

Zadanie - SIEM & SOC - Final Project

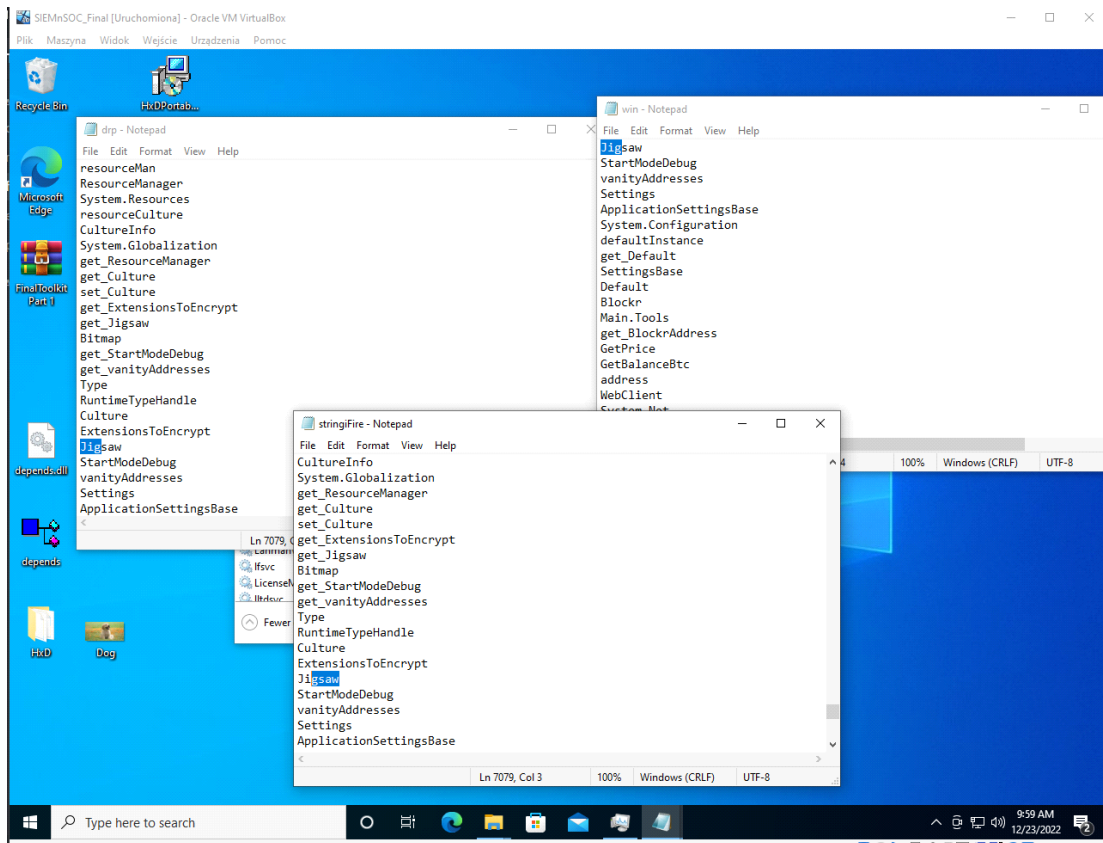
The malicious processes that I found are:

firefox.exe - This app is not installed in the system

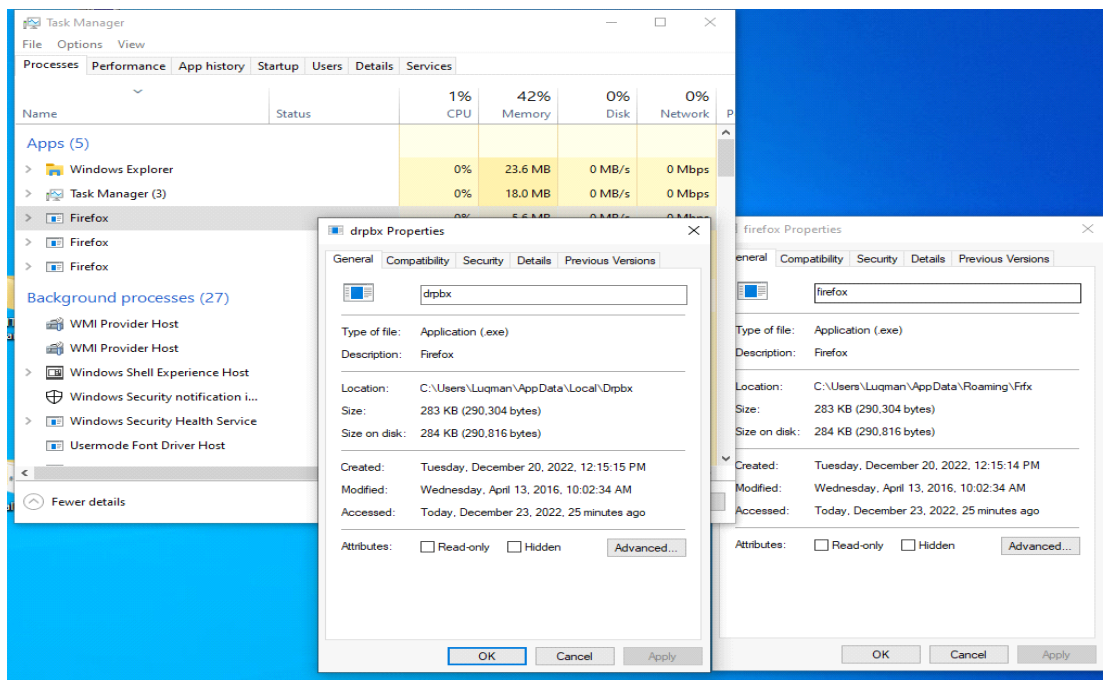
drpbx.exe - Does not exist in destined for him folder

WindowsUpdate.exe - Ment to be pre-installed in the system, not in Documents.

I used strings to prove they are malicious:

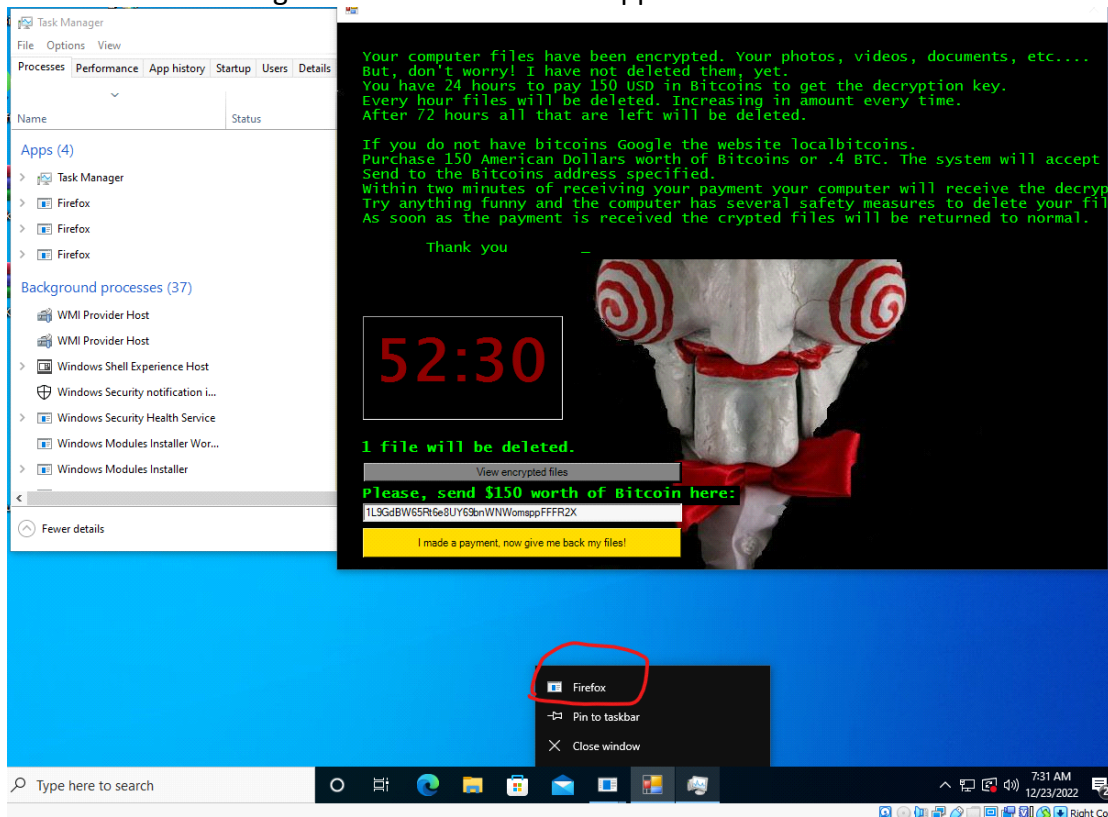


Directory of infected process:



This proves why malicious process and welcome screen are the same :

When I clicked the right mouse button on the app it shows firefox



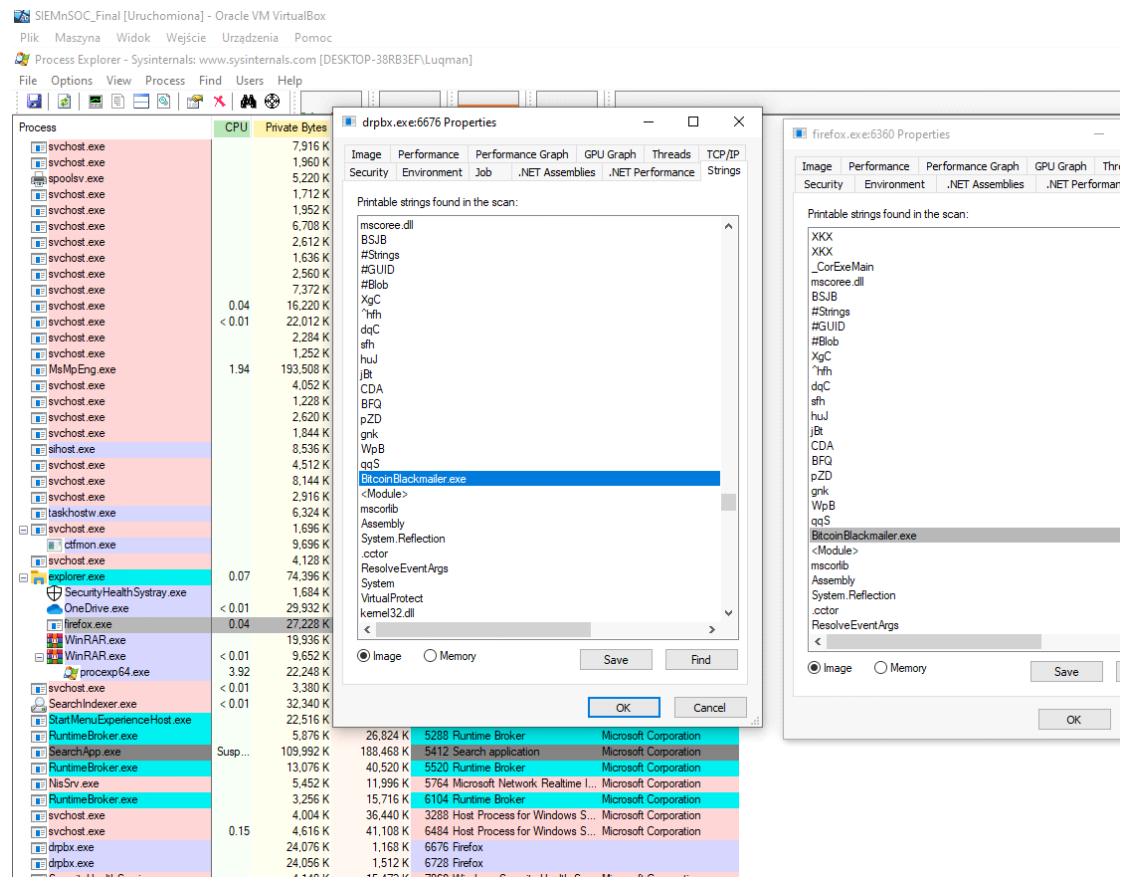
So the infected files are as showed before:

firefox.exe

drpbx.exe

WindowsUpdate.exe

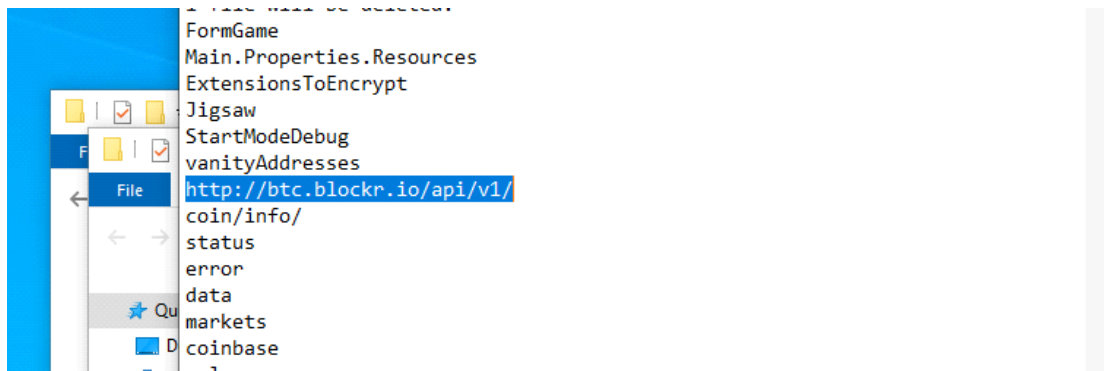
Strings indicated that this is malware:



```
stringiFire - Notepad
File Edit Format View Help
WelcomeMessage
TaskMessage
RansomUsd
Environment
SpecialFolder
StartModeType
Enum
value__
Debug
NothingHappens
DeleteItself
FormBackground
System.Windows.Forms
Form
components
IContainer
System.ComponentModel
timerActivateChecker
Timer
Ln 15, Col 6 100% Windows (CRLF) UTF-8
```

```
stringiFire - Notepad
File Edit Format View Help
GetManifestResourceStream
set_Position
ToLowerInvariant
IsNullOrEmpty
get_Flags
{{ file = {0}, ext = {1} }}
{{ file = {0}, fi = {1} }}
Congratulations. Your software has been registered. Confirmation code 994759
Email us this code in the chat to active your software. It can take up to 48
Thank you
Drpbx\drpbx.exe
Frfx\firefox.exe
System32Work\
Your computer files have been encrypted. Your photos, videos, documents, etc.
But, don't worry! I have not deleted them, yet.
You have 24 hours to pay 150 USD in Bitcoins to get the decryption key.
Every hour files will be deleted. Increasing in amount every time.
After 72 hours all that are left will be deleted.
If you do not have bitcoins Google the website localbitcoins.
Ln 1, Col 1 100% Windows (CRLF) UTF-8
```

I found associated website in strings of firefox.exe which is:



This site was associated with cryptocurrencies, now it's down, and that's why I wasn't able to check the IP. It's probably been used for scams and extorting money, and what surprised me also, there were no HTTPS implementations in it.

I terminated all processes, started Windows Defender, and run the update, which should work as a security measure, because Jigsaw is quite popular and doesn't work throughout internet and doesn't spread throu files

PART II

I've used magic bytes HxD to investigate te picture and it shows couple of interesting things like it uses .dll's on the system, and:

Decoded text

```
ExA.Ë.RegCloseKey.Ø.RegD
eleteValueA.Ô.RegDeleteK
eyA.ì.RegOpenKeyExA.ADVA
PI32.dll..8.ImageList_De
stroy.4.ImageList_AddMas
ked.7.ImageList_Create..
COMCTL32.dll....CoCreate
Instance....OleUninitial
ize.î.OleInitialize.e.Co
TaskMemFree.ole32.dll...
VerQueryValueA....GetFil
eVersionInfoA...GetFileV
ersionInfoSizeA.VERSION.
dll.....
```

which makes me think it is NOT only a picture.

I found 8 DLL's that this program uses

Checksum	Search (8 hits)	
Offset	Excerpt (hex)	Excerpt (text)
8741	72 73 69 6F 6E 00 00 4B 45 52 4E 45 4C 33 32 2E 64 6C 6C 00 00 C8 00 45 6E 64 50 61 69 6E 74 00	rsion..KERNEL32.dll..Ě.EndPaint.
8B43	65 73 73 61 67 65 41 00 00 55 53 45 52 33 32 2E 64 6C 6C 00 00 0E 02 53 65 6C 65 63 74 4F 62 6A	essageA..USER32.dll.....SelectObj
8BD4	74 42 6B 43 6F 6C 6F 72 00 00 47 44 49 33 32 2E 64 6C 6C 00 9A 00 53 48 46 69 6C 65 4F 70 65 72	tBkColor..GDI32.dll.š.SHFileOper
8C62	63 61 74 69 6F 6E 00 00 53 48 45 4C 4C 33 32 2E 64 6C 6C 00 E1 01 52 65 67 45 6E 75 6D 56 61 6C	cation..SHELL32.dll.á.RegEnumVal
8D05	4B 65 79 45 78 41 00 41 44 56 41 50 49 33 32 2E 64 6C 6C 00 00 38 00 49 6D 61 67 65 4C 69 73 74	KeyExA.ADVAPI32.dll..8.ImageList
8D51	72 65 61 74 65 00 00 43 4F 4D 43 54 4C 33 32 2E 64 6C 6C 00 00 10 00 43 6F 43 72 65 61 74 65 49	reate..COMCTL32.dll....CoCreatel
8DA2	73 6B 4D 65 6D 46 72 65 65 00 6F 6C 65 33 32 2E 64 6C 6C 00 0A 00 56 65 72 51 75 65 72 79 56 61	skMemFree.ole32.dll...VerQueryVa
8DF0	66 6F 53 69 7A 65 41 00 56 45 52 53 49 4F 4E 2E 64 6C 6C 00 00 00 00 00 00 00 00 00 00 00 00	foSizeA.VERSION.dll.....