Noberus：技術分析顯示了基於 Rust 的新勒索軟體的複雜性

2021 年 12 月 16 日發布｜威脅情報

威脅獵手團隊
賽門鐵克

在 11 月中旬的攻擊中使用的新勒索軟體，ConnectWise 可能是感染媒介。

賽門鐵克的威脅獵手團隊提供上周新出現的有關於 ALPHV／BlackCat 勒索軟體的其他技術資訊，且已經追蹤了幾周。

賽門鐵克是全球網通晶片巨擘：博通 (Broadcom 美國股票代碼：AVGO) 的企業安全部門，我們的研究人員追蹤勒索軟體 Ransom.Noberus，並於 2021 年 11 月 18 日在受害者組織上首次發現了它，攻擊者在攻擊過程中部署了三種 Noberus 變種。這似乎表明，這種勒索軟體比以前報導發現時更早，MalwareHunterTeam 告訴 *BleepingComputer*，他們於 11 月 21 日首次看到這種勒索軟體。

Noberus 是一個與眾不同的勒索軟體，因為它是使用 Rust 程式語言來撰寫，這是我們第一次看到使用這種程式語言撰寫，專業等級的全新勒索軟體已經進行實際的攻擊。Noberus 似乎執行現在典型的雙重勒索軟體攻擊，他們首先從受害者網路竊取資訊，然後再加密檔案。Noberus 將 .sykffle 副檔名新增到被加密檔中。

此部落格包含有關我們在一個受害者組織中觀察到的攻擊鏈資訊，以及有關此勒索軟體運作技術的詳細資訊。

賽門鐵克觀察到第一個可疑活動發生在 11 月 3 日，大約在 Noberus 部署前兩周發生在受害者的網路上。在此期間，觀察到可疑的網路活動。後來在 11 月 18 日，在 Noberus 部署前不久，ConnectWise 也被執行。幾個小時後，Noberus 被部署，這表明攻擊者可能已經利用對 ConnectWise 的存取許可權來部署其有效籌載。雖然它是一個合法的工具，但 ConnectWise 最近經常被勒索軟體攻擊者利用來存取受害者網路。

拆解攻擊手法

11 月 3 日，在最早被感染的受害者網路的電腦上發生了可疑的伺服器訊息區塊 (SMB) 請求。隨後是來自網路上的遠端區域安全認證子系統服務 (LSA) 登錄檔傾印嘗試。這意味著攻擊者可能已經破壞了網路上我們無法查看的另一台電腦，或者他們還也可能在發起攻擊傾印憑證的網域中新增電腦。

同一天，PsExec 也從遠端電腦執行以啟動命令提示字元。攻擊者使用它透過 Windows 登錄檔停用了稱為「受限管理員模式」的遠端受限管理功能。這有效地停用防止針對遠端桌面協定 (RDP)「傳遞雜湊 (pass-the-hash)」攻擊的保護措施，進而讓攻擊者嘗試獲得更高的管理權限。

- *reg add HKLMSYSTEMCurrentControlSetControlLsa /v DisableRestrictedAdmin /t REG_DWORD /d 0*

下一個活動發生在 11 月 18 日，當時 PsExec 被用來執行多個 PowerShell 命令並有效地停用 Windows Defender 防護。具體而言，PowerShell 命令將 *.exe 新增到病毒掃描的排外清單中，並且此命令套用在整個組織中執行。

11 月 18 日稍後，Noberus 勒索軟體的第一個實例透過 PsExec 部署。

為了讓 Noberus 能夠正確執行，它需要一個特定的「存取權杖 (Access Token)」。這是在存取 Noberus 營運商的 Tor 網站時區分受害者的唯一密鑰。觀察到正在執行以下類似的命令：

- *CSIDL_WINDOWStemppsexec.exe -accepteula [REDACTED] -u [REDACTED] -p [REDACTED] -s -d -f -c [REDACTED].exe --access-token [REDACTED] --no-prop-servers [REDACTED] --propagated*
- *[REDACTED].exe --access-token [REDACTED] --no-net*

在上面，PsExec 是使用以下特定的命令列參數啟動的：

- s -- 以系統帳號執行
- d -- 以非互動模式執行（不等待程序終止）
- f, c -- 將 Noberus 檔案複製到遠端電腦

對於上面第二個命令，「no-net」命令列參數指定 Noberus 在傳播過程中不要處理網路共用。有關支援命令列參數及其說明的完整清單，請參閱下面的技術詳細資訊。

在我們有權存取的所有 Noberus 範例中，受害者管理憑證都嵌入作為設定的一部份，表明此攻擊專門針對此受害者。

執行 Noberus 後，勒索軟體首先會刪除任何可用的磁碟陰影複製（這在勒索軟體攻擊中很常見），以阻止組織還原加密檔案。

- *cmd /c vssadmin.exe delete shadows /all /quiet*

然後 Noberus 執行命令以透過 WMIC 收集系統資訊，以便從每台電腦收集通用唯一辨識碼 (UUID)。然後這些用於生成「存取令牌」，該令牌構成受害者被指示存取唯一 Tor 位址的一部分。

- *Navigate to: http://mu75ltv3lxd24dbyu6gtvmnwybecigs5auki7fces437xvvflzva2nqd.onion/?access-key=${ACCESS_KEY}"*

我們還看到 Noberus 執行一個 fsutil 命令。Fsutil 執行與檔案配置表 (FAT) 和 NTFS 檔案系統相關的任務。在此事件中，攻擊者特別修改 SymLink 評估行為，並修改可在系統上建立的符號連結類型 (Symbolic links)。符號連結 (Symbolic links) 在目錄中建立一個檔案，該檔案作為另一個檔案或資料夾的捷徑方式。

- *cmd /c fsutil behavior set SymlinkEvaluation R2L:1*
- *cmd /c fsutil behavior set SymlinkEvaluation R2R:1*

此為追蹤各種類型的捷徑方式（本地和遠端），可能確保 Noberus 可以遵循這些捷徑方式並進行加密。

作為傳播機制的一部分，Noberus 嘗試掛載隱藏的分割區。然後，它嘗試透過「net use」命令進行傳播。嵌入的管理憑證與 PsExec 一起作為此機制的一部分，PsExec 以壓縮形式嵌入到 Noberus 中。

在攻擊期間，攻擊者還修改了電腦可透過 PsExec 發出最大同時請求數目(concurrent requests)的限制。

- *cmd /c reg add HKEY_LOCAL_MACHINESYSTEMCurrentControlSetServicesLanmanServerParameters /v MaxMpxCt /d 65535 /t REG_DWORD /f*

這可能有助於 Noberus 在整個網路中的傳播。

在此階段，Noberus 繼續終止一組預定義的程序並開始加密程序。

在攻擊過程中的某個時刻，組織意識到感染並部署了矯正軟體。但儘管如此，攻擊者似乎能夠重新開始並將其勒索軟體的另一種變種，部署到網路上其他系統。在這次入侵期間，總共發現這種勒索軟體的三種變種，導致網路上至少有 261 台電腦染了 Noberus。

Ransom.Noberus：技術細節

對 Noberus 本身技術分析發現，它的很多行為與我們在受害者網路上看到的活動是一致。

在受害者網路上部署後，第一步是刪除卷影副本：

- *cmd /c vssadmin.exe delete shadows /all /quiet*

然後，它會發出命令以從受感染的電腦收集通用唯一標識碼 (UUID)。

- *cmd /c wmic csproduct get UUID*

然後，UUID 和參數「存取令牌」用於生成「ACCESS_KEY」。

- *Navigate to: http://mu75ltv3lxd24dbyu6gtvmnwybecigs5auki7fces437xvvflzva2nqd.onion/?access-key=${ACCESS_KEY}"*

然後，Noberus 啟用遠端到本地和遠端到遠端符號連結評估。

- *cmd /c fsutil behavior set SymlinkEvaluation R2L:1*
- *cmd /c fsutil behavior set SymlinkEvaluation R2R:1*

然後，它嘗試透過發出以下命令來掛載隱藏分區：

- 使用以下指令，列出磁區：
  - *FindFirstVolume*
  - *FindNextVolume*
  - *FindVolumeClose*
- 然後透過以下方式取得路徑名稱：
  - *GetVolumePathNamesForVolumeName*
- 如果磁區沒有路徑名，Noberus 將使用以下命令掛載它：
  - *SetVolumeMountPoint.*

然後，Noberus 清理回收桶並嘗試透過網路共享進行傳播。

它透過使用「net use」命令或 NetShareEnum 函數查找可用共用。然後，使用內嵌管理憑證的方式透過網路共享進行傳播。

Noberus 還試圖透過 PsExec 進行傳播。

- *locker::core::windows::psexec*

PsExec 模組嵌入在 Noberus 程式碼中（參見圖 1）。它用 zlib 壓縮（圖2）。

```
.text:004CEB73                 mov     edx, 1
.text:004CEB78                 lock cmpxchg ds:dword_62E058, edx
.text:004CEB80                 jnz     loc_4CEC17
.text:004CEB86                 mov     eax, ds:Src
.text:004CEB8B                 lea     edx, [esp+1CCh+var_16C+4]
.text:004CEB8F                 mov     dword ptr [esp+1CCh+var_18C+4], 0
.text:004CEB97                 mov     dword ptr [esp+1CCh+var_18C], 0
.text:004CEB9F                 mov     dword ptr [esp+1CCh+var_184], offset PSEXEC_MODULE ; <----------
.text:004CEBA7                 mov     dword ptr [esp+1CCh+var_184+4], 60C0Ah
.text:004CEBAF                 mov     dword ptr [esp+1CCh+var_17C], 0
.text:004CEBB7                 mov     byte ptr [esp+1CCh+var_174+4], 20h ; ' '
.text:004CEBBC                 mov     byte ptr [esp+1CCh+var_17C+4], 4
.text:004CEBC1                 xor     esi, esi
.text:004CEBC3                 mov     dword ptr [esp+1CCh+var_16C], eax
.text:004CEBC7                 mov     dword ptr [edx+4], 0
.text:004CEBCE                 mov     dword ptr [edx], 0
.text:004CEBD4                 mov     dword ptr [edx+9], 0
.text:004CEBDB                 mov     dword ptr [edx+5], 0
.text:004CEBE2                 xor     edx, edx
.text:004CEBE4                 mov     dword ptr [esp+1CCh+var_1B8], eax
.text:004CEBE8                 mov     dword ptr [esp+1CCh+var_1B8+4], 0
.text:004CEBF0                 mov     [esp+1CCh+var_1B0], 0
.text:004CEBF8                 cmp     esi, edx
.text:004CEBFA                 jz      loc_4CF2F7
.text:004CEC00                 jmp     loc_4CF30E
.text:004CEC00 ; ---------------------------------------------------------------------------
.text:004CEC05                 align 10h
.text:004CEC10
.text:004CEC10 loc_4CEC10:                             ; CODE XREF: SELF_PROPAGATION+146A↓j
.text:004CEC10                 pause
.text:004CEC12                 mov     eax, ds:dword_62E058
.text:004CEC17
.text:004CEC17 loc_4CEC17:                             ; CODE XREF: SELF_PROPAGATION+13BB↑j
.text:004CEC17                                         ; SELF_PROPAGATION+13D0↑j
.text:004CEC17                 cmp     eax, 1
.text:004CEC1A                 jz      short loc_4CEC10
.text:004CEC1C                 cmp     eax, 2
.text:004CEC1F                 jnz     loc_4CFD58

000CDF9F 00000000004CEB9F: SELF_PROPAGATION+13EF (Synchronized with Hex View-1)
```

圖 1. 嵌入在勒索軟體程式碼中的 PsExec

```
.rdata:005ACB20                 db  0Ch
.rdata:005ACB21                 db   0
.rdata:005ACB22                 db   0
.rdata:005ACB23                 db   0
.rdata:005ACB24 PSEXEC_MODULE   db 0EDh ; í          ; DATA XREF: SELF_PROPAGATION+13EFto
.rdata:005ACB25                 db 0BDh ; ½
.rdata:005ACB26                 db   9
.rdata:005ACB27                 db  60h ; `
.rdata:005ACB28                 db  54h ; T
.rdata:005ACB29                 db  45h ; E
.rdata:005ACB2A                 db 0F6h ; ö
.rdata:005ACB2B                 db 0E8h ; è
.rdata:005ACB2C                 db 0DDh ; Ý
.rdata:005ACB2D                 db  9Dh
.rdata:005ACB2E                 db  74h ; t
.rdata:005ACB2F                 db  42h ; B
.rdata:005ACB30                 db   3
.rdata:005ACB31                 db  81h
.rdata:005ACB32                 db  0Eh
.rdata:005ACB33                 db  12h
.rdata:005ACB34                 db  20h
.rdata:005ACB35                 db  2Ah ; *
.rdata:005ACB36                 db  4Ah ; J
.rdata:005ACB37                 db  14h
.rdata:005ACB38                 db  50h ; P
.rdata:005ACB39                 db  94h ; ”
.rdata:005ACB3A                 db 0C5h ; Å
.rdata:005ACB3B                 db  40h ; @
.rdata:005ACB3C                 db  58h ; X
.rdata:005ACB3D                 db  12h
.rdata:005ACB3E                 db  12h
.rdata:005ACB3F                 db  20h
.rdata:005ACB40                 db   1
.rdata:005ACB41                 db  12h
.rdata:005ACB42                 db  40h ; @
.rdata:005ACB43                 db   9
.rdata:005ACB44                 db   6
.rdata:005ACB45                 db   2

001AAD24 00000000005ACB24: .rdata:PSEXEC_MODULE (Synchronized with Hex View-1)
```

圖 2. PsExec 由 zlib 在勒索軟體程式碼中壓縮

解壓縮後的 PsExec 檔是一個合法 Microsoft 簽名的乾淨檔（圖3）。

Address	Length	Type	String
.rdata:0045CB68	0000006F	C	The version of the PsExec service running on the remote system is not compabible with this ve...
.rdata:0045CDE8	0000004F	C	PsExec executes a program on a remote system, where remotely executed console\n
.rdata:0045CE38	00000025	C	applications execute interactively.\n
.rdata:0045CE60	000000D3	C	\nUsage: psexec [\\\\computer[,computer2[,...] | @file]][-u user [-p psswd]][-n s][-r servicena...
.rdata:0045CF38	0000004B	C	-a Separate processors on which the application can run with\n
.rdata:0045CF88	00000049	C	commas where 1 is the lowest numbered CPU. For example,\n
.rdata:0045CFD8	00000043	C	to run the application on CPU 2 and CPU 4, enter:\n
.rdata:0045D01C	0000001A	C	\"-a 2,4\"\n
.rdata:0045D038	000000C9	C	-c Copy the specified program to the remote system for\n execution. If you o...
.rdata:0045D108	00000048	C	-d Don't wait for process to terminate (non-interactive).\n
.rdata:0045D150	00000040	C	-e Does not load the specified account's profile.\n
.rdata:0045D190	00000072	C	-f Copy the specified program even if the file already\n exists on the remote sy...
.rdata:0045D208	000000DA	C	-i Run the program so that it interacts with the desktop of the\n specified sessi...
.rdata:0045D2E8	0000004A	C	-h If the target system is Vista or higher, has the process\n
.rdata:0045D338	00000046	C	run with the account's elevated token, if available.\n
.rdata:0045D380	0000004E	C	-l Run process as limited user (strips the Administrators group\n
.rdata:0045D3D0	0000004A	C	and allows only privileges assigned to the Users group).\n
.rdata:0045D420	00000047	C	On Windows Vista the process runs with Low Integrity.\n
.rdata:0045D468	0000004E	C	-n Specifies timeout in seconds connecting to remote computers.\n
.rdata:0045D4B8	0000008E	C	-p Specifies optional password for user name. If you omit this\n you will be pr...
.rdata:0045D548	00000051	C	-r Specifies the name of the remote service to create or interact.\n
.rdata:0045D59C	00000017	C	with.\n
.rdata:0045D5B4	0000003F	C	-s Run the remote process in the System account.\n
.rdata:0045D5F8	0000005C	C	-u Specifies optional user name for login to remote\n computer.\n
.rdata:0045D658	00000092	C	-v Copy the specified file only if it has a higher version number\n or is newer o...
.rdata:0045D6F0	00000047	C	-w Set the working directory of the process (relative to\n
.rdata:0045D738	00000023	C	remote computer).\n
.rdata:0045D760	00000064	C	-x Display the UI on the Winlogon secure desktop (local system\n only).\n
.rdata:0045D7C8	00000047	C	-arm Specifies the remote computer is of ARM architecture.\n
.rdata:0045D810	00000045	C	-priority\tSpecifies -low, -belownormal, -abovenormal, -high or\n

Line 1 of 694

圖 3. 解壓縮的 PsExec 檔

一旦它獲得了對機器的存取許可權，Noberus就會繼續殺死以下程序和服務：

- *"encsvc","thebat","mydesktopqos","xfssvccon","firefox","infopath","winword","steam","synctime", "notepad","ocomm","onenote","mspub","thunderbird","agntsvc","sql","excel","powerpnt", "outlook","wordpad","dbeng50","isqlplussvc","sqbcoreservice","oracle","ocautoupds", "dbsnmp","msaccess","tbirdconfig","ocssd","mydesktopservice","visio", "sql*", "mepocs","memtas","veeam","svc$","backup","sql","vss","msexchange"*

它還會從加密過程中排除某些目錄、檔名和檔案副檔名，例如：

- *"system volume information","intel","$windows.~ws","application data","$recycle.bin", "mozilla","program files (x86)","program files","$windows.~bt","public","msocache","windows","default","all users", "tor browser", "programdata","boot","config.msi","google","perflogs","appdata", "windows.old", "desktop.ini","autorun.inf","ntldr","bootsect.bak","thumbs.db","boot.ini","ntuser.dat", "iconcache.db","bootfont.bin","ntuser.ini","ntuser.dat.log","themepack","nls","diagpkg", "msi","lnk","exe","cab","scr","bat","drv","rtp","msp","prf","msc", "ico", "key","ocx","diagcab","diagcfg", "pdb","wpx","hlp","icns","rom","dll","msstyles","mod","ps1","ics","hta","bin","cmd","ani", "386","lock","cur","idx","sys","com","deskthemepack","shs","ldf","theme","mpa","nomedia", "spl","cpl","adv","icl","msu"*

然後，Noberus 繼續使用 AES 或 ChaCha20 進行檔案加密。

加密電腦的私鑰似乎是隨機生成的。Noberus 似乎使用 BCryptGenRandom 生成一個隨機號碼，並使用圖 4 中所示的字串計算每個位元組。

```
.rdata:0060E3E4 a00010203040506 db '000102030405060708091011121314151617181920212223242526272829303 13'
.rdata:0060E3E4                 db '233343536373839404142434445464748495051525354555657585960616263 64' ; 1/99^2
.rdata:0060E3E4                 db '656667686970717273747576777879808182838485868788899091929394959 69'
.rdata:0060E3E4                 db '79899'
```

圖 4. 用於計算私鑰的字串

已被加密的檔案在其檔名末尾附加了 .sykffle，格式如下：

- *[原始檔名].[原始副檔名].sykffle*

然後 Noberus 會建立一個勒索通知，一個 .txt 和一個向受害者顯示的 .png 圖檔，檔名如下：

- *RECOVER-sykffle-FILES.txt*
- *RECOVER-sykffle-FILES.txt.png*

文字檔告訴受害者以下內容：

> Introduction

Important files on your system was ENCRYPTED and now they have "sykffle" extension.

In order to recover your files you need to follow instructions below.

>> Sensitive Data

Sensitive data on your system was DOWNLOADED and it will be PUBLISHED if you refuse to cooperate.

Data includes:

- Employees personal data, CVs, DL, SSN.

- Complete network map including credentials for local and remote services.

- Financial information including clients' data, bills, budgets, annual reports, bank statements.

- Complete datagrams/schemas/drawings for manufacturing in solidworks format

- And more...

Private preview is published here: http://zujgzbu5y64xbmvc42addp4lxkoosb4tslf5mehnh7pvqjpwxn5gokyd[.]onion/[REDACTED]

>> CAUTION

DO NOT MODIFY FILES YOURSELF.

DO NOT USE THIRD PARTY SOFTWARE TO RESTORE YOUR DATA.

YOU MAY DAMAGE YOUR FILES, IT WILL RESULT IN PERMANENT DATA LOSS.

YOUR DATA IS STRONGLY ENCRYPTED, YOU CAN NOT DECRYPT IT WITHOUT CIPHER KEY.

>> Recovery procedure

Follow these simple steps to get in touch and recover your data:

1) Download and install Tor Browser from: https://torproject.org/

2) Navigate to: http://mu75ltv3lxd24dbyu6gtvmnwybecigs5auki7fces437xvvflzva2nqd[.]onion/?access-key=[REDACTED]

```
Important files on your system was ENCRYPTED.
Sensitive data on your system was DOWNLOADED.
To recover your files and prevent publishing of sensitive information follow
instructions in "${NOTE_FILE_NAME}" file.
```

圖5. Noberus 的勒索通知

這種新勒索軟體彰顯的意義

這是一種複雜的新型勒索軟體，其加密過程看不出來有明顯的破綻，這意味著除非受害者擁有完整的備份，否則他們將不得不支付贖金以恢復其檔案。它是用 Rust 編寫，這很有意思，雖然 Rust 通常不會被惡意軟體開發人員使用，但它越來越受歡迎，這表明勒索軟體開發人員也不怕在這一領域進行創新。

雖然到目前為止，回報這種勒索軟體的受害者數量似乎很少，但 Noberus 本身的複雜性以及我們觀察到的攻擊中攻擊者表現出堅定的決心，我們很可能在未來看到更多這種勒索軟體。另

據報導，這種勒索軟體背後開發人員正在俄語駭客論壇上積極尋找附屬下線機構，這意味著部署這種勒索軟體的惡意行動者的數量可能會增加。

最新防護

賽門鐵克已經於第一時間提供多種有效保護。以下說明為 Symantec 偵測到的惡意程式名稱及有效對應的防護機制：

檔案型 (基於回應式樣本的病毒定義檔) 防護：

- Ransom.Noberus
- Trojan.Gen.2
- Trojan.Gen.MBT
- Trojan.Gen.NPE

基於行為偵測技術(Snoar)的防護：

- SONAR.SuspLaunch!gen4

基於機器學習的防禦技術：

- Heur.AdvML.C
- Heur.AdvML.M

網路層防護：

我們的 Webpulse (網頁脈衝) 網頁自動回饋框架以及其他先進的網路層防護技術，已將其列為如下分類的網頁型攻擊：

- Attack: Ransom.Gen Activity 51

您也可以點擊此處獲取賽門鐵克原廠最新的防護公告 (Protection Bulletins)。

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/noberus-blackcat-alphv-rust-ransomware

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