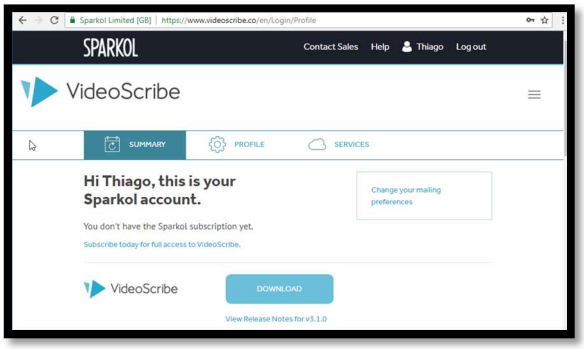
VideoScribe v3.1.0 Assessment

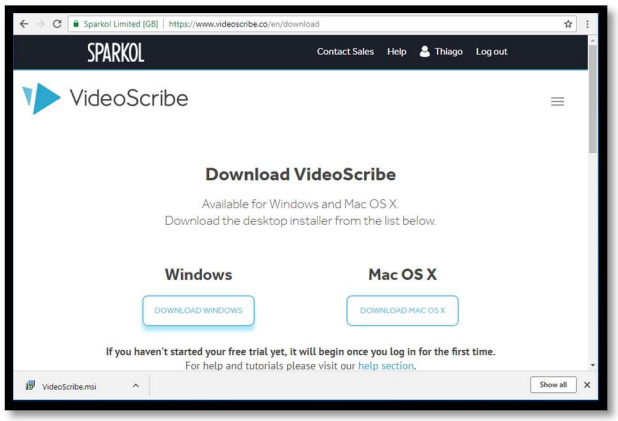
Date: August 06th, 2018.

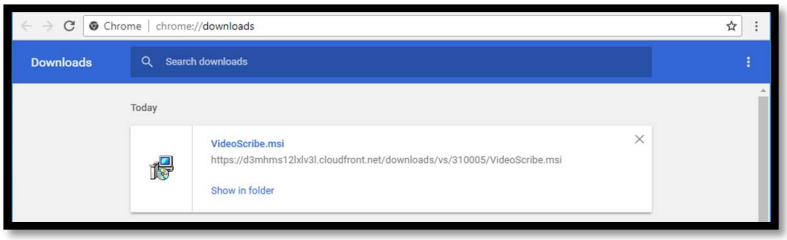
Description: These were vulnerabilities found during the installation and download of the VideoScribe software v3.1.0. The software may allow that unverifiable Object Linking and Embedding (OLE) streams in combination with suspicious websites succeed in an arbitrary code injection. The event could be triggered by packed icon files in the *.msi file.

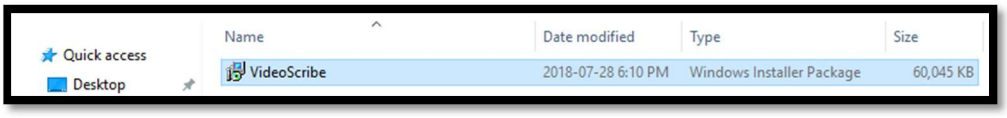
Sumário

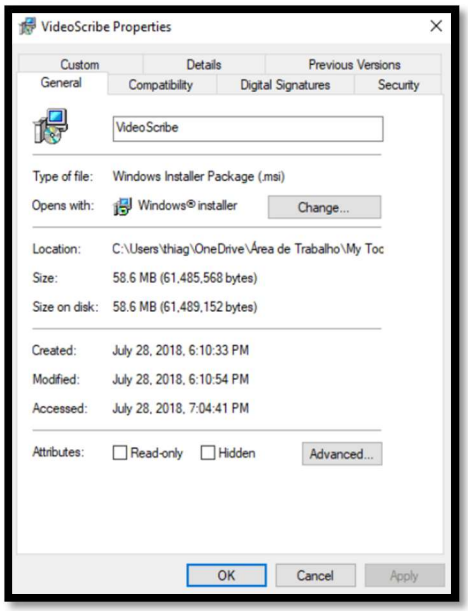
1. File Identification

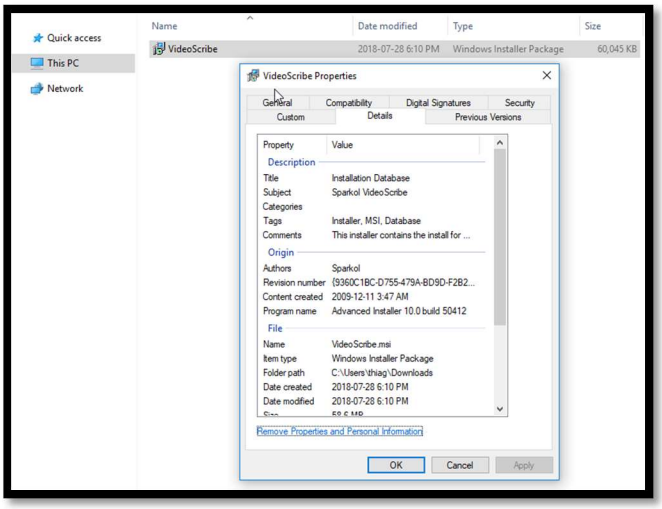


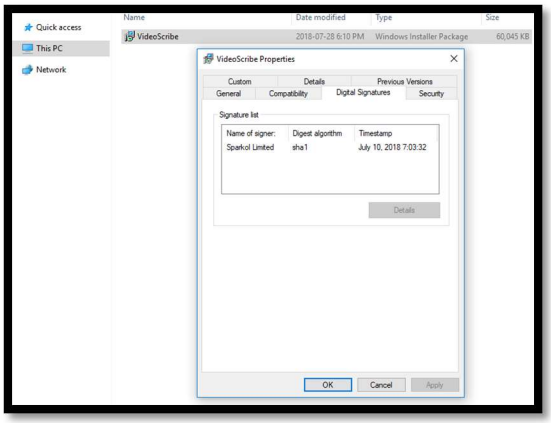






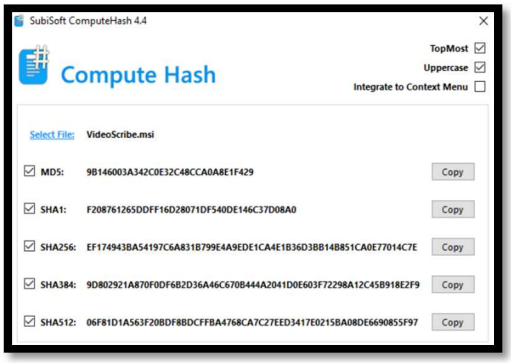

VideoScribe Properties
Custom
Details
Previous Versions
General
Compatibility
Digital Signatures
Security
VideoScribe
Type of file: Windows Installer Package (.msi)
Opens with: Windows® installer
Change...
Location: C:\Users\thiag\OneDrive\Área de Trabalho\My Toc
Size: 58.6 MB (61,485,568 bytes)
Size on disk: 58.6 MB (61,489,152 bytes)
Created: July 28, 2018, 6:10:33 PM
Modified: July 28, 2018, 6:10:54 PM
Accessed: July 28, 2018, 7:04:41 PM
Attributes: Read-only Hidden
Advanced...
OK
Cancel
Apply


Quick access
This PC
Network
Name
Date modified
Type
Size
VideoScribe
2018-07-28 6:10 PM
Windows Installer Package
60,045 KB
VideoScribe Properties
General
Compatibility
Digital Signatures
Security
Custom
Details
Previous Versions
Property
Value
Description
Title
Installation Database
Subject
Sparkol VideoScribe
Categories
Tags
Installer, MSI, Database
Comments
This installer contains the install for ...
Origin
Authors
Sparkol
Revision number
{9360C1BC-D755-479A-BD9D-F2B2...
Content created
2009-12-11 3:47 AM
Program name
Advanced Installer 10.0 build 50412
File
Name
VideoScribe.msi
Item type
Windows Installer Package
Folder path
C:\Users\thiag\Downloads
Date created
2018-07-28 6:10 PM
Date modified
2018-07-28 6:10 PM
Remove Properties and Personal Information
OK
Cancel
Apply

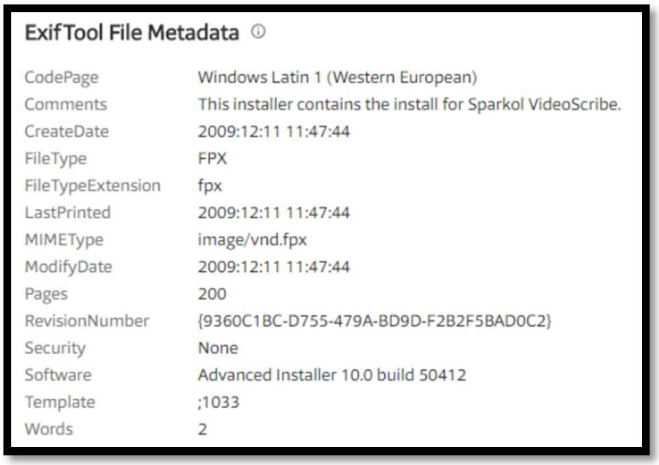

Quick access
This PC
Network
Name
Date modified
Type
Size
VideoScribe
2018-07-28 6:10 PM
Windows Installer Package
60,045 KB
VideoScribe Properties
Custom
Details
Previous Versions
General
Compatibility
Digital Signatures
Security
Signature list
Name of signer:
Digest algorithm
Timestamp
Sparkol Limited
sha1
July 10, 2018 7:03:32
Details
OK
Cancel
Apply

2. File Properties

Source: www.virustotal.com

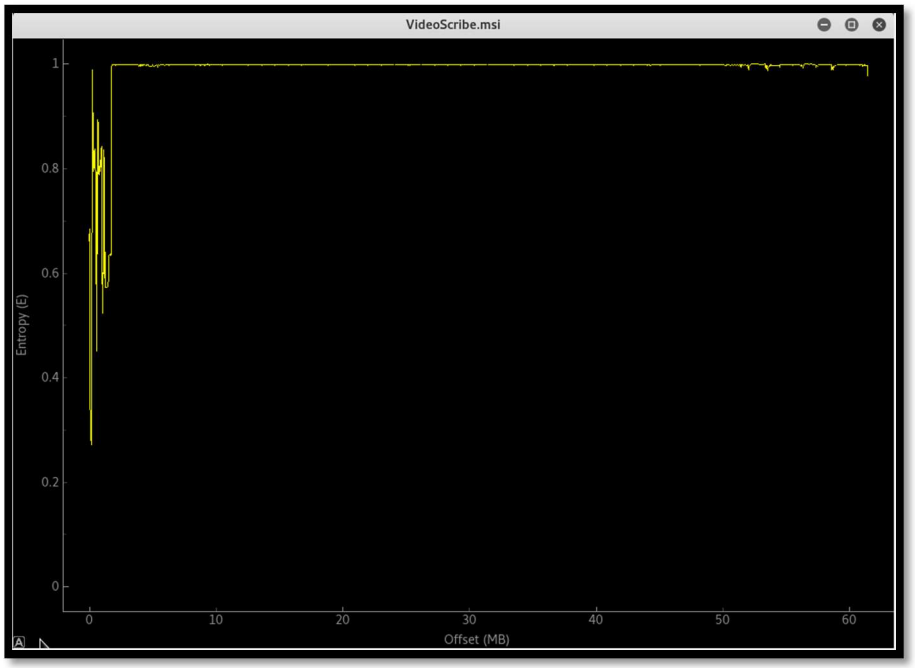


Source: Compute Hash



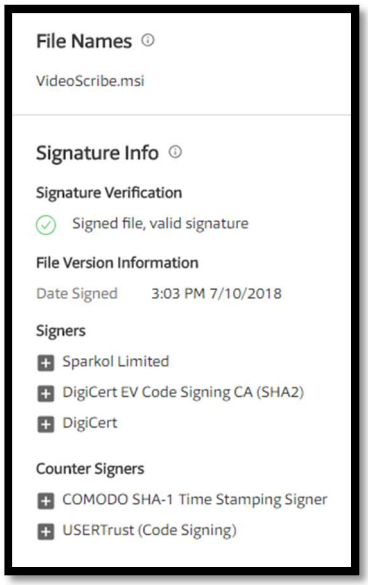
Source: www.virustotal.com

The entropy test below confirms the presence of compressed files.



Source: kali linux.

3. Valid Signatures



Source: www.virustotal.com

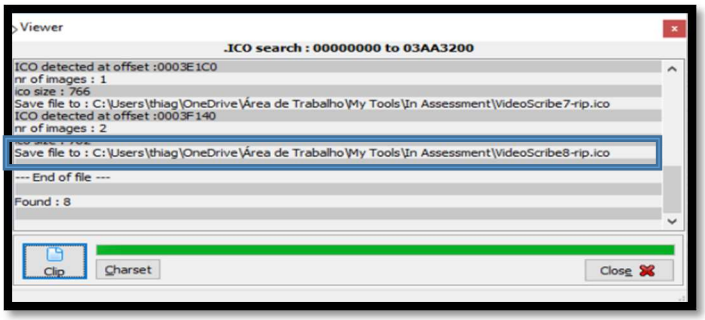
4. Object Linking and Embedding (OLE) streams

Object Linking and Embedding (OLE) structures allow the creation of objects in one application and be linked or embedded in a second application. In this process, data is stored in the streams, including the possibility of malware files.

In general, these objects can be part of a Rich Text Format (*.rtf), Microsoft Word (*.doc), Microsoft Excel (*.xlsx) file and would require attackers to send one of those types of files to the victim computer and would need the user action to open it. In this case, the OLE streams that are included as part of the software installation, and they do not need user action to open it. Then, without the user knowledge, these additional OLE components are also being deployed. The object could be embedded in a file or an icon activated by the user or remaining in a dormant stage.

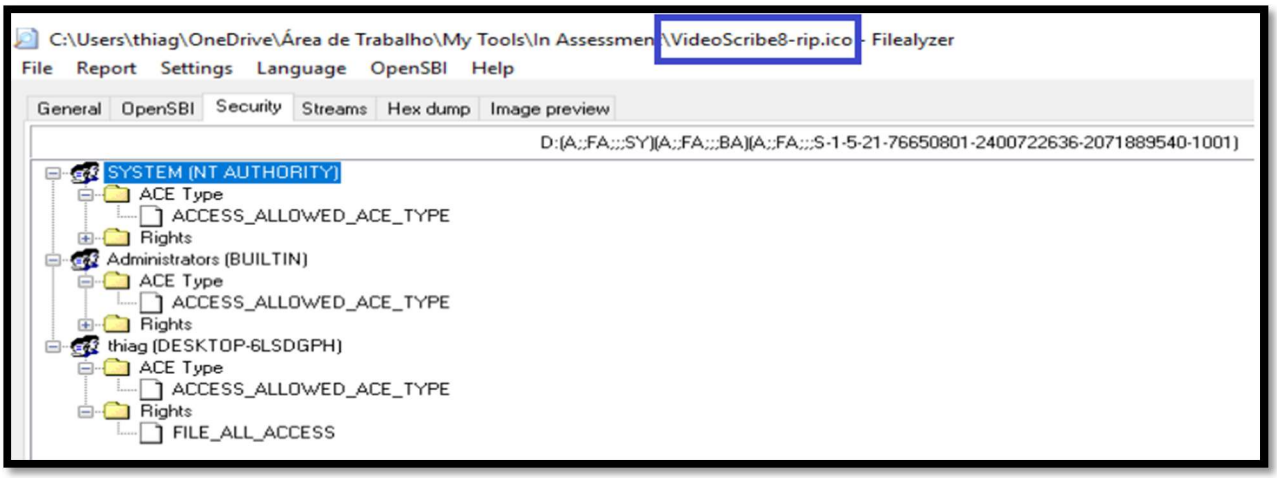
There were 08 hidden icons found in the software. Note that these files were packed. Once unpacked they show an ACCESS_ALLOWED_ACE_TYPE. This structure defines an access-control entry (ACE) for the discretionary access-control list (DACL) that controls access to an object for a specific subject identified by a security identifier (SID). In this case, the icon will grant all possible access rights for a file (FILE_ALL_ACCESS).

Hidden icons:



Source: Exeinfo PE

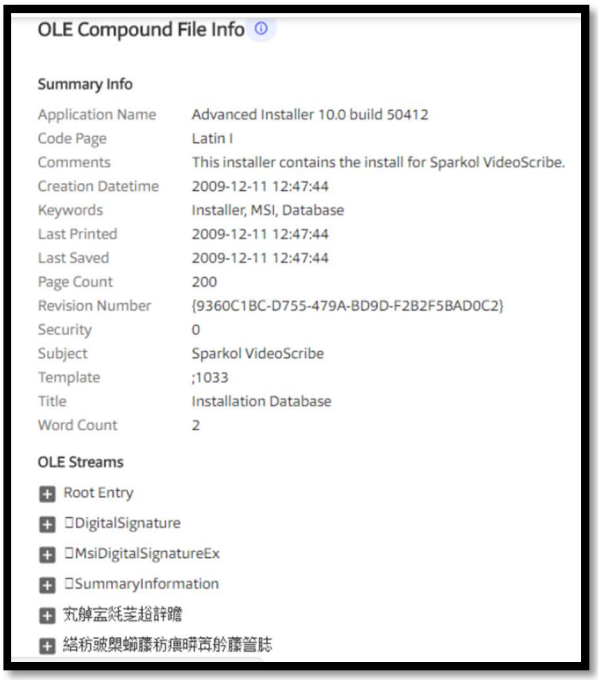
Source: www.virustotal.com

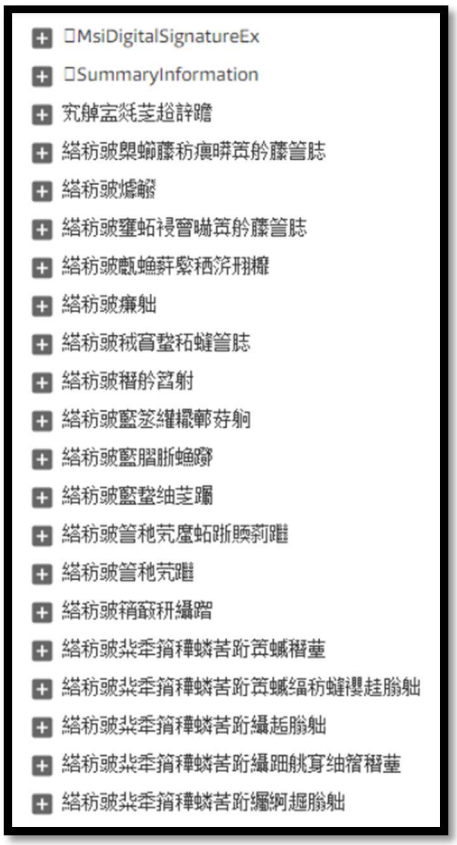


Source: FileAlyzer

By using WinINet.dll special features such as decompression support, credential cache and remote access could enable an unauthorized user to exploit the access through identified OLE Streams and suspicious websites.

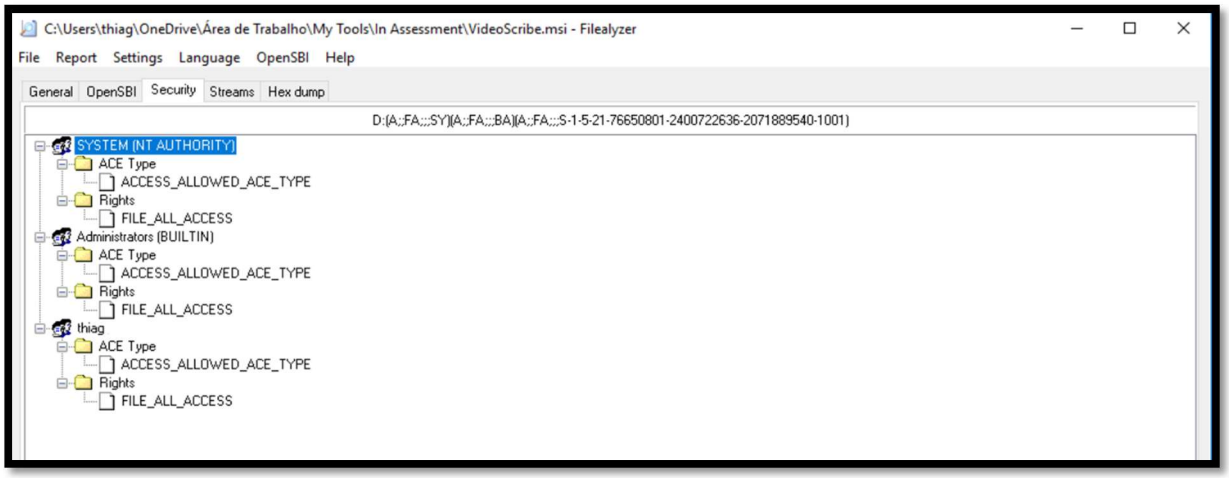
These were the OLE stream found:





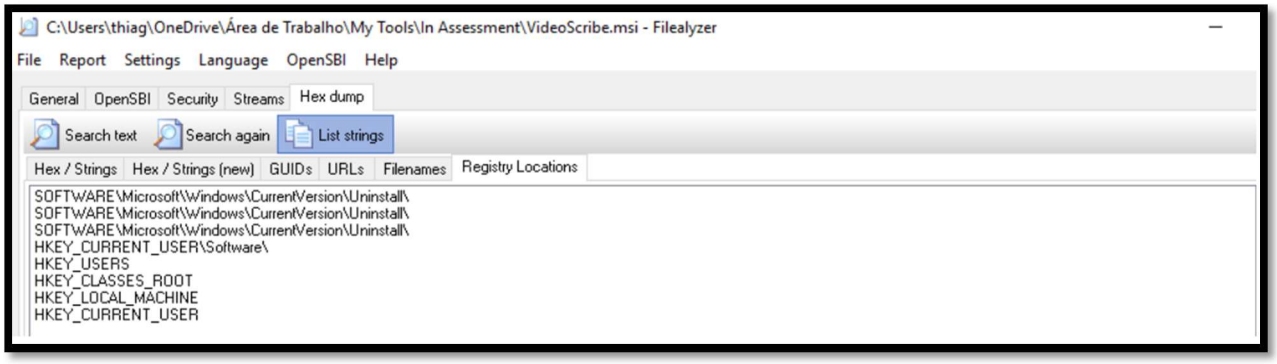
Source: www.virustotal.com

The exploit is successful because during the installation privileges are escalated granting full access.



Source: FileAlyzer

Then the access to Registry Locations such as HKEY_CLASSESS_ROOT allow the merge of default and processing settings to open specific files.

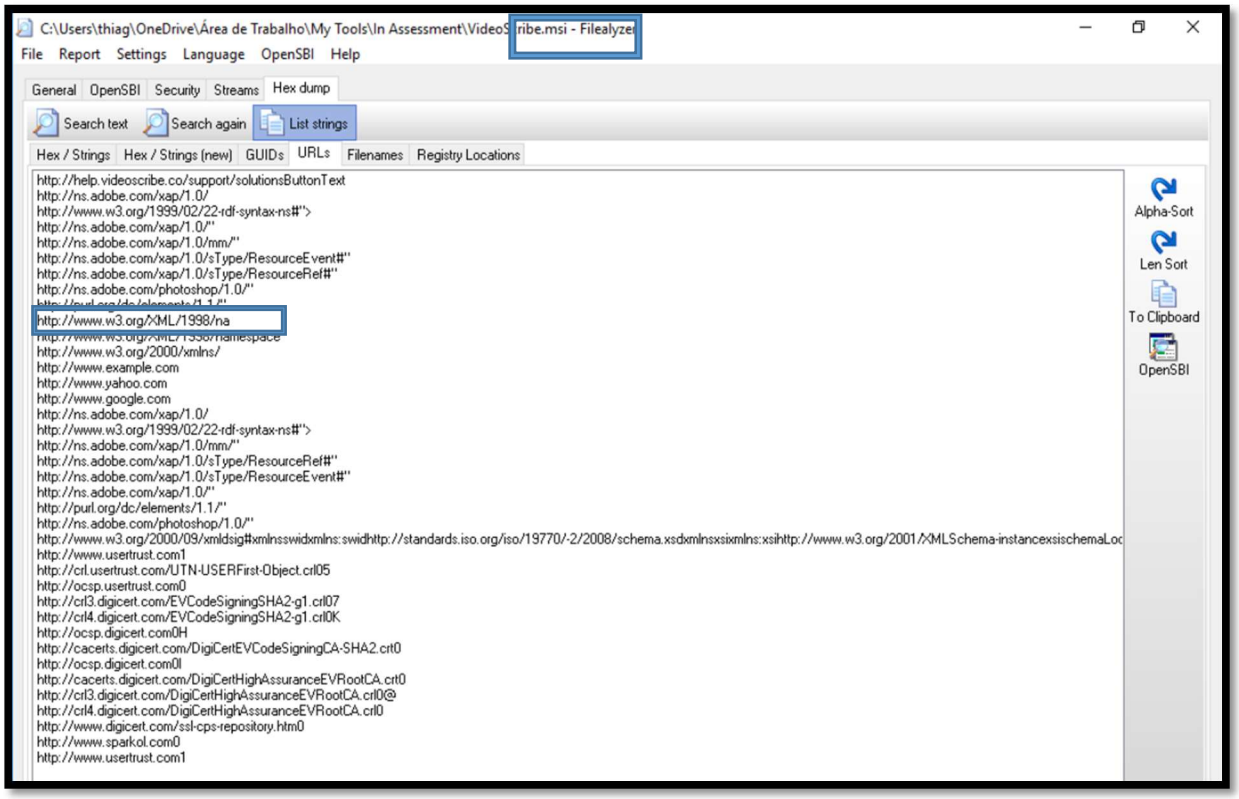


Source: FileAlyzer

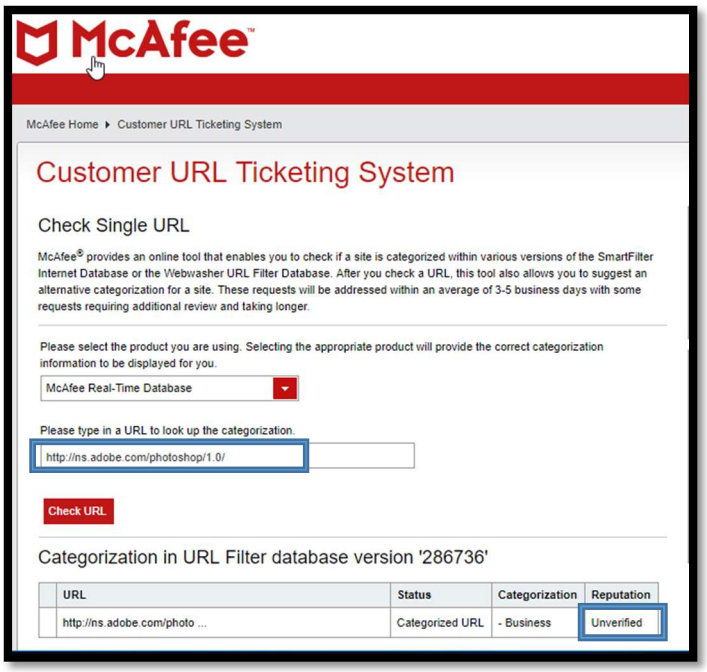
5. Suspicious Websites

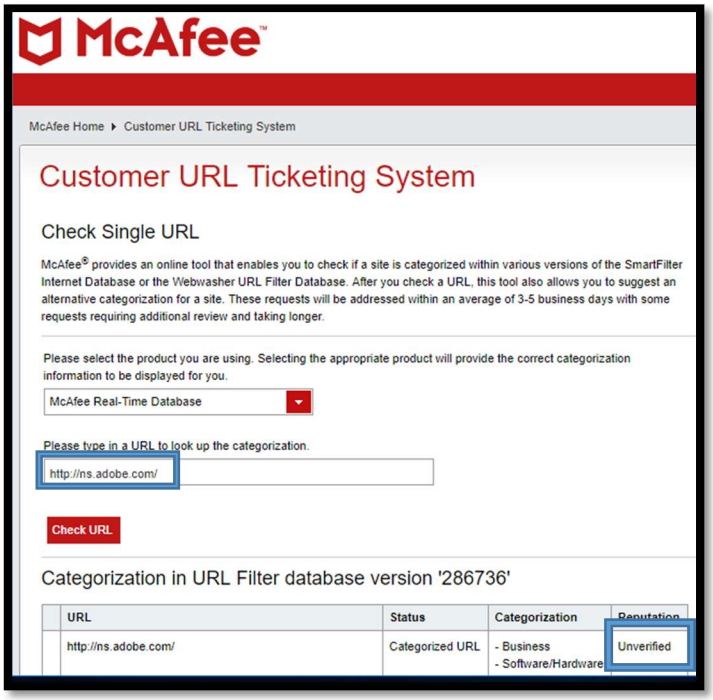
Suspicious websites were identified among acceptable ones such as www.google.com, for example. One website was selected for follow-up and demonstration.

- Example*: http://ns.adobe.com/photoshop/1.0/*

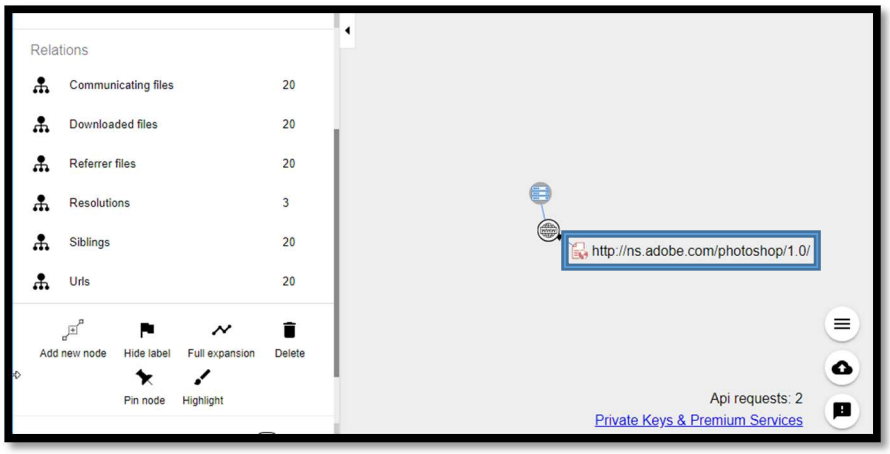


Source: FileAlyzer

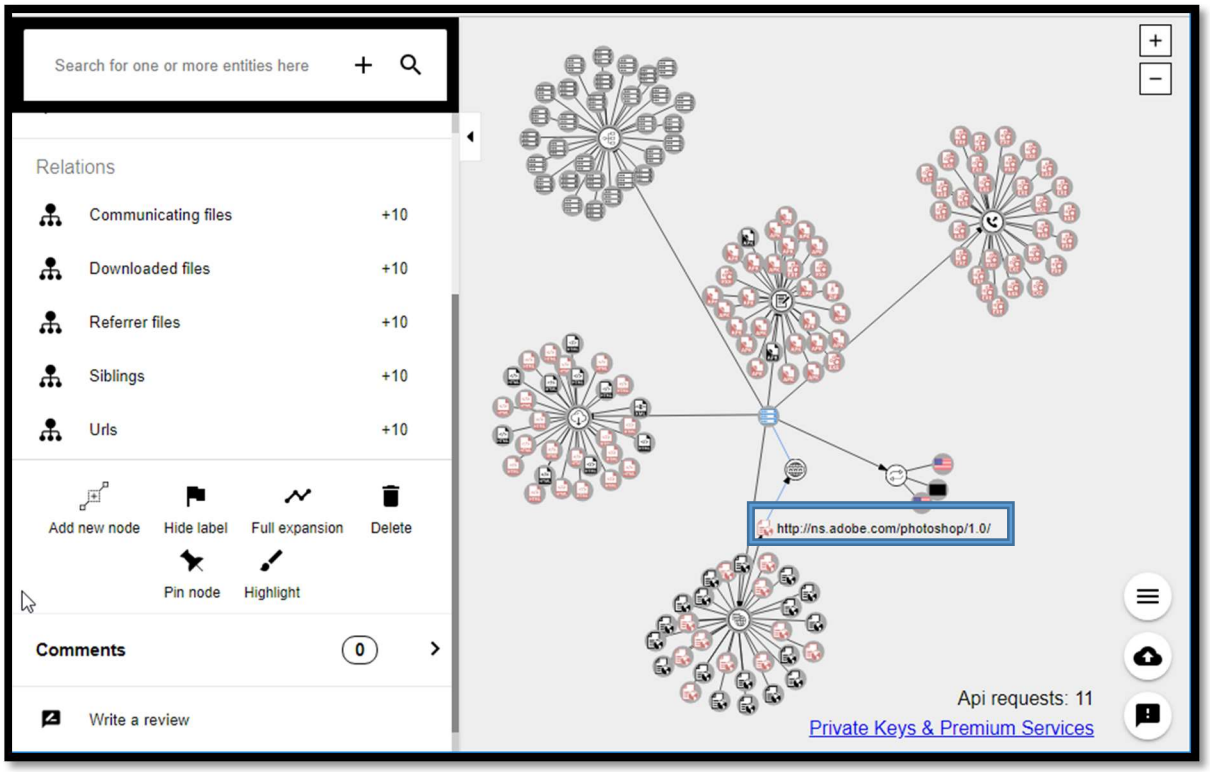




Source: www.trustedsource.org

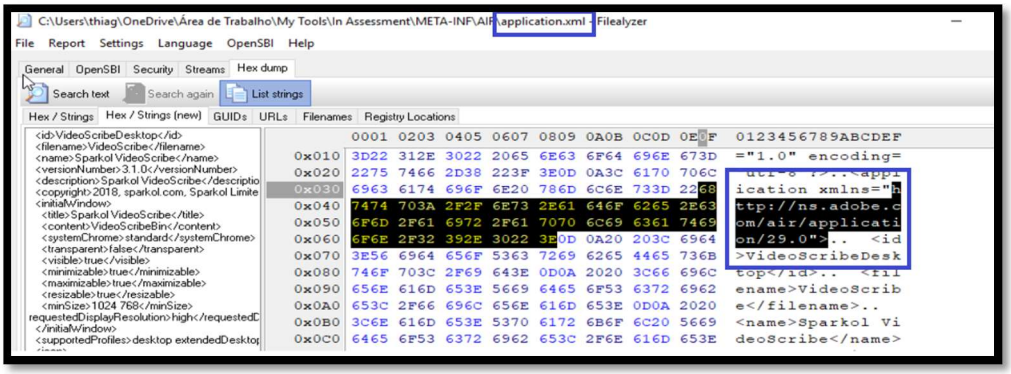


Source: www.virustotal.com



Source: www.virustotal.com

The suspicious websites were identified as part of XML files.

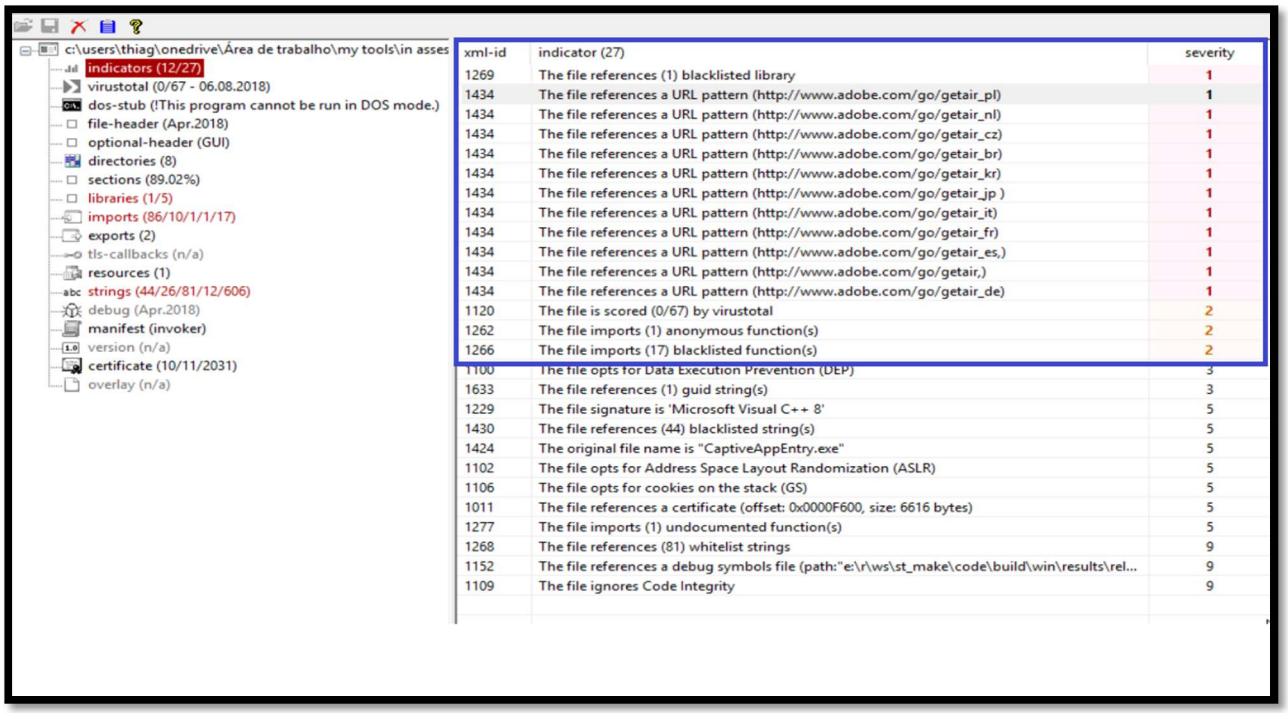


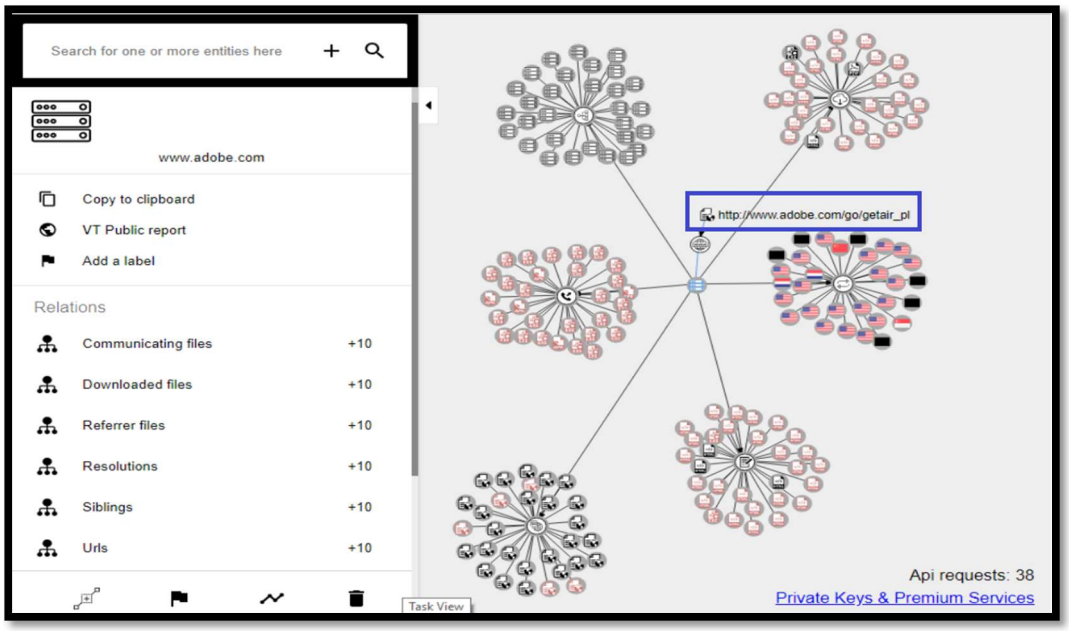
Source: FileAlyzer

6. Files Review

These were suspicious files found in the software by examining the strings using BinText. The first an executable file and list of dynamic-link libraries (dll).

It was identified the file CaptiveAppEntry.exe. The file shows the same behaviour to connect with suspicious websites and import blacklisted libraries and functions. From hybrid-analysis.com a suspicious behaviour was related to the capacity of this file query the CPU information (Attack-ID-T1082)



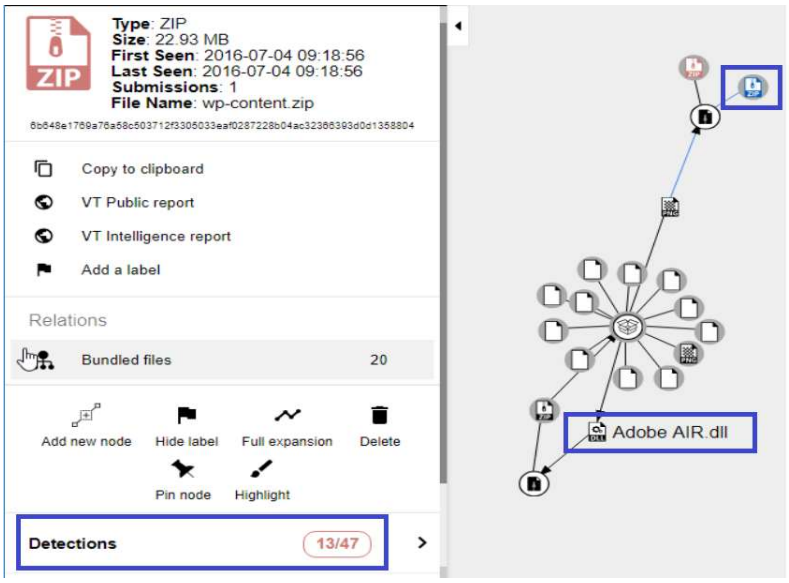


A complete list of DLL files would include:

1. mscoree.dll
2. user32.dll
3. kernel32.dll
4. Nmsi.dll
5. comdlg32.dll
6. ADVAPI32.dll
7. SHELL32.dll
8. ole32.dll
9. OLEAUT32.dll
10. ~1NXmlCfg.dll
11. WININET.dll
12. pWS2_32.dll
13. *NETAPI32.dll*
14. ZSHLWAPI.dll
15. kyZShell32.dll
16. TdB2msi.dll
17. P050dbghelp.dll
18. PSAPI.DLL
19. x86 Kernel32.dll
20. ldDbghelp.dll
21. y3\msi.dll
22. SHLWAPI.dll
23. VjResourceCleaner.dll
24. jJmsi.dll

25. JQExternalUICleaner.dll
26. CABINET.DLL
27. AdobeAIR.dll
28. SL AdobeCP.dll
29. 5L AdobeCP15.dll
30. aLV NPSWF32.dll
31. WebKit.dll

From the analysis of the DLL list, it is possible to identify ordinary libraries and possible malicious ones, such as the item 27 from the list, in which we can observe the connection with a few compressed and malicious files in a close loop:



7. References

- https://msdn.microsoft.com/en-us/library/dd942265.aspx
- https://docs.microsoft.com/en-us/windows/desktop/wininet/about-wininet
- https://attack.mitre.org/wiki/Technique/T1082