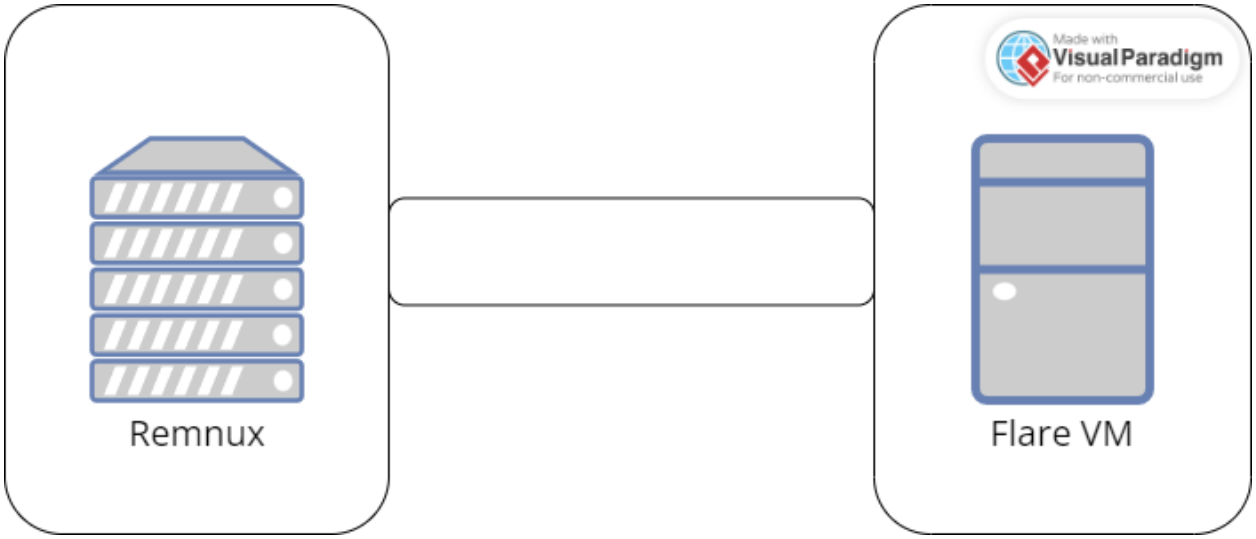
Introduction

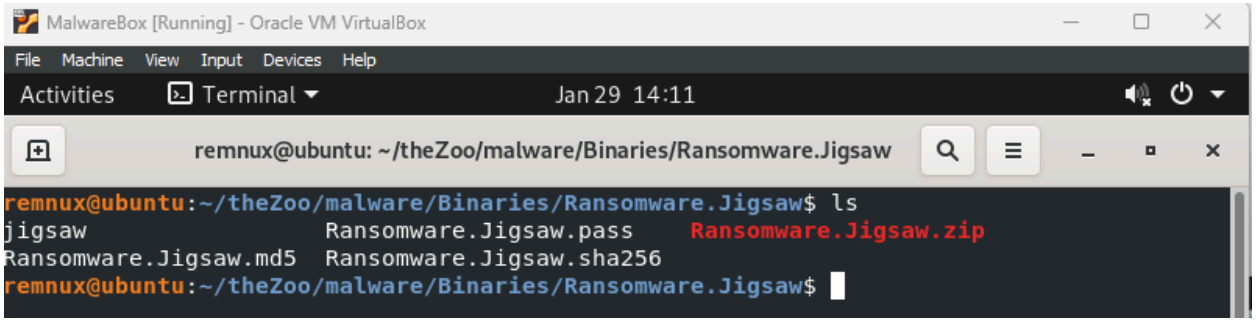
This report focuses on Jigsaw ransomware also known as the “BitcoinBlackmailer”. The tools used include a virtual machine with Flare VM installed for detonation and another virtual machine running Remnux (a Linux distro) to act as the DNS server to observe the behaviour of the malware over a connection.

Network Typology



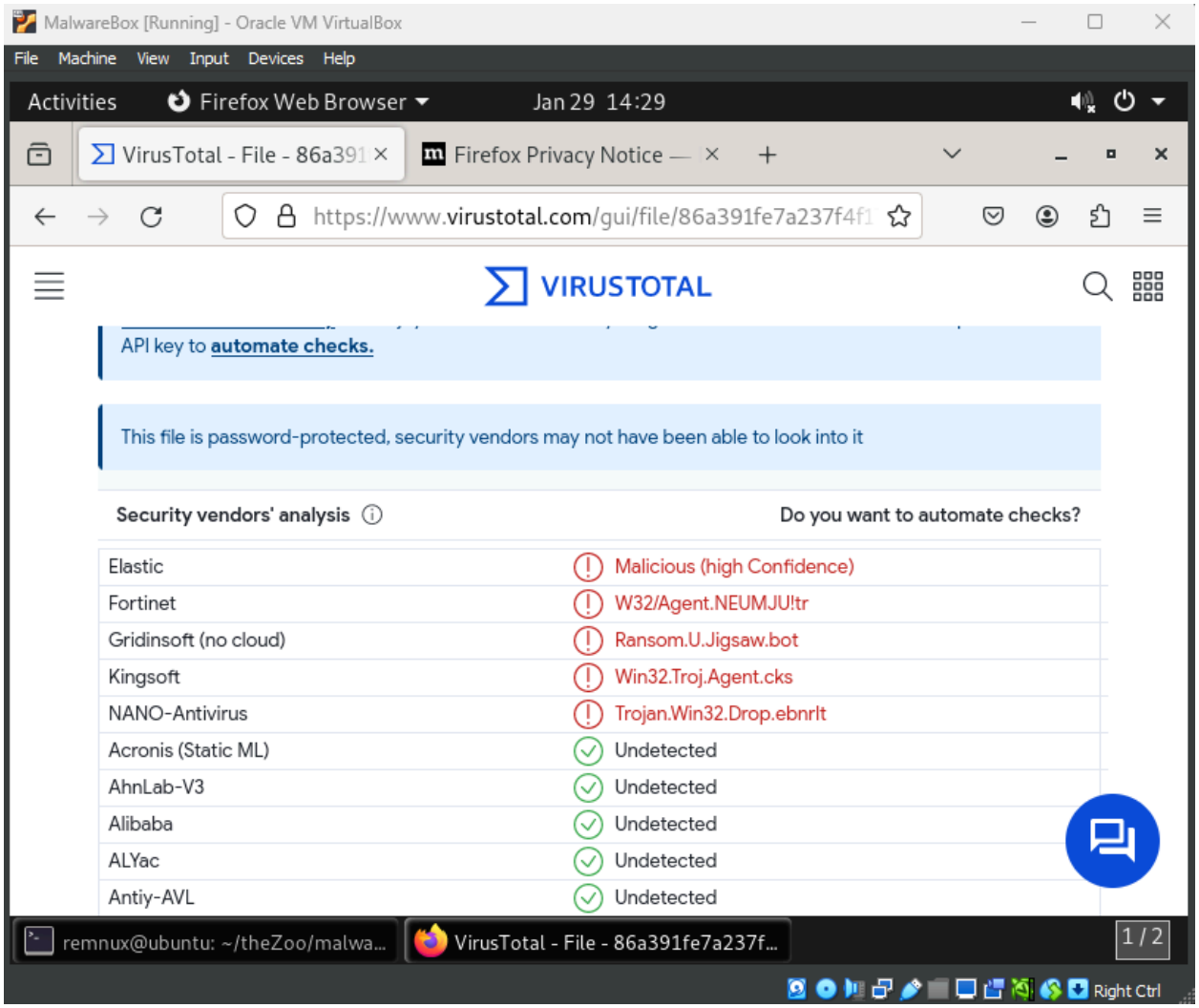
The two virtual machines are set to host-only to isolate the malware inside the network. You mustn't bridge them to any other virtual machine, or they might expose them to the malware once you detonate.

Fingerprinting



The malware to be analyzed is a ransomware called Jigsaw. We will load it up on remnux and unzip the malware binary from theZoo.

Report prepared by Niccolo Arboleda

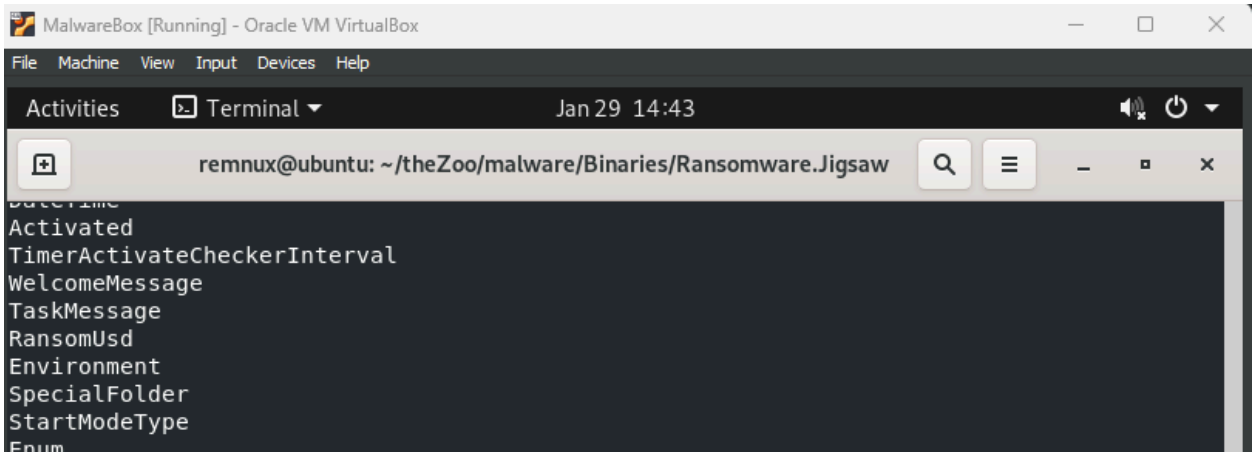


The first thing to do is see if this is a known Malware by extracting the hash from the md file and putting it into the VirusTotal (online malware repository) search. We can see that a few vendors have recognized this as a malicious program. A lot of information is also available if it is a known malware.

Jigsaw Hash (for reference):
footprint >
sha256,3AE96F73D805E1D3995253DB4D910300D8442EA603737A1428B613061E7F61E7

Filename: jigsaw

Report prepared by Niccolo Arboleda



Using the strings command, we can know the malware's processes in an infected system from start-up files, dll files, write commands and more.

Static Analysis

property	value
footprint > sha256	3AE96F73D805E1D3995253DB4D910300D8442EA603737A1428B613061E7F61E7
first-bytes-hex	4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00
first-bytes-text	M Z . . . . . @ . . . . .
file > size	290304 bytes
entropy	7.678
signature	Microsoft .NET
tooling	**costura .NET loader**
file-type	executable
cpu	32-bit
subsystem	**GUI**
file-version	37.0.2.5583
description	Firefox
stamps	
compiler-stamp	Thu Mar 31 06:28:14 2016 | UTC
debug-stamp	n/a
resource-stamp	n/a
import-stamp	n/a
export-stamp	n/a
names	
file	c:\users\malware\desktop\jigsaw
debug	n/a
export	n/a
version	BitcoinBlackmailer.exe
manifest	MyApplication.app
.NET > module	BitcoinBlackmailer.exe
certificate > program-name	n/a

Report prepared by Niccolo Arboleda

To start the basic static analysis, we put the jigsaw file inside our flare VM machine, and then we load the malware file into pestudio which can conduct a malware initial assessment. We look at the basic output and see that the file is executable, has a microsoft.NET signature, file version and other useful information to see the nature of the file.

property	value	value
section	section[0]	section[1]
name	!mmUPp	.text
footprint > sha256	2219DC92CF69A1E7780E019...	403EBD87FC73D52F2842FA4...
entropy	7.999	5.391
file-ratio (99.65%)	73.72 %	24.87 %
raw-address (begin)	0x00000400	0x00034800
raw-address (end)	0x00034800	0x00046200
raw-size (289280 bytes)	0x00034400 (214016 bytes)	0x00011A00 (72192 bytes)
virtual-address	0x00002000	0x00038000
virtual-size (287044 bytes)	0x00034260 (213600 bytes)	0x00011878 (71800 bytes)

Next, we can go to the file sections and look to see if the file is compressed and if it will hinder further tools from working on it. If the raw and virtual sizes have a huge discrepancy, they have most likely been packed or compressed. It looks like it is not compressed.

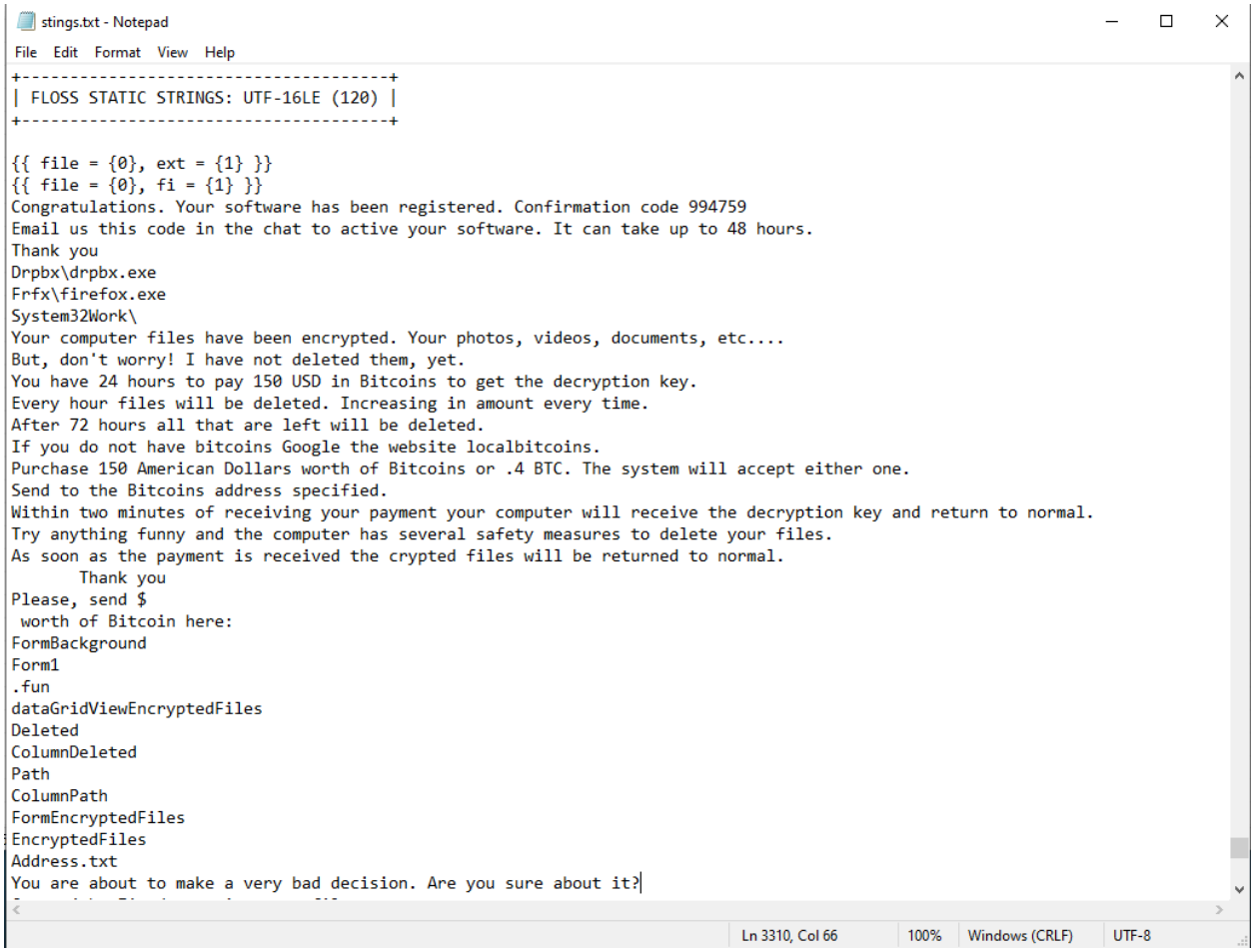
encoding (2)	size (bytes)	location	flag (21)	label (369)	group (10)	technique (5)	value
ascii	12	section:.text	-	import	windowing	-	SetWindowPos
ascii	12	-	-	import	windowing	-	SetWindowPos
ascii	25	section:.text	-	-	resource	-	ReadFromEmbeddedResources
ascii	25	-	-	-	resource	-	ReadFromEmbeddedResources
ascii	8	section:.text	-	import	registry	-	Registry
ascii	8	-	-	import	registry	-	Registry
ascii	11	section:.text	-	guid	registry	-	RegistryKey
ascii	11	-	-	guid	registry	-	RegistryKey
ascii	16	section:.text	x	-	obfuscation	-	FromBase64String
ascii	15	section:.text	-	-	obfuscation	T1001 | Data Obfuscation	CreateEncryptor
ascii	16	-	x	-	obfuscation	-	FromBase64String
ascii	15	-	-	-	obfuscation	T1001 | Data Obfuscation	CreateEncryptor
ascii	14	section:.text	-	-	network	-	DownloadString
ascii	14	-	-	-	network	-	DownloadString
ascii	14	section:.text	x	import	memory	T1055 | Process Injection	VirtualProtect
ascii	12	section:.text	x	import	memory	T1055 | Process Injection	MemoryStream
ascii	14	-	x	import	memory	T1055 | Process Injection	VirtualProtect
ascii	12	-	x	import	memory	T1055 | Process Injection	MemoryStream
ascii	15	section:.text	-	-	file	-	CreateDirectory
ascii	12	section:.text	-	-	file	-	WriteAllText
ascii	15	-	-	-	file	-	CreateDirectory
ascii	12	-	-	-	file	-	WriteAllText
ascii	7	section:.text	-	utility	execution	-	Process
ascii	7	-	-	utility	execution	-	Process
ascii	7	section:.text	x	-	execution	T1106 | Execution through API	WinExec
ascii	18	section:.text	x	-	execution	-	GetProcessesByName
ascii	5	section:.text	-	-	execution	T1497 | Sandbox Evasion	Sleep
ascii	18	section:.text	-	-	execution	-	get_ExecutablePath
ascii	7	-	x	-	execution	T1106 | Execution through API	WinExec
ascii	18	-	x	-	execution	-	GetProcessesByName

Next, we can look at the stings section to get an idea of the type of actions this malware takes. It can be seen on the right side of the screen.

Report prepared by Niccolo Arboleda

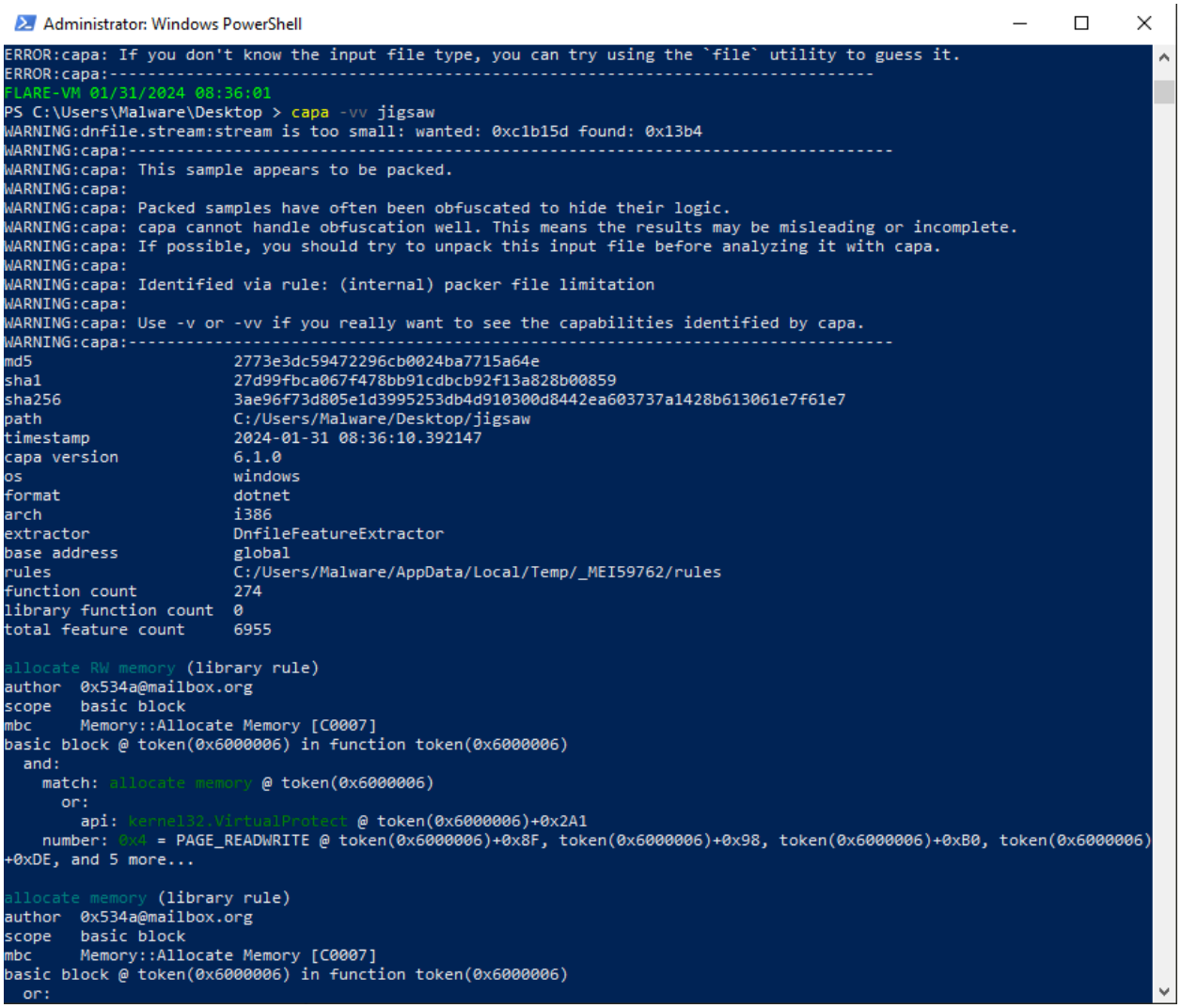
library (3)	duplicate (0)	flag (0)	first-thunk-original (INT)	first-thunk (IAT)	type (3)	imports (496)	group	description
mscoree.dll	-	-	0x00039AD0	0x0004E000	implicit	493	-	Microsoft .NET Runtime Execution Engine
kernel32.dll	-	-	n/a	n/a	p/invoke	2	-	Windows NT BASE API Client
user32.dll	-	-	n/a	n/a	p/invoke	1	-	Multi-User Windows USER API Client Library

As a last step for pestudio we can look at the libraries found within the file. We can see mscoree.dll, kernel32.dll, and user32.dll.



The next tool we are going to use is called floss. It extracts strings from the malware file to see what information it would convey to the victim. In our instance, we can see that jigsaw is a ransomware that encrypts files and coerces the victim to hand over 0.4 BTC in exchange for their files back

Report prepared by Niccolo Arboleda

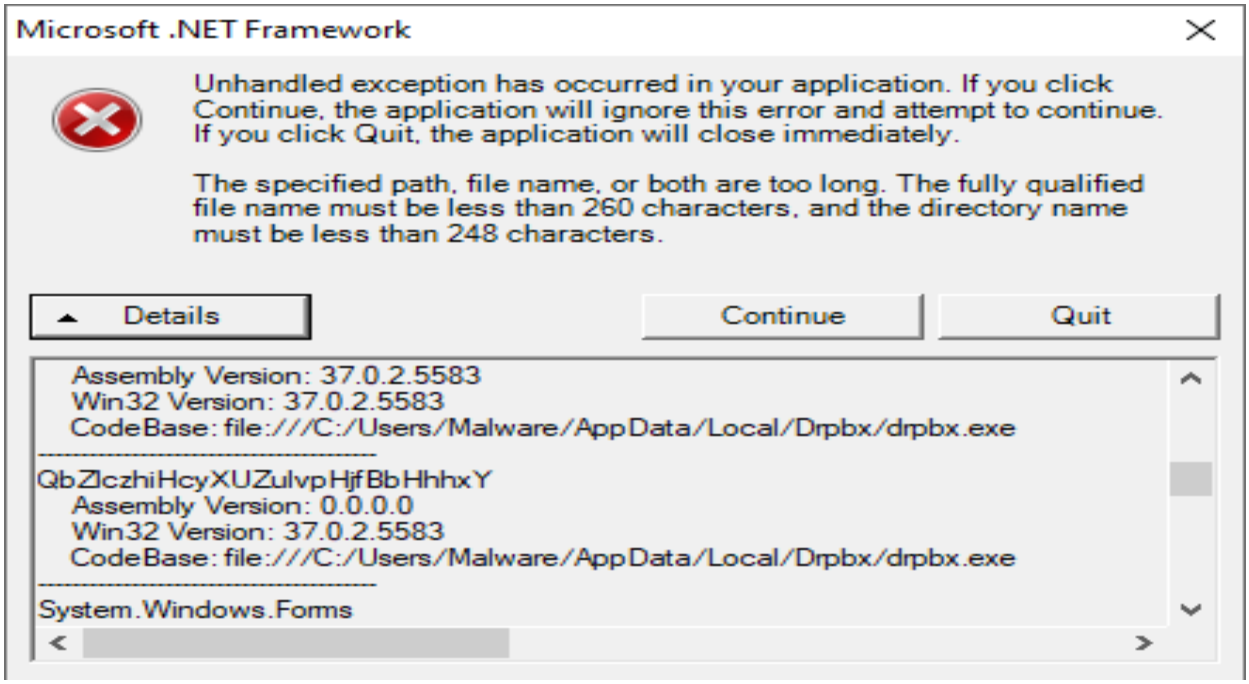


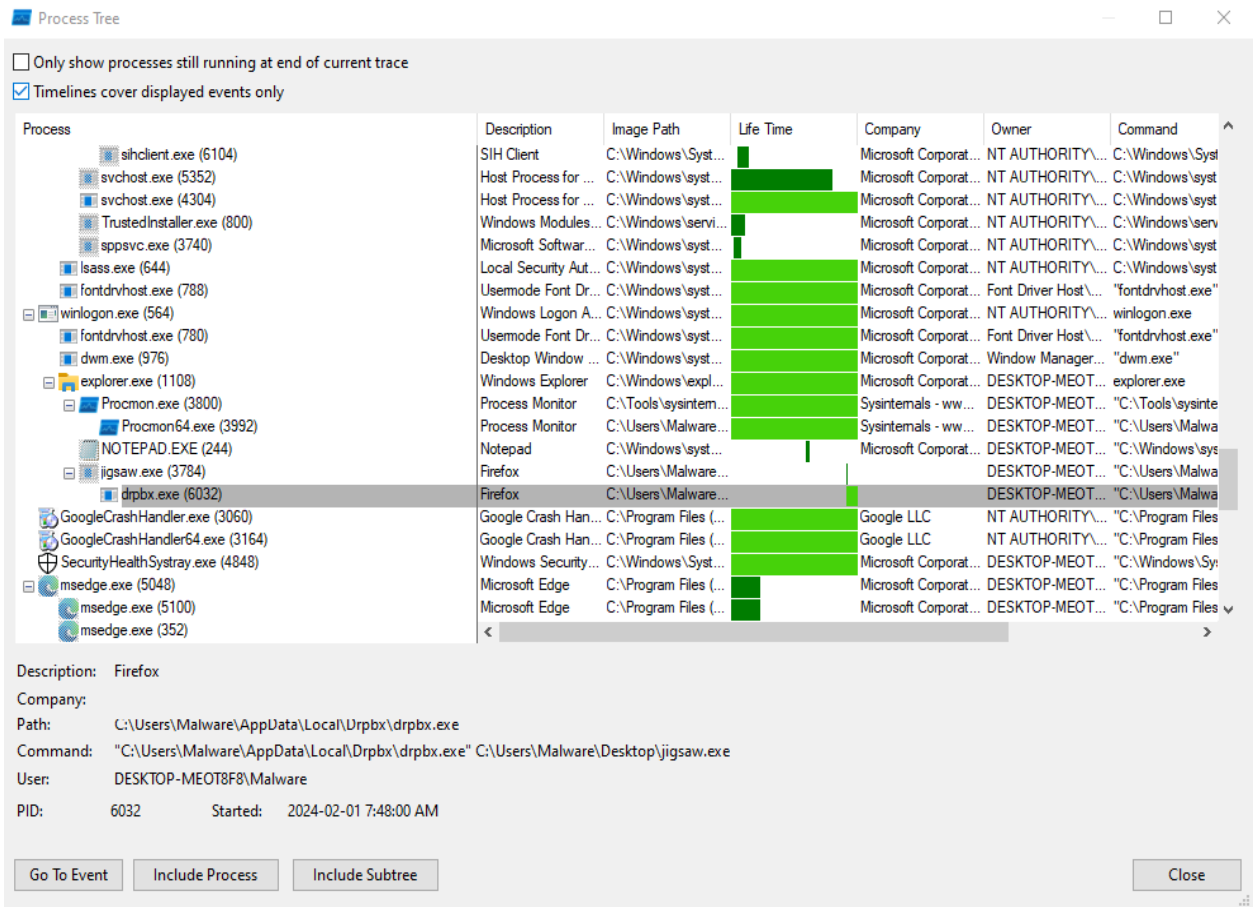
Using another tool called capa we can mirror a report to the MIREATTACK framework; unfortunately, it turns out the file is actually packed, and I cannot get the report I wanted. I used verbose Linux command to force the application to see where capa thinks it employs the processes within the malware's code.

Dynamic Analysis

To start the dynamic analysis, the procmon application will be loaded to monitor the processes in the computer as we run the malware to see what it did to the system and get an idea of its behaviour.

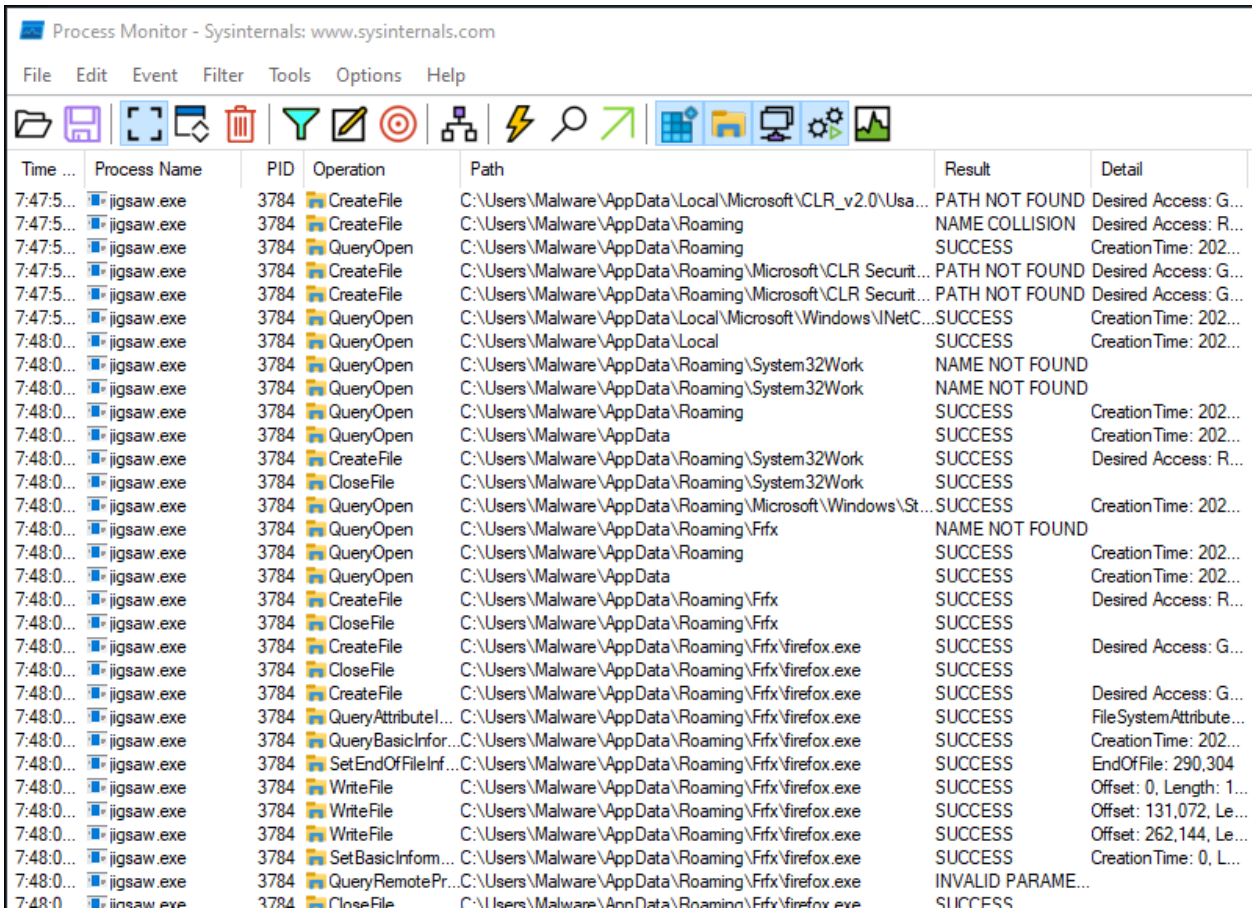
Report prepared by Niccolo Arboleda





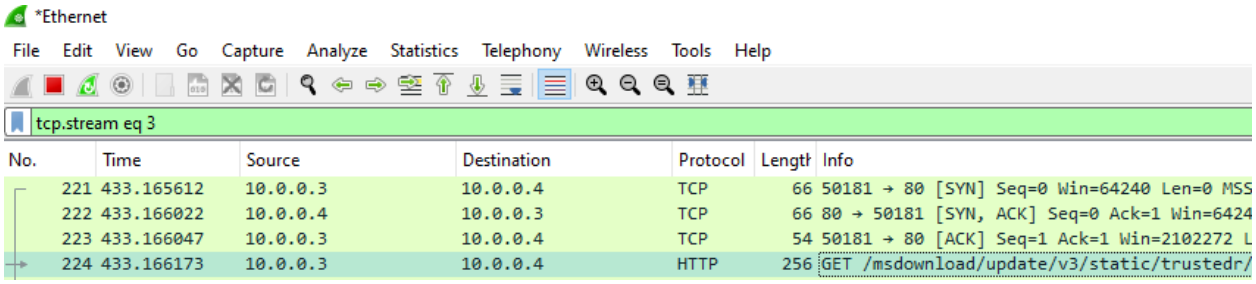
Report prepared by Niccolo Arboleda

In procmon, there is a process tree program where we can see what opened right after detonating the malware. There is a drpbx.exe that is activated on detonation, and it is tied to the Firefox browser and .NET framework.



Time ...	Process Name	PID	Operation	Path	Result	Detail
7:47:5...	jigsaw.exe	3784	CreateFile	C:\Users\Malware\AppData\Local\Microsoft\CLR_v2.0\Usa...	PATH NOT FOUND	Desired Access: G...
7:47:5...	jigsaw.exe	3784	CreateFile	C:\Users\Malware\AppData\Roaming	NAME COLLISION	Desired Access: R...
7:47:5...	jigsaw.exe	3784	QueryOpen	C:\Users\Malware\AppData\Roaming	SUCCESS	CreationTime: 202...
7:47:5...	jigsaw.exe	3784	CreateFile	C:\Users\Malware\AppData\Roaming\Microsoft\CLR Securit...	PATH NOT FOUND	Desired Access: G...
7:47:5...	jigsaw.exe	3784	CreateFile	C:\Users\Malware\AppData\Roaming\Microsoft\CLR Securit...	PATH NOT FOUND	Desired Access: G...
7:47:5...	jigsaw.exe	3784	QueryOpen	C:\Users\Malware\AppData\Local\Microsoft\Windows\INetC...	SUCCESS	CreationTime: 202...
7:48:0...	jigsaw.exe	3784	QueryOpen	C:\Users\Malware\AppData\Local	SUCCESS	CreationTime: 202...
7:48:0...	jigsaw.exe	3784	QueryOpen	C:\Users\Malware\AppData\Roaming\System32Work	NAME NOT FOUND	
7:48:0...	jigsaw.exe	3784	QueryOpen	C:\Users\Malware\AppData\Roaming\System32Work	NAME NOT FOUND	
7:48:0...	jigsaw.exe	3784	QueryOpen	C:\Users\Malware\AppData\Roaming	SUCCESS	CreationTime: 202...
7:48:0...	jigsaw.exe	3784	QueryOpen	C:\Users\Malware\AppData	SUCCESS	CreationTime: 202...
7:48:0...	jigsaw.exe	3784	CreateFile	C:\Users\Malware\AppData\Roaming\System32Work	SUCCESS	Desired Access: R...
7:48:0...	jigsaw.exe	3784	CloseFile	C:\Users\Malware\AppData\Roaming\System32Work	SUCCESS	
7:48:0...	jigsaw.exe	3784	QueryOpen	C:\Users\Malware\AppData\Roaming\Microsoft\Windows\St...	SUCCESS	CreationTime: 202...
7:48:0...	jigsaw.exe	3784	QueryOpen	C:\Users\Malware\AppData\Roaming\Frfx	NAME NOT FOUND	
7:48:0...	jigsaw.exe	3784	QueryOpen	C:\Users\Malware\AppData\Roaming	SUCCESS	CreationTime: 202...
7:48:0...	jigsaw.exe	3784	QueryOpen	C:\Users\Malware\AppData	SUCCESS	CreationTime: 202...
7:48:0...	jigsaw.exe	3784	CreateFile	C:\Users\Malware\AppData\Roaming\Frfx	SUCCESS	Desired Access: R...
7:48:0...	jigsaw.exe	3784	CloseFile	C:\Users\Malware\AppData\Roaming\Frfx	SUCCESS	
7:48:0...	jigsaw.exe	3784	CreateFile	C:\Users\Malware\AppData\Roaming\Frfx\firefox.exe	SUCCESS	Desired Access: G...
7:48:0...	jigsaw.exe	3784	CloseFile	C:\Users\Malware\AppData\Roaming\Frfx\firefox.exe	SUCCESS	
7:48:0...	jigsaw.exe	3784	CreateFile	C:\Users\Malware\AppData\Roaming\Frfx\firefox.exe	SUCCESS	Desired Access: G...
7:48:0...	jigsaw.exe	3784	QueryAttributeI...	C:\Users\Malware\AppData\Roaming\Frfx\firefox.exe	SUCCESS	FileSystemAttribute...
7:48:0...	jigsaw.exe	3784	QueryBasicInfor...	C:\Users\Malware\AppData\Roaming\Frfx\firefox.exe	SUCCESS	CreationTime: 202...
7:48:0...	jigsaw.exe	3784	SetEndOfFileInf...	C:\Users\Malware\AppData\Roaming\Frfx\firefox.exe	SUCCESS	EndOfFile: 290,304
7:48:0...	jigsaw.exe	3784	WriteFile	C:\Users\Malware\AppData\Roaming\Frfx\firefox.exe	SUCCESS	Offset: 0, Length: 1...
7:48:0...	jigsaw.exe	3784	WriteFile	C:\Users\Malware\AppData\Roaming\Frfx\firefox.exe	SUCCESS	Offset: 131,072, Le...
7:48:0...	jigsaw.exe	3784	WriteFile	C:\Users\Malware\AppData\Roaming\Frfx\firefox.exe	SUCCESS	Offset: 262,144, Le...
7:48:0...	jigsaw.exe	3784	SetBasicInform...	C:\Users\Malware\AppData\Roaming\Frfx\firefox.exe	SUCCESS	CreationTime: 0, L...
7:48:0...	jigsaw.exe	3784	QueryRemotePr...	C:\Users\Malware\AppData\Roaming\Frfx\firefox.exe	INVALID PARAME...	
7:48:0	jigsaw.exe	3784	CloseFile	C:\Users\Malware\AppData\Roaming\Frfx\firefox.exe	SUCCESS	

The process monitor reveals the number of actions the malware took upon detonation from making queries to writing and creating files. The host computer can no longer be restored to the previous state without loading a backup.



No.	Time	Source	Destination	Protocol	Length	Info
221	433.165612	10.0.0.3	10.0.0.4	TCP	66	50181 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS
222	433.166022	10.0.0.4	10.0.0.3	TCP	66	80 → 50181 [SYN, ACK] Seq=0 Ack=1 Win=6424
223	433.166047	10.0.0.3	10.0.0.4	TCP	54	50181 → 80 [ACK] Seq=1 Ack=1 Win=2102272 L
224	433.166173	10.0.0.3	10.0.0.4	HTTP	256	GET /msdownload/update/v3/static/trustedr/

Wireshark is used In order to see what the malware is doing on the network. It is good to consider what kind of requests it would have sent to the internet if it were connected.

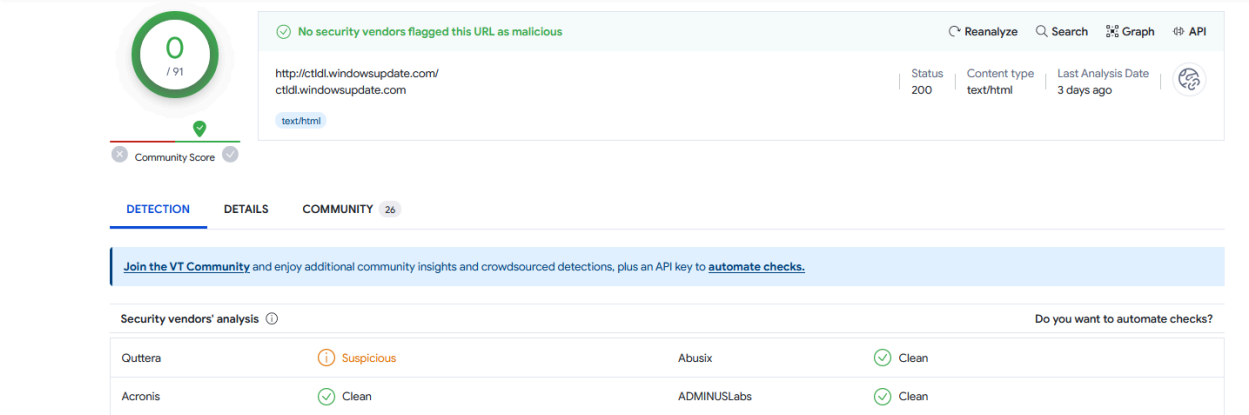
Report prepared by Niccolo Arboleda

Wireshark · Follow HTTP Stream (tcp.stream eq 3) · Ethernet

```
GET /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?ca8a2f3cc7519940 HTTP/1.1
Connection: Keep-Alive
Accept: */*
User-Agent: Microsoft-CryptoAPI/10.0
Host: ctldl.windowsupdate.com

HTTP/1.1 200 OK
Connection: Close
Content-Type: text/html
Date: Wed, 31 Jan 2024 03:36:40 GMT
Content-Length: 258
Server: INetSim HTTP Server

<html>
  <head>
    <title>INetSim default HTML page</title>
  </head>
  <body>
    <p></p>
    <p align="center">This is the default HTML page for INetSim HTTP server fake mode.</p>
    <p align="center">This file is an HTML document.</p>
  </body>
</html>
```



There is a request going to ctldl.windowsupdate.com. Using VirusTotal to see if any providers have flagged it as malicious can see if there is a connection to the malware.

Summary

The jigsaw ransomware once run changes the system configuration and runs processes that cripple the host computer and hold data hostage. It blackmails the user, threatening to delete their data if they do not transfer Bitcoin to the perpetrator. This report shows how it operates once it runs in a system through basic static and dynamic analysis.

Report prepared by Niccolo Arboleda