

## VideoScribe v3.1.0 Assessment

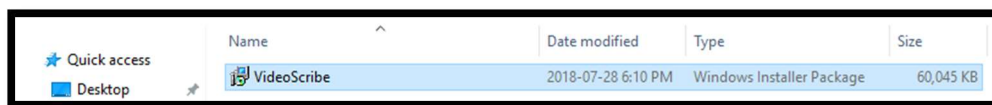
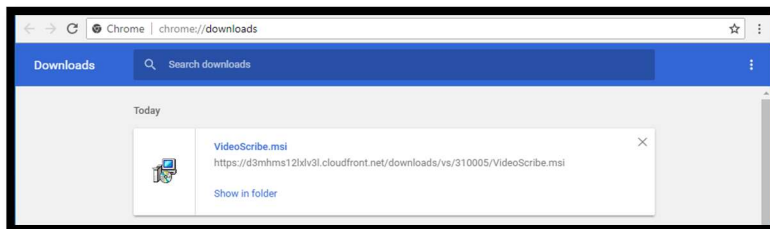
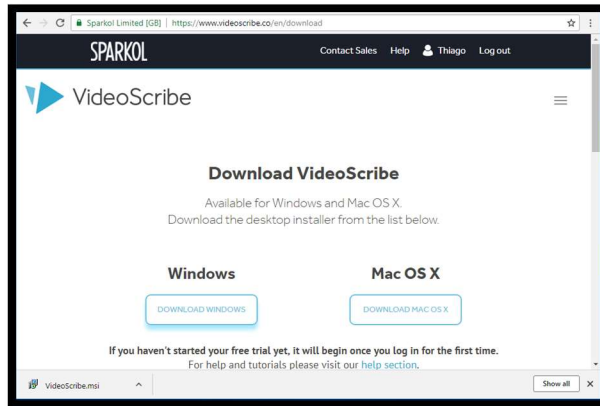
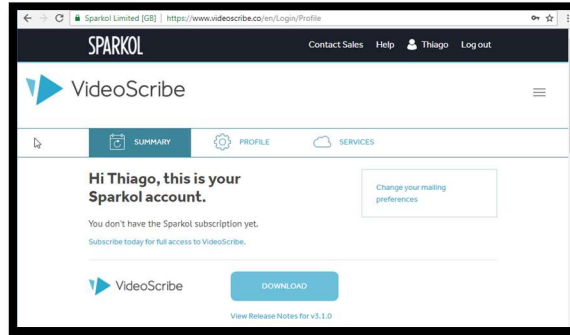
Date: August 23<sup>rd</sup>, 2018.

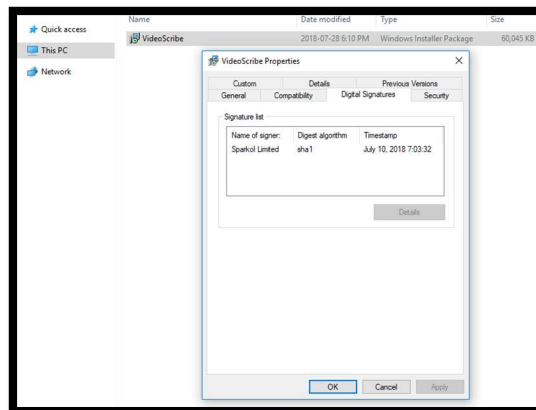
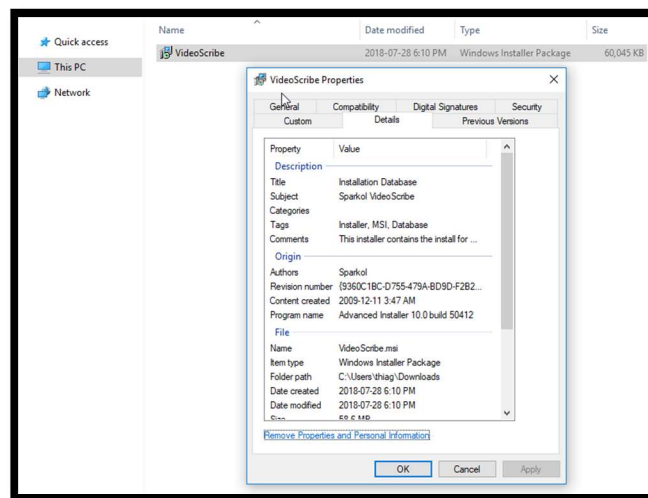
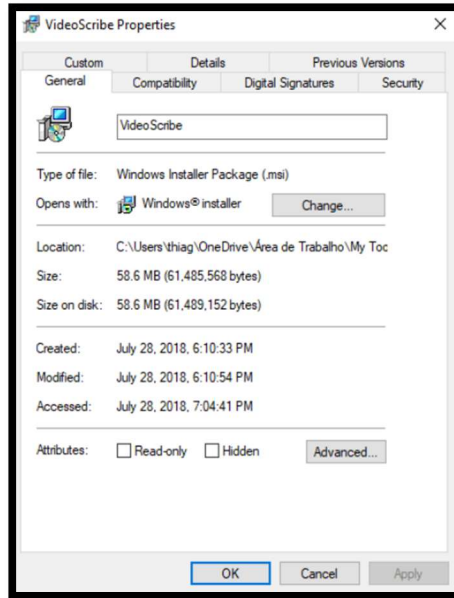
**Description:** These were vulnerabilities found during the installation and download of the VideoScribe software v3.1.0. The software may allow that unverifiable Object Linking and Embedding (OLE) streams in combination with suspicious websites succeed in an arbitrary code injection. The event could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

### Sumário

|   |    |
|---|----|
| 1. File Identification .....                        | 2  |
| 2. File Properties .....                            | 4  |
| 3. Valid Signatures .....                           | 5  |
| 4. Object Linking and Embedding (OLE) streams ..... | 6  |
| 5. Suspicious Websites .....                        | 9  |
| 6. Files Review .....                               | 12 |
| 7. Additional Information.....                      | 14 |
| 8. References.....                                  | 18 |

# 1. File Identification

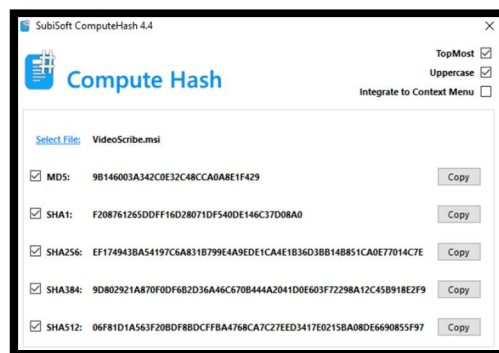




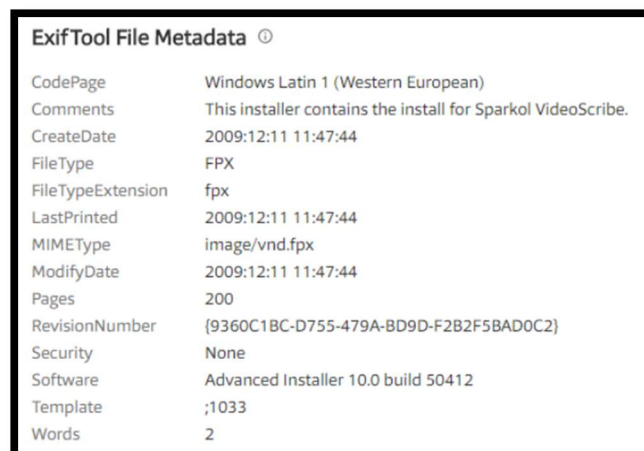
## 2. File Properties



Source: [www.virustotal.com](http://www.virustotal.com)

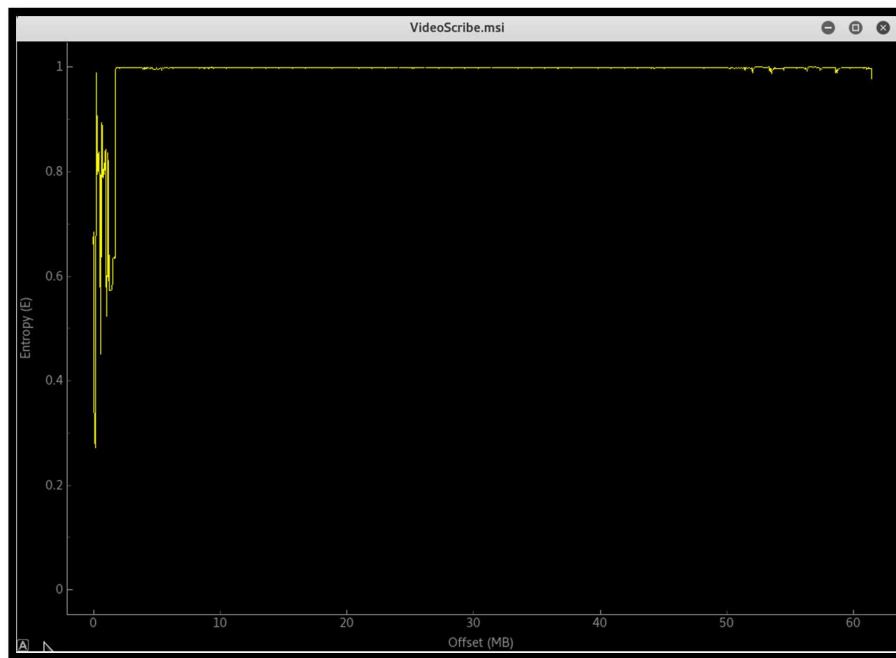


Source: Compute Hash



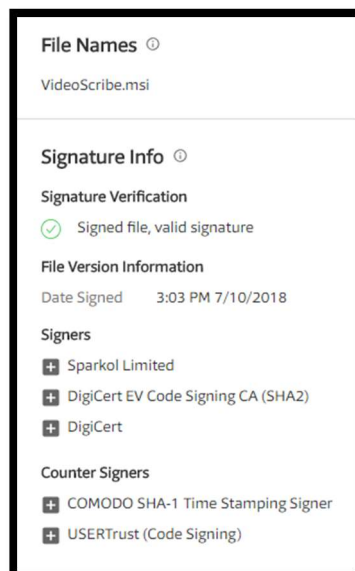
Source: [www.virustotal.com](http://www.virustotal.com)

The entropy test below confirms the presence of compressed files.



Source: kali linux.

### 3. Valid Signatures



Source: [www.virustotal.com](https://www.virustotal.com)

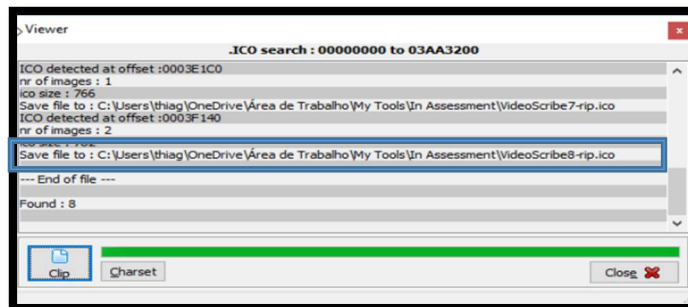
## 4. Object Linking and Embedding (OLE) streams

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).

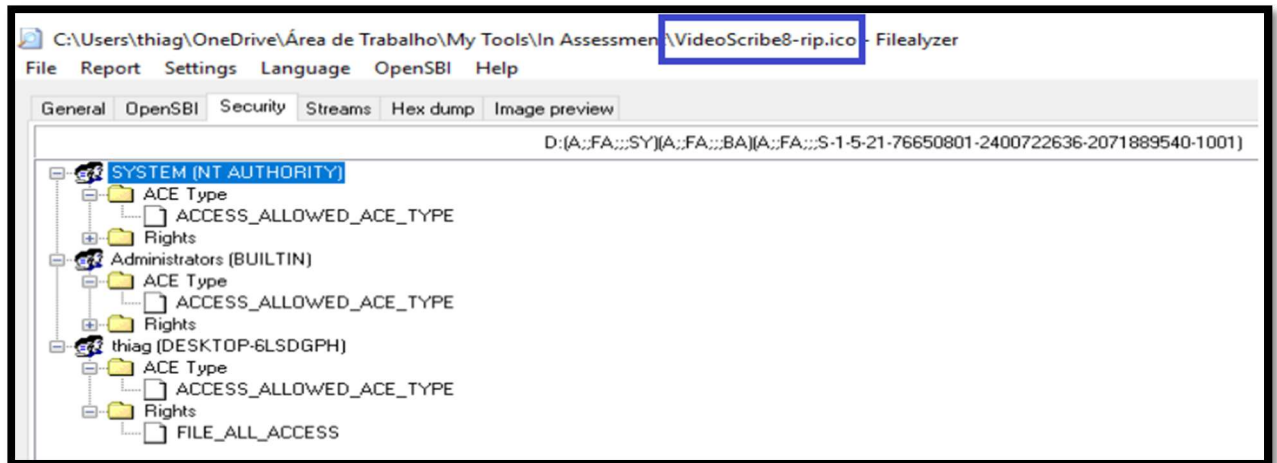
Hidden icons:



Source: Exeinfo PE



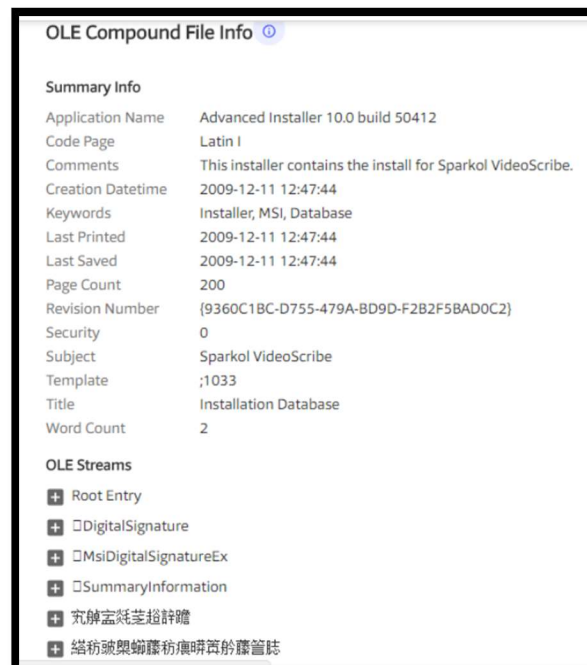
Source: [www.virustotal.com](http://www.virustotal.com)



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.

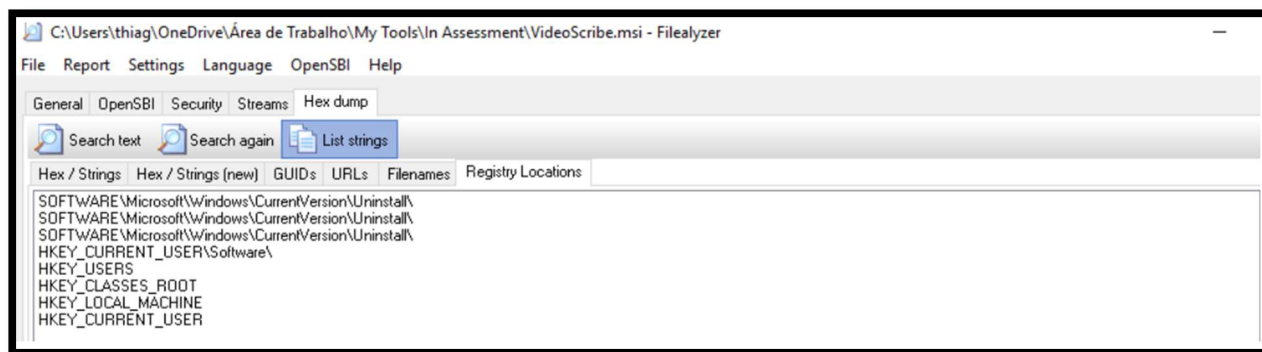
These were the OLE stream found:







Then the access to Registry Locations such as HKEY\_CLASSES\_ROOT allow the merge of default and processing settings to open specific files.

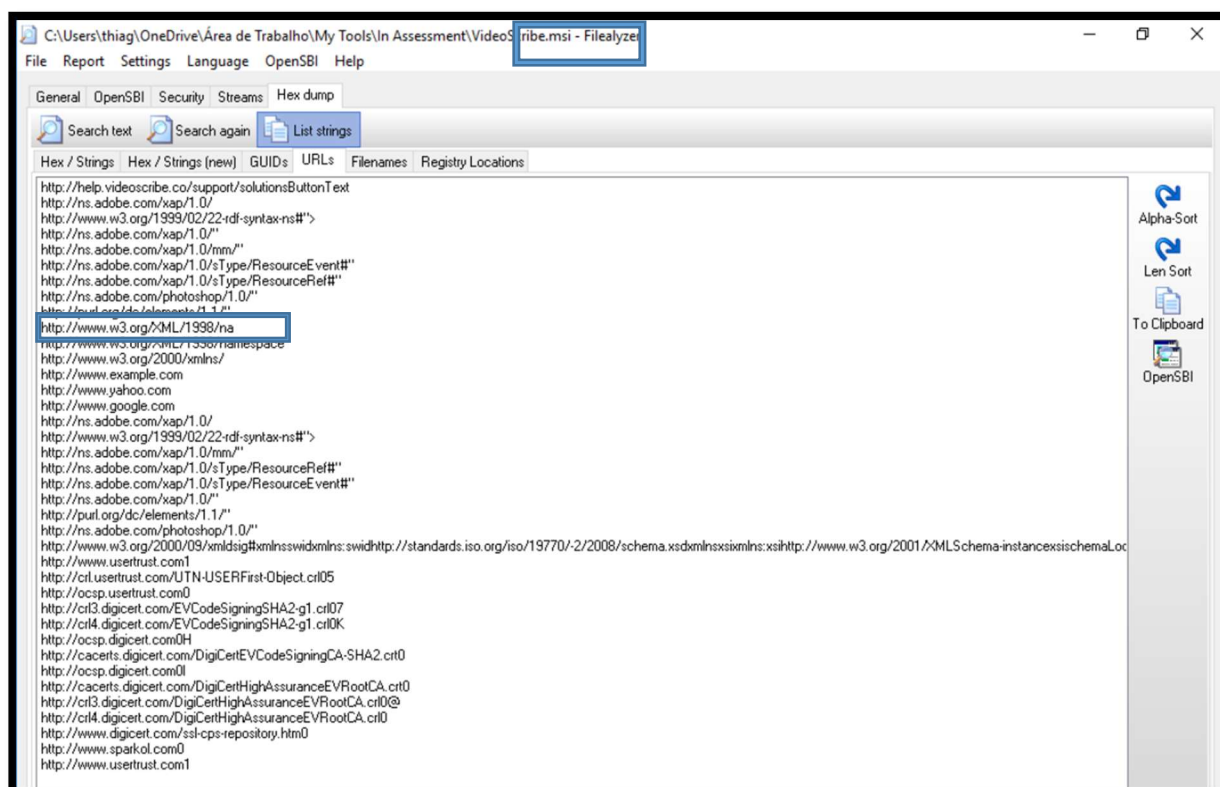


Source: FileAlyzer

## 5. Suspicious Websites

Suspicious websites were identified among acceptable ones such as [www.google.com](http://www.google.com), for example. One website was selected for follow-up and demonstration.

- Example: <http://ns.adobe.com/photoshop/1.0/>



Source: FileAlyzer

[McAfee Home](#) > [Customer URL Ticketing System](#)

## Customer URL Ticketing System

### Check Single URL

McAfee® provides an online tool that enables you to check if a site is categorized within various versions of the SmartFilter Internet Database or the Webwasher URL Filter Database. After you check a URL, this tool also allows you to suggest an alternative categorization for a site. These requests will be addressed within an average of 3-5 business days with some requests requiring additional review and taking longer.

Please select the product you are using. Selecting the appropriate product will provide the correct categorization information to be displayed for you.

McAfee Real-Time Database

Please type in a URL to look up the categorization.

http://ns.adobe.com/photoshop/1.0/

Check URL

#### Categorization in URL Filter database version '286736'

| URL                           | Status          | Categorization | Reputation |
|-------------------------------|-----------------|----------------|------------|
| http://ns.adobe.com/photo ... | Categorized URL | - Business     | Unverified |

[McAfee Home](#) > [Customer URL Ticketing System](#)

## Customer URL Ticketing System

### Check Single URL

McAfee® provides an online tool that enables you to check if a site is categorized within various versions of the SmartFilter Internet Database or the Webwasher URL Filter Database. After you check a URL, this tool also allows you to suggest an alternative categorization for a site. These requests will be addressed within an average of 3-5 business days with some requests requiring additional review and taking longer.

Please select the product you are using. Selecting the appropriate product will provide the correct categorization information to be displayed for you.

McAfee Real-Time Database

Please type in a URL to look up the categorization.

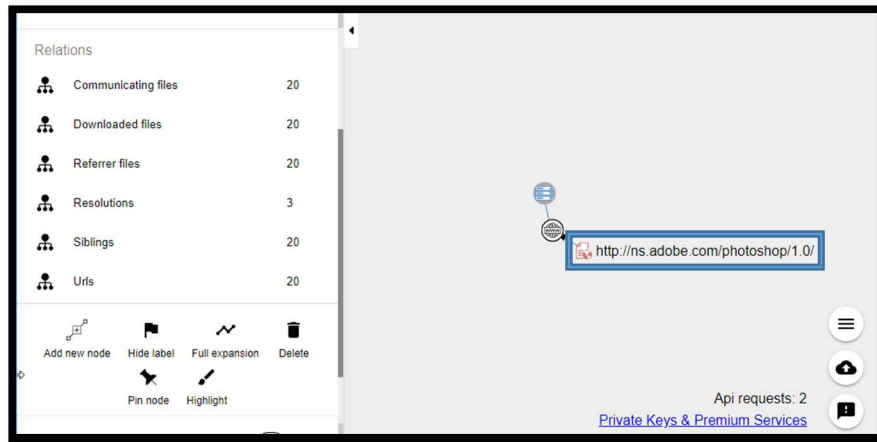
http://ns.adobe.com/

Check URL

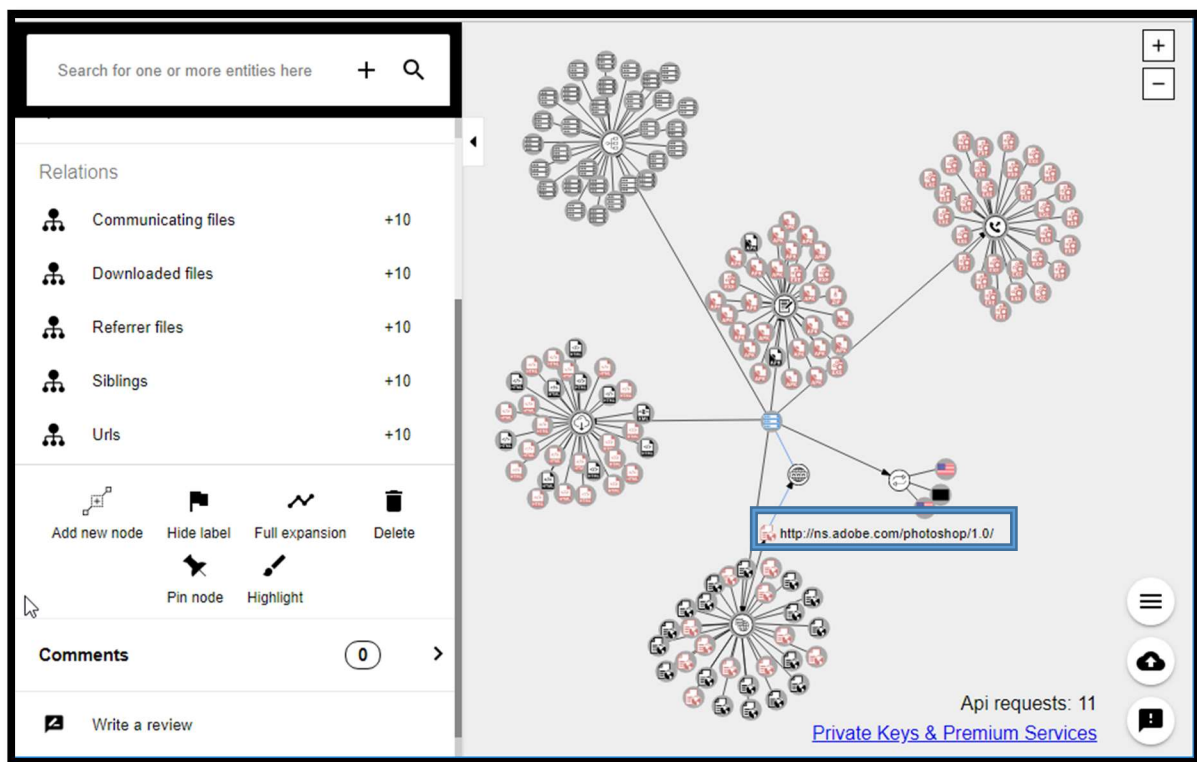
#### Categorization in URL Filter database version '286736'

| URL                  | Status          | Categorization                    | Reputation |
|----------------------|-----------------|-----------------------------------|------------|
| http://ns.adobe.com/ | Categorized URL | - Business<br>- Software/Hardware | Unverified |

Source: [www.trustedsource.org](http://www.trustedsource.org)

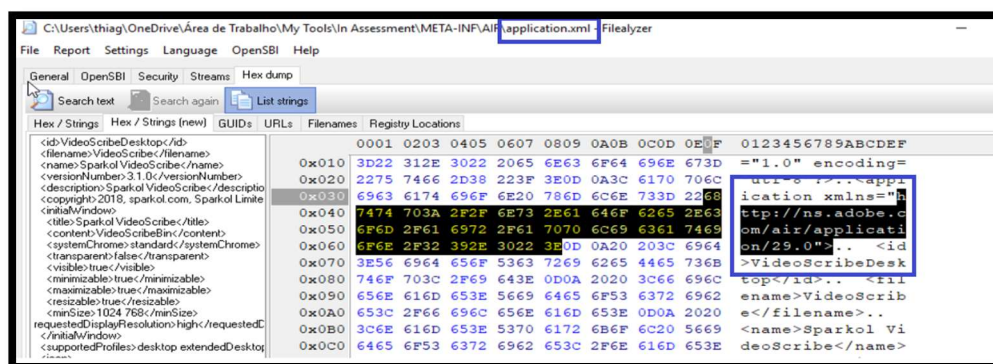


Source: www.virustotal.com



Source: www.virustotal.com

The suspicious websites were identified as part of XML files.



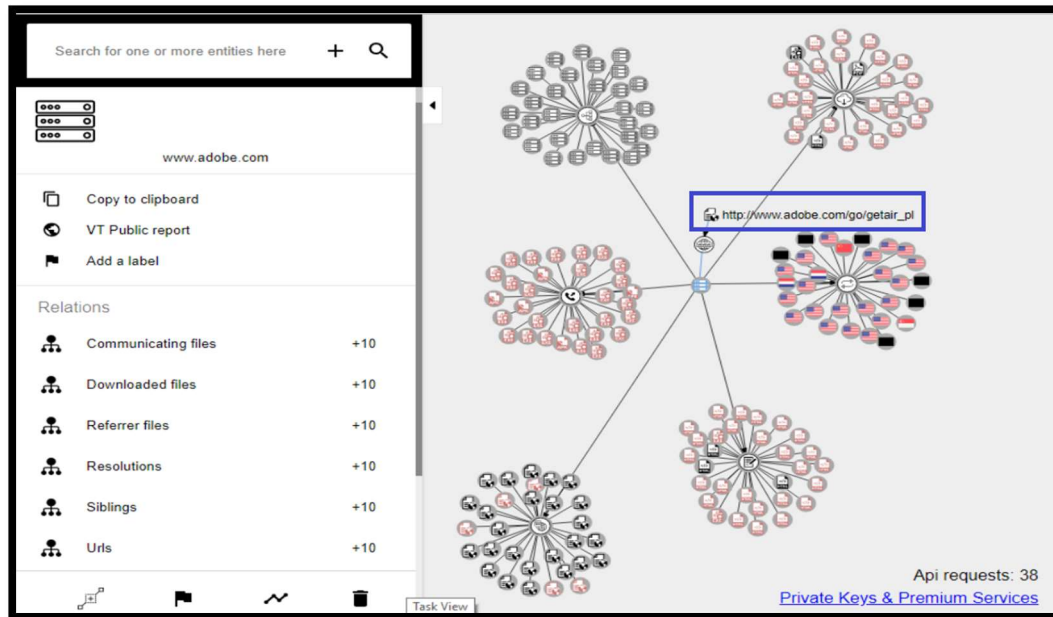
Source: FileAlyzer

## 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)

|  | xml-id | indicator (27)  | severity |
|--|--------|---|----------|
|  | 1269   | The file references (1) blacklisted library   | 1        |
|  | 1434   | The file references a URL pattern (http://www.adobe.com/go/getair_pl)                         | 1        |
|  | 1434   | The file references a URL pattern (http://www.adobe.com/go/getair_nl)                         | 1        |
|  | 1434   | The file references a URL pattern (http://www.adobe.com/go/getair_cz)                         | 1        |
|  | 1434   | The file references a URL pattern (http://www.adobe.com/go/getair_br)                         | 1        |
|  | 1434   | The file references a URL pattern (http://www.adobe.com/go/getair_kr)                         | 1        |
|  | 1434   | The file references a URL pattern (http://www.adobe.com/go/getair_jp)                         | 1        |
|  | 1434   | The file references a URL pattern (http://www.adobe.com/go/getair_it)                         | 1        |
|  | 1434   | The file references a URL pattern (http://www.adobe.com/go/getair_fr)                         | 1        |
|  | 1434   | The file references a URL pattern (http://www.adobe.com/go/getair_es)                         | 1        |
|  | 1434   | The file references a URL pattern (http://www.adobe.com/go/getair_)                           | 1        |
|  | 1434   | The file references a URL pattern (http://www.adobe.com/go/getair_de)                         | 1        |
|  | 1120   | The file is scored (0/67) by virustotal   | 2        |
|  | 1262   | The file imports (1) anonymous function(s)  | 2        |
|  | 1266   | The file imports (17) blacklisted function(s)   | 2        |
|  | 1100   | The file opts for Data Execution Prevention (DEP)   | 3        |
|  | 1633   | The file references (1) guid string(s)  | 3        |
|  | 1229   | The file signature is 'Microsoft Visual C++ 8'  | 5        |
|  | 1430   | The file references (44) blacklisted string(s)  | 5        |
|  | 1424   | The original file name is 'CaptiveAppEntry.exe'   | 5        |
|  | 1102   | The file opts for Address Space Layout Randomization (ASLR)                                   | 5        |
|  | 1106   | The file opts for cookies on the stack (GS)   | 5        |
|  | 1011   | The file references a certificate (offset: 0x0000F600, size: 6616 bytes)                      | 5        |
|  | 1277   | The file imports (1) undocumented function(s)   | 5        |
|  | 1268   | The file references (81) whitelist strings  | 9        |
|  | 1152   | The file references a debug symbols file (path: 'e:\rws\st_make\code\build\win\results\rel... | 9        |
|  | 1109   | The file ignores Code Integrity   | 9        |

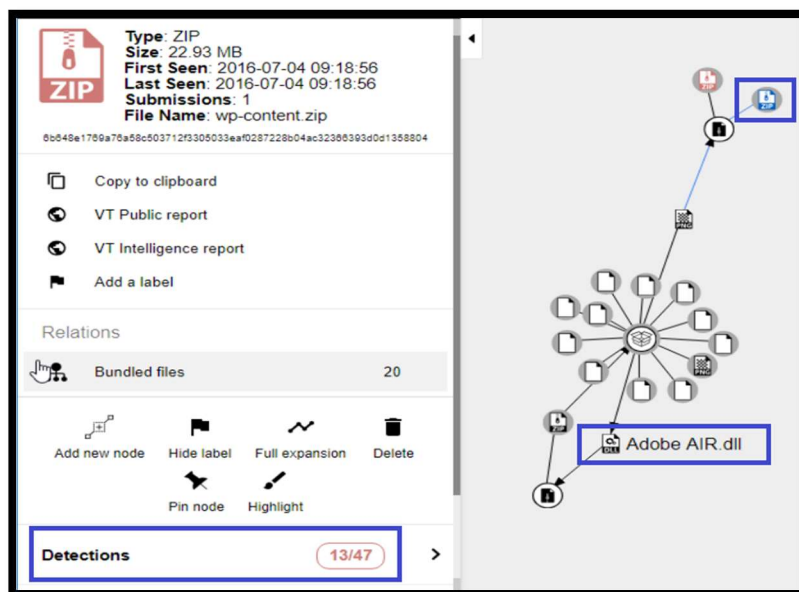


A complete list of DLL files would include:

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:

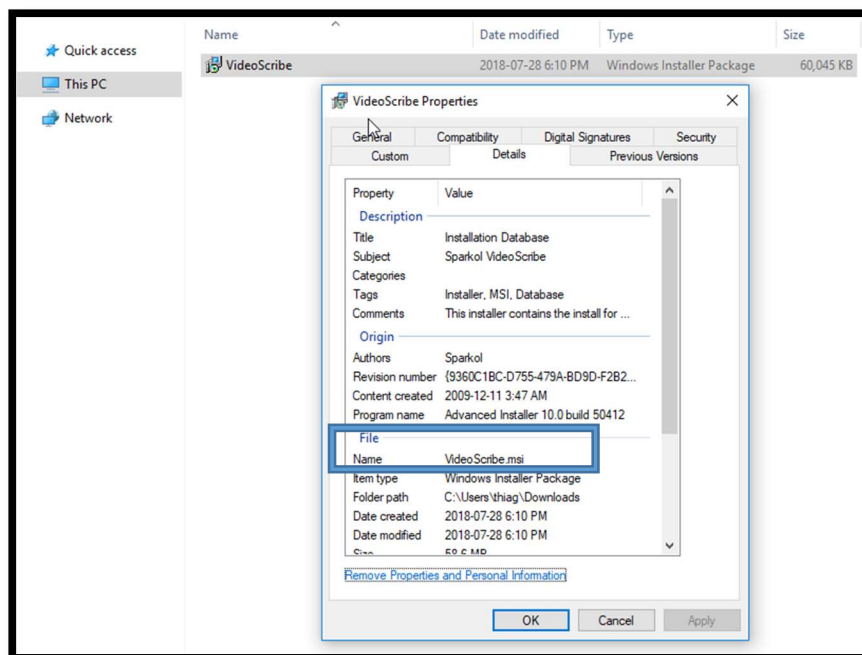
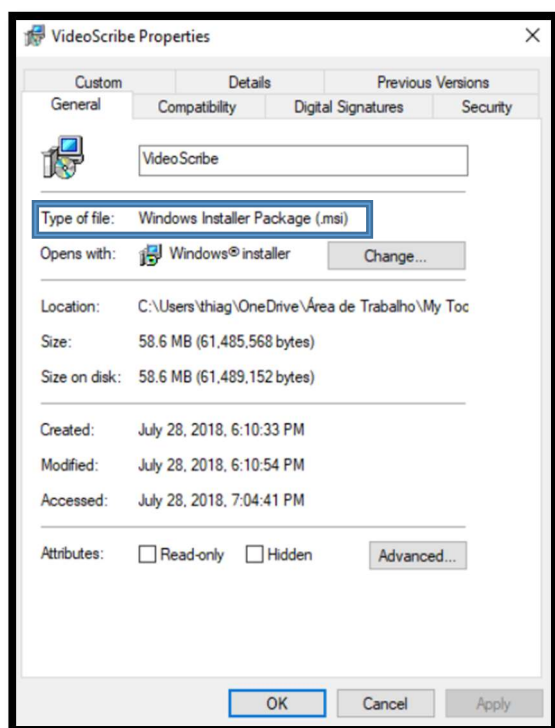


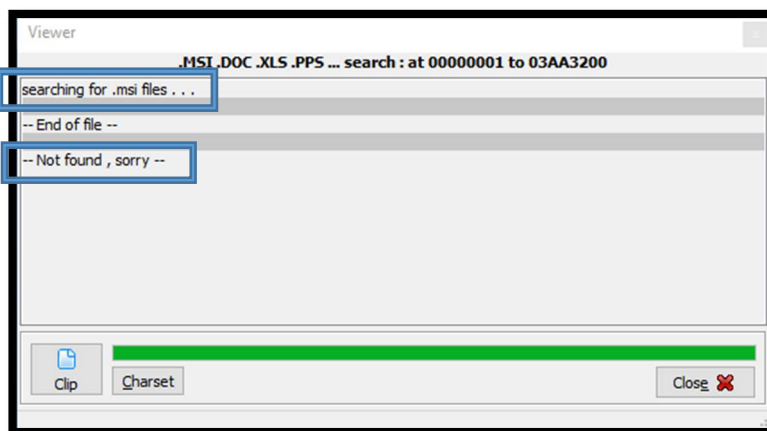
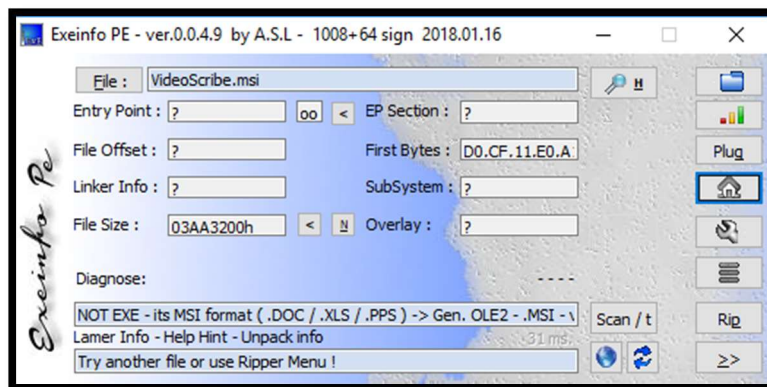
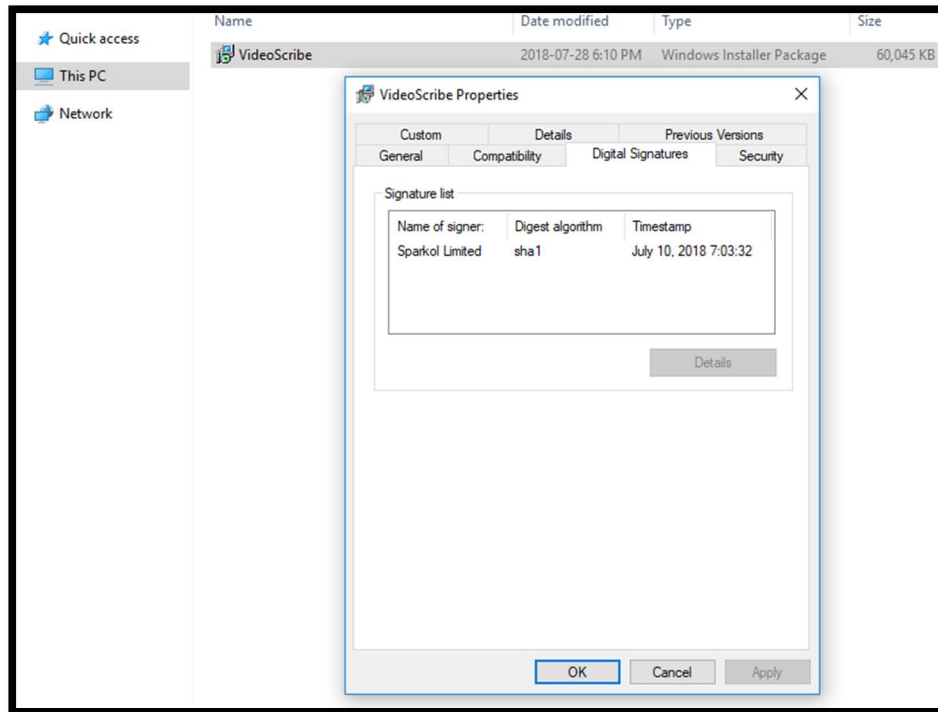
## 7. Additional Information

Initially, it was thought that the software was part of a possible file impersonation case, but this assumption was cleared directly by Microsoft as not a security breach (MSRC#47003-0461058685).

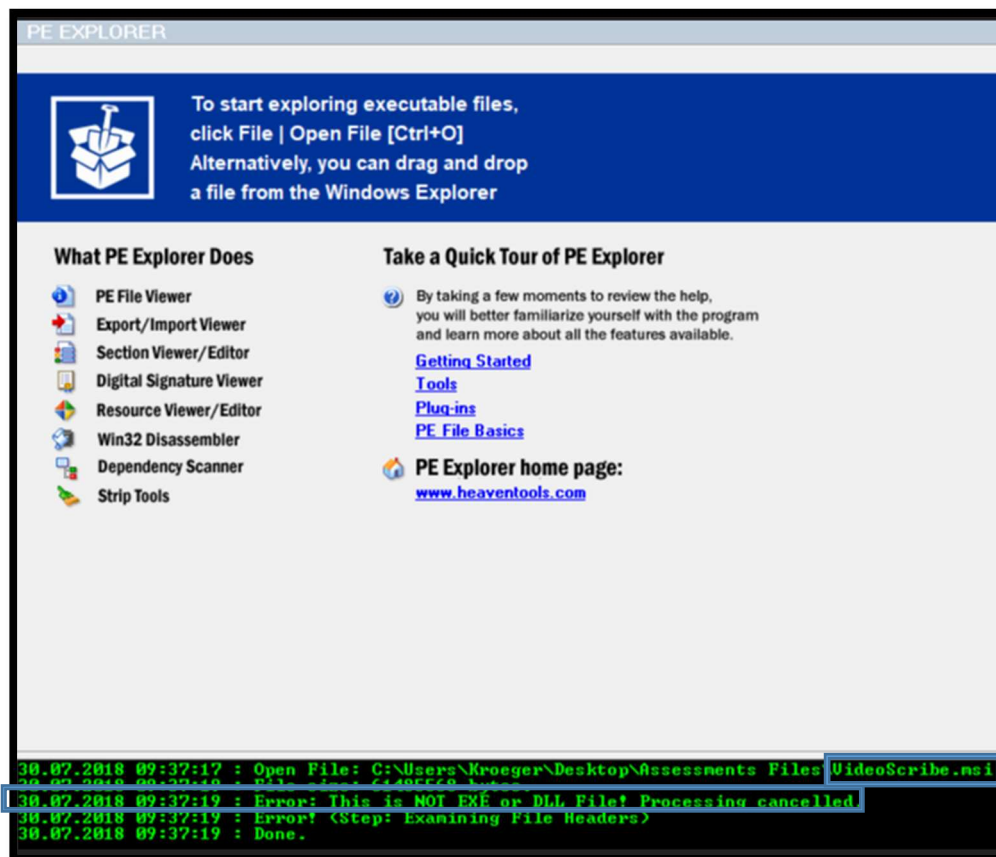
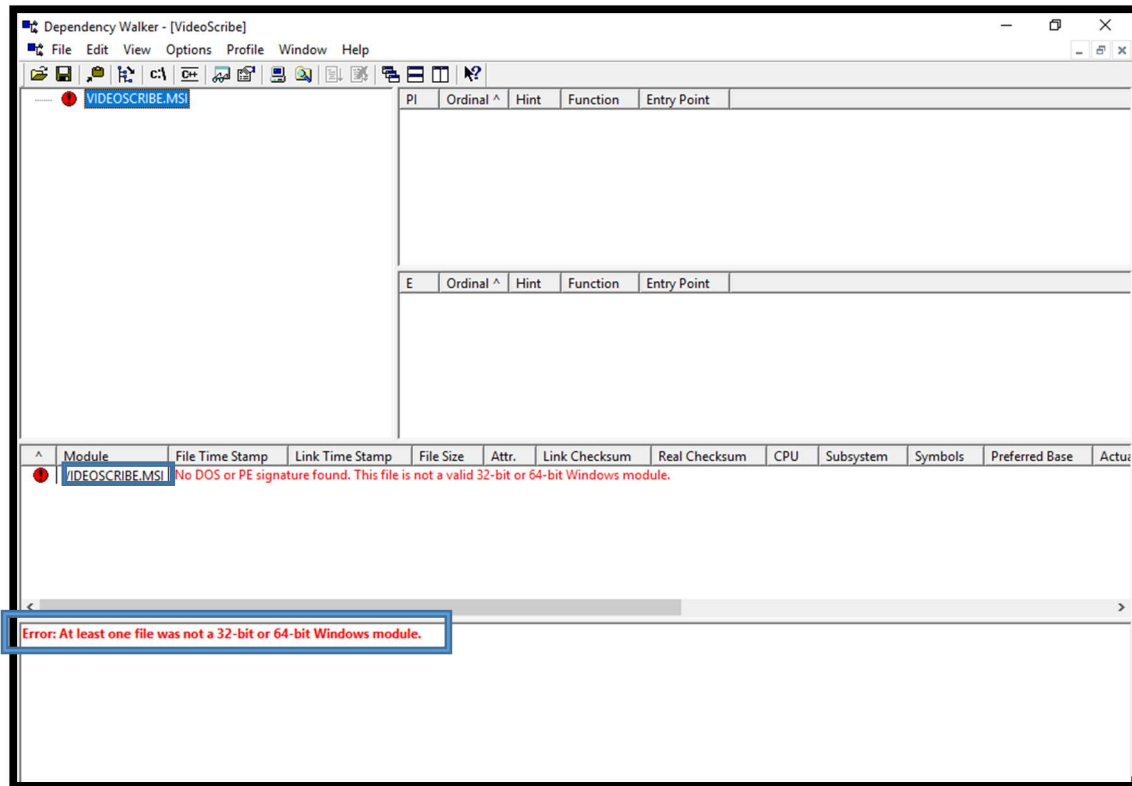
It was identified a vulnerability in the recognition of \*.msi files in Windows 10 during the installation and download of the VideoScribe software. The Windows 10 recognized the file as a Windows Installer Package, however there was no \*.msi file in the software or a valid 32-bit / 64-bit Windows module. In this case, Windows 10 would have to issue an error message such as “2766 – The file [2] is an invalid MSI storage file” preventing the installation of the software that includes an extensive list of unverifiable Object Linking and Embedding (OLE) streams and some suspicious websites.



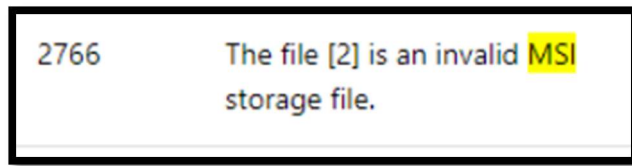








## Error Message



## 8. 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>
- <https://docs.microsoft.com/en-us/windows/desktop/Msi/windows-installer-error-messages>