

Date: August 26th, 2018.

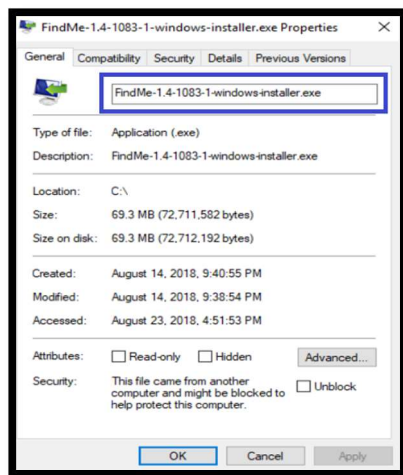
Description: The software FindMe-1.4-1083-1 by using a compression technique prevent the identification of malicious libraries in the software by obfuscation. The entropy results suggests encryption along with the compression process. That being said, once the file is unpacked it is possible to identify those libraries and how they can compromise a computer. The software relies in the use of a TLS callback and an additional executable file to enable the malicious libraries and their access to suspicious websites. The unpacked software can be exploited by several different types of documented techniques.

Summary

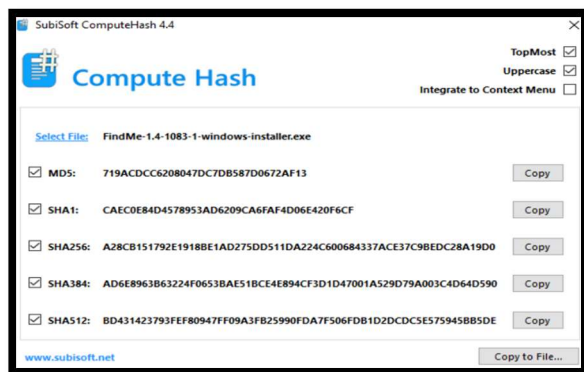
File Identification	2
Preliminar Threat Analysis	2
File Analysis.....	4
Unpacking the Software.....	9
Websites	11
Unpacked and vulnerabilities.....	11
Attacks	13
References	14

File Identification

The executable file

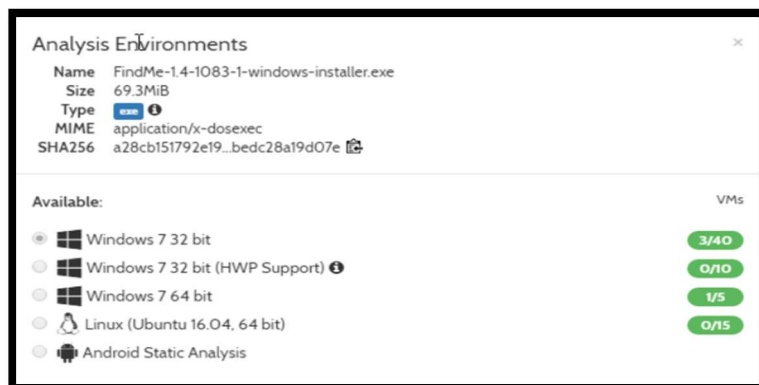


The calculated hash for the packed version:



Preliminar Threat Analysis

Initially the vulnerabilities are not easily identified with ambiguous results:



HYBRID ANALYSIS

Analysis Overview

[Report Abuse](#)

Submission name:	FindMe-1.4-1083-1-windows-installer.exe	no specific threat
Size:	69MiB	#evasive
Type:	peexe	Link
Mime:	application/x-dosexec	Twitter
SHA256:	a28cb151792e1918be1ad275dd511da224c600684337ace37c9 bedc28a19d07e	E-Mail
Operating System:	Windows	
Last Anti-Virus Scan:	08/24/2018 02:19:35	
Last Sandbox Report:	08/10/2018 14:57:47	

HYBRID ANALYSIS

FindMe-1.4-1083-1-windows-installer.exe

ambiguous

This report is generated from a file or URL submitted to this webservice on August 10th 2018 14:57:47 (CEST) not enough data to reliably determine

Guest System: Windows 7 32 bit, Home Premium, 6.1 (build 7601), Service Pack 1

Report generated by Falcon Sandbox v8.10 © Hybrid Analysis

[Overview](#)
[Login to Download Sample \(69MiB\)](#)
[Downloads](#)
[External Reports](#)
[Re-analyze](#)

[Hash Not Seen Before](#)
[Report Abuse](#)

Incident Response

Risk Assessment

Remote Access	Reads terminal service related keys (often RDP related)
Ransomware	Contains ability to create/switch the desktop
Spyware	Contains ability to open the clipboard Contains ability to retrieve keyboard strokes
Fingerprint	Reads the active computer name Reads the cryptographic machine GUID Reads the windows product ID

Falcon Sandbox Reports

NO VERDICT

FindMe-1.4-108...

Analyzed on: 08/10/2018 ...

Environment: Windows 7 ...

Threat Score: N/A

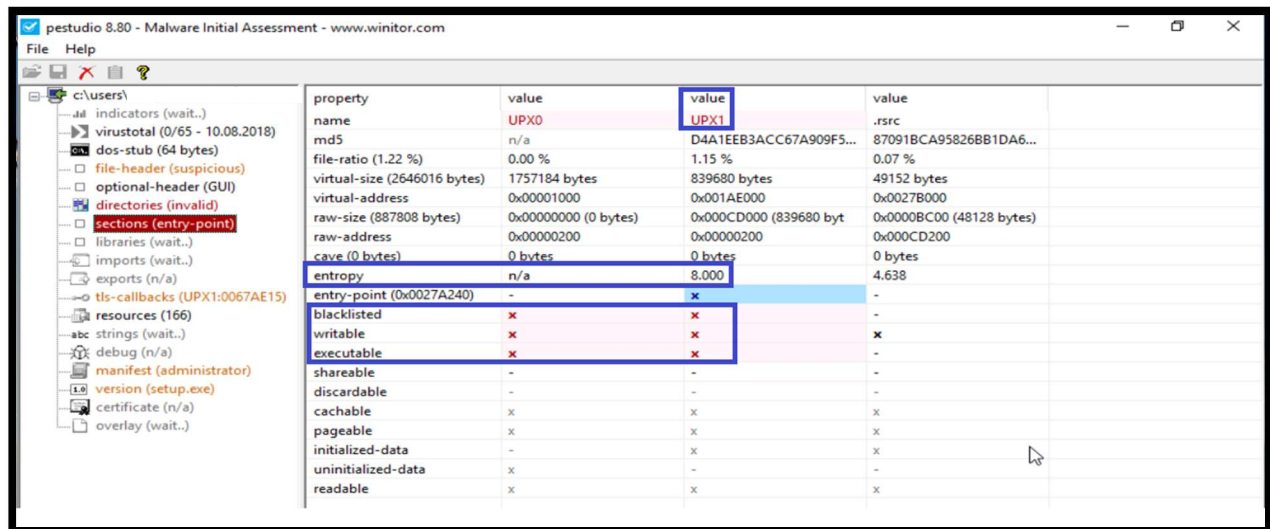
AV Detection: Marked as ...

Indicators: 7 33

Network: (none)

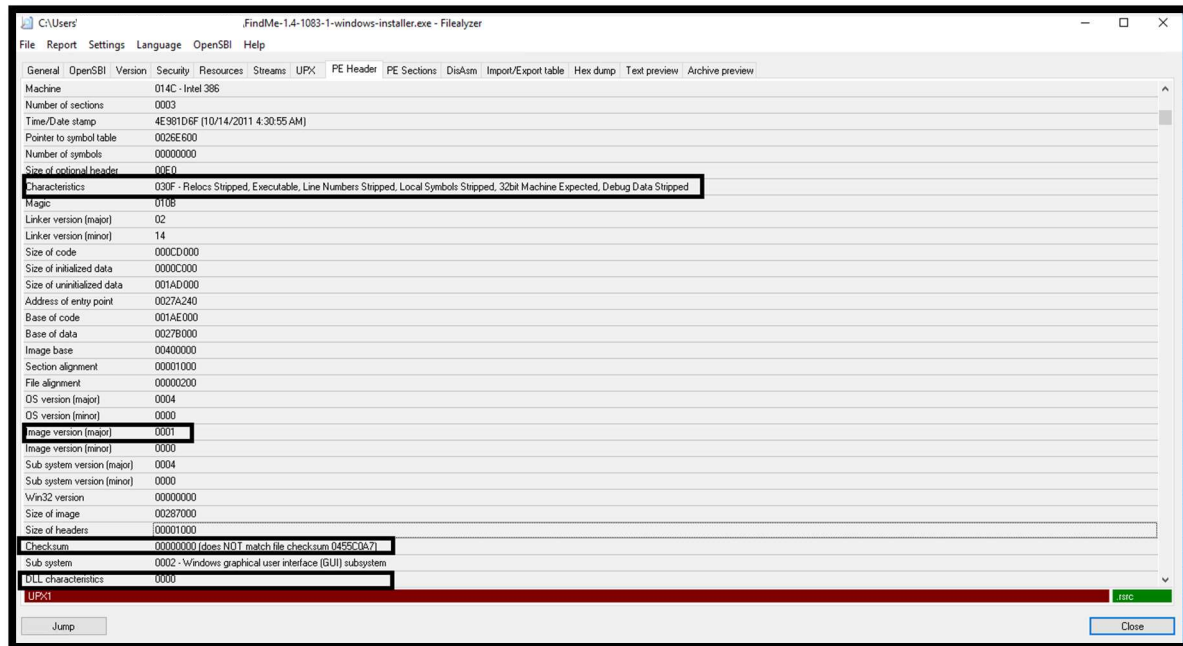
File Analysis

The entropy of 8 suggests encryption. The file has also writable and executable properties and is located in the entry-point. This may have obfuscated the initial analysis using anti-virus.

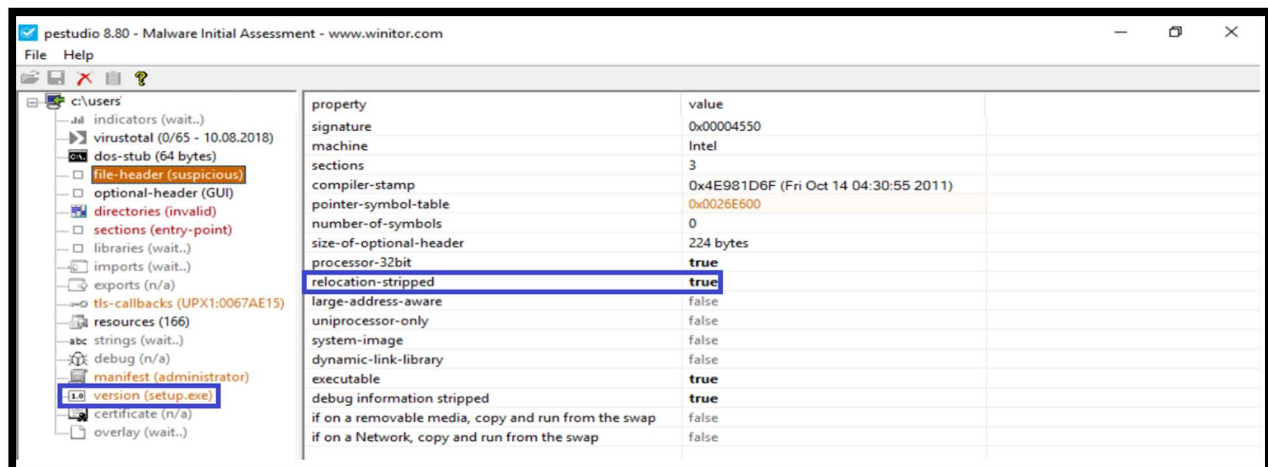


Some red flags are noticed in the PE Header, mainly related to the checksum, image version and the relocation stripped considering that:

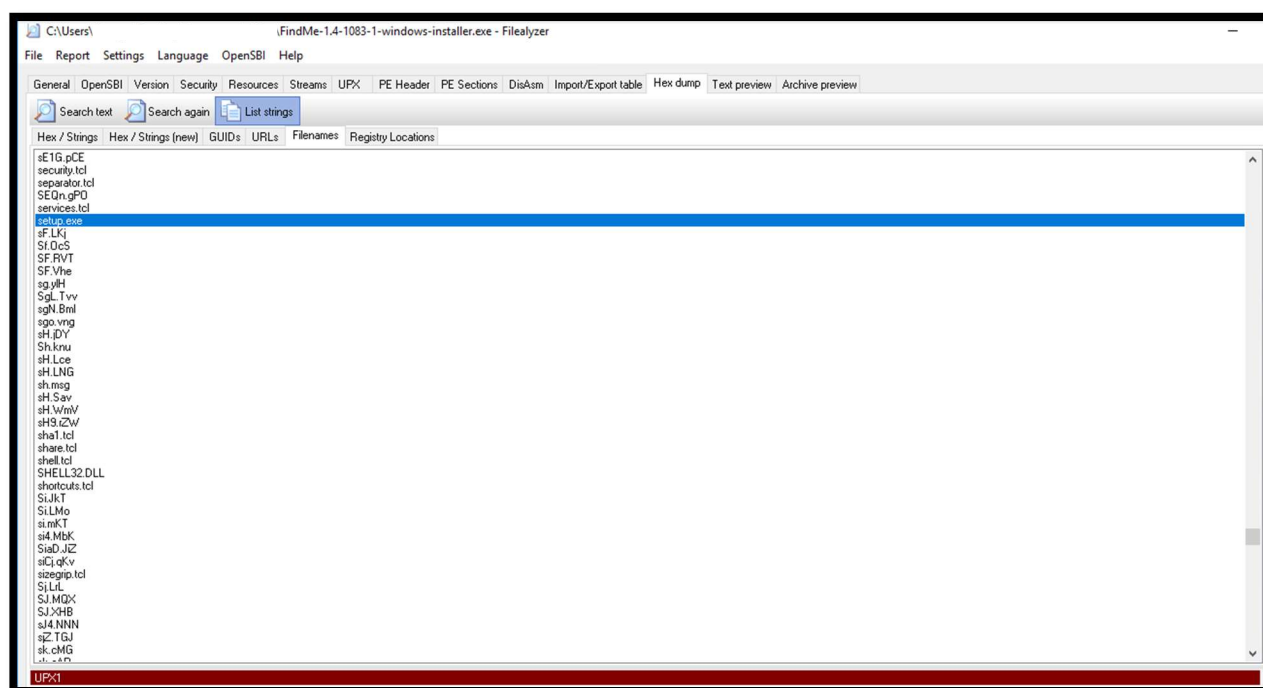
“DLLCharacteristics, MajorImageVersion, and CheckSum are equal to zero in more than 90% malware samples. However, most benign executables contain significant higher values in such fields” (Yibin Liao).



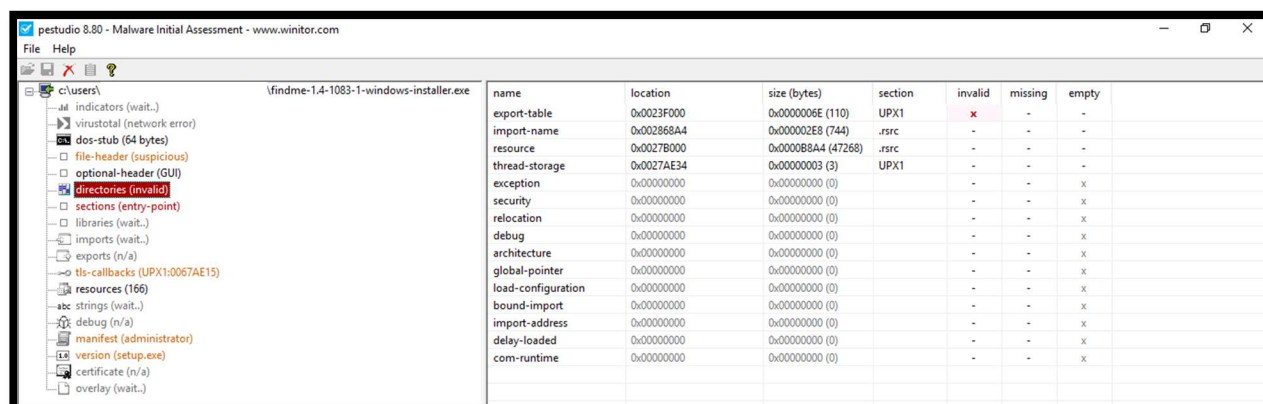
The relocation-stripped increases the susceptibility to code-reuse attacks. And as you can see as well another executable file (setup.exe) is embedded as part of the executable file. A possible explanation is that this file may be responsible to execute the *.dll files in the entry point.

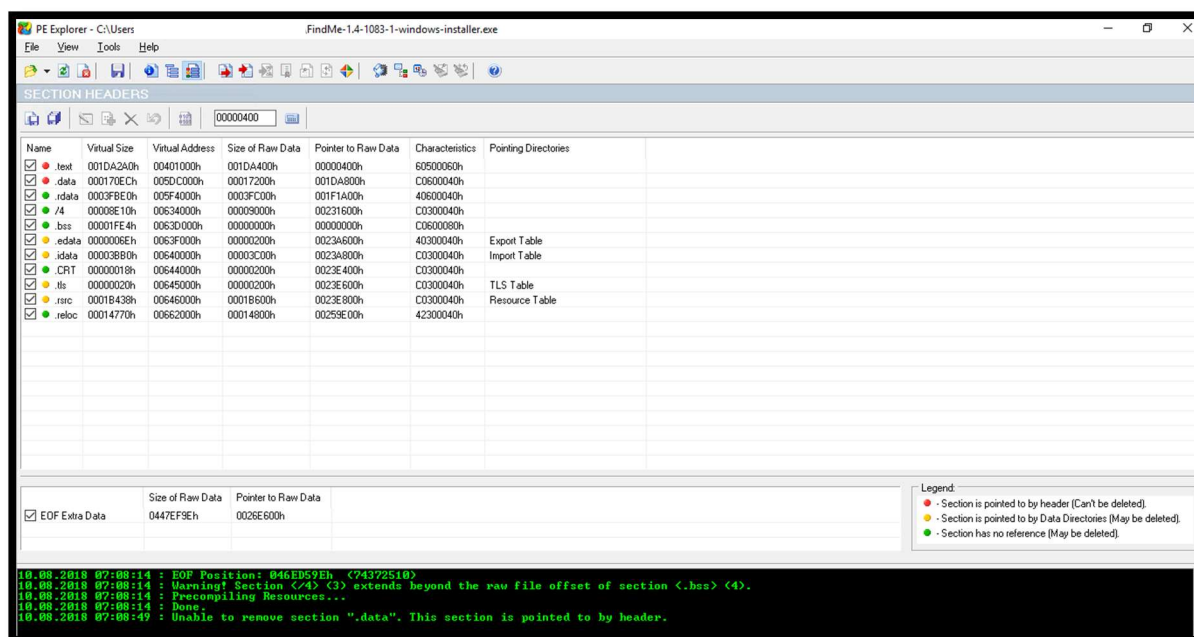
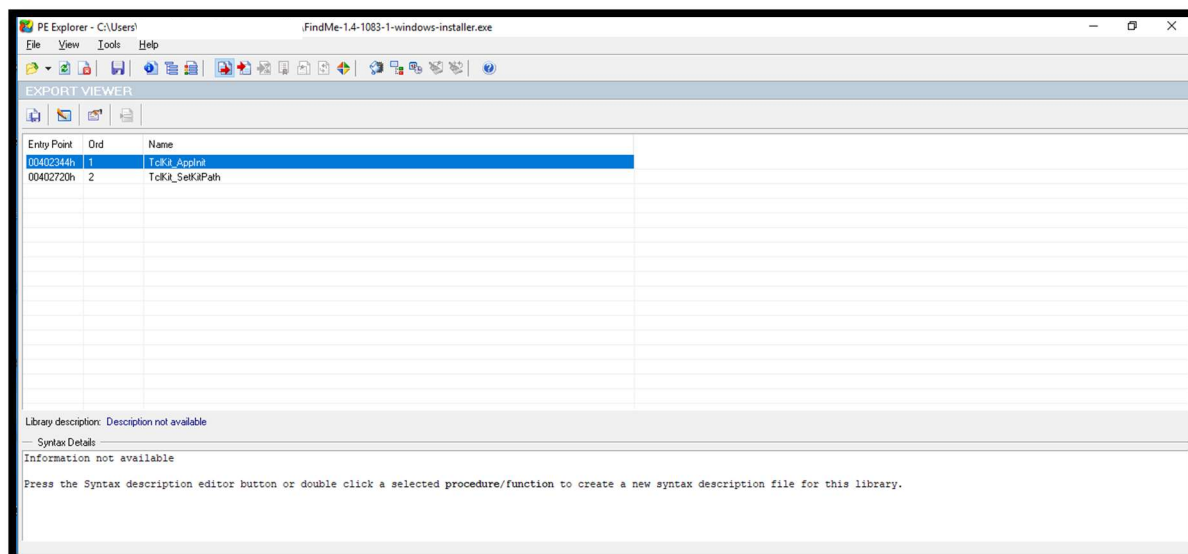


The executable file presented in the previous can be located through the strings as well:



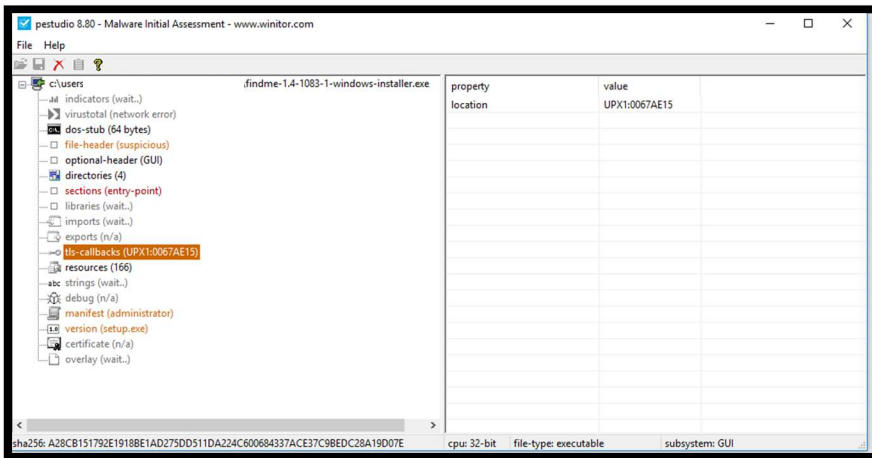
The invalid directory is likely to be associated with two export tables TcIKit_Applnit and TcIKit_SetKitPath and to be related to the tls-callbacks.



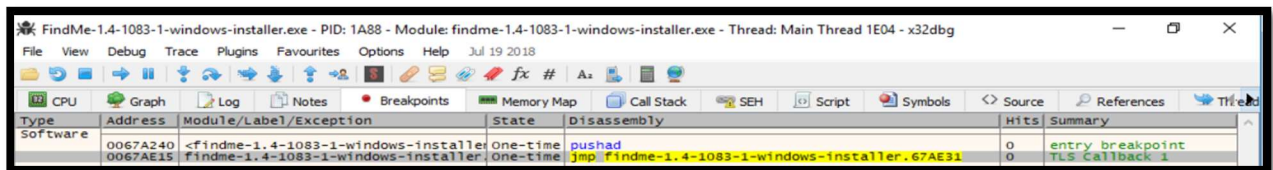


Note that the section “.data” is pointed to by header. Which means that there are data from the initialization process that goes into this section. This will become clearer when we unpack the software and see the sections properties.

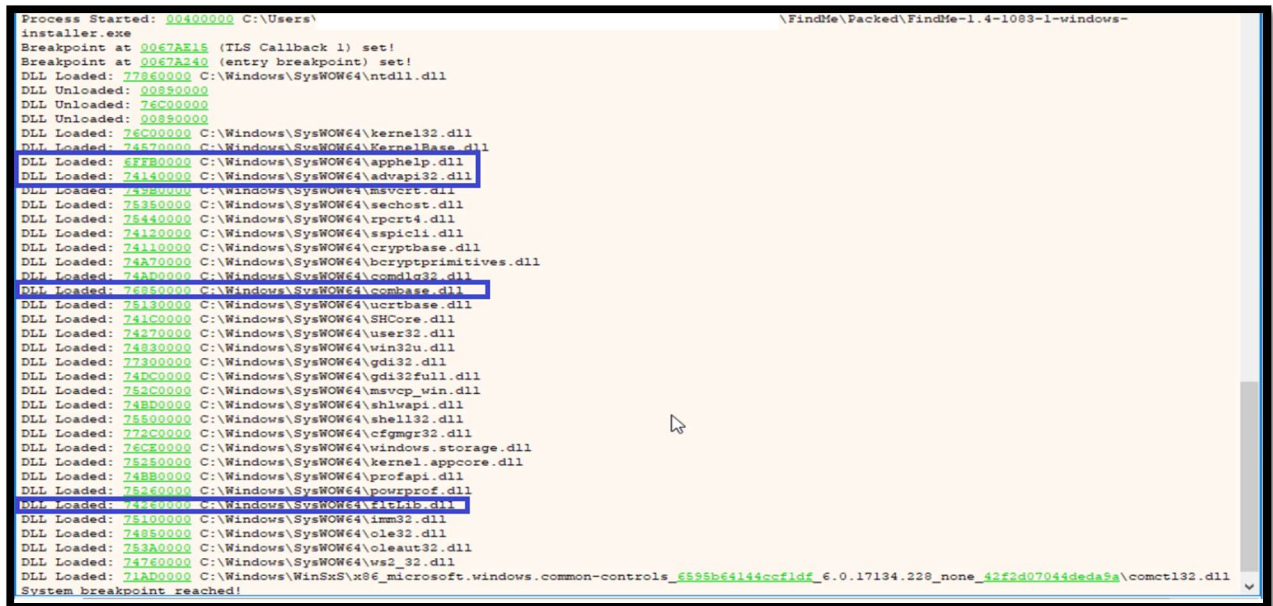
Next, it was located the TLS callback. Note that this mechanism is included in the encrypted portion of the executable file (UPX1). TLS callback allow malware authors to execute malicious code before the debugger has a chance to pause at the traditional Entry Point. The TLS table is identified below:



And by debugging it is possible to confirm that:

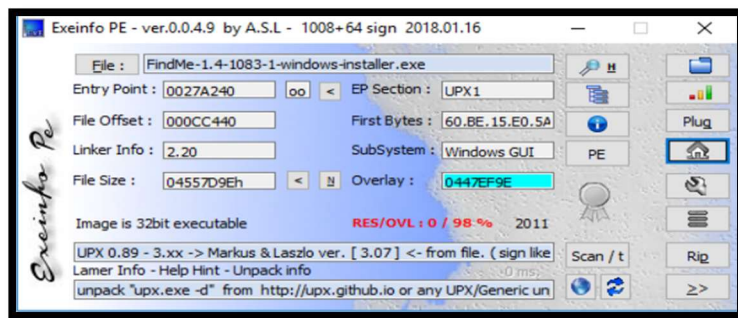


So, if the callback is successful then the software can load the libraries (*.dll) in which some would be interesting to further investigate if necessary:



Unpacking the Software

We can see that the software is packed.



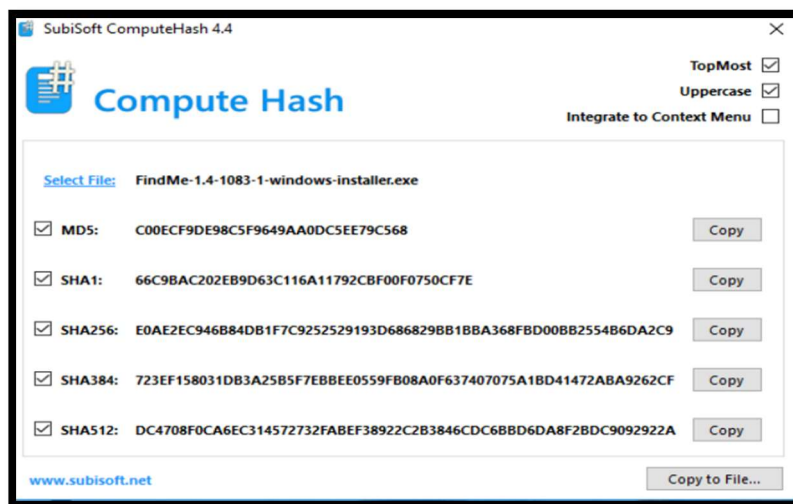
The software was unpacked:

```
C:\Users\ > \FindMe\Unpacked\upx394w\upx394w>upx -d FindMe-1.4-1083-1-windows-installer.exe
Ultimate Packer for eXecutables
Copyright (C) 1996 - 2017
UPX 3.94w Markus Oberhumer, Laszlo Molnar & John Reiser May 12th 2017

File size      Ratio      Format      Name
-----
74372510 <- 72711582 97.77% win32/pe FindMe-1.4-1083-1-windows-installer.exe

Unpacked 1 file.
C:\Users\ > \FindMe\Unpacked\upx394w\upx394w>
```

And the new hash for the file was calculated:



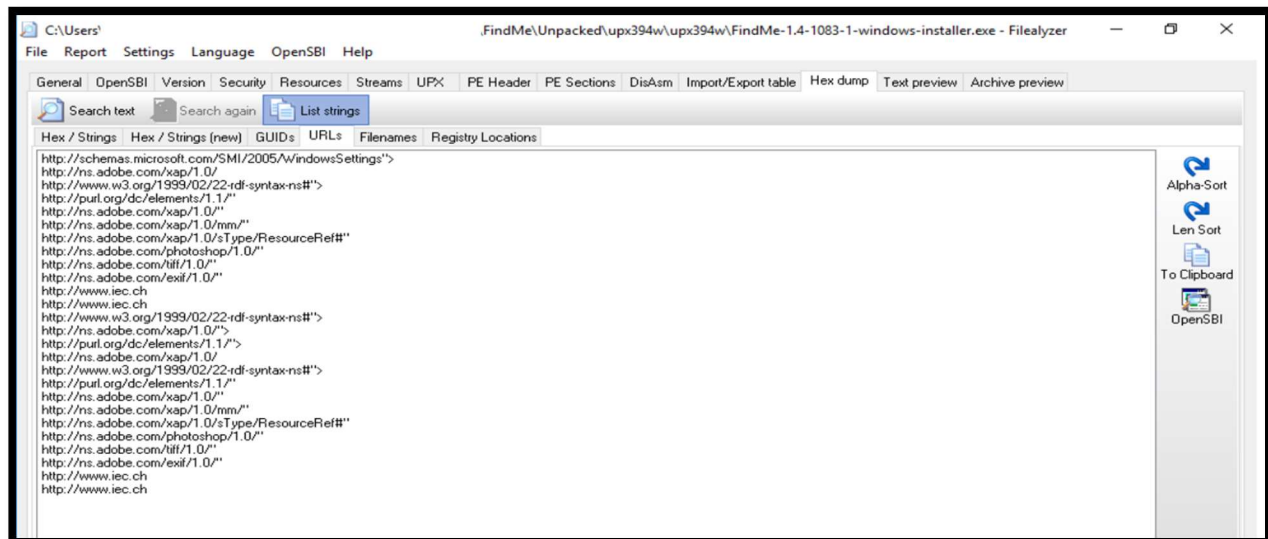
Once unpacked the software has several sections with access to write and initialize data after loading several *.dll and an excessive number of functions associated with:

Section	VirtSize	VirtAddr	PhysSize	PhysAddr	Flags	CRC32	MD5	Characteristics
.text	001DA2A0	00001000	001DA400	00000400	60500060	60FF1E29	541635...	Code, Initialized Data, Execute Access, Read Access
.data	000170EC	001DC000	00017200	001DA800	C0600040	C622CD53	506A64...	Initialized Data, Read Access, Write Access
.rdata	0003FBE0	001F4000	0003FC00	001FA000	40600040	F0AEDFB8	84D896...	Initialized Data, Read Access
/4	00008E10	00234000	00009000	00231600	C0300040	136D6EAD	8E38BD...	Initialized Data, Read Access, Write Access
.bss	00001FE4	0023D000	00000000	00000000	C0600080			Uninitialized Data, Read Access, Write Access
.edata	0000006E	0023F000	00000200	0023A600	40300040	2A830287	91C959...	Initialized Data, Read Access
.idata	00003BB0	00240000	00003C00	0023A800	C0300040	21D7ED81	19C955...	Initialized Data, Read Access, Write Access
.CRT	00000018	00244000	00000200	0023E400	C0300040	65B45D4F	66C72B...	Initialized Data, Read Access, Write Access
.tls	00000020	00245000	00000200	0023E600	C0300040	826C6DB0	3A2586...	Initialized Data, Read Access, Write Access
.rsrc	0001B438	00246000	0001B600	0023E800	C0300040	3C4136DE	159DA0...	Initialized Data, Read Access, Write Access
.reloc	00014770	00262000	00014800	00259E00	42300040	1A5423AD	E62C85...	Initialized Data, Discardable, Read Access

Library/Function	Ordinal	Address
Export table		
TclKit_ApplInit	0001	00002344
TclKit_SetKitPath	0002	00002720
Import table		
ADVAPI32.DLL	5	functions
COMCTL32.DLL	1	functions
COMDLG32.DLL	6	functions
GDI32.dll	73	functions
IMM32.DLL	5	functions
KERNEL32.DLL	161	functions
msvcrt.dll	116	functions
OLE32.dll	3	functions
OLEAUT32.DLL	7	functions
SHELL32.DLL	6	functions
USER32.dll	125	functions
WS2_32.DLL	26	functions

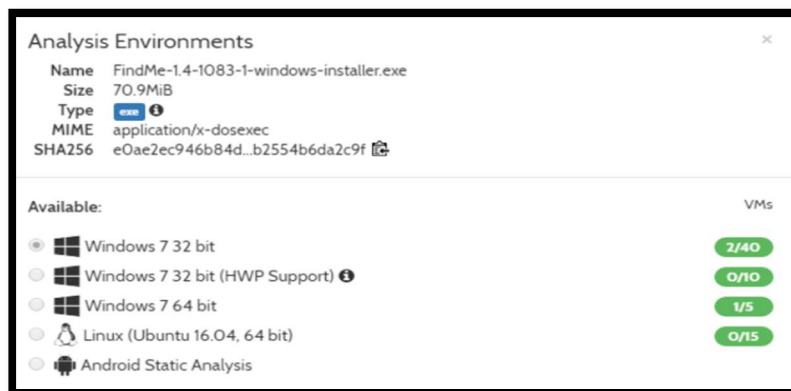
Websites

Several suspicious websites were located in the software:



Unpacked and vulnerabilities

The most interesting result is that if we scan the software unpacked we can observe several vulnerabilities, not identified by the initial obfuscation.



HYBRID ANALYSIS

Analysis Overview

[Report Abuse](#)

suspicious
Threat Score: 80/100
[#evasive](#)
[Link](#)
[Twitter](#)
[E-Mail](#)

Submission name:	FindMe-1.4-1083-1-windows-installer.exe
Size:	71MiB
Type:	peexe ⓘ
Mime:	application/x-dosexec
SHA256:	e0ae2ec946b84db1f7c9252529193d686829bb1bba368fbd0 0bb2554b6da2c9f ⓘ
Operating System:	Windows
Last Anti-Virus Scan:	08/25/2018 07:15:15
Last Sandbox Report:	08/10/2018 18:35:51

And still not detected by recognized antivirus tools.

HYBRID ANALYSIS

CLEAN
CrowdStrike Falcon Static Analysis (ML) ⓘ ⓘ ⓘ

N/A
Metadefender ⓘ

CLEAN
VirusTotal ⓘ ⓘ ⓘ

Falcon Sandbox Reports

SUSPICIOUS
 FindMe-1.4-108...
Analyzed on: 08/10/2018 ...
Environment: Windows 7 ...
Threat Score: 80/100
AV Detection: Marked as c...
Indicators: 7 36 ...
Network: (none)

The risks were now identified

FindMe-1.4-1083-1-windows-installer.exe

This report is generated from a file or URL submitted to this webservice on August 10th 2018 18:35:51 (CEST)
Guest System: Windows 7 32 bit, Home Premium, 6.1 (build 7601), Service Pack 1
Report generated by Falcon Sandbox v8.10 © Hybrid Analysis

Overview | Login to Download Sample (69MiB) | Downloads | External Reports | Re-analyze | Hash Not Seen Before | Report Abuse

Incident Response

Risk Assessment

- Remote Access**: Reads terminal service related keys (often RDP related)
- Ransomware**: Contains ability to create/switch the desktop
- Spyware**: Contains ability to open the clipboard
Contains ability to retrieve keyboard strokes
- Fingerprint**: Reads the active computer name
Reads the windows product ID

MITRE ATT&CK™ Techniques Detection

This report has 26 indicators that were mapped to 21 attack techniques and 9 tactics. [Click here to get the full picture.](#)

Incident Response
Indicators
File Details
Screenshots (2)
Hybrid Analysis (1)
Network Analysis
Extracted Strings
Extracted Files (9)
Notifications
Community (0)
Back to top

Attacks

And the types of possible attacks can be selected from one of the existent and documented categories:

MITRE ATT&CK™ Techniques Detection

Minimal

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
	Service Execution 1	Hooking 1	Access Token Manipulation 1	Access Token Manipulation 1	Hooking 1	File and Directory Discovery 1	Pass the Hash 1	Clipboard Data 1	Data Compressed 1	
		Kernel Modules and Extensions 1 1	Hooking 1	File Deletion 1 1	Input Capture 1	Peripheral Device Discovery 2 2	Remote Desktop Protocol 1	Input Capture 1		
			Process Injection 1	Process Injection 1		Query Registry 1 4				
						System Information Discovery 2				
						System Time Discovery 1				

Download as CSV Close

References

- http://cobweb.cs.uga.edu/~liao/PE_Final_Report.pdf
- <https://www.quora.com/What-is-another-file-type-alternative-to-running-a-exe-file>
- https://link.springer.com/chapter/10.1007/978-3-319-11379-1_4
- <https://www.hybrid-analysis.com/sample/a28cb151792e1918be1ad275dd511da224c600684337ace37c9bedc28a19d07e>
- <https://www.hybrid-analysis.com/sample/e0ae2ec946b84db1f7c9252529193d686829bb1bba368fbd00bb2554b6da2c9f>
- https://www.rsaconference.com/writable/presentations/file_upload/hta-t09-structural_entropy_analysis_for_automated_malware_classification_final_v2.pdf
- <https://msdn.microsoft.com/en-us/library/ms809762.aspx>
- <https://isc.sans.edu/diary/How+Malware+Defends+Itself+Using+TLS+Callback+Functions/6655>
- <https://www.malwaretech.com/2013/11/portable-executable-injection-for.html>