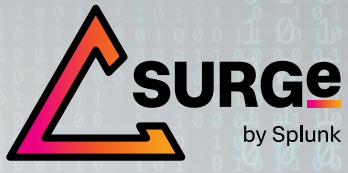
白皮書

勒索軟體二進位檔案的實證比較分析

Shannon Davis 著



splunk>
turn data into doing

執行摘要

雖然資訊安全研究和網路防禦人員已經寫過不少關於勒索軟體的文章，但是依然有許多組織仍然對此類攻擊保持隨機應變，而非留意警覺。這是因為缺少有關勒索軟體的基準知識。勒索軟體加密速度是一個值得進一步研究的領域。迄今為止，關於此主題最全面的資訊來自 LockBit 勒索軟體發行者本身，他們在自己的網站上比較各類勒索軟體的加密速度，以宣傳自己擁有「最快的」勒索軟體。 本文旨在闡明以往只有罪犯自己會研究的領域。我們在受控制的環境中利用科學方法，於不同的 Windows 作業系統和硬體規格上，測量了 10 種流行勒索軟體變體的速度，共加密近 100,000 個檔案 (總計近 53GB)。透過這項工作，我們希望為防禦人員提供更多的知識和信心，讓他們在偵測時就能「解除危機」，而不是如 Lockheed Martin Cyber Kill Chain 白皮書中討論的「目標行動」階段時才偵測。

為了判斷勒索軟體的加密速度，我們建立並修改了 Splunk Attack Range 實驗室環境，在四台主機上執行 10 種勒索軟體變體中各自的 10 個樣本。兩台主機執行 Windows 10 作業系統，另外兩台主機執行 Windows Server 2019。我們只挑選 VirusTotal 中 Microsoft Defender Antivirus 認定的樣本，將勒索軟體樣本歸類至各變體。我們為每個主機分配了「高級」或「中級」資源，以測試勒索軟體在不同處理器、記憶體和硬碟配置下的表現。為了收集、彙總和分析 Splunk 上的資料，我們在每台主機上啟用了 Windows 記錄。這使我們能夠測量勒索軟體變體加密近 100,000 個檔案的速度，以及勒索軟體如何利用處理器、記憶體和磁碟等系統資源。

在執行共 100 個勒索軟體樣本後，我們確定總加密時間 (TTE) 從 4 分鐘到 3 個半小時不等，速度中位數為 42 分鐘。由於時程不長，組織在加密完成前進行有效應對的時間也有限。在具有不同資源的系統中比較相同的勒索軟體病毒時，我們發現一些變數可能會影響 TTE，例如處理器速度或 CPU 核心。不過，影響並不一致，表示某些勒索軟體屬於單執行緒，或是不太能夠利用額外的資源。LockBit 勒索軟體是在任何系統上加密最快的變體。這與之前的報告一致，即 LockBit 每個檔案僅加密 4KB，使檔案無法使用並加速攻擊。「最快的勒索軟體」的標題也與 LockBit 開發人員在該組織 Tor 網站上的公開聲明相符。

SURGe 計劃在這項研究的基礎上為網路防禦人員建立全面性的勒索軟體整體概觀。尤其是，我們計劃使用開源檔案分析框架工具，例如 stoQ、模糊演算法和 Splunk 電腦學習工具套件 (MLTK)，來檢視多個勒索軟體樣本的檔案存取技術。此外，我們計劃調查現代勒索軟體不受 Packer 遮蔽的聲明，並判斷是否有可能在未知勒索軟體二進位檔案「部署」當下對待確定的分類器進行叢集，而非在執行後才偵測。我們計劃於 2022 年 6 月在 .conf22 上發布這項研究的資料集。我們鼓勵研究人員調查這個語料庫並驗證我們的發現，或據此來幫助全球網路資安社群。

關鍵發現

- 在我們的測試中，LockBit 勒索軟體在 10 種勒索軟體變體中執行速度最快，這與勒索軟體組織在其 Tor 網站上的聲明一致
- 勒索軟體變體在 98,561 個檔案的語料庫中 (大小為 53.83 GB) 加密的時間中位數為 42 分 52 秒，
- 單個勒索軟體樣本的加密速度差異極大，從四分鐘到三個半小時不等。
- 改進的硬體功能為一些勒索軟體樣本提供了更快的加密速度。其他樣本和變體無法利用增加的資源，有時在更高規格的系統上表現得更差。其他記憶體對任何樣本的加密速度沒有顯著影響。更高的磁碟速度可能會在較快的執行中發揮作用，但最有可能與可以利用的其他 CPU 核心變體結合使用。

緒論

在 2021 年 M-Trends 的報告中，Mandiant 發現，他們在 2020 年的調查裡有 25% 涉及到勒索軟體，高於 2019 年的 14%。[1]Verizon 2021 年資料外洩調查報告 (DBIR) 指出，從 2019 年到 2021 年，勒索軟體的發生頻率翻了一倍。[2]儘管在公眾意識中相對較新，但這種類型的惡意軟體自 1989 年在 AIDS 會議上透過軟碟片首次發布後就一直困擾著全世界。[3]

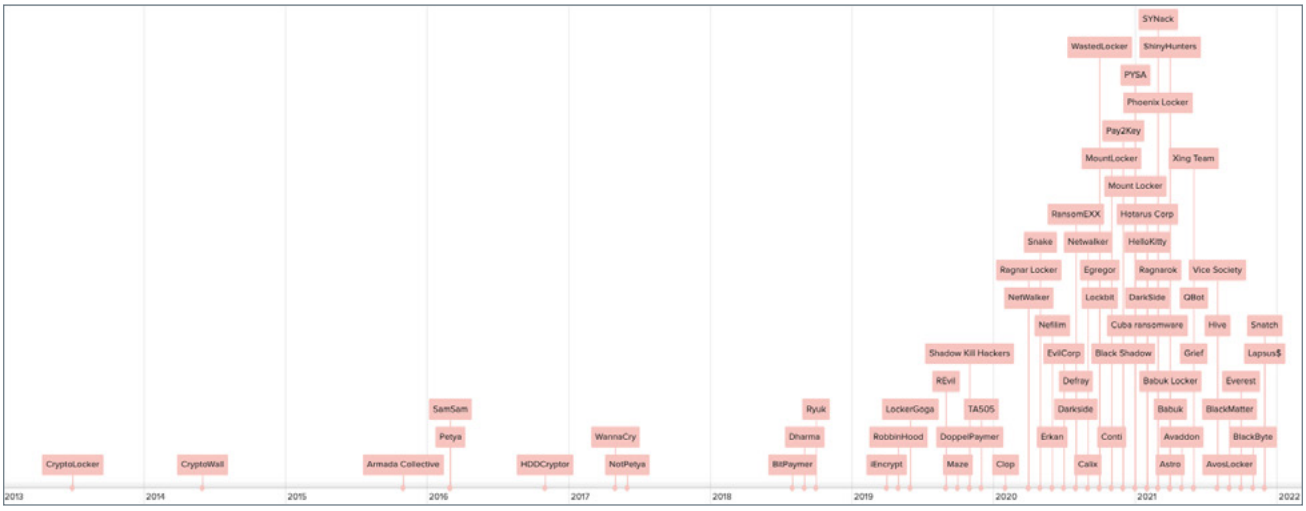


圖 1.Spunk 圖表凸顯出勒索軟體種類從 2013 至 2022 年的增長。

前面提到的 M-Trends 報告指出，在美洲，勒索軟體的停留時間中位數為三天。[4]三天停留時間聽起來並不多，但長期以來人們認為勒索軟體的停留時間更短，僅為幾小時甚至幾分鐘。如果停留時間中位數是以天而不是小時為單位來衡量，防禦人員還有小空檔能夠採取行動。2021 年，CERT NZ 發布了一份白皮書，概述了勒索軟體的生命週期，並提出建議，幫助組織應對這日益嚴重的威脅 (圖 2)。[5]

1. FireEye and Mandiant, "Fireeye-Rpt-Mtrends-2021.Pdf," April 13, 2021, 13, https://www.mandiant.com/resources/m-trends-2021.
2. Verizon, "DBIR 2021 Data Breach Investigations Report," May 12, 2021, 14, verizon.com/dbir.
3. "Case Study:AIDS Trojan Ransomware," SDxCentral，引用時間 2022 年 2 月 23 日 https://www.sdxcentral.com/security/definitions/case-study-aids-trojan-ransomware/。
4. FireEye and Mandiant, "M-Trends 2021," 14.
5. "How Ransomware Happens and How to Stop It," CERT NZ.，引用時間 2022 年 1 月 29 日 https://www.cert.govt.nz/it-specialists/guides/how-ransomware-happens-and-how-to-stop-it/。

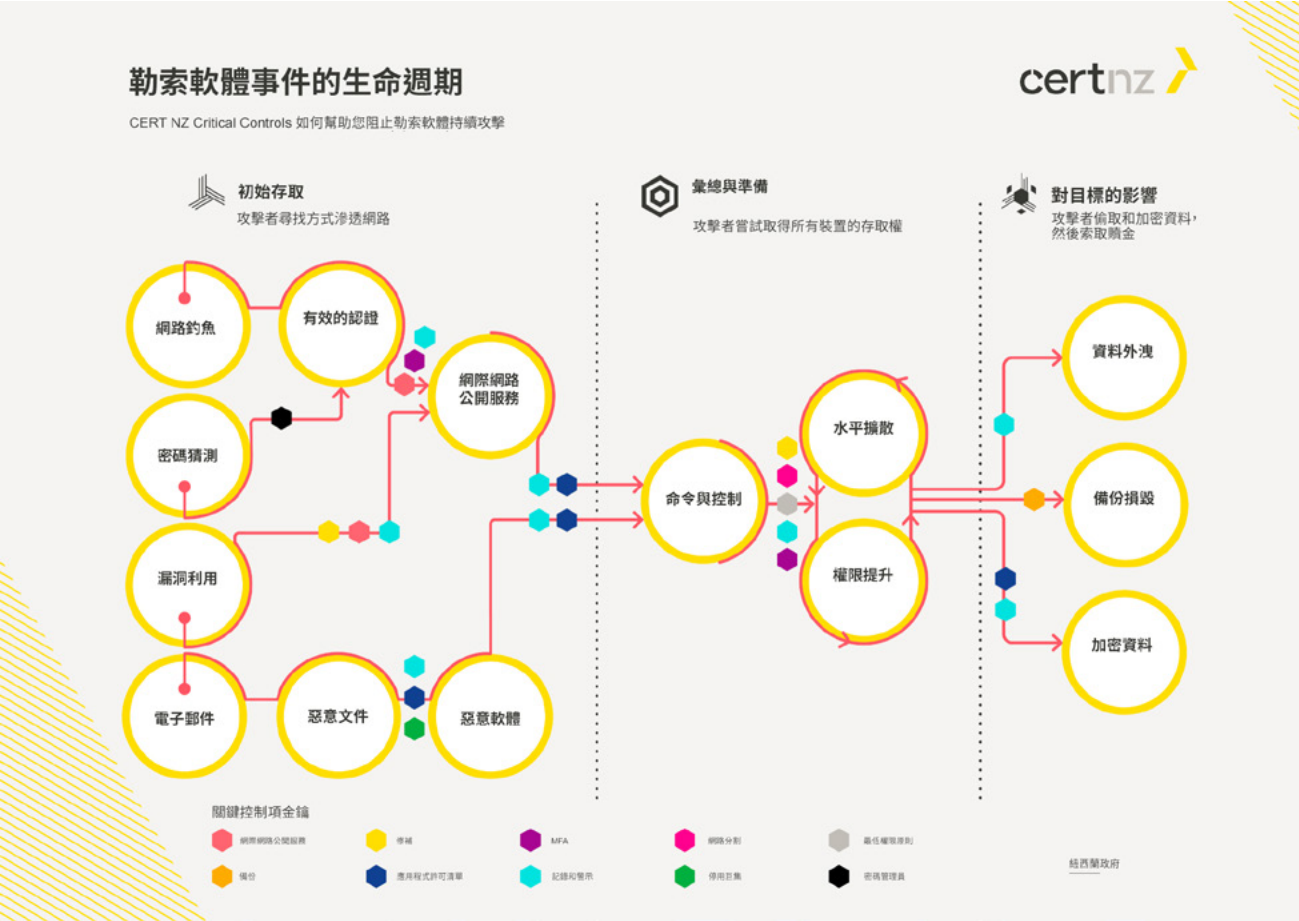


圖 2。CERT NZ 勒索軟體事件的詳細進展。

CERT NZ 的這項工作和引用 Mandiant 所說的三天停留時間讓我們想瞭解組織該如何積極地防禦勒索軟體。在開始研究防禦方法前，我們先決定調查兩個問題：

- 首先，勒索軟體病毒加密主機需要花費多久時間？
- 組織能否恢復或防止檔案系統的完全加密？

逆向工程師做了很多事來瞭解為什麼某些勒索軟體病毒加密速度如此之快。除了來自 Lockbit 勒索軟體團隊的宣傳外，我們無法找到任何實證研究來比較不同種類勒索軟體的加密速度。[6,7]本文概述了我們對 10 種勒索軟體加密速度的動態評估分析，並為資安團隊提供了一些建議，以更進一步決定防禦手段。應該注意的是，本文並非旨在建立勒索軟體偵測。相反，我們的目標是讓防禦人員瞭解勒索軟體加密速度的整體真相。

> 本文略述了我們對 10 種勒索軟體加密速度的動態評估分析，並為資安團隊提供了一些建議，可以為他們的防禦策略提供更進一步的資訊。

6. “LockBit BLOG.”，引用時間 2022 年 1 月 13 日 http://lockbitapt6vx57t3eeqjofwgcglmutr3a35nygvokja5uuccip4ykyd[.]onion.ly/conditions。
7. Gridinsoft LLC, “LockBit Ransomware.The Most Honest and the Fastest,” Gridinsoft LLC，引用時間 2022 年 1 月 29 日 https://gridinsoft.com。

準備就緒

我們開始不斷地丟問題來集思廣益提出的假設，像是勒索軟體加密速度有多快，以及假設勒索軟體加密比預期中快，組織如何才能「解決危機」[8]我們首先將問題彙總為一個假設：**假設敵人獲得對系統的存取權並部署勒索軟體，那麼加密的速度將比網路防禦人員實際上能阻止的速度更快**。Verizon DBIR 指出，大多數組織在敵人獲得系統存取權限後幾天才偵測到違規行為，而不是幾小時或幾分鐘。[9]為了測試我們的假設，我們需要建立一個實驗室進行重複測試，收集不同勒索軟體二進位檔案的樣本，然後分析我們的發現。我們也希望以符合資安團隊需求的方式進行這項研究。因此，我們選擇不對惡意軟體二進位檔案執行靜態的逆向工程，而是在受控環境中動態執行，並在相同的變因下對其進行測量。我們計劃在未來的部落格、論文和會議演講中詳細解釋我們的方法和技術流程。

白皮書的這一節，我們會解釋如何構建實驗來測試我們的假設。我們也會詳細介紹惡意軟體實驗室裡的概略架構、配置，以及我們獲取惡意軟體的方式和原因。最後，我們在研究和分析中列出所有已知的假設，這些假設可能會在我們的發現中呈現出偏差。

方法

為了測試我們的假設，我們需要在受控環境中執行各種勒索軟體病毒，從端點主機收集 Windows 本機效能遙測資料，並分析。我們選擇了 10 種勒索軟體，每種有 10 個獨立的二進位檔案，以防止出現叢集錯覺 (傾向看到不存在的模式) 以及確認偏差 (傾向尋找支持我方論點的資訊)。對於每個 Windows 端點類型和資源規格，在每種勒索軟體內建立一個 Amazon Web Services (AWS) 虛擬私有雲 (VPC)，每種個別的二進位檔案會在專門為其評估而建立的主機上執行。測試結果會轉送至中央 Splunk 執行個體內進行分析。每台主機在 100 個目錄中放置了 98,561 個檔案。這些檔案類型來自 Digital Corpora，創辦者認為是最有可能被勒索軟體二進位檔案加密的類型。[10,11,12]這些檔案是在 CC0 許可下提供的，並來自美國政府的公共網站。最後，我們在 Windows 主機上啟用了事件識別碼 4663，以便查看檔案加密情況和每個勒索軟體種類的速度基準。[13]

8. John McHale, "Defending DoD from Cyberattacks, Getting to the Left of the Boom - Military Embedded Systems."，引用時間 2022 年 1 月 30 日 http://militaryembedded.com/cyber/cybersecurity/defending-dod-from-cyberattacks-getting-to-the-left-of-the-boom。
9. Verizon, "DBIR 2021 Data Breach Investigations Report," 90.
10. Simson Garfinkel et al., "Bringing Science to Digital Forensics with Standardized Forensic Corpora," Digital Investigation 6 (September 2009):S2–11, https://doi.org/10.1016/j.diin.2009.06.016.
11. "Digital Corpora Downloads:Corpora/Files/Govdocs1/By_type/"，引用時間 2022 年 1 月 30 日 https://downloads.digitalcorpora.org/corpora/files/govdocs1/by_type/。
12. "Digital Corpora Downloads:Corpora/Files/Govdocs1/Zipfiles/"，引用時間 2022 年 1 月 30 日 https://downloads.digitalcorpora.org/corpora/files/govdocs1/zipfiles/。
13. Microsoft, "4663(S) An Attempt Was Made to Access an Object.(Windows 10) - Windows Security"，引用時間 2022 年 1 月 30 日 https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4663。

實驗室

如前所述，該研究針對在受控環境中執行的勒索軟體二進位檔案。我們使用 Windows 本機審核和記錄功能收集勒索軟體效能，這些功能將結果轉送回 Splunk 執行個體內。遙測設置的資訊在「實驗程序」一節中進行了更詳細的介紹。每個勒索軟體的樣本都是在獨立式環境下執行。每個勒索軟體環境中的 Splunk 執行個體將事件轉送到單個 Splunk 執行個體以進行比較、分析和報告。我們為實驗修改 Splunk 的開源 Attack Range 工具，以建立實驗室 (圖 3)。[14]Attack Range 允許網路防禦人員使用 Splunk 軟體在 AWS 中動態建立小型網路，並合併使用 Terraform 和 Ansible 中預先設定的記錄。

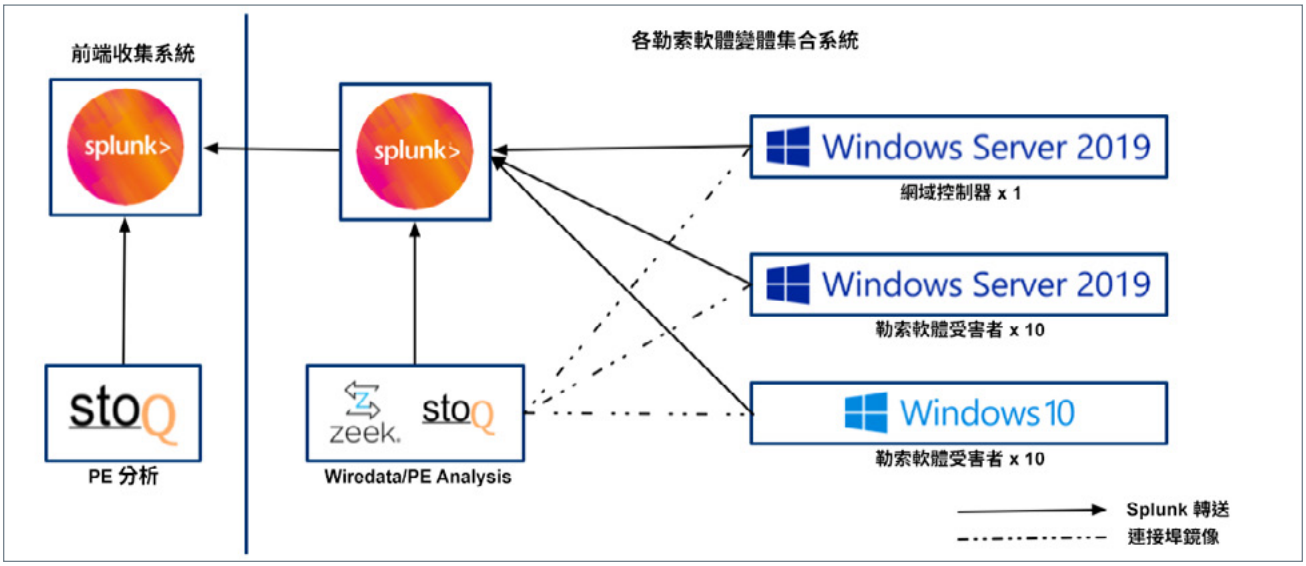


圖 3。我們自定義 Attack Range 的整體概述。

根據我們收集非正式意見的組織和 PC Mag 等流行網站，此範圍內的主機規格與許多現代筆記型電腦或伺服器版本一致。[15]這些主機已解除安裝 Microsoft Defender，並且沒有安裝其他防毒軟體 (AV) 或端點偵測與回應 (EDR) 工具。我們安裝了包括 Splunk 代理在內的其他工具，用於將訊息傳回 Splunk 和 Microsoft 應用程序 Sysmon。[16]最後，為了偵測蠕蟲或遠端對映檔案的加密，這些主機透過網域控制器上的開放共享網路 (C 槽) 被加入到 Windows 網域中。更多有關主機規格和記錄日誌設定的資訊，請參見附錄 A 和 B。為了擷取檔案加密事件，我們對測試目錄和所有子目錄啟用了物件層級稽核，以便檢查成功與失敗的存取嘗試。啟用物件層級稽核後，每次勒索軟體二進位檔案嘗試加密文件時，都會產生事件代碼 4663。最後一個顯示為檔案成功加密的 4663 事件是 DELETE，通常用來追蹤加密速度。雖然我們在測試的軟體種類上不斷看到此事件，但在其他軟體上有可能不會呈現出 DELETE 事件。如果是這種情況，可能需要不同的標記來測量 TTE。

14. Splunk Attack Range, Jinja (2019; repr., Splunk GitHub, 2022), https://github.com/splunk/attack_range.
15. "Dell Latitude 7420 Review | PCMag"，引用時間 2022 年 1 月 30 日 https://www.pcmag.com/reviews/dell-latitude-7420。
16. markruss, "Sysmon - Windows Sysinternals."，引用時間 2022 年 2 月 25 日https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon。

實驗程序

為了完美模擬現代勒索軟體的活動，我們透過 Windows Server 2019 網域控制器上的遠端 PowerShell 指令碼，在 10 台 Windows 10 主機和 10 台 Windows Server 2019 主機上執行勒索軟體。這種遠端 PowerShell 方法以前用於啟動勒索病毒感染，並非使用者手動執行二進位檔案。這種方法額外的好處是模擬現代勒索軟體活動，勒索軟體由操縱者透過指令碼執行，而不是由電腦受害者親自執行。此外，它還減少了「人為互動」造成的一些負荷，這使得勒索軟體能夠利用比原本更多的系統資源。我們在執行時沒有向勒索軟體傳遞任何旗標。我們唯一使用不同方式執行的勒索軟體變體是 Babuk，因為它無法可靠地使用遠端 PowerShell 方法來執行，因此我們在每台主機上以互動方式來啟動 Babuk。每個作業系統使用兩個不同的硬體資料來評估勒索軟體的效能。這些硬體資料的確切規格可在附錄 B 中找到。

PowerShell 指令碼允許我們選擇想要執行的勒索軟體樣本。該指令碼接著會在網域中 Windows 10 或 Windows Server 2019 主機數量內不斷執行，並透過遠端網頁伺服器啟動來下載勒索軟體二進位檔案。每次執行測試都分別在 Windows 10 或 Windows Server 主機上進行，不會同時執行。

每台主機完成下載後，PowerShell 指令碼會遠端啟動每個勒索軟體二進位檔案，但 Babuk 除外。然後，我們能夠使用 Windows 安全事件記錄檔分析每個變體加密檔案的速度。需要事件代碼 4663 (嘗試存取對象) 才能可靠地擷取加密事件。我們為 Windows 10 和 Windows Server 2019 主機上的 100 個測試目錄啟用了檔案系統稽核，以產生所需的事件記錄檔。

勒索軟體二進位檔案

來自 VirusTotal 的 10 個勒索軟體種類中的 100 個勒索軟體樣本我們僅利用 VirusTotal 的 Microsoft Defender 偵測勒索軟體種類屬性。勒索軟體種類的挑選是依照過去 12 到 24 個月內軟體的流行程度 (圖 4)。

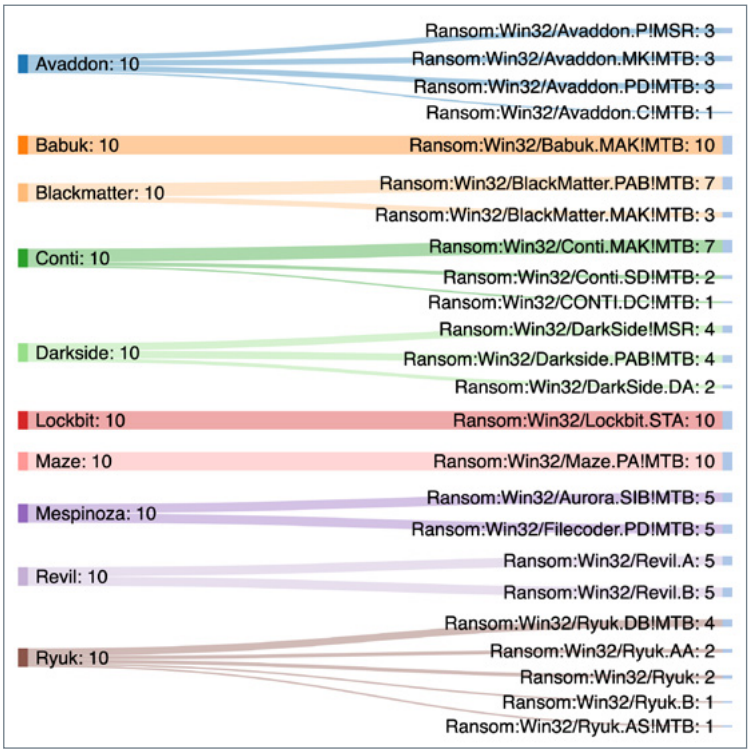


圖 4。我們選擇了 10 個勒索軟體種類及其各自的病毒檔案進行研究。

每種軟體中測試各個二進位檔案的 VirusTotal 偵測字串和 SHA256 雜湊可以在附錄 C 中找到。

結果

針對我們原先提出的勒索軟體加密速度有多快的問題，答案顯示勒索軟體種類間存在很大的差異。我們想瞭解每個樣本的加密速度和持續時間，以及各種類本身的速度和持續時間中位數。使用中位數值而非平均值可以防止少數異常值與特定種類的整體結果產生誤差。

在測試期間收集 Windows Perfmon 資料時，我們觀察到一些軟體種類比其他種類更會利用增加的系統資源。某些種類非常有效率，其他則傾向於利用高比例的 CPU 時間和極高的硬碟存取率。使用大量系統資源樣本與更快的加密速度之間並沒有直接關聯。 當部署在更快的測試系統上時，某些勒索軟體種類表現更差，甚至毀損。

在各樣本基礎上，觀察 98,561 個測試檔案時，加密最快的時間是 4 分 9 秒。這是在 Windows 2019 Server 高規格執行個體上執行 lockbit-9.exe (133adb408a4837d3a20634d79baf01151061c49cd936e9a8787b91df8997b6b0) 的結果 (圖 5)。

Variant	Endpoint	process_name	Duration	Encryptions_Per_Second
Lockbit	Server-2019-High	C:\ransom\lockbit-9.exe	00:04:09	396

圖 5。資料來自部署在 Windows 2019 伺服器上的 lockbit-9.exe 樣本。

相反的，同樣的測試檔案，觀察到的最慢加密時間是 3 小時 35 分 8秒。這是在 Windows 10 中等規格執行個體上執行 babuk-5.exe (1b9412ca5e9deb29aeaa37be05ae8d0a8a636c12fdff8c17032aa017f6075c02) 的結果 (圖 6)。

Variant	Endpoint	process_name	Duration	Encryptions_Per_Second
Babuk	Win-10-Mid	C:\ransom\babuk-5.exe	03:35:08	8

圖 6。資料來自部署在 Windows 10 執行個體上的 babuk-5.exe 樣本。

當我們查看每個測試種類的加密持續時間中位數時，我們發現雖然單個 Babuk 樣本是加密最慢的勒索軟體，但整體 Babuk 種類是第二快的，持續時間為 6 分 34 秒。LockBit 5 分 50 秒在整體中仍然是最快的。每種類最慢加密時間的中位數是 Mespinoza (PYSA)，持續時間中位數為 1 小時 54 分 54 秒。總體而言，所有勒索軟體種類的加密持續時間中位數為 42 分 52 秒 (圖 7)。

種類	持續時間中位數
LockBit	00:05:50
Babuk	00:06:34
Avaddon	00:13:15
Ryuk	00:14:30
Revil	00:24:16
BlackMatter	00:43:03
Darkside	00:44:52
Conti	00:59:34
Maze	01:54:33
Mespinoza (PYSA)	01:54:54
中位數平均值	**00:42:52**

圖 7。10 個勒索軟體種類的加密持續時間中位數。

持續時間中位數顯示出，一旦加密過程開始，要回應軟體攻擊的時機變得很有限。考量到災難性的高峰可能會是單一的關鍵檔案受到加密，而不是受害者的全部資料，這證明了反應時間更加有限。由於這些因素，一旦加密過程開始，大多數組織非常難減輕勒索軟體的攻擊。雖然偵測和防禦能力超出了本研究的範圍，但對於那些尋求辦法保護自己免受勒索軟體攻擊的人來說，還是有希望的。

我們注意並確保我們擷取資料的方法不會影響資料的結果。但是，我們無法衡量這些工具 (例如 Sysmon 和受限的 Object Level Auditing) 可能引入的延遲。我們相信這些工具不會導致任何顯著的延遲，從而大大地改變我們的研究結果。未來專研勒索軟體加密速度，希望會有方法可以測量工具所引入的延遲。最後，我們意識到很難將勒索軟體樣本歸類為「種類」。為了確保本研究的樣本選擇偏差一致，我們將每個樣本的雜湊與 VirusTotal 中獲得的 Microsoft Defender 結果進行了比較。擷取簽名，並標準化。然後，我們使用產生的標準值來識別特定的勒索軟體種類。

結論與未來建議發展

本研究的目的是實證上評估常見勒索軟體的種類在各種操作系統和硬體規格中的加密速度，以判斷組織實際上是否能及時做出反應並有效地緩解。根據我們的中位數結果，調查顯示，勒索軟體加密會導致資料在 43 分鐘內完全遺失。資料的加密和遺失是前面 Lockheed Martin Cyber Kill Chain 中提到的「目標行動」。正如 Mandiant M-Trends 報告的發現，43 分鐘使化解危機的時機相當有限，特別是考慮到平均偵測入侵的時間是三天。因此，我們推測許多組織不太可能防止勒索軟體所害的資料完全遺失。如果組織希望防禦勒索軟體，很明顯他們需要在網路攻擊狙殺鏈上向左移動，並在遞送或利用時進行偵測，而不是針對目標採取行動。我們希望這項研究的結果可以幫助網路防禦人員進一步探索和識別可能的緩解機會。也該注意的是，儘管我們將實驗室設定使用勒索軟體樣本來檢測蠕蟲行為，但大多數樣本並沒有出現這種行為。未來的研究將更深入探討蠕蟲的行為。

我們的研究並不止於這項工作。我們計劃在 Splunk BOSS 平台上發布此語料庫，以協助其他值得探索的研究領域。更具體而言，我們希望評估勒索軟體在加密檔案時表現出的模式、勒索軟體蠕蟲行為、如何根據模糊雜湊算法對相似的勒索軟體二進位檔案進行叢集，以及未來對勒索軟體種類屬性的分析。

感謝

像這樣的研究需要眾多調查人員才能完成。特別感謝 Allie Mellen、Mark Harris、David French、Ryan Kovar、Audra Streetman、Marcus LaFerrera、Mick Baccio、Dave Herrald、Drew Church、Johan Bjerke、John Stoner、Tamara Chacon、Kelcie Bourne、Scott Roberts、Adam Swanda、Michael Haag 和 Splunk Threat Research Team (STRT) 的 Splunk Attack Range 創辦者。

參考書目

- SDxCentral.“Case Study:AIDS Trojan Ransomware.” 引用時間 2022 年 2 月 23 日 https://www.sdxcentral.com/security/definitions/case-study-aids-trojan-ransomware/。
- “Dell Latitude 7420 Review | PCMag.” 引用時間 2022 年 1 月 30 日 https://www.pcmag.com/reviews/dell-latitude-7420。
- “Digital Corpora Downloads:Corpora/Files/Govdocs1/By_type/.” 引用時間 2022 年 1 月 30 日 https://downloads.digitalcorpora.org/corpora/files/govdocs1/by_type/。
- “Digital Corpora Downloads:Corpora/Files/Govdocs1/Zipfiles/.” 引用時間 2022 年 1 月 30 日 https://downloads.digitalcorpora.org/corpora/files/govdocs1/zipfiles/。
- FireEye, and Mandiant.“Fireeye-Rpt-Mtrends-2021.Pdf,” April 13, 2021.https://www.mandiant.com/resources/m-trends-2021。
- Garfinkel, Simson, Paul Farrell, Vassil Roussev, and George Dinolt.“Bringing Science to Digital Forensics with Standardized Forensic Corpora.” Digital Investigation 6 (September 2009):S2–11. https://doi.org/10.1016/j.diin.2009.06.016.
- CERT NZ.“How Ransomware Happens and How to Stop It.” 引用時間 2022 年 1 月 29 日 https://www.cert.govt.nz/it-specialists/guides/how-ransomware-happens-and-how-to-stop-it/。
- LLC, Gridinsoft.“LockBit Ransomware.The Most Honest and the Fastest.” Gridinsoft LLC.引用時間 2022 年 1 月 29 日 https://gridinsoft.com。
- “LockBit BLOG.” 引用時間 2022 年 2 月 13 日 http://lockbitapt6vx57t3eeqjofwgcglmutr3a35nygvokja5uuccip4ykyd.onion[.]ly/conditions。
- markruss.“Sysmon - Windows Sysinternals.” 引用時間 2022 年 2 月 25 日 https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon。
- McHale, John.“Defending DoD from Cyberattacks, Getting to the Left of the Boom - Military Embedded Systems.” 引用時間 2022 年 1 月 30 日 http://militaryembedded.com/cyber/cybersecurity/defending-dod-from-cyberattacks-getting-to-the-left-of-the-boom。
- Microsoft.“4663(S) An Attempt Was Made to Access an Object.(Windows 10) - Windows Security.” 引用時間 2022 年 1 月 30 日 https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4663。
- Microsoft Security Intelligence.“Trojan:PowerShell/Redearps.A Threat Description,” March 24, 2021. https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Trojan:PowerShell/Redearps.A&threatId=-2147189091.
- Splunk Attack Range.Jinja.2019.Reprint, Splunk GitHub, 2022. https://github.com/splunk/attack_range.
- Symantec.“THE INCREASED USE OF POWERSHELL IN ATTACKS.” Symantec Corporation, 2016. https://docs.broadcom.com/doc/increased-use-of-powershell-in-attacks-16-en.
- Verizon.“DBIR 2021 Data Breach Investigations Report,” May 12, 2021. verizon.com/dbir.

附錄 A：Windows 記錄設定

- 在 C:\Files\ 和所有子目錄 (目錄 0-99) 上啟用 Windows 檔案系統稽核 (事件代碼 4633)。失敗與成功的修改檔案嘗試都啟用此功能。
- Windows 啟用命令列記錄來建立處理程序 (事件代碼 4688)
- Sysmon 安裝並設定了來自 Olaf Hartong 的詳細設定

附錄 B：主機規格

- Win-10-High- Windows 10, AWS m5.2xlarge (8 CPU/32GB RAM) 300GB HDD (3000 IOPS/125MBs 輸送量)
- Win-10-Mid- Windows 10, AWS m5.xlarge (4 CPU/16GB RAM) 300GB HDD (3000 IOPS/125MBs 輸送量)
- Server-2019-High- Windows Server 2019, AWS m5.4xlarge (16 CPU/64GB RAM) 300GB HDD (10000 IOPS/500MBs 輸送量)
- Server-2019-Mid- Windows Server 2019, AWS m5.2xlarge (8 CPU/32GB RAM) 300GB HDD (3000 IOPS/125MBs 輸送量)

附錄 C：勒索軟體種類和二進位檔案

二進位檔案	SHA256 雜湊	VirusTotal 廠商	VirusTotal 偵測
avaddon-0.exe	078de7d019f5f1e546aa29af7123643bd250341af71506e6256dfee8f245a2a7	microsoft	Ransom:Win32/Avaddon.P!MSR
avaddon-1.exe	18c1ad49bf46b44df5926851ca30f00f6675c535b6826a3c779099643327ea33	microsoft	Ransom:Win32/Avaddon.P!MSR
avaddon-2.exe	288165763637cda27304d90bb7ec47e103dfb69fdf6c009d113b1f6852c091a0	microsoft	Ransom:Win32/Avaddon.MK!MTB
avaddon-3.exe	3a040105b3cb704c838a87061dba6b03712d308636a438004300ec154de2d4d6	microsoft	Ransom:Win32/Avaddon.PD!MTB
avaddon-4.exe	4adc6cac6071cd67773c9cefab479f0ffde370c4cedac31b6db4de065c3ec7af	microsoft	Ransom:Win32/Avaddon.PD!MTB
avaddon-5.exe	572610a5033a2060afa67ddbfd7345013e82c6904dd7ace22cb6f0b0bedcb550	microsoft	Ransom:Win32/Avaddon.MK!MTB
avaddon-6.exe	743079700007b64647d9ea4a0c361e6e981518ed06a5902ab9f275c38aa45c7b	microsoft	Ransom:Win32/Avaddon.MK!MTB
avaddon-7.exe	b9e62cb99e71c856cc41edfd837689993b7fc63c780e5786c34b2a8f63ef37b6	microsoft	Ransom:Win32/Avaddon.P!MSR
avaddon-8.exe	cc95a8d100f70d0fbf4af14e852aa108bdb0e36db4054c3f60b3515818a71f46	microsoft	Ransom:Win32/Avaddon.C!MTB
avaddon-9.exe	d8acd139f4f99b3137ab4cea9ef9e515e3a560f25a79666ac302f21d468340f8	microsoft	Ransom:Win32/Avaddon.PD!MTB
babuk-0.exe	04126b30c1c2663cdf2b6386781aedbfce2ef418a0b01de510bd536903f577e3	microsoft	Ransom:Win32/Babuk.MAK!MTB
babuk-1.exe	049e53f72c8afa5ccb850429d55a00e2fbe799e68247fd13f5058146cf0f4cf8	microsoft	Ransom:Win32/Babuk.MAK!MTB
babuk-2.exe	106118444e0a7405c13531f8cd70191f36356581d58789dfc5df3da7ba0f9223	microsoft	Ransom:Win32/Babuk.MAK!MTB
babuk-3.exe	12c561ac827c3f79afff026b0b1d3ddec7c4b591946e2b794a4d00c423b1c8f8	microsoft	Ransom:Win32/Babuk.MAK!MTB
babuk-4.exe	1b04e1fbddfcdb16a3d103e50261937815668d92d4909a15352dd5e2615adbf4	microsoft	Ransom:Win32/Babuk.MAK!MTB
babuk-5.exe	1b9412ca5e9deb29aeaa37be05ae8d0a8a636c12fdff8c17032aa017f6075c02	microsoft	Ransom:Win32/Babuk.MAK!MTB

二進位檔案	SHA256 雜湊	VirusTotal 廠商	VirusTotal 偵測
babuk-6.exe	1f37064ff61211d7a0d0428af856323bafb734b3f8b0e44d04e8e0db872349ee	microsoft	Ransom:Win32/Babuk.MAK!MTB
babuk-7.exe	245e191bfe998ad9ef2d6b169af22f3c290e9950234f8ddd0f4a03cb3eebf761	microsoft	Ransom:Win32/Babuk.MAK!MTB
babuk-8.exe	2509e5a4535d25110663a698410847aa0cb9ce734722076ada4c651532f318a5	microsoft	Ransom:Win32/Babuk.MAK!MTB
babuk-9.exe	25835a890a218fd26bfd8b23696576402b5eb8a4c9af4a51529e14c4f00a9cce	microsoft	Ransom:Win32/Babuk.MAK!MTB
blackmatter-0.exe	8eada5114fbbc73b7d648b38623fc206367c94c0e76cb3b395a33ea8859d2952	microsoft	Ransom:Win32/BlackMatter.PAB!MTB
blackmatter-1.exe	26a7146fbed74a17e9f2f18145063de07cc103ce53c75c8d79bbc5560235c345	microsoft	Ransom:Win32/BlackMatter.PAB!MTB
blackmatter-2.exe	2aad85dbd4c79bd21c6218892552d5c9fb216293a251559ba59d45d56a01437c	microsoft	Ransom:Win32/BlackMatter.PAB!MTB
blackmatter-3.exe	496cd9b6b6b96d6e781ab011d1d02ac3fc3532c8bdd07cae5d43286da6e4838d	microsoft	Ransom:Win32/BlackMatter.MAK!MTB
blackmatter-4.exe	b4b9fdf30c017af1a8a3375218e43073117690a71c3f00ac5f6361993471e5e7	microsoft	Ransom:Win32/BlackMatter.MAK!MTB
blackmatter-5.exe	6d4712df42ad0982041ef0e2e109ab5718b43830f2966bd9207a7fac3af883db	microsoft	Ransom:Win32/BlackMatter.MAK!MTB
blackmatter-6.exe	be5bc29f58b868f4ff8cd66b4526535593e515a697bb8951c625bdfed13cccb7	microsoft	Ransom:Win32/BlackMatter.PAB!MTB
blackmatter-7.exe	ed47e6ecca056bba20f2b299b9df1022caf2f3e7af1f526c1fe3b8bf2d6e7404	microsoft	Ransom:Win32/BlackMatter.PAB!MTB
blackmatter-8.exe	7a223a0aa0f88e84a68da6cde7f7f5c3bb2890049b0bf3269230d87d2b027296	microsoft	Ransom:Win32/BlackMatter.PAB!MTB
blackmatter-9.exe	9bae897c19f237c22b6bdc024df27455e739be24bed07ef0d409f2df87eeda58	microsoft	Ransom:Win32/BlackMatter.PAB!MTB
conti-0.exe	004ede55a972e10d9a21bcf338b4907d6eed65bf5ad6abbbd5aec7d8484bdedf	microsoft	Ransom:Win32/Conti.SD!MTB
conti-1.exe	17ac91a36237d8f37dcee961ba74c9310a45c009780ea092c3a1e428870ff8a1	microsoft	Ransom:Win32/Conti.MAK!MTB
conti-2.exe	34366c9a9ac34dd9016abd406cffe713a3e8606e8600e6cb07e0242904f91a5b	microsoft	Ransom:Win32/Conti.MAK!MTB
conti-3.exe	49dc5a243d322cd4d467e5f24b61ff749869564ddcf6a2f700839cf5ae9e37ea	microsoft	Ransom:Win32/Conti.MAK!MTB
conti-4.exe	0b0b902af452e1c949a609a3b29a9de21dac639846c77427de06e6e63c1fe904	microsoft	Ransom:Win32/Conti.MAK!MTB
conti-5.exe	73bd8c2aa71f5dcd9d2ddd79e53656c6ae3db2535e08cf9dab1cd13bdd6d5ea3	microsoft	Ransom:Win32/CONTI.DC!MTB
conti-6.exe	8df9b346bf591629a9eb0bf9f32c545a1266873495ceec9ba990be1dd22b9aa9	microsoft	Ransom:Win32/Conti.MAK!MTB
conti-7.exe	0ffbc914e3bb09df586a93e5a5a557d03c5fcce7e8ee4a36bd3a09b8ed429c7a	microsoft	Ransom:Win32/Conti.SD!MTB
conti-8.exe	d43b52e3453ce77d2694a239232f39341a98fa704954a558125e74a85f22a346	microsoft	Ransom:Win32/Conti.MAK!MTB
conti-9.exe	1201e76d42f85feb89d64e6fd497144ed3afe66281b2464e84f3b889f2867c9b	microsoft	Ransom:Win32/Conti.MAK!MTB
darkside-0.exe	22d7d67c3af10b1a37f277ebabe2d1eb4fd25afbd6437d4377400e148bcc08d6	microsoft	Ransom:Win32/DarkSide!MSR
darkside-1.exe	2c323453e959257c7aa86dc180bb3aaaa5c5ec06fa4e72b632d9e4b817052009	microsoft	Ransom:Win32/Darkside.PAB!MTB
darkside-2.exe	45ecce9dfec886e2b092a996f6affb9e7417d6121e58b0ec643be7e36a03106d	microsoft	Ransom:Win32/Darkside.PAB!MTB
darkside-3.exe	7f6dd0ca03f04b64024e86a72a6d7cfab6abccc2173b85896fc4b431990a5984	microsoft	Ransom:Win32/DarkSide!MSR

二進位檔案	SHA256 雜湊	VirusTotal 廠商	VirusTotal 偵測
darkside-4.exe	84af3f15701d259f3729d83beb15ca738028432c261353d1f9242469d791714f	microsoft	Ransom:Win32/Darkside.PAB!MTB
darkside-5.exe	c6e2ef30a86baa670590bd21acf5b91822117e0cbe6060060bc5fe0182dace99	microsoft	Ransom:Win32/Darkside.PAB!MTB
darkside-6.exe	2c1e20a4b38634b97de398246bc3c8082d47663702a46bb885dc7fcc5f71daa1	microsoft	Ransom:Win32/DarkSide!MSR
darkside-7.exe	43e61519be440115eeaa3738a0e4aa4bb3c8ac5f9bdfce1a896db17a374eb8aa	microsoft	Ransom:Win32/DarkSide!MSR
darkside-8.exe	533672da9d276012ebab3ce9f4cd09a7f537f65c6e4b63d43f0c1697e2f5e48d	microsoft	Ransom:Win32/DarkSide.DA
darkside-9.exe	5da3e6b4bea1eaceddb048a4a6bd702291189f42d15c4b2670de78984329b0a9	microsoft	Ransom:Win32/DarkSide.DA
lockbit-0.exe	00ad914476509f84b40f2dbe804dc7c37a1a24ef3472674574d3367079bf0a2a	microsoft	Ransom:Win32/Lockbit.STA
lockbit-1.exe	04f65270c92dda82c759c1eee49cf8f4c98a2ed0071272e49132331fda482dba	microsoft	Ransom:Win32/Lockbit.STA
lockbit-2.exe	082f91d85c437f415cea44b36afb4198da07b78593c836a398cd96365166e7d8	microsoft	Ransom:Win32/Lockbit.STA
lockbit-3.exe	50d08c974f7abce2da5c2a8976d3c6017334a418359d7bb031bd0914b848b24a	microsoft	Ransom:Win32/Lockbit.STA
lockbit-4.exe	0cd33e6b180862072a00a0c2f897afa754df071bcec3d13e581c41a5c27a3102	microsoft	Ransom:Win32/Lockbit.STA
lockbit-5.exe	7a1fb0eac9b62ce510030f9ff983d9d6225fd8dad6f05c1051c335aca87ffa24	microsoft	Ransom:Win32/Lockbit.STA
lockbit-6.exe	0d4966b4724f141adb7a7db1d9ae48f5c293c6049cc7f949220256c2e72ab5ac	microsoft	Ransom:Win32/Lockbit.STA
lockbit-7.exe	bb736c8d3dd2b3ebcacd3e2a61f95b20d23bc981cc22888dff88cfd2e720ee99	microsoft	Ransom:Win32/Lockbit.STA
lockbit-8.exe	d68cad561a949648a84ffc2f2db186f585cd4a90951eea91c1c100d996cb3688	microsoft	Ransom:Win32/Lockbit.STA
lockbit-9.exe	133adb408a4837d3a20634d79baf01151061c49cd936e9a8787b91df8997b6b0	microsoft	Ransom:Win32/Lockbit.STA
maze-0.exe	f03172bd32ed16df6dda8e8146d24b073b864da59d669218fcc5e97835a5e956	microsoft	Ransom:Win32/Maze.PA!MTB
maze-0.exe	f03172bd32ed16df6dda8e8146d24b073b864da59d669218fcc5e97835a5e956	microsoft	Ransom:Win32/Maze.PA!MTB
maze-1.exe	0b9c99276ed36110afc58b3fb59ada135146180189c25d99618ca5897537ee21	microsoft	Ransom:Win32/Maze.PA!MTB
maze-2.exe	2a6c602769ac15bd837f9ff390acc443d023ee62f76e1be8236dd2dd957eef3d	microsoft	Ransom:Win32/Maze.PA!MTB
maze-3.exe	b3473d205ba722e229f49002093b61fc35902e1a67bcd558bf9a7811278e5cb2	microsoft	Ransom:Win32/Maze.PA!MTB
maze-4.exe	5a06ae8540d5a0d7fb88e80d3e61c3a6079f3abdafe998ce70ffdcac9e940520	microsoft	Ransom:Win32/Maze.PA!MTB
maze-5.exe	877c439da147bab8e2c32f03814e3973c22cbcd112d35bc2735b803ac9113da1	microsoft	Ransom:Win32/Maze.PA!MTB
maze-6.exe	9d86beb9d4b07dec9db6a692362ac3fce2275065194a3bda739fe1d1f4d9afc7	microsoft	Ransom:Win32/Maze.PA!MTB
maze-8.exe	e45eacf5158bb2aa11f29f0675b4cb68dbf7e376569516fe33f84be524c67763	microsoft	Ransom:Win32/Maze.PA!MTB
maze-9.exe	ecd04ebbb3df053ce4efa2b73912fd4d086d1720f9b410235ee9c1e529ea52a2	microsoft	Ransom:Win32/Maze.PA!MTB
mespinoza-0.exe	0433efd9ba06378eb6eae864c85aafc8b6de79ef6512345294e9e379cc054c3d	microsoft	Ransom:Win32/Aurora.SIB!MTB
mespinoza-1.exe	0f0014669bc10a7d87472cafc05301c66516857607b920ddeb3039f4cb8f0a50	microsoft	Ransom:Win32/Filecoder.PD!MTB

二進位檔案	SHA256 雜湊	VirusTotal 廠商	VirusTotal 偵測
mespinoza-2.exe	164cb8e82d7e07cca0409925cadd8be5e3e8e07db88526ff7fe87596c6a6bd07	microsoft	Ransom:Win32/Aurora.SIB!MTB
mespinoza-3.exe	4dc802894c45ec4d119d002a7569be6c99a9bba732d0057364da9350f9d3659b	microsoft	Ransom:Win32/Aurora.SIB!MTB
mespinoza-4.exe	1e2009549452ed6b524b94ed683079ee60c2b9542b1bfd5b9ee42e9161d5e7c8	microsoft	Ransom:Win32/Filecoder.PD!MTB
mespinoza-5.exe	327934c4c11ba37f42a91e1b7b956d5a4511f918e63047a8c4aa081fd39de6d9	microsoft	Ransom:Win32/Aurora.SIB!MTB
mespinoza-6.exe	425945a93beb160f101d51de36363d1e7ebc45279987c3eaf5e7f183ed0a3776	microsoft	Ransom:Win32/Filecoder.PD!MTB
mespinoza-7.exe	44f1def68aef34687bfacf3668e56873f9d603fc6741d5da1209cc55bdc6f1f9	microsoft	Ransom:Win32/Aurora.SIB!MTB
mespinoza-8.exe	4770a0447ebc83a36e590da8d01ff4a418d58221c1f44d21f433aaf18fad5a99	microsoft	Ransom:Win32/Filecoder.PD!MTB
mespinoza-9.exe	48355bd2a57d92e017bdada911a4b31aa7225c0b12231c9cbda6717616abaea3	microsoft	Ransom:Win32/Filecoder.PD!MTB
revil-0.exe	d74cd044351030290f6ad8f70f91d51b6c39675ca3c70c45b5b0c5bd09589ff6	microsoft	Ransom:Win32/Revil.A
revil-1.exe	338e8f24eeb38b5ef67ef662b65d592c816eba94dfaaac856021dac407daf294	microsoft	Ransom:Win32/Revil.A
revil-2.exe	ab53e6823e47b446a245374c7760006ee84c8ea457a5fe9ca9df4732bf55a32a	microsoft	Ransom:Win32/Revil.A
revil-3.exe	73dd3cb487dfb863304d9f6d79f60b2ab4adbd162e460a2210b4a6abf049ea53	microsoft	Ransom:Win32/Revil.B
revil-4.exe	151271bf05310f94cd33cba3eb90be264edc4828c04e4e82f492b8e2576ee7a6	microsoft	Ransom:Win32/Revil.B
revil-5.exe	97f905bb24c5054d09fe79a20e04fe84042ad985b5c6e09afad21efa83dcd7a0	microsoft	Ransom:Win32/Revil.A
revil-6.exe	19f1a30555b83f23acc245ef6fe745f3292ef015c71abef8daa077e31f259179	microsoft	Ransom:Win32/Revil.B
revil-7.exe	1f7b15f6cf07c5943ce8ab5bfd0700e4919808fca4260ffd2a509100d45fadaf	microsoft	Ransom:Win32/Revil.B
revil-8.exe	1fb842e87f23e37ab39e201a024845c323c3d239331768db694dca96ed53d8c7	microsoft	Ransom:Win32/Revil.B
revil-9.exe	21bcb9c0095424a179399379939f6ebdf1dfe202825c1ca5acdd25a8f751402f	microsoft	Ransom:Win32/Revil.A
ryuk-0.exe	487d4698c6c938ca3e9251827a5813ddd21e26584b3459d768e457ddd4e8c4d4	microsoft	Ransom:Win32/Ryuk.DB!MTB
ryuk-1.exe	4cb0bf61d61ad3383636df11b3e4da8e67bb0acea03e981ecdd48d08ed8c796c	microsoft	Ransom:Win32/Ryuk.AA
ryuk-2.exe	dea1b54618643ffe59506398f0f131300abe0988da89b5414955843ae5b53fee	microsoft	Ransom:Win32/Ryuk.DB!MTB
ryuk-3.exe	0cf36731f5b8651d53fc651607c3fccac24b631c08dca4493d8e07d2fbff1db3	microsoft	Ransom:Win32/Ryuk.AA
ryuk-4.exe	8027a5e9dfcb379592868fb61fd8ed5f1605f0e4460db53d23a859d2a9743b91	microsoft	Ransom:Win32/Ryuk.DB!MTB
ryuk-5.exe	d4b8cbfa94bac3dbd58452fcc6c4e0b56b65a54a671a2184d9fb6e3694a0266f	microsoft	Ransom:Win32/Ryuk.DB!MTB
ryuk-6.exe	ba595e53ea6b0ef7f3332c2fec6a644c3cbc9756d2978c49e69eba92526904d8	microsoft	Ransom:Win32/Ryuk.B
ryuk-7.exe	fc4d44faf906e7a6ba133dae5f33ce22b8569943574ffccadd0292b12abcc8fa	microsoft	Ransom:Win32/Ryuk.AS!MTB
ryuk-8.exe	fe55650d8b1b78d5cdb4ad94c0d7ba7052351630be9e8c273cc135ad3fa81a75	microsoft	Ransom:Win32/Ryuk
ryuk-9.exe	568d73074880063d4d2b3e9d3ddb938685de8ec8e24974ff32f5f47d55a2dcb0	microsoft	Ransom:Win32/Ryuk

附錄 D：加密檔案類型語料庫

副檔名	數量	總大小 (MB)
html	25364	1,589.66
pdf	25185	15,116.11
txt	14856	12,632.61
doc	7955	5,019.95
jpg	7095	1,020.12
ppt	5576	11,044.64
xls	4238	4,384.81
gif	2010	114.83
ps	1186	2,024.57
csv	1005	224.24
xml	918	137.19
gz	794	435.43
log	514	622.12
unk	433	63.2
PNG	317	19.12
text	184	136.18
dbase3	170	3.03
f	129	14.11
rtf	128	31.35
eps	67	14.23
pps	65	164.05
swf	43	20.41
wp	42	4.2
fits	39	58.58
tex	36	2.25

副檔名	數量	總大小 (MB)
java	36	1.24
kml	32	4.03
kmz	28	2
pptx	21	75.78
troff	21	1.9
bmp	13	5.23
docx	13	0.85
sgml	9	0.22
sql	7	0.46
hlp	7	0.02
dwf	5	0.56
gls	5	0.02
tmp	4	0.9
資料	2	0.77
沒有副檔名的檔案名稱。	1	124.94
zip	1	0.84
vrml	1	0.32
wk1	1	0.31
py	1	0.23
ttf	1	0.12
g3	1	0.12
xlsx	1	0.05
pub	1	0.000049
	98,561 個檔案	**總計 53.83 GB**

附錄 E：端點效能發現

Windows Server 2019 高規格

Endpoint Specifications

Endpoint	OS	CPU Cores	GB RAM	Disk IOPS	Disk Throughput MB/s
Win-10-Mid	Windows 10	4	16	3000	125
Win-10-High	Windows 10	8	32	3000	125
Server-2019-Mid	Windows Server 2019	8	32	3000	125
Server-2019-High	Windows Server 2019	16	64	10000	500

Median Resource Utilization

Variant	Endpoint	%_Privileged_Time	%_Processor_Time	%_User_Time	Handle_Count	Thread_Count	Priority	Page_Faults/sec	IO_Read_KBytes/sec	IO_Write_KBytes/sec	Private_MBytes	Virtual_MBytes	Working_Set(MBytes)
Avaddon	Server-2019-High	95.52	96.18	61.64	628.67	67.62	8	167890.42	54246.70	55118.46	17.28	227.62	26.13
Babuk	Server-2019-High	34.82	99.74	99.36	452.19	67.89	8	3853.88	28099.74	26860.70	25.72	178.65	19.27
Blackmatter	Server-2019-High	8.25	11.90	5.47	313.81	35.74	10	1962.33	10263.18	10283.99	12.70	117.03	16.99
Conti	Server-2019-High	6.88	12.97	8.59	257.58	18.58	8	343.72	11532.70	11492.30	164.83	237.50	17.46
Darkside	Server-2019-High	6.94	21.29	16.21	311.21	35.54	10	1670.40	8721.45	8731.53	12.00	113.81	16.41
Lockbit	Server-2019-High	27.02	41.55	15.94	502.12	28.07	8	1531.18	1237.26	1399.21	7.79	110.66	19.06
Maze	Server-2019-High	4.29	5.88	4.40	365.64	3.38	8	2086.59	13216.13	4831.49	4.19	86.45	16.28
Mespinoza	Server-2019-High	5.76	7.54	4.97	153.03	2.03	8	64.42	8191.90	6142.31	3.48	47.67	8.07
Revil	Server-2019-High	7.06	18.38	13.29	243.36	35.16	8	2425.00	14108.76	14068.99	11.61	105.26	15.01
Ryuk	Server-2019-High	53.31	86.33	20.02	171279.74	53.82	8	2931.32	62045.03	82201.84	181.45	296.14	102.16

Median Encryption Speeds

Variant	Endpoint	Total_Encryptions	Duration_In_Minutes	Encryptions_Per_Minute	Encryption_Speed_MB_Per_Second
Avaddon	Server-2019-High	43868	7.58	5787.00	53.9
Babuk	Server-2019-High	98560	5.55	17760.00	166
Blackmatter	Server-2019-High	98553	37.41	2635	24.55
Conti	Server-2019-High	98560	64.07	1538	14.34
Darkside	Server-2019-High	98553	43.60	2260	21.07
Lockbit	Server-2019-High	98548	5.30	18622	173
Maze	Server-2019-High	98560	86.53	1139	10.62
Mespinoza	Server-2019-High	97080	102.55	946.70	8.824
Revil	Server-2019-High	98553	27.25	3618	33.71
Ryuk	Server-2019-High	89521	8.92	9266	93.6

Windows Server 2019 中規格

Endpoint Specifications

Endpoint	OS	CPU Cores	GB RAM	Disk IOPS	Disk Throughput MB/s
Win-10-Mid	Windows 10	4	16	3000	125
Win-10-High	Windows 10	8	32	3000	125
Server-2019-Mid	Windows Server 2019	8	32	3000	125
Server-2019-High	Windows Server 2019	16	64	10000	500

Median Resource Utilization

Variant	Endpoint	%_Privileged_Time	%_Processor_Time	%_User_Time	Handle_Count	Thread_Count	Priority	Page_Faults/sec	IO_Read_KBytes/sec	IO_Write_KBytes/sec	Private_MBytes	Virtual_MBytes	Working_Set(MBytes)
Avaddon	Server-2019-Mid	95.42	97.16	51.46	467.96	35.69	8	166866.12	44362.49	45706.62	14.84	140.11	23.97
Babuk	Server-2019-Mid	29.07	160.58	147.78	380.75	36.21	8	2985.14	21796.16	20907.03	17.95	133.61	16.87
Blackmatter	Server-2019-Mid	7.40	9.33	4.55	313.49	19.62	10	1688.89	8863.80	8850.98	11.45	95.38	16.49
Conti	Server-2019-Mid	7.10	12.33	7.93	241.00	10.41	8	117.35	10851.88	10881.95	83.15	145.91	16.57
Darkside	Server-2019-Mid	6.23	18.67	14.12	332.28	19.48	10	1495.22	7732.50	7725.44	10.86	95.34	16.22
Lockbit	Server-2019-Mid	22.40	33.26	13.45	458.79	18.10	8	1205.07	975.23	1092.23	7.02	96.55	18.76
Maze	Server-2019-Mid	4.02	4.94	3.95	333.54	4.46	8	1572.07	10751.79	3887.37	3.46	68.76	13.73
Mespinoza	Server-2019-Mid	5.39	6.70	4.65	153.03	2.02	8	80.30	6782.18	5023.70	3.55	47.27	8.11
Revil	Server-2019-Mid	6.62	17.54	12.86	254.25	19.30	8	2147.04	12687.87	12605.01	11.11	86.37	15.27
Ryuk	Server-2019-Mid	41.19	59.49	14.45	218856.14	53.61	8	1965.13	38545.07	56935.97	182.73	300.70	102.88

Median Encryption Speeds

Variant	Endpoint	Total_Encryptions	Duration_In_Minutes	Encryptions_Per_Minute	Encryption_Speed_MB_Per_Second
Avaddon	Server-2019-Mid	50307	8.75	5749.00	53.6
Babuk	Server-2019-Mid	98560	6.51	15140.00	141
Blackmatter	Server-2019-Mid	98553	43.18	2283	21.27
Conti	Server-2019-Mid	98560	67.60	1458	13.59
Darkside	Server-2019-Mid	98553	50.47	1953	18.20
Lockbit	Server-2019-Mid	98548	6.76	14594	136
Maze	Server-2019-Mid	98560	114.75	858.94	8.006
Mespinoza	Server-2019-Mid	97080	124.55	779.48	7.265
Revil	Server-2019-Mid	98553	29.56	3336	31.07
Ryuk	Server-2019-Mid	93014	12.67	7289	68.4

Windows 10 高規格

Endpoint Specifications

Endpoint	OS	CPU Cores	GB RAM	Disk IOPS	Disk Throughput MB/s
Win-10-Mid	Windows 10	4	16	3000	125
Win-10-High	Windows 10	8	32	3000	125
Server-2019-Mid	Windows Server 2019	8	32	3000	125
Server-2019-High	Windows Server 2019	16	64	10000	500

Median Resource Utilization

Variant	Endpoint	%_Privileged_Time	%_Processor_Time	%_User_Time	Handle_Count	Thread_Count	Priority	Page_Faults/sec	IO_Read_KBytes/sec	IO_Write_KBytes/sec	Private_MBytes	Virtual_MBytes	Working_Set(MBytes)
Avaddon	Win-10-High	68.96	77.37	31.62	457.12	37.10	8	88500.41	28297.32	28647.71	15.05	168.35	23.63
Babuk	Win-10-High	38.54	94.00	93.48	376.90	37.86	8	3189.90	21838.42	21783.18	19.83	151.92	17.53
Blackmatter	Win-10-High	6.74	8.91	4.58	299.34	21.56	10	1598.82	8358.30	8351.87	10.45	108.34	15.39
Conti	Win-10-High	7.95	15.24	9.83	228.03	11.32	8	261.15	12402.19	12389.49	83.23	167.86	15.25
Darkside	Win-10-High	6.90	20.24	15.05	393.16	23.78	10	1665.17	8488.67	8470.35	10.75	114.21	17.02
Lockbit	Win-10-High	28.78	44.13	17.42	498.25	24.38	8	1440.13	1251.17	1417.23	9.20	119.75	20.38
Maze	Win-10-High	4.10	5.00	3.91	323.62	5.11	8	1564.34	10369.55	3806.94	3.70	85.59	14.08
Mespinoza	Win-10-High	6.23	7.29	4.68	144.07	2.24	8	147.27	7219.82	5397.70	3.58	61.30	8.30
Revil	Win-10-High	8.09	21.70	15.75	252.97	19.27	8	2732.09	17054.07	16986.81	10.48	100.22	14.25
Ryuk	Win-10-High	43.93	56.51	11.68	106061.45	64.46	8	1941.94	33521.11	41399.72	182.68	326.10	103.71

Median Encryption Speeds

Variant	Endpoint	Total_Encryptions	Duration_In_Minutes	Encryptions_Per_Minute	Encryption_Speed_MB_Per_Second
Avaddon	Win-10-High	98560	14.10	6990.00	65.2
Babuk	Win-10-High	98560	6.52	15130.00	141
Blackmatter	Win-10-High	98553	45.23	2179	20.31
Conti	Win-10-High	98560	58.30	1691	15.76
Darkside	Win-10-High	98553	45.38	2172	20.24
Lockbit	Win-10-High	98548	5.40	18259	170
Maze	Win-10-High	98560	115.45	853.71	7.957
Mespinoza	Win-10-High	97080	115.60	839.83	7.828
Revil	Win-10-High	98553	23.70	4160	38.76
Ryuk	Win-10-High	98284	17.17	5740	53.37

Windows 10 中規格

Endpoint Specifications

Endpoint	OS	CPU Cores	GB RAM	Disk IOPS	Disk Throughput MB/s
Win-10-Mid	Windows 10	4	16	3000	125
Win-10-High	Windows 10	8	32	3000	125
Server-2019-Mid	Windows Server 2019	8	32	3000	125
Server-2019-High	Windows Server 2019	16	64	10000	500

Median Resource Utilization

Variant	Endpoint	%_Privileged_Time	%_Processor_Time	%_User_Time	Handle_Count	Thread_Count	Priority	Page_Faults/sec	IO_Read_KBytes/sec	IO_Write_KBytes/sec	Private_MBytes	Virtual_MBytes	Working_Set(MBytes)
Avaddon	Win-10-Mid	84.53	88.58	35.93	376.26	21.10	8	109298.88	31681.35	31810.25	8.82	145.11	18.33
Babuk	Win-10-Mid	28.88	92.38	91.30	342.77	21.67	8	2573.52	18024.88	17406.98	14.48	124.84	15.87
Blackmatter	Win-10-Mid	7.09	9.93	5.65	299.84	14.13	10	1713.94	9098.79	9079.02	9.82	98.72	14.88
Conti	Win-10-Mid	8.03	15.45	9.92	219.44	7.29	8	67.98	12578.51	12631.15	42.55	122.58	14.83
Darkside	Win-10-Mid	7.05	21.41	15.69	393.82	15.86	10	1647.89	8560.02	8550.47	10.30	104.35	16.85
Lockbit	Win-10-Mid	28.65	42.79	15.75	533.11	16.01	8	1319.68	1149.89	1246.13	10.74	111.46	20.72
Maze	Win-10-Mid	4.29	5.31	4.06	318.91	5.09	8	1561.72	10573.49	3707.72	3.63	82.95	13.79
Mespinoza	Win-10-Mid	6.39	7.56	4.79	144.08	2.23	8	137.56	7402.86	5527.32	3.58	61.26	8.23
Revil	Win-10-Mid	8.44	22.78	15.96	253.35	12.48	8	2710.56	16585.00	16521.51	9.70	91.44	14.05
Ryuk	Win-10-Mid	43.86	54.72	12.19	126006.82	63.22	8	1599.03	33496.12	41261.27	182.21	322.15	95.17

Median Encryption Speeds

Variant	Endpoint	Total_Encryptions	Duration_In_Minutes	Encryptions_Per_Minute	Encryption_Speed_MB_Per_Second
Avaddon	Win-10-Mid	98560	12.63	7804.00	72.7
Babuk	Win-10-Mid	98560	7.84	12580.50	117
Blackmatter	Win-10-Mid	98553	42.92	2297	21.40
Conti	Win-10-Mid	98560	59.34	1661	15.48
Darkside	Win-10-Mid	98553	44.72	2204	20.54
Lockbit	Win-10-Mid	98548	5.84	16881	157
Maze	Win-10-Mid	98560	115.12	856.19	7.980
Mespinoza	Win-10-Mid	97080	114.20	850.09	7.924
Revil	Win-10-Mid	98553	23.67	4166	38.81
Ryuk	Win-10-Mid	87739	16.98	5270	48.15

關於 SURGe

建立於 2021 年 10 月，SURGe 是 Splunk 的戰略網路安全研究部門，致力於研究、回應與教育影響世界的網路威脅。作為值得信賴的顧問，SURGe 透過研究論文、會議論文和線上研討會中的回應指南和深入分析，在高調、時機敏感的網路攻擊中為組織提供技術指導。組織可以依靠 SURGe 提供的適當內容和及時的建議，憑藉著自信和智慧來應對全球安全事件。
了解更多資訊。

22-23023-Splunk-EmpiricallyComparativeAnalysisofRansomwareBinaries-A4-WP-101