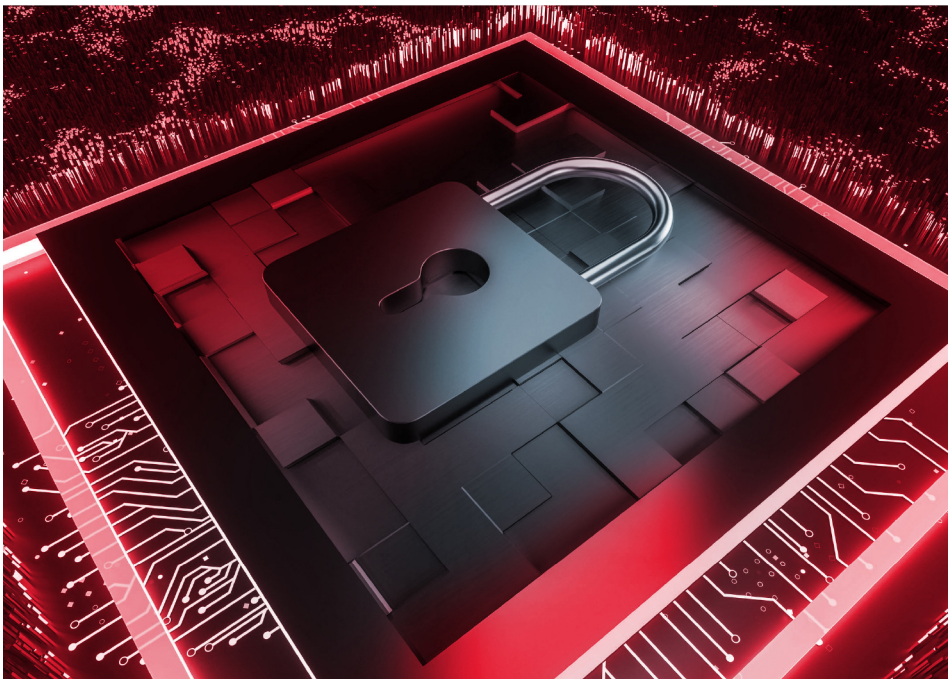
白皮書

目標式勒索軟體攻擊

由賽門鐵克威脅獵手 (Threat Hunter) 團隊撰寫

目錄



簡介

在過去的 18 個月裡，目標式勒索軟體攻擊已經從一個有利可圖但利基的網路犯罪領域轉變為可能是所有企業面臨的最危險威脅。在此期間，發動這類攻擊的團體數量倍增。大量報導的贖金支付，助長駭客圈充斥淘金心態，一些資深的網路犯罪分子放棄了他們的傳統業務領域，轉向目標式勒索軟體攻擊。

勒索軟體活動增加的因素之一，就是勒索軟體即服務 (Ransomware-as-a-service，RaaS) 的出現，例如：惡意程式開發人員建立的勒索軟體套件，即可輕易用來建立及自訂新型勒索軟體變種。開發人員通常會向攻擊者提供套件，並收取一定比例的利潤。

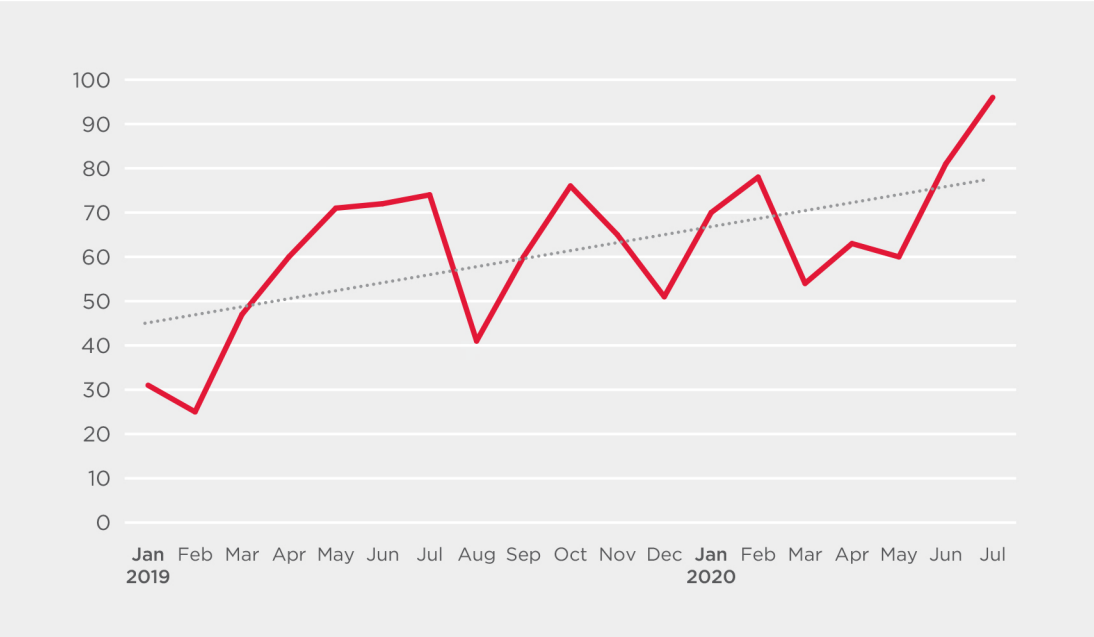
這些戰術已隨著時間演變，攻擊者找到了更多勒索受害者組織的方法。現在，越來越多的攻擊者在加密電腦之前會先從目標竊取重要資料。然後攻擊者威脅，除非支付贖金，否則就會公布這些資料。公布資料的威脅增加了受害組織的支付壓力，這讓原本可全身而退，從完整備份資料恢復的的企業，也面臨巨大的支付贖金壓力。

威脅級別表示各種規模的組織都應該了解這些攻擊是如何展開的，並採取一切可能的步驟來降低成功攻擊的風險。

目標式勒索軟體攻擊發展趨勢

在過去一年半中，受目標式勒索軟體攻擊所影響的組織數量呈現穩步增長趨勢。檢視 10 個知名的目標式勒索軟體家族，我們發現雖然每個月被攻擊的組織數量有所波動，但整體趨勢是向上的。

圖 1：受目標式勒索軟體攻擊影響的組織數量，2019 年 1 月至 2020 年 7 月

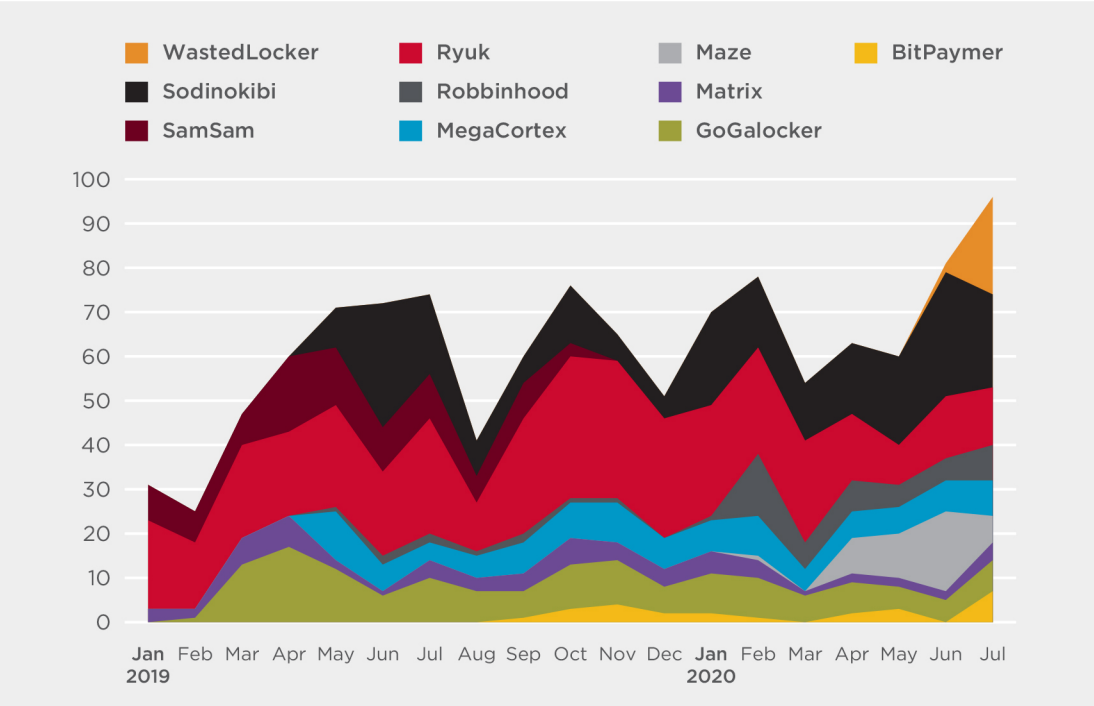


賽門鐵克是博通（Broadcom--納斯達克股票代碼：AVGO）的企業安全部門，觀察到在 2019 年 1 月有 31 個組織受到攻擊。此一數字在 2020 年 7 月上升到 89 個。

遭受目標式勒索軟體攻擊的實際數量可能更高。一些勒索軟體家族，例如：Dharma (也稱為 Crysis)，除了用於目標攻擊之外，還透過垃圾郵件活動進行散布。無法確定有多少受害者遭受這些目標攻擊感染，又有多少受害者是經由其他方式所感染的。

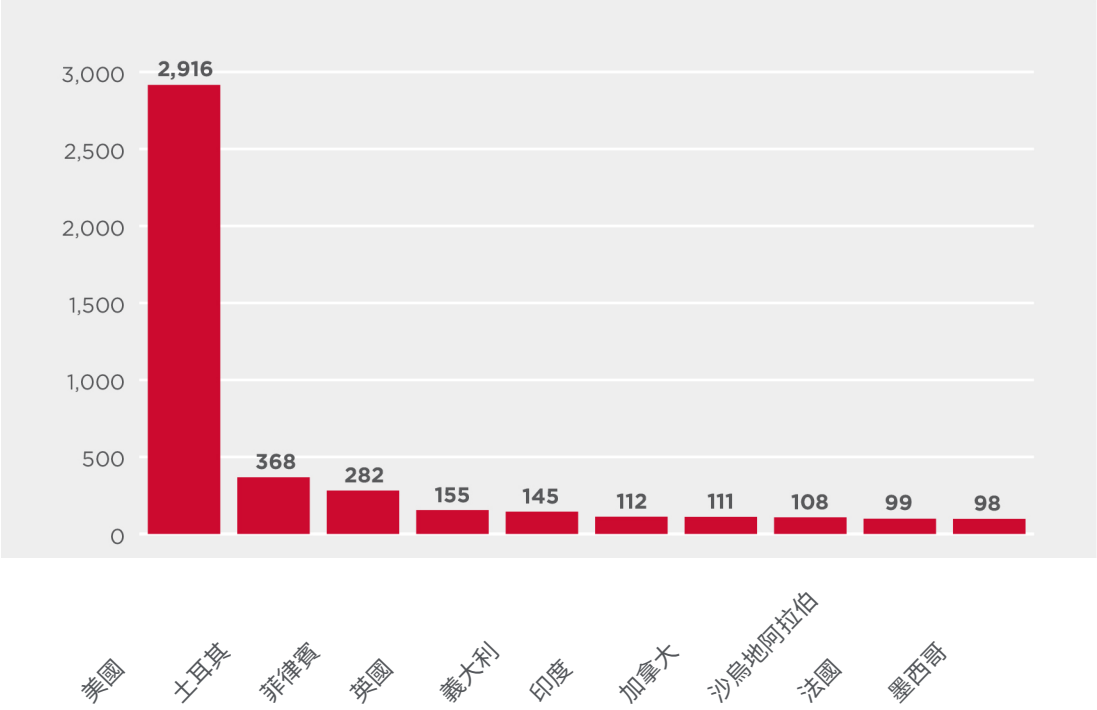
除了這些目標攻擊之外，來自上述 10 個勒索軟體家族的確認攻擊，可能只是涉及這些威脅攻擊總數的一個代表性樣本而已。大多數目標式勒索軟體攻擊，會為每次新的攻擊重新編譯他們的勒索軟體。這意味著攻擊中，使用的勒索軟體變種可能會被通用或基於機器學習的檢測特徵檔所阻止，而不會被歸類到該勒索軟體家族相關的檢測。

圖 2：按家族分列的受目標式勒索軟體攻擊影響的組織數量，2019 年 1 月至 2020 年 7 月



當攻擊根據勒索軟體家族進行分類時，很明顯的，新參與者的大量湧入正在推動攻擊的增長。2019 年 1 月，只有三個家族處於「活躍」狀態。到 2020 年 7 月已有 8 個家族進行了襲擊。2020 年，Sodinokibi、Maze 和最近的 WastedLocker 等相對較新的攻擊出現，對攻擊整體增加有功不可沒的貢獻。

圖 3：根據國家／地區分列的目標式勒索軟體攻擊感染數量，從 2019 年 1 月至 2020 年 7 月



在按地理區域分析攻擊時，需要採用不同的方法，因為目標式勒索軟體攻擊的許多受害者在多國家／跨地區都有營運據點。通過計算上面列出的 10 個目標式勒索軟體攻擊家族識別感染，美國仍然是迄今為止攻擊組織最嚴重的目標國家。但很不尋常的是，緊跟在後的居然是土耳其和菲律賓。這些國家通常在網路犯罪統計數字中並沒有那麼突出。其他排名前 10 名的國家並不令人意外。

攻擊者背景

Maze(* 迷宮)

Maze 於 2019 年 5 月首次出現，在此期間一直是最活躍的目標式勒索軟體攻擊家族之一。該家族最出名的是在加密之前從受害者組織中竊取資料並威脅要發布這些資料，除非支付贖金。這增加了受害者支付贖金的壓力，並提供了一個新的壓力點在原先能夠從備份中恢復受影響系統的受害者。這一戰術很快被其他目標式勒索軟體家族效仿，包括 Sodinokibi、Nemty 和 DoppelPaymer。

圖4：Maze 攻擊影響的組織數目，2020 年 1 月至 2020 年 7 月

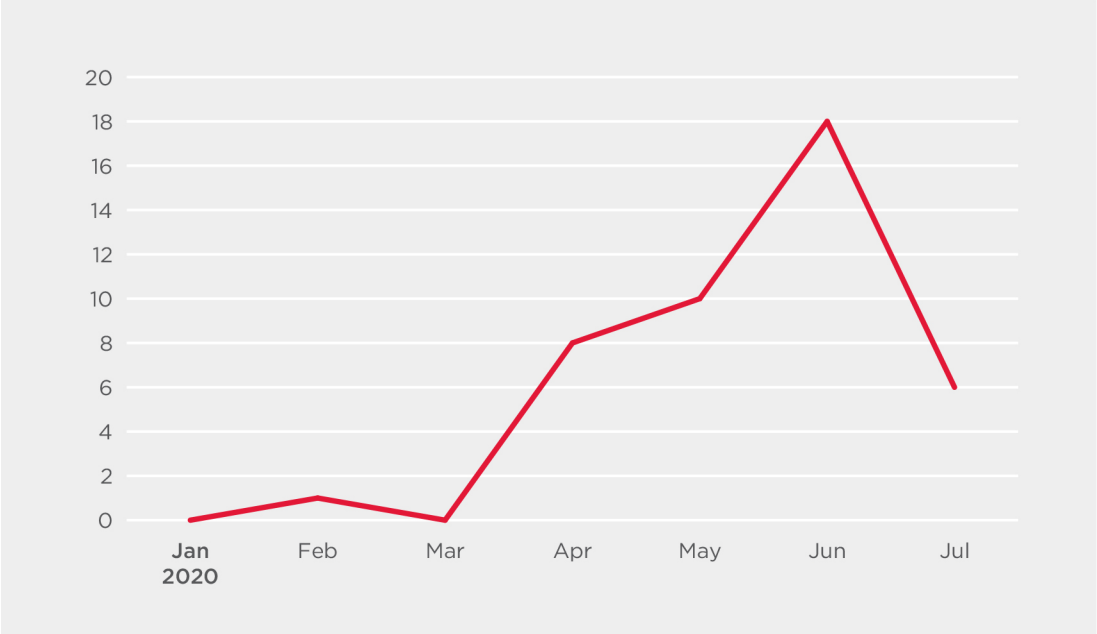
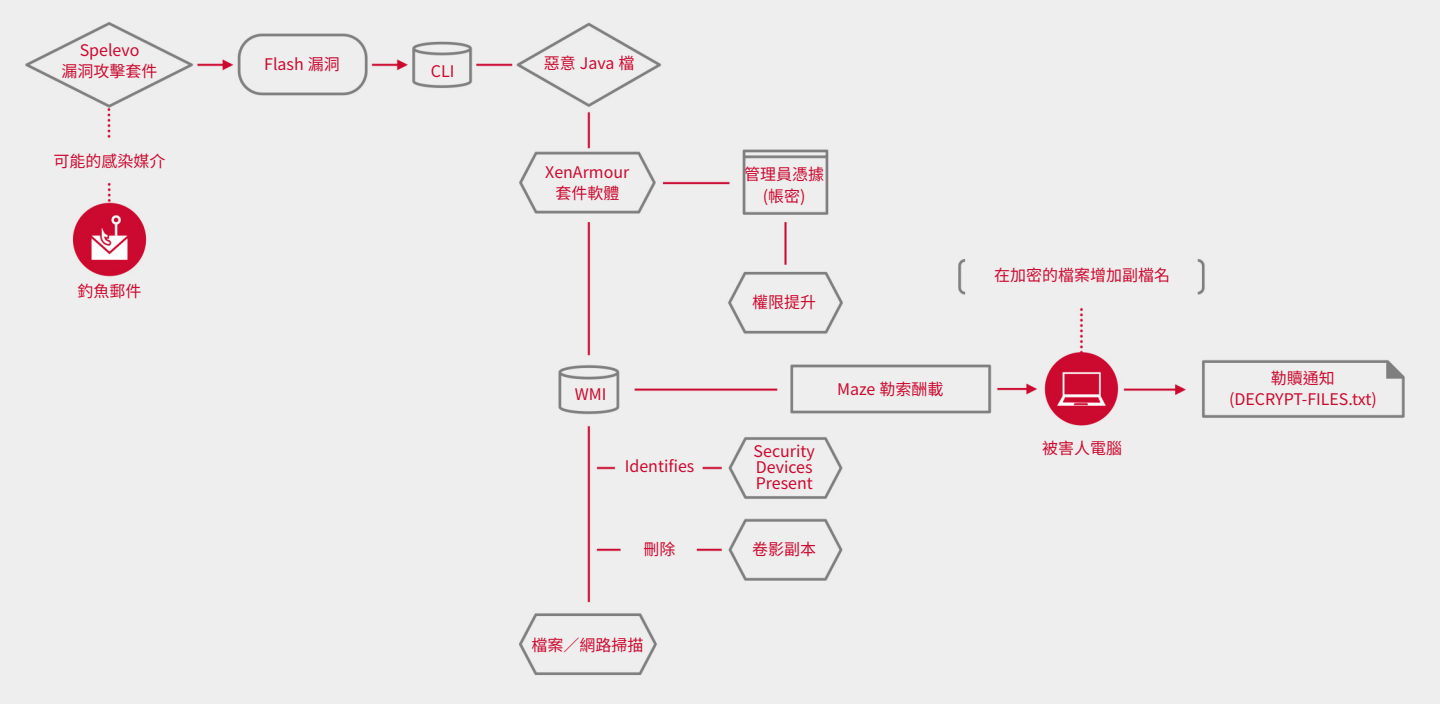


圖5：Maze 攻擊流程圖



Maze 主要發佈管道是利用 Fallout 和 Spelevo 這兩種漏洞攻擊套件--受害者經由垃圾郵件活動而上鉤。一旦攻擊者獲得對網路上任何一台電腦的存取權限，他們就會下載「現貨商品」的惡意程式--Cobalt Strike 和 Metasploit 框架，以便在網路中橫向移動並如同弱點掃描檢測一樣，列舉所有電腦的相關資訊，例如：安裝那些軟體、軟體版本、帳號密碼……。

攻擊者掃描網路上運行位址解析協議 (RDP) 的電腦，並使用暴力攻擊來取得身分憑證，以獲得對伺服主機的特權存取。這種特權存取，如虎添翼般地讓攻擊者能夠搜尋和發掘檔案伺服器及資料庫的詳細資料，有助於竊取隨後用於勒索受害者的資料。

該集團往往會在受害者的網路上滯留很長一段時間，從初始入侵到勒索軟體被執行，最久長達 21 天。

Maze 攻擊值得注意的特點，是攻擊者會檢查受害者系統所使用的語系，如果語言設置為俄語，則該惡意軟體就不會被執行。

Maze 還有一種不尋常的付款方式，要求受害者分別支付兩筆款項。第一筆付款是為了換取不分享從受害者那裡竊取資料的承諾，第二次付款是獲得解密的密鑰。

如果受害者沒有在截止日期前完成第一筆付款，Maze 將在其自己的公開網站上發布被盜資料。它還使用社交媒體帳戶提醒受害組織及其客戶注意資料外洩。

根據第三方報導，該組織將向付款的受害者提供解密密鑰，但它仍會經常在黑市出售被盜資料--即使受害者已經支付了贖金。

Maze 還將向其他攻擊者提供勒索軟體服務 (Ransomware-as-a-service，RaaS)。該組織也經常在駭客論壇和黑市發布訊息，像是在 Twitter 等社交媒體上也非常活躍，經常用它來嘲諷受害者。

Sodinokibi(* 索迪諾基比)

Sodinokibi (也稱為 REvil) 首次出現在 2019 年 4 月，儘管其創建者投入勒索軟體行業的時間更長，並負責在 Sodinokibi 發布之前就已停產較舊的 GandCrab 勒索軟體。

Sodinokibi 與 GandCrab 一樣，都是以勒索軟體即服務 (RaaS) 的商業模式運營，將其工具出租給執行攻擊特定數量的團體，即「攻擊發動分紅組織」或稱「附屬」公司。Sodinokibi 作者及其附屬公司，縝密分工並分潤。據信，許多 GandCrab 附屬公司轉換跑道成為 Sodinokibi 的附屬公司。

圖6：受 Sodinokibi 攻擊影響的組織數目，2019 年 1 月至 2020 年 7 月

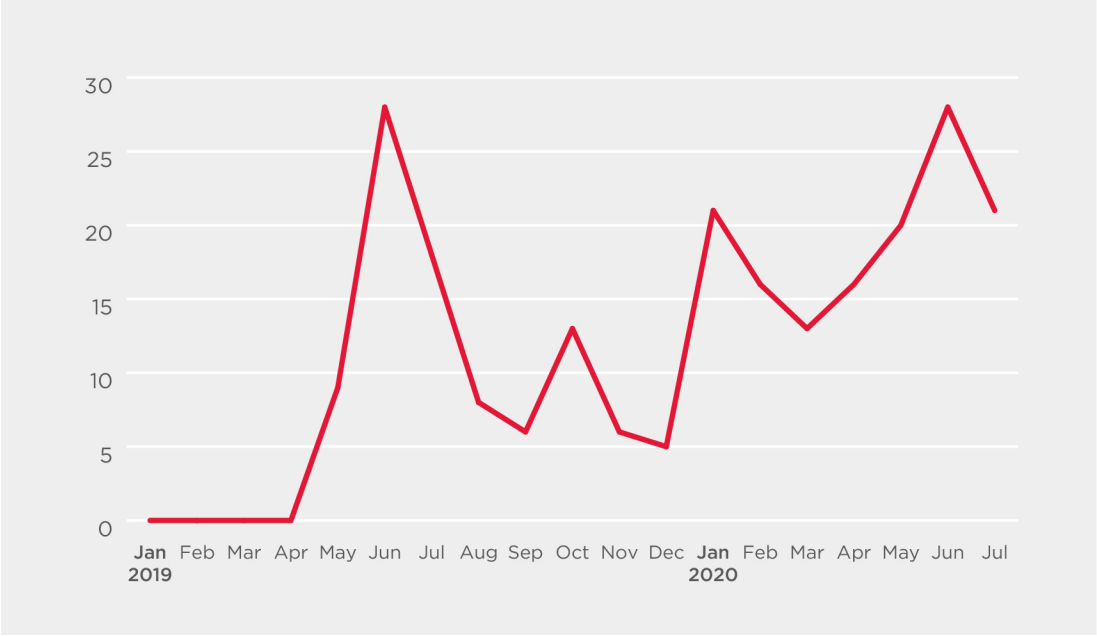
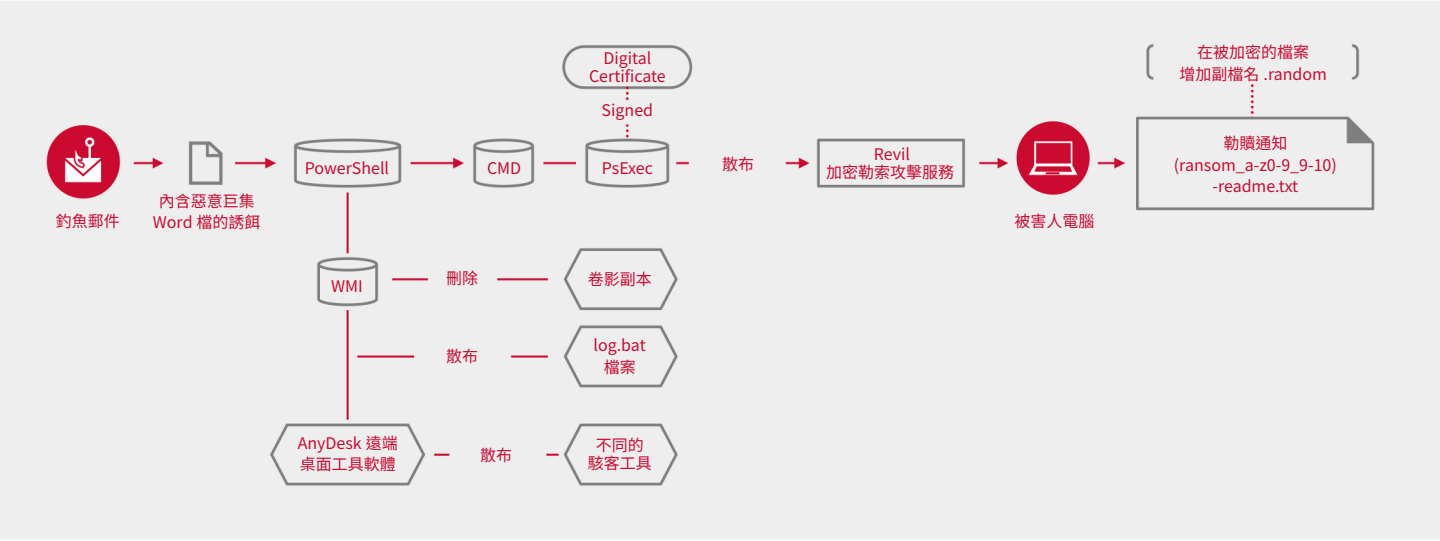


圖7：Sodinokibi 攻擊攻流程圖



攻擊通常始於帶有附件，包含惡意巨集的 Word 檔案的網路釣魚電子郵件。一旦進入受害者的網路，攻擊者將花費三到八天的時間為攻擊做準備。與許多其他目標式勒索軟體攻擊家族一樣，Sodinokibi 攻擊往往會廣泛使用受害者環境中的資源以及公開可用的工具，以便在執行勒索軟體酬載 (Payload) 之前對環境進行最佳籌畫。在這種情況下，它使用 PowerShell、WMI、PsExec 和 AnyDesk 遠端桌面工具。攻擊者還會刪除 Windows 磁碟區陰影複製，以干擾被加密機器的恢復。

Sodinokibi 以鎖定大型組織而聞名。較大的公司有能力支付更大的贖金，並且通常會因機密資料被公開而損失更多。該組織與 2020 年 1 月對外匯服務公司--Travelex 的攻擊有關，該攻擊勒索了高達 230 萬美元的贖金，遠高於大多數企業勒索軟體攻擊中的平均 260,000 美元。

Sodinokibi 迅速模仿了從受害者網路中竊取資料的戰術。該組織通常會將所竊取資料的樣本發佈到 Pastebin 等公開網站，以證明他們手上掌握了受害者的重要資料。然後，攻擊者會再威脅如不支付贖金就會要發佈被盜資料，以此步步進逼勒索受害者。受害者如逾期支付贖金每超過一小時，就會再公開更多的資料，同時也會同步增加贖金要求。

即使受害者支付了贖金，他們仍然可能會資料外洩，因為也有人觀察到 Sodinokibi 在地下論壇上將受害者資料出售給出價最高的人。

Sodinokibi 攻擊的另一個有趣特徵是，在某些情況下，攻擊者會被觀察到掃描受害者網路以獲取信用卡或銷售點 (PoS) 軟體。目前尚不清楚攻擊者是針對該軟體進行加密，還是因為他們想通過擷取這些資料從這次攻擊中賺取更多的錢。

BitPaymer

BitPaymer 與 Evil Corp 網路犯罪組織有關聯，該組織隨後開始使用 WastedLocker 勒索軟體（也在本文中進行了介紹）。

Evil Corp 因涉及 Dridex 銀行木馬的攻擊而一戰成名，但在 2017 年，它徹底改革了其運營並轉向了目標式勒索軟體攻擊。BitPaymer 攻擊始於 2019 年 6 月，一直持續到 2020 年 6 月，之後該組織似乎已轉向到 WastedLocker。

圖8：受 BitPaymer 攻擊影響的組織數目，2019 年 1 月至 2020 年 7 月

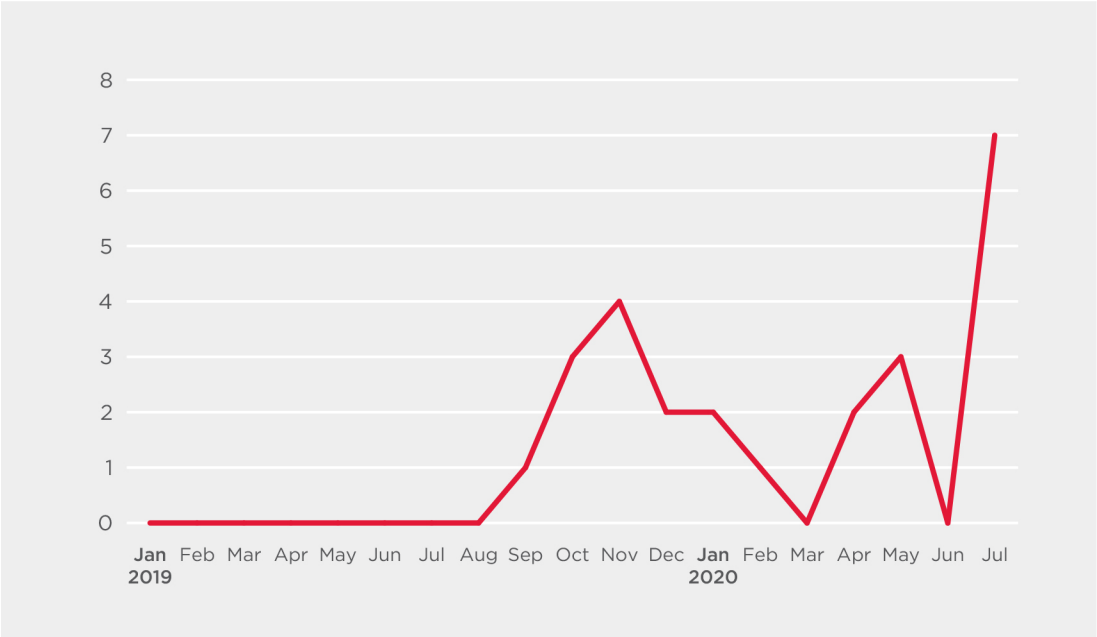
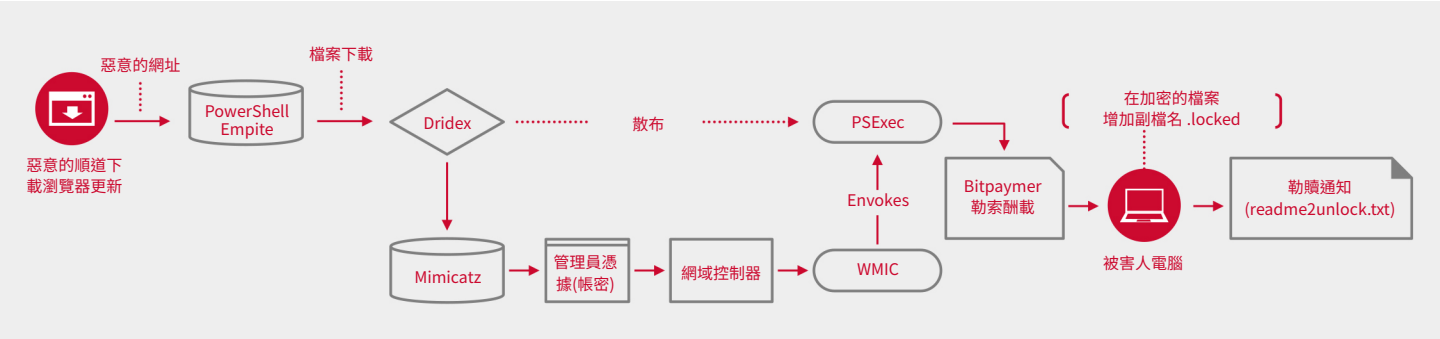


圖9：BitPaymer 攻擊流程圖



BitPaymer 攻擊通常始於使用網路釣魚電子郵件或傳送假冒瀏覽器更新的漏洞攻擊套件感染受害者。除此之外，該組織還有大量潛在的受害者，這些已經感染了 Dridex 木馬的受害者，讓攻擊者可以隨時對他們發動再次攻擊。

Dridex 不僅僅是用作感染媒介。該惡意軟體還針對新的受害者部署。Dridex 本質上是模組化的，包括憑證竊取功能和提供額外惡意軟體的能力。該攻擊者本質上是將其從主要酬載 (Payload) 轉變為用於發動攻擊前，能讓攻擊者先立足於受害者環境內的工具。

通常，BitPaymer 攻擊者在執行勒索軟體之前，會在受害者的網路上蟄伏 5 到 8 天的時間。為了提升特權並稍後在網路上移動，攻擊者利用了環境中已經存在的許多系統和管理工具，也就是「就地取材」。這降低了安全軟體識別惡意活動的機會，增加了成功入侵的機會。

攻擊通常始於使用 PowerShell（和 PowerShell Empire 框架）下載 Cobalt Strike。Cobalt Strike 原本作為滲透測試工具出售，但後來經常用於惡意目的。

此外，WMIC 和 PsExec 等合法管理工具被用於獲取存取權限、停用安全軟體、刪除備份和恢復功能及散布和執行 BitPaymer 酬載 (Payload)。

WastedLocker

WastedLocker 是一個新的目標式勒索軟體攻擊家族，與 Evil Corp 網路犯罪集團有關。它似乎於 2020 年 5 月左右開始運營。

攻擊始於一個名為 SocGholish 的惡意 JavaScript 框架，偽裝成軟體更新。已在 150 多個受感染網站上發現了 SocGholish，其中包括數十個美國新聞網站。

圖10：受 WastedLocker 攻擊影響的組織數量，2020 年 1 月至 2020 年 7 月

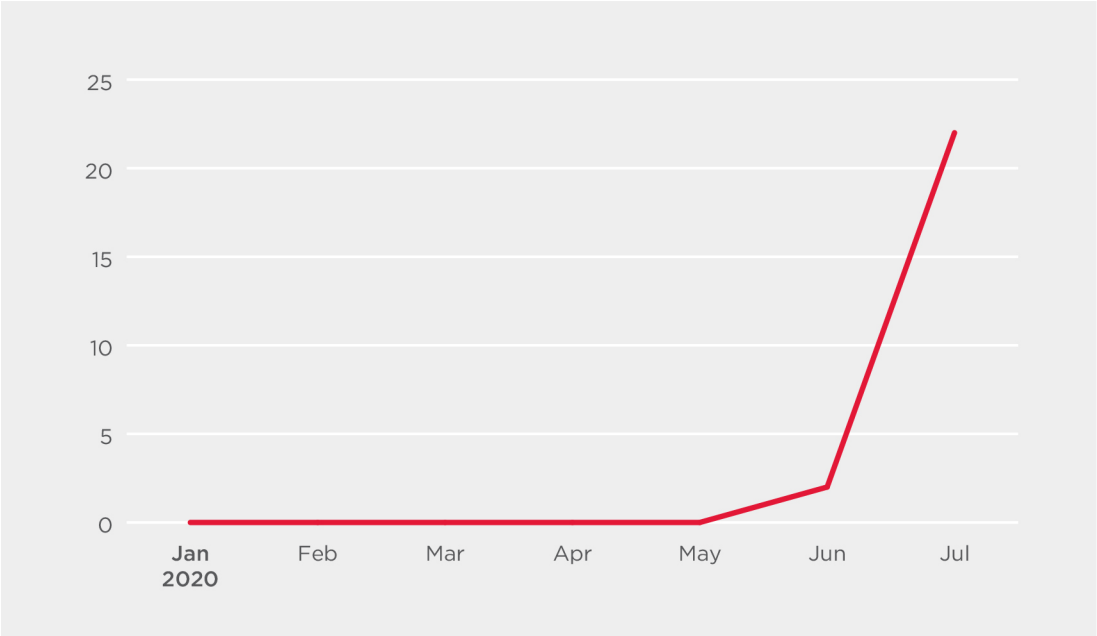
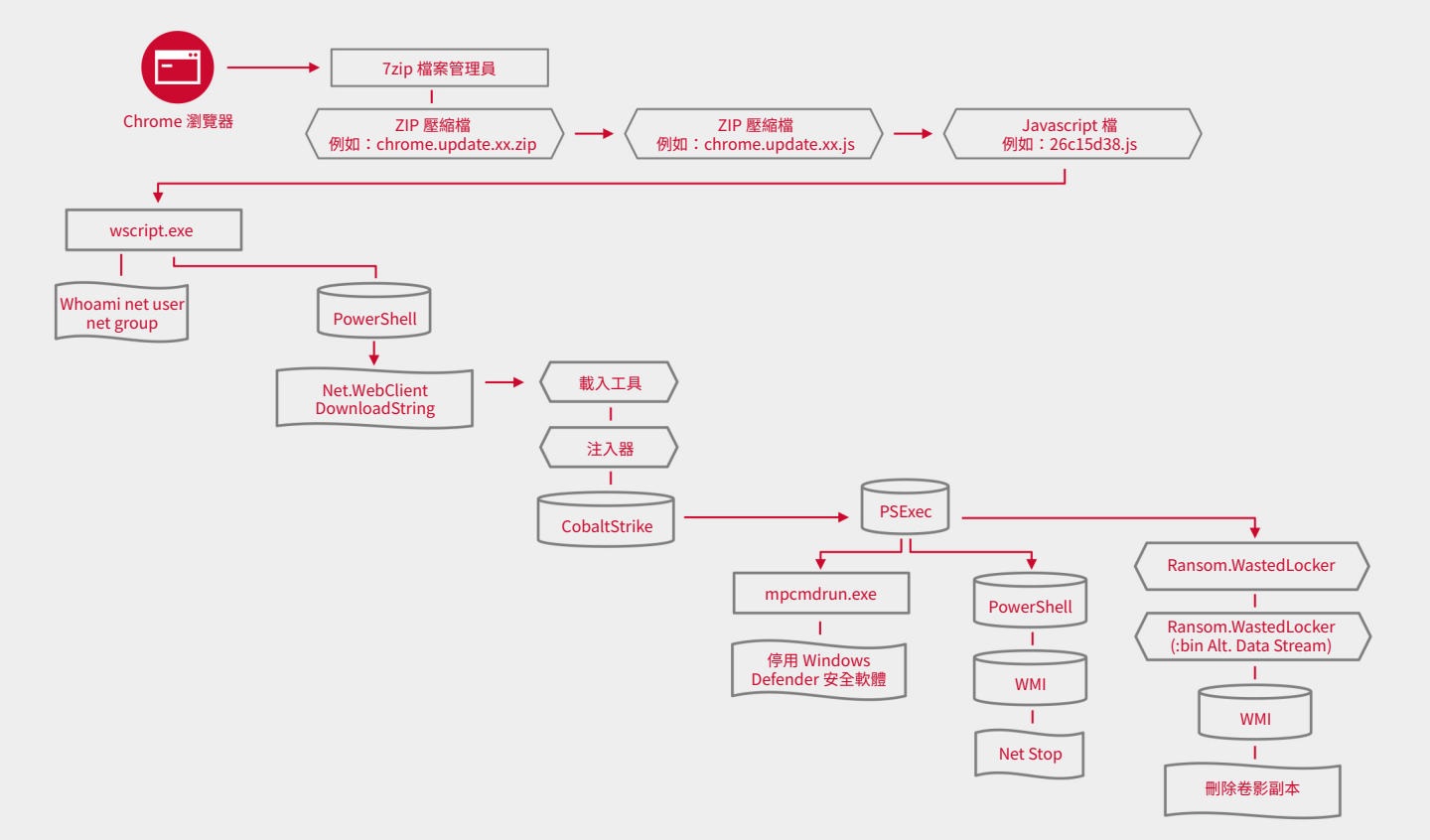


圖11：WastedLocker 攻擊流程圖



一旦攻擊者在受害者的網路上獲得立足點，就會使用 PowerShell 下載並執行載入工具 (loader)。該載入工具包含一個 .NET 注入器以及一個用於 Cobalt Strike Beacon 的載入工具，據報導該載入工具取自一個名為 Donut 的開放原始碼計畫，該項目旨在幫助注入和執行記憶體中的酬載 (Payload)。

Cobalt Strike Beacon 可用於執行命令、注入其他程序 (processes)、提升當前程序或模擬其他程序以及上傳和下載檔案。攻擊者將 PowerView 的 Get-NetComputer 命令重新命名為隨機名稱。然後，此命令使用 *server* 或 *2003* 或 *7* 等過濾條件搜索 Active Directory 資料庫中的所有電腦對象（返回所有 Windows Server、Windows Server 2003 或 Windows 7 實例）。攻擊者然後將此資訊記錄在 .tmp 檔案中。

權限提升是使用了已公開記錄的技術所執行，該技術涉及軟體授權用戶界面工具 (slui.exe)，這是一個負責啟動和更新 Windows 作業系統的 Windows 命令列工具。

攻擊者使用 Windows Management Instrumentation 命令列工具 (wmic.exe) 在遠端電腦上執行命令，例如新增使用者或執行其他下載的 PowerShell 腳本。Cobalt Strike 還用於使用 ProcDump 執行憑證傾倒 (credential dumping) 和清空日誌檔案。

為了部署勒索軟體，攻擊者使用 Windows Sysinternals 的工具--PsExec 啟動一個合法的命令列工具來管理 Windows Defender (pcmdrun.exe) 以停用掃描所有下載的檔案和附件，刪除所有已安裝的定義檔，並在某些情況下，停用即時監控。

在透過內建 WMI win32_service 指令獲取服務名稱後，隨後使用 PsExec 來啟動 PowerShell，並使用 netstop 命令來停止這些服務。在停用 WindowsDefender 並在整個組織中停止服務後，PsExec 用於啟動 WastedLocker 勒索軟體本身，然後開始加密檔案並刪除 Windows 磁碟區陰影複製。

Miner(* 礦工)：Ryuk、GoGalocker 和 MegaCortex

在 2019 年的一篇論文中，我們發現了 GoGalocker 和 MegaCortex 勒索軟體家族之間存在聯繫。現在我們找到了更有力的證據，表明他們與 Ryuk 一起被我們命名為 Miner 的單一對手所控制。

圖12：受 Ryuk 攻擊影響的組織數量，2019 年 1 月至 2020 年 7 月

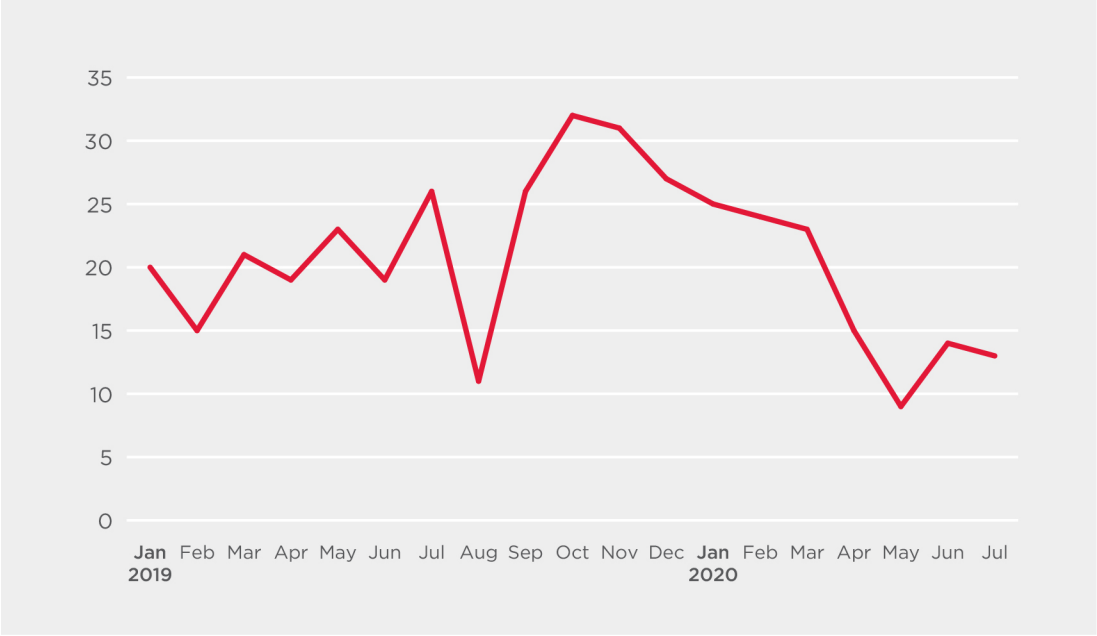
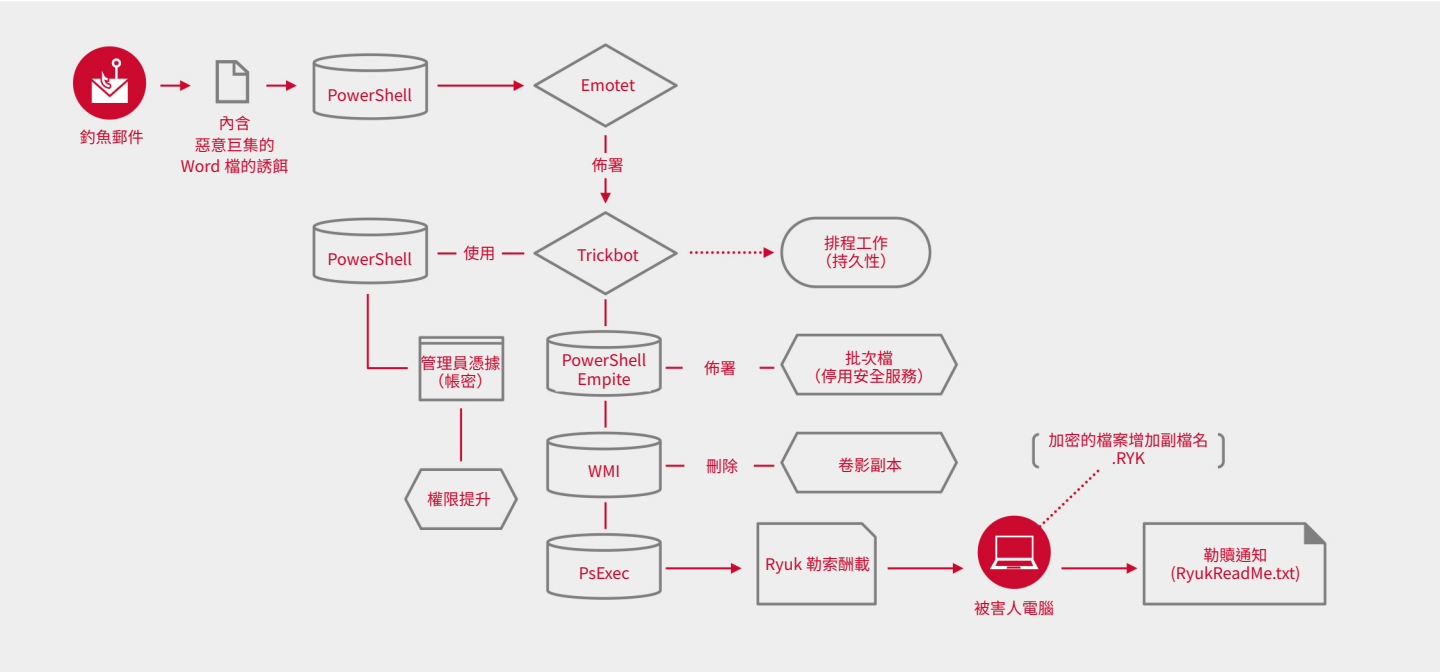


圖13：Ryuk 攻流程圖



儘管 Miner 使用了不同的勒索軟體有效酬載 (Payloads)，但自開始發動目標式勒索軟體攻擊以來，其整體運作方式一直保持一致。雖然一些工具隨著時間的推移發生了變化，但作業程序並沒有太大變化。

在所有行動中看到的一個方法是使用 Cobalt Strike，它在受感染電腦的記憶體中運行 (也就是無檔案攻擊--Fileless)，這使得檢測變得困難。Miner 使用 Cobalt Strike 下載額外的工具並建立一個反向 shell，為攻擊者提供額外的存取權限。Cobalt Strike 是少數在所有作業中保持一致的工具之一，無論 Miner 勒索攻擊中使用的酬載 (Payload) 如何。

在某些情況下，Miner 使用 Mimikatz 來獲取受害者憑證 (帳密)，而在其他情況下，攻擊者會利用 TrickBot 惡意軟體中的功能實現相同的目的。在這種情況下，Miner 改變了使用的工具，但戰術保持不變。應使用每次攻擊中涉及的方式和步驟來識別 Miner 活動，而不是工具本身。

圖14：受 GoGalocker 攻擊影響的組織數量，2019 年 1 月至 2020 年 7 月

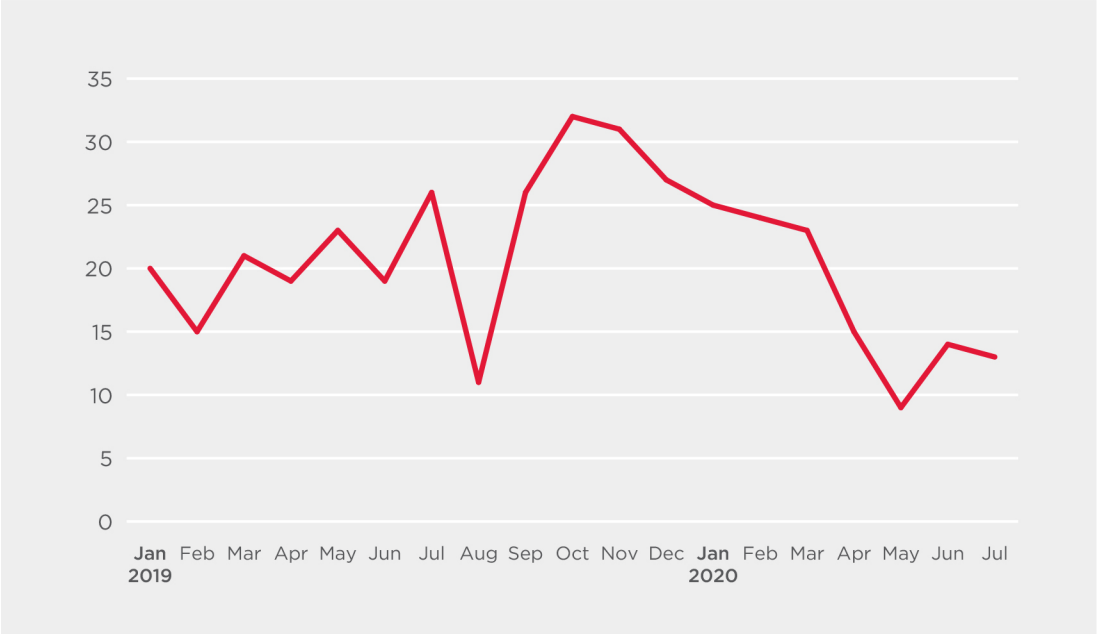
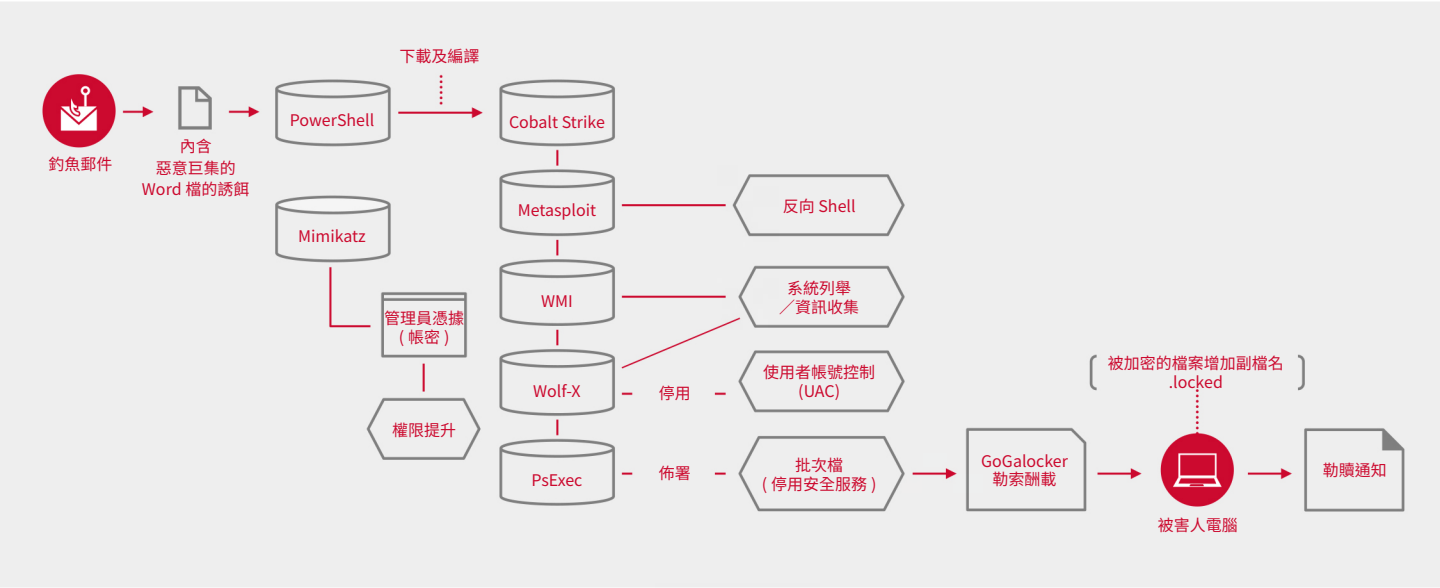


圖15：GoGaLocker 攻流程圖



與許多其他目標式勒索軟體攻擊者一樣，Miner 廣泛利用在受害者環境中發現的資源。攻擊始於包含惡意檔案的網路釣魚電子郵件，如果開啟惡意檔案，受害者將感染 Emotet 或 TrickBot 惡意軟體。Emotet 的設計是為了當存取開放式共享時能夠在受害者的網路中自我傳播，使其成為橫向移動的有用工具。同時，TrickBot 採用模組化設計，可以載入與正在進行的攻擊相關的模組。在這種情況下，透過 TrickBot 可以竊取憑據（帳密），以提升權限。

然後使用 Cobalt Strike 和 Metasploit 等公開可用的惡意軟體來列舉（搜尋和發掘）網路的詳細資料以進行橫向移動並提高權限。完成此步驟後，Miner 將獲得對網域控制器 (DC) 的管理存取權限。然後攻擊者使用經由 PsExec 部署的批處理檔來停用和刪除整個環境中的備份／恢復功能和安全服務。此時，網路已準備就緒，可以散佈和執行勒索軟體酬載 (Payload)。

圖16：受 MegaCortex 攻擊影響的組織數量，2019 年 1 月至 2020 年 7 月

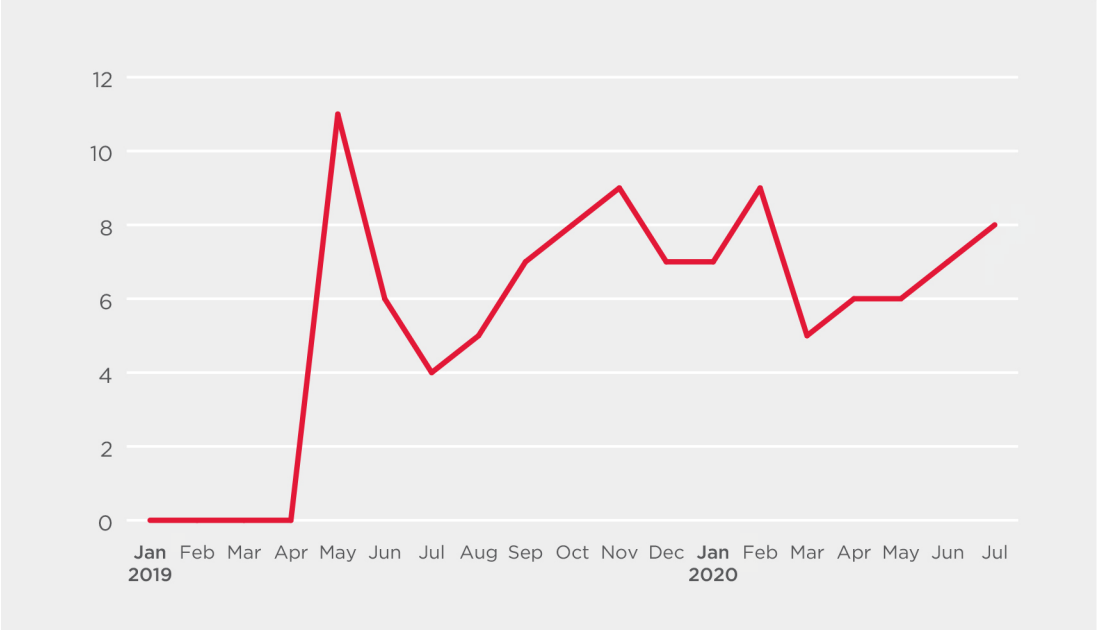
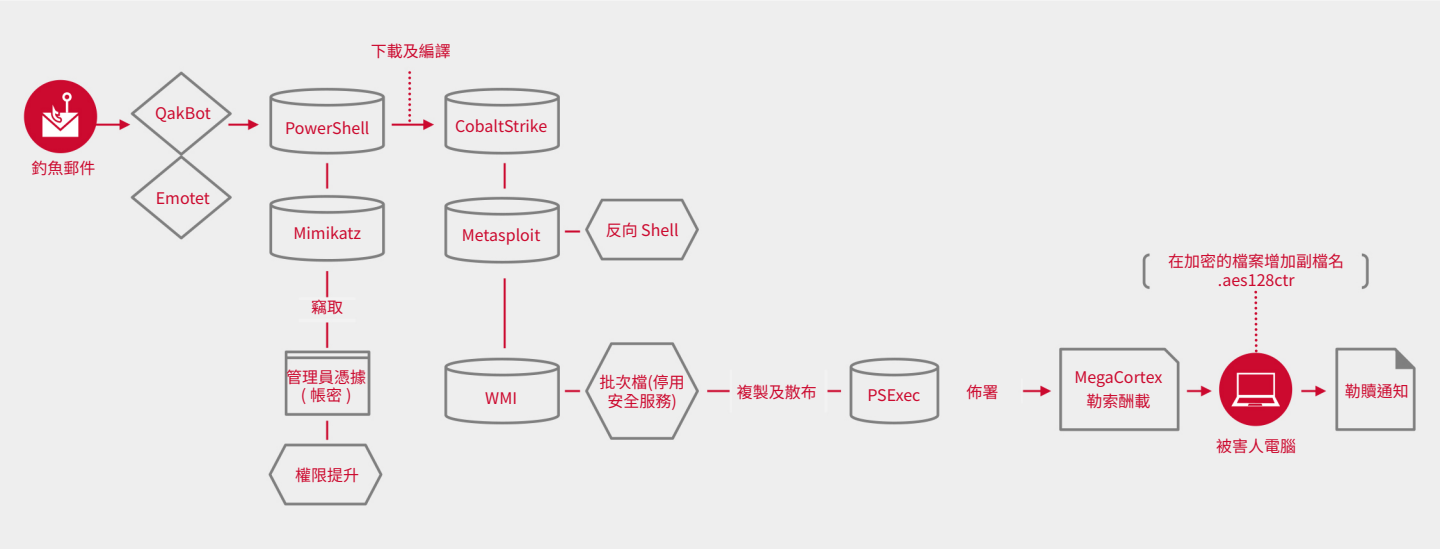


圖17：MegaCortex 攻擊流程圖



基礎設施重疊

Miner 由幾個 IP 位址去下載 Cobalt Strike，大多是在 89.105.198.XX

- 89.105.198.21 -- GoGalocker attack
- 89.105.202.58 -- GoGalocker attack
- 89.105.198.28 -- MegaCortex attack

批次檔的檔案名相似之處

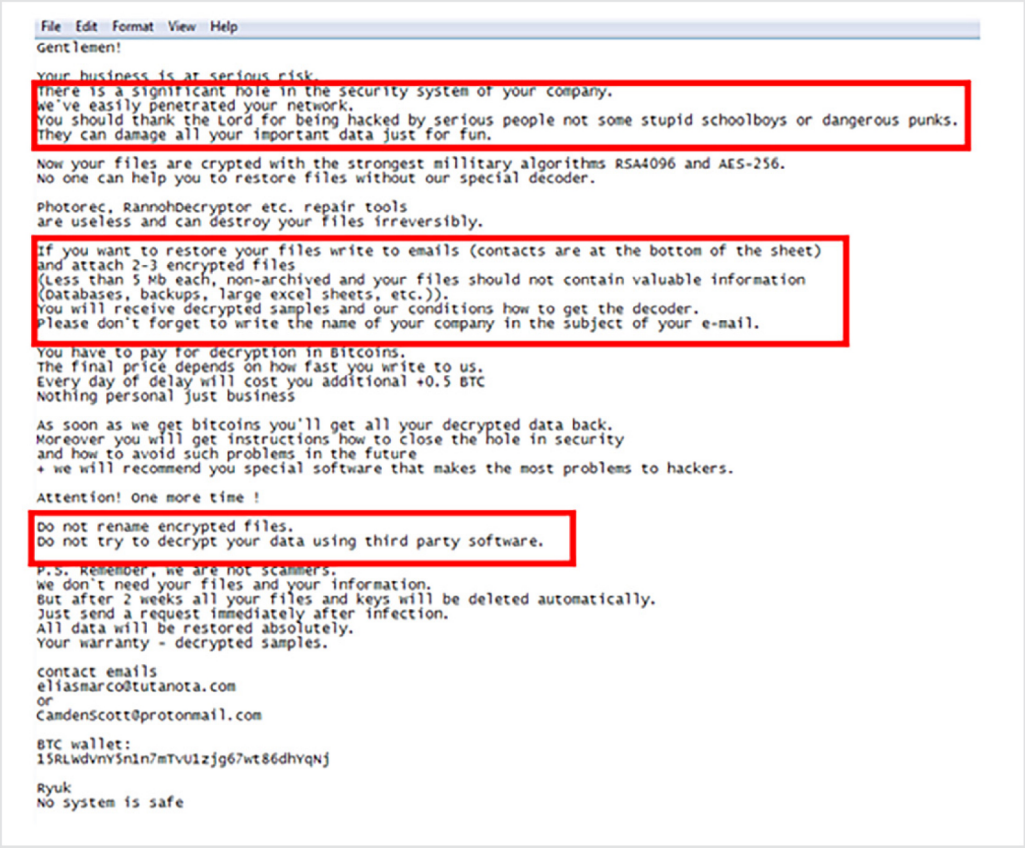
具有罕見檔名的批次檔 (Bat) 檔案，被用於與這三個勒索軟體系列的攻擊有關。

- kill.bat -- 被用於 MegaCortex, GoGalocker, Ryuk
- xaa.bat -- 被用於 GoGalocker, Ryuk
- xab.bat --被用於 GoGalocker, Ryuk
- xac.bat -- 被用於 GoGalocker, Ryuk
- xaj.bat -- 被用於 GoGalocker

勒贖通知的相似之處

在勒贖通知中也發現了相似之處

圖18：Ryuk 勒贖通知



File Edit Format View Help

Gentlemen!

Your business is at serious risk.
There is a significant hole in the security system of your company.
We've easily penetrated your network.
You should thank the Lord for being hacked by serious people not some stupid schoolboys or dangerous punks.
They can damage all your important data just for fun.

Now your files are crypted with the strongest millitary algorithms RSA4096 and AES-256.
No one can help you to restore files without our special decoder.

Photorec, RannohDecryptor etc. repair tools
are useless and can destroy your files irreversibly.

If you want to restore your files write to emails (contacts are at the bottom of the sheet)
and attach 2-3 encrypted files
(Less than 5 Mb each, non-archived and your files should not contain valuable information
(Databases, backups, large excel sheets, etc.)).
You will receive decrypted samples and our conditions how to get the decoder.
Please don't forget to write the name of your company in the subject of your e-mail.

You have to pay for decryption in Bitcoins.
The final price depends on how fast you write to us.
Every day of delay will cost you additional +0.5 BTC
Nothing personal just business

As soon as we get bitcoins you'll get all your decrypted data back.
Moreover you will get instructions how to close the hole in security
and how to avoid such problems in the future
+ we will recommend you special software that makes the most problems to hackers.

Attention! One more time !

Do not rename encrypted files.
Do not try to decrypt your data using third party software.

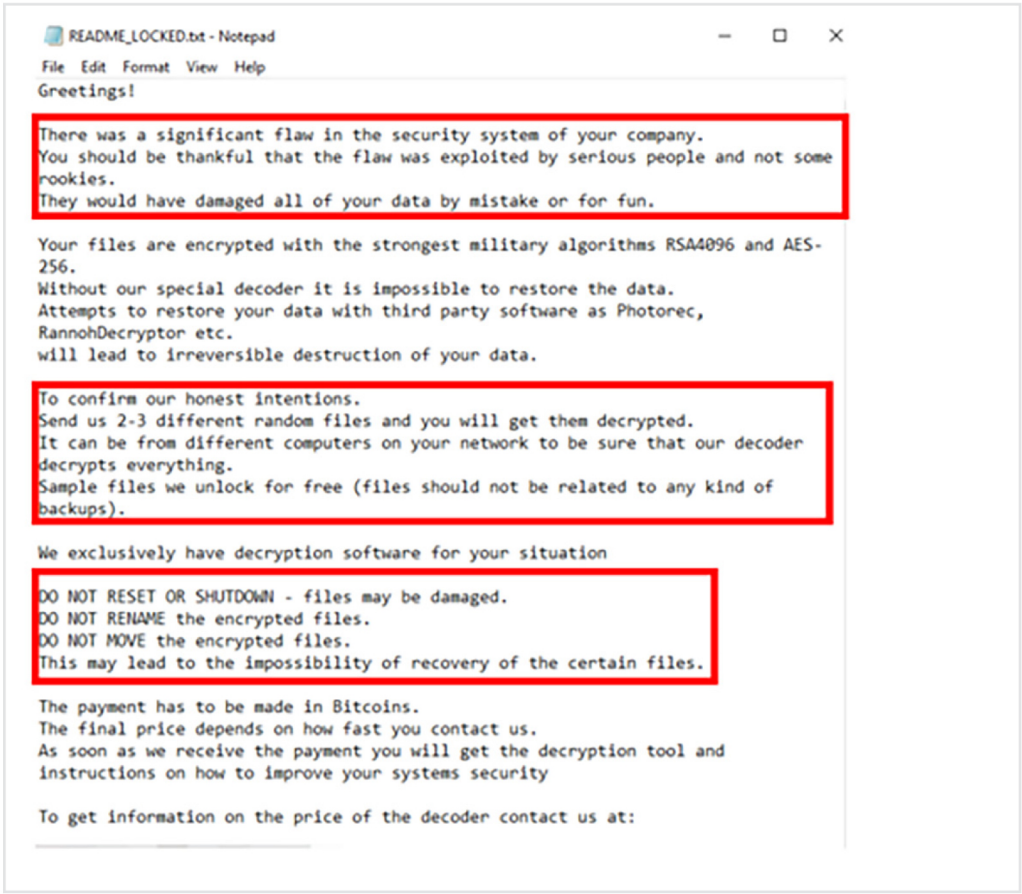
P.S. Remember, we are not scammers.
We don't need your files and your information.
But after 2 weeks all your files and keys will be deleted automatically.
Just send a request immediately after infection.
All data will be restored absolutely.
Your warranty - decrypted samples.

contact emails
eliasmarco@tutanota.com
or
CamdenScott@protonmail.com

BTC wallet:
15RLWdVnY5n1n7mTvU1zjg67wt86dhYqNj

Ryuk
No system is safe

圖19：GoGalocker 勒贖通知



README_LOCKED.txt - Notepad

File Edit Format View Help

Greetings!

There was a significant flaw in the security system of your company.
You should be thankful that the flaw was exploited by serious people and not some rookies.
They would have damaged all of your data by mistake or for fun.

Your files are encrypted with the strongest military algorithms RSA4096 and AES-256.
Without our special decoder it is impossible to restore the data.
Attempts to restore your data with third party software as Photorec,
RannohDecryptor etc.
will lead to irreversible destruction of your data.

To confirm our honest intentions.
Send us 2-3 different random files and you will get them decrypted.
It can be from different computers on your network to be sure that our decoder decrypts everything.
Sample files we unlock for free (files should not be related to any kind of backups).

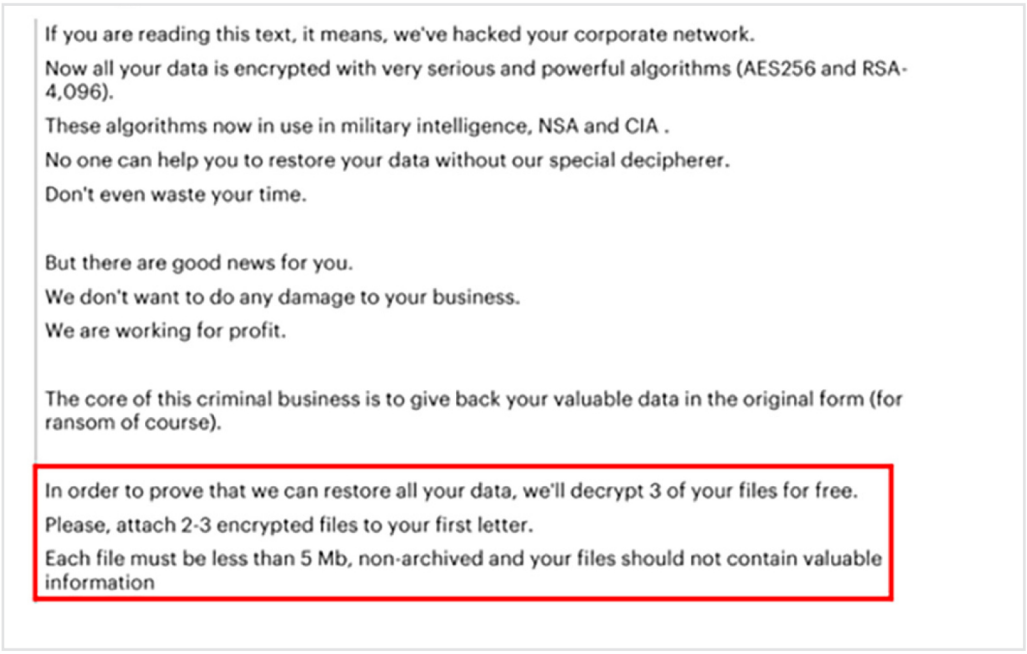
We exclusively have decryption software for your situation

DO NOT RESET OR SHUTDOWN - files may be damaged.
DO NOT RENAME the encrypted files.
DO NOT MOVE the encrypted files.
This may lead to the impossibility of recovery of the certain files.

The payment has to be made in Bitcoins.
The final price depends on how fast you contact us.
As soon as we receive the payment you will get the decryption tool and instructions on how to improve your systems security

To get information on the price of the decoder contact us at:

圖20：MegaCortex 勒贖通知


If you are reading this text, it means, we've hacked your corporate network.
Now all your data is encrypted with very serious and powerful algorithms (AES256 and RSA-4,096).
These algorithms now in use in military intelligence, NSA and CIA .
No one can help you to restore your data without our special decipherer.
Don't even waste your time.

But there are good news for you.
We don't want to do any damage to your business.
We are working for profit.

The core of this criminal business is to give back your valuable data in the original form (for ransom of course).

In order to prove that we can restore all your data, we'll decrypt 3 of your files for free.
Please, attach 2-3 encrypted files to your first letter.
Each file must be less than 5 Mb, non-archived and your files should not contain valuable information

感染媒介

目標式勒索軟體攻擊集團使用形形色色的散布方法。由於目標式勒索軟體攻擊的盛行率相對較低，因此有時很難建立感染媒介。目標式勒索軟體攻擊集團通常會運用它們的方法從間諜團體那裡獲取線索，以在受害者的網路上獲得立足點。

網路釣魚

網路釣魚是使用最廣泛的感染媒介之一，藉由偽裝為例行信件或與工作相關的信件（發票、出貨通知等）發送給員工的電子郵件。一些網路釣魚活動以無差別方式，對屬意的受害者傳送大量惡意電子郵件。在其他情況下，攻擊者可能會預先選擇他們的受害者並向組織中選定的員工發送魚叉式網路釣魚電子郵件。

魚叉式網路釣魚活動可以配合目標的屬性或偏好量身定制，使用與組織業務相關的主旨。如果收件人被引誘開啟惡意附件或使用惡意連結，惡意軟體將下載到受害者的機器上，從而允許攻擊者開始在受害者的網路中移動。

惡意廣告

這算是一種尚未被公開的感染媒介。WastedLocker 加密勒索的運營商已在 2020 年利用惡意廣告作為勒索軟體的感染媒介。該組織已被觀察到入侵破壞媒體網站，以提供惡意廣告，其中包含一個名為 SocGholish 且偽裝為軟體更新的的 JavaScript 型框架。

漏洞刺探利用

進入組織網路的另一條途徑是攻擊在公開伺服器上執行的易受攻擊軟體。迄今為止，在大多數情況下，尚未使用零日漏洞，攻擊者利用未修補軟體（如 JBoss 或 Apache Web 服務器）中的已知漏洞。這種戰術的主要用戶之一是現已解散的 SamSam 組織，該組織於 2019 年 11 月停止運營。

二度傷害感染

這正成為入侵受害者組織日益流行的途徑。網路犯罪分子正在利用原先已存在殭屍網路的傀儡／殭屍電腦來在受害者的網路上取得立足點。只需讓網路上的一台電腦受到殭屍網路的攻陷，即可提供進入的途徑。

BitPaymer 幕後的攻擊者利用他們自己的 Dridex 殭屍網路，該網路最初是為發動金融攻擊而構建的，為他們提供了一種能夠傳送勒索軟體到達組織的方法。

同時，Ryuk、GoGalocker 和 MegaCortex 幕後的 Miner 組織也使用 Emotet 殭屍網路發動攻擊，並可能從 Emotet 的運營商那裡租用了存取權限。

不安全的服務

入侵不安全的服務是另一個感染媒介。曾多次觀察到 Crysis（也稱為 Dharma）透過不安全的 RDP 服務攻擊組織，利用的方式是洩露或弱憑證 (帳密)。現已解散的 GandCrab 小組被觀察到在網際網路上掃描暴險的 MySQL 資料庫，然後它會感染惡意軟體。

憑證竊取與橫向移動

目標式勒索軟體攻擊可以分為四個主要階段：初始入侵、權限提升／憑證 (帳密) 盜取、橫向移動和加密／刪除備份。

橫向移動是一個關鍵階段。從攻擊者的角度來看，被加密的電腦比例越高，受害者願意支付贖金的可能性就越大。

勒索軟體攻擊者往往從間諜參與者那裡獲取線索，並在橫向移動這個階段，部署一系列類似的戰術和工具。為了降低被偵測到的風險，許多（但不全然）攻擊者開始改變戰術，擴大選用的工具種類，且不再仰賴傳統的惡意程式攻擊工具組和零時差漏洞。「自給自足」(living off the land) 並不是新技術，且越來越多團體均加以採用，使用各種作業系統內建功能、合法工具及雲端服務來入侵網路。這種戰術讓攻擊更難以被偵測，因為相較於惡意程式，更難找出合法工具的惡意用途。

最常用的兩用工具包括：

- **PowerShell**：Microsoft 程序檔編寫工具，可用於運行命令以下載酬載 (Payloads)、在入侵網路周遊，並執行偵察行動。
- **PsExec**：由 Microsoft Sysinternals 提供的遠端指令功能工具，可在其他系統執行程序。該工具主要被攻擊者用來在受害者網路上橫向移動。
- **PsInfo**：另一個 Microsoft Sysinternals 工具，允許用戶收集有關網路上其他電腦的 Windows 系統的資訊。
- **Windows Management Instrumentation(WMI)**：Microsoft 命令列工具，是一項核心的 Windows 管理技術；使用者可以使用 WMI 管理本機和遠端電腦。
- **Mimikatz**：免費提供的工具，能夠根據配置以明文形式更改權限、取得憑證和恢復 Windows 密碼。
- **Cobalt Strike**：「現貨商品」的惡意程式，可用於執行命令、注入其他程序 (processes)、提升當前程序或模擬其他程序以及上傳和下載檔案。它還可用於使用 ProcDump 執行憑證傾倒（credential dumping）。
- **Metasploit**：滲透測試框架，允許用戶在遠端系統上執行漏洞利用並提供酬載 (Payload)。
- **AnyDesk**：合法的、公開可用的遠端桌面工具。
- **PuTTY**：是知名的 Windows 開源的 SSH 命令列管理工具，可以使用 Putty 進行 SSH 遠端連線，當然也可以使用 Putty 建立遠端存取將資料傳到外部伺服器。

結論

百家爭鳴的勒索軟體集團，大量採用包括資料盜竊和加密在內的的創新戰術，這種「雙重敲詐勒索軟體」的目標式攻擊，意味著對組織構成更殘酷的威脅。數百萬美元的贖金要求現在已經是「行情價」，即使是不願支付贖金的組織也會面臨更嚴重的清理成本和聲譽損失。

縱深防禦是阻止此類攻擊的關鍵，了解大多數駭客集團採用的攻擊鏈將有助於確定安全優先等級。將 EDR 解決方案與 Endpoint Protection 相結合，可以最大限度地提高在部署酬載 (Payload) 之前發現網路上可疑活動的機率。

保護

賽門鐵克採取了以下保護措施來保護客戶免受這些攻擊：

檔案型防護

賽門鐵克會隔離下列類型的檔案型的風險：

- Ransom.Maze
- Ransom.Sodinokibi
- Ransom.BitPaymer
- Ransom.WastedLocker
- Ransom.Ryuk
- Ransom.Crysis
- Ransom.GoGalocker
- Ransom.MegaCortex
- Ransom.Robbinhood
- Hacktool.Mimikatz
- Backdoor.Cobalt(Cobalt Strike)
- Trojan.Agentemis(Cobalt Strike)

AI 型防護

賽門鐵克的目標性攻擊雲端分析（賽門鐵克 Endpoint Security Complete 產品的一部分）利用進階機器學習來找出與目標性攻擊相關聯的活動模式。

威脅獵手

賽門鐵克的威脅獵手團隊 (Threat Hunter)（賽門鐵克 Endpoint Security Complete 產品的一部分）積極分析雲端分析警報並調查潛在的關鍵事件。2020 年 6 月，威脅獵手團隊最早發現了數十個早期階段的 WastedLocker 攻擊，並能夠在攻擊者部署其酬載 (Payload) 之前通知受影響的組織。

端點偵測和回應 (EDR)

Symantec EDR 具有攻擊鏈緩解 (ACM：Attack Chain Mitigation) 功能，可提供增強的早期預防功能。EDR 專注於行為而不是檔案，而且可以加強魚叉式網路釣魚的防禦和就地取材工具的使用。例如，如果 Word 通常不會在客戶環境中啟動 PowerShell，則這應該進入「攔截」模式。EDR 的 UI 可讓客戶輕鬆地瞭解常見且應該允許的行為、可見但仍應該發出警示的行為，以及不常見且應該攔截的行為。您也可以被動地處理缺口，作為調查和回應資安事端警示的一部分。資安事端警示將會顯示所有已觀測為缺口的行為，並提供功能讓這立即從資安事端詳細資料頁面進入攔截模式。

緩和勒索軟體的最佳實務準則

賽門鐵克建議用戶遵循以下最佳做法來防範目標式勒索軟體攻擊：

保護本機環境

- **確保您擁有最新版本的 PowerShell**，並且已啟用記錄功能。
- **限制對 RDP 服務的存取。**僅允許來自特定已知 IP 位址的 RDP，並確保您正在使用多重驗證。使用「檔案伺服器資源管理員 (SRM)」，鎖定在需要使用者寫入存取權的檔案共用上寫入已知勒索程式延伸的功能。
- **從檔案伺服器資源管理員 (FSRM)** 在使用者需要存取的共用資料夾內，鎖定／限制已知勒索病毒附檔名的寫入能力 (如果您有使用 Symantec SEP，則可使用該內建的應用程式控管功能，更簡單)。
- **建立計畫以考量外部方的通知。**若要確保正確地通知到必要組織 (例如：FBI 或其他法律執行機構／機關)，請務必制定驗證計畫。
- **建立一個仿效戰爭時「jump bag：跳袋」概念的機制，裡面同時存放所有關鍵管理資訊的紙本拷貝和電子檔備份。**為了防止這些關鍵資訊的可用性受到影響，將其與排除故障所需的硬體和軟體一起存放在一個跳袋中。當存放在網路的檔案被加密時，這些資訊也一樣化為烏有。「跳袋」一詞在第二次世界大戰期間一直用於傘兵。他們必須將任何落在敵後需要使用的東西塞進一個袋子裡。
- **對管理帳戶的使用實施適當的稽核和控制。**您還可以為管理工作實施一次性憑證，以幫助防止盜竊和使用管理憑證。
- **建立管理工具使用情況的設定檔。**攻擊者使用其中多種工具，在透過網路橫向移動時不被偵測到。如果使用者帳戶具有以 admin 身分在少量系統上使用 PsInfo/PsExec 執行的記錄，則可能很好，但在所有系統上執行 PsInfo/PsExec 的服務帳戶都是可疑的。

保護電子郵件系統

- **啟用雙重驗證 (2FA)**，防止在網路釣魚攻擊期間危害憑證。
- **強化電子郵件系統周圍的安全架構**，最大限度地減少到達一般使用者收件匣的垃圾郵件數量，並確保您遵循電子郵件系統的最佳實務準則，包括對網路釣魚攻擊使用 SPF 和其他防禦方法。

進行備份

- 定期備份用戶端和伺服器上的檔案。您可以在電腦離線時備份檔案，或是使用網路電腦和伺服器無法寫入的系統。如果您沒有專用的備份軟體，也可以將重要檔案複製到抽取式媒體。然後退出並拔掉抽取式媒體；不要讓抽取式媒體持續插著。
- **對備份複本實作異地儲存。**安排至少有四週異地儲存、每週完整和每日增量備份。
- **實作現場離線備份。**確保您的備份未連線至網路，以防止勒索軟體將它們進行加密。最好在系統關閉網路時進行移除，以防止任何潛在的威脅散佈。
- **確認並測試伺服器層級備份解決方案。**這應該已是災難復原程序的一部分。
- **提高備份檔和備份資料庫的檔案層級的安全等級。**可避免已被備份的檔案及資料庫被加密。
- **測試還原功能。**確保還原功能支援業務需求。
- 用密碼和存取控制限制保護對應網路磁碟機，來鎖定這些磁碟機。
- 對網路磁碟機上的檔案，使用唯讀存取權，除非絕對需要擁有這些檔案的寫入存取權。限制使用者權限可限制威脅可以加密哪些檔案。

附錄 1：躲藏時間分析

躲藏時間是攻擊者初始存取受害者環境到嘗試執行勒索軟體酬載 (Payload) 之間的時間。這提供了有關攻擊者在加密受害者資料之前在網路上花費了多少時間的數據。從理論上講，這一段時間是受害者在成為勒索軟體受害者之前找出活動的最後機會，並提供有關攻擊者在最終攻擊階段之前需要花費多少時間暫存環境的額外數據。我們分析了五個不同勒索軟體家族的攻擊，其中我們有關於初始入侵和嘗試執行酬載 (Payload) 的日期的資料。

勒索軟體	躲藏時間 (天)
Ryuk	14 天
BitPaymer	5 天
Maze	14 天
Sodinokibi	8 天
GoGalocker	2 天

附錄 2：MITRE ATT&CK® 技術手法列表

目標式勒索軟體攻擊運營商使用了以下 Mitre ATT&CK 技術清單：

團體	技術 ID	技術手法名稱	技術運用
Ryuk	T1134	訪問令牌操作	Ryuk 已嘗試調整其令牌權限以擁有 SeDebugPrivilege。
Ryuk	T1547	引導或登錄自動啟動執行	Ryuk 已使用 Windows 命令行在 HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run 下創建註冊表項以建立持久性。
Ryuk	T1059	命令和腳本解釋器	Ryuk 已使用 cmd.exe 創建註冊表項以建立持久性。
Ryuk	T1486	為影響而加密的數據	Ryuk 使用對稱 (AES) 和非對稱 (RSA) 加密的組合來加密文件。文件已使用其自己的 AES 密鑰加密，並賦予文件擴展名 .RYK。 加密目錄已將 RyukReadMe.txt 的贖金記錄寫入該目錄。
Ryuk	T1083	檔案和目錄搜尋	Ryuk 已調用 GetLogicalDrives 來枚舉所有已安裝的驅動器，並調用 GetDriveTypeW 來確定驅動器類型。
Ryuk	T1562	削弱防禦	Ryuk 已停止與防病毒相關的服務。
Ryuk	T1490	禁止系統恢復	Ryuk 使用 vssadmin Delete Shadows /all /quiet 來刪除卷影副本，並使用 vssadmin 調整 shadowstorage 的大小來強制刪除由第三方應用程序創建的捲影副本。
Ryuk	T1036	偽裝	Ryuk 通過調用 GetWindowsDirectoryW 然後在路徑的第四個字符處插入一個空字節來構建合法的出現安裝文件夾路徑。 對於 Windows Vista 或更高版本，路徑將顯示為 C:\Users\Public。
Ryuk	T1106	原生 API	Ryuk 使用了多個原生 API，包括 ShellExecuteW 來運行可執行文件，GetWindowsDirectoryW 來創建文件夾，以及 VirtualAlloc、WriteProcessMemory 和 CreateRemoteThread 用於程序注入。
Ryuk	T1057	程序發現	Ryuk 調用了 CreateToolhelp32Snapshot 來枚舉所有正在運行的程序。

團體	技術 ID	技術手法名稱	技術運用
Ryuk	T1055	程序注入	Ryuk 將自身注入遠程程序以使用 VirtualAlloc、WriteProcessMemory 和 CreateRemoteThread 的組合來加密檔案。
Ryuk	T1489	停止服務	Ryuk 調用 kill.bat 來停止服務、停用服務和終止程序。
Ryuk	T1016	系統網路配置偵測	Ruk 調用 GetIpNetTable 以標識具有 Address Resolution Protocol (ARP) 記錄的所有掛載磁碟和主機。
Maze	T1071	應用層通訊協定	Maze 經由 HTTP 與複雜編碼的 IP 位址進行通訊。
Maze	T1059	命令和腳本解譯器	Maze 加密過程使用了帶有各種命令的批次處理腳本。
Maze	T1486	資料加密的影響	Maze 通過加密目標機器上的檔案來破壞系統，聲稱如果支付贖金就可以解密文件。 Maze 使用了基於 Salsa20 的 ChaCha 演算法和 RSA 演算法來加密檔案。
Maze	T1568	動態分辨率	Maze 在與 C2 建立連接時以包含“forum”、“php”、“view”等可能性列表中隨機選擇偽造 POST 字串，阻礙檢測工作。
Maze	T1562	削弱防禦	Maze 已停用包括 IDA 調試器、x32dbg 和 OllyDbg 等動態分析和其他安全工具。
Maze	T1070	主機上的指標刪除	Maze 在嘗試刪除卷影后使用了“Wow64RevertWow64FsRedirection”函數，以使系統保持重定向前的狀態。
Maze	T1490	禁止系統復原	Maze 嘗試在加密過程之前和之後刪除受感染電腦的備份快照。
Maze	T1106	原生 API	Maze 在整個加密過程中使用了多個 Windows API 函數，包括 IsDebuggerPresent、TerminateProcess、Process32FirstW 等。
Maze	T1027	混淆的檔案或訊息	Maze 在加密過程中解密字串與其他重要訊息。 Maze 還會動態調用某些函數來阻礙分析。
Maze		二進制填充	Maze 插入了大量垃圾代碼，其中包括一些用於解密字串和其他重要訊息的元件，以便稍後在加密過程中使用。
Maze	T1057	程序偵測	Maze 收集了所有正在執行的系統程序。
Maze	T1055	程序注入	Maze 將惡意軟體 DLL 注入目標程序。
Maze	T1082	系統訊息偵測	Maze 使用“GetUSerDefaultUILanguage”功能檢查受感染系統的語言。
Maze	T1049	系統網路連線偵測	Maze 使用“WNetOpenEnumW”、“WNetEnumResourceW”、“WNetCloseEnum”和“WNetAddConnection2W”函數來列出受感染電腦上的網路資源。
Maze	T1047	Windows 管理規範	Maze 使用“wmic.exe”試圖刪除電腦上的備份快照。
RobbinHood	T1059	命令和腳本解譯器	RobinHood 在受害者的電腦上使用 cmd.exe。
RobbinHood	T1486	資料加密的影響	RobinHood 搜尋 RSA 加密密鑰，然後對系統檔案進行加密。
RobbinHood	T1562	削弱防禦	RobinHood 在系統上搜尋與防毒軟體相關的 Windows 服務並終止該程序。
RobbinHood	T1070	刪除主機上的指標	RobinHood 使用 net use * /DELETE /Y 命令中斷電腦上的所有網路共用。

團體	技術 ID	技術手法名稱	技術運用
RobbinHood	T1490	禁止系統復原	RobinHood 刪除備份快照以確保所有資料無法輕易恢復。
RobbinHood	T1489	服務停止	RobinHood 在開始加密過程之前停止系統上的 181 個 Windows 服務。
SamSam	T1059	命令和腳本解譯器	SamSam 使用自定義批次處理腳本來執行某些元件。
SamSam	T1486	資料加密的影響	SamSam 使用 RSA-2048 加密受害者的檔案，並要求以比特幣支付贖金以解密這些檔案。
SamSam	T1070	刪除主機上的指標	SamSam 刪除自己的檔案和有效載荷，以使分析攻擊更加困難。
SamSam	T1027	混淆的檔案或訊息	SamSam 使用 AES 或 DES 來加密有效載荷和有效載荷元件。
GoGalocker	T1531	刪除存取帳戶	已觀察到 GoGalocker 更改帳戶密碼並登出當前用戶。
GoGalocker	T1486	資料加密的影響	GoGalocker 使用 RSA-OAEP MGF1 加密檔案，包括 Windows 作業系統核心檔案，然後要求用比特幣支付解密密鑰。
GoGalocker	T1562	削弱防禦	GoGalocker 進行安裝時會先立即執行“task kill”命令以停用防毒軟體。
GoGalocker	T1070	刪除主機上的指標	GoGalocker 在執行後刪除其原始啟動器。
GoGalocker	T1570	橫向工具轉移	GoGalocker 透過 SMB 在受害者網路中移動，這表明該勒索軟體背後的參與者正在手動將檔案在電腦間複製，而不是自我傳播。
GoGalocker	T1553	顛覆信任控制	GoGalocker 使用被盜憑證進行簽章，以使其看起來更合法。
GoGalocker	T1529	系統關閉 / 重啟	觀察到 GoGalocker 會關閉受感染的系統。