



SIEM & SOC – FINAL PROJECT

DEKSHINAMURTHY MEENAKSHI
Sstudy2016@gmail.com

Table of Contents

Malware Analysis:	2
Part 1:.....	2
Lab Setup:.....	2
Observations on bootup:	3
.NET error.....	3
Recent Documents.....	3
A Virus PopUP!!!:	4
Analysing using Autorun:	4
Identifying the File	7
HashMyFiles:.....	9
Check the file in Virustotal:.....	10
IpAddress and Domain of the virus:.....	11
Removal of Threat!	21
Key Findings	23
Part 2:.....	24
Identify the malicious File	24
Strings Tool.....	24
PEView	25
Analyzing in virus total:.....	25
Some DLLs in Dog.jpg:.....	26

Malware Analysis:

The process of understanding the behaviour and purpose of a suspicious file or URL.

It aims to find, how did the machine become affected and what the malware does, so that the effect of malware can be mitigated

Part 1:

Lab Setup:

Import the task ova into the virtual box manager.

Appliance settings

These are the virtual machines contained in the appliance and the suggested settings of the imported VirtualBox machines. You can change many of the properties shown by double-clicking on the items and disable others using the check boxes below.

Virtual System 1	
Name	SIEMnSOC_Final
Guest OS Type	Windows 10 (64-bit)
CPU	1
RAM	4096 MB
DVD	<input checked="" type="checkbox"/>
USB Controller	<input checked="" type="checkbox"/>
Sound Card	<input checked="" type="checkbox"/> Intel HD Audio
Network Adapter	<input checked="" type="checkbox"/> Intel PRO/1000 MT Desktop (82540EM)
Storage Controller (SATA)	AHCI
Virtual Disk Image	SIEMnSOC_Final-disk001.vmdk
Base Folder	C:\Users\meena\VirtualBox VMs
Primary Group	/Lab

Machine Base Folder: C:\Users\meena\VirtualBox VMs

MAC Address Policy: Include only NAT network adapter MAC addresses

Additional Options: ☒ Import hard drives as VDI

Appliance is not signed

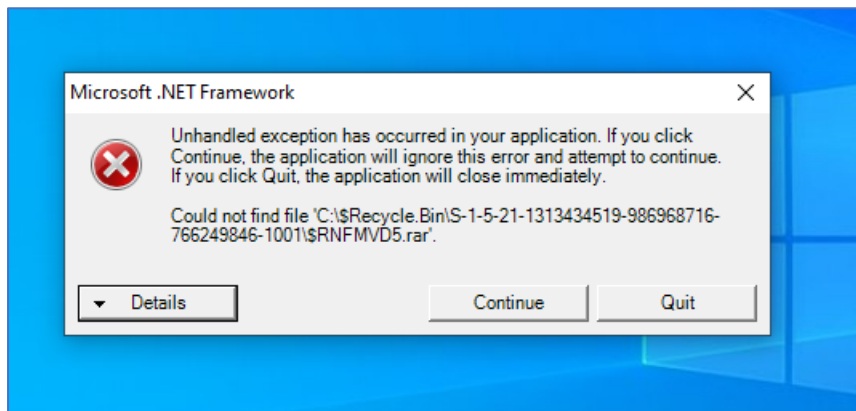
Restore Defaults

Import

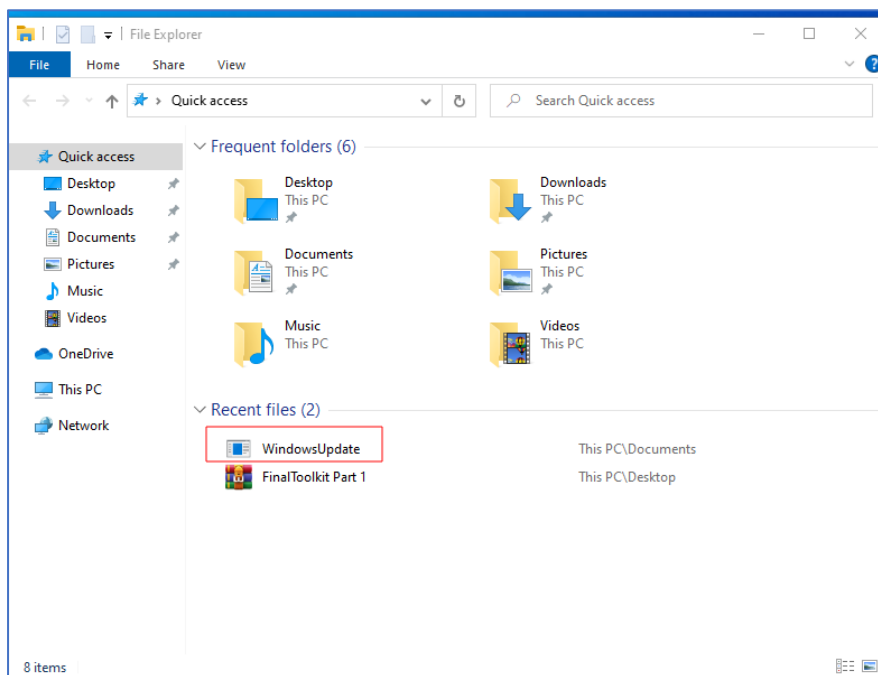
Cancel

Observations on bootup:

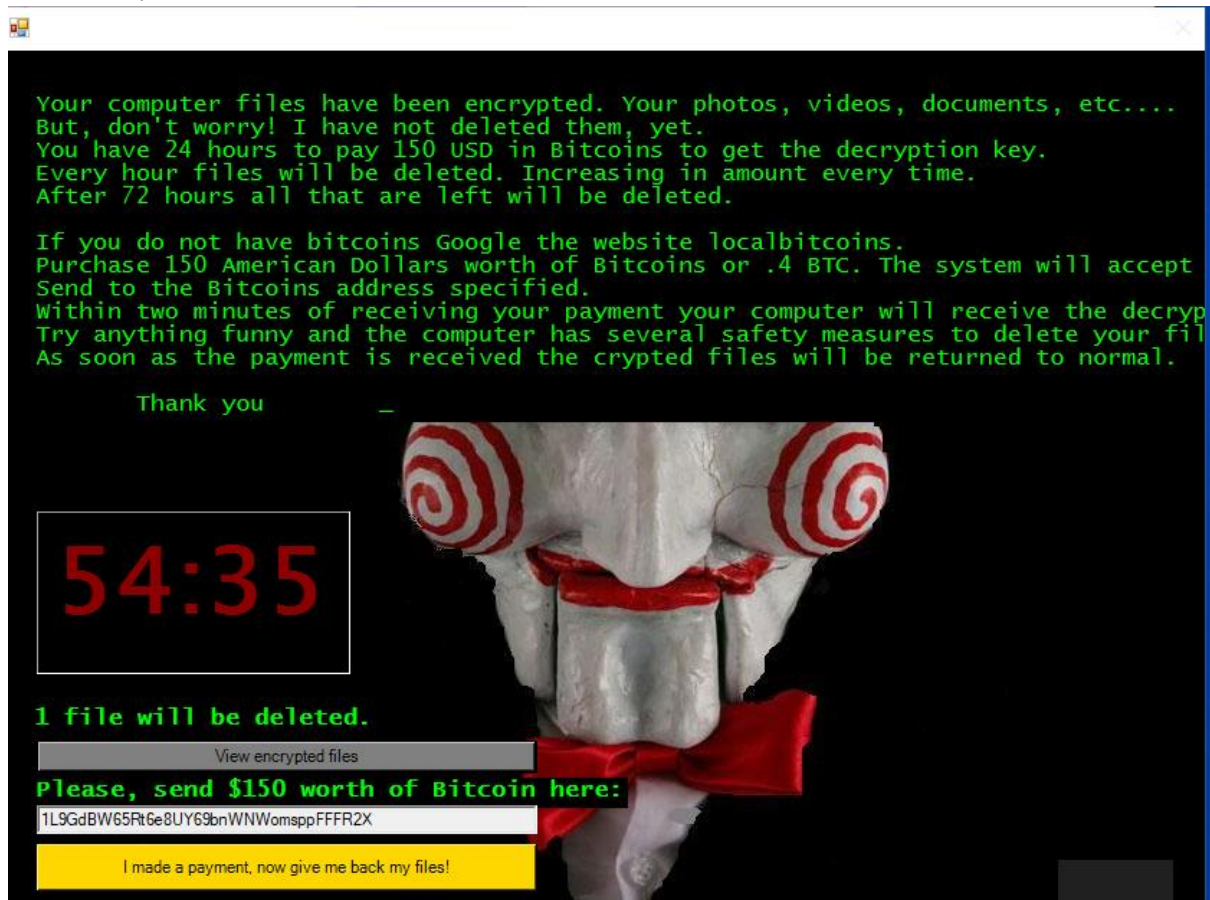
.NET error



Recent Documents



A Virus PopUP!!!:



Analysing using Autorun:

Autorun is a Sysinternals Tool from Microsoft that enumerates all programs that automatically start on a windows machine. These programs can be examined to find more details. We find couple of programs whose publisher is not verified, firefox.exe and Windowsupdate.exe

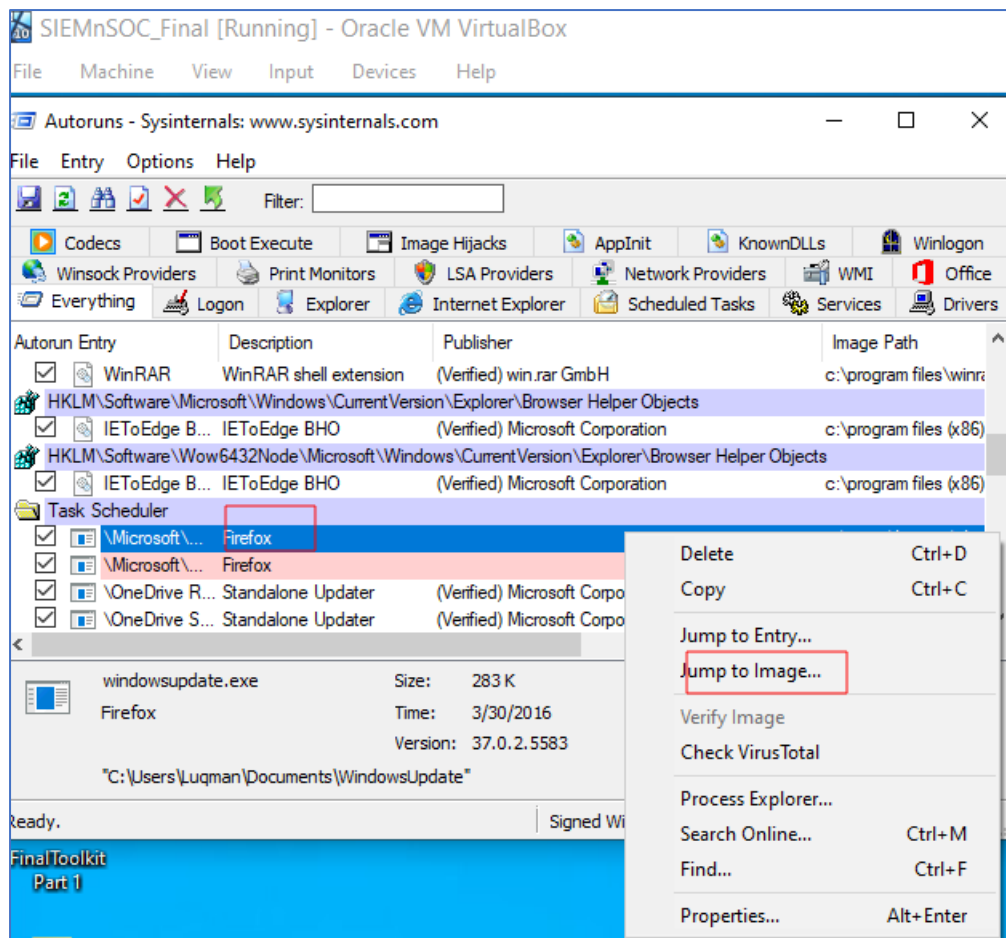
Autoruns - Sysinternals: www.sysinternals.com					
File Entry Options Help					
Filter:					
Everything Logon Explorer Internet Explorer Scheduled Tasks Services Drivers Codecs Boot Execute Image Hijacks AppInit KnownDLLs					
Autorun Entry	Description	Publisher	Image Path	Timestamp	VirusTotal
<input checked="" type="checkbox"/> HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\AlternateShell				12/7/2019 2:15 AM	
<input checked="" type="checkbox"/> cmd.exe	Windows Command Proc...	(Verified) Microsoft Windows	c:\windows\system32\cmd.exe	1/26/2037 8:29 AM	
<input checked="" type="checkbox"/> HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run				5/23/2022 4:16 AM	
<input checked="" type="checkbox"/> VBoxTray	VirtualBox Guest Addition...	(Verified) Oracle Corporation	c:\windows\system32\vbboxtray.exe	2/18/2020 10:16 AM	
<input checked="" type="checkbox"/> HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run				5/22/2022 1:27 AM	
<input checked="" type="checkbox"/> firefox.exe	Firefox		c:\users\luqman\appdata\roaming\frfx\firefox.exe	3/30/2016 11:28 PM	
<input checked="" type="checkbox"/> Microsoft Ed...	Microsoft Edge	(Verified) Microsoft Corporation	c:\program files (x86)\microsoft\edge\application\...	5/18/2022 10:45 AM	
<input checked="" type="checkbox"/> OneDrive	Microsoft OneDrive	(Verified) Microsoft Corporation	c:\users\luqman\appdata\local\microsoft\onedriv...	5/16/2030 1:20 AM	
<input checked="" type="checkbox"/> HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components				12/20/2020 12:44 AM	
<input checked="" type="checkbox"/> Microsoft Ed...	Microsoft Edge Installer	(Verified) Microsoft Corporation	c:\program files (x86)\microsoft\edge\application\...	5/18/2022 10:45 AM	
<input checked="" type="checkbox"/> n/a	Microsoft .NET IE SECU...	(Verified) Microsoft Corporation	c:\windows\system32\vmcores.dll	10/24/2019 8:45 PM	
<input checked="" type="checkbox"/> HKLM\SOFTWARE\Wow6432Node\Microsoft\Active Setup\Installed Components				12/20/2020 12:44 AM	
<input checked="" type="checkbox"/> n/a	Microsoft .NET IE SECU...	(Verified) Microsoft Corporation	c:\windows\syswow64\vmcores.dll	10/25/2019 1:48 AM	
<input checked="" type="checkbox"/> HKLM\Software\Classes\ShellEx\ContextMenuHandlers				12/15/2020 1:03 AM	
<input checked="" type="checkbox"/> WinRAR	WinRAR shell extension	(Verified) win.rar GmbH	c:\program files\winrar\varext.dll	12/1/2020 11:00 AM	
<input checked="" type="checkbox"/> HKLM\Software\Classes\Folder\ShellEx\ContextMenuHandlers				12/15/2020 1:03 AM	
<input checked="" type="checkbox"/> WinRAR	WinRAR shell extension	(Verified) win.rar GmbH	c:\program files\winrar\varext.dll	12/1/2020 11:00 AM	
<input checked="" type="checkbox"/> HKLM\Software\Classes\Folder\ShellEx\DragDropHandlers				12/15/2020 1:03 AM	
<input checked="" type="checkbox"/> WinRAR	WinRAR shell extension	(Verified) win.rar GmbH	c:\program files\winrar\varext.dll	12/1/2020 11:00 AM	
<input checked="" type="checkbox"/> HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects				9/27/2020 7:36 AM	
<input checked="" type="checkbox"/> IEToEdge B...	IEToEdge BHO	(Verified) Microsoft Corporation	c:\program files (x86)\microsoft\edge\application\...	5/18/2022 10:45 AM	
<input checked="" type="checkbox"/> HKLM\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects				9/27/2020 7:36 AM	
<input checked="" type="checkbox"/> IEToEdge B...	IEToEdge BHO	(Verified) Microsoft Corporation	c:\program files (x86)\microsoft\edge\application\...	5/18/2022 10:45 AM	
<input checked="" type="checkbox"/> Task Scheduler					
<input checked="" type="checkbox"/> \Microsoft\...	Firefox		c:\users\luqman\documents\windowsupdate.exe	3/30/2016 11:28 PM	
<input checked="" type="checkbox"/> \Microsoft\...	Firefox		c:\users\luqman\documents\windowsupdate.exe	3/30/2016 11:28 PM	
<input checked="" type="checkbox"/> \OneDrive R...	Standalone Updater	(Verified) Microsoft Corporation	c:\users\luqman\appdata\local\microsoft\onedriv...	7/6/1998 3:54 AM	
<input checked="" type="checkbox"/> \OneDrive S...	Standalone Updater	(Verified) Microsoft Corporation	c:\users\luqman\appdata\local\microsoft\onedriv...	7/6/1998 3:54 AM	
<input checked="" type="checkbox"/> HKLM\System\CurrentControlSet\Services				5/23/2022 3:37 PM	

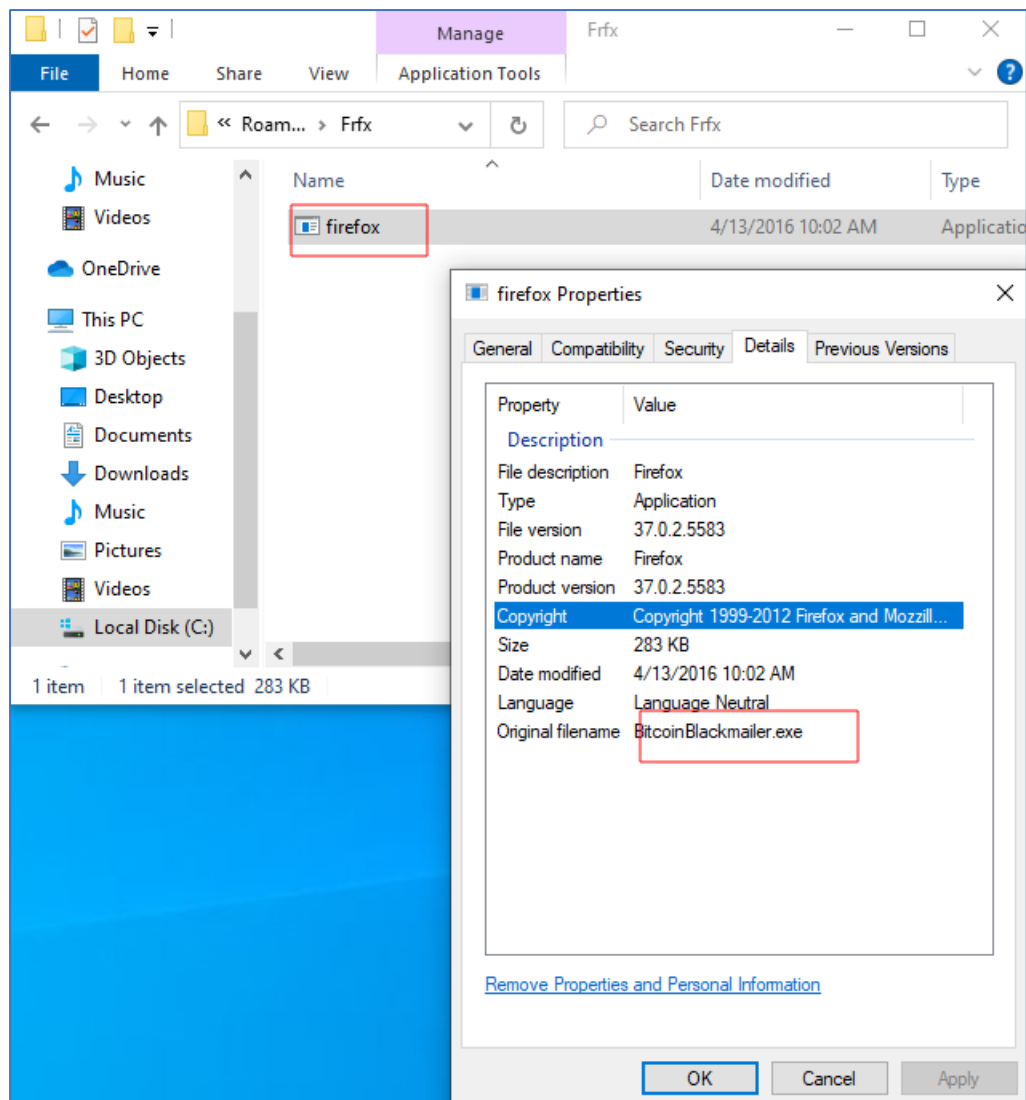
Two process named firefox were found to be running with image path referring to Windowsupdate.exe

Autoruns - Sysinternals: www.sysinternals.com			
File Entry Options Help			
Filter:			
Codecs Boot Execute Image Hijacks AppInit KnownDLLs Winlogon			
Winsock Providers Print Monitors LSA Providers Network Providers WMI Office			
Everything Logon Explorer Internet Explorer Scheduled Tasks Services Drivers			
Autorun Entry	Description	Publisher	Image Path
<input checked="" type="checkbox"/> WinRAR	WinRAR shell extension	(Verified) win.rar GmbH	c:\program files\winra
<input checked="" type="checkbox"/> HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects			
<input checked="" type="checkbox"/> IEToEdge B...	IEToEdge BHO	(Verified) Microsoft Corporation	c:\program files (x86)
<input checked="" type="checkbox"/> HKLM\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects			
<input checked="" type="checkbox"/> IEToEdge B...	IEToEdge BHO	(Verified) Microsoft Corporation	c:\program files (x86)
<input checked="" type="checkbox"/> Task Scheduler			
<input checked="" type="checkbox"/> \Microsoft\...	Firefox		c:\users\luqman\doc
<input checked="" type="checkbox"/> \Microsoft\...	Firefox		c:\users\luqman\doc
<input checked="" type="checkbox"/> \OneDrive R...	Standalone Updater	(Verified) Microsoft Corporation	c:\users\luqman\app
<input checked="" type="checkbox"/> \OneDrive S...	Standalone Updater	(Verified) Microsoft Corporation	c:\users\luqman\app
<div> <div>firefox.exe</div> <div>Size: 283 K</div> </div> <div> <div>Firefox</div> <div>Time: 3/30/2016</div> </div> <div> <div></div> <div>Version: 37.0.2.5583</div> </div> <div> <div>C:\Users\Luqman\AppData\Roaming\FrFx\firefox.exe</div> </div>			
Ready. Signed Windows Entries Hidden.			

Jump to Image:

Choose the entry with firefox. Right Click and choose "Jump to Image"





It takes us to the application “firefox” whose original file name is BitCoinBlackmailer.exe

Identifying the File

The Windowsupdate.exe is analysed with strings tool. The output is captured in the strings.txt

```
\\Desktop\FinalToolkit Part 1\FinalToolkit Part 1\SysinternalsSuite>strings.exe C:\Users\Luqman\Documents\
xe
```

Strings:


```
strings - Notepad
File Edit Format View Help
4.0.0.0
KMicrosoft.VisualStudio.Editors.SettingsDesigner.SettingsSingleFileGenerator
14.0.0.0
VS_VERSION_INFO
VarFileInfo
Translation
StringFileInfo
000004b0
Comments
CompanyName
FileDescription
Firefox
FileVersion
37.0.2.5583
InternalName
BitcoinBlackmailer.exe
```

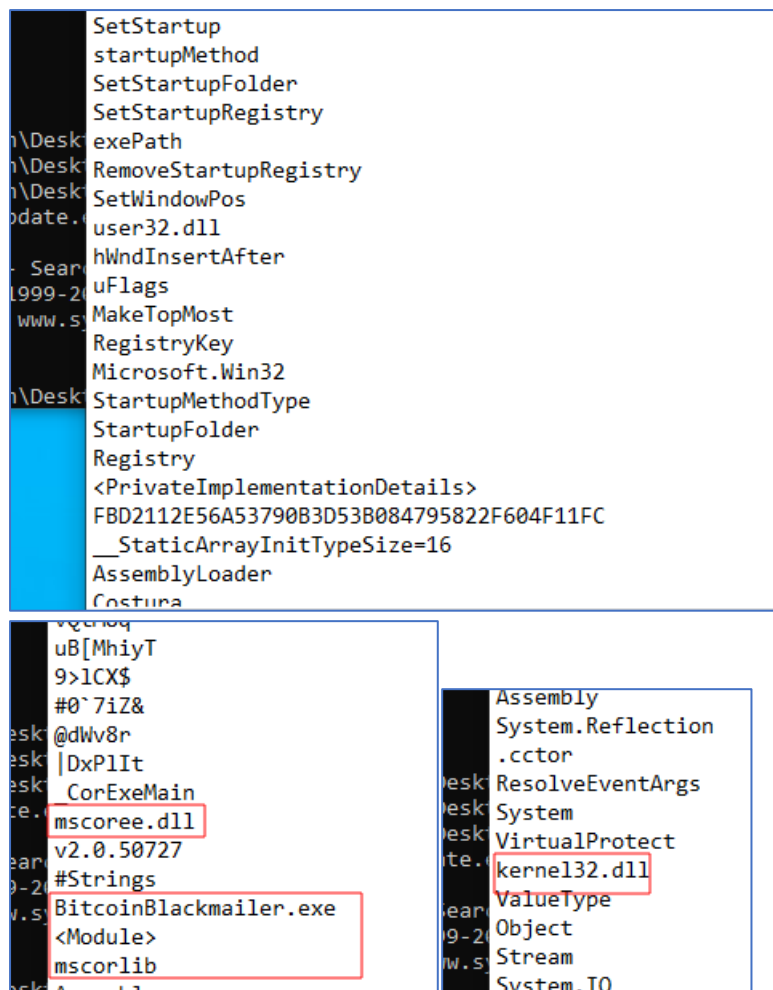
The information on extension of .fun

```
You have 24 hours to pay 150
Every hour files will be dele
After 72 hours all that are i
If you do not have bitcoins C
Purchase 150 American Dollars
Send to the Bitcoins address.
Within two minutes of receivi
Try anything funny and the co
As soon as the payment is rec

Thank you
Please, send $
worth of Bitcoin here:
FormBackground
Form1
.fun
YES
dataGridViewEncryptedFiles
Deleted
ColumnDeleted
Path
ColumnPath
FormEncryptedFiles
EncryptedFiles
Address.txt

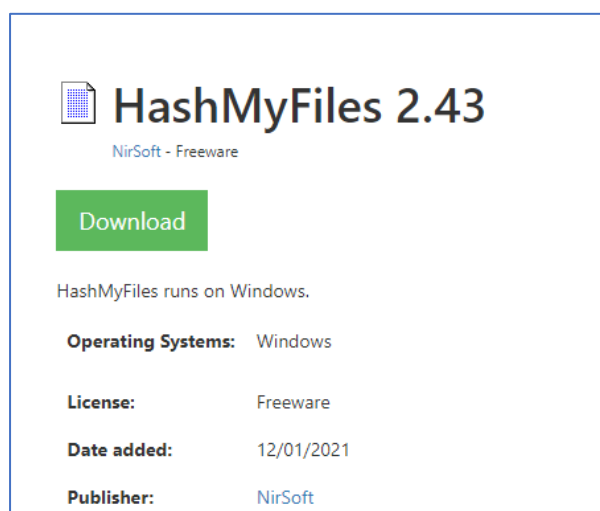
txttest.txt
I am a txt test.
NotTxtTest.nottxt
I am NOT a txt test.
C:\Windows
OoIsAwwF23cICQoLDA00De==
EncryptedFileList.txt
SOFTWARE\Microsoft\Windows\CurrentVersion\Run
.zip
{0}. {1}
```

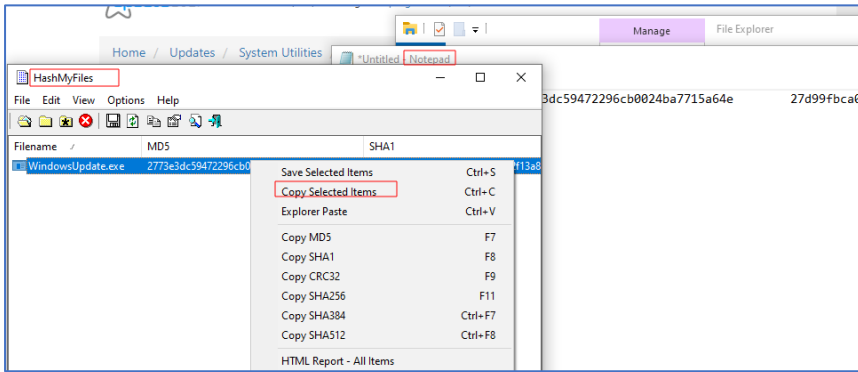
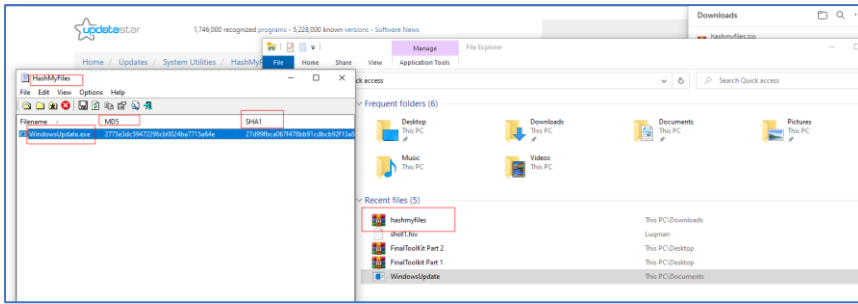
Looks like some files are really encrypted



HashMyFiles:

Searching using the hash of the file , Input the hash to the virustotal and checked it is the ransomware jigsaw

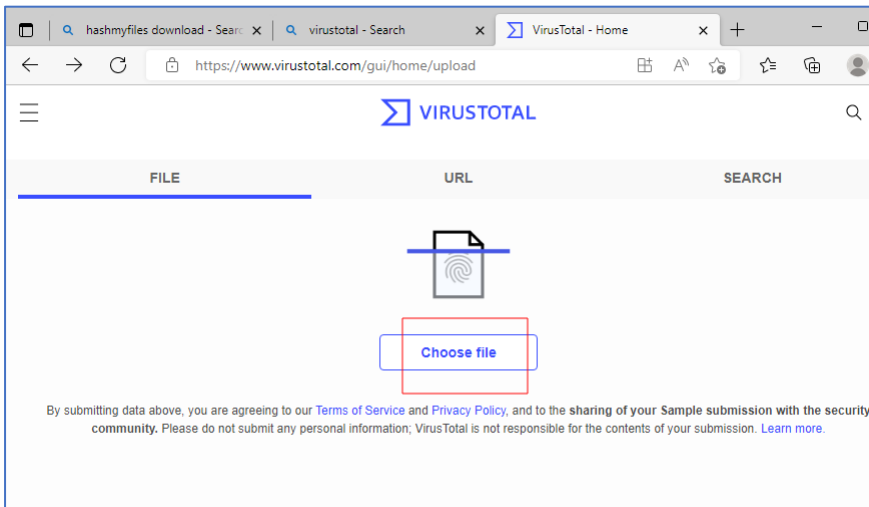




27d99fbc067f478bb91cdbc92f13a828b00859

By submitting data above, you are agreeing to our [Terms of Service](#) and [Privacy Policy](#), and to the sharing of your sample submission with the security community. Please do not submit any personal information; VirusTotal is not responsible for the contents of your submission. [Learn more](#).

Check the file in Virustotal:

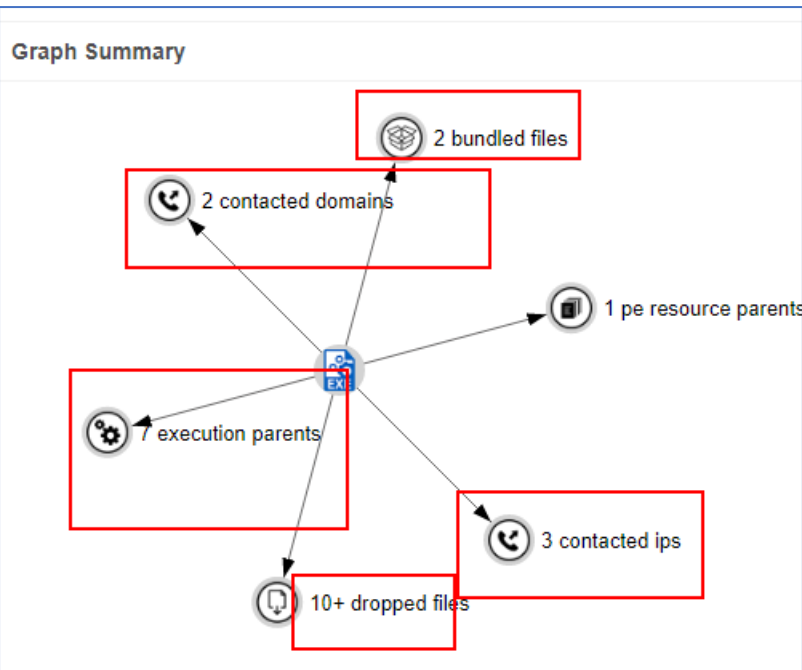


Security Vendors' Analysis	
Acronis (Static ML)	Suspicious
Ad-Aware	Trojan.GenericKD.50143194
AhnLab-V3	Win-Trojan/JigsawLocker.Gen
Alibaba	Trojan.MSIL/Filecoder.b8777336
ALYac	Trojan.Ransom.Jigsaw
Arcabit	Trojan.Generic.D2FD1FDA
Avast	MSIL.Ransom-AX [Trj]
AVG	MSIL.Ransom-AX [Trj]
Avira (no cloud)	TR/FileCoder.aqne

IpAddress and Domain of the virus:

Contacted Domains		
Domain	Detections	Registrar
arc.msn.com	0 / 90	MarkMonitor Inc.
sfd-production.azurefd.net	0 / 90	MarkMonitor Inc.

Contacted IP Addresses		
IP	Detections	Country
192.168.0.74	0 / 90	-
20.82.209.183	0 / 90	IE
23.216.147.76	0 / 90	US



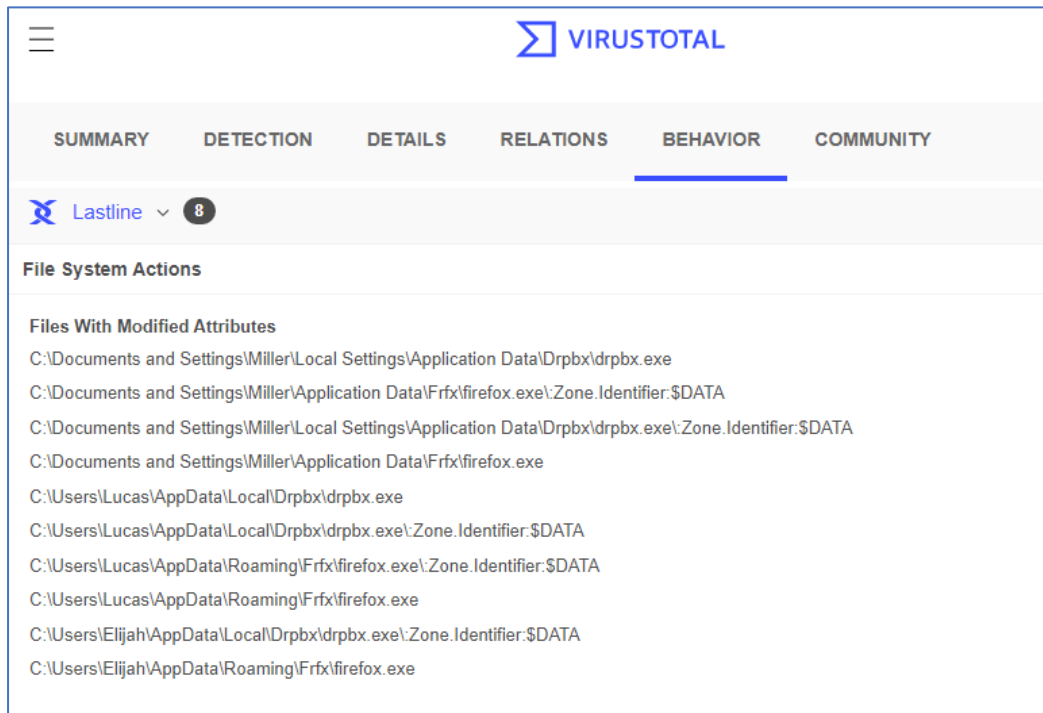
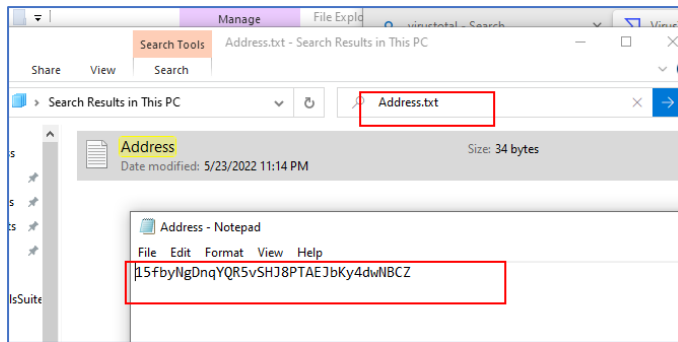
Process And Service Actions

Processes Created

C:\DOCUME~1\Miller\LOCALS~1\Temp\jigsaw.exe
C:\Documents and Settings\Miller\Local Settings\Application Data\Drpbx\drpbx.exe
C:\Users\Lucas\AppData\Local\Temp\jigsaw.exe
C:\Users\Lucas\AppData\Local\Drpbx\drpbx.exe
C:\Users\Lucas\AppData\Local\Temp\jig.exe
C:\Users\Lucas\AppData\Local\Temp\primary_analysis_subject.exe
C:\Users\Lucas\AppData\Local\Temp\ud5-dl1qkgvdx-290694387.exe
C:\Users\Lucas\AppData\Local\Temp\2773e3dc59472296cb0024ba7715a6nalysis_subject.exe
C:\Users\Elijah\AppData\Local\Temp\2773e3dc59472296cb0024ba7715a6nalysis_subject.exe
C:\Users\Elijah\AppData\Local\Drpbx\drpbx.exe

Further Analysis using Virustotal:

Address.txt string found in the output of strings tool on the virus program seems encrypted



Registry Actions	
Registry Keys Set	
+	HKU\S-1-5-21-1229272821-1563985344-1801674531-1003\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\INTERNET SETTINGS\ZONEMAP
+	HKU\S-1-5-21-1229272821-1563985344-1801674531-1003\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\EXPLORER\SHELL FOLDERS
+	HKU\S-1-5-21-1229272821-1563985344-1801674531-1003\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\EXPLORER\SHELL FOLDERS
+	HKU\S-1-5-21-1229272821-1563985344-1801674531-1003\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\INTERNET SETTINGS\ZONEMAP
+	HKU\S-1-5-21-1229272821-1563985344-1801674531-1003\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\EXPLORER\SHELL FOLDERS
+	HKU\S-1-5-21-1229272821-1563985344-1801674531-1003\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\INTERNET SETTINGS\ZONEMAP
+	HKU\S-1-5-21-1229272821-1563985344-1801674531-1003\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\EXPLORER\MOUNTPOINTS2\{4D7134C0-AF74-11E5-A617-806D6172696F}
+	HKU\S-1-5-21-1229272821-1563985344-1801674531-1003\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\EXPLORER\MOUNTPOINTS2\{A7A58122-718B-11E3-95AC-806D6172696F}
+	HKU\S-1-5-21-1229272821-1563985344-1801674531-1003\SOFTWARE\MICROSOFT\WINDOWS\SHELLNOROAMMUICACHE
+	HKU\S-1-5-21-1229272821-1563985344-1801674531-1003\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\EXPLORER\SHELL FOLDERS
▼	

Process And Service Actions	
Processes Created	
C:\DOCUME~1\Miller\LOCALS~1\Temp\jigsaw.exe	
C:\Documents and Settings\Miller\Local Settings\Application Data\Drpbx\drpbx.exe	
C:\Users\Lucas\AppData\Local\Temp\jigsaw.exe	
C:\Users\Lucas\AppData\Local\Drpbx\drpbx.exe	
C:\Users\Lucas\AppData\Local\Temp\jig.exe	
C:\Users\Lucas\AppData\Local\Temp\primary_analysis_subject.exe	
C:\Users\Lucas\AppData\Local\Temp\ud5-dl1qkgvdx-290694387.exe	
C:\Users\Lucas\AppData\Local\Temp\2773e3dc59472296cb0024ba7715a6nalysis_subject.exe	
C:\Users\Elijah\AppData\Local\Temp\2773e3dc59472296cb0024ba7715a6nalysis_subject.exe	
C:\Users\Elijah\AppData\Local\Drpbx\drpbx.exe	
▼	

Shell Commands	
C:\DOCUME~1\Miller\LOCALS~1\Temp\jigsaw.exe	
"C:\Documents and Settings\Miller\Local Settings\Application Data\Drpbx\drpbx.exe" C:\DOCUME~1\Miller\LOCALS~1\Temp\jigsaw.exe	
C:\Users\Lucas\AppData\Local\Temp\jigsaw.exe	
C:\Users\Lucas\AppData\Local\Drpbx\drpbx.exe C:\Users\Lucas\AppData\Local\Temp\jigsaw.exe	
C:\Users\Lucas\AppData\Local\Temp\jig.exe	
C:\Users\Lucas\AppData\Local\Drpbx\drpbx.exe C:\Users\Lucas\AppData\Local\Temp\jig.exe	
C:\Users\Lucas\AppData\Local\Temp\primary_analysis_subject.exe	
C:\Users\Lucas\AppData\Local\Drpbx\drpbx.exe C:\Users\Lucas\AppData\Local\Temp\primary_analysis_subject.exe	
C:\Users\Lucas\AppData\Local\Temp\ud5-dl1qkgvdx-290694387.exe	
C:\Users\Lucas\AppData\Local\Drpbx\drpbx.exe C:\Users\Lucas\AppData\Local\Temp\ud5-dl1qkgvdx-290694387.exe	

Processes Tree

- ↳ 268 - C:\DOCUME~1\Miller\LOCALS~1\Temp\jigsaw.exe
- ↳ 452 - C:\Documents and Settings\Miller\Local Settings\Application Data\Drpbx\drpbx.exe

Synchronization Mechanisms & Signals

Mutexes Created

CTF.Compart.MutexDefaultS-1-5-21-1229272821-1563985344-1801674531-1003
CTF.TMD.MutexDefaultS-1-5-21-1229272821-1563985344-1801674531-1003
Local\ZonesCounterMutex
Local\ZonesLockedCacheCounterMutex
CTF.Layouts.MutexDefaultS-1-5-21-1229272821-1563985344-1801674531-1003
CTF.Asm.MutexDefaultS-1-5-21-1229272821-1563985344-1801674531-1003
Local\ZoneAttributeCacheCounterMutex
CTF.TimListCache.FMPDefaultS-1-5-21-1229272821-1563985344-1801674531-1003MUTEX.Def
1003
Local\ZonesCacheCounterMutex
CTF.LBES.MutexDefaultS-1-5-21-1229272821-1563985344-1801674531-1003



SUMMARY

DETECTION

DETAILS


RELATIONS

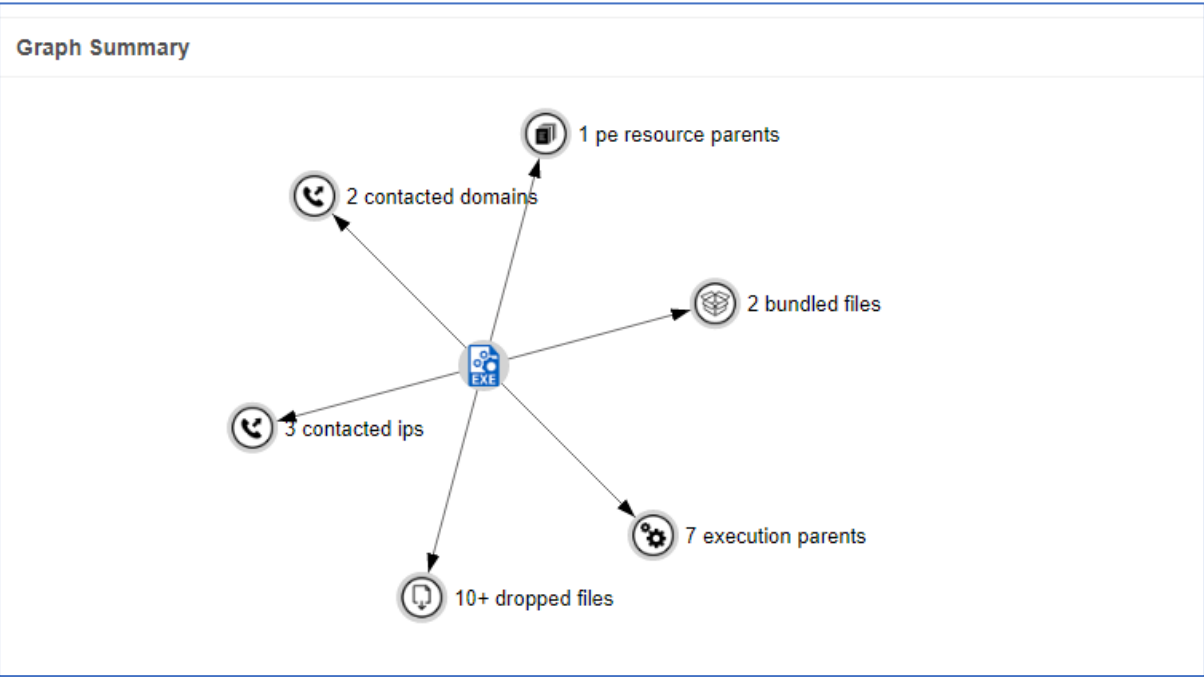
BEHAVIOR

COMMUNITY

Contacted Domains

Domain	Detections	Created	Registrar
arc.msn.com	0 / 90	1994-11-10	MarkMonitor Inc.
sfd-production.azurefd.net	0 / 90	2018-05-08	MarkMonitor Inc.

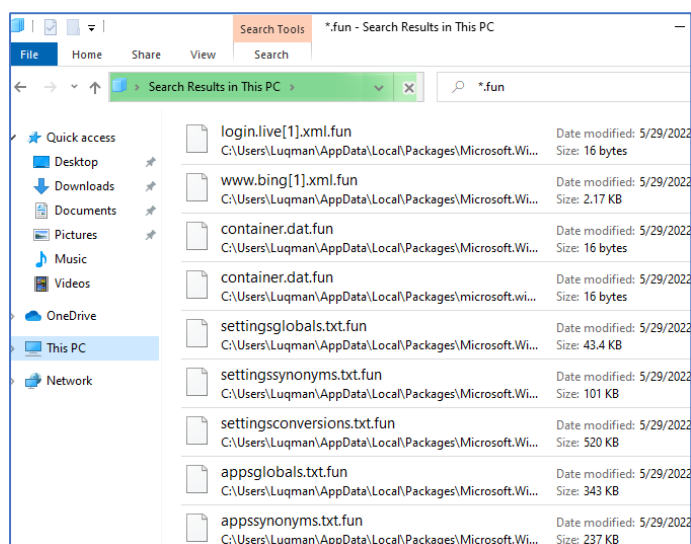
Execution Parents				
Scanned	Detections	Type	Name	
2021-12-14	44 / 68	Win32 EXE	virussign.com_a76fec8271a1013b0059f138599c7220.vir	
2021-04-07	42 / 68	Win32 EXE	jigsaw	
2020-05-27	64 / 72	Win32 EXE	181cd8e49e6ff6d4d17c72bbe97655df7b9e88d0e840ee75814e4b78228214ae	
2021-03-13	48 / 68	Win32 EXE	Output2.exe	
2021-04-13	30 / 69	Win32 EXE	jigsaw	
2022-05-22	61 / 68	Win32 EXE	windowsupdate.exe	
2018-05-10	60 / 66	Win32 EXE	fb9f55dd90911882ac6e0f4b28046682b61c1c6396f6a6d99de0ff275e9973fe	



Bundled Files			
Scanned	Detections	File type	Name
✓ 2016-12-25	0 / 55	?	rk_7E24.tmp
✓ 2020-09-22	0 / 58	?	

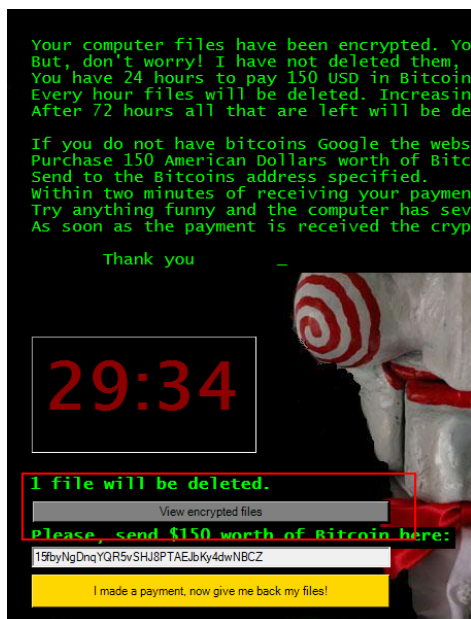
Dropped Files			
Scanned	Detections	File type	Name
✓ 2021-06-01	0 / 59	DOS COM	customizations.xml.fun
✓ 2021-06-01	0 / 59	DOS COM	customizations.xml.fun
✓ 2021-06-01	0 / 60	DOS COM	energy-report-2021-05-15.xml.fun
✓ 2021-06-01	0 / 59	DOS COM	customizations.xml.fun
✓ 2021-06-28	0 / 57	DOS COM	RunTime.xml.fun
✓ 2021-06-01	0 / 59	DOS COM	customizations.xml.fun
✓ 2021-06-01	0 / 59	DOS COM	customizations.xml.fun
✓ 2022-05-11	0 / 58	DOS COM	energy-report-2022-03-19.xml.fun
✓ 2022-05-11	0 / 53	DOS COM	energy-report-2022-03-18.xml.fun
✓ 2021-06-01	0 / 59	DOS COM	energy-report-2021-03-23.xml.fun

It is noticed that the txt files turned to txt.fun Probably the virus is infecting the files. Searching the computer for the files with extension “.fun” gives a long list of infected files



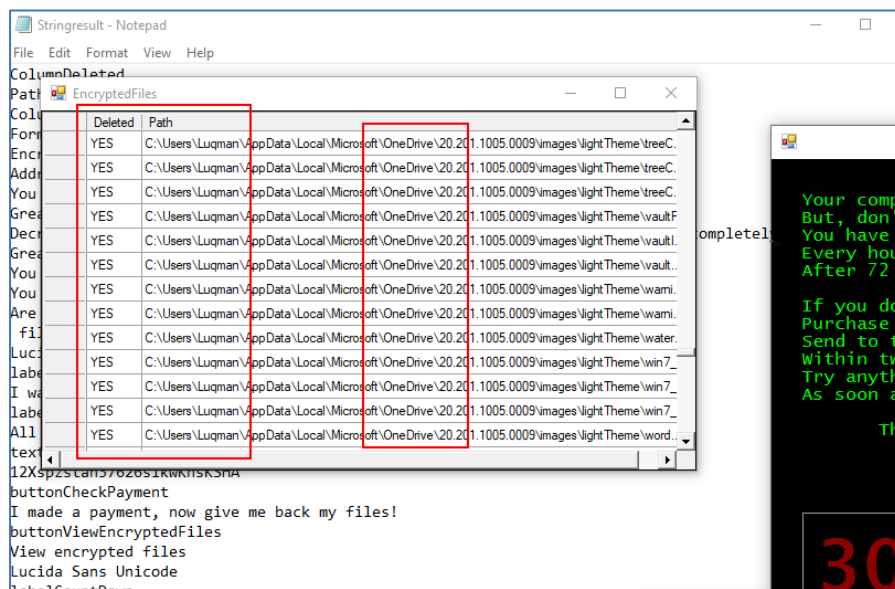
It was also noticed the files start missing... like the dog.jpg was removed

A part of the virus activity.



Clicking on the “View encrypted files” shows the file / directory location affected

Looks like C:/users/luqman is infected



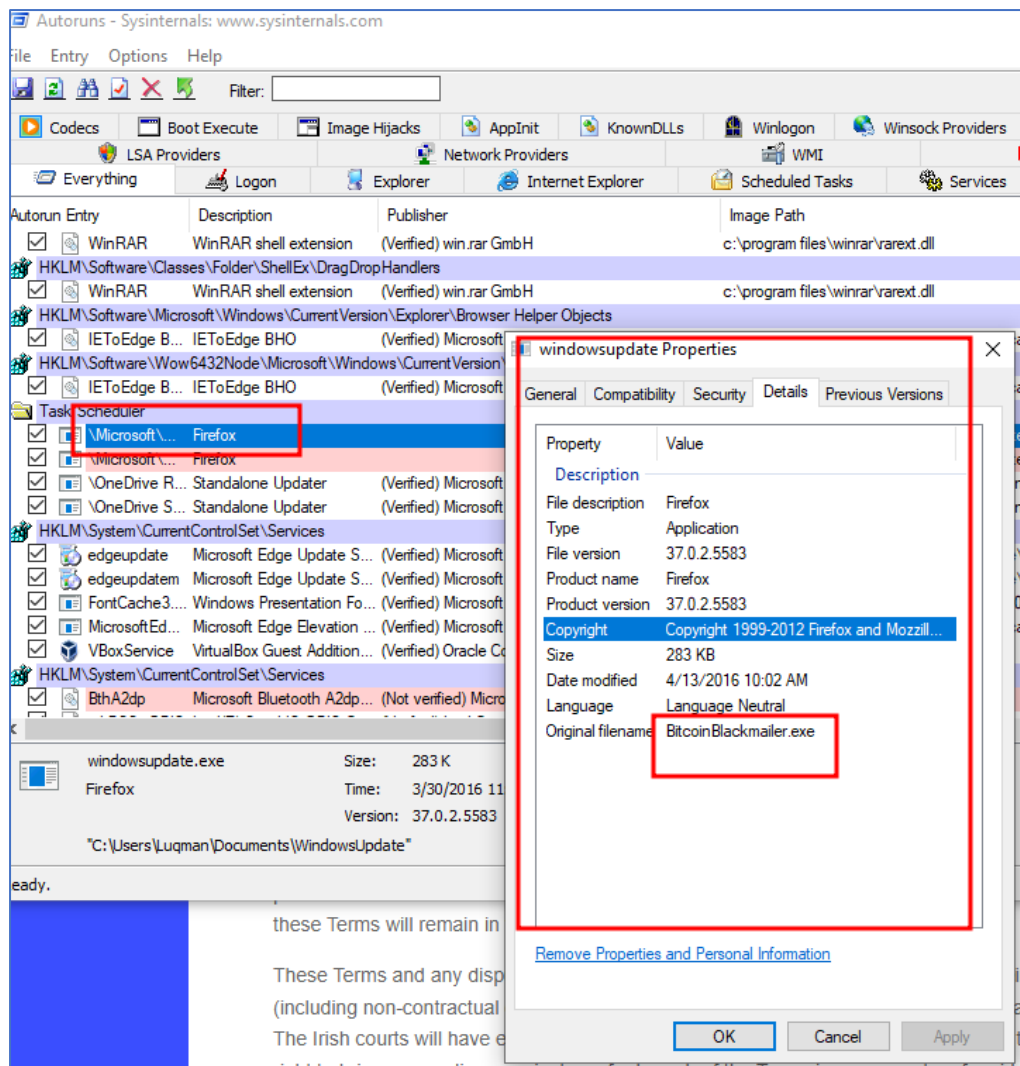
PREVIEW

PEView - C:\Users\Luqman\Documents\WindowsUpdate.exe

File View Go Help

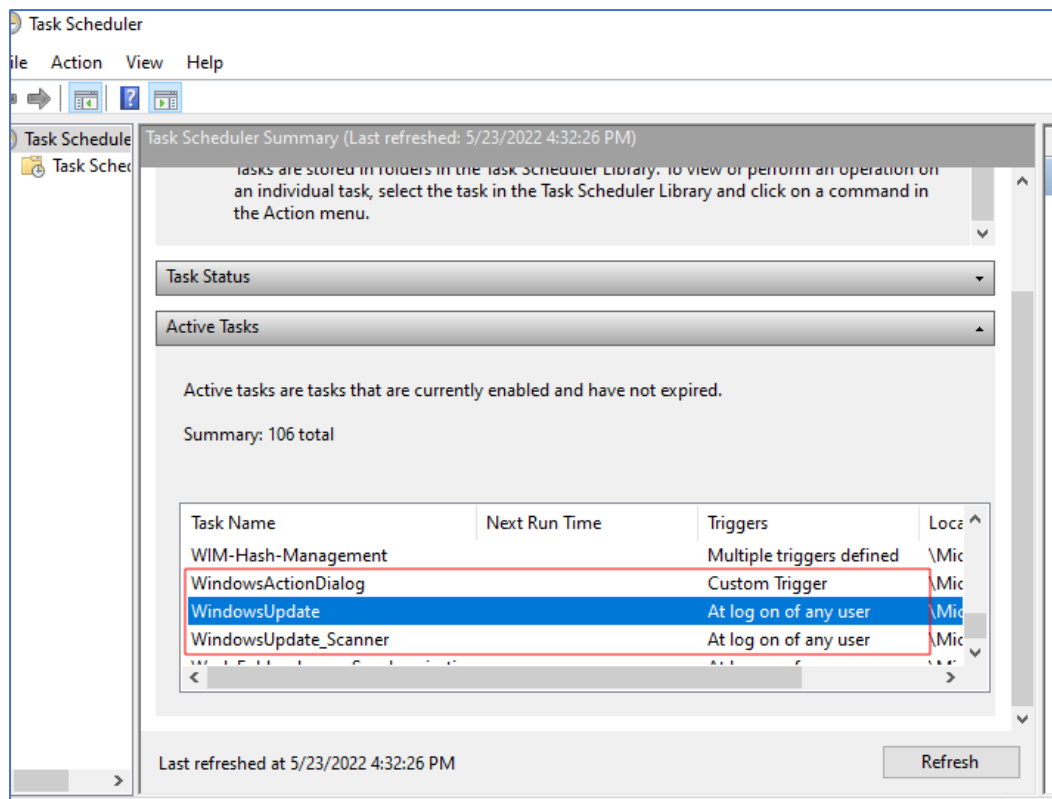
	pFile	Data	Description	Value
WindowsUpdate.exe				
IMAGE_DOS_HEADER	00000084	014C	Machine	IMAGE_FILE_MACHINE_I386
MS-DOS Stub Program	00000086	0005	Number of Sections	
IMAGE_NT_HEADERS				
Signature	00000088	56FCC37E	Time Date Stamp	2016/03/31 Thu 06:28:14 UTC
IMAGE_FILE_HEADER	0000008C	00000000	Pointer to Symbol Table	
IMAGE_OPTIONAL_H	00000090	00000000	Number of Symbols	
IMAGE_SECTION_HEAD	00000094	00E0	Size of Optional Header	
IMAGE_SECTION_HEAD	00000096	0102	Characteristics	IMAGE_FILE_EXECUTABLE_IMAGE
IMAGE_SECTION_HEAD		0002		IMAGE_FILE_32BIT_MACHINE
IMAGE_SECTION_HEAD		0100		
IMAGE_SECTION_HEAD				
SECTION 0mmUPp				
SECTION .text				
SECTION .rsrc				
SECTION .reloc				
SECTION				

The Characteristics and timestamp of creation are seen



IEToEdge BHO	IEToEdge BHO	(Verified) Microsoft Corporation
HKLM\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects		
IEToEdge BHO	IEToEdge BHO	(Verified) Microsoft Corporation
Task Scheduler		
Microsoft\Windows\WindowsUpdate	WindowsUpdate	Firefox
Microsoft\Windows\WindowsUpdate	WindowsUpdate_Scanner	Firefox
OneDrive Reporting Task-S-1-5-21-1313434519-986968716-766249846-1001	Standalone Updater	(Verified) Microsoft Corporation
OneDrive Standalone Update Task-S-1-5-21-1313434519-986968716-766249846-1001	Standalone Updater	(Verified) Microsoft Corporation
HKLM\System\CurrentControlSet\Services		
edgeupdate	Microsoft Edge Update S...	(Verified) Microsoft Corporation

The Task Scheduler shows that the virus exe is run on the logon of the user




Removal of Threat!

Microsoft Defender is an enterprise endpoint security platform designed to help prevent, detect (offers real-time threat detection), investigate and respond to advanced threat

Windows Security continually scans for malware, viruses and security threats. Updates are automatically downloaded to help keep the device safe and protect it from threats.

For a best solution, the windows defender can be combined with any good antivirus software like Norton.

Threat found -
action needed.
5/23/2022 4:13 PM

Severe ^

Detected: Trojan:MSIL/Cryptor

Status: Active
Active threats have not been remediated
and are running on your device.

Date: 5/23/2022 4:13 PM
Details: This program is dangerous and
executes commands from an
attacker.

Affected items:
file: \\localhost\C\$\Users\Lugman
\AppData\Roaming\Frfr\firefox.exe


[Learn more](#)

Actions ^

+ Add an exclusion

C:\
Folder

Remove

Current threats

Threats found. Start the recommended actions.

Trojan:MSIL/Cryptor


5/23/2022 4:53 PM (Active)

Severe

Start actions

[Scan options](#)
[Allowed threats](#)
[Protection history](#)

After removal of virus:

Current threats

No current threats.
Last scan: 5/23/2022 4:51 PM (quick scan)
2 threats found.
Scan lasted 3 minutes 59 seconds
37201 files scanned.

Quick scan

[Scan options](#)
[Allowed threats](#)
[Protection history](#)

Process Name	Description	Publisher	Image Path	Timestamp	Visa Total
WLM SYSTEM CurrentControlSet Control SafeBoot AlternateShell	Windows Command Proc...	(Verified) Microsoft Windows	c:\windows\system32\cmd.exe	12/26/2019 2:15 AM	
cmd.exe	Windows Command Proc...	(Verified) Microsoft Windows	c:\windows\system32\cmd.exe	1/26/2017 8:29 AM	
HKLM SOFTWARE Microsoft Windows CurrentVersion Run	VirtualBox Guest Addition...	(Verified) Oracle Corporation	c:\windows\system32\vbtray.exe	5/23/2022 4:16 AM	
vbtray	VirtualBox Guest Addition...	(Verified) Oracle Corporation	c:\windows\system32\vbtray.exe	2/18/2020 10:16 AM	
firefox.exe	File not found: C:\Users\Luqman\AppData\Roam...			5/22/2022 1:27 AM	
MicrosoftEdgeAutoLaunch_36AF229D71648D8CF7EC495D36E1F	Microsoft Edge	(Verified) Microsoft Corporation	c:\program files (x86)\microsoft\edge\application...	5/18/2022 10:45 AM	
OneDrive	Microsoft OneDrive	(Verified) Microsoft Corporation	c:\users\luqman\appdata\local\microsoft\onedrive...	5/16/2020 1:20 AM	
HKLM SOFTWARE Microsoft Windows CurrentVersion Installed Components	Microsoft Edge	(Verified) Microsoft Corporation	c:\program files (x86)\microsoft\edge\application...	12/20/2020 12:44 AM	
Microsoft Edge	Microsoft Edge Installer	(Verified) Microsoft Corporation	c:\program files (x86)\microsoft\edge\application...	5/18/2022 10:45 AM	
n/a	Microsoft .NET IE SECU...	(Verified) Microsoft Corporation	c:\windows\system32\mscories.dll	10/24/2019 6:45 PM	
WLM SOFTWARE Wow6432Node Microsoft Windows CurrentVersion Explorer Installed Components	Microsoft .NET IE SECU...	(Verified) Microsoft Corporation	c:\windows\system32\mscories.dll	10/25/2019 1:48 AM	
n/a	Microsoft .NET IE SECU...	(Verified) Microsoft Corporation	c:\windows\system32\mscories.dll	9/27/2020 7:36 AM	
HKLM Software Microsoft Windows CurrentVersion Explorer Browser Helper Objects	IEToEdge BHO	(Verified) Microsoft Corporation	c:\program files (x86)\microsoft\edge\application...	5/18/2022 10:45 AM	
IEToEdge BHO	IEToEdge BHO	(Verified) Microsoft Corporation	c:\program files (x86)\microsoft\edge\application...	9/27/2020 7:36 AM	
IEToEdge BHO	IEToEdge BHO	(Verified) Microsoft Corporation	c:\program files (x86)\microsoft\edge\application...	5/18/2022 10:45 AM	
Task Scheduler	Task Scheduler				
OneDrive Reporting Task: S-1-5-21-1313434519-98936716-76248846-1001	Standalone Updater	(Verified) Microsoft Corporation	c:\users\luqman\appdata\local\microsoft\onedrive...	7/6/1998 3:54 AM	
OneDrive Standalone Update Task: S-1-5-21-1313434519-98936716-76248846-1001	Standalone Updater	(Verified) Microsoft Corporation	c:\users\luqman\appdata\local\microsoft\onedrive...	7/6/1998 3:54 AM	
HKLM System CurrentControlSet Services	Microsoft Bluetooth A2dp...	(Not verified) Microsoft Corporation	c:\windows\system32\drivers\lbtah2dp.sys	5/23/2022 4:49 PM	
BthA2dp	Microsoft Bluetooth A2dp...	(Not verified) Microsoft Corporation	c:\windows\system32\drivers\lbtah2dp.sys	11/16/2023 3:59 PM	
WLM SOFTWARE Classes\HidClass\Shell Open Command (Default)	Internet Explorer	(Verified) Microsoft Corporation	c:\program files\internet explorer\iexplore.exe	9/27/2020 7:33 AM	
C:\Program Files\Internet Explorer\iexplore.exe	Internet Explorer	(Verified) Microsoft Corporation	c:\program files\internet explorer\iexplore.exe	10/31/1904 12:37 PM	
WLM SYSTEM CurrentControlSet Session Manager\KnownDlls					
Wow64cpu			c:\windows\system32\wow64cpu.dll	12/7/2019 2:15 AM	
Wowamthw			c:\windows\system32\wowamthw.dll		
Wowamthw			c:\windows\system32\wowamthw.dll		
Atapi			c:\windows\system32\atapi.dll		
Wow64			c:\windows\system32\wow64.dll		
Wow64win			c:\windows\system32\wow64win.dll		
WLM SYSTEM CurrentControlSet Control Network Provider Order	VirtualBox Shared Folders	(Verified) Oracle Corporation	c:\windows\system32\vbosmmp.dll	10/26/2020 8:06 AM	
VBosMP	VirtualBox Shared Folders	(Verified) Oracle Corporation	c:\windows\system32\vbosmmp.dll	2/18/2020 10:16 AM	

Key Findings

WindowsUpdate.exe and firefox.exe are the malicious process

These process are listed in Autoruns tools as running without a verified publisher.

Analysed these EXE files using strings.exe in the SysInternalsSuite Tool. The generated output has the exact same wordings and various reference to the popup message shown by the jigsaw Virus.

It has reference to the list of encrypted files and the url to which the victim has to send his money for recovery of this files. The proof for sudden appearance of the files with .fun has also been cited in the output of strings file

The users home directory C:/users/luqman and files in it is infected

Stringresult - Notepad

File Edit Format View Help

ColumnDeleted

Path EncryptedFiles

Deleted	Path
YES	C:\Users\Luqman\AppData\Local\Microsoft\OneDrive\20.201.1005.0009\images\Night Theme\treeC...
YES	C:\Users\Luqman\AppData\Local\Microsoft\OneDrive\20.201.1005.0009\images\Night Theme\treeC...
YES	C:\Users\Luqman\AppData\Local\Microsoft\OneDrive\20.201.1005.0009\images\Night Theme\treeC...
YES	C:\Users\Luqman\AppData\Local\Microsoft\OneDrive\20.201.1005.0009\images\Night Theme\vault F...
YES	C:\Users\Luqman\AppData\Local\Microsoft\OneDrive\20.201.1005.0009\images\Night Theme\vault...
YES	C:\Users\Luqman\AppData\Local\Microsoft\OneDrive\20.201.1005.0009\images\Night Theme\wami...
YES	C:\Users\Luqman\AppData\Local\Microsoft\OneDrive\20.201.1005.0009\images\Night Theme\wami...
YES	C:\Users\Luqman\AppData\Local\Microsoft\OneDrive\20.201.1005.0009\images\Night Theme\water...
YES	C:\Users\Luqman\AppData\Local\Microsoft\OneDrive\20.201.1005.0009\images\Night Theme\win7...
YES	C:\Users\Luqman\AppData\Local\Microsoft\OneDrive\20.201.1005.0009\images\Night Theme\win7...
YES	C:\Users\Luqman\AppData\Local\Microsoft\OneDrive\20.201.1005.0009\images\Night Theme\win7...
YES	C:\Users\Luqman\AppData\Local\Microsoft\OneDrive\20.201.1005.0009\images\Night Theme\word...

12Xspzctm776205IKWIKSKNA

buttonCheckPayment

I made a payment, now give me back my files!

buttonViewEncryptedFiles

View encrypted files

Lucida Sans Unicode

labelCountDown

completely

Your computer is infected with a virus. But, don't worry. You have a chance to recover your files. Every hour, your files are being encrypted. After 72 hours, your files will be permanently lost. If you do not purchase the recovery kit, your files will be lost forever. Purchase the recovery kit now. Send to the following address within two hours. Try anything else. As soon as you receive the kit, follow the instructions. The recovery kit will cost you \$99.99. The recovery kit will be shipped to you within 24 hours. The recovery kit will be shipped to you within 24 hours. The recovery kit will be shipped to you within 24 hours.

30

Malicious process and Welcome screen is same, because the same message displayed by the virus is seen in the strings output of the EXE

URL: <http://btc.blockr.io/api/v1/coin/info>

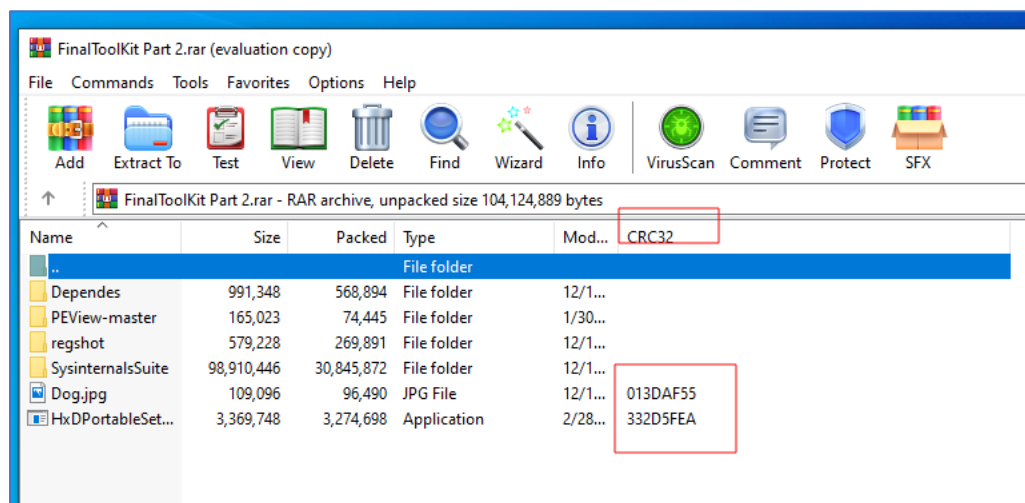
```
vanityAddresses
http://btc.blockr.io/api/v1/
coin/info/
status
markets
coinbase
address/balance/
balance
\DeleteItself.bat
del "{0}"
```

Part 2:

Identify the malicious File

The recent files were searched.

The rar on the Desktop was extracted



The Dog.jpg was located

Strings Tool

Strings tool was used to analyse it. The out of strings is redirected to a file str.txt

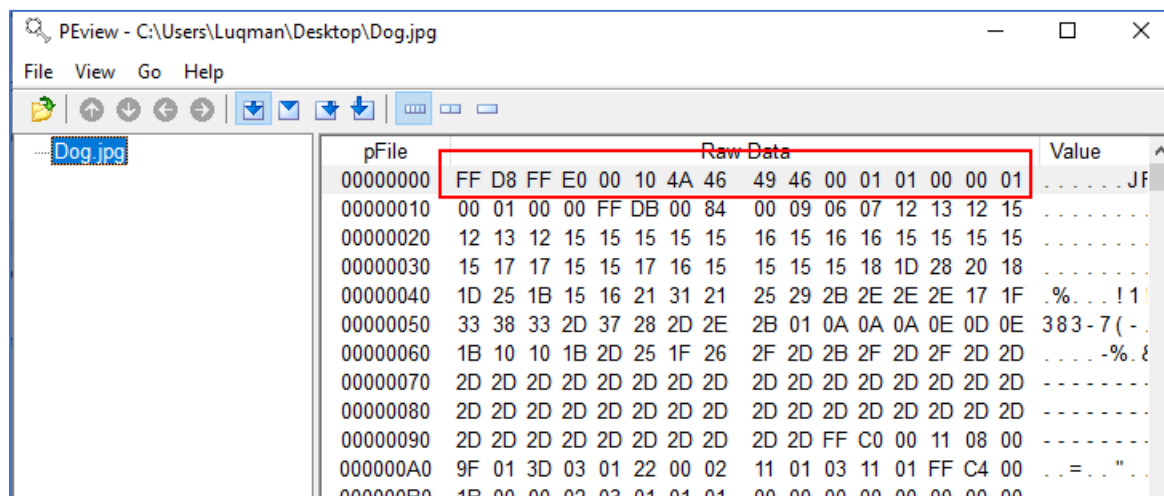
```
C:\Users\Lugman\Desktop\FinalToolKit Part 1\FinalToolKit Part 1\SysinternalsSuite> strings.exe C:\Users\Lugman\Desktop\Dog.jpg > str.txt
Strings v2.53 - Search for ANSI and Unicode strings in binary images.
Copyright (C) 1999-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

C:\Users\Lugman\Desktop\FinalToolKit Part 1\FinalToolKit Part 1\SysinternalsSuite>
```

A magic number is a number embedded at or near the beginning of a file that indicates its file format (i.e., the type of file it is). It is also sometimes referred to as a file signature.

PEview

Using PEView to check the file signature of “Dog.jpg ”



The magic bytes differ indicating the file could be malicious

Analyzing in virus total:

The file was checked in virustotal detects the dog.jpg to be malicious

SUMMARY	DETECTION	DETAILS	RELATIONS	COMMUNITY
Security Vendors' Analysis				
Avira (no cloud)	① DR/FakePic.Gen			
Cynet	① Malicious (score: 99)			
Cyren	① W32/Boaxxe.PQDO-5801			
Fortinet	① W32/Boaxxe.BVBltr			
Ikarus	① Dropper.FakePic			
NANO-Antivirus	① Trojan.Win32.Inject.cthmrm			
Rising	① Trojan.Inject8.103 (CLOUD)			
Tencent	① Win32.Trojan.Hiddencode.Akfv			
VBA32	① Trojan.Inject			
Acronis (Static ML)	✓ Undetected			
Ad-Aware	✓ Undetected			

SUMMARY

DETECTION

DETAILS

RELATIONS

COMMUNITY

Bundled Files

Scanned	Detections	File type	Name
2022-02-06	56 / 65	Win32 EXE	mcwsazmq.exe
2019-02-23	0 / 53	?	setup.dat

Graph Summary

2 bundled files

MD5	79bf480968f4b4be28a39fe3afa4b0d7
SHA-1	0c6bbb2054403daaba4fcdac316ff33e852ea411
SHA-256	42aeb242a30f7dea5a8b5f7c41682cfd3ce7c287f0695b223709c8a8f721532b
SSDEEP	1536:CbXwMpgpHzb9dZVX9fHMvG0D3XJcMZxshYdgOzLXehOTJHCyScYFwv5SZUsZMegh:C8agXdZt9P6D3XJcMX
TLSH	T172B3F11AAEC18973CA9382722D767375DBBBCB1891B14F83AB609F367C91153070E381
File type	JPEG
Magic	JPEG image data, JFIF standard 1.01
TrID	JFIF JPEG bitmap (38.1%)
TrID	JPEG bitmap (28.5%)
TrID	MP3 audio (ID3 v1.x tag) (23.8%)
TrID	MP3 audio (9.5%)
File size	106.54 KB (109096 bytes)
Cyren packer	appended, NSIS, appended
History	
First Seen In The Wild	2020-12-19 23:12:33 UTC
First Submission	2021-04-24 04:19:24 UTC
Last Submission	2022-01-31 20:49:54 UTC
Last Analysis	2022-04-29 18:55:11 UTC
Names	
Dog.jpg	
program_FF	

Some DLLs in Dog.jpg:

From the Strings.exe output, some dlls were found to be used

A jpg file does not have need of a Kernel32.dll, SHELL32.dll , USER32.dll. All these dlls make the jpg file suspicious

