2024 年第一季勒索軟體活動報告：儘管遭到執法單位圍剿，但仍然維持很高的活動水準

2024 年 7 月 11 日發布｜威脅情報

威脅獵手團隊
賽門鐵克

2024 年第一季的勒索軟體活動略有下降，因為兩個主要勒索軟體組織成為執法行動的目標

2024 年第一季，勒索軟體活動略有下降，這主要是由於兩個主要勒索軟體組織受到執法部門的圍剿。然而，整體活動水準仍呈上升趨勢，2024 年第一季的勒索軟體攻擊數量高於 2023 年同期。

分析勒索軟體洩漏網站的資料後發現，勒索軟體行為者聲稱發動 962 次攻擊，低於 2023 年第四季的 1190 次，但仍高於 2023 年第一季的 886 次。

整體活動水準的下降可能與 LockBit 和 Noberus 這兩個組織被執法單位圍剿有關，這兩個勒索軟體組織是 2023 年最多產的勒索軟體。2023 年 12 月，Noberus(又稱 ALPHV、BlackCat) 成為美國主導的執法行動的目標。儘管 Noberus 在接下來的幾周裡試圖捲土重來，但最終還是在 2024 年 3 月以執法行動的影響為由關閉了，有報道稱它與許多同盟的附屬組織鬧翻。同時，LockBit 在 2024 年 2 月成為第二次國際執法行動的目標，但它仍在繼續運作。

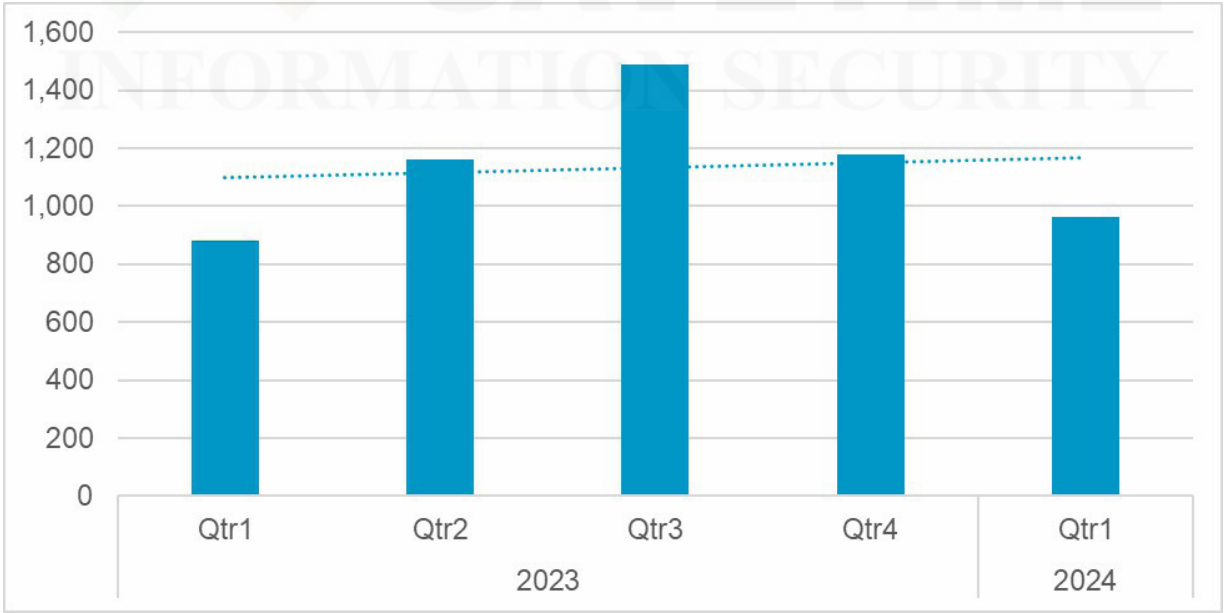

圖 1. 2023-2024 年營運資料外洩網站的行為者聲稱發起的勒索軟體攻擊。

在 2024 年第一季，LockBit 仍然是頭號勒索軟體威脅，在所有聲稱的攻擊中佔比超過 20%。緊隨其後是最近被報導已開始提供勒索軟體即服務的 Play(7%)、多產的 Phobos 附屬組織 8Base(6%) 和新出現的 Qilin 勒索軟體 (6%)。

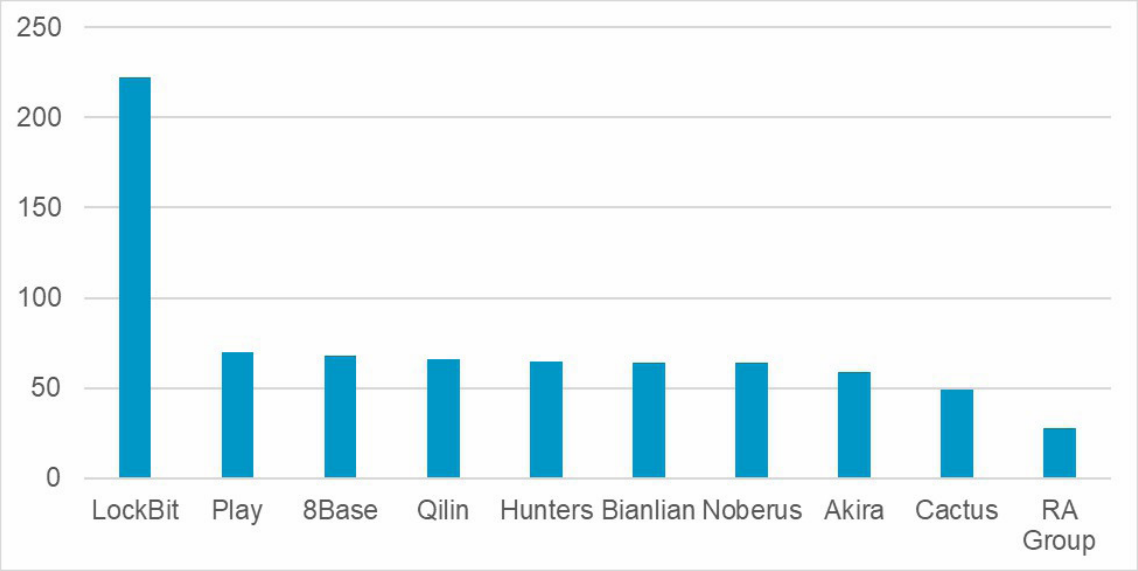

圖 2. 2024 年第一季依照聲稱攻擊次數統計最多的勒索軟體活動。

公開宣稱整體活動水準與賽門鐵克調查的勒索軟體活動之間再次出現巨大差異。在這兩種情況下，LockBit 在攻擊中所佔比例最大，而在賽門鐵克第一季調查的攻擊中，Akira 是第二大最熱門的勒索軟體系列 (14%)，但它只佔所有聲稱攻擊的 5.5%。同樣，Blacksuit 在賽門鐵克調查攻擊中佔 11%，但在所有公開報告的攻擊中僅佔 1.6%。透過比較，我們可以看出與每個活動有關行為者的成功率。要讓賽門鐵克確定攻擊與某個勒索軟體家族有關，攻擊必須發展到攻擊者嘗試部署有效載荷的階段。這表明使用 Akira 和 Blacksuit 的攻擊者更有可能將攻擊至少推進到有效酬載部署階段。

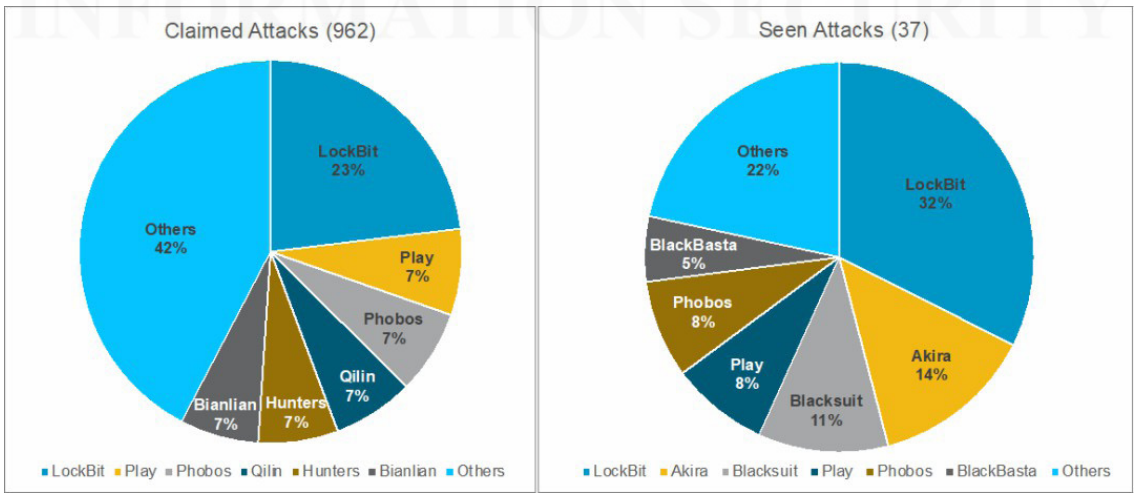

圖 3. 2024 年第一季，公開宣稱攻擊比例與賽門鐵克調查的勒索軟體攻擊比例。

攻擊途徑與手法

現有證據表明，利用面向公眾的應用程式中已知漏洞，仍然是勒索軟體攻擊的主要途徑。攻擊者持續以最近已揭露的公開漏洞 (一般而言，原廠都已經釋出修補程式) 為目標，試圖找到

未修補的系統。例如：最近幾週，賽門鐵克發現一個正在進行的攻擊行動，攻擊者利用最近披露的 PHP 漏洞攻擊網路伺服器。此漏洞 (CVE-2024-4577) 是一個 CGI 參數注入漏洞，影響安裝在 Windows 作業系統上的所有 PHP 版本。該問題也會影響安裝在 Windows 上所有版本的 XAMPP 開發環境。成功利用該漏洞可導致遠端程式碼執行 (RCE)。

一旦攻擊者獲得存在漏洞伺服器的存取權，他們就會下載一些工具，包括一個惡意 HTA 檔案，其中包含一個開源權限提昇工具 BadPotato 的副本；一個自定義的 Web shell；以及之前觀察到用於部署 TellYouThePass 勒索軟體的惡意軟體載入器。

改變戰術

在 2024 年第一季一個顯著進展是 Clop(又稱 Cl0p) 勒索軟體的重出江湖。Clop 由 Snakefly 網路犯罪集團經營，在 2023 年期間已不再使用，因為該集團開始放棄檔案加密勒索，轉而專注於資料竊取勒索。威脅者主要透過利用軟體中的零時差漏洞來實現這一目的，這些漏洞允許他們同時攻擊多個受害者，在活動被發現之前竊取他們的資料，並威脅說如果不支付贖金就公佈這些資料。在 2023 年 Snakefly 參與最引人注目的攻擊是利用 Progress Software 的 MOVEit Transfer 檔案傳輸應用程式之漏洞。然而，最近幾週，賽門鐵克的威脅獵人團隊發現 Clop 有效酬載再次被使用，這表明 Snakefly 正在重新發動傳統的雙重勒索攻擊戰術。

自帶漏洞驅動程式 (BYOVD) 仍然是勒索軟體組織青睞的戰術，尤其是作為停用安全防護軟體的一種手段。由於驅動程式已簽署並可獲得核心存取權限，因此經常被用來強制終止處理程序。正確編寫的驅動程式會包含檢查功能，以確保只有與之協作使用的軟體才能發出命令，而且只能用於預期目的。易受攻擊的驅動程式一旦落入壞人之手，則成為實質上的權限提昇工具。

近來最常見的此類工具是 Warp AV Killer，最近幾週至少有一個 LockBit 同盟附屬組織使用該工具，它利用一個易受攻擊的 Avira anti-rootkit 驅動程式來停用安全產品。

持續性的危險

儘管勒索軟體的運作在 2024 年經歷了較高程度的破壞，但對整體勒索活動的影響相對有限。在可預見的未來，勒索軟體仍將是企業面臨的主要威脅之一。

防護方案／緩解措施

有關 Alpha 最新的防護更新，請訪問賽門鐵克原廠最新的防護公告 (Protection Bulletins)。

入侵指標 (Indicators of Compromise)

如果 IOC 是惡意的並且我們能夠使用該檔案，Symantec Endpoint 產品將檢測並阻止該檔案。

4de4621da1b7da597c2c8def4c08b8d405672dadb9c70d7dffd647c8d6abd394 - Web shell

95279881525d4ed4ce25777bb967ab87659e7f72235b76f9530456b48a00bac3 - Loader

5e446efb6c4f296fb8f25ef7a1a0a482f51dc475bd5ef3e89be9d43782a9f60f – TellYouThePass
7d6877eb8a3e2da1e8b06e2ed41604c6c3d5ced8293f7cc7e760ba972303bd0e – TellYouThePass
f572898ab9f9a0fabac77d5d388680f84f85f9eb2c01b4e5de426430c6b5008f – TellYouThePass
7101db8cb05e989c018ebc5df47819029cd76c4093b22c4582288795e46f6689 – TellYouThePass
2881194b7e0939d47165c894c891737d8c189ee8fb4720e814a4bcdd804d00d1 – TellYouThePass
ea59d6a130a279dfde4df53640bd720419c7b5d9711a21a78af9453b1b3b5805 – TellYouThePass
170d654b61810992fef6f18dbce5b4c7f5762cf36c9b41c36a14c9f6609f6e7d – TellYouThePass
aa0ef20f9f8ca111b0d8a550daf6651f5b0557f0acb0a26545755c5a02263a9b – TellYouThePass
3e65437f910f1f4e93809b81c19942ef74aa250ae228caca0b278fc523ad47c5 – TellYouThePass
2fc2d747847eb04561a435e65954f0103101e2190458eb3c125deda49326c597 – TellYouThePass
21ff399e57cc306a1ae1daab6009ea40c8aa96c39296d0f8781626de6bd19256 – TellYouThePass
d18453e564ca27514227478f225d85811fe15d08aa5fb1f613022c43155c5c54 – TellYouThePass
9562ad2c173b107a2baa7a4986825b52e881a935deb4356bf8b80b1ec6d41c53 – TellYouThePass
3f41e2ceff3a04cd6de6aadce7e7b7c8584940e4320a7db55dd712debb061510 – Clop
4d571f4d0008deb01e3144e0e3d5f882c5422acfcb4dd260082852a822d8d2fb – Clop
6192488729850a7a28498f233346e856b0097e4b3160baa641f8cf9571b56da8 – Clop
a702a671b7911a09ccb5b4f42923e8b301e0bbb851443dd52622022959a3055a – Clop
bef2d817f1813eb0629222112fd3721865a2a4eb1f4d51ad1f09fd807d4380ab – Clop
f6afa84b0847414220bb15517b8b5e2c505b64b53efbba73b753379c66ac5017 – Clop
6fb438feeb8369c5b82bfaa77144a641f7645c321f0b24dd97cfe2687b1ebd44 – Suspected Clop
88efa81984852dac62d325f2091a09de1e6423a711d7913aeac103c50664cf84 – Suspected Clop
38f0750cbe49b30db326b53b9f752b66c4f5e23cc3bbbd6d1844e2878a19b9a7 – Suspected Clop
aa43f34c3fa67aea994c1babeb71b46c7b24eccaa0455ae21aa561e251e7cc4d – Suspected Clop
1453179d46ef89eb780f8b82632f352017a3586e8d49fc3f087f633f7bebbf0a – Warp AV Killer
67e4c18e80d4d1acb9395f4a1fe9c2a75d95fcccdb33bcdd5259ba6f47e60e57 – Warp AV Killer

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/threat-intelligence/ransomware-q2-2024
本文件由保安資訊有限公司專業細心整理後提供。如有遺誤、更新或異動均以上Symantec原廠公告為準，請知悉。2024/7

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)

關於賽門鐵克 (Symantec)

賽門鐵克 (Symantec) 已於 2019/11 併入全球網通晶片巨擘--博通 (BroadCom，美國股市代號 AVGO，全世界網際網路流量有 99.9% 經過博通的網通晶片) 軟體事業部的企業安全部門 (SED)，特別是近年以半導體的嚴謹、系統化以及零錯誤思維來改造核心技術、管理框架以及整合最完整的資安生態體系，讓賽門鐵克的解決方案在穩定性、相容性、有效性以及資安生態系整合擴充性，有著脫胎換骨並超越業界的長足進步。博通 (Broadcom) 是務實的完美主義者，致力於追求卓越、關注細節並且有系統和紀律地投入科技創新與嚴謹工藝，同時也大大降低交易複雜性。Symantec 持續創新的技術能為日新月異的資安問題提供更好的解決方案，近三年 Symantec 很少出現在由公關機制產生的頭版文章中，而且在全球前兩千大企業的市佔率及營收成長均遠遠高於併入博通之前，增長幅度也領先其他競爭對手，是科技創新驅動的解決方案非常穩健可靠深受大型企業信賴的實證，也顯示大型企業顧客對轉型中的新賽門鐵克未來充滿信心。(美籍華人王嘉廉創辦的企業軟體公司，組合國際電腦（CA Technologies）以及雲端運算及「硬體虛擬化」的領導廠商--VMware， 也是博通軟體事業部的成員)。2021 年八月，因應國外發動的針對性攻擊日益嚴重，美國網路安全暨基礎架構安全管理署（CISA）宣布聯合民間科技公司，發展全國性聯合防禦計畫 JCDC(Joint Cyber Defense Collaborative)，而博通賽門鐵克是首輪被徵招的一線廠商，如就地緣政治考量，Symantec 也絕對是最安全的資安廠商。擁有更強大資源與技術為後盾的賽門鐵克已更專注於整合各種最新科技於既有領先業界的端點、郵件、網頁以及身分認證等安全解決方案。

關於保安資訊 www.savetime.com.tw

保安資訊團隊是台灣第一家專注在賽門鐵克解決方案的技術型領導廠商，被業界公認為賽門鐵克解決方案專家。自 1995 年起就全心全力專注在賽門鐵克資訊安全解決方案的技術支援、銷售、規劃與整合、教育訓練、顧問服務，特別是提供企業 IT 專業人員的知識傳承 (Knowledge Transfer)、協助顧客符合邏輯地解決資安問題本質的效益上，以及基於比原廠更孰悉用戶使用情境的優勢能提供更快速有效的技術支援回應，深獲許多中大型企業與組織的信賴，長期合作的意願與滿意度極高。許多顧客樂意與我們建立起長期的友誼，把我們當成可信任的資安建議者、可以提供良好諮商的資安策略夥伴以及總是第一個被想到的好用資源。

保安資訊連絡電話：**0800-381-500**。