BlackMatter(*黑物質)：被用於先進攻擊的創新資料滲透工具

2021 年 11 月 1 日發布｜威脅情報

威脅獵手團隊
賽門鐵克

自訂工具的開發指出了勒索軟體攻擊者正試圖提高攻擊速度。

BlackMatter (*黑物質) 勒索軟體集團至少一個關聯／附屬公司，已經開始在其攻擊行動中使用了自定義的資料滲透工具。由賽門鐵克威脅獵手團隊發現 Exmatter (*外物質) 的功能是設計用來從選定多個目錄中竊取特定類型的檔案，並在受害者網路中部署勒索軟體之前，將其上傳到攻擊者控制的伺服器。

這是繼早些時候發現與 LockBit 勒索軟體營運相關 Ryuk 竊盜工具和稱為 StealBit 新增竊密功能的進化版後，勒索軟體運營商第三次開發的自定義資料滲透工具。

運轉中的 Exmatter(* 外物質)

Exmatter (*外物質) 是基於 .NET 編譯並經混淆的可執行檔。運行時，它會檢查其命令列參數，以尋找以下字串："nownd"和"-nownd"。如果發現其中任何一個，它會試圖利用呼叫「ShowWindow」API 來隱藏自己的視窗，如下所示：

- ShowWindow(Process.GetCurrentProcess().MainWindowHandle, 0);

為了識別用於滲透的檔案，它將檢索受感染計算機上所有磁碟，並收集所有檔案路徑名稱，而略過下列目錄內的所有內容：

- C:Documents and Settings
- C:PerfLogs
- C:Program FilesWindows Defender Advanced Threat ProtectionClassificationConfiguration
- C:Program FilesWindowsApps
- C:ProgramDataApplication Data
- C:ProgramDataDesktop
- C:ProgramDataDocuments
- C:ProgramDataMicrosoft
- C:ProgramDataPackages
- C:ProgramDataStart Menu
- C:ProgramDataTemplates
- C:ProgramDataWindowsHolographicDevices

- C:Recovery
- C:System Volume Information
- C:UsersAll Users
- C:UsersDefault
- C:UsersPublicDocuments
- C:Windows

它還將排除大小小於 1，024 位元組的檔案和具有以下屬性的檔案也會被排除：

- FileAttributes.System
- FileAttributes.Temporary
- FileAttributes.Directory

只會滲透下列表列的類型檔案：

- .doc
- .docx
- .xls
- .xlsx
- .pdf
- .msg
- .png
- .ppt
- .pptx
- .sda
- .sdm
- .sdw
- .csv

它試圖利用「最後寫入時間」屬性對檔案進行排序以進行滲透優化。
然後，使用以下參數將符合條件的檔案上傳到遠端安全檔案傳輸協定伺服器(SFTP)：

- Host: 165.22.84.147
- Port: 22

Exmatter還包括SOCKS5 配置，但未使用：

- Host: 10.26.16.181
- Port: 1080

當它完成滲出資料後，Exmatter 開始以下列程序刪除其任何自身痕跡：

- Filename: "powershell.exe"

- Arguments:
  - -WindowStyle Hidden -C $path = '[FILEPATH_OF_THE_EXECUTING_SAMPLE]';Get-Process | Where-Object {$_.Path -like $path} | Stop-Process -Force;[byte[]]$arr = new-object byte[] 65536;Set-Content -Path $path -Value $arr;Remove-Item -Path $path;

此舉將試圖在刪除檔案之前覆蓋檔案的初始部分，讓災後復原變得更困難。

最新的變種

已找到 Exmatter (*外物質) 的多個變種，意味著攻擊者持續改進該工具，以便在最短的時間內竊取最多高價值的檔案。

在第二個變種中，原先在排除清單的“C:\Program Files\Windows Defender Advanced Threat Protection\Classification\Configuration”目錄，已經被“C:\Program Files\Windows Defender Advanced Threat Protection" 這個目錄所取代。而檔案類型「.xlsm」和「.zip」也被添加到包含清單中。

第三個版本的註釋添加了 WebDav 用戶端。程式碼結構表明，SFTP 仍然是首選的協定，WebDav 充當備胎。WebDav 用戶端使用以下網址：

- https://157.230.28.192/data/

除此之外，Exmatter 還被配置為跳過對包含以下任何字串的名稱的檔案的滲透：

- .json
- .config
- .ts
- .cs
- .js
- .aspx
- .pst

除此之外，Exmatter 還被配置為跳過對包含以下任何字串的名稱的檔案的滲透：

- OneDriveMedTile
- locale-
- SmallLogo
- VisualElements
- adobe_sign
- Adobe Sign
- core_icons

第四個變種包含更新的 SFTP 伺服器詳細資訊：

- Host: 159.89.128.13
- Port: 22

WebDav 用戶端使用以下更新的 URL：

- https://159.89.128.13/data/

最後的變動是，將 .png 檔案也排除在包含的檔案清單列表之外。

資深的勒索軟體營運商

BlackMatter (*黑物質) 與Coreid (*科裡德) 網路犯罪集團有關，後者以前主導 Darkside (*暗側) 勒索軟體。在過去的 12 個月裡，它一直是最令人膽顫心驚、恨之入骨的目標式勒索軟體集團之一，其工具已被用於一些野心更大的攻擊，最明顯是 2021 年 5 月發動對美國能源關鍵基礎設施--殖民地管道的 Darkside (*暗側) 攻擊，導致東岸燃油供應一度中斷。

Coreid 在勒索軟體及服務 (RaaS) 的模式下運營，與附屬 (關聯／分紅) 公司合作進行勒索軟體攻擊的分工，然後從中分得一部分利潤。與大多數勒索軟體參與者一樣，與 Coreid 相關攻擊竊取了受害者的資料，然後該組織威脅要公佈這些資料，以進一步迫使受害者支付贖金要求。Exmatter 竊密工具是 Coreid 本身所建立還是其附屬 (關聯／分紅) 公司自行建立還有待觀察，但其發展表明，資料盜竊和勒索仍然是該集團的核心重點。

保護／緩解措施

有關最新的防護更新，請參考最新賽門鐵克防護公告。

入侵 / 感染指標 (IOC:Indicators of Compromise)

325ecd90ce19dd8d184ffe7dfb01b0dd02a77e9eabcb587f3738bcfbd3f832a1
5e355f90b398cbb54829038c6e5d68e8c578405d142bdcc2386cf6161c8d7014
8eded48c166f50be5ac33be4b010b09f911ffc155a3ab76821e4febd369d17ef
b6bc126526e27c98a94aab16989864161db1b3a75f18bd5c72bacbdfccad7bd7
fcaed9faa026a26d00731068e956be39235487f63e0555b71019d16a59ea7e6b
157.230.28.192
159.89.128.13
165.22.84.147

原廠網址：https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/blackmatter-data-exfiltration
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。2021/11

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。

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