FindMe-1.4-1083-1 Evaluation

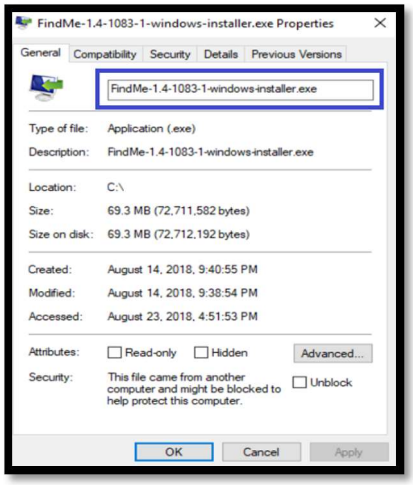
Date: August 26th, 2018.

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.

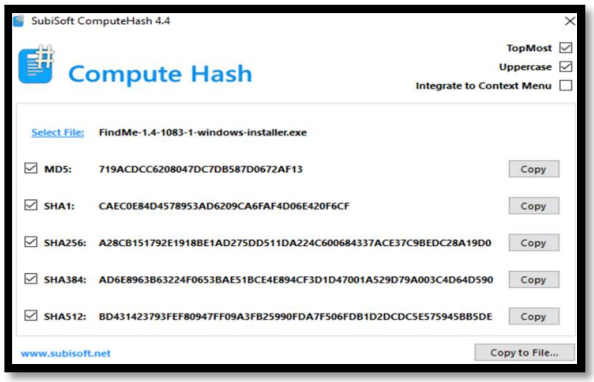
Summary

File Identification

The executable file

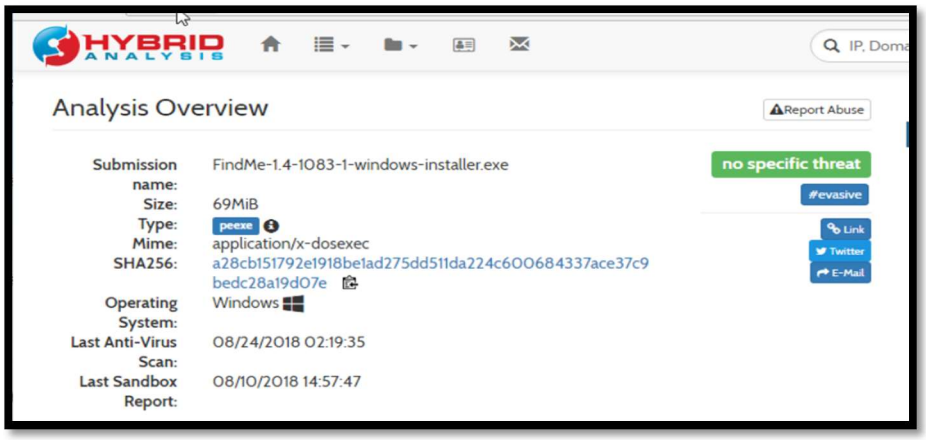


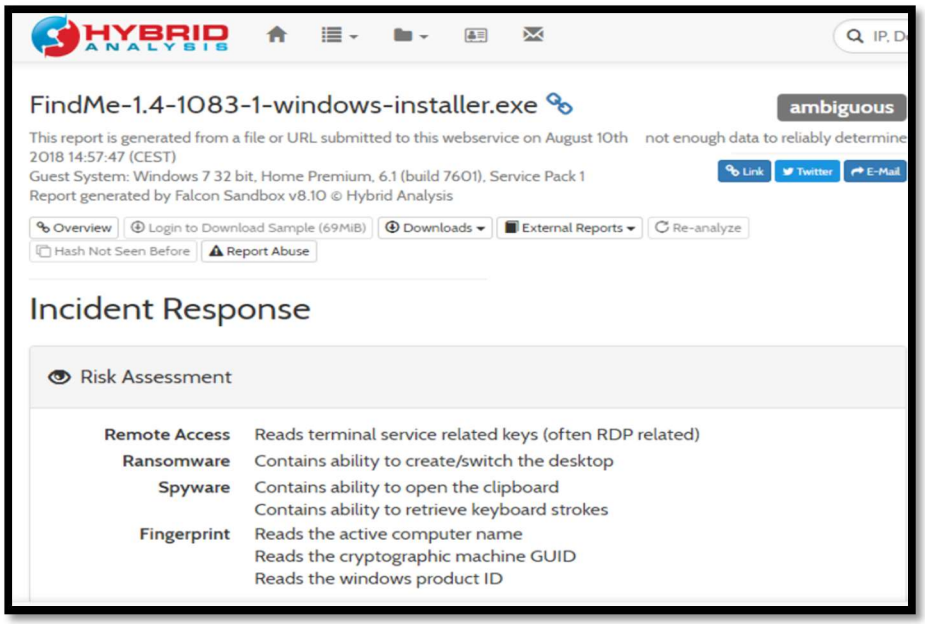
The calculated hash for the packed version:

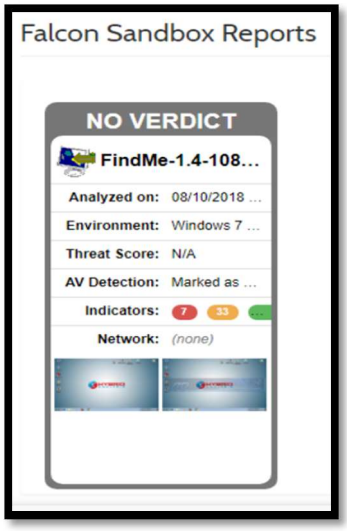


Preliminar Threat Analysis

Initially the vulnerabilities are not easily identified with ambiguous results:

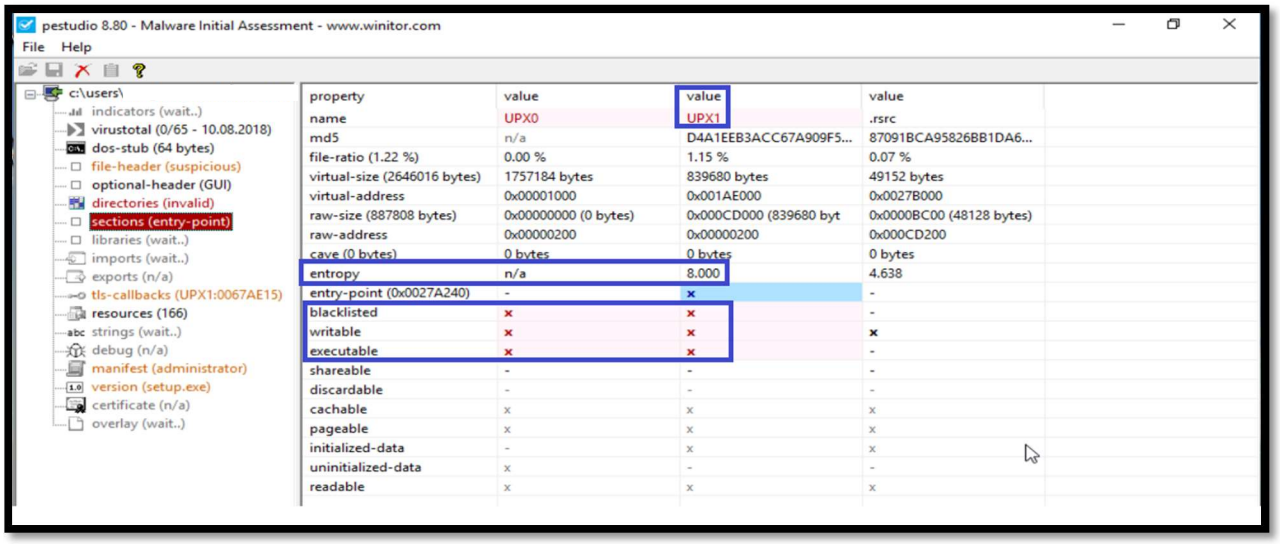

HYBRID ANALYSIS
Analysis Overview
Report Abuse
Submission name: FindMe-1.4-1083-1-windows-installer.exe
Size: 69MiB
Type: peexe
Mime: application/x-dosexec
SHA256: a28cb151792e1918be1ad275dd511da224c600684337ace37c9bedc28a19d07e
Operating System: Windows
Last Anti-Virus Scan: 08/24/2018 02:19:35
Last Sandbox Report: 08/10/2018 14:57:47
no specific threat
#evasive
Link
Twitter
E-Mail


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
Link
Twitter
E-Mail
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:
Network: (none)

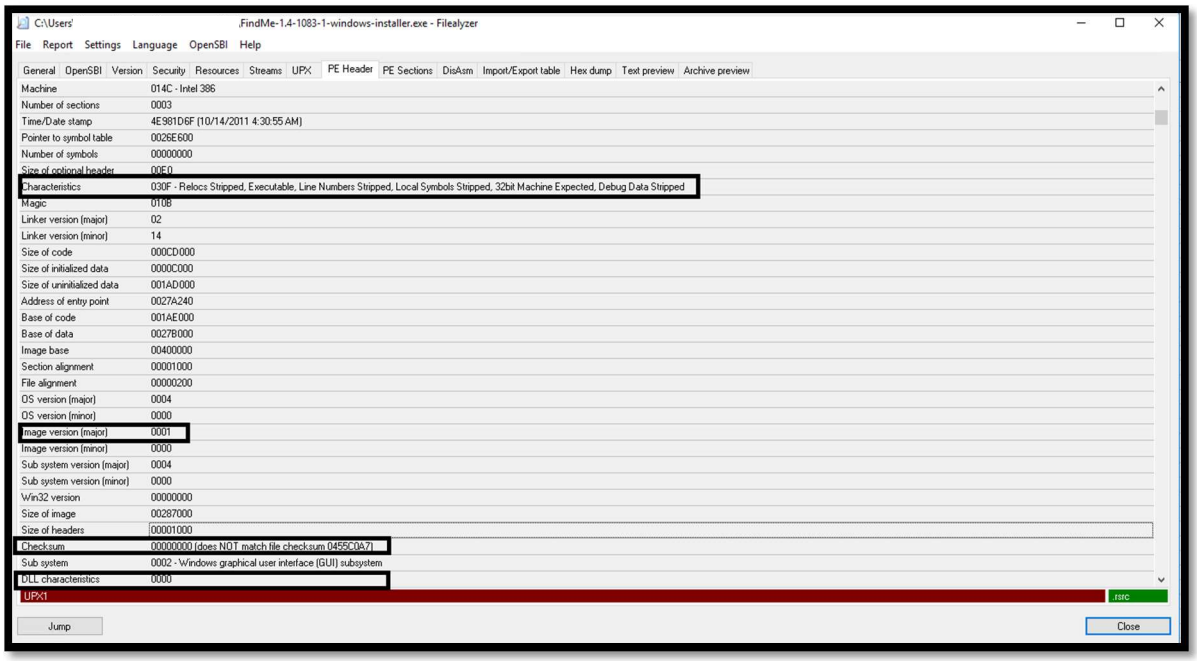
File Analysis

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

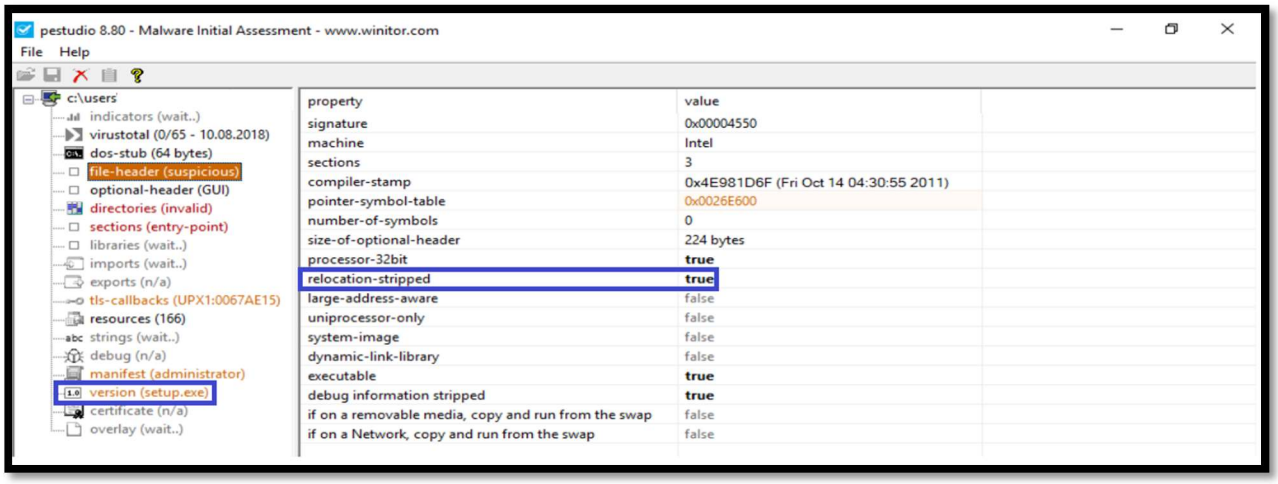


Some red flags are noticed in the PE Header, mainly related to the checksum, image version and the relocation stripped considering that:

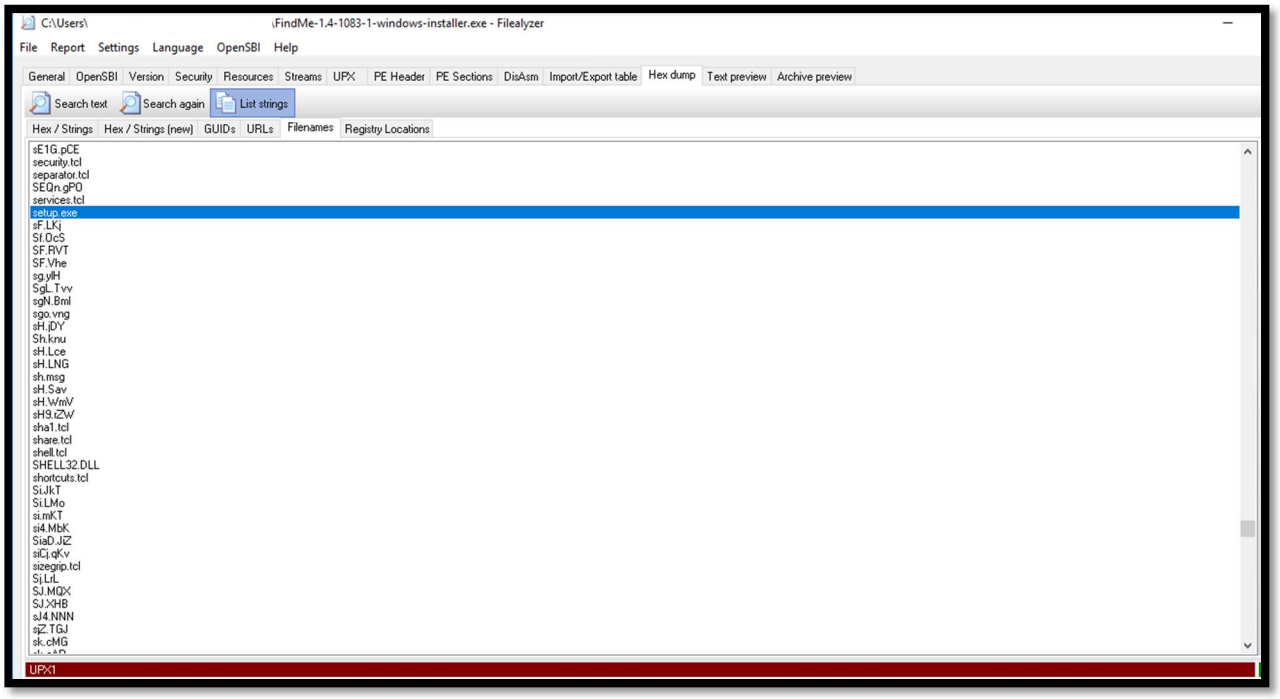
> "DLLCharacteristics, MajorImageVersion, and CheckSum are equal to zero in more than 90% malware samples. However, most benign executables contain significant higher values in such fields" (Yibin Liao).



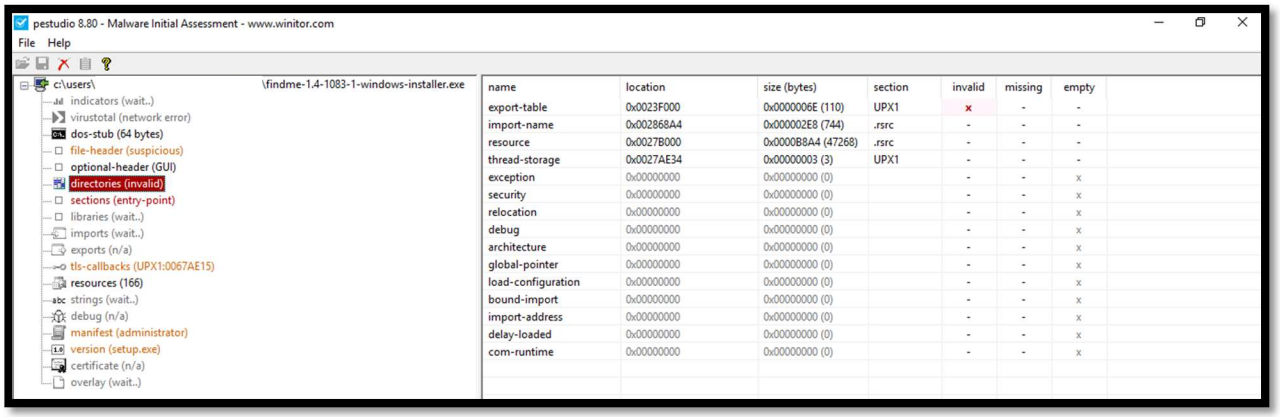
The relocation-stripped increases the susceptibility to code-reuse attacks. And as you can see as well another executable file (setup.exe) is embedded as part of the executable file. A possible explanation is that this file may be responsible to execute the *.dll files in the entry point.

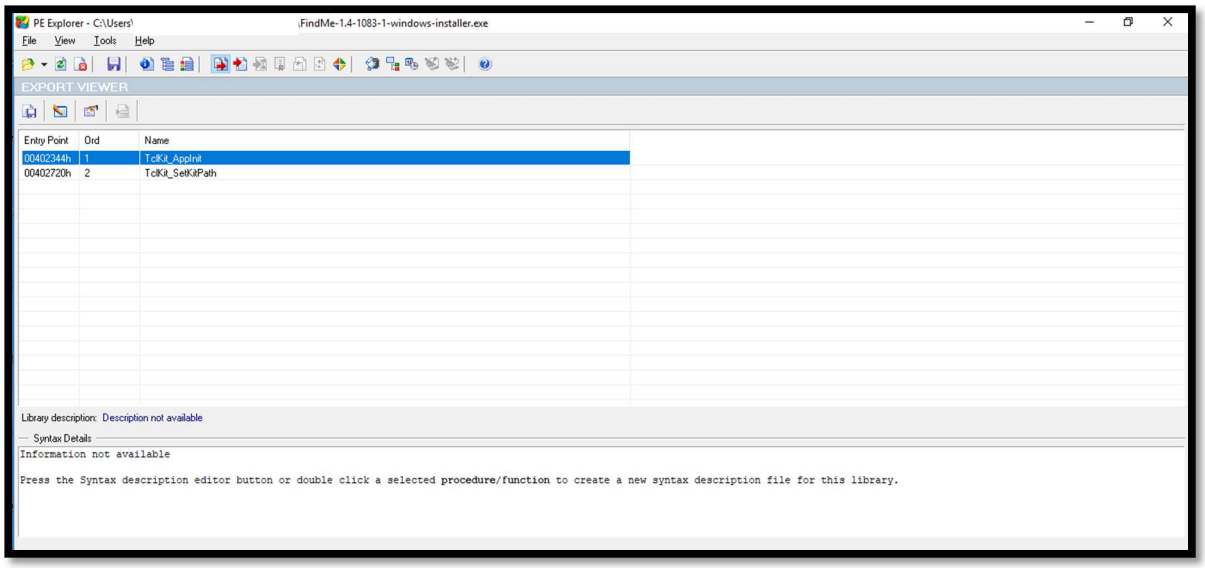


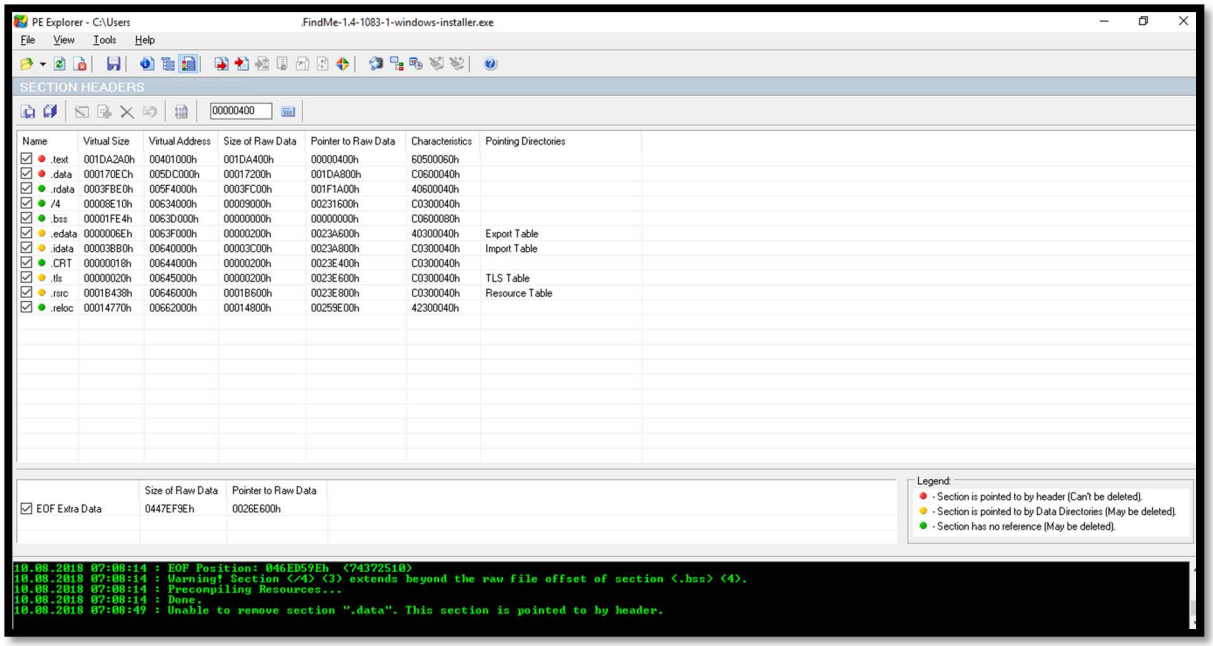
The executable file presented in the previous can be located through the strings as well:



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

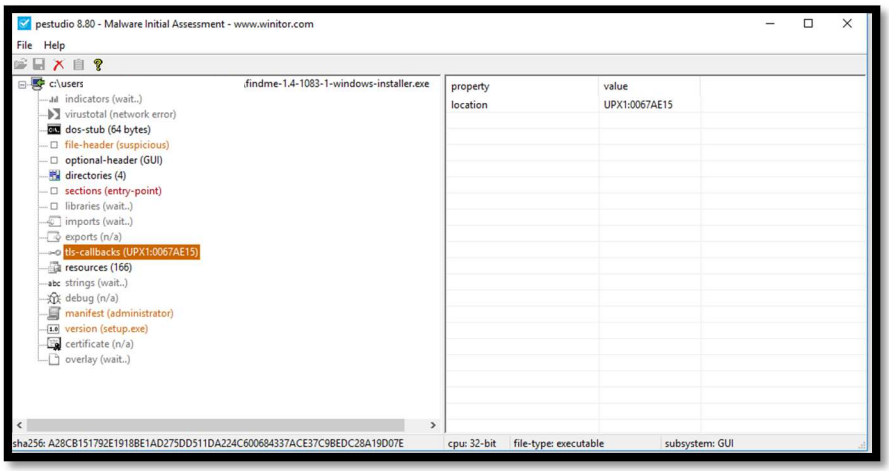




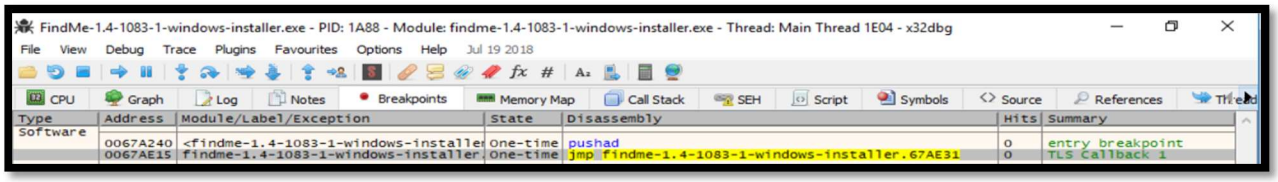


Note that the section ".data" is pointed to by header. Which means that there are data from the initialization process that goes into this section. This will become clearer when we unpack the software and see the sections properties.

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:



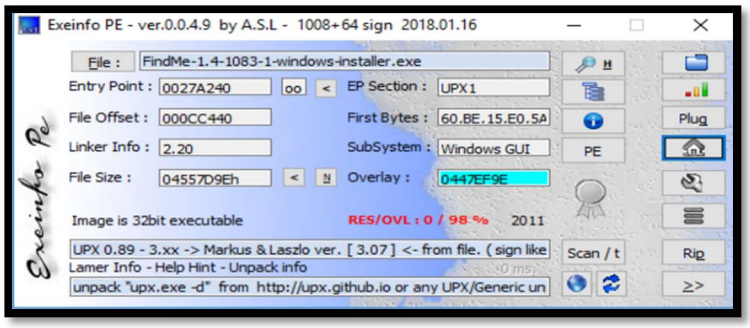
And by debugging it is possible to confirm that:



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

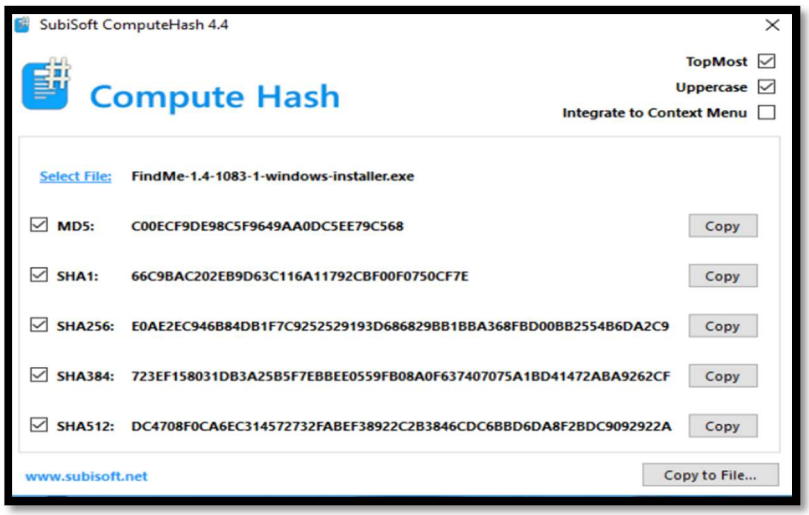
We can see that the software is packed.



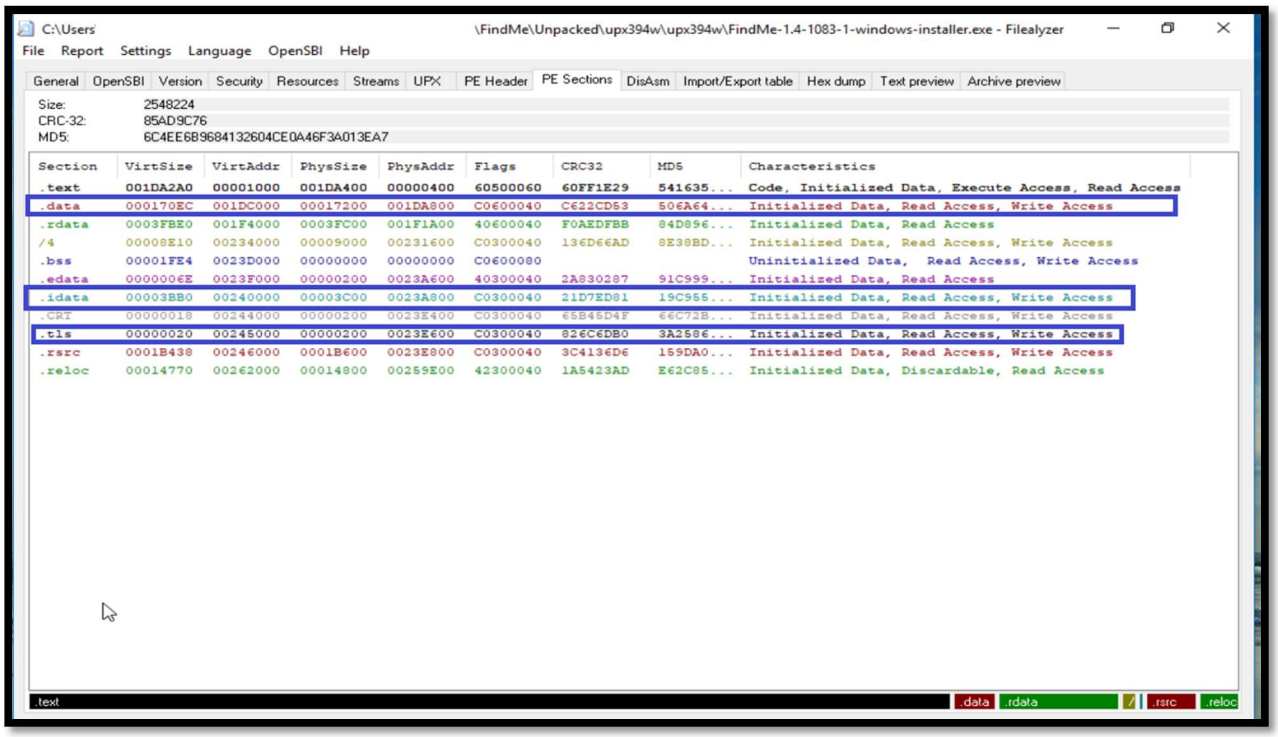
The software was unpacked:

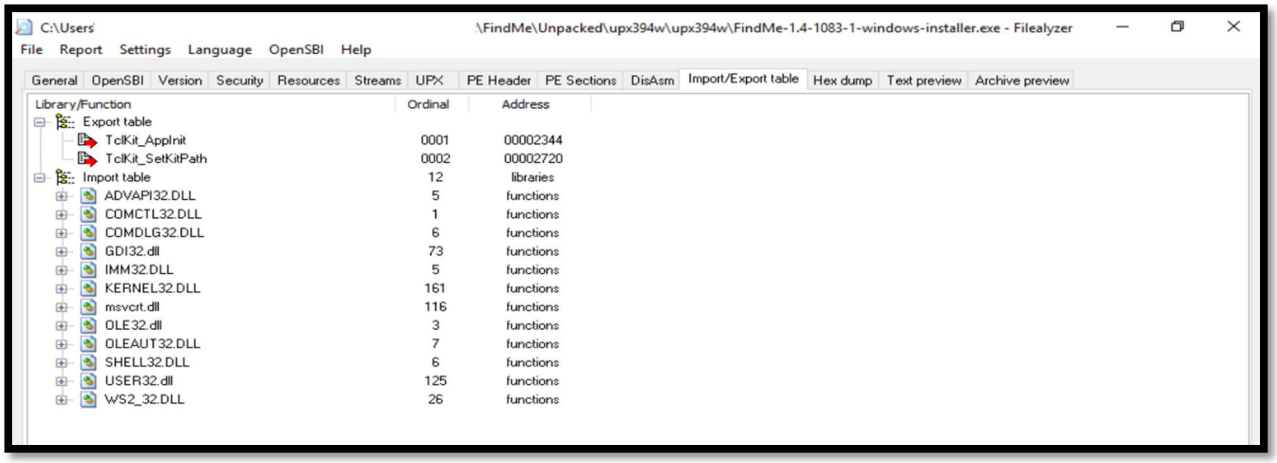
```
C:\Users\                                    \FindMe\Unpacked\upx394w\upx394w>upx -d FindMe-1.4-1083-1
-windows-installer.exe
                       Ultimate Packer for eXecutables
                          Copyright (C) 1996 - 2017
UPX 3.94w       Markus Oberhumer, Laszlo Molnar & John Reiser  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



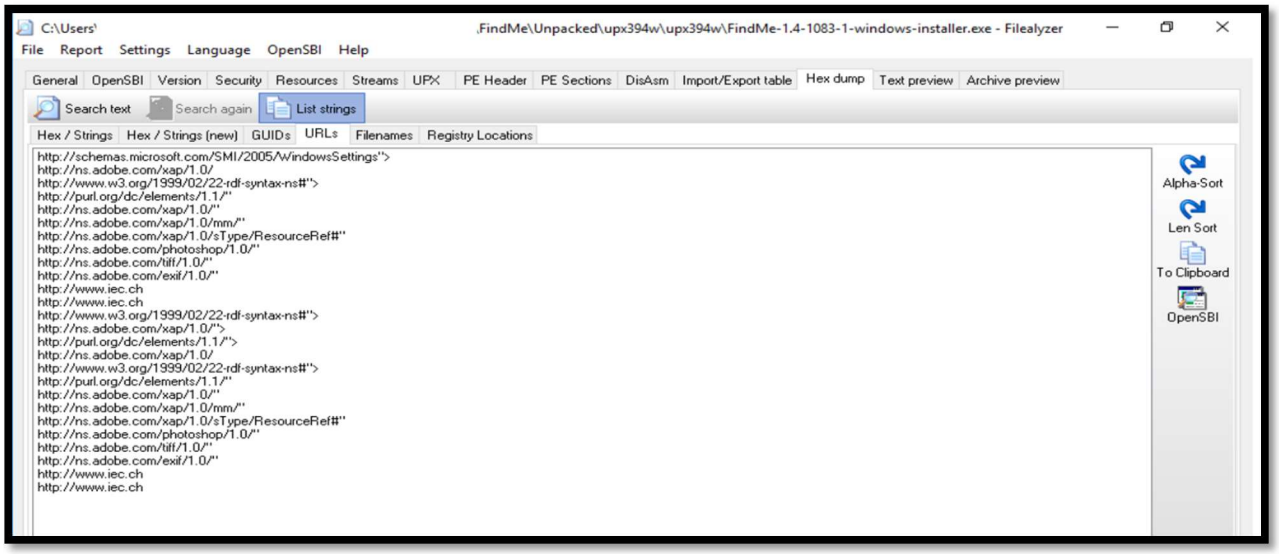
Once unpacked the software has several sections with access to write and initialize data after loading several *.dll and an excessive number of functions associated with:





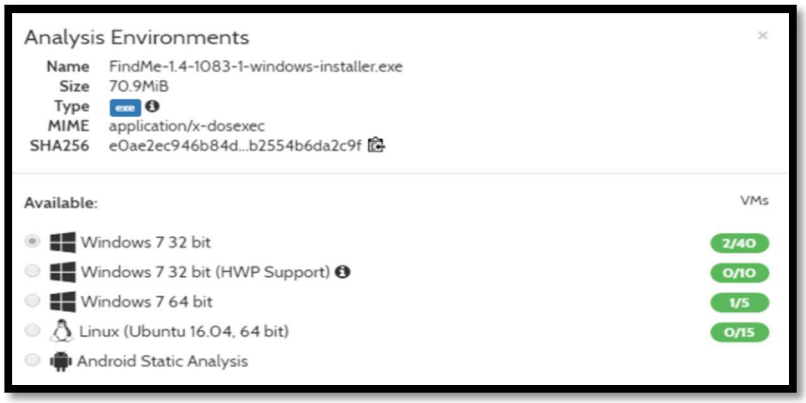
Websites

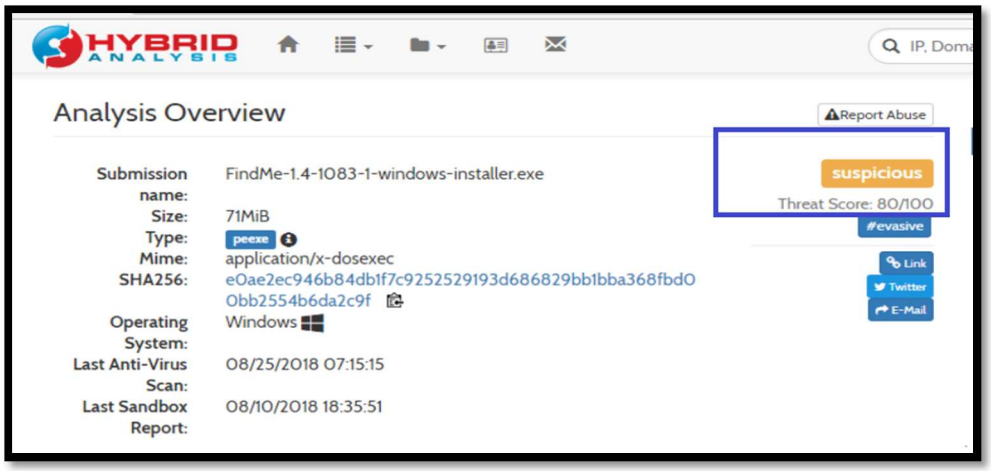
Several suspicious websites were located in the software:



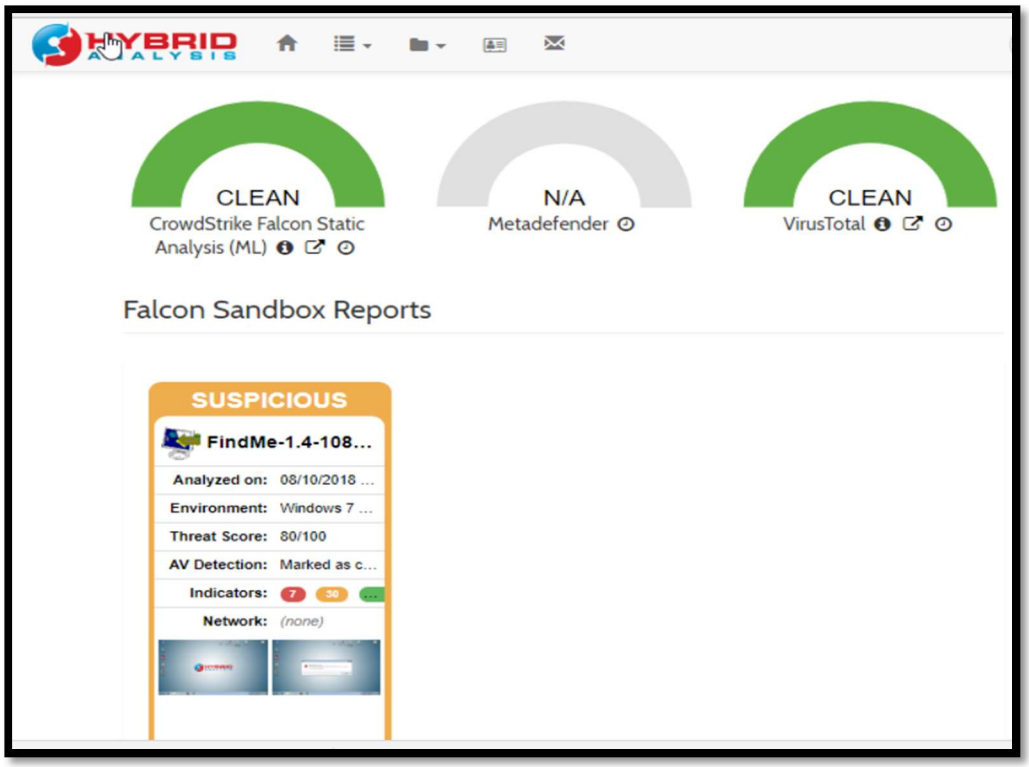
Unpacked and vulnerabilities

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

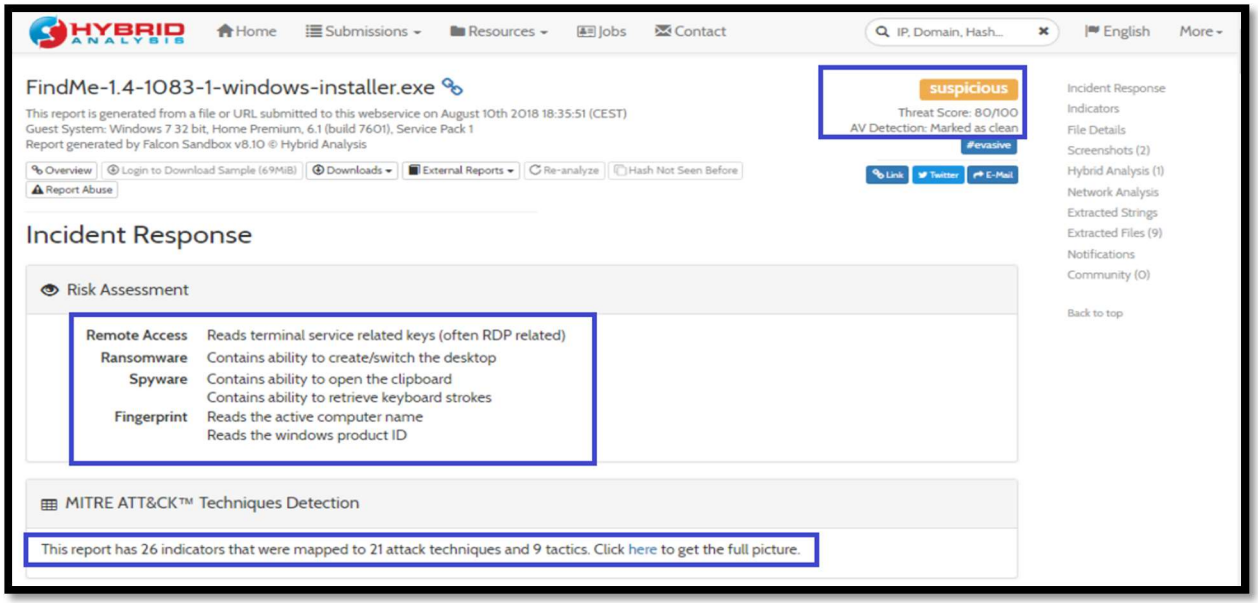




And still not detected by recognized antivirus tools.

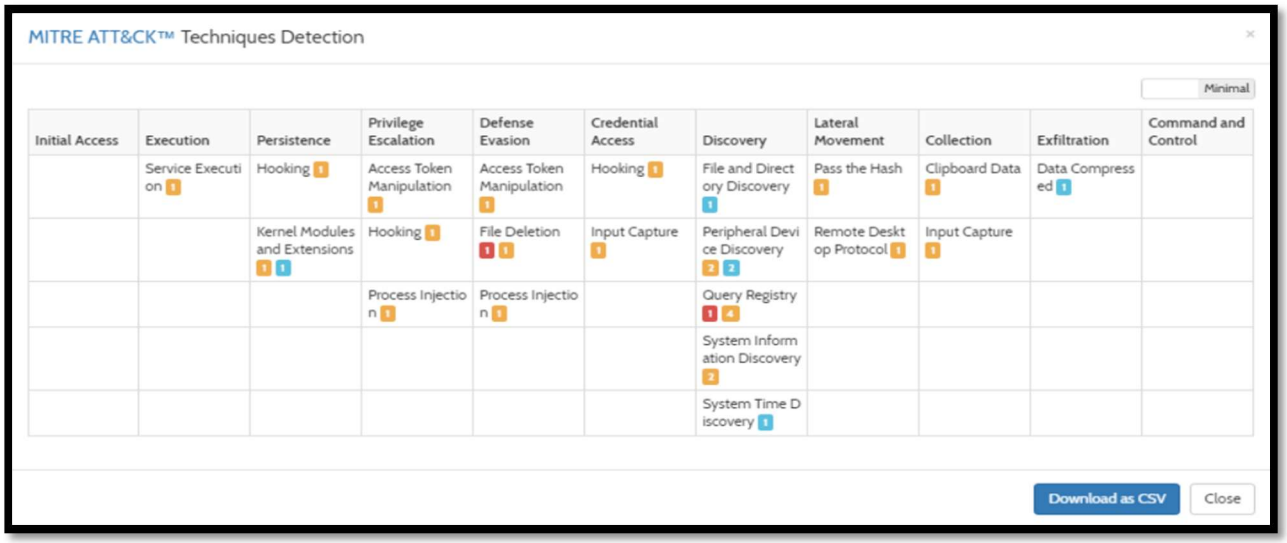


The risks were now identified



Attacks

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



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