白皮書

不斷演變的勒索軟體威脅態勢：預見驚濤駭浪的2022年

由賽門鐵克威脅獵手 (Threat Hunter) 團隊撰寫

目錄

簡介

勒索軟體是 2021 年的主要網路犯罪趨勢，在 2022 年也沒有改變的跡象。勒索軟體領域的大公司排名可能會發生變化，執法單位的取締、安全認知與防禦實作的提升以及後起之秀的急起直追，迫使現有的勒索軟體家族接受並適應這種適者生存的競爭環境，但攻擊活動仍然層出不窮，完全沒有減緩的徵兆。像 Ryuk、REvil ／ Sodinokibi 和 Darkside 這樣重量級的大公司，在過去一段時間裡已經式微或消失，但更多像 Hive 和 AvosLocker 這樣的新公司便脫穎而出。

雖然排名起起落落，勒索軟體開發商及其聯盟成員使用的攻擊手法、技術與過程 (TTPs) 一再翻新，但勒索軟體由於其獲利能力難以取代，不太可能消失或急劇下降。只有在出現對網路犯罪分子來說更有利可圖和更能駕輕就熟的機會時，勒索軟體才有可能消失，但目前看來這種可能性並不大。

網路保險上的變化--例如：保險公司拒絕承保勒索軟體攻擊--或監管單位對加密貨幣的監管加強，是最有可能影響勒索軟體開發商獲利的兩個外部因素。加密貨幣圈的任何變化都可能影響勒索軟體開發商，但我們已經看到一些網路保險公司對勒索軟體的理賠變得日漸嚴格，這使得該領域備受矚目。許多公司依靠保險理賠來支付贖金並從勒索軟體攻擊中復原。

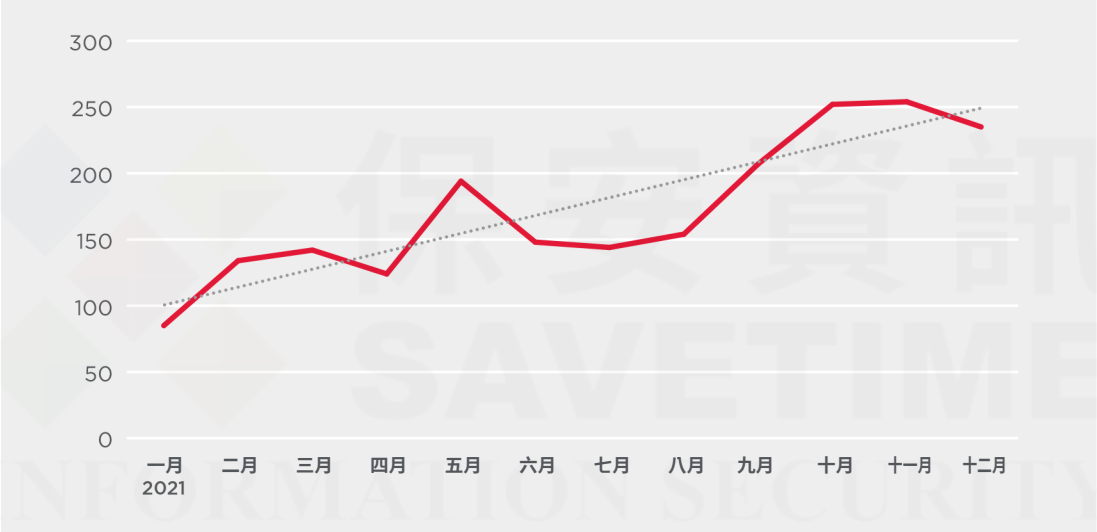
本文的一些主要發現包括：

- 2021 年，針對性的目標式勒索軟體攻擊呈上升趨勢，在 2021 年第一季度和最後一個季度之間幾乎翻了三倍。
- 勒索軟體攻擊參與者使用的手法、技術與過程 (TTPs) 總是不斷推陳出新。雖然攻擊參與者經常利用駭客工具和商業化的惡意軟體，但由於極力隱蔽他們的活動不被發現，直到他們能夠部署他們的有效酬載，兩用工具和就地取材戰術仍是大受歡迎。
- 檯面上主要勒索軟體家族不斷變化，這往往是由於被取締、制裁或執法部門加強審查的影響。像 Pinion (Hive) 和 Sirex (AvosLocker) 這樣的新進者現在非常活躍，而 Miner (Conti) 也繼續在勒索軟體舞臺上占有一席之地。
- 2021 年底，Emotet 僵屍網路的回歸有可能對 2022 年勒索軟體的態勢發展投入超級震撼彈。

勒索軟體趨勢

從圖 1 中可以看出，2021 年遭針對性的目標式勒索軟體攻擊的組織數量呈上升趨勢。

圖 1：針對性的目標式勒索軟體攻擊的數量，2021 年 1 月至 12 月

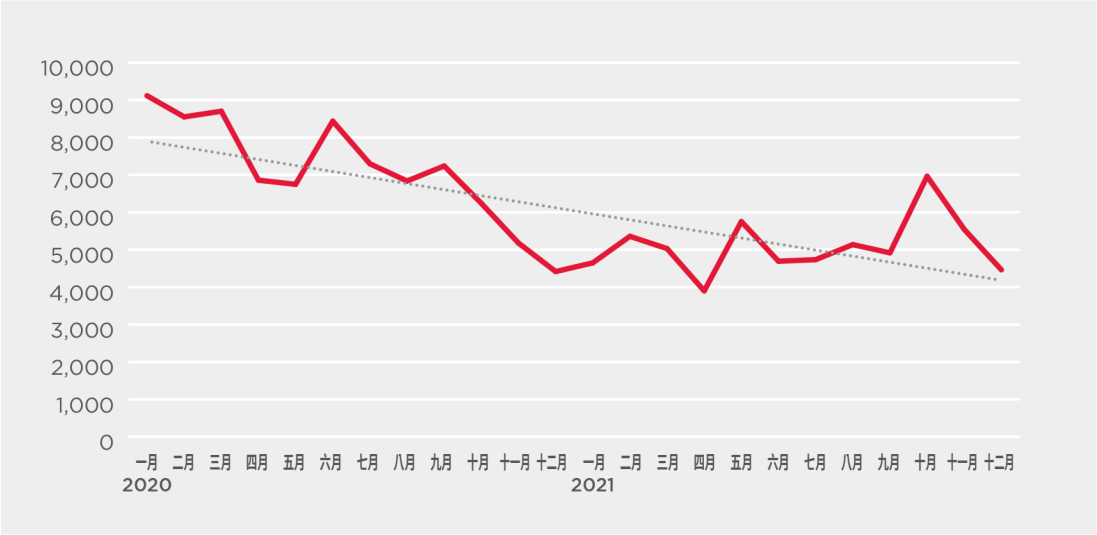


我們在去年的勒索軟體威脅態勢白皮書中指出，2020 年 1 月至 2021 年 6 月期間，有針對性的目標式勒索軟體攻擊數量大幅成長了 83%。我們可以看到，這種增長在 2021 年下半年繼續，2021 年 10 月和 11 月都有超過 250 次針對性的目標式勒索軟體攻擊記錄。在 2021 年 1 月和 2021 年 11 月之間，目標式勒索軟體攻擊的數量幾乎翻了三倍，從 85 次增加到 254 次，增長幅度趨近於 200%。

當關注在有針對性的目標式勒索軟體的數字時，也必須注意這些數字看起來似乎很小，確認後歸屬到已知的目標式勒索軟體家族的攻擊，可能只是涉及這些威脅總體攻擊數量的一個代表性樣本。許多目標式勒索軟體攻擊，在有效酬載被部署之前就被阻止，這意味著它們可能不會被識別為勒索軟體。此外，大多數目標式勒索軟體營運商，為每次新的攻擊重新編譯他們使用過的勒索軟體。這意味著攻擊中使用的勒索軟體的變種，可能會被通用或基於機器學習的檢測特徵檔所阻止，而不會被歸類到該勒索軟體家族相關的檢測。

雖然目標式勒索軟體攻擊的數量在過去幾年中呈上升趨勢，但從圖 2 中可以看出，博通公司旗下的企業安全部門--賽門鐵克公司檢測到的勒索軟體攻擊總數一直在下降。這很可能反映亂槍打鳥式的垃圾郵件勒索軟體活動日漸式微，這一領域的大多數網路犯罪分子，現在的重點是目標式勒索軟體。這絕不是表明勒索軟體所帶來的危險正在以任何方式下降。隨著攻擊者越來越專注在目標式勒索軟體，大型組織的危險可能只會增加。

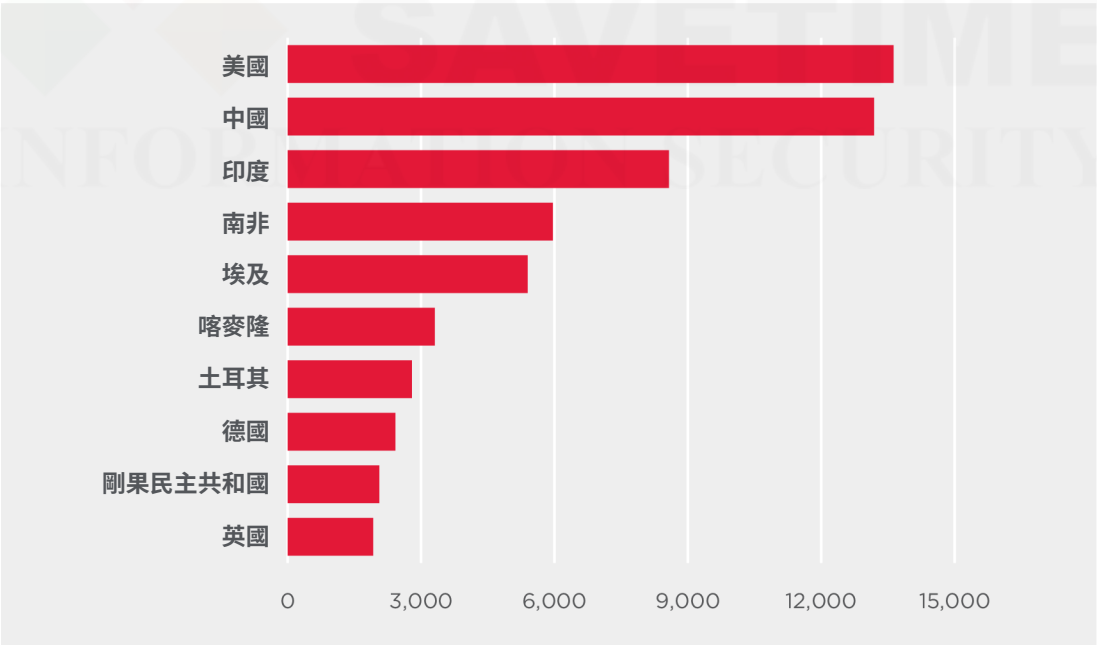
圖 2：所有勒索軟體的檢測結果，2020 年 1 月至 2021 年 12 月



讓我們看一下各國檢測到勒索軟體的總體數量 (圖 3)，與各國檢測到目標式勒索軟體的數量 (圖 4) 相比，可以看出亂槍打鳥的隨機式勒索軟體攻擊和目標式勒索軟體攻擊之間的區別。

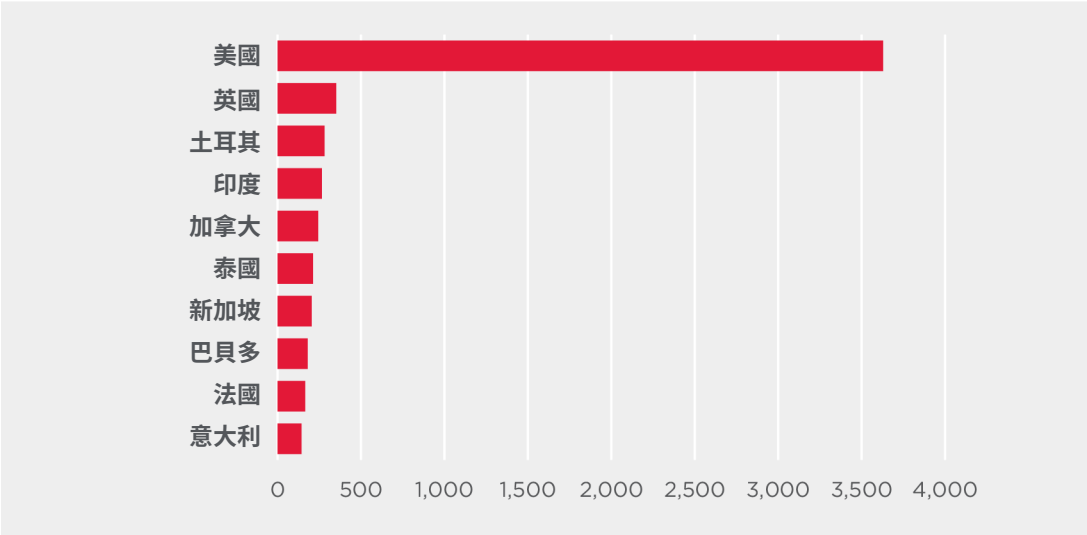
雖然美國在這兩種情況下都是最具指標性的國家，但總體數量往往由亂槍打鳥的大規模垃圾郵件攻擊所主導，其中列出剛果民主共和國 (DRC)、衣索比亞和其他沒有出現在目標勒索軟體名單中的國家。

圖 3：2021 年 1 月至 12 月各國檢測到的勒索軟體的總體數量



較富裕的國家在遭受目標式勒索軟體攻擊名列前茅，包括英國、法國和意大利。美國再次位居榜首，遭受目標式勒索軟體攻擊的次數是第二名 (英國) 的 10 倍以上。鑒於美國是一個擁有最多大型企業組織的富裕國家，而且許多目標式勒索軟體集團聲稱專門針對總部設在美國的公司，這並不令人驚訝。

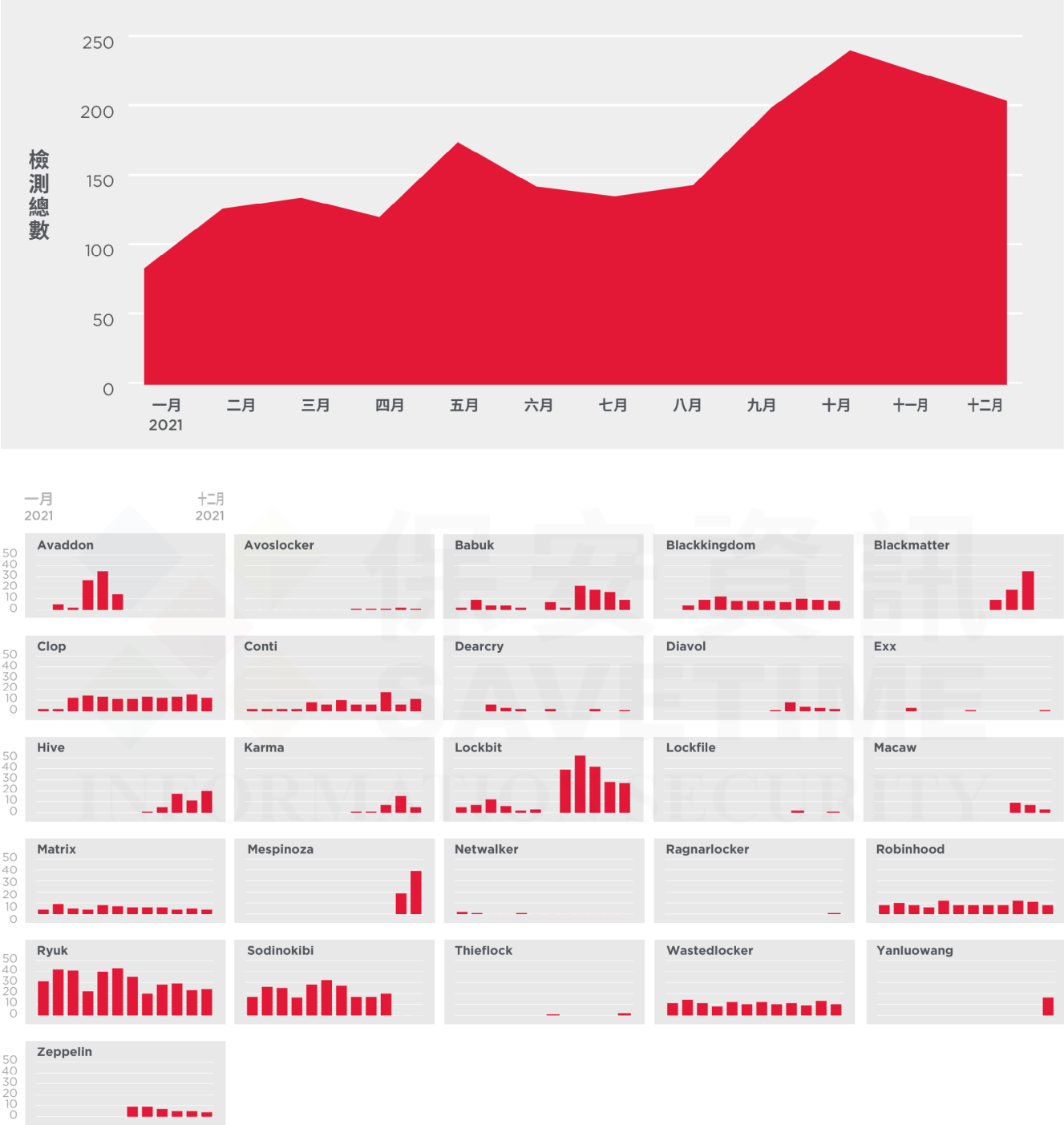
圖 4：2021 年 1 月至 12 月按國家劃分的目標勒索軟體檢測結果



像位於加勒比海與大西洋之間的島國：巴貝多，這樣的小國出現在圖 4 的前 10 名中可能會引起人們的注意，但這是對檢測到目標式勒索軟體家族電腦的統計，而不是對組織的統計。許多目標式勒索軟體的受害者多是跨國企業，不止一個國家有業務。

雖然總體活動和受影響之國家是非常寶貴的資訊，但許多人更關心的是他們現在需要注意最活躍的勒索軟體家族。勒索軟體的態勢是不斷在變化，曾經赫赫有名的勒索軟體家族已經變得默默無聞--有時是因為被取締，有時是因為營運商決定「金盆洗手」(據說某個特定的家族就是這樣)--而新的勒索軟體家族已經開始嶄露頭角。

圖 5：2021 年 1 月至 12 月按家族分類的目標式勒索軟體攻擊總偵測數



雖然一些勒索軟體家族，如：Conti 和 LockBit 在 2021 年的大部分時間都很活躍，但許多現在最主要的勒索軟體家族只出現在 2021 年的下半年，甚至最後一個季度。Mespinoza、AvosLocker、Hive 和 Zeppelin 都是目前非常活躍且危險的勒索軟體家族，所有這些家族在 2021 年下半年的活動都在增加，突顯勒索軟體格局快速變化的性質。

有關這些活動威脅的詳細資訊，請參閱本白皮書的勒索軟體威脅參與者部分。

再次強調，這些統計數據應被視為賽門鐵克產品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的階段或在它們與任何特定的勒索軟體系列相關聯之前就被阻止。

案例研究：
Revil 遭取締，山雨欲來的前兆？

惡名昭彰的勒索軟體團體 REvil /Sodinokibi (又名 Leafroller) 於 2021 年 10 月被迫離線，當時其基礎設施的控制權在多國行動中被剝奪。REvil 最初於 2021 年 7 月下線，當時其主要發言人“Unknown”似乎也從網際網路上消失，但該勒索軟體於 9 月重新上線。

在 IT 管理軟體公司 Kaseya 遭受備受矚目的 REvil 勒索軟體攻擊後不久，REvil 於 7 月關閉了。然而，雖然這種消失是暫時，但有跡象顯示，今年 10 月的取締行動可能會產生更持續性的影響。媒體報導稱，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對 10 月份針對 REvil 的協調行動負責。

2022 年 1 月，俄羅斯宣佈 14 名 Revil 勒索軟體集團同夥被俄羅斯當局逮捕，這是俄羅斯司法當局非常罕見的舉動。俄羅斯司法當局表示，他們從美國當局得到 Darkside 勒索軟體的訊息後，逮捕這些人。白宮表示，在此次扣押搜查被逮捕的人中，有 2021 年 5 月發生殖民地管道勒索軟體攻擊事件的負責人。儘管這次攻擊與 Darkside 勒索軟體有關，但 Darkside 的開發者--Corid--被認為是 Darkside 幫兇。

2021 年發生的勒索軟體攻擊，如：殖民地管道、Kaseya，以及美國食品生產巨頭 JBS 食品，似乎讓政府更加願意對參與勒索軟體攻擊的網路犯罪團體採取強硬立場。

同樣在 2021 年，我們看到 Emotet 僵屍網路在 1 月份被取締，儘管它現在可能已經恢復，Netwalker 勒索軟體基礎設施也在同一個月被查封並逮捕。

戰術、工具及程序 (TTPs)

大多數有針對性的目標式勒索軟體攻擊都是一個多階段的過程，攻擊者會採取許多步驟並在部署勒索軟體有效酬載之前部署一系列的 TTPs。對於尋求保護其網路免受勒索軟體攻擊者滲透的組織而言，瞭解勒索軟體攻擊者通常使用的 TTPs 是關鍵，因為發現這種勒索軟體前的活動可以讓防禦者在發生攻擊之前阻止攻擊。

攻擊者利用這些 TTPs 進行各種操作，包括滲透受害者的網路、竊取憑證、提升特權、在網路中橫向移動以及部署其勒索軟體有效酬載。

我們在 2021 年的攻擊中，最常用於攻擊的前勒索軟體工具可以在表 1 中看到。值得注意的是，像 PsExec 這樣的 Windows 作業系統工具，是 2021 年 4 月至 12 月期間調查中最多的工具 (34%)。雖然像 Cobalt Strike 這樣的商品化惡意軟體，在勒索軟體攻擊者使用的工具清單中也佔有重要地位，但大量利用的就地取材和兩用工具顯示，在勒索軟體攻擊者中，就地取材的戰術繼續流行，因為他們努力隱藏其在受害者網路上的活動，直到勒索軟體有效酬載被部署。他們透過利用合法的程序和工具來實現這一目標，這些程序和工具不太可能觸發安全軟體或讓網路上的用戶產生可懷疑。

表 1：2021 年 4 月至 12 月最常見的佈署勒索前的軟體工具

Tool	Percentage of Investigations
PsExec	34%
Cobalt Strike	18%
Mimikatz	11%
VssAdmin	10%
NetScan	7%
Bitsadmin	4%
AdFind	5%
Nsudo	5%
PowerShell	5%
MSIExec	4%
WEIRDLOOP	3%
IcedID	3%
Disable Defender	3%
WMI	4%
rclone	3%
NetworkShare	2%
PAExec	2%
RaccoonStealer	2%
PasswordRevealer	2%
Netsh	2%
ProcDump	2%
ScreenConnectInstaller	2%
SystemBC	2%
Delete Shadow Copies	1%
Qakbot	1%

在 2021 年 9 月與客戶分享的勒索軟體白皮書中，我們列出了在勒索軟體攻擊中看到的許多工具。幾乎所有這些工具現在仍然具有相關性，但我們也看到在最近的攻擊中其他被利用的一些工具。這些包括：

- **VssAdmin**：合法的 Windows 程序，可用於管理或刪除 Windows 電腦上的陰影備份。
- **MSIExec**：合法的 Windows 安裝程式，攻擊者會濫用該安裝程式將惡意有效酬載載入到受害電腦上。
- **NetworkShare**：攻擊者可以發出命令，以便將其惡意有效酬載傳播到同一網路上的其他電腦。
- **PAExec**：允許使用者在遠端 Windows 電腦上啟動 Windows 程式，而無需先在遠端電腦上安裝軟體。與 PsExec 一樣，它主要被攻擊者用在受害者網路上橫向移動。
- **RaccoonStealer**：資訊竊取者出租，其營運商向其他網路罪犯收取費用。它可以用來從受感染的機器上竊取各種資訊，但最有可能被勒索軟體攻擊者用來竊取憑證，以允許許可權提升和橫向移動。
- **PasswordRevealer**：駭客工具，在安裝它的機器上顯示隱藏為星號的密碼。
- **Netsh**：Windows 命令行應用工具，允許使用者配置和顯示各種網路通信伺服器角色和元件的狀態。已用於 LockBit 和 Mespinoza / Pysa 攻擊。

- **ScreenConnectInstaller**：ScreenConnect（現在稱為 ConnectWise）的安裝程式，這是一種合法的遠端存取工具，經常被惡意行為者用來提供對受害電腦的存取。最近被濫用於利用 Yanluowang 和 Noberus（ALPHV / BlackCat）勒索軟體的攻擊。

下面列出了我們的統計資訊中提供的工具，以及 9 月份勒索軟體白皮書中出現的工具。

- **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。
- **PowerShell**：可用於各種惡意目的的合法工具，包括直接從記憶體執行命令以及將惡意軟體注入其他合法程序。由於 **PowerShell** 有許多合法用途，因此它為攻擊者隱藏其惡意活動提供了一種理想的方法。
- **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。
- **Rclone**：一種開放原始碼命令列應用程式，可以合法地用於管理雲端的內容，但已被勒索軟體行為者濫用以從受害電腦中泄露數據。
- **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。

瞭解勒索軟體攻擊者使用的 TTPs，可讓防禦者更好地瞭解其組織如何受到損害，並且可以就防禦措施的優先順序提供一些導引。

新增和最新的勒索軟體威脅參與者

我們在 2021 年 9 月發布的勒索軟體白皮書詳細介紹許多新增和最新的主要勒索軟體威脅系列。然而，不斷變化的網路犯罪態勢的性質，特別是勒索軟體態勢，意味著從那當時到現在的短時間內，幾個全新的勒索軟體家族已經營造出知名度和影響力。本節詳細介紹一些當前最活躍的勒索軟體家族。

新增的勒索集團簡介：

Birdwing

別名：Pysa、Mespinoza

勒索軟體家族：Pysa

活動起始時間：2018

Birdwing 開發 Mespinoza /Pysa 勒索軟體，該勒索軟體已被用來對許多行業及國家的受害者發動攻擊，儘管其大多數受害者都在美國。目前尚不完全清楚 Birdwing 是否自己部署勒索軟體，或者是透過勒索軟體即服務 (RaaS) 的營運模式，由其聯盟成員負責部署勒索軟體來獲得分潤。

至少從 2018 年 10 月開始活躍，Birdwing 的活動最近有所增加，聯邦調查局於 2021 年 3 月發布有關該集團的警報。Birdwing 勒索信內文包含「Protect Your System Amigo* 保護您的系統朋友」一詞，這或許就是代表「 Pysa 」的意思。

Birdwing 通常透過入侵遠端桌面協議 (RDP) 憑證和／或透過網路釣魚電子郵件獲得對受害者網路的未經授權存取。該組織對遭入侵的系統進行偵察，可能是先確定是否有足夠有價值的資料來決定是否值得發動全面攻擊，並蒐索「clandestine」、「fraud」、「ssn」等關鍵字，可能查找機敏文件來做為脅迫洩露的談判籌碼。網路攻擊者使用 Advanced Port Scanner 和 Advanced IP Scanner 進行網路偵察，並繼續安裝開放原始碼工具，例如：PowerShell Empire、Koadic 和 Mimikatz。PsExec、PowerShell 和 netsh 等其他開放原始碼工具也多有被部署在 Birdwing 攻擊中。包括 Windows Defender 在內的安全產品通常也會在部署勒索軟體之前被停用，並且會從受害系統中刪除陰影副本，讓受害者無法從中恢復資料。

Palo Alto 表示，在 Birdwing 攻擊中，它觀察到一個名為 Gasket 的新後門被下載以保持對網路的存取。Gasket 還引用一項名為「MagicSocks」的功能，該功能使用開放原始碼 Chisel 專案來建立通道，以便繼續遠端存取網路。攻擊者建立一個獨立版本的 MagicSocks 工具，除了 Gasket 之外，他們還使用該工具來加密傳輸流量。賽門鐵克研究人員還觀察到大約在 Birdwing 攻擊時，勒索軟體被部署到受害者電腦前 24 小時，攻擊者透過 PsExec 部署一個名為 p.ps1 的惡意腳本。Birdwing 使用各種方法從受害者網路中竊取檔案。聯邦調查局報告說，人們已經看到它使用免費的開放原始碼工具 WinSCP，而賽門鐵克和 Palo Alto 研究人員都觀察到，Birdwing 攻擊者使用基於 IP 的 URL 包含相同 URI 樣本來洩露受害者資料，例如：URI /upload-wekkmferokmsdderiuheoirhuiewiwnijnfrer?token=<base64 token value>&id=<unique number for organization>&fullPath=<path on disk of file exfiltrated>。在一些 Birdwing 攻擊中，被盜資料已被上傳到 Mega.nz 檔案共享網站。

一旦資料遭竊取後，受感染網路上的資料就會被勒索軟體加密。在某些情況下，Birdwing 下載檔名為 svchost.exe 的有效酬載，很可能是透過為其提供相同的名稱來將勒索軟體偽裝成通用的 Windows 主機程序。執行勒索軟體時，會生成詳細的勒索訊息並顯示在受害者登錄或鎖定螢幕時的螢幕畫面上。

賽門鐵克研究人員在 2021 年 10 月下旬觀察到 Pysa 勒索軟體攻擊，當時攻擊者在部署勒索軟體有效酬載之前只在網路上停留了三到四天，這對勒索軟體攻擊者來說是一個相對較短的停留時間。

Sirex

別名：AvosLocker

勒索軟體家族：AvosLocker

活動起始時間：2021

Sirex 於 2021 年 6 月首次出現。它是一家勒索軟體營運商，它透過多家聯盟成員使用其 AvosLocker 勒索軟體進行攻擊，以獲取分潤。它不僅提供了惡意軟體，還協助管理與受害者的通信，以及託管在攻擊行動中被盜的資料。

AvosLocker 通常透過垃圾郵件行動或惡意廣告傳播，由於 Sirex 採用勒索軟體即服務 (RaaS) 方式營運，勒索軟體由聯盟成員公司傳遞，因此發動 AvosLocker 勒索軟體攻擊所採用的的 TTPs 可能各不相同。使用 AvosLocker 的攻擊者也被發現利用 Microsoft Exchange 伺服器中的已知漏洞來獲取對受害者網路的初始存取權限。一旦勒索軟體被執行，就會建立 GET_YOUR_FILES_ BACK.txt 的勒索信。然後，勒索軟體會加密用戶的檔案，並將 .avos 副檔名附加到其中。勒索信中的鏈結將受害者引導到 Tor 網站，該網站要求回應勒索信中的 ID。如果不支付贖金，贖金會在一段時間後增加，該組織還威脅要公開透露受害者組織已被駭客入侵。

當有效酬載爆發時，如果檔案被其他程序存取，勒索軟體會結束程序，並進行內容加密。勒索軟體讀取案檔內容並進行加密後，用特有的簽章在加密檔案中寫入內容。此簽章用於識別檔案是否加密。同時加密網路共享磁碟。

Malwarebytes 的分析得出結論說，AvosLocker 是「與其他勒索軟體沒有太大區別」(除異常聲量外) 的普通勒索軟體家族。但是，由於其加密沒有弱點，如果沒有解密密鑰，就無法恢復加密資料。

2021 年 9 月，Sirex 更新了網站並新增系統以拍賣拒絕支付贖金要求企業被盜的資料，而不是在線上免費下載。

Pinion

別名：Hive

勒索軟體家族：Hive

活動起始時間：2021

值得注意的是，Pinion 似乎沒有將任何部門排除在其攻擊之外的盜義，正如許多勒索軟體營運商經常聲稱的那樣，例如：已知它已經攻擊了醫療保健領域的多個受害者。這些攻擊似乎不是無心之過，因為勒索軟體是人為操作，從命令列輸入指令，這顯示攻擊者既了解他們所處的環境，又可以定製其專屬攻擊以發揮最大作用。

在 2021 年 8 月對美國一個非營利性的綜合醫療保健系統--MHS(Memorial Health Systems) 的攻擊中，採用 Hive 勒索軟體的攻擊者宣稱竊取高達 20 萬名患者的資料。另外，由於此次攻擊，手術被取消，醫療量能被迫縮減。據了解，與勒索軟體集團攻擊醫療服務提供者後免費提供解密檔案的類似勒索軟體攻擊不同，Pearning 並沒有這樣做，MHS 支付近 200 萬美元贖金。

Pinne 採用勒索軟體即服務 (RaaS) 方式營運，其聯盟成員使用 Hive 勒索軟進行攻擊，以獲取分潤。Hive 用於雙重勒索軟體攻擊，受害者資訊被竊取，他們的檔案也被加密。

Pinne 及其聯盟成員公司利用其勒索軟體使用多種機制來入侵網路，包括透過惡意附件的釣魚電子郵件獲得存取權限及 RDP 在網路上橫向移動。還發現使用 Hive 的攻擊者利用 Cobalt Strike 和合法 ConnectWise 工具在受感染的網路上保持持續性。

勒索軟體會查找與備份、防病毒／反間諜軟體和檔案複製相關的程序，並終止它們以利檔案加密。它將 .hive 副檔名新增到被加密檔案中，然後將 hive.bat 批次檔本放入目錄中，該批次檔強制執行一秒的執行超時延遲，以便在加密完成後透過刪除 Hive 可執行檔和 hive.bat 批次檔來執行清理。第二個檔案 (shadow.bat) 將放入目錄中，以刪除陰影副本 (包括磁碟備份副本或快照)，然後刪除 shadow. bat 檔。在加密過程中，加密檔將使用 *.key.hive 或 *.key.* 的雙重副檔名命名。贖金說明信 (HOW_TO_DECRYPT.txt) 將放入每個受影響的目錄中，並指出如果 *key.* 檔被修改、重新命名或刪除，則被加密檔將無法再恢復。

勒索信包含一個「銷售部門」連結，可透過 Tor 瀏覽器訪問，允許受害者透過即時聊天與駭客聯繫。據聯邦調查局稱，一些受害者還回報說，他們接到勒索集團的電話，要求為他們的檔案付款。該說明還告知受害者，如果他們不支付贖金，他們的資料將被發佈在資料外洩的網站上。

還有一些 Hive 變種還能夠加密 Linux 和 FreeBSD 系統。

Dryxiphia

別名：Yanluowang

勒索軟體家族：Yanluowang

活動起始時間：2021

賽門鐵克研究人員發現 Dryxiphia 於 2021 年 9 月首次被觀察到試圖使用 Yanluowang 勒索軟體進行勒索軟體攻擊。該攻擊針對一家大型企業組織，並在研究人員注意到 AdFind 的可疑使用後被發現，AdFind 是一種合法命令列 Active Directory 查詢工具，經常被勒索軟體攻擊者濫用。在受害者機器上看到可疑的 AdFind 使用幾天後，攻擊者試圖部署 Yanluowang 勒索軟體。

在我們最初發現 Yanluowang 之後，賽門鐵克研究人員隨後發現證據顯示，至少自 2021 年 8 月以來，它也被另一個威脅集團所使用，對美國公司進行有針對性的攻擊。攻擊者使用許多以前與 Canthroid（Thieflock）勒索軟體攻擊相關的 TTPs，這顯示他們可能是 Thieflock 的聯盟成員公司，他們移情別戀到新的 Yanluowang 勒索軟體家族。

YanLuwang 看起來是相當新開發的勒索軟體，目前還不清楚是作為勒索軟體即服務 (RaaS) 營運方式的一環租賃給聯盟成員使用，還是 Dryxiphia 直接進行大部分的攻擊。此勒索軟體主要針對金融行業。

同樣值得注意的是，在其勒索軟體說明信中，Dryxiphia 警告受害者不要聯繫執法部門或勒索軟體談判公司。如果攻擊者的規則被破壞，勒索軟體營運商表示他們將對受害者進行分散式拒絕服務 (DDoS) 攻擊，並「打電話給員工和業務合作夥伴」。犯罪分子還威脅要在「幾周內」重複攻擊並刪除受害者的資料。這是依據我們最近看到的趨勢，如果受害者試圖讓任何第三方參與勒索軟體談判，勒索軟體攻擊者會發出進一步的威脅。

Batfly

別名：Nemty、Karma

勒索軟體家族：Karma、Nemty、JSWorm、Nefilim、Fusion、Milihpen、Gangbang

活動起始時間：2019

自 2019 年以來，Batfly 負責著名的 Nemty 和 Karma 勒索軟體家族，並參與開發各種其他勒索軟體變種，包括 Nefilim、Gangbang 和 Milihpen。Batfly 被觀察到第一次公開活動是在 2019 年 4 月以 JSWorm 為暱稱。Nemty 於 2019 年 8 月首次被發現，它經歷許多不同的版本。Nemty 和 Karma 都曾被命名，因為它們被新增到加密檔中的副檔名。

當 Nemty 首次出現時，它可以在網路犯罪論壇上購買，按照目前的標準，所要求的贖金並不多，相當於大約 1,000 美元。在 Nemty 營運的早期，Batfly 非常積極地發佈新版本來修復錯誤並進行改進。其中一些是安全研究人員和公司所必須要做的，而另一些則受到地下網路犯罪論壇用戶批評的刺激，這些論壇是 Batfly 最初出售 Nemty 的通路。

Batfly 也是早期進行雙重勒索攻擊的勒索軟體開發商之一，攻擊者竊取資料用於勒索目的並對其進行加密，自 2019 年 8 月以來經營資料洩漏網站。Nemty 透過垃圾郵件行動、漏洞利用工具包和暴力破解 RDP 端點進行散布，並一度透過 Trik 殭屍網路散布。

2020 年 3 月／ 4 月，Batfly 將其勒索軟體更名為 Nefilim，並宣佈將「私有化」。這意味著它不再可以在勒索軟體論壇上免費購買，並且其開發人員只能與受信任的聯盟成員公司合作，這通常是 RaaS 產品現在的運作方式。

Milihpen 變種於 2021 年 1 月出現。它以 C++ 編寫，保留早期變種的主要功能、執行程序、加密方案和資料外洩網站位址，而 2021 年 2 月出現的 Gangbang 與 Milihpen 相同。Karma 出現在 2021 年 5 月，研究人員得出結論，由於 Karma、Gangbang 和 Milihpen 之間的代碼相似性，它很可能來自與 Nemty 相同的開發人員。相似之處包括排除的資料夾、檔案類型和使用的除錯訊息。但是，也進行一些修改，包括使用 Salsa20 加密的 Karma，同時它還為枚舉和加密建立一個新的執行序 (thread)，可能為了確保更可靠的結果。Karma 要求的贖金規模尚不清楚，但勒索軟體似乎主要針對收入超過 10 億美元的大型組織部署。

Batfly 較舊的「企業洩密」資料外洩網站大約在 Karma 及其資料洩露網站出現的同時進入休眠狀態，這顯示無論如何，就目前而言，Karma 似乎是 Batfly 的主要焦點。

Pollen

別名：Zeppelin、VegaLocker

勒索軟體家族：Zeppelin、Buran、VegaLocker

活動起始時間：2019

Pollen 自 2019 年以來一直活躍，最初使用 VegaLocker 勒索軟體，該勒索軟體針對說俄語人士，並透過在俄羅斯的線上廣告在網路上傳播惡意廣告。當時，以亂槍打鳥進行無差別攻擊，在 2019 年期間，出現多個新版本的 VegaLocker -- Jamper、Storm、Buran -- 其中一些在地下論壇上出售。

然而，當 Pollen 於 2019 年 11 月推出 Zeppelin 勒索軟體時，其方法發生了變化，該勒索軟體被用於針對美國和歐洲科技及醫療保健領域精心挑選的組織。Zeppelin 與 Pollen 勒索軟體的早期版本不同的另一個特點是，如果它在俄羅斯或其他「獨立國家國協 (CIS) 」國家的機器上執行，它會自動停止。

Pollen 在地下論壇上銷售 Zeppelin，允許惡意軟體的購買者決定他們希望如何使用它，而不是透過我們通常看到的勒索軟體開發商現在運行的更典型、受控的 RaaS 營運模式來散布。與當今大多數勒索軟體集團不同，Pollen 還因不經營資料洩露網站而聞名。Zeppelin 也因長期不活動而引人注目，許多人認定它已在 2020 年底退役，然後 Pollen 重返提供新版本的勒索軟體，並在 2021 年年中開始銷售。

使用 Zeppelin 的網路犯罪分子通常使用常見的初始攻擊媒介，如 RDP、VPN 漏洞和網路釣魚，同時也可以看到它透過受感染的網站或僅在散布期間活動的臨時 C&C 基礎設施進行散布。最近 Zeppelin 變種還包括一個持續 26 秒的休眠功能，以試圖繞過先進的動態分析引擎和沙箱。

賽門鐵克研究人員在 2021 年 11 月觀察到 Zeppelin 勒索軟體攻擊，該攻擊濫用本地網路分享作為勒索軟體酬載和名為 w.ps1 的惡意 PowerShell 腳本的暫存伺服器。在部署勒索軟體之前，觀察到許多行徑，包括：

- 使用 comsvcs 進行憑證轉儲
- 停用安全服務
- 刪除磁碟陰影副本
- 使用 BCDEdit 禁止系統復原
- 使用 CVTRES 進行遠端編譯和執行

PsExec 用於執行 w.ps1 並將勒索軟體有效酬載複製到網路上的所有電腦。在這次攻擊中，加密檔案副檔名為 .v-society.9BF-C5F-9E3 並且勒索信顯示「VICE SOCIETY」對此負責。

因為 Zeppelin 相對容易可以在地下論壇上購買，所以採用 Zeppelin 的網路犯罪分子可能比正常情況更多，這使得拆解典型的 Zeppelin 攻擊鏈更具挑戰性，因為他們所採用的 TTPs 可能會有很大差異。

案例研究：
Noberus：以 Rust 編碼的勒索軟體只想要維持談判的隱私，避免被公諸於世？

Noberus (又名 ALPHV ／ BlackCat) 於 2021 年 11 月 18 日首次出現在受害者組織中，在一次攻擊過程中它部署三種 Noberus 變種。Noberus 很有趣，因為它是用 Rust 編碼，這是我們第一次看到實際攻擊的專業勒索軟體類型使用這種程式語言編碼。

Noberus 執行我們現已慣於看到的典型雙重勒索軟體攻擊，並在其攻擊過程中部署常見的勒索軟體工具，如：PsExec 和 PowerShell。它似乎也利用合法的 ConnectWise 工具來部署其有效籌載。它還執行各種其他常見的勒索軟體前置操作，例如：停用 Window Defender 和刪除陰影複製。

Noberus 所做的另一件有趣事項是透過執行 wmic 命令列管理工具收集系統資訊，以便從每台裝置上收集通用唯一識別碼 (UUID)。然後這些識別碼用於產生「存取權杖」，該權杖構成受害者被指示存取的唯一 Tor 位址 (洋蔥路由器--The Onion Router) 的一部分。受害者需要擁有這個獨特的位址才能與攻擊者進行談判。攻擊者這樣做很可能是為了阻止他們的談判被其他人 (例如：資安研究人員或記者) 滲透。

談判記錄被洩露很大程度上源於這樣一個事實，即贖金談判的首選方式是一個聊天網站，每個受害者都有一個唯一的網址 (URL)。雖然它使受害者很容易聯繫攻擊者，但這卻意味著任何知道該 URL 的人都可以查看對話，甚至可以發布自己的訊息。勒索談判的 URL 通常包含在勒索軟體有效籌載中，如果該樣本被上傳到 VirusTotal，這意味著即使受害者不想公開談判，也可能會被協力廠商存取分析。但如果在攻擊期間建立這類唯一的存取密鑰，就可防止上述情況發生。

最近，談判被洩露或滲透似乎激怒勒索軟體攻擊者，不止一個勒索軟體組織威脅說，如果受害者聘請專業談判人員或有關攻擊的訊息被洩露給媒體，他們就會停止談判。

Conti (又名 Miner) 表示，如果公開分享贖金談判的成果或螢幕截圖，它將立即洩露受害者資料。同時，Grief 勒索軟體表示，如果受害者聘請專業談判人員，它就會刪除解密密鑰，而 RagnarLocker 表示，如果聯繫司法部門，它將公開洩露受害者資料。

Miner (* 礦工)

沒有減少活動的跡象

別名：巫師蜘蛛

勒索軟體家族：Diavol、Conti、Ryuk、GoGaLocker (非活躍)、MegaCortex (非活躍)

活動起始時間：2014

作為近年來最活躍的勒索軟體開發商之一，Miner 沒有表現出打算在 2021 年結束時放緩其活動的跡象。Conti 仍然是最活躍的目標式勒索軟體家族之一，澳洲網路安全中心 (ACSC) 在 2021 年 12 月發布有關濫用此勒索軟體進行攻擊的警告。ACSC 表示，在 2021 年 11 月和 2021 年 12 月，澳洲組織「多次」受到 Conti 勒索軟體的影響。

據報導，在其他地方與 Conti 相關的攻擊者，參與 2021 年最後一個季度 Emotet 殭屍網路的重返 (參見案例研究)。但是尚不清楚這是 Miner 還是 Conti 的聯盟成員。

與此同時，最近幾個月，Miner 與一種名為 Diavol 的新勒索軟體有關，該軟體似乎變得越來越活躍。Fortinet 研究人員在 7 月份將其與 Miner 聯繫起來，當時它說勒索軟體被用於某次攻擊，在此期間 Conti 也部署在同一網路上。這兩種惡意軟體之間以及使用的 TTPs 之間也有一些相似之處。Diavol 與 Conti 的命令列參數「幾乎相同」，它們功能也相似，例如：記錄檔、加密本地磁碟機或網路共用及掃描特定主機以尋找網路共用。在對檔案路徑進行佇列以進行加密時，Diavol 和 Conti 都具有非同步 I/O 操作行為。

在勒索軟體領域遭受重創的時期，Miner 仍一直保持活躍。如果該組織現在也將 Emotet 殭屍網路納入可運用的工具之列，那麼使用該組織開發的勒索軟體攻擊，可能會在 2022 年持續增加。

Coreid (* 核芯)

與惡名昭彰的 FIN7 網路犯罪組織有關連

別名：Darkside

勒索軟體家族：Darkside、BlackMatter

活動起始時間：2020

Coreid 最著名的是與 Darkside 勒索軟體有關，該勒索軟體被濫用於 2021 年 5 月，對美國東岸的殖民地管道公司：Colonial Pipeline 所發動的攻擊。在這次攻擊之後，因媒體和司法部門的強烈關注，迫使 Coreid 退出 Darkside，該組織聲稱在司法行動後它失去了對其伺服器和加密貨幣錢包的存取權限。

然而，在 2021 年 7 月，專家普遍認為 Coreid 的死灰復燃與 BlackMatter 勒索軟體的出現有關。BlackMatter 使用與 Darkside 相同的加密程式，而區塊鏈分析公司 Chainalysis 也發現這兩個勒索軟體家族之間的金流關聯性。美國政府於 2021 年 10 月發布有關 BlackMatter 的警告，稱它已被用於針對該國關鍵基礎設施 (CNI) 組織的多次針對性攻擊。然而，在 11 月初，BlackMatter 發布消息稱，由於「與當局壓力相關的某些無法解決的情況」，它將停止營運。這可能意味司法機關的逮捕行動，使後續營運勒索軟體變得更困難。它在活躍後僅四個多月就消失，這突顯勒索軟體領域的動盪性質。

最初賽門鐵克研究人員將 Coreid 視為一個獨立團體進行追蹤，但在 2021 年下半年，CrowdStrike 的研究將 Coreid 與惡名昭彰的 FIN7 (又名碳蜘蛛) 網路犯罪集團聯繫起來，並指出 FIN7 其實是 Darkside 和 BlackMatter 勒索軟體幕後的藏鏡人。FIN7 是一個多產的網路犯罪組織，至少自 2016 年以來一直活躍。據 CrowdStrike 稱，該組織最初以在零售業和飯店業的 pos 系統上安裝惡意軟體而聞名，該組織在 2020 年轉移了重點並開始執行一些使用 REvil 勒索軟體的勒索軟體攻擊。CrowdStrike 表示，FIN7 負責開發 Darkside 和 BlackMatter 勒索軟體系列，並開放這兩種勒索軟體給聯盟成員。

像 FIN7 這樣知名且多產的網路犯罪集團致力於勒索軟體開發這一事實表明，勒索軟體目前在網路犯罪領域的影響力 : 它是老練的網路犯罪分子使用的主要營利工具。現在該集團已被迫退出 Darkside 和 BlackMatter，或許司法壓力對該組織的活動已經產生不可逆轉的影響，後續它們是否會產出新的勒索軟體，這將是一件值得觀察的事情。

Hispid (* 硬皮)

集團首次推出兩種全新的勒索軟體

別名：EvilCorp、Indrik Spider、TA505

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

活動起始時間：2011

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，然後在 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，可能是為了規避這些制裁並從美國公司那裡獲得付款。

在 2021 年下半年，人們看到 Hispid 開發出兩個全新的勒索軟體系列。Grief 勒索軟體於 6 月出現，並於 10 月聲稱對襲擊美國國家步槍協會 (NRA) 的勒索軟體攻擊負責。此外 2021 年 9 月，Grief 在其資料洩露網站上發布一份聲明，威脅說如果受害者聘請談判公司，將刪除其受害者的解密密鑰。

與此同時，2021 年 10 月 Hispid 推出另一個新的勒索軟體 Macaw。由於 Macaw 的網路攻擊，致使美國廣播公司、奧林巴斯和辛克萊廣播集團的轉播訊號嚴重中斷，導致電視廣播被取消，新聞主播只能使用紙本稿和白板報導。據報導，攻擊者要求受害者公司支付 2,800 萬美元和 4,000 萬美元的贖金。

隨著該組織繼續試圖逃避對其的制裁，我們很可能會在 2022 年看到更多全新名稱的 Hispid 變種。

案例研究：
Exmatter：BlackMatter、Conti 攻擊中所使用的資料洩露工具

Exmatter 是由賽門鐵克威脅獵手團隊在 2021 年 10 月發現的可自訂資料洩露工具。主要的目的在從多個選定目錄中竊取特定檔案類型，並將其上傳到攻擊者控制的伺服器，然後再部署勒索軟體本身在受害者的網路上。這是勒索軟體營運廠商第三次開發的可自訂資料洩露工具，此前發現與 LockBit 勒索軟體相關聯的 Ryuk Stealer 工具和 StealBit。

雖然 Exmatter 最初被發現用於 BlackMatter 勒索軟體攻擊，但隨後也被用於 2021 年 12 月部署 Conti 的攻擊中。這表明 Exmatter 可能是勒索軟體聯盟成員公司的產品，而不是 Coreid 或 Miner (勒索軟體 BlackMatter 和 Conti 幕後的開發商)。

Exmatter 執行後，該工具會嘗試根據一些硬編碼規則從本地電腦中竊取檔案。它將在多個指定目錄中搜索以下檔案類型：.doc、.docx、.xls、.xlsx、.pdf、.msg、.png、.ppt、.pptx、.sda、.sdm、.sdw 或 .csv。它嘗試使用 LastWriteTime 屬性來對目標檔案優先進滲透。已觀察到 Exmatter 的多個變種，這表明其幕後的參與者正在不斷優化該工具，以盡快加速最大量的高價值資料的洩露。

一旦完成從受害者裝置中竊取資料，Exmatter 就會執行一個命令來刪除它自己的任何痕跡。

感染媒介

通常很難確定勒索軟體攻擊過程中使用的初始感染媒介。但是，目標勒索軟體攻擊者常用的一些已知媒介包括：

- 電子郵件--網路釣魚和垃圾郵件行動
- 漏洞利用
- 殭屍網路

勒索軟體攻擊者所使用初始進入媒介是相關的，因為如果勒索軟體攻擊者發現一個可以讓他們廣泛存取受害者網路的媒介，它可能允許他們執行極具破壞性和高投報率的攻擊。如果他們發現一種方法可以滲透到其他勒索軟體參與者無法滲入的受害者網路，例如：瞭解零時差漏洞或存取特別強大的殭屍網路，它還可以讓他們成為勒索軟體領域舉足輕重的人物。

用於傳播 SquirrelWaffle 載入器的電子郵件

SquirrelWaffle 是一種惡意軟體載入器，於 2021 年 9 月首次出現，一些研究人員將其描述為有望成為 Emotet 的繼任者，在 Emotet 重新出現之前 (參見案例研究)。電子郵件是一種已知的傳遞勒索軟體威脅的工具，SquirrelWaffle 主要透過垃圾郵件行動傳播，並用於傳遞 Qakbot 和 Cobalt Strike，這些都是常見的勒索軟體前置工具。

發送 SquirrelWaffle 的垃圾郵件通常包含指向惡意 Zip 檔案的超連結，其中包含惡意 .doc 或 .xls 附件。在 Cisco Talos 分析的一項活動中，攻擊者使用 DocuSign 簽名平臺誘騙收件人在惡意文件上啟用巨集。

如果受害者在檔案上啟用巨集，就會被 SquirrelWaffle 感染，從而最終將 Qakbot 和 Cobalt Strike 下載到受害者裝置上。SquirrelWaffle 與其 C&C 伺服器之間的所有通信都是加密的，而該惡意軟體還包含一個 IP 位址黑名單清單，該清單涵蓋各個著名的安全研究公司，藉此以逃避檢測和分析。思科 Talos 研究人員在並發現 SquirrelWaffle 的「散布行動、基礎架構和 [C&C]) 具有幾個值得注意的技術，這些技術與其他更成熟的威脅極度相似」。

Qakbot 和 Cobalt Strike 是典型的勒索軟體前置工具。賽門鐵克研究人員在 2021 年 10 月發現一場行動，該行動部署許多與 SquirrelWaffle 活動中所見相同的戰術。此行動中使用的路徑和檔案名稱與 Netskope 在部落格中提到 SquirrelWaffle 活動中所使用的路徑和檔案名稱相同，但我們沒有發現部署 SquirrelWaffle 載入器。在這次活動中，Qakbot 被用來傳遞 Cobalt Strike，雖然沒有觀察到勒索軟體被傳遞，但據了解這可能是該活動的最終目標。

受害者收到一封附有 Zip 壓縮檔的電子郵件。此 Zip 壓縮檔包含惡意 Excel 檔案。如果受害者打開惡意 Excel 檔案，Qakbot 就會在他們的裝置上啟動。一旦 Qakbot 被執行，攻擊者就會進行一些偵察活動，包括發現設備上的共用資源，以及設備上的伺服器名稱和本地群組。同時，AdFind 等各種可疑檔案也會被執行。Cobalt Strike 信標發送載入程式也從排程工作中執行。攻擊者隨後試圖執行另一個可能是勒索軟體的未知檔案。

勒索軟體攻擊者利用的面向公眾服務的應用程式中的漏洞

在過去幾年中，利用直接提供面向公眾服務的應用程式中的漏洞，已成為網路犯罪分子和進階持續威脅 (APT) 組織日益流行的攻擊媒介，勒索軟體攻擊者也不例外。

Microsoft Exchange Server 中的 ProxyLogon 漏洞於 2021 年 3 月曝光，已知被勒索軟體攻擊者等利用。AvosLocker (又名 Sirex) 勒索軟體是一種勒索軟體即服務 (RaaS)，於 2021 年 7 月首次出現，於 2021 年 11 月下旬和 2021 年 12 月被發現，它利用 Microsoft Exchange Server 中的漏洞獲得對受害者網路的初始存取權限。然後它會將 web shell 放在伺服器上的非標準資料夾中，可能會允許遠程程式碼執行。

攻擊者還濫用合法的 SoftEther VPN，將其副本重命名為「systemresetosupdate.exe」以隱藏其功能。Mimikatz 和 SecretsDump 也因認證竊取而被偷偷載入。Certutil 用於下載額外的有效籌載，而 AnyDesk 用於橫向移動。

在其他地方，虛擬私人網路 (VPN) 中的漏洞也是一個受歡迎的目標。眾所周知，Fortinet 的 VPN 產品中的一個已知錯誤 (CVE-2018-13379) 已被目標式勒索軟體攻擊者濫用。澳洲網路安全中心 (ACSC) 在 2021 年年中發布一份公告，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。在其他地方，已知 Canthroid（又名 Thieflock）透過利用 SonicWall VPN (CVE-2021-20016) 中的漏洞來入侵受害者。該漏洞已於 2021 年 2 月修補，但 Canthroid 仍繼續攻擊還在使用尚未修補軟體的組織。若此漏洞被成功利用，則允許攻擊者建立自己的憑證並加入目標網路。

最近據報導，2021 年 12 月發現的 Apache Log4j 中的漏洞被多個勒索軟體家族所利用。Dridex 殭屍網路被報告為已利用這些漏洞散播勒索軟體。與此同時，據報導一個名為 Khonsari 的勒索軟體家族，正試圖利用這些漏洞存取受害者網路。

案例研究：
殭屍網路：Emotet 的重返和存取代理的重要性

在過去幾個月中，勒索軟體感染媒介領域的最大發展是眾所周知的 Emotet 殭屍網路的重返。

Emotet 在 2021 年初被司法部門取締之前，是網路犯罪領域最惡名昭彰的殭屍網路之一。眾所周知，Emotet 充當各種威脅的散布者和載入器，但在消失之前，它與 Trickbot 和 Ryuk 勒索軟體的合作關係最為密切。當 Emotet 被強制下線並清理被它感染的電腦時，執法機關被認為取得重大勝利，但在 2021 年 11 月中旬，Emotet 重新出現。

雖然在以前的場景中，經常看到 Emotet 提供 Trickbot，但當它重返時，Trickbot 似乎被用來將 Emotet 放到受害裝置上，以重建殭屍網路。隨後 Advanced Intel 的一份報告稱，與 Conti 有關聯者參與 Emotet 的重返，據報導已成功說服前 Emotet 營運商重新投入，建立後端基礎設施並重振他們惡意軟體的功力。重返顯然是由對初始存取類型惡意軟體的需求驅動，據報導，Conti 相信透過將 Emotet 納入他們的勢力範圍，他們可以壟斷勒索軟體市場，因為這將使他們比競爭對手的勒索軟體營運廠商更具優勢。自從 Emotet 重新出現以來，也有人看到它放棄 Cobalt Strike，這是一種常見的預勒索軟體工具。

眾所周知，殭屍網路是勒索軟體攻擊者首選散布方法之一，而 Emotet 並非唯一用於散布勒索軟體有效籌載的殭屍網路。其他的有--用於此目的的已知殭屍網路包括前面提到的 Trickbot (與 Miner 相關聯)、Dridex (與 Hispid 相關聯) 和 IcedID (與 Conti 一起使用)。然而，Emotet 在其鼎盛時期就是一個特別強大的殭屍網路，如果它恢復到被取締之前的巔峰時期狀態，滲透率又與之前相似，則其對勒索軟體和網路犯罪態勢的影響將不容小覷。

結論

有跡象印證，到了 2022 年，勒索軟體仍將是網路犯罪領域的主要威脅。因為執法取締和制裁對勒索軟體開發商及其聯盟成員產生影響，勒索軟體領域的主要排名可能會繼續變化。然而，正如 Hispid (又名 Evil Corp) 所表明的那樣，僅靠制裁並不一定足以阻止這些勒索軟體同夥，而像這樣的行動只會迫使他們頻繁地重新改名稱。然而，在 2021 年變得很明顯，特別是自殖民地管道攻擊以來，當局越來越願意採取行動破壞和打擊勒索軟體和其他網路犯罪同夥。

2022 年前幾週發生的一件大事，是俄羅斯當局在俄羅斯逮捕 REvil 勒索軟體集團 14 名成員，俄羅斯司法部門表示，他們在收到美國當局關於涉嫌 REvil 成員的資訊後採取這一行動。這是俄羅斯警方一個非常不尋常的舉動，以往在俄羅斯境內的駭客組織或個人如果沒有成為當局立案目標，他們據信通常對在該國活動的大量勒索軟體集團的活動視而不見。這就是為什麼我們經常看到位於俄羅斯和其他獨立國協國家的電腦，被排除在勒索軟體試圖感染的國家名單之外。但是，如果最近的這次行動表明俄羅斯當局更願意對該國的勒索軟體集團採取行動，則可能會對勒索軟體領域產生重大影響。

儘管執法取締和逮捕重擊勒索軟體生態，但勒索軟體營運廠商仍在繼續創新。這一點在 Noberus 的開發中可看出端倪，Noberus 是第一個用 Rust 編碼的專業勒索軟體類型，已用於現實世界的攻擊和勒索軟體攻擊的新工具的開發，例如 ：SquirrelWaffle 載入器和 Exmatter 滲漏工具。Emotet 殭屍網路的重返，如果它能達到關閉前的影響力，也可能對 2022 年的勒索軟體格態勢產生重大影響。

雖然網路犯罪活動的變化快速特性，很難預測任何特定年度的網路犯罪領域會發生什麼，但大型企業組織今年將繼續面臨的主要威脅仍是有針對性的目標式勒索軟體攻擊，其受危害程度可能超越以往。這就是為什麼所有組織都必須制定有效的網路安全戰略，以保護自己並減緩有針對性的目標式勒索軟體攻擊之危害。

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。

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

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