Noberus: Technical Analysis Shows Sophistication of New Rust-based Ransomware

symantec-enterprise-blogs.security.com/blogs/threat-intelligence/noberus-blackcat-alphv-rust-ransomware

Threat Hunter TeamSymantec

New ransomware used in mid-November attack, ConnectWise was likely infection vector.

Symantec's Threat Hunter Team has additional technical information to share on the new ALPHV/BlackCat ransomware that was first published about last week, and which we have been tracking for several weeks.

Symantec, a division of Broadcom Software, tracks this ransomware as Ransom.Noberus and our researchers first spotted it on a victim organization on November 18, 2021, with three variants of Noberus deployed by the attackers over the course of that attack. This would appear to show that this ransomware was active earlier than was previously reported, with MalwareHunterTeam having told *BleepingComputer* they first saw this ransomware on November 21.

Noberus is an interesting ransomware because it is coded in Rust, and this is the first time we have seen a professional ransomware strain that has been used in real-world attacks coded in this programming language. Noberus appears to carry out the now-typical double extortion ransomware attacks where they first steal information from victim networks before encrypting files. Noberus adds the .sykffle extension to encrypted files.

This blog contains information about the attack chain we observed in one victim organization, as well as technical details about the operation of this ransomware.

The first suspicious activity observed by Symantec occurred on a victim's network on November 3, approximately two weeks before Noberus was deployed. During this time, suspicious network activity was observed. Later on November 18, shortly before Noberus was deployed, ConnectWise was also executed. A few hours later, Noberus was deployed, indicating that the attackers may have leveraged access to ConnectWise to deploy their payload. While it is a legitimate tool, ConnectWise has frequently been exploited by ransomware attackers in recent times to gain access to victim networks.

Anatomy of an attack

On November 3, suspicious Server Message Block (SMB) requests occurred on the earliest machine to get infected on the victim network. This was followed by remote Local Security Authority (LSA) registry dump attempts from a remote machine on the network. This suggests the attackers may have compromised another machine on the network where we didn't have visibility, or they could also have added a new machine to the domain from which they were launching attacks to dump credentials.

On the same day, PsExec was also executed from a remote machine to launch a command prompt. The attackers used this to disable a restricted remote administration feature known as 'RestrictedAdmin mode' via the Windows registry. This effectively disables safeguards guarding against 'pass the hash' attacks targeting Remote Desktop Protocol (RDP), allowing the attackers to attempt to gain higher administrative privileges.

> *reg add HKLM\SYSTEM\CurrentControlSet\Control\Lsa /v DisableRestrictedAdmin /t REG_DWORD /d 0*

The next activity occurred on November 18 when PsExec was used to run multiple PowerShell commands to effectively disable Windows Defender. Specifically, the PowerShell command used added *.exe to an exclusion list for AV scanning, and this command was executed across the entire organization.

Later on November 18, the first instance of Noberus ransomware was deployed via PsExec.

In order for Noberus to execute properly, it requires a specific 'access-token'. This acts as a unique key, which is used to distinguish the victim when visiting the Noberus operators' Tor site. The following similar commands were observed being executed:

- *CSIDL_WINDOWS\temp\psexec.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*

In the above, PsExec is launched with the following specific command line arguments:

- s – Run under the System account
- d – Run as a non-interactive process (don't wait for the process to terminate)
- f, c – Copy Noberus file to the remote machine

For the second command above, the 'no-net' command line argument instructs Noberus not to process network shares during propagation. See the Technical Details below for a full list of support command line arguments and their description.

In all the samples of Noberus that we have access to, the victim's administrative credentials are embedded as part of the configuration block, showing that this attack was specifically targeted at this victim.

Once Noberus is executed, the ransomware first deletes any available shadow copies, which is typical in ransomware attacks, in order to stop the organization from restoring encrypted files.

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

Noberus then runs commands to collect system information via WMIC, in order to collect Universally Unique Identifiers (UUIDs) from each machine. These are then used to generate the 'access token' that makes up part of the unique Tor address victims are instructed to visit.

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

We also saw a fsutil command being executed by Noberus. Fsutil performs tasks that are related to file allocation table (FAT) and NTFS file systems. In this incident, the attacker is specifically modifying the SymLink Evaluation behavior to modify the type of symbolic links that can be created on the system. Symbolic links create a file in your directory that acts as a shortcut to another file or folder.

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

This is used to follow various types of shortcuts (local and remote), likely to ensure Noberus can follow these shortcuts and perform encryption.

As part of the propagation mechanism, Noberus attempts to mount hidden partitions. It then attempts to spread via the 'net use' command. The embedded administrative credentials are used as part of this mechanism along with PsExec, which is embedded in a compressed form within Noberus.

During the attack, the attackers were also seen modifying the maximum limit of concurrent requests machines could make via PsExec.

> *cmd /c reg add HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters /v MaxMpxCt /d 65535 /t REG_DWORD /f*

This was likely to aid in the propagation of Noberus across the network.

At this stage, Noberus proceeds to terminate a set of pre-defined processes and begin the encryption process.

At some point during the attack the organization became aware of the infection and deployed remediation software. However, despite this, it appears the attackers were able to return and deploy another variant of their ransomware to other systems on the network. In total, three variants of this ransomware were identified during this intrusion, leading to at least 261 machines on the network becoming infected with Noberus.

Ransom.Noberus: Technical Details

A technical analysis of Noberus itself found that a lot of its behavior is consistent with the activity we saw on the victim network.

The first step it takes after being deployed on victim networks is to remove shadow copies:

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

It then issues a command to collect Universally Unique Identifiers (UUIDs) from infected machines.

> *cmd /c wmic csproduct get UUID*

The UUID and parameter ‘access token’ are then used to generate "ACCESS_KEY".

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

Noberus then enables the remote-to-local and remote-to-remote symbolic link evaluations.

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

It then attempts to mount a hidden partition, by issuing the following commands:

- *Enumerates volumes by*
  - *FindFirstVolume*
  - *FindNextVolume*
  - *FindVolumeClose*

- *Then gets the pathname by:*
  GetVolumePathNamesForVolumeName
- *If the volume does not have a pathname, Noberus mounts it with:*
  SetVolumeMountPoint.

Noberus then cleans up the Recycle Bin and attempts to propagate via network share.

It looks for available shares by using the ‘net use’ command or NetShareEnum function. Embedded administrative credentials may then be used for propagation via network share.

Noberus also attempts to propagate via PsExec.

locker::core::windows::psexec

The PsExec module is embedded in the Noberus code (*see Figure 1*). It is compressed with zlib (*Figure 2*).

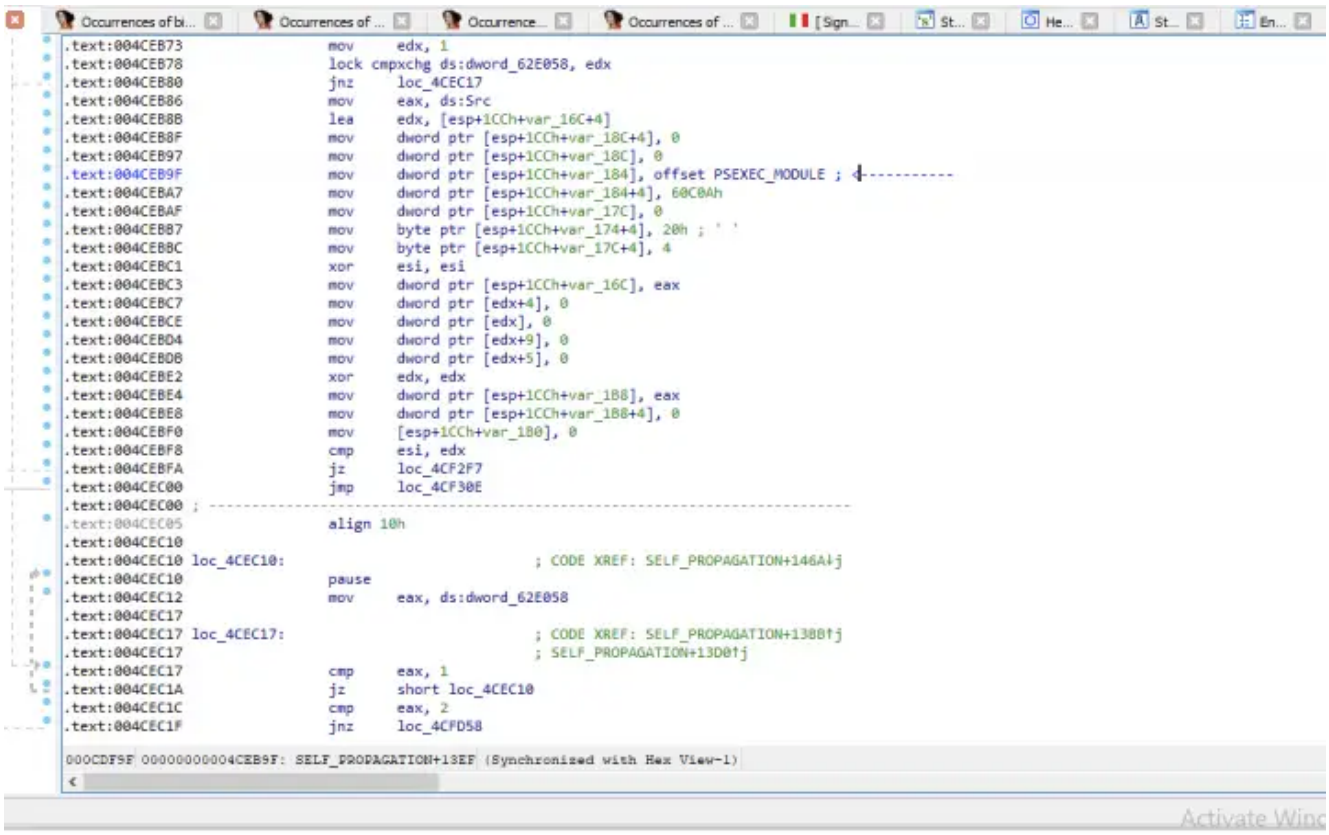

Figure 1. PsExec embedded in ransomware code

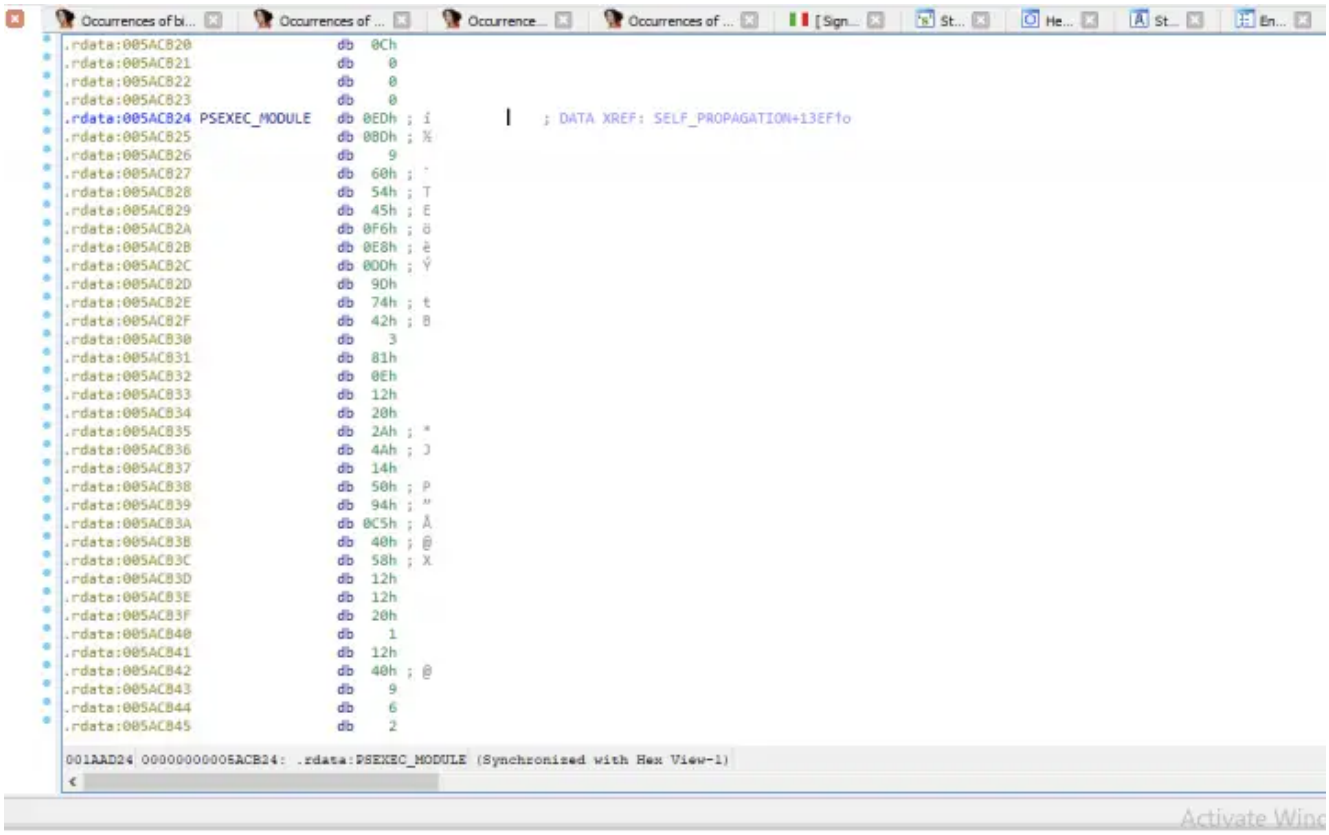

Figure 2. PsExec compressed by zlib in ransomware code

The decompressed PsExec file is a legitimate Microsoft-signed clean file (*Figure 3*).

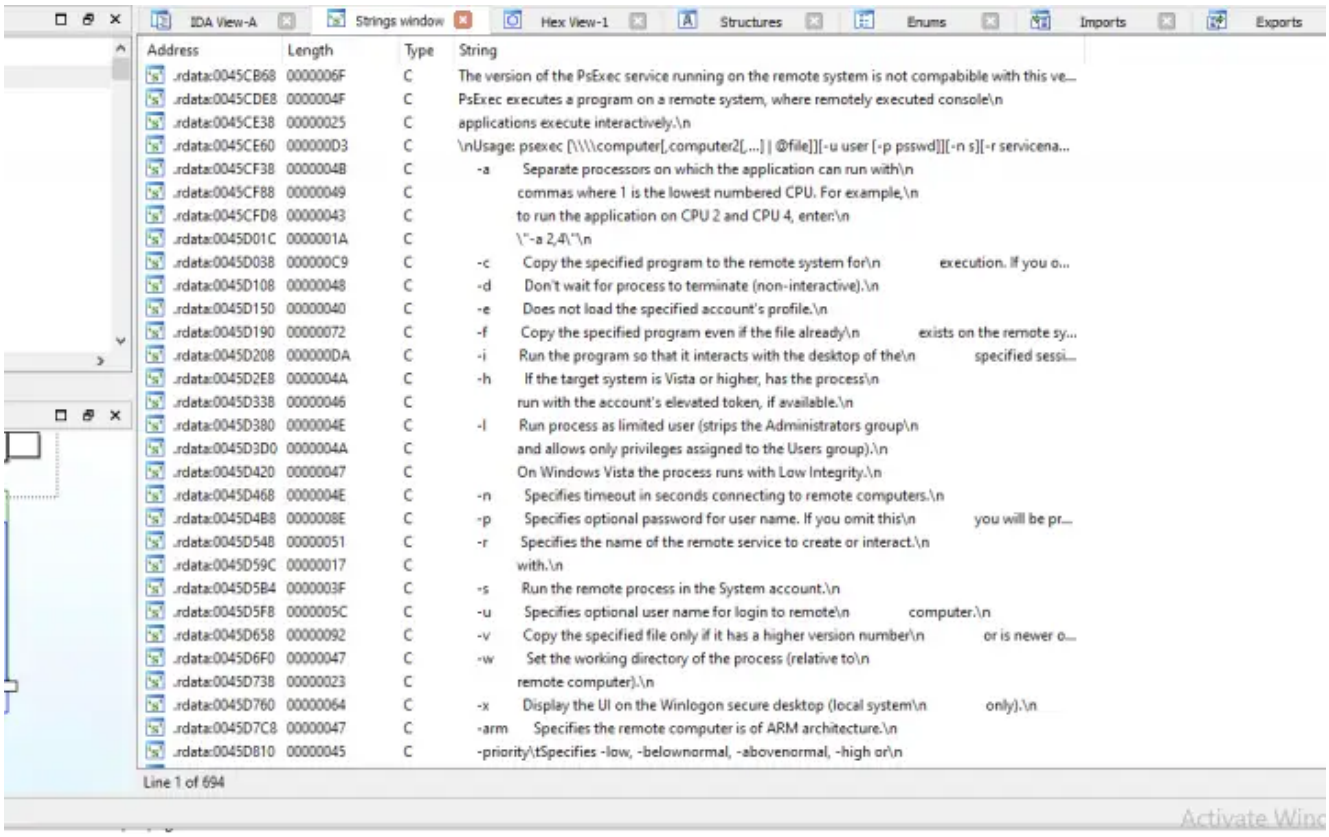

Figure 3. Decompressed PsExec file

Once it has gained access to a machine, Noberus then proceeds to kill the following processes and services:

> *"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"*

It also excludes certain directories, filenames, and file extensions from the encryption process, such as:

> *"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"*

Noberus then proceeds to encrypt files using either AES or ChaCha20 encryption.

The private key for encrypted machines appears to be generated randomly. It appears that Noberus generates a random number using BCryptGenRandom and calculates each byte with the string shown in *Figure 4*.

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

Figure 4. String used to calculate the private key

Files that have been encrypted have .sykffle appended to the end of their filename, in the following format:

> *[original filename].[extension].sykffle*

Noberus then creates a ransomware note, creating a .txt and a .png file that are displayed to victims, with the following filenames:

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

The text file tells victims the following:

> 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.
```

Figure 5. Noberus ransom note

Significance of this new ransomware

This is a sophisticated new ransomware with no apparent weaknesses in its encryption process, meaning unless victims have comprehensive backups they will be obliged to pay the ransom to recover their files. The fact it is written in Rust is interesting, as while Rust is not typically seen being used by malware developers, it is growing in popularity and it shows that ransomware developers too are not afraid to innovate in this area.

While the reported number of victims of this ransomware so far appears to be small, the sophistication of Noberus itself and the level of determination shown by the attackers in the attack we did observe indicates it is likely we will see more of this ransomware in the future. It is also reported that the developers behind this ransomware are actively seeking affiliates on Russian-speaking hacking forums, meaning the number of malicious actors deploying this ransomware is likely to grow.

Protection

File-based

Ransom.Noberus

For the latest protection updates, please visit the Symantec Protection Bulletin.

Yanluowang: Further Insights on New Ransomware Threat

At least one attacker now using Yanluowang may have previously been linked to Thieflock ransomware operation.

About the Author

Threat Hunter Team

Symantec

The Threat Hunter Team is a group of security experts within Symantec whose mission is to investigate targeted attacks, drive enhanced protection in Symantec products, and offer analysis that helps customers respond to attacks.

Want to comment on this post?