勒索軟體：第三季威脅程度仍較高

2024 年 10 月 17 日發布｜威脅情報

威脅獵手團隊
賽門鐵克

最近成立的 RansomHub 組織取代 LockBit 成為最多產的勒索軟體活動

今年第三季度，勒索軟體攻擊持續以接近高峰的等級發生，新成立的 RansomHub 組織也取代老牌的 LockBit 組織，成為第一大勒索軟體威脅。

從勒索軟體外洩網站的資料分析發現，勒索軟體攻擊者聲稱 2024 年第三季發生 1,255 起攻擊，較第二季的 1,325 起略有下降，但攻擊總數仍在繼續呈現上升趨勢。

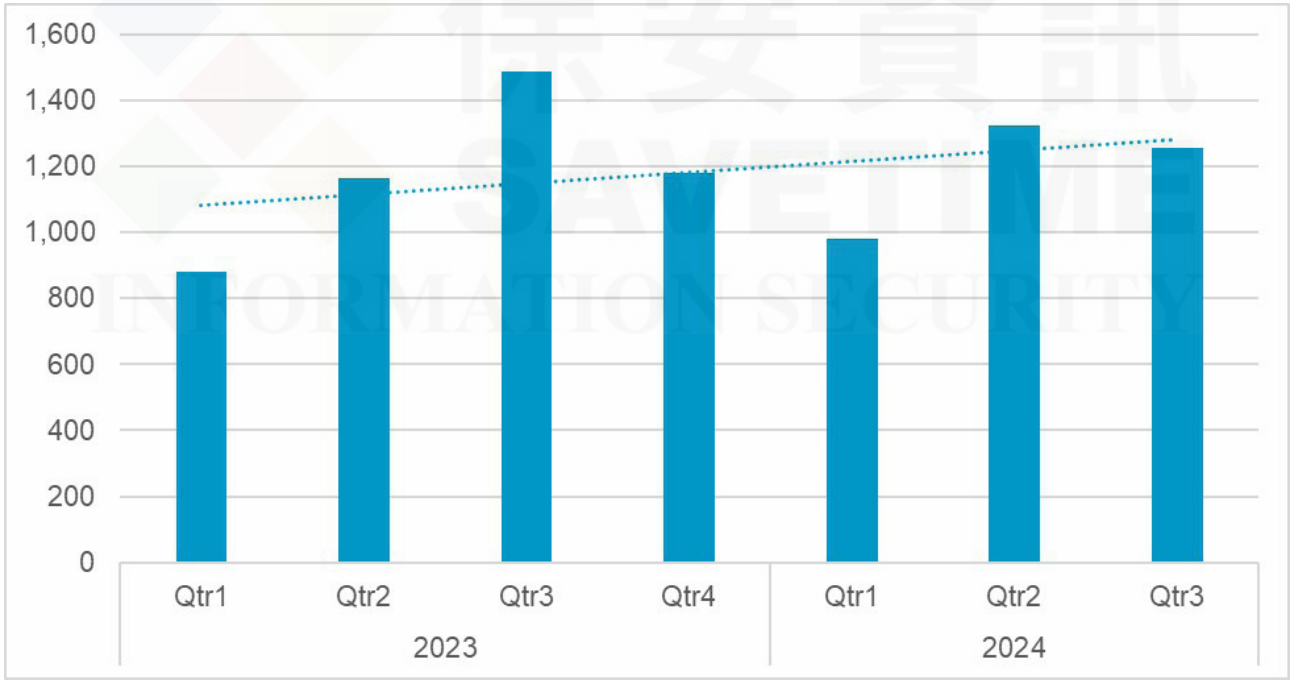

圖 1. 2023~2024 年，經營資料外洩網站的攻擊者聲稱勒索軟體攻擊數量

本季最大的情況是 LockBit 的衰落，該公司之前是勒索軟體生態系統的主導者，第二季度攻擊次數是其最接近競爭對手 Qilin 的三倍多。第三季聲稱 LockBit 攻擊數量為 188 起，低於第二季 353 起攻擊。 LockBit 是 2024 年 2 月國際執法行動的目標，其影響今年第一季的活動水準。到第二季，它似乎完全恢復了，但該行動可能導致 LockBit 附屬公司之間失去信任，特別是因為當局表示他們已經收集可以識別附屬公司的資訊。

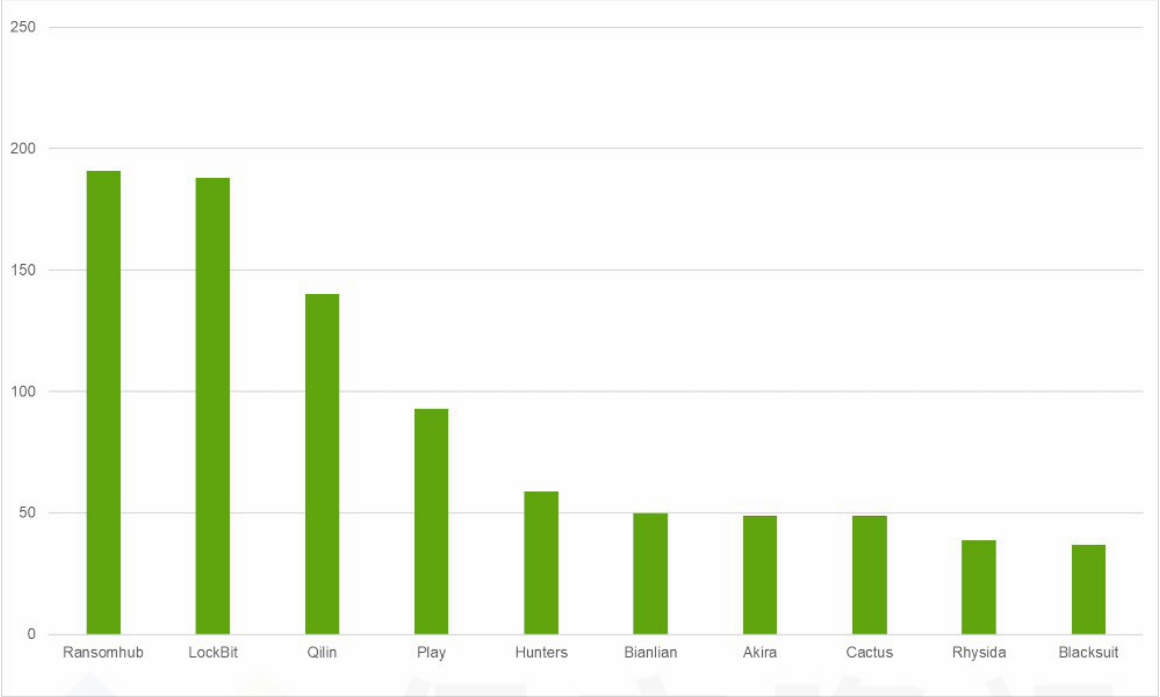

圖 2. 2024 年第 3 季，依所宣稱最多產的勒索軟體活動

LockBit 下降的最大受益者是 RansomHub，該公司於 2024 年 2 月才開始活躍，但就其承認的攻擊數量而言，是現在排名第一的勒索軟體活動。 RansomHub 在第三季號稱發生 191 次攻擊，高於第二季 75 次。該組織的迅速崛起可能是因為其成功為其勒索軟體即服務業務招募經驗豐富的附屬機構，據報道，該機構提供的條款比競爭對手更具吸引力。

另一個加強攻擊的組織是 Qilin(又稱 Agenda)，該組織在第三季發動 140 次攻擊，高於第二季 97 次。

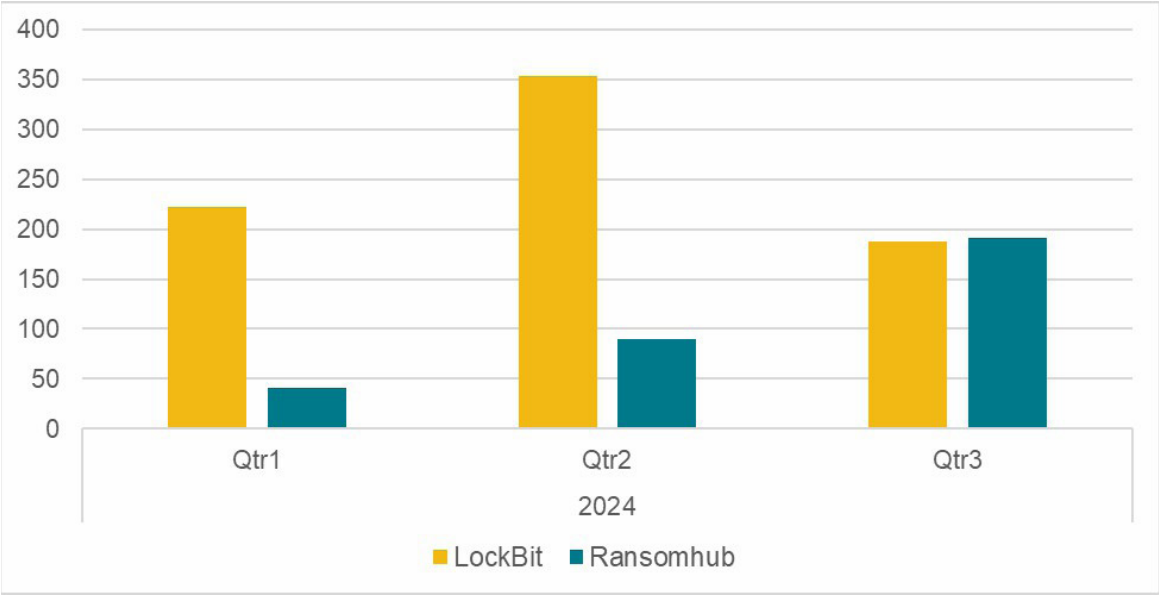

圖 3. LockBit 和 RansomHub 所承認的攻擊，2024 年第一季至第三季

公開聲稱的整體活動水準與賽門鐵克調查的勒索軟體活動之間再次存在顯著差異。雖然 LockBit 在所承認的攻擊數量中仍然佔據很高的比例，但它僅佔賽門鐵克第三季調查攻擊中的 7%。雖然 RansomHub 佔公開聲稱攻擊的 15%，但它在賽門鐵克調查攻擊裡有可靠的識別度，這部份支持有關其正在從競爭對手組織招募經驗豐富的附屬攻擊者報告。

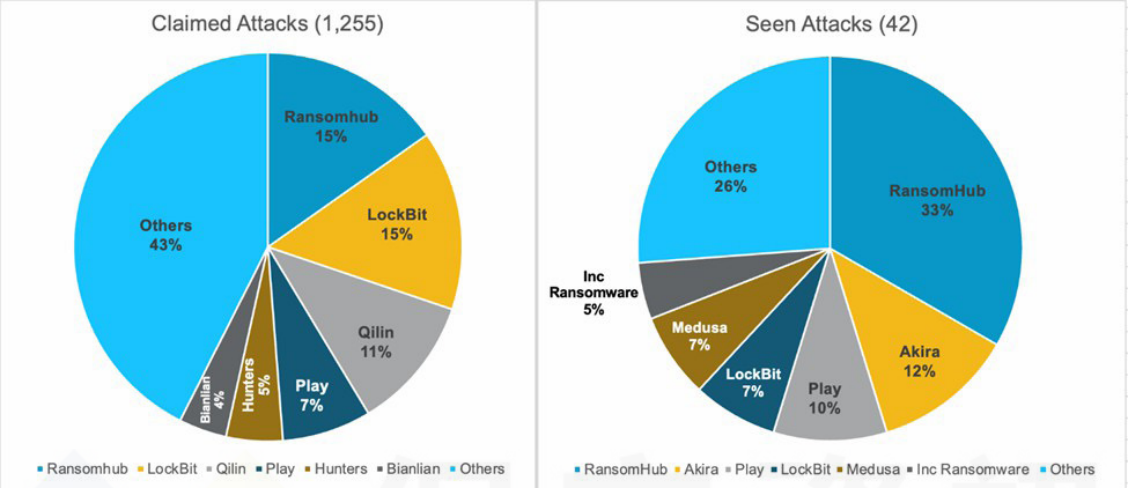

圖 4. 公開聲稱的攻擊的比例與賽門鐵克調查的勒索軟體攻擊的比例，2024 年第 3 季

兩用工具

目前勒索軟體攻擊是複雜且多階段入侵，涉及部署多種工具，而且攻擊者通常需要進行大量的鍵盤操作活動。對勒索軟體攻擊中最常見的工具分析顯示目前勒索軟體攻擊者最喜歡的策略、技術和程序 (TTP)。

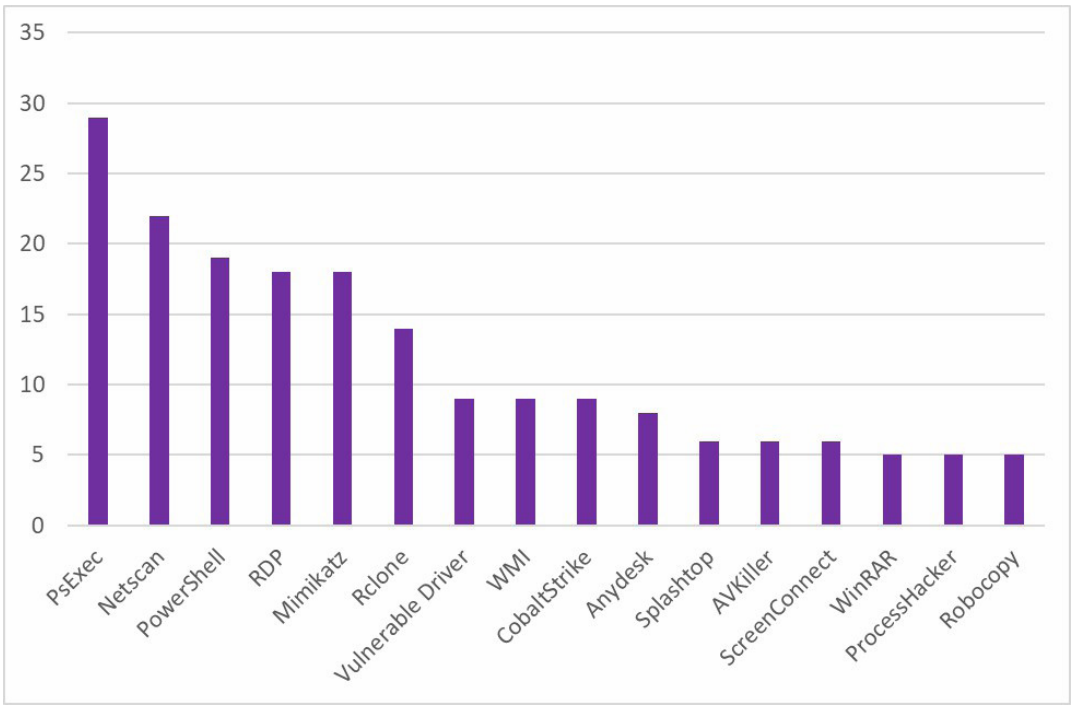

圖 5. 2024 年 1~9 月，勒索軟體攻擊中最常見的工具

這些工具主要分為四大類：

Living off the Land：可被攻擊者利用的 Windows 環境本機常用程式。攻擊者可以利用 PsExec 和 WMI 等工具在網路上橫向移動並在遠端電腦上執行命令。同時，PowerShell 是一種功能強大的腳本工具，可用於執行命令、下載有效負載、橫向移動和進行偵察。

削弱防禦：越來越多的攻擊者正在使用利用自帶易受攻擊的驅動程式 (BYOD) 技術的工具。攻擊者將帶有簽章的易受攻擊的驅動程式部署到目標網路，並使用該驅動程式來停用安全軟體。該驅動程式被授予核心存取權限，這意味著它們可以用來終止進程。在大多數情況下，易受攻擊的驅動程式與惡意可執行檔一起被部署，惡意可執行檔將使用該驅動程式發出指令。

遠端桌面／遠端管理：雖然這些軟體套件合法用於遠端管理或技術支援，但攻擊者正在轉向使用它們，因為它們可有效地提供對電腦的後門存取。RDP、AnyDesk、Splashtop 和 ScreenConnect 等工具經常被勒索軟體攻擊者部署。

資料外洩：大多數勒索軟體團體都會進行雙重勒索攻擊，在加密之前從受害者的網路中竊取資料，並利用洩露被盜資料的威脅作為另一種形式的操作利用。Rclone 是最常用的滲漏工具。勒索軟體攻擊者使用許多遠端管理套件也具有滲透功能。

強大的生態系統

RansomHub 和 Qilin 等勒索軟體業務的成長與 LockBit 的競爭並不是什麼好消息，因為這可能會使勒索軟體生態系統更加強大，並且在主要的營運商被取締或下線時不太可能遭受重大破壞。

防護方案／緩解措施

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

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://www.security.com/threat-intelligence/ransomware-threat-level-remains-high
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。2024/10

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**。