資料。據報導，攻擊者使用 pCloud，這是一種加密的雲存儲服務。

工具、戰術和程序 (TTPs)

大多數勒索軟體攻擊是一個多階段的過程，特別是有針對性的目標式勒索軟體攻擊通常會採取許多步驟和需要攻擊者相當高水準的靈機應變。一系列的工具、策略和程序 (TTPs) 用於滲透受害者的網路、竊取憑證，提升特權，在網路中橫向移動以及在多台電腦上部署勒索軟體有效酬載。

了解勒索軟體攻擊者使用的 TTPs 可以讓網路防御者對他們的組織如何受到威脅有更好的了解，並可以為防禦措施的輕重緩急提供一些指導。例如，Windows 工具（如 PsExec）經常被攻擊者濫用，減少具有管理員權限的帳戶數量，同時增加對管理員帳戶的保護可以降低被成功攻擊的風險。

表 1：最常見的勒索軟體 TTPs，2021 年 4 月至 2021 年 6 月

TTP	Percentage of Ransomware Investigations
Cobalt Strike	41%
PsExec	33%
Netscan	15%
Mimikatz	15%
Adfind	15%
Weirdloop	11%
IcedID	11%
SystemBC	7%
ProcDump	7%
Nsudo	7%
Disable Defender	7%
Delete Shadow Copies	7%
WMI	4%
rclone	4%
Qakbot	4%
BITSAdmin	4%

透過最近調查勒索軟體中發現前導工具的檢驗結果，賽門鐵克能夠了解哪些是勒索軟體攻擊中最常用的 TTPs。雖然最常用的工具是商品化惡意軟體 Cobalt Strike (在 41% 調查中可見)，但其中很大一部分是免費提供的兩用工具或作業系統功能，例如：PsExec 和 WMI。

- **Cobalt Strike**：現成的工具，可用於執行命令、注入其他程序、提升當前程序或假冒其他程序以及上傳和下載檔案。它表面上作為滲透測試工具具有合法用途，但總是被惡意行為者利用。
- **PsExec**：Microsoft Sysinternals 工具，用於在其他系統上執行程序。該工具主要由攻擊者用於在受害者網路上橫向移動。
- **NetScan**：SoftPerfect Network Scanner，一種公開可用的工具，用於探索主機名稱和網路服務。
- **Mimikatz**：這款免費提供的工具能夠變更權限、匯出安全憑證以及根據配置以純文字回復 Windows 密碼。
- **AdFind**：一個免費的工具，可用於查詢 Active Directory。
- **Weirdloop**：Cobalt Strike HTTPS Stager 載入器在 2021 年涉及 Ryuk 的一些攻擊中被使用。
- **IcedID**：殭屍網路惡意軟體最初是作為金融木馬被開發，但現在經常與勒索軟體攻擊者合作使用。
- **SystemBC**：商品化的惡意軟體，可以在受感染的電腦上打開後門，並使用 SOCKS5 代理協定與命令和控制 (C&C) 伺服器進行通信。
- **ProcDump**：Microsoft 系統內部工具，用於監視應用程式的 CPU 峰值和生成故障轉儲，但也可以用作一般程序轉儲應用程式。

- **Nsudo**：一種開放原始碼系統管理工具，可以被濫用以提升權限。
- **Windows Management Instrumentation (WMI) (wmic.exe)**：可用於在遠端電腦上執行命令的 Microsoft 命令列工具。
- **Qakbot**：最初作為金融木馬被開發的殭屍網路惡意軟體。
- **BITSAdmin**：一個 Microsoft 命令列工具，可用於建立、下載或上傳作業並監視其進度。

案例研究：勒索軟體供應鏈攻擊

雖然有針對性的目標式勒索軟體攻擊已被證明對攻擊者來說利潤非常豐厚，但這並沒有阻止他們不斷改進戰術。2020 年主要創新是在加密網路上的電腦之前竊取資料的做法，然後威脅要發布這些資料，除非支付贖金。資料洩露的威脅增加受害者組織的支付壓力。它還為攻擊者提供脅迫對可能已經能夠從備份中恢復加密系統之受害者就範的強大籌碼。

2021 年 7 月，使用 Sodinokibi 勒索軟體的攻擊者嘗試了一種新戰術：透過供應鏈攻擊傳遞勒索軟體。該攻擊涉及利用 KaseyaVSA 軟體中的零時差漏洞 (CVE-2021-30116)，該漏洞用於透過使用該軟體的多個代管服務提供商 (MSP) 入侵受害組織。

據了解，該勒索軟體已感染全球至少 1,500 個組織。大部分過程似乎是自動化，勒索軟體將在多個組織中同時爆發，估計是為了對受害者發動沒有預警的攻擊。這次攻擊的時間恰逢美國 7 月 4 日假期週末，當地的許多組織可能人手不足。

攻擊者利用該漏洞向 Kaseya VSA 客戶端發送惡意腳本和名為 agent.crt 的 ASCII PEM。植入程式偽裝在 ASCIIPEM 檔案中，該檔案在嘗停用 Microsoft Defender 後使用 Certutil 進行解碼。它植入了兩個資源，一個舊的但合法之 Windows Defender (MsMpEng.exe) 副本和一個自定義惡意載入器。植入程式將這兩個檔案寫入磁碟並執行 MsMpEng.exe，然後側加載並執行自訂載入器導出 (mpsvc.dll)。

這次攻擊是否為新趨勢的開始還有待觀察。攻擊的性質意味著它可能不如“傳統”的針對性勒索軟體攻擊有效。攻擊的自動化性質，意味著攻擊者不得不放棄在此類攻擊中採取的一些標準步驟，例如：資料洩露和備份刪除。

攻擊後不到兩週，Sodinokibi 幕後集團 Leafroller 就下線。這次失踪的原因仍不清楚，也不知道這是巧合還是與 Kaseya 攻擊事件有任何關聯。

攻擊發生幾週後，Kaseya 表示它已經獲得用於勒索軟體的解密工具。該公司表示，它已從“受信任的第三方”獲得解密工具，現在正在提供給受影響的客戶。

事發後，有報導指稱攻擊者獅子大開口，通用解密工具索價 7,000 萬美元，每個 MSP 需要 500 萬美元，或者每台加密電腦需要 4 萬美元。Kaseya 表示，它既無法確認也無法否認是否支付贖金以獲得解密工具。

感染媒介

目標式勒索軟體集團使用多種形形色色的散布方法。由於有針對性的勒索軟體攻擊的普遍性相對較低 (全世界可能只有這一起)，因此有時很難確認感染媒介。目標式勒索軟體集團經常從間諜組織那裡獲得線索，以在受害者的網路上獲得立足點。

二次感染

在過去的十二個月中，這已迅速成為勒索軟體集團最熱門的入侵方式之一。一般來說，它與用來群發大量夾帶惡意軟體的郵件的殭屍網路有關，因為它為勒索軟體集團提供大量潛在受害者。曾經用於金融欺詐的特洛伊木馬，例如：Trickbot，最近主要用作其他惡意軟體的散布通路，其中最著名的是勒索軟體。

在某些情況下，勒索軟體攻擊者已經控制殭屍網路，例如：擁有 Trickbot 殭屍網路的 Miner 集團。Trickbot 被視為 Ryuk 攻擊的前導部隊，這歸因於 Miner。同樣，Hispid 也利用他們自己的 Dridex 殭屍網路，該網路最初是為發動金融攻擊而構建，為他們提供一種將勒索軟體傳遞給組織的方法。

此後，其他攻擊者試圖複製這種攻擊模式，尋求與已建立的殭屍網路營運商合作。其中最值得注意的是 Conti 勒索軟體至少一個聯盟成員營運商使用 IcedID（請參閱案例研究：IcedID 和 Conti 合作）。

案例研究：IcedID 和 Conti 合作

賽門鐵克最近對涉及 Conti 勒索軟體的攻擊幾項調查發現，多起攻擊中存在一致的攻擊鏈，這表明至少有一名使用 Conti 的攻擊者已經開始與 IcedID 殭屍網路合作。

目標組織中惡意活動的第一個證據是目標網路上存在 IcedID。隨後，IcedID 被用於傳遞稱為 Longlist 的惡意軟體，該惡意軟體又用於安裝 Cobalt Strike。攻擊中使用的其他工具，包括公開可用的憑證轉儲工具 LaZagne 和 Adfind，這是一種免費的兩用工具，可用於查詢 Active Directory。

雖然 IcedID 是廣泛分佈的惡意軟體，但它與這些其他工具的存在，很可能顯示勒索軟體攻擊正在準備中。

網路釣魚

網路釣魚是使用最廣泛的感染媒介之一，發送給員工的電子郵件偽裝成與工作相關的信件 (發票及出貨明細、遞送確認等)。一些網路釣魚行動可能是無差別地大範圍傳送，可能會吸引受害者的電子郵件來提高命中率。在其他情況下，攻擊者可能會預先選擇他們的受害者，並向組織中選定的員工發送魚叉式網路釣魚電子郵件。

魚叉式網路釣魚行動可以針對目標量身定制，使用與組織業務相關的主題。如果收件人被誘騙打開惡意附件或點擊惡意鏈接，惡意軟體將被下載到受害者的電腦上，進而允許攻擊者開始在受害者的網路中移動。

惡意廣告

迄今為止，惡意廣告不被稱為勒索軟體的感染媒介，2020 年，WastedLocker 的營運商利用惡意廣告。有人觀察到該組織入侵媒體網站，以投放包含基於 JavaScript 的框架 SocGholish 惡意廣告，該框架偽裝成軟體更新。

漏洞利用

進入組織網路的另一條途徑是濫用在面向公眾服務的伺服器上運行有漏洞之脆弱軟體。迄今為止，在大多數情況下，沒有使用零時差漏洞，攻擊者多利用已公告 (已知) 卻未修補的軟體中漏洞，例如：JBoss 或 Apache Web 服務器。該戰術的主要使用者之一是現已解散的 SamSam 集團，該集團於 2019 年 11 月停止營運。最近，Canthroid 集團利用 Sonicwall VPN 中的零時差漏洞 (CVE-2021-20016），而 Proxylogon Exchange Server 漏洞也被多個攻擊者濫用來執行勒索軟體攻擊。

安全性不夠的服務

另一個感染媒介來自於安全性不夠的服務。Crysis (又名 Dharma) 一再被觀察到透過安全性不夠的 RDP 服務攻擊組織，利用被洩露或弱憑證。觀察到現已解散的 GandCrab 集團，在網際網路上掃描暴險的 MySQL 資料庫，然後它感染惡意軟體。

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。

關於賽門鐵克

賽門鐵克公司 (Symantec) 已於 2019/11 合併入博通 (BroadCom) 的企業安全部門，Symantec 是世界首屈一指的網路安全公司，無論資料位在何處，賽門鐵克皆可協助企業、政府和個人確保他們最重要資料的安全。全球各地的企業均利用賽門鐵克的政策性整合式解決方案，在端點、雲端和基礎架構中有效地抵禦最複雜的攻擊。賽門鐵克經營的安全情報網是全球規模最大的民間情報網路之一，因此能成功偵測最進階的威脅，進而提供完善的防護措施。
若想瞭解更多資訊，請造訪原廠網站 https://www.broadcom.com/solutions/enterprise-security/enterprise-security-solutions 或
賽門鐵克解決方案專家：保安資訊有限公司的中文網站 https://www.savetime.com.tw/(好記：幫您.節省時間.的公司.在台灣)

保安資訊 SAVETIME INFORMATION SECURITY

保安資訊有限公司｜地址：台中市南屯區三和街 150 號
電話：0800-381500｜+886 4 23815000｜www.savetime.com.tw