Acronis

2022 年
報告

Acronis 網路資安防護營運中心報告：

2022 年年終報告及 2023 年網路威脅預測

Acronis
網路資安防護營運中心報告

目錄

作者：

Alexander Ivanyuk
Acronis 產品與技術定位部
資深總監

Candid Wuest
Acronis 網路資安防護研究部
副總裁

Irina Artioli
Acronis 網路資安防護
傳授專員

簡介與摘要

Acronis 是第一家開始執行全方位整合式網路資安防護來保護所有資料、應用程式和系統的公司。網路資安防護需要對威脅進行主動式研究和監控，以及遵循 SAPAS 的五大面向：安全、易用性、隱私權、真實性和安全性。基於此策略，Acronis 在全球建立了四個網路資安防護營運中心，全年無休 (24/7) 地監控和研究網路威脅。

Acronis 對於目前的旗艦產品進行了升級：Acronis Cyber Protect Cloud 作為一款雲端解決方案新增至 Acronis Cyber Cloud 平台，而 Acronis Cyber Protect 15 則是一款地端部署解決方案。在這些發行之前，Acronis 憑藉其創新 Acronis Active Protection 防勒索軟體技術一直是資料防護市場的領導者，隨著時間的推移，該技術證實公司在化解以資料為目標之威脅方面的獨特專業經驗。然而值得注意的是，Acronis 在 2016 年研發的人工智慧 (AI) 和行為型偵測技術已擴展為可處理所有形式的惡意軟體和其他潛在的威脅。

該報告涵蓋依 Acronis 檢測和分析人員在 2022 年下半年之所見分析得出的威脅態勢。報告中提供的一般惡意軟體資料收集於今年七到十一月，反映我們在這幾個月內觀察到的、以端點為目標的威脅。

該報告代表一個全球視角，以超過 750,000 個、遍佈於世界各地的特有端點的資料為基礎撰寫。討論的大多數統計資料關注的是針對 Windows 作業系統的威脅，因為它們比 macOS 和 Linux 更流行。

此報告的五個重要數據：

- 2022 年第三季度遭受攻擊次數最多的國家/地區 (依每個使用者的惡意軟體) 是韓國、約旦和中國。
- 2022 年 7 月到 11 月，Acronis 在端點上阻止了大約 4 千萬個 URL，過去兩個的數字明顯高於夏季的數字。
- 收到的所有電子郵件中，30.6% 的電子郵件是垃圾郵件，1.6% 的電子郵件包含惡意軟體或網路釣魚連結。
- 預計 2023 年資料外洩的平均成本會達到 500 萬美元。
- 2022 年第三季度，平均 7.7% 的端點嘗試了存取一些惡意 URL，較第二季度的 8.3% 稍微下降。

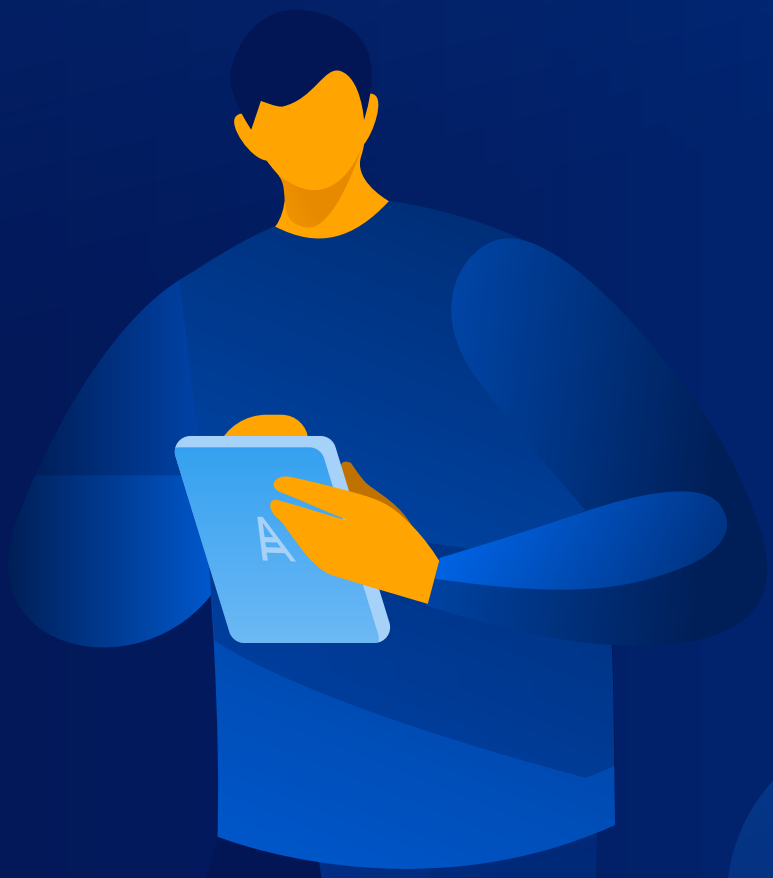
以下是 Acronis 在 2022 年下半年觀察到的網路資安趨勢：

- 勒索軟體仍然是政府、醫療保健和其他關鍵組織等大中型企業的頭號威脅。
- 認證外洩或遭竊是 2022 年上半年報告的幾乎一半的資料外洩事故的原因所在。遭竊的認證仍然是資料外洩背後的驅動力，攻擊者可借助這些認證輕鬆執行網路釣魚和勒索軟體活動。
- 在 12,985 個報告的弱點中，有 475 個弱點在 2022 年上半年遭到積極利用。
- 2022 年 7 月到 10 月，網路釣魚攻擊的比例增加了 1.3 倍，現在佔所有攻擊的 76% (相較於 2022 年上半年的 58% 有所上升)。

在此報告中，您將發現：

- 以下是 Acronis 在 2022 年下半年觀察到的重大安全性/威脅趨勢
- 為什麼 Acronis 會看到越來越多的資料外洩
- 一般惡意軟體統計資料和重要系列審核
- 含部分最危險威脅之深入分析的勒索軟體統計資料
- 哪些弱點會促成攻擊成功進行
- Acronis 安全性建議
- Acronis 對 2023 年的安全性預測

2022年下半年重要的網路威脅和趨勢



1. 勒索軟體的數量下降了，但威脅比以往任何時候都要大

不幸的是，勒索軟體威脅仍在惡化。雖然我們看到攻擊、樣本和新系列的數量有所下降，但現有的系列對運作它們的網路罪犯來說表現不錯。今年下半年，勒索軟體團體每個月都會在其混合清單上新增 200 到 300 個新的受害者。到第三季度末，主要運營商發佈的遭入侵目標總數如下所示：

當一些產品系列，或確切地說是「勒索軟體」品牌（例如 Egregor、REvil、BlackMatter 和 DoppelPaymer）退出了市場，它們背後的人只需進行品牌重塑即可開始新的營運。這種策略可讓他們避開執法活動（或至少降低他們的進度），多爭取幾個月，甚至是幾年的成功犯罪活動。

我們以前看到過這樣的例子：WastedLocker 再次出現為 Hades 勒索軟體或 Cryptolocker，隨後在秋季變更為 PayloadBin 和 Macaw。DarkSide 勒索軟體已重塑為 DarkSide 2.0，接著再次變為 BlackMatter。今年初，BlackCat 勒索軟體團體已證實，他們是 DarkSide/BlackMatter 營運的前成員。

雖然執法單位在 2022 年與勒索軟體運營商的鬥爭中取得了一些重大的成功，但網路罪犯仍是贏家。荷蘭國家警署與網路資安機構 Responders.NU 進行了合作，透過偽造贖金支付引誘 DeadBolt 勒索軟體團體交出 155 個解密金鑰。可惜的是，在意識到他們被騙並不會獲得付款後，DeadBolt 團體改變了他們的策略，現在要求雙重確認之後才釋放解密金鑰。

「明面」的巨大勝利是最近在加拿大逮捕了一名俄羅斯籍 LockBit 成員（此人負責索要贖金）。但是根據歐洲刑警組織的說法，他很可能是整個網路罪犯運營的一個會員，而非管理人員。主要發動者仍在外面作惡。

2022 年勒索軟體領域的四大巨頭

如上所述，勒索軟體運營商的市場實際上只由 4-5 個參與者支配。2022 年最活躍的四個是 LockBit、Black Basta、Hive 和 BlackCat。

當然，其他參與者仍然存在，只是造成的損害要小得多。STOP、Inlock、Dharma、Xorist、Venus、Cuba、Pendragon、Chaos、Killnet、Zeppelin 之類的集團仍在積極發佈新的樣本並感染使用者。

我們來看看勒索軟體領域的主要威脅執行者引起的一些案例：

LockBit 3.0

LockBit 是目前最先進的勒索軟體系列之一。它採用了大量的防偵錯、防偵測機制，可以停用 Windows Defender 和刪除備份。2022 年 9 月，Twitter 上公佈了一個被洩漏的 LockBit 3.0 建立器。集團發言人「LockBitSupp」聲稱，該團體未被駭客入侵，而是譴責一位前開發人員洩漏了訊息。無論如何，我們希望看到這一事件的後果，因為其他組織利用洩漏的程式碼來武器化自己的攻擊。

不幸的是，與此同時，我們必須說 LockBit 運營商的表現非常不錯。他們在市場上遙遙領先，根據各種專家的估計，市場佔有率高達 40-50%，并且繼續將越來越多的高知名度受害者新增到其清單中。

7 月，LockBit 攻擊了 FAAC（Fabbrica Automatismi Apertura Cancelli）集團。該集團在五大洲的 53 家公司合併銷售額超過 6 億歐元，在全球擁有超過 3,600 名員工。其次是對擁有 2,740 名員工、年收入超過 5.13 億美元的 La Poste Mobile 進行了攻擊。

LockBit 繼續對加拿大安大略省聖瑪麗斯鎮（擁有 7,500 位居民）和科羅拉多弗雷德里克鎮（人口為 15,000）進行了攻擊。該集團索要 20 萬美元的贖金才不會公佈被竊取的資料。

IHG 目前在 100 多個國家/地區運營著 6,028 家酒店，遭受了網路攻擊。目前還不知道誰發動了此次攻擊，但最近 Lockbit 勒索軟體團隊聲稱對 Holiday Inn Istanbul Kadıköy 發動了攻擊。

日本科技公司 Oomiya 也遭受了攻擊。Oomiya 年收入達 5 千萬美元，擁有大約 500 名員工。該企業專注於設計和製造微電子和設施系統設備。該事件可能會對第三方組織有重大的影響，因為 Oomiya 是全球多個行業主要組織的供應鏈，其中包括製造業、半導體、汽車、通訊和醫療保健。

巴西利亞銀行 (BRB) 被索要大約 50 個比特幣，以避免公開洩漏被存取的內容。Pendragon 集團在英國擁有超過 200 家汽車經銷商，年收入超過 39 億美元，被要求支付 6 千萬美元來解密這些檔案並保密。Pendragon 向英國當局通知了該事件，報告已移交到執法機構進行調查。有趣的是，當瑞典公司 Hedin Mobility Group 提出以超過 4.5 億美元收購 Pendragon 時，LockBit 攻擊了他們。

Black Basta

如我們之前報道，Black Basta 出現在 2022 年 4 月左右，由 Conti 和 REvil 勒索軟體團體的前成員組成，他們具有相似的策略、技術和程序。就在最近，SentinelLabs 的安全研究員發現了將 Black Basta 勒索軟體團體與具有財務動機的駭客集團 FIN7 (亦稱為 Carbanak) 關聯的證據。我們將看到其發展情況，Black Basta 已成功進行一些大型攻擊。

年收入超過 110 億美元的 Knauf 集團已成為 Black Basta 的受害者。Knauf 是全球領先的建築材料製造商，雇用超過 35,000 人，運營著 150 個生產場地。

11 月，加拿大食品零售巨頭 Sobeys 在週末遭受到攻擊。此連鎖店擁有超過 134,000 名工作人員，為加拿大 10 個省 1,500 個雜貨店和藥店提供服務。Sobeys 是加拿大僅有的兩家大型食品雜貨商之一，在 Sobeys、Safeway、IGA、Foodland、FreshCo、Thrifty Foods 和 Lawtons Drugs 零售之名下經營。Black Basta 勒索軟體對 Sobeys 的電腦進行了加密，並在本報告發佈的同時，攻擊者正在與公司代表進行談判。

Hive

Hive 勒索軟體團體也獲得了巨大的成功。最近印度最大的電力公司 Tata Power 也成為了受害者。該公司透過經銷商為超過 1200 萬位客戶提供服務，收入超過 50 億美元。Hive 的運營商將竊取的資料發佈在其洩漏網站上；檔案包括合約、財務和業務文件、工程專案和員工的個人可識別資訊 (PII)，例如 Aadhaar 卡號。此外，資料傾印還包含工程圖、財務和銀行記錄以及客戶資訊。

在此之前，Hive 將 Eurocell 新增到其受害者清單，索要 600 萬美元。Eurocell 是英國的一家建築產品經銷商，年收入 4.2 億美元。

Hive 勒索軟體還攻擊了 Bell 加拿大子公司 Bell Technical Solutions (BTS) 的系統。BTS 是一家獨立的子公司，擁有 4,500 多名員工，專門在 Ontario 和 Québec 省安裝 Bell 服務。

在全球擁有 130 家門店的法國服裝公司 Damart 也受到了攻擊，92 家門店受到了影響。Hive 運營商要求 200 萬美元的贖金。

BlackCat/ALPHV

BlackCat 集團以其三重勒索策略而聞名，在竊取公司資料後，如果要求得不到滿足，受害者就收到洩漏和分散式阻絕服務 (DDoS) 攻擊的威脅。BlackCat 在 2022 年下半年有著各種大目標。

他們聲稱從歐洲天然氣管道運營商 Creos Luxembourg S.A 竊取了超過 150 GB 的資料。該公司年收入 2.9 億歐元，擁有超過 800 名員工。

日本著名的視訊游戲公司 Bandai Namco 也遭受了攻擊，該公司以發佈包括 Elden Ring、Pac-Man 和 Tekken 在內等衆多視訊游戲而聞名，其年收入約 73 億美元。

BlackCat/ALPHV 勒索軟體是義大利能源服務組織 Gestore dei Servizi Energetici SpA (GSE) 遭受攻擊的幕後黑手；網路罪犯從其 IT 基礎架構中竊取了大約 700 GB 的資料。

巴西第二大電視台 Record TV、SBT 和 TV Cultura 最近也遭受了網路攻擊。目前還不清楚這些行動是否協調，但勒索軟體涉及到其中，并且 BlackCat 被懷疑是罪魁禍首。該事件對內部網路、電話服務、郵件和當地電視頻道的傳輸產生了影響。廣播公司尚未發佈公開的評論，但他們不得不暫停直播節目的傳輸。

其他值得注意的案例

當然，其他集團也很活躍，入侵了全球多個大中型企業。

德國電子製造商 Semikron 遭受了 LV 勒索軟體集團的攻擊。Semikron 在全球 24 個辦事處擁有超過 3,000 名員工，年收入達 4.6 億美元。

阿根廷 Córdoba 的司法機構成為 PLAY 勒索軟體集團的受害者。目前還不清楚 PLAY 如何外洩司法機構網路，但在 3 月，員工的電子郵件地址清單在 Lapsus$ 外洩 Globant 的過程中被洩漏。

Clop 勒索軟體團體聲稱從 South Staffs Water 竊取了 5 TB 資料，該組織年收入 3.35 億美元，每天向 160 萬名消費者提供 3.3 億升的飲用水。

年收入 2.7 億歐元的希臘最大天然氣經銷商 DESFA 表示，在 Ragnar Locker 勒索軟體的網路攻擊後，他們遭受了有限範圍的資料外洩和 IT 系統中斷。Ragnar Locker 團體還聲稱是葡萄牙 TAP Air 攻擊的負責人。該團體在其資料洩漏網站上發佈了一個新的條目，該網站包含 9,000 多位客戶的個人資訊。

網路犯罪集團 RansomHouse 聲稱已入侵了義大利的八個地區，並發佈了從弗洛倫薩托斯卡納聯盟竊取的全部 2.1 TB 的資料。在這則訊息中，RansomHouse 宣稱他們對義大利政府基礎架構的攻擊利用了弱式密碼習慣，例如使用「12345678」來保護敏感資料安全。

距離巴黎中心 28 公里且擁有 1000 個床位的醫院 Center Hospitalier Sud Francilien (CHSF) 遭受了網路攻擊。這家為 600,000 位居民提供服務的醫療中心被迫將患者轉到其他機構，並延遲了手術預約。攻擊者要求 1 千萬美元的贖金來換取解密金鑰。

Bombardier Recreational Products (BRP) 於 2022 年 8 月 8 日披露，RansomEXX 勒索軟體團體聲稱對其遭受的網路攻擊負責。BRP 擁有超過 20,000 名員工，年銷售額進 60 億美元，並在 120 多個國家/地區分銷各種產品。RansomEXX 在其資料洩漏網站上列出了 Bombardier 娛樂產品，以及據稱從該公司竊取的進 30 GB 的檔案。這些檔案包括保密合約、護照和 ID、材料供應合約、合約續約等。該公司在聲明中公佈了其內部調查的初步結果，稱攻擊者透過供應鏈攻擊外洩了其系統。

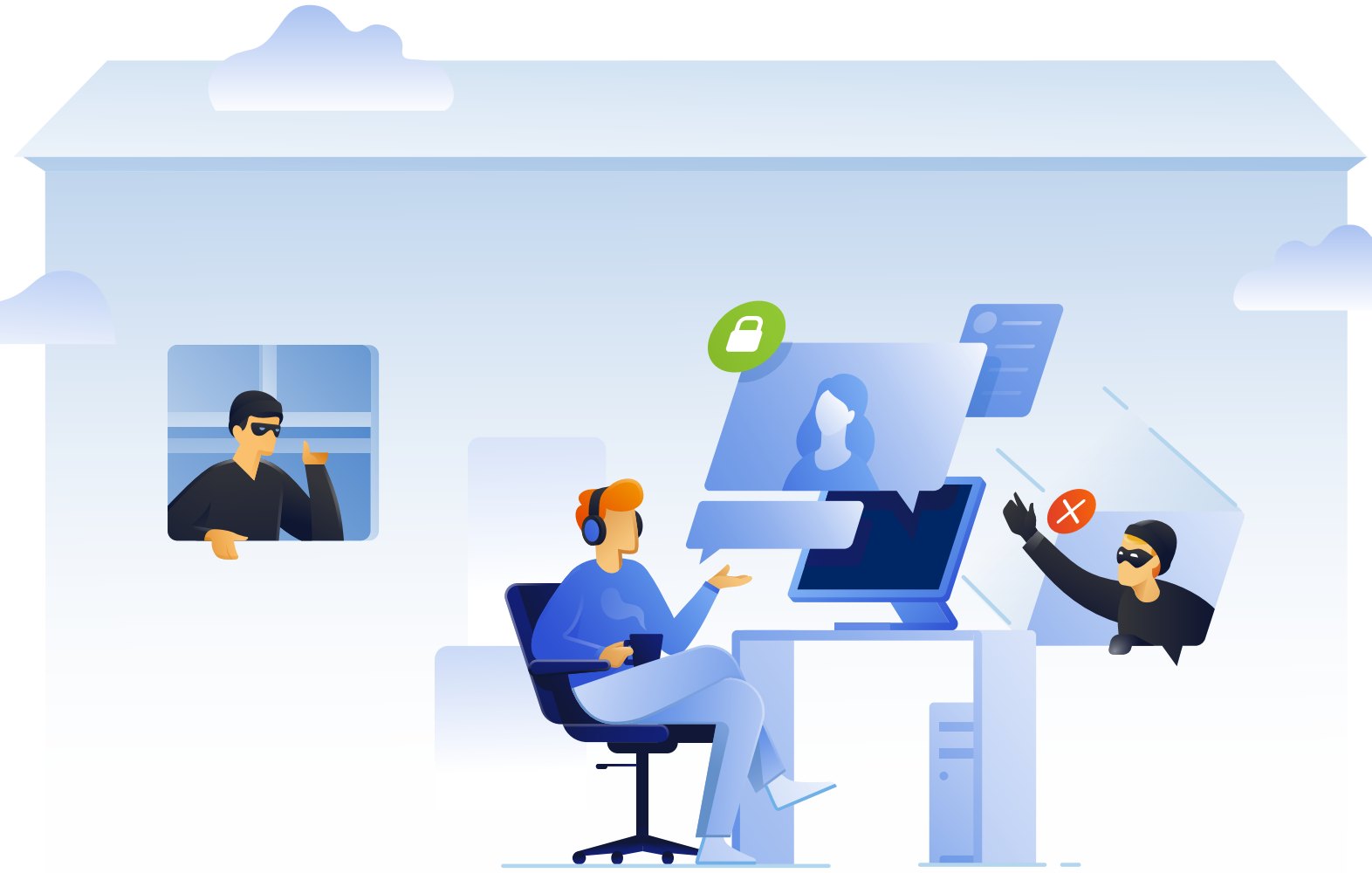
Consorci Sanitari Integral (CSI) 是 RansomEXX 的另一個受害者。該事件影響了 Barcelona 和 Baix Llobregat 所有組織的醫療中心，讓工作人員無法存取患者資訊或程序。CSI 是一個公共實體，擁有大約 3,500 名員工，隸屬於 Sant Joan Despí 和 l' Hospitalet de Llobregat、Consell Comarcal del Baix Llobregat 和 Creu Roja 的醫療部。它包含 13 個中心，為公共衛生和初級保健、醫院和社會健康中心 (兩個地方) 的患者提供服務；CSI 還管理著 Barcelona 和 l' Hospitalet 的

撫養和殘疾評估服務。雖然醫療管理部未提供具體細節，但此事件的經濟影響遠遠大於毒品走私。

Vice Society 勒索軟體團體聲稱他們從 Los Angeles Unified School District (LAUSD) 竊取了超過 500 GB 的資料。該地區擁有超過 640,000 名學生。

Everest 勒索軟體集團聲稱可以存取南非公共機構 Eskom Hld SOC Ltd 的所有伺服器。攻擊者要求支付 200,000 美元的贖金 （可用比特幣或門羅幣支付） 來購買套件，其中包括含 Linux and Windows 伺服器的管理員、root 和系統管理員密碼的伺服器。Eskom 是一家國有電力公司，為南非和南部非洲發展共同體 (SADC) 地區的客戶提供超過 90% 的電力。Everest 的運營商曾在 2022 年 3 月宣稱以 125,000 美元價格出售了南非電力公司的根存取權，但當時 Eskom 否認存在任何安全漏洞。當 Everest 集團最進再次發佈了 Eskom 漏洞時，安全性專家指出，這家公共事業機構正在經歷一些伺服器問題。

由於我們不得不談論房間裡的大象，Cisco 最近宣佈其基礎架構被 Yanluowang 勒索軟體團體外洩。隨後的調查顯示，沒有任何內容被竊取或洩漏。



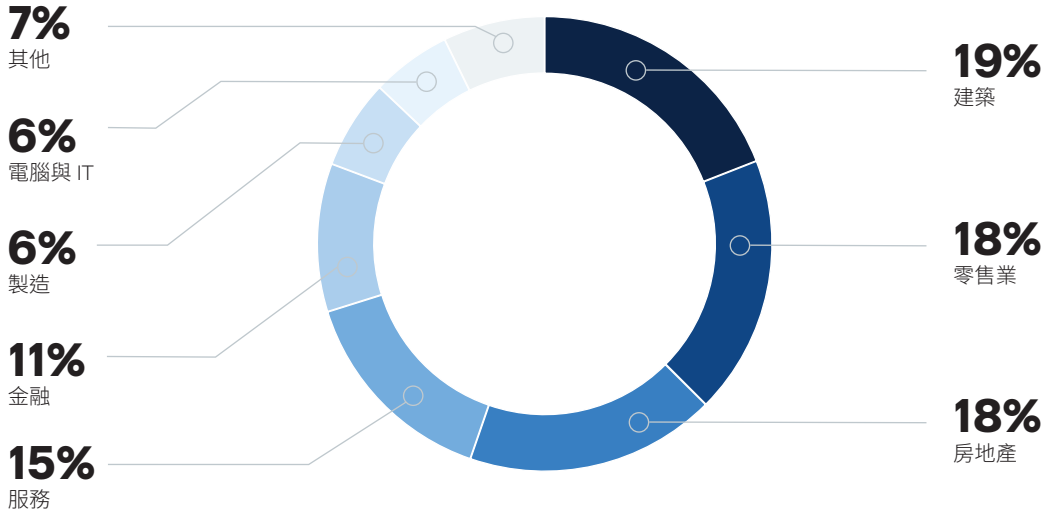
2. 網路釣魚和惡意電子郵件仍然是主要的感染載體

以下電子郵件和網路釣魚統計資料來自 Acronis Cyber Protect Cloud 的 Advanced Email Security 附加元件套件，該套件由 Perception Point 提供技術支援。Acronis 和 Perception Point 攜手時刻為組織提供保護，確保他們免遭電子郵件帶來的威脅。這些資料收集於 2022 年下半年，與端點上 Acronis 惡意軟體遙測資料和 URL 區塊相結合。

在此期間，我們發現電子郵件夾帶威脅的數量顯著增長。惡意訊息的比率在短短 4 個月上升了 0.6 個百分點（增加了 60%）。垃圾郵件比率在同一時期增加了 15% 以上，目前佔所有傳入流量的 30.6%。值得注意的是，與 Perception Point 對其他客戶的基準相比，Acronis 客戶更容易受到垃圾郵件攻擊，後者的垃圾郵件率達到 19.3%。不過，這還沒有結束：我們預計在 12 月因假期原因還會有一次上漲。

沒有人是安全的，電子郵件夾帶攻擊幾乎針對所有行業。但對前 50 個遭受攻擊次數最多的組織的分析建議，以下行業面臨的風險最大：

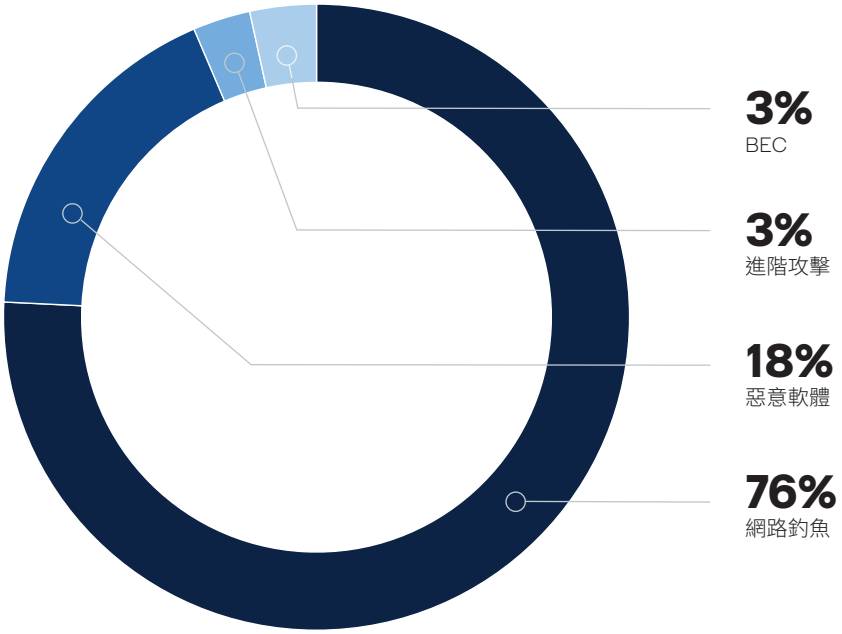
- 建築
- 零售業
- 房地產
- 專業服務，包括 IT
- 金融



2022 年 7 月到 11 月遭受攻擊次數最多的行業

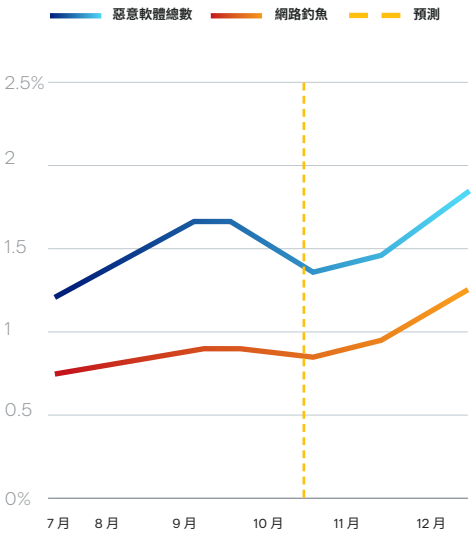
包括魚叉式網路釣魚和網路捕鯨之類特定形式在內的網路釣魚仍然是組織的頭號威脅。2022 年 7 月到 11 月，網路釣魚活動增加了 130%；現在佔所有電子郵件型攻擊的 76%（相較於 2022 年上半年的 58% 有所上升）。隨著這一上升，惡意軟體的電子郵件攻擊百分比相應地下降了。在過去的 4 個月，社交工程威脅還出現了上升，現在佔所有攻擊的 3%（與我們之前報告中的 2% 相比）。

包括魚叉式網路釣魚和網路捕鯨之類特定形式在內的網路釣魚仍然是組織的頭號威脅。2022 年 7 月到 11 月，網路釣魚活動增加了 130%；現在佔所有電子郵件型攻擊的 76% (相較於 2022 年上半年的 58% 有所上升)。隨著這一上升，惡意軟體的電子郵件攻擊百分比相應地下降了。在過去的四個月，社交工程威脅還出現了上升，現在佔所有攻擊的 3% (與我們之前報告中的 2% 相比)。



2022 年月份	已阻止的 URL
1 月	5,786,801
2 月	5,288,611
3 月	8,075,799
4 月	9,306,368
5 月	4,903,640
6 月	6,940,702
7 月	5,619,052
8 月	7,096,120
9 月	4,785,525
10 月	13,025,443
11 月	15,202,217

隨時間推移的網路釣魚和惡意活動比率 (不包含垃圾郵件)



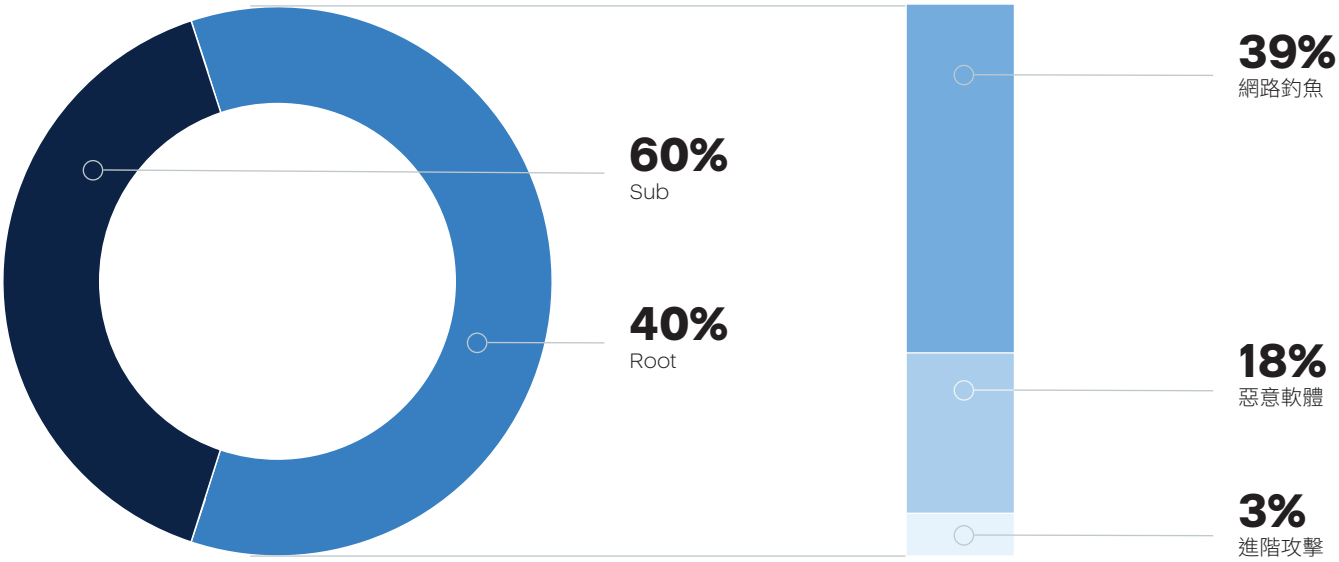
- 10 月發現了 229,000 個惡意事件
- 其中 128,000 個是網路釣魚

Acronis CPOC 在 2022 年第三季度攔截了 17,500,697 個網路釣魚和惡意 URL。比第二季度 (21,150,710) 減少了 17%，比第一季度 (19,151,211) 減少了 8%。

很不幸，很多含有惡意內容 (尤其是 URL) 的電子郵件仍然突破了基本的電子郵件篩選器並到達了使用者的端點。惡意附件通常也具有多層，例如包含下載最終承載之 LNK 檔案、受密碼保護的 ZIP 封存檔。這是為什麼擁有一個多層次防禦機制非常重要的另一個原因。

由於網路釣魚在攻擊總數中佔了很大一部分，它改變了一年來惡意攻擊率的趨勢。根據我們的分析，在考量季節性因素 (例如，即將到來的假期) 後，我們預計攻擊率在 12 月將進一步上升，達到超過所有流量 2% 的年度峰值。

為了避開安全性措施，攻擊者試圖將惡意承載隱藏在檔案中。多虧了遞迴拆解功能，我們在平台的防規避層發現了超過 235,000 個隱藏在子檔案和 URL 中的惡意事件。在該平台識別的攻擊中，這佔了六成。對隱藏攻擊的深入分析顯示，該技術主要用於隱藏網路釣魚威脅，在所有嘗試的攻擊中這佔 40%。



重大事件和網路釣魚趨勢

網路釣魚仍是網路罪犯最喜歡的滲透系統的工具之一。我們來看看 Acronis 和其他網路資安研究人員在 7 月至 11 月發現的一些重大事件。

攻擊者用稱作 GIFShell 的新攻擊技術，透過 Microsoft Teams 執行命令，使用 GIF 竊取資料來發起網路釣魚攻擊。Microsoft Teams 每月有超過 2.7 億活躍使用者，其眾多的弱點和瑕疵可以串連在一起用於命令執行、安全控制避開、網路釣魚攻擊和透過 GIF 竊取資料。GIFShell 允許攻擊者建立反轉 shell，透過 Teams 中的 Base64 編碼 GIF 提供惡意命令，並透過 Microsoft 自己的基礎架構擷取的 GIF 外洩輸出。GIFShell 要求在 GIF 內安裝執行收到的命令的可執行檔。所有收到的訊息都儲存在這些記錄中，並可由所有 Windows 使用者群組讀取，這意味著裝置上的任何惡意軟體都可以存取它們。

另一個針對 Microsoft 的網路釣魚活動實際上是冒充 Microsoft 團隊，試圖引誘收件人將他們的備忘錄文字新增到一個紀念 Her Majesty Queen Elizabeth II 的線上紀念板 (她於 9 月去世)。攻擊者竊取了 Microsoft 帳戶的詳細資料，並試圖讓受害者的多重要素驗證 (MFA) 程式碼接管他們的帳戶。網路釣魚頁面使用 EvilProxy 網路釣魚工具組建立。這是一個利用熱門新聞作為誘餌的典型範例，經常奏效。

還發現了另一個針對 Microsoft M365 電子郵件服務憑證的大型網路釣魚活動。其目標是美國、英國、紐西蘭和澳大利亞的金融科技、貸款、會計、保險和聯邦信用社組織。此活動之所以引人注目，是因為威脅執行者正在使用自訂基於 Proxy 的網路釣魚工具組來避開多重要素驗證。此工具組可以輕鬆地修改從公司登入頁面提取的合法登入頁面並新增他們自己的網路釣魚元素。威脅執行者正在轉變為使用 Evilginx2、Muraena 和 Modlishka 之類的工具來避開 MFA。使用這些反向代理，攻擊者可以處在受害者和電子郵件提供商的伺服器之間，因此它們被稱為 AitM (中間對手)。

其他熱門公司和服務也被濫用。例如，LinkedIn 功能 Smart Links 被濫用以避開安全篩選器。此功能允許客戶建立最多包含 15 個文件的登錄頁面，並透過可跟蹤的連結向其他人傳送這些頁面的存取權。不幸的是，這可以用作重新導向程式，讓攻擊者建立將收件人傳送到網路釣魚頁面的連結。最近的一個主題是模仿 Slovakian 郵政服務的套件傳送訊息。另一個網路釣魚執行者目前正在攻擊美國的政府承包商。該電子郵件承諾存取政府入口網站，允許對利潤豐厚的政府專案進行招標，但實際上電子郵件鏈接到一個 PDF，該 PDF 會重新導向到一個惡意網路釣魚網站。

一個新的 Instagram 網路釣魚活動試圖透過使用藍色徽章引誘使用者來欺騙這個熱門社交媒體平台的使用者。在此過

程中，使用者被要求洩漏包括密碼在內的個人資訊，當然，這些資訊隨後會直接傳送給攻擊者。該活動每日傳送 1,000 封電子郵件，活躍了幾週。攻擊者製造了一種緊迫感和機會有限的假像，他們警告使用者若忽略這條訊息，藍色徽章的提交表單將在 48 小時內被永久刪除。啟用 MFA 可幫助將風險降至最低和保護您的帳戶，但這並不是高招。

在一個新的兩步網路釣魚活動中，Dropbox 被用來投放承載。使用者首先被導向一個含按鈕或可點選文字的乾淨網站。按一下之後，他們會被引導到一個惡意網站，並被要求登入其帳戶。使用者不知不覺地落入攻擊者的騙局 — 鉤、線和憑證。兩步網路釣魚攻擊的獨特之處在於，它們通常透過已被同一技術入侵的電子郵件帳戶傳送，並可以透過向受害者的聯絡人傳送更多網路釣魚電子郵件來傳播。

我們不應忘記特定地區特有的本地網路釣魚活動。

9 月，美國以 COVID-19 為主題的網路釣魚訊息的數量翻倍。這些電子郵件通常冒充美國小型企業管理局 (SBA) 機構，濫用 Google Forms 來主控竊取企業所有者個人詳細資料的網路釣魚頁面。由於 SBA 之前運營著 COVID-19 財務恢復項目，網路釣魚電子郵件中使用的誘餌承諾透過 Paycheck Protection 計畫、振興基金和 COVID 經濟傷害災難貸款等專案提供流行財務支援。如果想要使用這些程式，只需按一下嵌入式按鈕就可以進入模仿 SBA 的合法表單的 Google Form，並請求 Google 帳戶憑證、SSN、EIN、州 ID 和駕照詳細資料以及銀行帳號等。

研究人員發現了一個新的針對美國和紐西蘭求職者的網路釣魚活動。這些惡意電子郵件向收件人提供了一份所謂的高薪工作，但實際上包含了惡意文件。在某些情況下，開啓文件會觸發攻擊，並導致下載託管在 Bitbucket 存放庫上的 Word 範本。在其他情況下，安裝 Cobalt Strike 指標用於遠端存取受害者裝置。Cobalt Strike 指標使威脅行為人能夠在受感染的裝置上遠端執行命令，允許他們竊取資料或透過網路橫向傳播。目前的網路釣魚活動有幾個階段，大多數步驟依賴於從主機的記憶體中執行混淆指令碼和濫用 Bitbucket 服務來避開偵測。

一個全新的網路釣魚活動正在匈牙利傳播 Warzone RAT。該活動包含一封精心製作的偽造政府電子郵件，引誘使用者執行附件的惡意軟體。收件人會收到一封冒充匈牙利政府入口網站的電子郵件，該網站用於在線上進行正式的業務運作，例如提交文件和訂購 ID。電子郵件通知收件人存取入口網站的新憑證在附加的 ZIP 檔中。一旦附件被開啓，它就會擷取 Warzone RAT 並執行它。Warzone 是一個在惡意軟體即服務 (MaaS) 模型下執行的流行木馬程式。它可以以每月 37 美元的訂購價購買。網路罪犯可以使用此木馬程式下載和上傳各種檔案、執行并刪除它們，向受感染電腦的 CMD（命令提示字元）傳送命令，透過任務管理器查看和刪除處理程序，並使用電腦的 IP 位址瀏覽網頁。Warzone 可以用來存取受害者的網路攝影機，並從瀏覽器和電子郵件用戶端竊取儲存的密碼。

另一個範例是最近大量散佈的 Lampion 惡意軟體，威脅行為人濫用 WeTransfer 作為其網路釣魚活動的一部分。WeTransfer 是一個合法的檔案共用服務，可免費使用。該服務在 190 個國家/地區擁有 8700 萬名月度活躍使用者。在新的活動中，Lampion 運營商從被入侵的公司帳戶傳送網路釣魚電子郵件，敦促使用者從 WeTransfer 下載「付款證明」文件。目標會收到一個包含 VBS (Virtual Basic 指令碼) 檔案的 ZIP 封存檔。受害者必須啟動檔案才能開始攻擊。此時，所包含的 DLL 承載被載入到記憶體中，允許 Lampion 在被入侵的系統上秘密執行。Lampion 從電腦中竊取資料，通過從 C2 擷取植入並在登入頁面上覆蓋自己的表單來鎖定銀行帳戶。當使用者輸入他們的憑證時，這些偽造的登入表單將被竊取並傳送至攻擊者。

簡而言之：

包括防網路釣魚技術的多層網路防禦方法非常重要。即使網路釣魚嘗試不會立即被解除，其他偵測工具可以阻止惡意軟體的執行。

3. 資料外洩一直居高不下

根據 IBM 的《2022 年資料外洩成本報告》，現在全球資料外洩的平均總成本為 435 萬美元，今年增加了 11 萬美元。最近的一項 Surfshark 調查發現，2022 年第三季度超過 1 億個帳戶被外洩。

根據 Identity Theft 2022 年第三季度《資料外洩分析》，網路攻擊佔資料外洩的 88%，這并不意外。IT 治理在 2022 年 7 月至 9 月期間確定了 285 起公開披露的安全事件，導致 232,266,148 條記錄被外洩。ENISA（歐盟網路資安機構）最新的報告顯示，超過 10 TB 的資料在每月勒索軟體攻擊中被竊取。KELA 的一份新報告顯示，初始存取代理人（IAB）正以 4,000,000 美元的累計銷售價格出售全球 576 個企業網路的存取權，這激勵了其他網路罪犯攻擊企業。

雖然數字可能會因來源的不同而略微不同，但 Acronis 可以確定資料外洩在 2022 年下半年增長，全年也是如此。越來越多的攻擊者利用所謂的 MFA 疲勞攻擊，這種攻擊在備受關注的外洩中效果很好。此類社交工程技術已在入侵大型和著名組織時被 Lapsus$ 和 Yanluowang 威脅行為人證實非常成功但資料漏洞不僅與勒索軟體有關。傳統的資料外洩仍非常流行，我們在 2022 年第三季度看到了大量的巨大外洩事件（以下方的使用者測量）：

- **Neopets (6900 萬)**
- **Shanghai COVID-19 應用程式 (4850 萬)**
- **Mangatoon (2300 萬)**
- **Swachh City 平台 (1640 萬)**

加密行業雖然已經衰落，但仍是最吸引網路罪犯的攻擊目標。加密貨幣橋 Nomad 在一次攻擊中損失了幾乎 2 億美元。Nomad 是 Ethereum、Moonbeam、Avalanche、Evmos 和 Milkomeda 之間的一個跨鏈接橋。Twitter 使用者 foobar 指出，在區塊鏈安全機構 Quantstamp 今年進行的稽核中，發現了據稱涉及網路搶劫的問題和其他數十個問題。然而，Nomad 認為這次攻擊不是由一個攻擊者執行的；此外，許多白帽駭客或安全研究人員可能已經將代幣轉移到自己的地址，以保護資金。如果這是真的，白帽駭客可能會返還 Nomad 為此提供錢包地址的資金。

最近的另一個加密案例是 QANplatform 駭客。加密貨幣橋表示，在攻擊者操縱其中一個智慧合約之後損失了預估 2 百萬美元的加密貨幣。

大型企業仍然處在攻擊之下。Medibank 是澳大利亞最大私人健康保險提供商之一，擁有大約 390 萬名客戶，披露在最近的勒索軟體攻擊之後客戶的個人資訊被未經授權地存取。經過調查，該公司報告稱，屬於其 ahm 健康保險子公司和國際學生的個人資料已被洩露，但目前尚不清楚總共有多少客戶受到影響。被洩漏的資料包括姓名、姓氏、地址、出生日期、醫療保險號碼、保單號碼、電話號碼和護照號碼。Medibank 強調，它沒有發現直接借貸詳細資料被存取的證據。該公司通知澳大利亞聯邦警署（AFP），承認有犯罪分子與他們聯絡，聲稱已獲得 200 GB 的資料。Medibank 估計，該事件造成的損失在 1600 萬到 2200 萬美元之間。

澳大利亞還發生了其他兩起重大事件。零售業巨頭 Woolworths 披露影響大約 220 萬名 MyDeal 客戶的資料外洩。Optus 是擁有超過 1050 萬名訂閱者的 Singtel 的子公司，澳大利亞第二大行動運營商，也披露一個安全漏洞。攻擊者聲稱已竊取 1100 萬名客戶的資料。被竊取資料的小範本發佈在被入侵的論壇上，贖金要求為 1 百萬美元。作為回應，Optus 與執行機構合作調查該事件。由於沒有支付贖金，攻擊者公佈了更大的被盜資料樣本，允許其他威脅行為人下載並濫用這些資料進行攻擊。最終，在受到執法單位越來越多的關注後，威脅行為人撤回了勒索要求。攻擊者還向個人資料已被洩漏的 1 萬多人道歉。

Uber 揭露在 9 月年遭受的安全性外洩事件。威脅行為人獲取了其網路的存取權並竊取了內部文件。據《紐約時報》報導，駭客入侵了一名員工的 Slack 帳戶，並用它通知公司內部人員，公司遭遇了資料外洩，並提供了一份據稱被駭客入侵的內部資料庫清單。該公司被迫將其內部通訊和工程系統離線，以減輕攻擊並調查入侵。據稱，攻擊者入侵了幾個內部系統，並向《紐約時報》和一些網路資安研究人員提供了電子郵件、雲端儲存和程式碼存放庫的影像。這名駭客自稱 18 歲，並補充說 Uber 的安全性很弱；在透過 Slack 傳送的訊息中，他還表示 Uber 駕駛員應獲得更高的工資。這不是公司第一次遭到安全外洩事件了。2017 年，發生在 2016 年的另一起資料外洩事件成為了頭條新聞。Uber 將此歸咎於據稱隸屬於 Lapsus$ 駭客集團的的威脅行為人。

電子行業巨頭 Samsung 證實，繼 7月份美國部分系統遭到入侵後，又發生了一起新的資料外洩事件。該電子巨頭在 8 月 4 日發現，威脅行為人已獲得其系統的存取權，並竊取了客戶個人資訊。

Shangri-La 酒店集團披露了一起資料外洩事件，攻擊者在 5 月至 7 月期間訪問了其亞洲八家酒店的一個包含客戶個人資訊的資料庫。此事件對位於香港、新加坡、清邁、台北和東京的酒店造成了影響。該公司已展開調查，以確定攻擊者竊取了哪些資料，並已通知當局和任何可能受到影響的客人。

American Airlines 披露了一起資料外洩事件，威脅行為人存取了數量不詳的員工電子郵件帳戶。被洩漏的資料包括姓名、出生日期、郵寄地址、電話號碼、電子郵件地址、駕照號碼、護照號碼和/或受影響人員提供的特定醫療資訊。該安全漏洞於 7 月 5 日被發現，隨後該航空公司迅速採取措施減輕事件的影響，並保護受影響的電子郵件帳戶。American Airlines 在領先網路資安鑑定機構的幫助下展開了調查。

英國金融科技公司 Revolut 遭受了一次網路攻擊，威脅行為人獲得了成百上千位客戶的個人資訊。該機構證實，全球 50,150 名客戶（包括歐洲經濟區的 20,687 名客戶）的資料被洩漏。被洩漏的資料包括姓名、地址、電子郵件、郵政地址、電話號碼、部分支付卡資料（根據公司提供的資訊，卡號已被遮蓋）、帳戶資料等。攻擊者沒有取用使用者的資金。

威脅行為人聲稱在入侵了開發商 Rockstar Games 之後洩漏了即將推出的視訊游戲 Grand Theft Auto 6 (GTA6) 的原始程式碼和游戲視訊。攻擊者似乎已入侵了 Rockstar Game 的 Slack 伺服器和 Confluence wiki。

Starbucks 新加坡分公司遭受了資料外洩事件，影響了其超過 219,000 名客戶。論壇上的一名資料賣方聲稱已經以 3,500 美元的價格出售了一份被盜的資料，並願意向感興趣的買家提供至少四份副本。

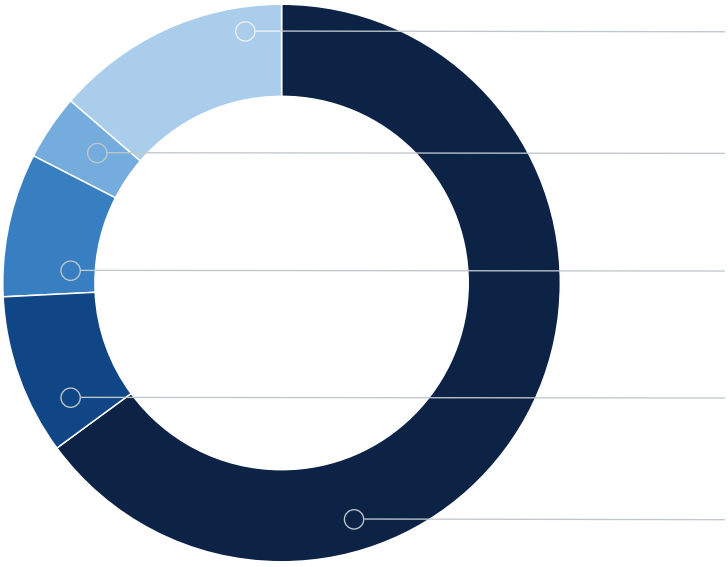
最後但並同樣重要的是：永遠不要忘記，資料外洩的後果不僅是遺失資料、金錢和時間，還有潛在的監管罰款。2022 的範例案例是 SHEIN：紐約司法辦公室已因 2018 年資料外洩事件對零售商罰款了 190 萬美元，在此期間駭客竊取了 642 萬位客戶的詳細資料。

一般惡意軟體威脅

2022 年第三季度，我們平均 11.7% 的客戶成功在其端點上阻止了至少一次惡意軟體攻擊。與 2022 年第 2 季度的 9.4% 相比略有增長。這些高百分比表明，儘管組織在意識訓練和修補方面做出了很大的努力，仍有十分之一的威脅到達了端點。由於這些數字來自端點上的偵測，這也意味著部署的任何代理或電子郵件安全性都沒有阻止這些威脅。

AV-TEST

2022 年 11 月前兩週偵測到的惡意軟體類型
(來源：av-test.org)



13.8% 其他

3.6% 後門

8.4% 下載程式

9.3% 蠕蟲病毒

64.9% 木馬程式

遭受惡意軟體攔截的客戶百分比

2022 年月份	遭受惡意軟體攔截的客戶百分比
1 月	10.7
2 月	8.7
3 月	8
4 月	9.2
5 月	9.7
6 月	9.4
7 月	8.7
8 月	8.4
9 月	17.9
10 月	9.6
11 月	10.4

自然環境中出現的新惡意軟體樣本數量自 2021 年起些微增加，但每年的增長變慢。有消息稱，這個比率仍然是每月幾乎 900 萬個新的樣本。這個比例與 Acronis CPOC 看到的新樣本數量相符。

2022 年 11 月惡意軟體樣本的平均存留時間為 1.7 天，之後威脅即會消失並再也不會出現。2022 年第 2 季度，該數字為 2.3 天，這表明惡意軟體的存留時間更短，因為攻擊者會使用自動化操作來建立全新的個人化惡意軟體，頻率超過了傳統簽章型偵測。在我們的客戶群中，觀察到的樣本中 74% 只出現過一次。

第 3 季度最常見的惡意軟體系列如下，明顯集中在 Bot 和資訊盜竊程式上：

- FormBook
- AgentTesla
- LokiBot
- Snake Keylogger
- Remcos
- RedLine Stealer
- Emotet
- Raccoon Stealer
- njRAT
- AsyncRAT

2022 年 10 月擁有最多惡意軟體感染數量的國家/地區是美國，佔 22.1%，其次是德國 8.8%，及巴西 7.8%。這些數字與第二季度的數字非常相似，除了美國和德國（有小幅增長，尤其是在金融木馬程式方面）。

在這些國家/地區，MSP 和大型企業是網路罪犯最感興趣的目標。

例如，英國國家衛生署（NHS）111 緊急服務受到了嚴重持續中斷的影響。這是因為，為 85% 的熱線服務提供軟體的英國 MSP 公司 Advanced 的系統遭到了網路攻擊。Advanced 為全球各個垂直行業的 22,000 多家客戶提供商業軟體，從醫療保健和教育到非營利組織。MSP 的客戶清單包括 NHS、英國就業和養老金部 (DWP) 和倫敦城市機場。英國國家犯罪局 (NCA) 和國家網路資安中心 (NCSC) 都參與了調查。

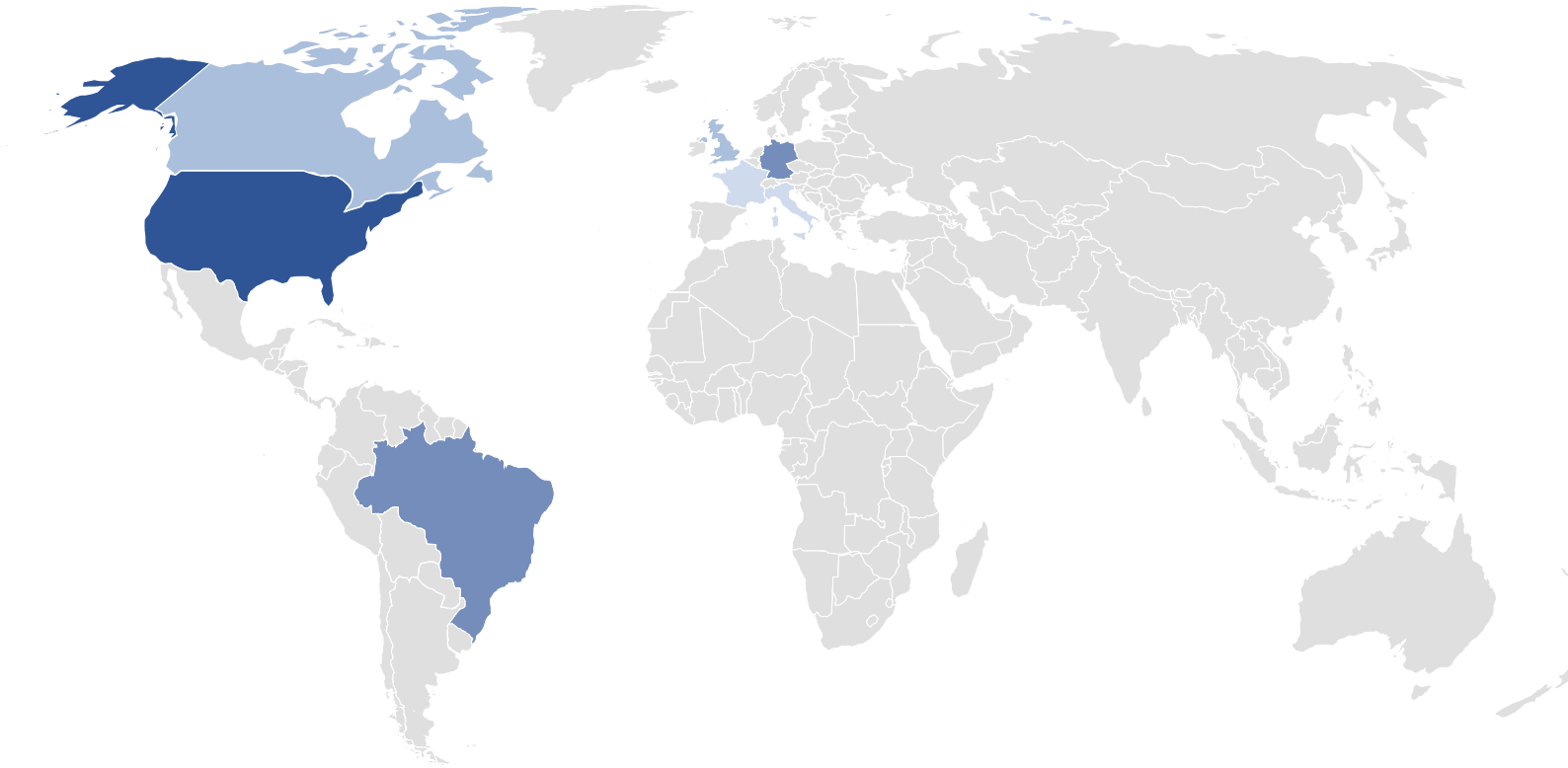
世界 15 大 IT 服務供應商之一的 SHI，擁有 5,000 多名員工，年銷售額在 2021 年達到 123 億美元，增長了 10%。SHI 成為了一場專業惡意軟體攻擊的受害者，儘管沒有證據表明他們的 15,000 家公司、企業、公共部門或學術客戶中的任何一家的資料被洩漏，也沒有證據表明其供應鏈中的任何第三方系統在攻擊中受到影響。事實上，系統被離線，恢復工作仍在進行中，這表明勒索軟體可能涉及其中。這家總部位於新澤西州的經銷商正在與美國聯邦調查局和網路資安和基礎設施安全局等美國機構合作，調查此次攻擊。

銀行業仍是主要的目標，威脅也在不斷演變。歐洲安全交易協會 (EAST)，一個由於銀行和 ATM 廠商組成的行業集團，表示已經發現了至少 501 起 ATM 盜竊事件，其中攻擊者使用新型 ATM MitM/中繼攻擊來攔截和竊取客戶的資金。

2022 年依國家/地區排列的每月佔全球偵測數量的百分比

國家/地區	1 月	2 月	3 月	4 月	5 月	6 月	7 月	8 月	9 月	10 月	11 月
美國	24.4	25.4	24.6	23.7	22.8	21.8	20.1	22.6	21.9	22.1	21.5
德國	13.2	12.7	11.2	11	9.4	8.9	8.2	8.5	9.1	8.8	8.9
巴西	4.7	3.6	3.9	4.5	7.2	7.8	9.6	9.5	7.7	7.3	6.9
義大利	4.8	4.3	5.1	5.7	6.6	6	6.2	4.5	5.9	5	5.1
加拿大	7.1	7.2	7.3	6.5	6.2	5.6	4.9	6	4.7	5.5	5.8
英國	5	5.4	5.4	5.3	5.3	4.9	4.8	5	6.7	5.2	4.9
新加坡	4.2	5	4.9	4.9	3.9	4.8	5.4	4.6	3.5	4.3	4.5
日本	2.6	3	3.1	3	2.8	3.1	3.2	3	3.1	3.7	3.4
法國	2.8	2.9	2.8	2.9	2.9	2.5	2.7	2.5	3.5	3	3.2
瑞士	3	2.8	2.9	2.6	2.4	4.1	2.3	2.7	2.9	2.7	3.2

2022 年 11 月惡意軟體偵測數量



百分比

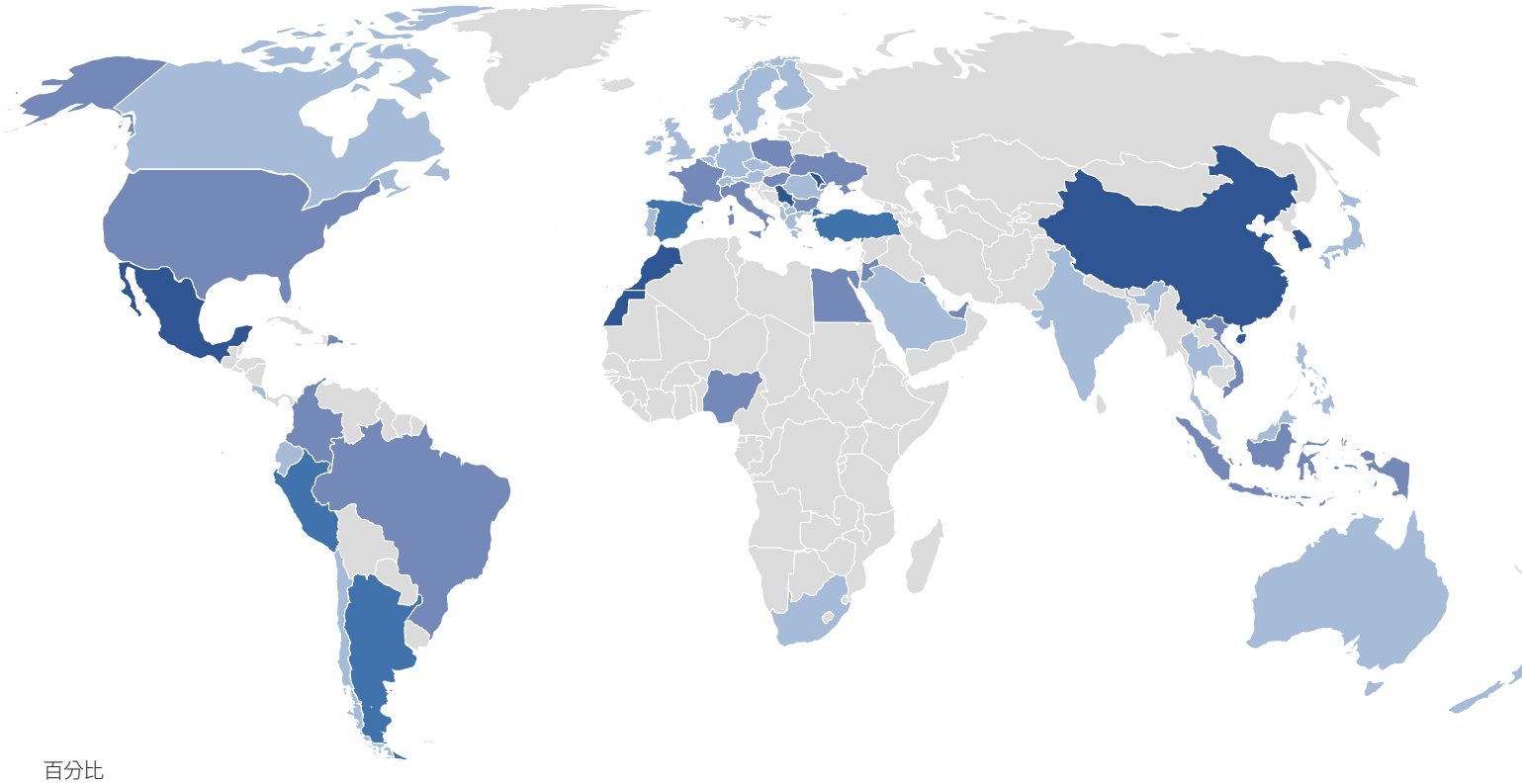
3% 22%

如果我們標準化每個國家/地區每個活躍用戶端的偵測數量，我們就會看到稍微不同的分佈。下表顯示了 2022 年 11 月每個國家/地區至少有 25 個活動中機器和至少 25 個惡意軟體偵測的標準化用戶端百分比。這個百分比意味著，在該國家/地區中所有主動受保護的工作負載中，此特定數量至少阻止了一次惡意軟體攻擊。

2022 年依國家/地區排列的每月佔全球偵測數量的百分比

排名	國家/地區	2022 年 11 月偵測到惡意軟體的用戶端數量百分比
1	埃及	32.3
2	中國	27.6
3	奈及利亞	26.3
4	摩洛哥	25.2
5	泰國	25
6	韓國	24.5
7	土耳其	23.9
8	越南	22.5
9	印度	22.5
10	新加坡	21.7
11	台灣	21.5
12	摩爾多瓦共和國	21.3
13	多明尼加共和國	21.2
14	塞爾維亞	19
15	保加利亞	18.6
16	匈牙利	18
17	秘魯	17.9
18	以色列	17.7
19	阿根廷	16.6
20	約旦王國	16.5
21	菲律賓	15.9
22	印尼	15.6
23	巴西	15
24	西班牙	14.6
25	阿拉伯聯合大公國	14.5
26	烏克蘭	14.2
27	厄瓜多爾	14
28	科威特	13.8
29	墨西哥	13.7
30	北馬其頓	13.3

2022 年 11 月標準化惡意軟體偵測數量



百分比

4% 32%

區域性標準化惡意軟體偵測數量

前 10 個國家/地區：依區域排列的標準化惡意軟體偵測數量

亞洲

排名	國家/地區	2022 年 11 月區域性標準化勒索軟體偵測數量百分比
1	中國	27.6
2	泰國	25
3	韓國	24.5
4	越南	22.5
5	印度	22.5
6	新加坡	21.7
7	台灣	21.5
8	菲律賓	15.9
9	印尼	15.6
10	日本	12.2

歐洲、中東及非洲地區

排名	國家/地區	2022 年 11 月區域性標準化勒索軟體偵測數量百分比
1	埃及	32.3
2	奈及利亞	26.3
3	摩洛哥	25.2
4	土耳其	23.9
5	摩爾多瓦共和國	21.3
6	塞爾維亞	19
7	保加利亞	18.6
8	匈牙利	18
9	以色列	17.7
10	約旦王國	16.5

美洲

排名	國家/地區	2022 年 11 月區域性標準化勒索軟體偵測數量百分比
1	多明尼加共和國	21.2
2	秘魯	17.9
3	阿根廷	16.6
4	巴西	15
5	厄瓜多爾	14
6	墨西哥	13.7
7	哥倫比亞	12
8	哥斯大黎加	11.5
9	美國	10.1
10	智利	8.8

勒索軟體威脅

我們在重要趨勢一節中已經提到，勒索軟體仍是企業的頭號網路威脅。在本節中，我們將重點關注 2022 年 11 月的活動，包括我們威脅不可知的 Acronis Active Protection 阻止的攻擊和勒索軟體運營商地下洩漏網站上發佈的資料。

以下是在 2022 年第 3 季度到第 4 季度觀察到和追蹤到的前 10 個活躍勒索軟體系列。

- LockBit
- Black Basta
- LV
- Ragnar Locker
- STOP
- BlackCat/ALPHV
- Vice Society
- Hive
- Everest
- Royal

請記住，部分組織嘗試用一個廣泛的途徑盡可能感染更多的使用者，而其他組織則重點關注高價值目標，他們僅試圖進行少量的感染，但追求高回報。因此，單獨的威脅偵測量並不能表明威脅真實的危險程度。此外，很多集團勒索將勒索軟體當作一項服務業務，攻擊者可能在類似的攻擊中使用多個威脅系列。

第 3 季度，我們發現了 576 個公開提到的勒索軟體入侵，比第 2 季度略有增加。當然，這僅僅是實際受害者的一部分，因為有些人會協商並最終向勒索軟體集團付款以免被公開提及。此外，一些集團轉為僅外洩資料；此類攻擊可能不會被稱作勒索軟體事件，但僅被稱為資料外洩。

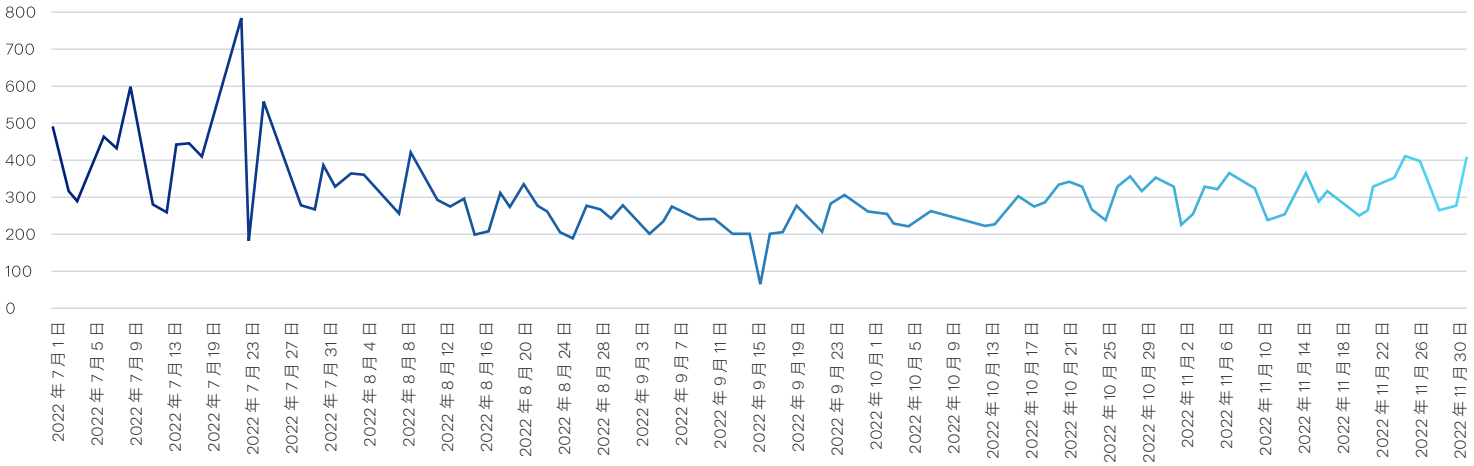
每日勒索軟體偵測數量

在夏季達到高點后，勒索軟體案件數量在第三季度有些許下降。從 7 月到 8 月，我們在全球範圍阻止的勒索軟體攻擊增加了 49%，接著在 9 月減少了 12.9%，在 10 月減少了 4.1%。

每個地區每季度的勒索軟體偵測數量的變化：

月份	歐洲、中東及非洲地區	美洲	亞洲	全球
7 月到 8 月	36.3	23.3	28.6	49
8 月到 9 月	-11.7	-5.9	-21.2	-12
9 月到 10 月	-23.2	5.8	-6	-4.1

全球每日勒索軟體偵測數量：



每日勒索軟體偵測數量：

月份	每日勒索軟體偵測數量
1 月	540
2 月	335
3 月	201
4 月	237
5 月	566
6 月	329
7 月	272
8 月	242
9 月	237
10 月	295
11 月	307

前 10 個國家/地區：依區域排列的勒索軟體偵測數量佔比

亞洲

國家/地區	2022 年第 3 季度區域性勒索軟體偵測數量百分比	2022 年第 2 季度區域性勒索軟體偵測數量百分比	2022 年第 1 季度區域性勒索軟體偵測數量百分比
日本	26.6	37.3	34.3
中國	9.8	12	13.1
菲律賓	2.4	5.8	4
台灣	3.9	5.1	4.9
印度	2.5	4.2	5.9
韓國	2.9	4.1	4.5
土耳其	2.6	4	5.1
新加坡	0.6	3	1.8
越南	1.4	2.6	1.4
泰國	1.5	2.1	2.7

歐洲、中東及非洲地區

國家/地區	2022 年第 3 季度區域性勒索軟體偵測數量百分比	2022 年第 2 季度區域性勒索軟體偵測數量百分比	2022 年第 1 季度區域性勒索軟體偵測數量百分比
德國	54.2	44	48.1
英國	11.1	8.7	7.7
法國	9.3	8.1	7.1
義大利	7.6	6.2	5.3
瑞士	6.5	4.7	5
西班牙	4.1	4.6	3.5
荷蘭	3.7	2.9	3
奧地利	3.3	2.6	2.8
捷克	2.5	1.8	2
烏克蘭	1.8	1.8	1.9

美洲

國家/地區	2022 年第 3 季度區域性勒索軟體偵測數量百分比	2022 年第 2 季度區域性勒索軟體偵測數量百分比	2022 年第 1 季度區域性勒索軟體偵測數量百分比
美國	60	62.7	65
加拿大	19.7	23.9	25.1
墨西哥	2.7	3.8	2.8
巴西	1.4	1.7	1.6
阿根廷	1.2	1.4	0.9
哥倫比亞	0.5	1.1	0.6
秘魯	0.4	0.9	0.5
智利	0.5	0.8	0.6
瓜地馬拉	0.1	0.6	0.4
厄瓜多爾	1.2	0.4	0.3

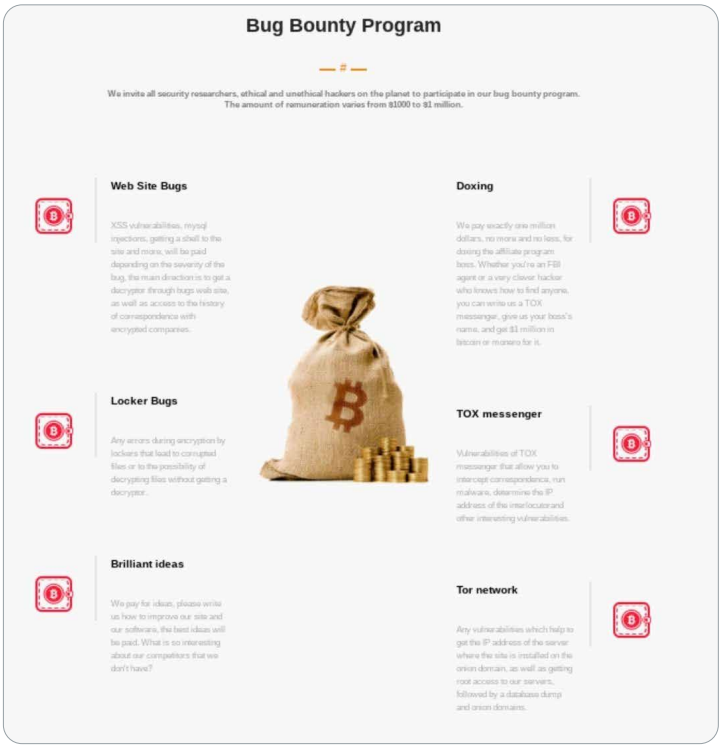
備受關注的勒索軟體集團

LockBit 3.0：帶有漏洞回報獎勵計畫的勒索軟體

2022 年 5 月 17 日，LockBit 發言人 LockBitSupp 宣佈，這個臭名昭著的勒索軟體的新版本將在不久的將來推出。

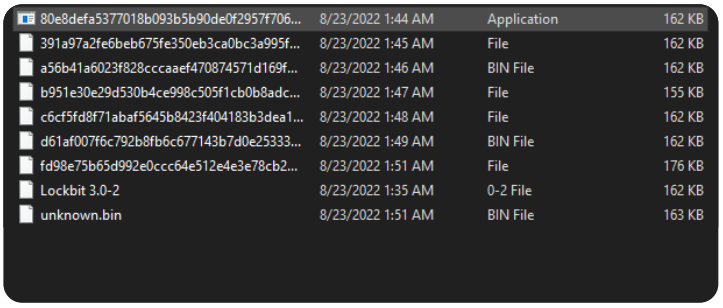
隨後 vx-underground 在 Twitter 上分享了 LockBit 3.0 網站的相片，產生了勒索軟體檔案和加密結果。3.0 版被威脅行為人命名為 LockBit Black，網路資安分析人員發現與 BlackMatter/DarkSide 勒索軟體的相似之處。

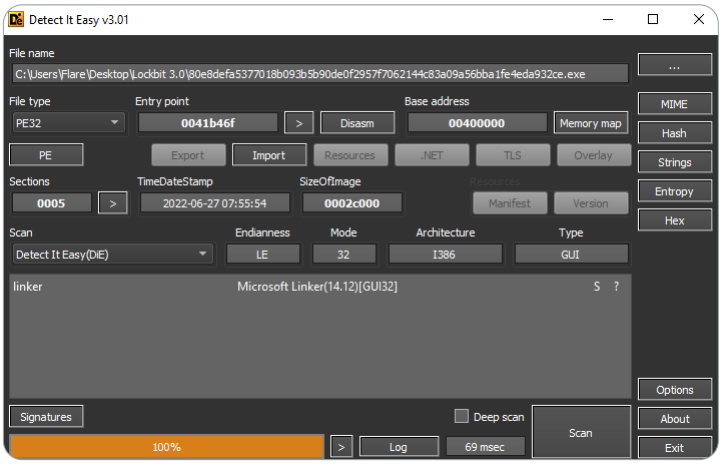
3.0 版本的 .text 一節中有編碼功能，只能使用密鑰進行解密，必須在命令提示字元中以 -pass 引數形式提供。它會加密檔案，變更它們的圖示、檔案名和擴展名，變更桌面背景，並在每個加密資料夾中放置贖金備註。值得注意的是，LockBit 3.0 引入了第一個勒索軟體漏洞回報獎勵計畫，向提交漏洞報告的使用者提供資金。已經有多人提交了此類申請，至少有一人獲得資金。



Lockbit 3.0 概觀

幾乎所有已發現的樣本都是 PE32 可執行檔，且大小相似。事實上都是使用相同的邏輯，且 Detect It Easy 無法定義它們是使用哪種語言編寫的。





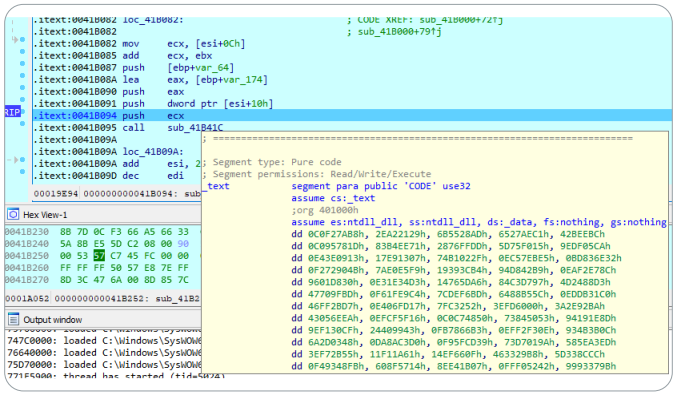
初看 IDA 反組譯工具，這些樣本沒有很多的功能、字串和匯入，但有一個具有執行權限的加密「.text」區段，佔檔案重量的一半以上。

```
.text:00401000 ; Segment type: Pure code
.text:00401000 ; Segment permissions: Read/Write/Execute
.text:00401000 _text           segment para public 'CODE' use32
.text:00401000                 assume cs:_text
.text:00401000                 ;org 401000h
.text:00401000                 assume es:nothing, ss:nothing, ds:_data, fs:nothing, gs:nothing
.text:00401000                 dd 0C0F27AB8h, 2EA22129h, 6B5528ADh, 6527AEC1h, 42BEEBCh
.text:00401000                 dd 0C095781Dh, 83B4EE71h, 2876FFDDh, 5D75F015h, 9EDF05CAh
.text:00401000                 dd 0E43E0913h, 17E91307h, 74B1022Fh, 0EC57EBE5h, 0BD836E32h
.text:00401000                 dd 0F2729048h, 7AE0E5F9h, 19393CB4h, 94D842B9h, 0EAF2E78Ch
.text:00401000                 dd 9601D830h, 0E31E34D3h, 14765DA6h, 84C3D797h, 4D2488D3h
.text:00401000                 dd 47709FBDh, 0F61FE9C4h, 7CDEF6BDh, 6488B55Ch, 0EDDB31C0h
.text:00401000                 dd 46FF2BD7h, 0E406FD17h, 7FC3252h, 3EFD6000h, 3A2E92BAh
.text:00401000                 dd 43056EEAh, 0EFCF5F16h, 0C0C74850h, 73845053h, 94191E8Dh
.text:00401000                 dd 9EF130CFh, 24409943h, 0FB7866B3h, 0EFF2F30Eh, 934B3B0Ch
.text:00401000                 dd 6A2D0348h, 0DA8AC3D0h, 0F95FCD39h, 73D7019Ah, 585EA3EDh
```

執行

LockBit 3.0 必須透過帶「-pass」引數的命令提示字元執行。這類似於 ALPHV 勒索軟體，後者使用存取權杖來開始執行。如果是 LockBit，此引數是一個密鑰，用於解密「.text」區段；不同樣本的密鑰也不同。例如，如果是 sha256:80e8defa5377018b093b5b90de0f29 57f7062144c83a09a56bba1fe4eda932ce 樣本，密鑰將為：db66023ab2abcb9957fb01ed50cdfa6a

執行開始時，LockBit 將叫用「sub41B000」功能，該功能接受提供的密鑰並將「.text」區段載入到「sub_41B41C」功能中。



LockBit 將載入的區段分為更小的區段，並用「sub_41B41C」功能解密功能將其解密。

```
.itext:0041B41C push    ebp
.itext:0041B41D mov     ebp, esp
.itext:0041B41F push    ebx
.itext:0041B420 push    esi
.itext:0041B421 push    edi
.itext:0041B422 xor     eax, eax
.itext:0041B424 mov     ebx, [ebp+arg_C]
.itext:0041B427 xor     ecx, ecx
.itext:0041B429 xor     edx, edx
.itext:0041B42B mov     esi, [ebp+arg_4]
.itext:0041B42E mov     edi, [ebp+arg_0]
.itext:0041B431 test    esi, esi
.itext:0041B433 jz      short loc_41B468
.itext:0041B435 push    ebp
.itext:0041B436 mov     ebp, [ebp+arg_8]
.itext:0041B439
.itext:0041B439 loc_41B439:                             ; CODE XREF: sub_41B41C+49↓j
.itext:0041B439 mov     dl, [ebp+ecx+var_s0]
.itext:0041B43D add     dl, bl
.itext:0041B43F mov     bl, [ebp+edx+var_s0]
.itext:0041B443 mov     dl, [ebp+ebx+var_s0]
.itext:0041B447 mov     dl, [ebp+edx+var_s0]
.itext:0041B44B inc     dl
.itext:0041B44D mov     al, [ebp+edx+var_s0]
.itext:0041B451 xor     [edi], al
.itext:0041B453 mov     dl, [ebp+ebx+var_s0]
.itext:0041B457 xchg    dl, [ebp+ecx+var_s0]
.itext:0041B45B mov     [ebp+ebx+var_s0], dl
.itext:0041B45F inc     cl
.itext:0041B461 inc     edi
.itext:0041B462 dec     esi
.itext:0041B463 test    esi, esi
.itext:0041B465 jnz     short loc_41B439
.itext:0041B467 pop     ebp
```

之後，它將從解密的區段中叫用功能：

```
.itext:0041B46F public start
.itext:0041B46F start:
.itext:0041B46F nop
.itext:0041B470 nop     dword ptr [eax+eax+00000000h]
.itext:0041B478 call    sub_41B000                      ; decrypt
.itext:0041B47D nop     dword ptr [eax+00h]
.itext:0041B481 call    loc_408254                      ; decrypted segment
.itext:0041B486 xchg    ax, ax
.itext:0041B488 call    sub_40B804
.itext:0041B48D nop     dword ptr [eax+eax+00h]
.itext:0041B492 call    loc_418F78                      ; decrypted segment
.itext:0041B497 nop     dword ptr [eax+eax+00000000h]
.itext:0041B49F push    0
.itext:0041B4A1 call    dword_4275C0
```

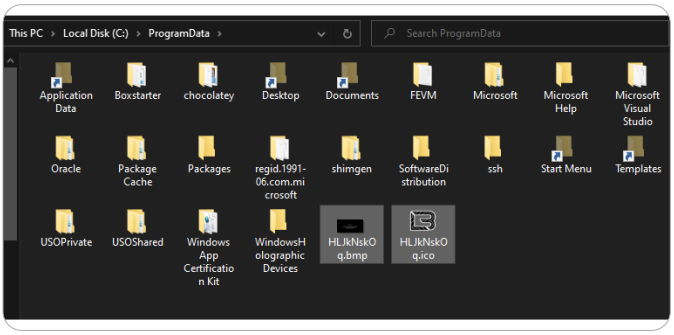
在解密的區段中，LockBit 會隱藏其 WinAPI 功能、叫用和字串。它將使用「sub_407C5C」功能解析實際的 API。此技術還被 BlackMatter 勒索軟體使用。

```
.text:004082B1 push    offset unk_407DA4
.text:004082B6 push    offset unk_427408
.text:004082BB call    sub_407C5C
.text:004082C0 push    edi
.text:004082C1 push    esi
.text:004082C2 push    offset unk_407E94
.text:004082C7 push    offset unk_4274F4
.text:004082CC call    sub_407C5C
.text:004082D1 push    edi
.text:004082D2 push    esi
.text:004082D3 push    offset unk_407F88
.text:004082D8 push    4275E4h
.text:004082DD call    sub_407C5C
.text:004082E2 push    edi
.text:004082E3 push    esi
.text:004082E4 push    40802Ch
.text:004082E9 push    427684h
.text:004082EE call    sub_407C5C
.text:004082F3 push    edi
.text:004082F4 push    esi
.text:004082F5 push    40804Ch
.text:004082FA push    427694h
.text:004082FF call    sub_407C5C
.text:00408304 push    edi
.text:00408305 push    esi
.text:00408306 push    40807Ch
.text:0040830B push    4276CCh
.text:00408310 call    sub_407C5C
.text:00408315 push    edi
.text:00408316 push    esi
.text:00408317 push    4080D4h
.text:0040831C push    427720h
.text:00408321 call    sub_407C5C
```

此功能會載入混淆處理的字串，並以「4506DFCA」作為密鑰執行 XOR 作業。結果將是 WinAPI 名稱。

```
.text:00407C62 mov     esi, [ebp+arg_4]
.text:00407C65 lodsd
.text:00407C66 xor     eax, 4506DFCAh
.text:00407C6B push    eax
.text:00407C6C call    sub_407AE0
.text:00407C71 test    eax, eax
.text:00407C73 jz      loc_407D9C
.text:00407C79 mov     edi, [ebp+arg_0]
.text:00407C7C add     edi, 4
```

執行期間，LockBit 會將兩個檔案放入 C:\ProgramData 資料夾。第一份檔案（「.bmp」）將用於變更桌面背景，第二份（「.ico」）將用於變更加密的檔案圖示。



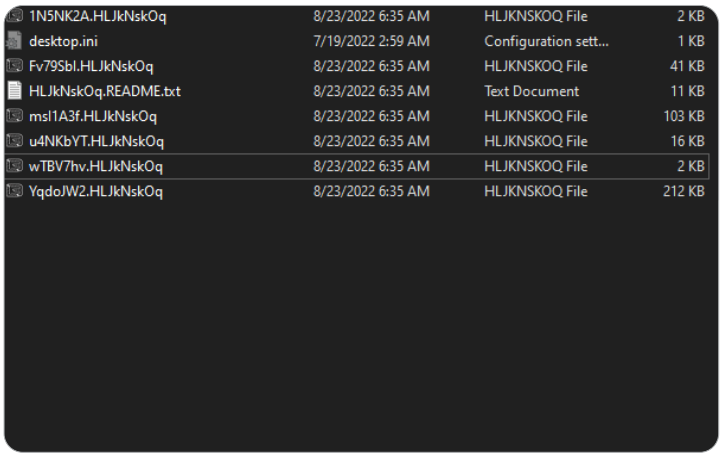
為了避開偵測，LockBit 在執行後會修改 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\WINEVT\Channels\ 路徑中的所有子機碼。這些機碼與 Windows 事件記錄有關，且 LockBit 會變更其中的兩個值：

ChannelAccess – O:BAG:SYD:(A;;0x1;;;SY)(A;;0x5;;;BA)(A;;0x1;;;LA)

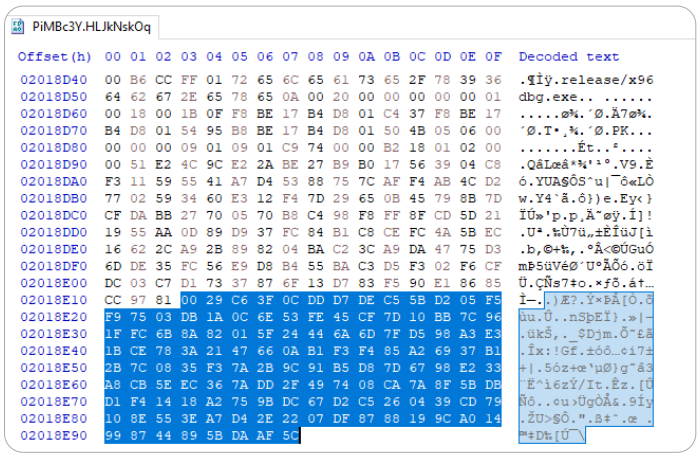
Enabled – 0

Name	Type	Data
(Default)	REG_SZ	(value not set)
ChannelAccess	REG_SZ	O:BAG:SYD:(A;;0x1;;;SY)(A;;0x5;;;BA)(A;;0x1;;;LA)
Enabled	REG_DWORD	0x00000000 (0)
Isolation	REG_DWORD	0x00000001 (1)
MaxSize	REG_DWORD	0x00040000 (262144)
MaxSizeUpper	REG_DWORD	0x00000000 (0)
OwningPublisher	REG_SZ	{11cd958a-c507-4ef3-b3f2-5fd9dfbd2c78}
Type	REG_DWORD	0x00000001 (1)

加密的檔案擁有「.HLJkNskOq」副檔名，一個全新隨機產生的名稱和一個變更的圖示。所有加密的檔案還在檔案結尾附加了 133 個位元組，用作解密 ID。

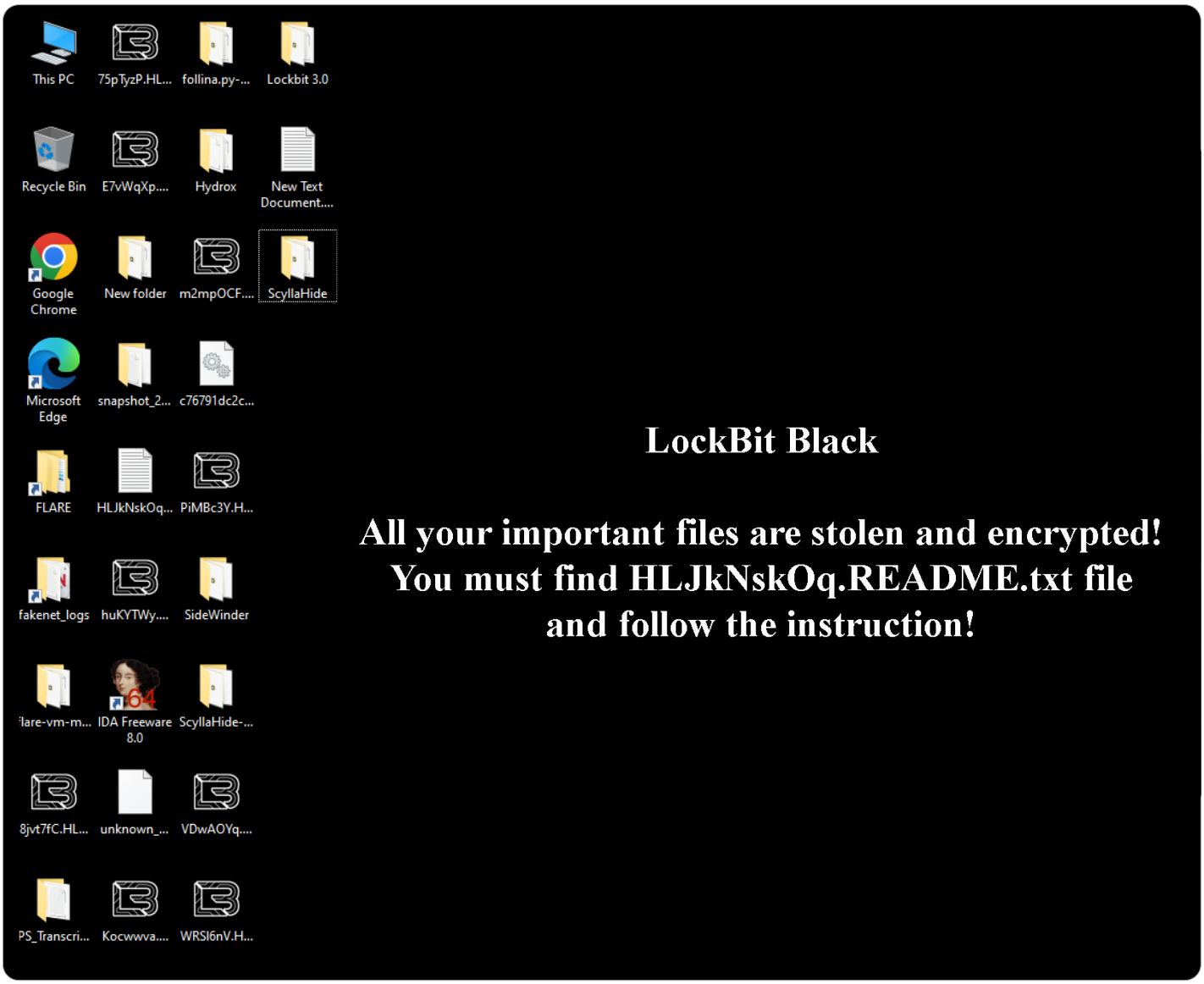


1N5NK2A.HLJkNskOq	8/23/2022 6:35 AM	HLJKNSKOQ File	2 KB
desktop.ini	7/19/2022 2:59 AM	Configuration sett...	1 KB
Fv79Sbl.HLJkNskOq	8/23/2022 6:35 AM	HLJKNSKOQ File	41 KB
HLJkNskOq.README.txt	8/23/2022 6:35 AM	Text Document	11 KB
msl1A3f.HLJkNskOq	8/23/2022 6:35 AM	HLJKNSKOQ File	103 KB
u4NKbYT.HLJkNskOq	8/23/2022 6:35 AM	HLJKNSKOQ File	16 KB
wTBV7hv.HLJkNskOq	8/23/2022 6:35 AM	HLJKNSKOQ File	2 KB
YqdoJW2.HLJkNskOq	8/23/2022 6:35 AM	HLJKNSKOQ File	212 KB



PiMBc3Y.HLJkNskOq

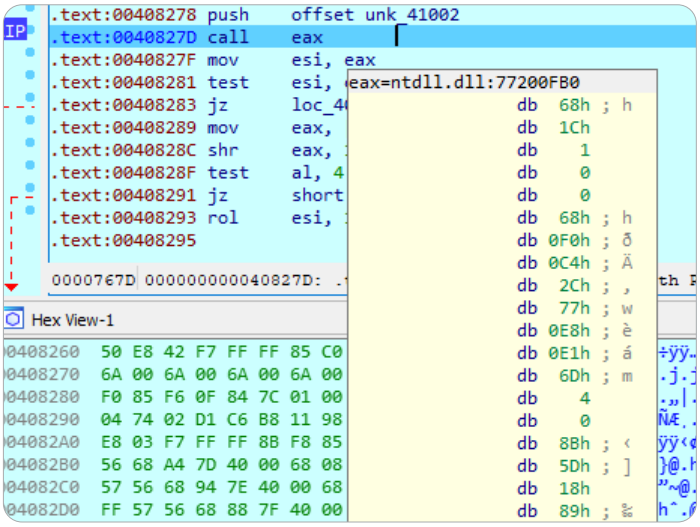
Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
02018D40	00	B6	CC	FF	01	72	65	6C	65	61	73	65	2F	78	39	36	.¶Ìÿ.release/x96
02018D50	64	62	67	2E	65	78	65	0A	00	20	00	00	00	00	00	01	dbg.exe.. .....
02018D60	00	18	00	1B	0F	F8	BE	17	B4	D8	01	C4	37	F8	BE	17	.....ø¾.´Ø.Ä7ø¾.
02018D70	B4	D8	01	54	95	B8	BE	17	B4	D8	01	50	4B	05	06	00	´Ø.T•¸¾.´Ø.PK...
02018D80	00	00	00	09	01	09	01	C9	74	00	00	B2	18	01	02	00	.....Ét..²....
02018D90	00	51	E2	4C	9C	E2	2A	BE	27	B9	B0	17	56	39	04	C8	.QâLœâ*¾'¹°.V9.È
02018DA0	F3	11	59	55	41	A7	D4	53	88	75	7C	AF	F4	AB	4C	D2	ó.YUA§ÔS^u|¯ô«LÒ
02018DB0	77	02	59	34	60	E3	12	F4	7D	29	65	0B	45	79	8B	7D	w.Y4`ã.ô})e.Ey‹}
02018DC0	CF	DA	BB	27	70	05	70	B8	C4	98	F8	FF	8F	CD	5D	21	ÏÚ»'p.p¸Ä˜øÿ.Í]!
02018DD0	19	55	AA	0D	89	D9	37	FC	84	B1	C8	CE	FC	4A	5B	EC	.Uª.‰Ù7ü„±ÈÎüJ[ì
02018DE0	16	62	2C	A9	2B	89	82	04	BA	C2	3C	A9	DA	47	75	D3	.b,©+‰‚.ºÂ<©ÚGuÓ
02018DF0	6D	DE	35	FC	56	E9	D8	B4	55	BA	C3	D5	F3	02	F6	CF	mÞ5üVéØ´UºÃÕó.öÏ
02018E00	DC	03	C7	D1	73	37	87	6F	13	D7	83	F5	90	E1	86	85	Ü.ÇÑs7‡o.×ƒõ.á†…
02018E10	CC	97	81	00	29	C6	3F	0C	DD	D7	DE	C5	5B	D2	05	F5	Ì—.).Æ?.Ý×ÞÅ[Ò.õ
02018E20	F9	75	03	DB	1A	0C	6E	53	FE	45	CF	7D	10	BB	7C	96	ùu.Û..nSþEÏ}.»|–
02018E30	1F	FC	6B	8A	82	01	5F	24	44	6A	6D	7F	D5	98	A3	E3	.ük Š‚._$Djm.Õ˜£ã
02018E40	1B	CE	78	3A	21	47	66	0A	B1	F3	F4	85	A2	69	37	B1	.Îx:!Gf.±óô…¢i7±
02018E50	2B	7C	08	35	F3	7A	2B	9C	91	B5	D8	7D	67	98	E2	33	+|.5óz+œ'µØ}g˜â3
02018E60	A8	CB	5E	EC	36	7A	DD	2F	49	74	08	CA	7A	8F	5B	DB	¨Ë^ì6zÝ/It.Êz.[Û
02018E70	D1	F4	14	18	A2	75	9B	DC	67	D2	C5	26	04	39	CD	79	Ñô..¢u›ÜgÒÅ&.9Íy
02018E80	10	8E	55	3E	A7	D4	2E	22	07	DF	87	88	19	9C	A0	14	.ŽU>§Ô."..ß‡ˆ.œ .
02018E90	99	87	44	89	5B	DA	AF	5C									™‡D‰[Ú¯\



一旦執行完成，LockBit 會自行刪除。

混淆處理

LockBit 使用編碼的程式碼片段，這些只能在偵錯期間存取。它使用功能叫用混淆處理，將其載入到一個一般用途登錄中。



該惡意軟體還有動態解析 WinAPI 功能名稱的功能。這樣做是為了在靜態分析中隱藏其真正的匯入表格。

贖金備註

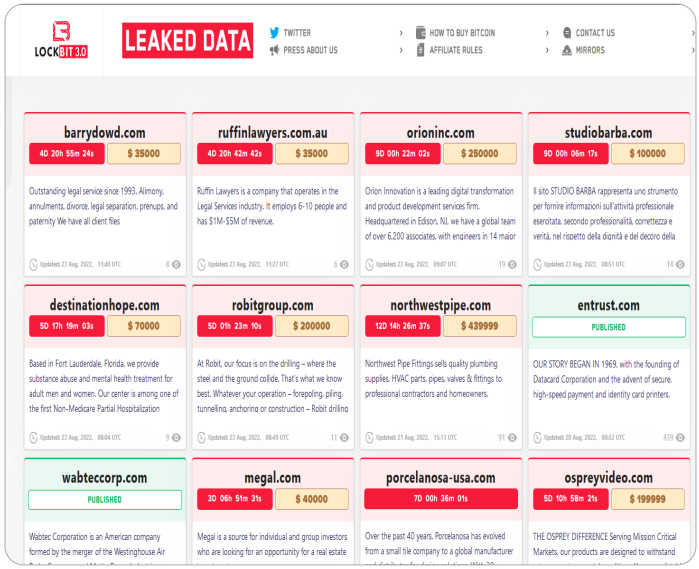
LockBit 3.0 在每個內容已加密的資料夾中放入了贖金備註「HLJkNskOq.README.txt」。此檔案非常長，包含受害者的 ID 以及資料洩漏網站和聊天的連結 (適用於 Tor 和普通瀏覽器)。此備註警告受害者，如果不支付贖金、報警或試圖以其他方式復原自己的資料，他們的檔案會發生什麼。

資料洩漏網站

在資料洩漏載入時，會列印以下文字：

> 有沒有人知道一個良好 torrent 跟蹤器，我可以在其中上傳窮盡的 entrust.com 常見檔案？請寫入 tox 3085B89A0C515D2FB124D645906F5D3DA5CB97CEBEA975959AE4F95302A04E1D709C3C4AE9B7

該資料洩漏頁面將包含受害者集合。每位受害者都有一個計時器和價格，他們必須向威脅執行人支付贖金才能解密他們的資料 (以及阻止其發佈)。該網站還列出了沒有支付贖金的受害者，並公佈了他們的資料。



結論

Lockbit 3.0 或 LockBit Black 現在使用金鑰開始執行，一個與 ALPHV 勒索軟體類似的策略，後者使用存取權杖。

初始樣本沒有很多的字串、匯入和功能；相反，一個「.text」區段佔用一般以上的檔案重量。該區段在執行時使用提供的金鑰解碼為可執行檔程式碼，包含使用 XOR 密碼動態解析 WinAPI 功能名稱的功能。

在加密過程中，LockBit 3.0 會對桌面背景和登錄進行變更。所有加密的檔案都有一個改變的名稱、圖示和副檔名。與其他勒索軟體相比，在最新的樣本中，LockBit 仍擁有最快的加密速度，這甚至會在同時接收新功能時增加。目前還沒有正式的 LockBit 3.0 通用解密程式，但 **RansomHunter 團隊提供了解密檔案**的說明。

聲望全新的勒索軟體攻擊了交通運輸和物流組織

2022 年 10 月 14 日，Microsoft Security Intelligence 發現了一個全新的勒索軟體，目標是烏克蘭和波蘭的交通運輸和物流組織。此威脅於 2022 年 10 月 11 日部署在受害者的電腦上，並用作威脅行為人將額外的惡意檔案部署到系統中的方式，兩次攻擊之間有一小時的延遲。勒索軟體名稱（「Prestige」）取自贖金備註中的電子郵件地址。

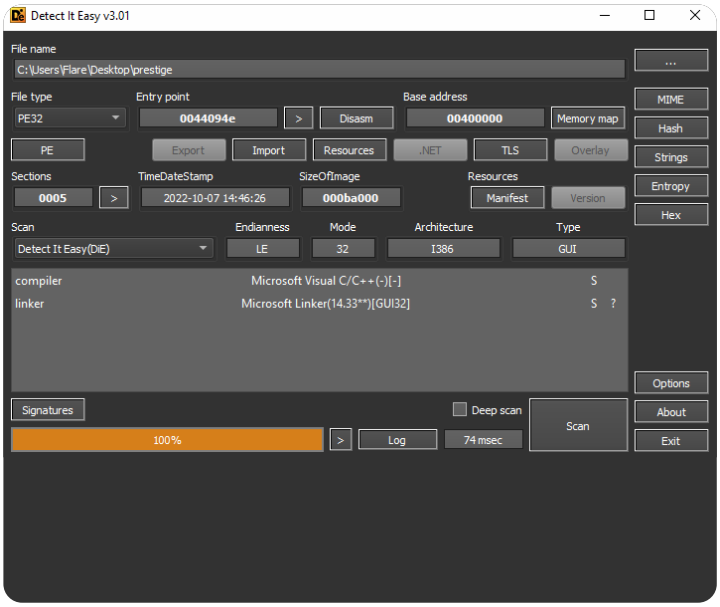
傳遞

Prestige 已使用三個不同的觀察方式部署在遠端系統上：

- 獲得存取權和將惡意檔案複製到 ADMIN$ 共用，使用 Impacket 工具建立將執行勒索軟體的排定工作
- 獲得存取權和將惡意檔案複製到 ADMIN$ 共用，使用 Impacket 工具載入和執行將輪流執行勒索軟體的 PowerShell 指令碼
- 將惡意檔案複製到 Active Directory 網域控制站並使用預設網域群組原則控制器部署到系統

概述

Prestige 樣本是一個以 C++ 程式化語言編寫的 PE32 檔案，擁有編譯時間戳記 07.10.2022（在觀察到的攻擊之前的四天）。此檔案未被封裝或混淆處理。



執行

執行開始時，Prestige 會檢查 CPU 資訊，其中「cpuid」指令和「IsProcessorFeaturePresent」功能帶有引數值 '10'，這 (如果找到) 表明系統支援 SSE2 指令集。

```
.text:0043FF9C    push    10              ; ProcessorFeature
.text:0043FF9E    call    ds:IsProcessorFeaturePresent
.text:0043FFA4    test    eax, eax
.text:0043FFA6    jz      loc_440158
.text:0043FFAC    and     [ebp+var_10], 0
.text:0043FFB0    xor     eax, eax
.text:0043FFB2    push    ebx
.text:0043FFB3    push    esi
.text:0043FFB4    push    edi
.text:0043FFB5    xor     ecx, ecx
.text:0043FFB7    lea     edi, [ebp+var_24]
.text:0043FFBA    push    ebx
.text:0043FFBB    cpuid
```

Prestige 在程式碼中使用了大量的 SSE2 指令，因此為了能正常的運行，它需要在處理器中使用此功能。

```
.text:0045045B    movapd  xmm5, xmm0
.text:0045045F    unpcklpd xmm0, xmm0
.text:00450463    psrlq   xmm5, 34h
.text:00450468    pextrw  ecx, xmm5, 0
.text:0045046D    movapd  xmm1, ds:xmmword_474110
.text:00450475    movapd  xmm3, ds:xmmword_474170
.text:0045047D    movapd  xmm4, ds:xmmword_474120
.text:00450485    movapd  xmm6, ds:xmmword_474130
.text:0045048D    andpd   xmm0, xmm1
.text:00450491    orpd    xmm0, xmm3
.text:00450495    addpd   xmm4, xmm0
.text:00450499    pextrw  eax, xmm4, 0
.text:0045049E    and     eax, 7F0h
.text:004504A3    movapd  xmm4, ds:xmmword_476470[eax]
.text:004504AB    movapd  xmm7, ds:xmmword_476880[eax]
.text:004504B3    andpd   xmm6, xmm0
.text:004504B7    subpd   xmm0, xmm6
.text:004504BB    mulpd   xmm6, xmm4
.text:004504BF    subpd   xmm6, xmm3
.text:004504C3    addsd   xmm7, xmm6
.text:004504C7    mulpd   xmm0, xmm4
.text:004504CB    movapd  xmm4, xmm0
.text:004504CF    addpd   xmm0, xmm6
```

Prestige 樣本中的 SSE2 指令使用範例

首先，Prestige 勒索軟體必須擁有管理權限。它使用附加到「MSSQLSERVER」的硬式編碼指令終止 MSSQL Windows 服務：

```
.text:00405A8F    mov     [esp+38h+var_28], 0C0000000h
.text:00405A97    push    23h
.text:00405A99    push    offset aCWindowsSystem ; "C:\\Windows\\System32\\net.exe stop {}"
.text:00405A9E    mov     [eax+4], ecx
.text:00405AA1    lea     ecx, [esp+40h+CommandLine]
.text:00405AA5    mov     dword ptr [eax], 1
.text:00405AAB    call    sub_407B19
.text:00405AB0    add     esp, 10h
.text:00405AB3    lea     ecx, [esp+30h+CommandLine] ; lpCommandLine
```

為了防止加密後系統還原，它使用 WBAdmin 刪除了備份目錄，使用 VSSAdmin 刪除所有的磁碟區陰影複製。

```
aCWindowsSystem_2:                      ; DATA XREF: sub_411979+3B2↑o
                text "UTF-16LE", 'C:\Windows\System32\wbadmin.exe delete catalog -qui'
                text "UTF-16LE", 'et',0
                align 10h
aCWindowsSystem_3:                      ; DATA XREF: sub_411979+3F5↑o
                text "UTF-16LE", 'C:\Windows\System32\vssadmin.exe delete shadows /al'
                text "UTF-16LE", 'l /quiet',0
```

這些命令使用位於 System32 資料夾中的工具，而 Prestige 樣本是一個 32 位元應用程式。它會使用 'Wow64DisableWow64FsRedirection' 功能停用檔案系統重新導向。執行命令之後，將叫用 'Wow64RevertWow64FsRedirection' 功能還原檔案系統重新導向。

```
.text:00431947                  call    edi ; CryptAcquireContextA
.text:00431949                  test    eax, eax
.text:0043194B                  jnz     short loc_43197A
.text:0043194D                  push    ebx
.text:0043194E                  call    ds:GetLastError
.text:00431954                  push    8               ; dwFlags
.text:00431956                  push    1               ; dwProvType
.text:00431958                  push    0               ; szProvider
.text:0043195A                  push    offset szContainer ; "Crypto++ RNG"
.text:0043195F                  push    esi             ; phProv
.text:00431960                  mov     ebx, eax
.text:00431962                  call    edi ; CryptAcquireContextA
.text:00431964                  test    eax, eax
.text:00431966                  jnz     short loc_431979
.text:00431968                  push    28h             ; dwFlags
.text:0043196A                  push    1               ; dwProvType
.text:0043196C                  push    eax             ; szProvider
.text:0043196D                  push    offset szContainer ; "Crypto++ RNG"
.text:00431972                  push    esi             ; phProv
.text:00431973                  call    edi ; CryptAcquireContextA
.text:00431975                  test    eax, eax
.text:00431977                  jz      short loc_43198C
```

贖金備註在程式碼中硬式編碼，將以 README 檔案 (沒有副檔名) 放入 C/Users/Public 資料夾。

```
aPrestigeRanuso:                        ; DATA XREF: .rdata:off_49EF00↑o
                text "UTF-16LE", 'Prestige.ranusomeware@Proton.me',0
aYouPersonalFil:                        ; DATA XREF: sub_40226F+8E↑o
                text "UTF-16LE", 'YOU PERSONAL FILES HAVE BEEN ENCRYPTED.',0Dh,0Ah
                text "UTF-16LE", 0Dh,0Ah
                text "UTF-16LE", 'To decrypt all the data, you will need to purchase '
                text "UTF-16LE", 'our decryption software.',0Dh,0Ah
                text "UTF-16LE", 'Contact us {}. In the letter, type your ID = {:X}.',0Dh
                text "UTF-16LE", 0Ah
                text "UTF-16LE", 0Dh,0Ah
                text "UTF-16LE", '* ATTENTION *',0Dh,0Ah
                text "UTF-16LE", '- Do not try to decrypt your data using third party'
                text "UTF-16LE", ' software, it may cause permanent data loss.',0Dh,0Ah
                text "UTF-16LE", '- Do not modify or rename encrypted files. You will'
                text "UTF-16LE", ' lose them.',0Dh,0Ah,0
                align 10h
```

一旦贖金備註被刪除，會進行兩次登錄變更。第一個是已加密檔案之新檔案副檔名 ('.enc') 的註冊，第二個是在使用者開啓任何加密的檔案之後用於在記事本中啟動贖金備註。

```
aCWindowsSystem_0:                      ; DATA XREF: sub_4112A8+14↑o
                text "UTF-16LE", 'C:\Windows\System32\reg.exe add HKCR\.enc /ve /t RE'
                text "UTF-16LE", 'G_SZ /d enc /f',0
                align 10h
aCWindowsSystem_1:                      ; DATA XREF: sub_4112A8+34↑o
                text "UTF-16LE", 'C:\Windows\System32\reg.exe add HKCR\enc\shell\open'
                text "UTF-16LE", '\command /ve /t REG_SZ /d "C:\Windows\Notepad.exe C'
```

檔案加密

加密過程開始之前，Prestige 會載入必須加密的副檔名清單：

.1cd, .7z, .abk, .accdb, .accdc, .accde, .accdr, .alz, .apk, .apng, .arc, .asd, .asf, .asm, .asx, .avhd, .avi, .avif, .bac, .backup, .bak, .bak2, .bak3, .6h, .bkp, .bkup, .bkz, .bmp, .btr, .6z, .6z2, .bzip, .bzip2, .c, .cab, .cer, .cf, .cfu, .cpp, .crt, .css, .db, .db-wal, .db3, .dbf, .der, .dmg, .dmp, .doc, .docm, .docx, .dot, .dotm, .dotx, .dpx, .dsk, .dt, .dump, .dz, .ecf, .edb, .epf, .exb, .ged, .g1f, .gpg, .gzi, .gzip, .hdd, .img, .1so, .jar, .Java, .jpeg, .jpg, .js, .json, .kdb, .key, .1z, .1z4, .1zh, .1zma, .mdmr, .mkv, .mov, .mp3, .mp4, .mpeg, .myd, .nude, .nvram, .oab, .odf, .ods, .old, .ott, .ovf, .p12, .pac, .pdf, .pem, .pfl, .pfx, .php, .pkg, .png, .pot, .potm, .potx, .pps, .ppsm, .ppsx, .ppt, .pptm, .pptx, .prf, .pvm, .py, .qcow, .qcow2, .r0, .rar, .raw, .rz, .s7z, .sdb, .sdc, .sdd, .sdf, .sfx, .skey, .sldm, .s1dx, .sql, .sqlite, .svd, .svg, .tar, .taz, .tbz, .tbz2, .tg, .tib, .tiff, .trn, .txt, .txz, .tz, .vb, .vbox, .vbox-old, .vbox-prev, .vdi, .vdx, .vhd, .vhdx, .vmc, .vmdk, .vmem, .vmsd, .vmsn, .vmss, .vmx, .vmxf, .vsd, .vsdx, .vss, .vst, .vsx, .vtx, .wav, .wbk, .webp, .wmdb, .wmv, .xar, .xlm, .xls, .xlsb, .xlsm, .xlsx, .xlt, .xltm, .xltx, .x1w, .xz, .z, .zbf, .zip, .zipx, .z1, .zpi, .zz

Prestige 將使用 Crypto++ 加密程式庫來透過 AES 演算法執行檔案加密。RSA 公開金鑰是硬式編碼的，每個樣本都不同。

```
.rdata:0049FDC8 aBeginPublicKey db '-----BEGIN PUBLIC KEY-----',0Ah
.rdata:0049FDC8                                 ; DATA XREF: sub_40221B+5To
.rdata:0049FDC8                 db 'MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA4mpkHWE1p0nefE0PL/Qk',0Ah
.rdata:0049FDC8                 db 'gT7bjLTeJ9bpH6v41L1YGI688cwfEnjmIaDa0zwvHfbT8dn4o+Wh2iSpUZk0BYIi',0Ah
.rdata:0049FDC8                 db 'Lw6u5+9nSd2UzD4sB+MY9dv6oVTHInxqp4VNLHR2nMjgIS4rFHYzNJ7Tsj/j3YJZ',0Ah
.rdata:0049FDC8                 db 'dVPuPVCqbpZg5boXoSFbgLNIn6Mnr+vKc5tGh+pkGty0otyFd/ghM0b/xitowcvx',0Ah
.rdata:0049FDC8                 db 'eqZezPO0YXmkjjeTi0jFa7E9IIP3Z/DMOR9r/oJR0NyEIs9HNKdFGTAjJKDAKWxu',0Ah
.rdata:0049FDC8                 db '1nEPXiZoPPHgS7fxqg40+ciCjj2i7eUwqVkop5Pvwjqtq Q0TkIt8EqjvkmDtMrp8',0Ah
.rdata:0049FDC8                 db 'ZQIDAQAB',0Ah
.rdata:0049FDC8                 db '-----END PUBLIC KEY-----',0Ah,0
```

‘CryptAcquireContextA’ 功能則用於獲取 Crypto++ RNG (RandomNumberGenerator) 金鑰容器的控點。

```
.text:00431947                  call    edi ; CryptAcquireContextA
.text:00431949                  test    eax, eax
.text:0043194B                  jnz     short loc_43197A
.text:0043194D                  push    ebx
.text:0043194E                  call    ds:GetLastError
.text:00431954                  push    8               ; dwFlags
.text:00431956                  push    1               ; dwProvType
.text:00431958                  push    0               ; szProvider
.text:0043195A                  push    offset szContainer ; "Crypto++ RNG"
.text:0043195F                  push    esi             ; phProv
.text:00431960                  mov     ebx, eax
.text:00431962                  call    edi ; CryptAcquireContextA
.text:00431964                  test    eax, eax
.text:00431966                  jnz     short loc_431979
.text:00431968                  push    28h             ; dwFlags
.text:0043196A                  push    1               ; dwProvType
.text:0043196C                  push    eax             ; szProvider
.text:0043196D                  push    offset szContainer ; "Crypto++ RNG"
.text:00431972                  push    esi             ; phProv
.text:00431973                  call    edi ; CryptAcquireContextA
.text:00431975                  test    eax, eax
.text:00431977                  jz      short loc_43198C
```

若要對 AES 執行加密，Prestige 會檢查 AES-NI (AES New Instructions) 和 SSE2 指令是否受 CPU 支援。

```
cmp     byte_4AFD92, 0
push    esi
jz      short loc_432405
mov     ecx, [esp+8+arg_0]
push    offset aAesni   ; "AESNI"
call    sub_405C0D
mov     eax, [esp+8+arg_0]
pop     esi
pop     ecx
retn    4
```

```
cmp     byte_4AFD8D, 0
jz      short loc_43242E
mov     ecx, [esp+8+arg_0]
push    offset aSse2    ; "SSE2"
call    sub_405C0D
mov     eax, [esp+8+arg_0]
pop     esi
pop     ecx
retn    4
```

如果 CPU 支援這些指令，則加密程序會開始。‘aesenc’ 指令將執行一輪加密，‘aesenclast’ 將執行最後一輪加密。

```
sub     [esp+8+arg_4], 1
lea     edi, [edi+10h]
movups  xmm1, xmmword ptr [edi-10
movups  xmm0, xmmword ptr [ecx]
aesenc  xmm0, xmm1
movups  xmmword ptr [ecx], xmm0
movups  xmm0, xmmword ptr [edx]
aesenc  xmm0, xmm1
movups  xmmword ptr [edx], xmm0
movups  xmm0, xmmword ptr [esi]
aesenc  xmm0, xmm1
movups  xmmword ptr [esi], xmm0
movups  xmm0, xmmword ptr [eax]
aesenc  xmm0, xmm1
movups  xmmword ptr [eax], xmm0
jnz     short loc_43CF50
mov     edi, [esp+8+arg_14]
```

```
mov     eax, [esp+8+arg_10]
add     edi, edi
movups  xmm0, xmmword ptr [ecx]
movups  xmm1, xmmword ptr [eax+ec
mov     eax, [esp+8+arg_C]
aesenclast xmm0, xmm1
movups  xmmword ptr [ecx], xmm0
movups  xmm0, xmmword ptr [edx]
aesenclast xmm0, xmm1
movups  xmmword ptr [edx], xmm0
movups  xmm0, xmmword ptr [esi]
aesenclast xmm0, xmm1
movups  xmmword ptr [esi], xmm0
movups  xmm0, xmmword ptr [eax]
aesenclast xmm0, xmm1
pop     edi
movups  xmmword ptr [eax], xmm0
```

‘aeskeygenassist’ 用於協助金鑰的產生，而 ‘aesimc’ 則用於執行反轉混合欄轉型。

```
call    sub_441A20
movaps  xmm1, [esp+3Ch+var_10]
mov     edx, edi
shr     edx, 2
add     esp, 0Ch
aeskeygenassist xmm0, xmm1, 0
pextrd  ecx, xmm0, 3
xor     ecx, [esi]
lea     eax, [edx+7]
mov     [esp+30h+var_24], offset unk_46FCF
shl     eax, 4
xor     ecx, 1
add     eax, esi
mov     [esi+edx*4], ecx
mov     [esp+30h+var_20], eax
```

```
aesimc  xmm0, xmmword ptr [edx+ec
aesimc  xmm1, xmmword ptr [edx+ea
movups  xmmword ptr [edx+eax*4],
add     eax, 4
movups  xmmword ptr [edx+ecx*4],
sub     ecx, 4
cmp     eax, ecx
jb      short loc_43D0A0
```

加密檔案之後，Prestige 會將 ‘.enc’ 附加到副檔名。還會將 ‘enc’ 寫入所有已加密檔案的結尾處。

```
00000B80  1F EB AF BE 50 2A E0 64 3C 8A 89 D7 0D B2 A6 DE   ë¯¾P*àd<ŠŠ×.²¦Þ
00000B90  65 36 F4 77 65 7A 60 AE 13 7A 55 2A 44 45 A0 BA   e6ôwez`®zU*DE º
00000BA0  E3 F6 06 44 1F 51 9D 96 95 DC 6A D0 00 B0 30 10   ãöD Q ÜjÐ °0
00000BB0  F2 61 76 85 3E 40 80 93 24 35 72 F8 DF DC F3 42   òav>@$5røßÜóB
00000BC0  45 81 06 07 04 75 E9 45 29 3B F3 C3 15 56 08 F5   E uéE);óÃ V õ
00000BD0  DC 63 AC FC E0 FC 90 66 AF 8B 8F C8 63 21 2A 7A   Üc¬üàü f¯ Èc!*z
00000BE0  EE 08 1B 56 15 E3 26 8C 08 15 06 34 3D 22 13 C5   î V ã&  4="Å
00000BF0  3C 67 31 A8 26 A7 72 85 21 0D BF 5F 29 82 68 17   <g1¨&§r!¿_)h
00000C00  C0 51 29 DE BE E9 22 3A 98 C9 17 AE 3E 8A A0 4C   ÀQ)Þ¾é":ÉŠ>L
00000C10  50 3D 99 04 53 E7 8D 9E 59 F0 31 B7 86 EA B6 7C   P=Sç YÐ1·êÊ¶|
00000C20  B9 05 49 14 D3 89 65 6E 63                        ¹ IÓenc
```

贖金備註

‘C/Users/Public’ 資料夾中的贖金備註 ‘README’ 會被刪除，並在每次開啓任何加密的檔案時於記事本中啟動。此備註包含唯一的受害者 ID 和電子郵件地址，您可以透過該地址來聯絡威脅行為人。

README - Notepad

File Edit Format View Help

```
YOU PERSONAL FILES HAVE BEEN ENCRYPTED.

To decrypt all the data, you will need to purchase our decryption software.
Contact us Prestige.ranusomeware@Proton.me. In the letter, type your ID = 289B23AC.

* ATTENTION *
- Do not try to decrypt your data using third party software, it may cause permanent data
- Do not modify or rename encrypted files. You will lose them.
```

結論

這個新發現的勒索軟體名為 Prestige，針對交通運輸和物流組織。它可能與現在的俄烏衝突有關，目的是破壞行動。此勒索軟體可以至少三種方式傳遞給受害者，第一次攻擊會延遲一小時發生。事實上，所有針對烏克蘭的攻擊都有這些相似之處，都使用了相同的安全性弱點。此樣本相對原始，不安全但仍危險。

上面分析的所有已發現樣本已成功偵測到並由 Acronis Cyber Protect 阻止，強調了企業使用現代化網路資安防護解決方案的重要性。

惡意網站

2022 年第三季度，平均 7.7% 的端點嘗試了存取惡意 URL，較第二季度的 8.3% 稍微下降。

2022 年 11 月端點上惡意 URL 阻止率最高的是美國，佔 20.5%。其次是德國的 9.0% 及義大利的 8.6%。

惡意 URL 在電子郵件中非常常見，但我們也發現它們在其他通訊媒介（如 Slack 或 Teams 聊天）中的使用次數有所增加。攻擊者正在嘗試進一步個人化連結，企圖讓它們更難以被所有使用者阻止，即使成功偵測到單一執行個體亦如此。來自網路釣魚電子郵件的惡意連結通常包含目標的電子郵件地址作為引數。這允許攻擊者驗證按下連結之人，還允許網路釣魚網站動態地適應目標使用者。例如，一些網路釣魚工具組將使用電子郵件地址中的網域，並將該主頁作為背景載入到網路釣魚網站，提供另一個注意力分散標識。

月份	點擊了惡意 URL 之使用者的百分比
1 月	8.5
2 月	8.1
3 月	9
4 月	8
5 月	8.1
6 月	8.8
7 月	8.1
8 月	8.5
9 月	6.6
10 月	8.5
11 月	8.7

2022 年 11 月被阻止 URL 數量最多的前 10 個國家/地區

排名	國家/地區	2022 年 11 月被阻止的 URL 數量的百分比
1	美國	20.5
2	德國	9
3	義大利	8.6
4	日本	5.4
5	巴西	5.4
6	英國	5.2
7	哥倫比亞	4.3
8	法國	3.4
9	加拿大	3.3
10	新加坡	2.8

與惡意軟體偵測統計資料類似，我們根據每個國家/地區中至少有 25 個被阻止 URL 的活動機器的數量對這些數字進行標準化處理。這些區域性標準化細分狀況如下所示。

前 10 個國家/地區：依區域排列的標準化已阻止的 URL

亞洲

排名	國家/地區	2022 年 11 月被阻止的 URL 數量的區域性標準化百分比
1	菲律賓	19
2	印度	16.8
3	日本	16.2
4	馬來西亞	15.4
5	印尼	14.8
6	中國	14.4
7	台灣	13.8
8	韓國	12.4
9	香港	12.1
10	新加坡	11.4

歐洲、中東及非洲地區

排名	國家/地區	2022 年 11 月被阻止的 URL 數量的區域性標準化百分比
1	科威特	33.6
2	沙烏地阿拉伯	18.7
3	斯洛伐克	16.7
4	保加利亞	16.3
5	義大利	14.1
6	希臘	13.9
7	北馬其頓	13.7
8	約旦王國	13.3
9	葡萄牙	12.9
10	阿拉伯聯合大公國	12.4

美洲

排名	國家/地區	2022 年 11 月被阻止的 URL 數量的區域性標準化百分比
1	海地	39.9
2	巴拿馬	36.4
3	秘魯	25.6
4	哥倫比亞	23.6
5	哥斯大黎加	19
6	多明尼加共和國	14.4
7	智利	11.2
8	巴西	9.9
9	美國	8.1
10	墨西哥	7.9

Windows OS 與軟體中的弱點

我們 Acronis 在不斷地發現和警告企業和家庭使用者，新的零時差弱點以及舊的未修補弱點，是系統入侵網路攻擊的主要媒介。雖然軟體廠商嘗試跟進並定期發佈新的修補程式，但這遠遠不夠。

就最近的一個案例來說，針對一個被積極利用的零時差攻擊發佈了一個免費的非官方修補程式，該修補程式允許帶有錯誤格式簽名的檔案避開 Windows 10 和 Windows 11 中的 Mark-of-the-Web (MotW) 安全警告。

我們在上一個報告中已經提到，Microsoft 現在為從網際網路下載的檔案新增了一個 MotW 標幟，使得作業系統在檔案啟動時顯示安全警告。但威脅行動人接著開始使用獨立的 JavaScript 檔案在受害者的裝置上安裝 Magniber 勒索軟體，并且 Windows 在啟動時沒有顯示任何安全警告，即使它們包含 MotW。如何可以這樣做？由於 JavaScript 檔案是使用格式錯誤的簽名以數位方式簽署的，而 Windows 允許執行已簽名的檔案。

由於此零時差弱點正在勒索軟體攻擊中被積極利用，0patch 決定發佈一個非官方的修正程式，可以在 Microsoft 發佈官方安全更新之前使用。0Patch 共同創辦人 Mitja Kolsek 在一篇部落格文章解釋，這個錯誤是由 Windows SmartScreen 無法剖析檔案中錯誤格式簽名引起的。Microsoft 隨後在 11 月的修補程式星期二中發行了官方修正程式。

Microsoft 修補程式星期二

一如往常，Microsoft 在修補其熱門產品上有很多事情要做。7 月，公司發佈了 84 個修正程式，四個評級為嚴重。我們在下方列出了最重要的變更。

修復的最嚴重的弱點是 Windows Graphic 元件中的遠端程式碼執行。CVE-2022-30221 獲得了 8.8 的 CVSS 評分。為了充分利用這個瑕疵，攻擊者需要說服使用者連接至惡意 RDP 伺服器，這可能不太容易。

同樣為嚴重，CVSS 評分 8.1 的是一個名為 CVE-2022-22029 的網路檔案系統 RCE。與前一個 RCE 弱點類似，攻擊者需要建立未驗證、專門設計的 NFS 服務叫用來觸發遠端程式碼的執行。

8 月，Microsoft 發佈了 123 個修正程式，17 個評級為嚴重。這 17 個嚴重弱點中有三個是 Exchange 中權限弱點的提高。隨著越來越多的安全瑕疵被發現和在網路攻擊中使用，Exchange 今年一直在定期進行安全更新。CVE-2022-24477、CVE-2022-24516 和 CVE-2022-21980 都有 8.0 的 CVSS 基礎評分。Microsoft 還提到，除了安裝最新的更新外，容易受到此問題影響的客戶還需要啟用擴充保護才能防止此類攻擊。

另一個嚴重弱點是 Windows 11 專屬的。根據官方公告，CVSS 基礎評分 8.8 的 CVE-2022-35804 很可能已被利用。Microsoft Server Message Block 3.1.1 (SMBv3) 通訊協定中的一個問題以及其處理特定請求的方式讓成功利用弱點的攻擊者在目標系統上執行程式碼。

9 月的修正程式較少：總共 63 個，其中 5 個評級為嚴重。這五個中只有一個更容易被利用。CVE-2022-34718 是一個遠端

程式碼執行弱點，CVSS 評分高達 9.8。一旦被利用，未驗證的攻擊者就可以向已啟用 IPSec 的 Windows 節點傳送一個專門製作的 IPv6 封包。反之，這可以在該機器上啟用遠端程式碼執行入侵。然而，這也意味著只有執行 IPSec 服務的系統才容易遭受此攻擊。

另外兩個嚴重弱點 CVE-2022-34721 和 CVE-2022-34722 在 Windows Internet Key Exchange (IKEv1) 通訊協定中啟用遠端程式碼執行。所有 Windows Server 都會受到影響，因為它們接受 v1 和 v2 封包。這些弱點允許未驗證的攻擊者向執行 Windows 和已啟用 IPSec 的目標機器傳送一個專門設計的 IP 封包，從而允許遠端程式碼執行。

10 月修補程式星期二擁有 89 個修正程式，其中 13 個評級為嚴重。這次，最嚴重的一個在熱門 SharePoint 網站中進行了修補。CVE-2022-41038 收到了 8.8 的 CVSS 基礎評分。攻擊者必須通過目標站點的驗證，並且擁有存取和使用 Sharepoint 中的管理清單的權限。如果利用此弱點，會讓攻擊者在 SharePoint 伺服器上遠端執行程式碼。此外，還修復了 SharePoint 的三個不太嚴重的弱點。CVE-2022-41037、CVE-2022-41036 和 CVE-2022-38053 全部都是 CVSS 評分 8.8 的 RCE 弱點。

Windows 點對點通道通訊協定中修補了七個嚴重的弱點。全部都收到了 8.1 的 CVSS 基礎評分。為了利用弱點，攻擊者需要向 PPTP 伺服器傳送一個專門設計的惡意 PPTP 封包。如果成功，攻擊者接著可以在目標機器上遠端執行程式碼。

最後一個重要弱點 (CVE-2022-37968) 收到了最高 10 的 CVSS 基礎評分。它在 Azure Arc 啟用的 Kubernetes 叢集的叢集鏈接功能中。由於 Azure Stack Edge 允許使用者透過 Azure Arc 將 Kubernetes 工作負載部署在裝置上，Azure Stack Edge 裝置也會被視為容易受攻擊。

2022 年 11 月的修補程式星期二，總共修復了 68 個瑕疵，為六個被積極利用的 Windows 弱點提供了修正程式。這包括 11 個允許進行權限提升、詐騙或遠端程式碼執行的嚴重弱點。這些數字不包括 11 月 2 日披露的兩個 OpenSSL 弱點，我們隨後會涵蓋在此報告中。

我們來檢查一下嚴重的吧。CVE-2022-41128 - Windows Scripting Languages 遠端程式碼執行弱點要求裝有受影響版本 Windows 的使用者存取惡意伺服器。攻擊者必須託管一個專門設計的伺服器共用或網站，接著說服使用者造訪它，通常以引誘的電子郵件或聊天訊息的方式。

Windows Mark of the Web 安全性功能避開弱點 (名為 CVE-2022-41091) 也得到了修復。Windows Print Spooler 權限提高弱點 (CVE-2022-41073) 可讓成功利用此弱點的攻擊者獲得系統權限。

Microsoft Exchange Server 權限提高弱點 (CVE-2022-41040) 透過零時差計畫披露。如果被觸發，攻擊者將可以在系統上下文中執行 PowerShell。

另一個 Exchange 弱點 (CVE-2022-41082) 也允許遠端程式碼執行。作為一名驗證的使用者，攻擊者可以嘗試透過網路叫用在伺服器帳戶的上下文中觸發惡意程式碼。

Google、Adobe 以及其他修補活動

今年下半年，Google 一如既往地專注於其 Chrome 瀏覽器安全性修正程式。從今年開始，瀏覽器的最新版本 107.0.5304.87/88 包含第七個零時差弱點的修正程式。前六個以每個月大約一次的頻率修復，最近的三個發生在九月 (CVE-2022-3075)、八月 (CVE-2022-2856) 和七月 (CVE-2022-2294)。某些情況下，在 Google 發現並修補之前，這些弱點被國家資助的威脅行為人利用了幾週。

上述新版 Chrome 中修復的高嚴重性瑕疵 (CVE-2022-3723) 是 V8 Javascript 引擎中的類型混淆錯誤。當計畫使用類型分配資源、物件或變數，然後使用其他不相容的類型存取它，導致超出邊界的記憶體存取時，就會出現類型混淆弱點。透過存取應用程式上下文中禁止的記憶體區域，攻擊者可以讀取其他應用程式中的機密資訊，造成當機或執行任意程式碼。

Adobe 在過去的五個月有很多事情要做。他們最近一批安全性修補程式包含多個企業面向產品中 29 個已記錄弱點的修正程式，駭客可以利用這些弱點來完全控制容易受攻擊的機器。這些弱點可能使 Windows 和 macOS 使用者遭受任意程式碼執行、任意檔案系統寫入、安全性功能避開和權限提升攻擊。根據 Adobe 嚴重級別報告，總共修復了 13 個 ColdFusion 瑕疵，包括一些具有 CVSS 9.8/10 嚴重性評分。

Adobe Commerce 和 Magento 開放原始碼瑕疵 (CVE-2022-35698) 被廠商描述為跨站點指令碼 (儲存的 XSS) 錯誤 (CVSS 嚴重性評分為 10.0)。

Adobe Dimension 產品也有具有最高嚴重性評分的錯誤。公司解決了九個記錄的威脅，並指出 Windows 和 macOS 使用者都面臨著程式碼執行和記憶體洩漏攻擊的風險。

在此之前，Adobe 發佈了 25 個已記錄安全性弱點的修補程式，這些弱點會讓使用者遭受惡意攻擊。Acrobat 和 Reader 更新解決了多個嚴重和重要的弱點。成功利用會導致任意程式碼的執行和記憶體洩漏。Adobe 還發佈了一個公告，包含 Adobe Illustrator 2022 軟體中四個安全性缺陷的詳細資料。

在九月的安全性更新中，Adobe 解決了七個產品中的 63 個弱點。所有這些弱點都收到 5.3 到 7.8 之間的 CVSS 基礎評分，其中 35 個為嚴重。利用會導致大量問題，例如任意程式碼執行、安全性功能避開、任意檔案系統讀取和記憶體洩漏。

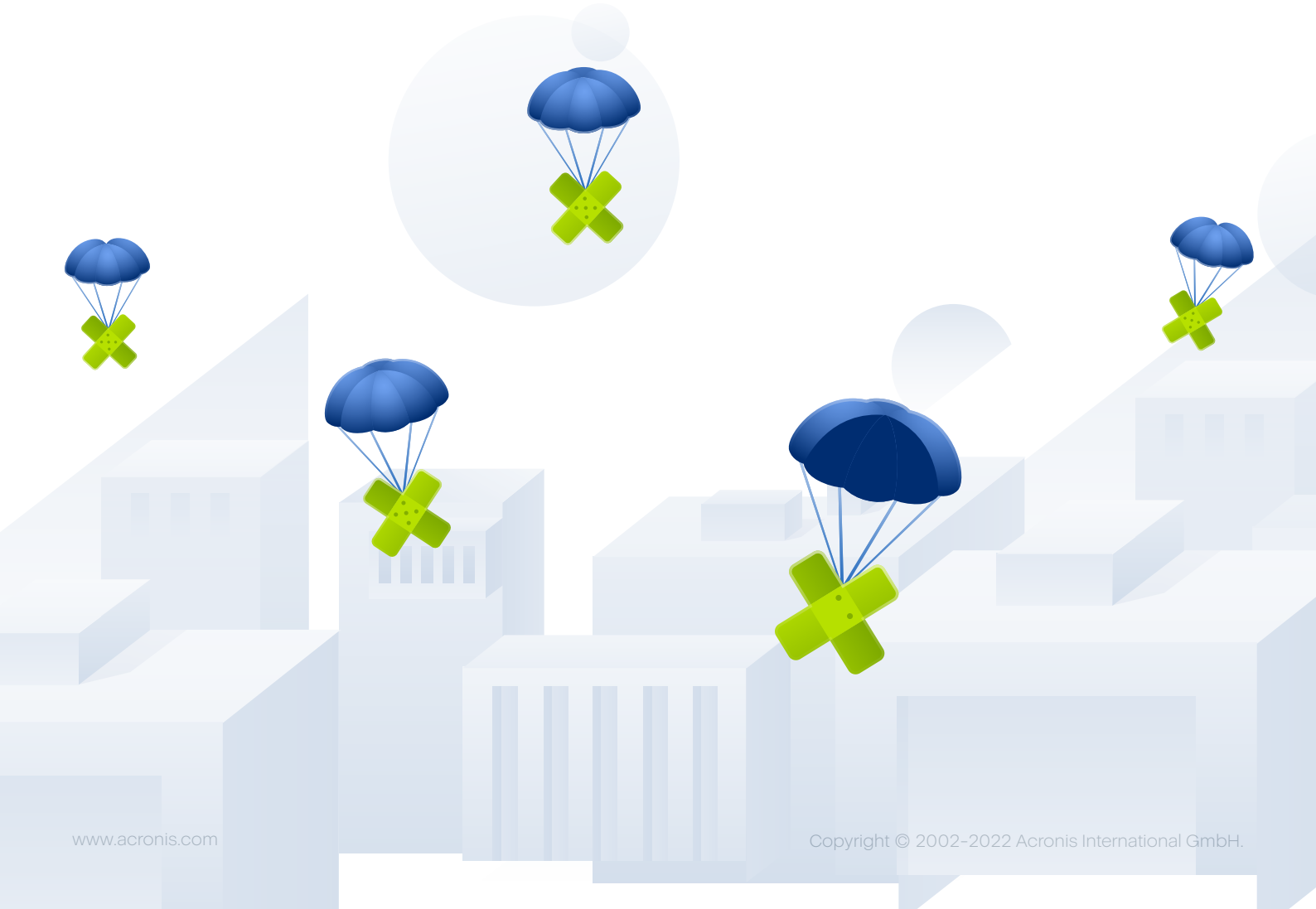
最嚴重的情況是針對 Windows 和 macOS 的 Adobe Bridge (APSB22-49)，12 個已修補弱點中的 10 個標記為嚴重。適用於 Windows 和 macOS 的 Adobe InDesign (APSB22-50) 在 18 個弱點 (包括 8 個嚴重) 修復之前處於不利地位。最後但同樣重要的是適用於 Windows 和 macOS 的 Adobe Photoshop 2021 和 2022 (APSB22-52)，10 個弱點已修補，其中的九個為嚴重。

其他廠商也發佈了重要的更新。OpenSSL 專案修補了用於加密通訊通道和 HTTPS 連線的開放原始碼加密程式庫中的兩個高嚴重性安全性瑕疵。弱點 (CVE-2022-3602 和 CVE-2022-3786) 會影響 OpenSSL 版本 3.0.0，並已在 OpenSSL 3.0.7 中予以解決。

CVE-2022-3602 是一個會觸發當機或導致遠端程式碼執行 (RCE) 的任意 4 位元組堆疊緩衝區溢位，而 CVE-2022-3786 可由攻擊者透過惡意電子郵件地址利用來透過緩衝區溢位觸發拒絕服務狀態。OpenSSL 還提供了緩解措施，要求操作 TLS 伺服器的管理員停用 TLS 用戶端驗證，直至修補程式已套用。

同樣地，Cisco 警告客戶 Cisco AnyConnect Secure Mobility Client for Windows 中的兩個安全性弱點正在被利用。兩個安全性瑕疵 (CVE-2020-3433 和 CVE-2020-3153) 可讓本地攻擊者執行 DLL 劫持攻擊和複製檔案至具有系統層級權限的系統目錄中。成功利用之後，攻擊者可以在具有系統權限的目標 Windows 裝置上執行任意程式碼。這兩個弱點都需要驗證，需要攻擊者擁有有效的系統憑證。

這僅僅是過去五個月發現和修復的大量弱點中的一小部分。我們知道，勒索軟體攻擊在相同時期利用了 150 多個弱點，再次強調了按時修補和擁有弱點評估功能來保護企業和家庭使用者的重要性。



Acronis 關於在目前和未來威脅環境中保持安全的建議

現代網路攻擊、資料洩漏和勒索軟體爆發都表明了同一件事：網路資安是失敗的。出現此失敗是技術薄弱和人為錯誤的雙重結果，人為錯誤通常由聰明的社交工程導致。

即使您的備份解決方案運作良好且未被盜用，在網路事件之通常需要幾小時和幾天的時間來將系統（含資料）還原至運作狀態。網路資安解決方案失敗時備份是必要的，但同時這些工具可能會被盜用、停用，緩慢地執行，導致企業因停機時間而損失大量的資金。

為了解決這些問題，我們建議使用整合式網路資安防護解決方案，例如 Acronis Cyber Protect，它將防惡意軟體、EDR、DLP、電子郵件安全性、弱點評估、修補程式管理、RMM 及備份功能結合在一系列 Windows 作業系統下執行的單一代理程式。這種整合可讓您維持最佳的效能、消除相容性問題，及確保快速地復原：如果在資料改動期間威脅未發現或偵測到，則資料將立即從備份中還原。由於有了單一代理程式，解決方案知道資料何時遺失和需要還原。

對於在備份解決方案中執行單獨代理程式的防惡意軟體解決方案，這是不可能的。其他網路資安產品可能會阻止威脅，但無法還原已經遺失的任何資料。備份代理程式自動知道該情況，并且資料會被緩慢地還原(如果有的話)。

當然，Acronis Cyber Protect Cloud 會在威脅危害環境之前偵測並消除它們，努力讓資料復原不需要進行。這會透過我們增強的多層網路資安功能實現。

也就是說，公司和家庭使用者不可忘記基本的安全規則，即便他們使用的是 Acronis Cyber Protect 之類的現代解決方案。

修補您的作業系統和應用程式

修補非常關鍵，因為很多攻擊因未修補的弱點而成功進行。藉由 Acronis Cyber Protect 之類的解決方案，您就被內嵌式弱點評估和修補程式管理功能所覆蓋。我們會追蹤所有已發現的弱點和已發行的修補程式，並允許管理員或技術人員使用靈活的組態和詳細的報告來輕鬆地修補所有端點。Acronis Cyber Protect 支援所有內嵌式 Windows 應用程式以及 300 個熱門第三方應用程式，其中包括 Zoom 和 Slack 之類的電信工具，及遠端工作中使用的熱門 VPN 用戶端。請確保先修補高嚴重性的弱點，並遵循成功報告來檢查修補程式是否已正確套用。

若您沒有 Acronis Cyber Protect 且/或未使用任何修補程式管理軟體，工作就會困難很多。至少，您需要確定 Windows 獲取所有需要的更新并且這些更新已及時安裝。使用者常常會忽略系統郵件，尤其在 Windows 要求重新啟動時，這是一個很嚴重的錯誤。確保 Adobe 之類的熱門軟體廠商的自動更新已啟用，且 PDF Reader 之類的應用程式也及時進行了更新。

準備好應對網路釣魚嘗試，不要按下可疑的連結

主題型網路釣魚和惡意網站每天都會大量地出現。這些時常在瀏覽器層級被篩選出來，但是有了 Acronis Cyber Protect 之類的網路資安防護解決方案后還會優惠專屬的 URL 篩選功能。惡意連結隨處可來：即時訊息應用程式、電子郵件、論壇貼文等。請勿按下您不需要或您不希望收到的連結。

惡意主題附件也可以透過電子郵件傳送。始終檢查帶有附件的郵件的真實出處，並問您自己是否希望收到它。無論如何，在開啓附件之前，須由您的反惡意軟體解決方案進行察看。

在處理業務資料時使用 VPN

無論您是連接至遠端公司來源和服務，還是您的工作不需要這些活動，您只需要瀏覽部分網路資源和使用電信工具，使用虛擬私人網路 (VPN)。VPN 會加密所有流量，使其安全以防攻擊者試圖擷取您正在傳輸的資料。

如果您的公司有一個 VPN 程序，您將很可能獲得來自管理員或 MSP 技術人員的指導。如果您必須親自保護自己的工作場所，請使用推薦的知名 VPN 應用程式和服務，這些應用程式和服務是軟體市場廣泛提供的，或直接從廠商處購買。

確保您的網路資安正常地執行

Acronis Cyber Protect 使用很多平衡良好且精確調整的安全性技術，包括多個偵測引擎。我們建議用此解決方案取代嵌入式 Windows 或 macOS 安全性工具。

但僅擁有一種防惡意軟體防禦能力是不夠的，他們應正確地設定。

這意味著：

- 每天應至少執行一次全面的掃描。
- 產品需要檢查和擷取，並經常更新 (每天，最好是每小時)。
- 產品應連接到其雲端偵測機制，如果是 Acronis Cyber Protect，則連接至 Acronis Cloud Brain。它依預設是開啓的，但您需要確定網際網路可用且不會意外被防惡意軟體阻止。
- 隨需和即時監視 (即時) 掃描應啟用，並對每個已安裝或已執行的新軟體進行應變。

此外，不要忽略來自防惡意軟體解決方案中的訊息。如果您正在使用安全廠商提供的付費版本，請仔細地閱讀這些訊息，確保授權是合法的。

只讓您自己知道密碼和保持工作隱私權

安全性秘訣 1：確定您的密碼和您員工的密碼為強式且私密。不要與任何人分享密碼。

針對您所使用的每個服務使用不同的長密碼；密碼管理軟體可幫助您記住它們。一個建立強式密碼的方法是建立一組您可以輕鬆記住的長片語。現在，8 個字元的密碼可輕鬆地暴力破解。可能的話，使用多重要素驗證來獲得額外的安全層級。

即使在家工作，也要記得將您的筆記型電腦/桌上型電腦鎖定並限制它的存取。他人可以輕鬆地檢視、竊取或刪除 (甚至是意外的) 未鎖定系統中的機密檔案。

Acronis 針對 2023 年的網路資安趨勢與預測

當今世界比以往任何時候都要依賴於數字。IT 環境正變得越來越複雜，彈性的小瑕疵可能會對組織在發生安全事件或漏洞後繼續運營的能力產生重大影響。

以下是塑造 2023 年網路資安態勢的十個趨勢：

1. 驗證和身分管理系統在視綫範圍內

驗證和身分存取管理系統（IAM）將被更頻繁地成功攻擊。很多攻擊者已經開始竊取或避開多重要素驗證（MFA）權杖。在其他情況下，用 MFA 請求壓倒目標會導致不需要弱點即可成功登入。最近針對 Okta 和 Twilio 的攻擊表明，這些外部服務也被洩漏。當然，這是多年以來使用者選取（以及重複使用）弱式密碼的問題。更重要的是確保 MFA 已正確設定，並為所有公司員工提供所需的最低存取權。

2. 勒索軟體會帶來更大的損害

勒索軟體威脅仍在不斷地壯大。雖然我們看到了更多的資料洩漏，主要行為人仍在繼續使其作業專業化。

大多數大型參與者已擴展到 macOS 和 Linux，并且還在關注雲端環境。諸如 Go 和 Rust 之類的新程式化語言正在變得越來越常見，需要在分析工具中進行調整。

攻擊的數量會繼續增長，因為它們仍然有利可圖，尤其在網路保險涵蓋了部分影響時。這無疑會進一步增加網路保險費的成本。攻擊者會越來越多地關注解除安裝安全性工具、刪除備份和盡可能停用災難復原計畫。離地攻擊技術將在這方面發揮重要的作用。

3. 大衆的資料外洩

Raccoon 和 RedLine 之類的資訊竊取惡意軟體正在成為感染的常態。被竊取的資料通常包含使用者憑證，接著會透過初始存取代理人來出售以利未來的攻擊。資料 Blob 數量越來越多加上互連雲端服務的複雜性，使得組織更難追蹤資料。多方存取資料的需求使得對資料加密和保護變得更加困難。一個被洩漏的 API 存取金鑰，例如 GitHub 或行動應用程式上的 API 存取金鑰，就足以竊取所有資料。這將導致隱私權友好的運算變得有進步。

4. 網路釣魚不僅僅是電子郵件

數百萬的惡意電子郵件和網路釣魚攻擊將繼續傳送。攻擊者將繼續試圖使用之前洩漏的資料自動化和個人化其攻擊。社交設計的詐騙，例如商務電子郵件入侵（BEC）攻擊，將越來越多地傳播到其他訊息傳送服務（SMS/文字、Slack、Teams 聊天等），以避免篩選和偵測。另一方面，網路釣魚將繼續使用代理來擷取作業階段權杖、竊取 MFA 權杖和使用 QR 碼之類的轉移來進一步自我隱藏。

5. Not-so-smart contracts

對加密貨幣交換和各種區塊鏈上智慧合約的攻擊遠遠沒有結束。甚至國家攻擊者也在試圖竊取數億的數位貨幣。除了針對使用者的傳統網路釣魚和惡意軟體攻擊之外，針對智慧合約、演算法貨幣和 DeFi 解決方案還會繼續進行更複雜的攻擊。

6. 依靠基礎架構

服務供應商越來越多地被攻擊和入侵。攻擊者接著會濫用 PSA、RMM 或其他部署工具之類的已安裝工具來進行離地攻擊。這不僅會威脅到受管理的 IT 服務提供者，還會威脅到諮詢公司、一級支援組織和類似的合作夥伴。外包的內部人員通常被部署為目標組織中最弱的環節，不需要精心設計軟體供應鏈攻擊。

7. 從瀏覽器內部叫用

瀏覽器中或透過瀏覽器會有更多的攻擊，導致從作業階段內部進行攻擊。惡意瀏覽器副檔名可以交換加密貨幣交易的目標地址，或在背景中竊取密碼。還有一種趨勢是劫持此類工具的原始程式碼，並透過 GitHub 存放庫新增後門。另一方面，網站將繼續使用 JavaScript 跟蹤使用者，並跨 HTTP 推薦者向行銷服務過度共用作業階段 ID。攻擊者將使用 Formjacking/Magecart 技術擴展，其中新增的小片段會竊取原始網站背景中所有資訊。隨著無伺服器運算的增加，此類攻擊的分析會變得更複雜。

8. 透過 API 進行雲端自動化

資料、程序和基礎架構已向雲端轉移。隨著不同服務之間的自動化提高，這種情況會繼續。很多 IoT 裝置將成為此大型超連接的服務雲端的一部分。這會導致很多 API 可從網際網路存取，從而增加了大規模自動化攻擊的風險。

9. 業務流程攻擊

攻擊者總會提出如何為自己的利益修改業務流程的新想法，例如在組織的帳務系統範本中變更接收銀行賬戶的詳細資料，或將其雲端 bucket 新增為電子郵件伺服器的備份目的地。這些攻擊通常不涉及惡意軟體，但需要對使用者行為進行密切的分析，就像越來越多的內部攻擊一樣。

10. AI 無處不在

AI 和 ML 程序將由所有規模和行業的企業使用。綜合資料建立的進步將進一步助長使用深度偽造的內容進行身分欺詐和錯誤資訊活動。更令人擔憂的趨勢是針對 AI 和 ML 模式自身的攻擊。攻擊者會嘗試使用模式中的弱點，故意在資料集中植入偏差，或僅使用觸發程序向 IT 公司傳送警報。

Acronis 簡介

Acronis 結合資料保護與網路資安，提供整合式的自動化 網路資安防護 ，解決現代數位世界在安全、易用性、隱私權、真實性與安全性 (SAPAS) 幾方面的挑戰。Acronis 的靈活部署模型符合服務供應商與 IT 專業人員的需求，藉由創新的新世代防毒、備份、災難復原以及 AI 提供的端點防護管理解決方案，為資料、應用程式和系統提供優越的網路資安防護。依靠進階防惡意軟體 (由先進的機器智慧和區塊鏈資料驗證技術提供支援的)，Acronis 可在任何環境 (包括雲端、混合和地端部署) 提供防護，且價格實惠。

Acronis 於 2003 年在新加坡創立，並於 2008 年在瑞士註冊成立有限公司，目前在全球擁有 34 個辦公據點和 2,000 多名員工。Acronis 的解決方案廣獲超過 550 萬名居家使用者及 500,000 家公司，以及頂級的職業運動隊伍信賴。Acronis 的服務範圍遍及全球超過 150 個國家/地區，共有 50,000 多個合作夥伴及服務供應商提供 Acronis 的產品，服務語言超過 26 種。

Acronis

瞭解詳情：
www.acronis.com