VideoScribe v3.1.0 Assessment

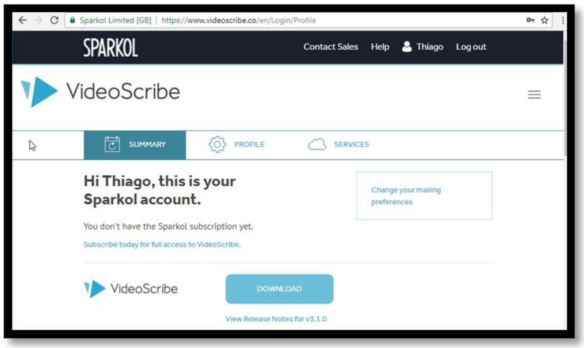
Date: August 26th, 2018.

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 or a PE executable files embedded in the software that revealed itself as a document (*.doc) file, suggesting some degree of file impersonation.

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** 20

1. File Identification



Sparkol Limited [GB] | https://www.videoscribe.co/en/Login/Profile

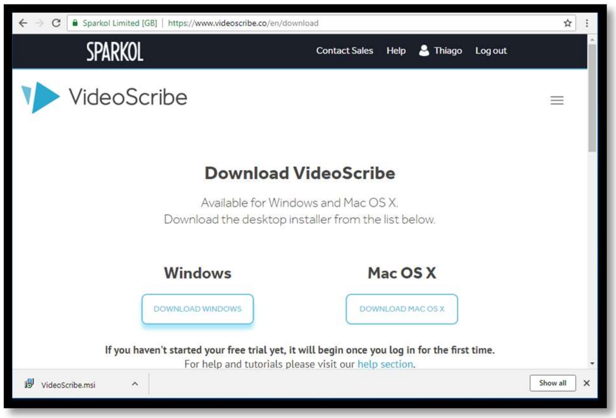
Hi Thiago, this is your Sparkol account.

You don't have the Sparkol subscription yet.

Subscribe today for full access to VideoScribe.

Change your mailing preferences

View Release Notes for v3.1.0



Sparkol Limited [GB] | https://www.videoscribe.co/en/download

Download VideoScribe

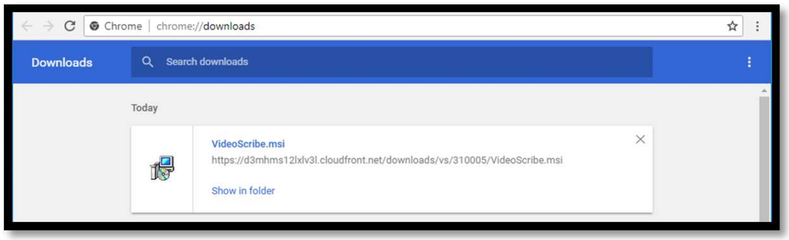
Available for Windows and Mac OS X.
Download the desktop installer from the list below.

Windows DOWNLOAD WINDOWS

Mac OS X DOWNLOAD MAC OS X

If you haven't started your free trial yet, it will begin once you log in for the first time.
For help and tutorials please visit our help section.

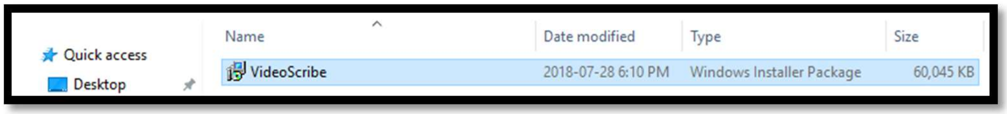
VideoScribe.msi



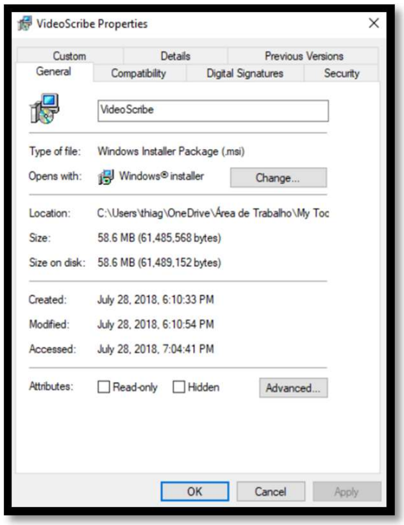
Chrome | chrome://downloads

Today

VideoScribe.msi
https://d3mhms12lxlv3l.cloudfront.net/downloads/vs/310005/VideoScribe.msi
Show in folder



Name	Date modified	Type	Size
VideoScribe	2018-07-28 6:10 PM	Windows Installer Package	60,045 KB



VideoScribe

Type of file: Windows Installer Package (.msi)

Opens with: Windows® installer

Location: C:\Users\thiag\OneDrive\Área de Trabalho\My Toc

Size: 58.6 MB (61,485,568 bytes)

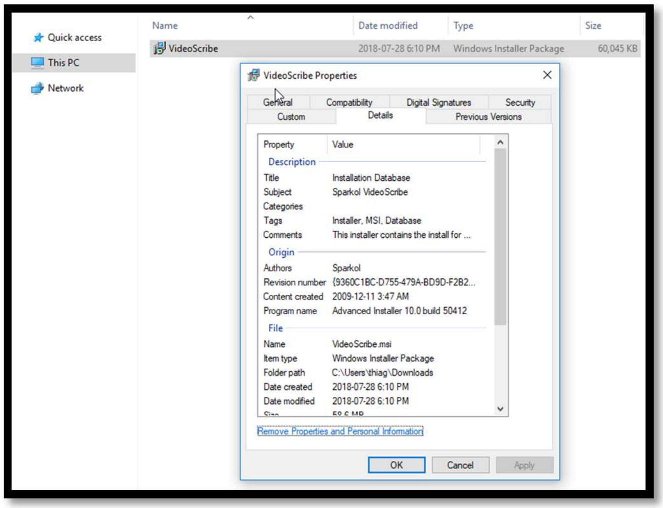
Size on disk: 58.6 MB (61,489,152 bytes)

Created: July 28, 2018, 6:10:33 PM

Modified: July 28, 2018, 6:10:54 PM

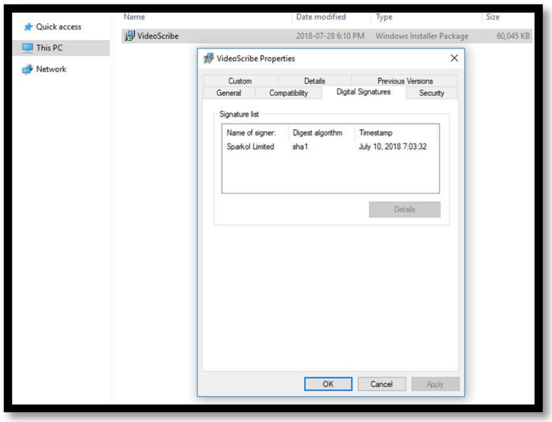
Accessed: July 28, 2018, 7:04:41 PM

Attributes: □ Read-only □ Hidden



Name	Date modified	Type	Size
VideoScribe	2018-07-28 6:10 PM	Windows Installer Package	60,045 KB

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
Size	58.6 MB

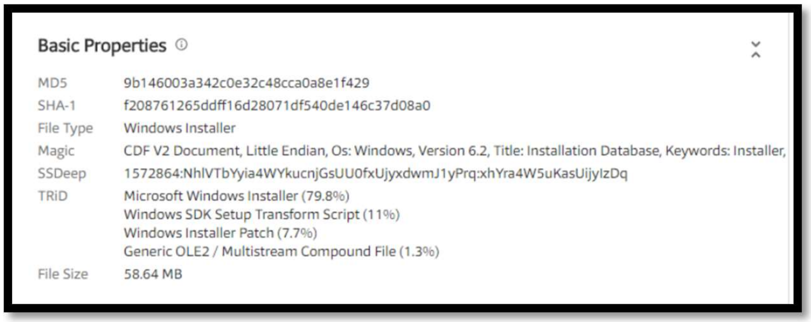


Name	Date modified	Type	Size
VideoScribe	2018-07-28 6:10 PM	Windows Installer Package	60,045 KB

Signature list

Name of signer:	Digest algorithm	Timestamp
Sparkol Limited	sha1	July 10, 2018 7:03:32

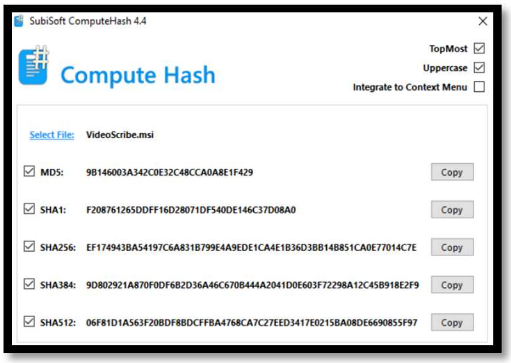
2. File Properties



Basic Properties

MD5	9b146003a342c0e32c48cca0a8e1f429
SHA-1	f208761265ddff16d28071df540de146c37d08a0
File Type	Windows Installer
Magic	CDF V2 Document, Little Endian, Os: Windows, Version 6.2, Title: Installation Database, Keywords: Installer,
SSDeep	1572864:NhlVTbYyia4WYkucnjGsUU0fxUjyxdwmJ1yPrq:xhYra4W5uKasUijyIzDq
TRiD	Microsoft Windows Installer (79.8%) Windows SDK Setup Transform Script (11%) Windows Installer Patch (7.7%) Generic OLE2 / Multistream Compound File (1.3%)
File Size	58.64 MB

Source: www.virustotal.com



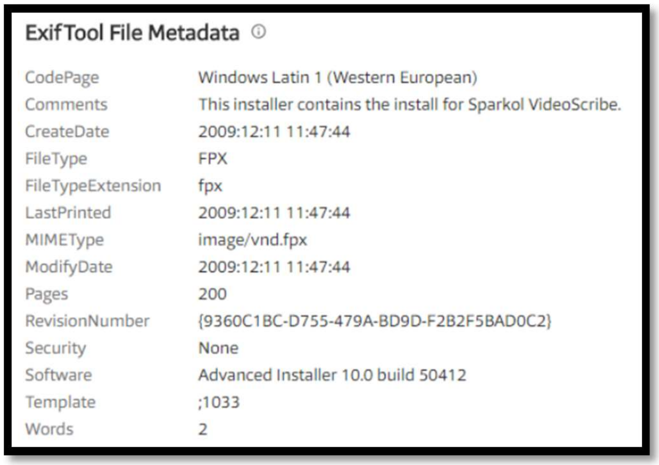
Compute Hash

TopMost ☑
Uppercase ☑
Integrate to Context Menu □

Select File: VideoScribe.msi

☑	MD5:	9B146003A342C0E32C48CCA0A8E1F429	Copy
☑	SHA1:	F208761265DDFF16D28071DF540DE146C37D08A0	Copy
☑	SHA256:	EF174943BA54197C6A831B799E4A9EDE1CA4E1B36D3BB14B851CA0E77014C7E	Copy
☑	SHA384:	9D802921A870F0DF6B2D36A46C670B444A2041D0E603F72298A12C45B918E2F9	Copy
☑	SHA512:	06F81D1A563F20BDF8BDCFFBA4768CA7C27EED3417E0215BA08DE6690855F97	Copy

Source: Compute Hash

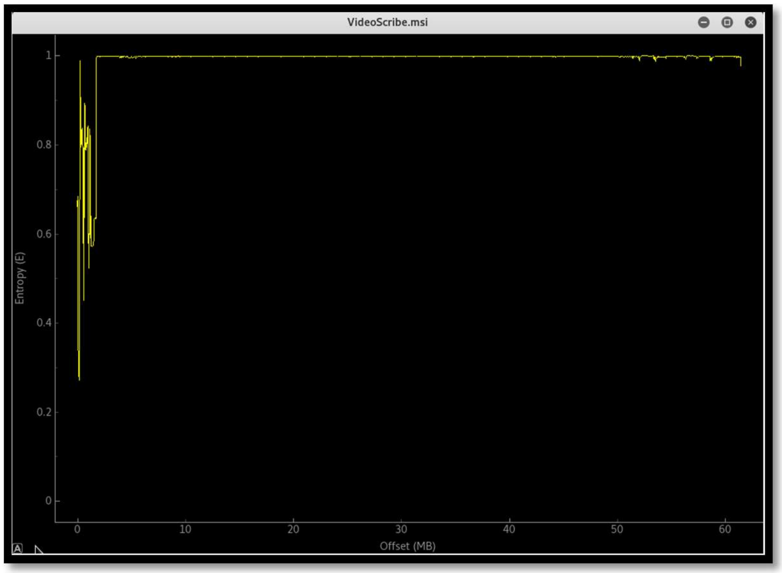


ExifTool File Metadata

CodePage	Windows Latin 1 (Western European)
Comments	This installer contains the install for Sparkol VideoScribe.
CreateDate	2009:12:11 11:47:44
FileType	FPX
FileTypeExtension	fpx
LastPrinted	2009:12:11 11:47:44
MIMEType	image/vnd.fpx
ModifyDate	2009:12:11 11:47:44
Pages	200
RevisionNumber	{9360C1BC-D755-479A-BD9D-F2B2F5BAD0C2}
Security	None
Software	Advanced Installer 10.0 build 50412
Template	;1033
Words	2

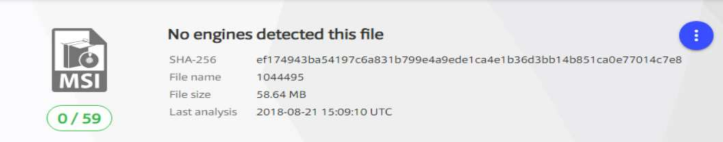
Source: www.virustotal.com

The entropy test below confirms the presence of compressed files.



Source: kali linux.

Which does not allow the detection of malicious files:



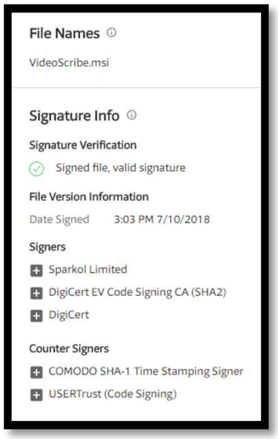
0 / 59

No engines detected this file

SHA-256 ef174943ba54197c6a831b799e4a9ede1ca4e1b36d3bb14b851ca0e77014c7e8
File name 1044495
File size 58.64 MB
Last analysis 2018-08-21 15:09:10 UTC

Source: Virus Total.

3. Valid Signatures



File Names

VideoScribe.msi

Signature Info

Signature Verification

✓ Signed file, valid signature

File Version Information

Date Signed 3:03 PM 7/10/2018

Signers

- Sparkol Limited
- DigiCert EV Code Signing CA (SHA2)
- DigiCert

Counter Signers

- COMODO SHA-1 Time Stamping Signer
- USERTrust (Code Signing)

Source: www.virustotal.com

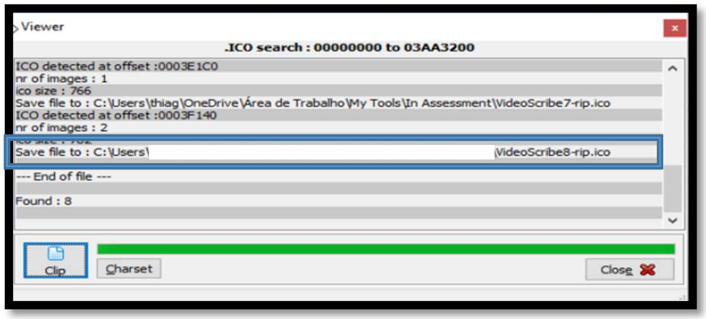
4. Object Linking and Embedding (OLE) streams

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.

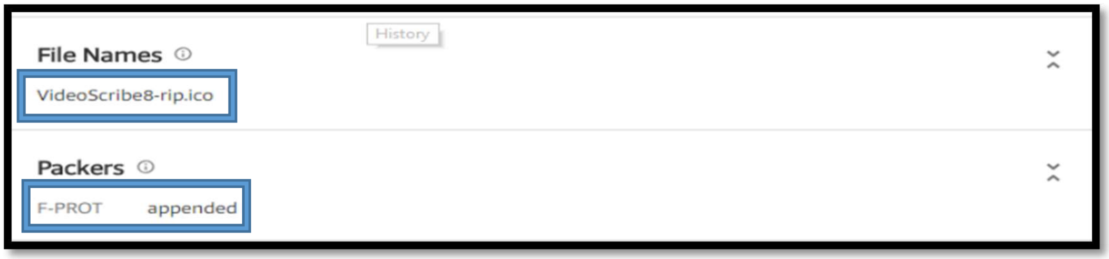
There were 08 hidden icons found in the software. Note that these files were packed. Once unpacked they show an ACCESS_ALLOWED_ACE_TYPE. This structure defines an access-control entry (ACE) for the discretionary access-control list (DACL) that controls access to an object for a specific subject identified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

Hidden icons:



```
ICO detected at offset :0003E1C0
nr of images : 1
ico size : 766
Save file to : C:\Users\thiag\OneDrive\Área de Trabalho\My Tools\In Assessment\VideoScribe7-rip.ico
ICO detected at offset :0003F140
nr of images : 2
Save file to : C:\Users\[redacted]\VideoScribe8-rip.ico
--- End of file ---
Found : 8
```

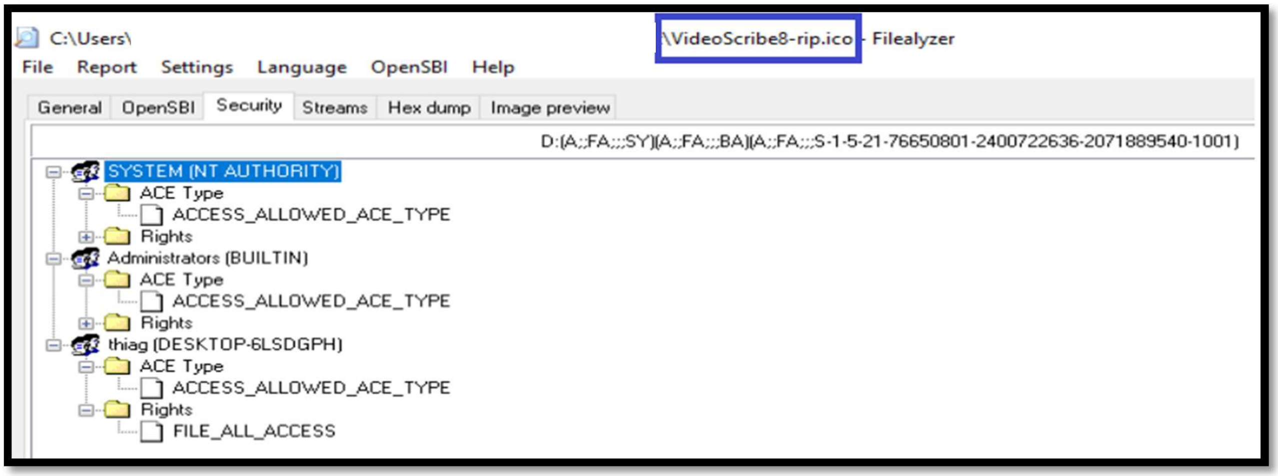
Source: Exeinfo PE



File Names: VideoScribe8-rip.ico

Packers: F-PROT appended

Source: www.virustotal.com



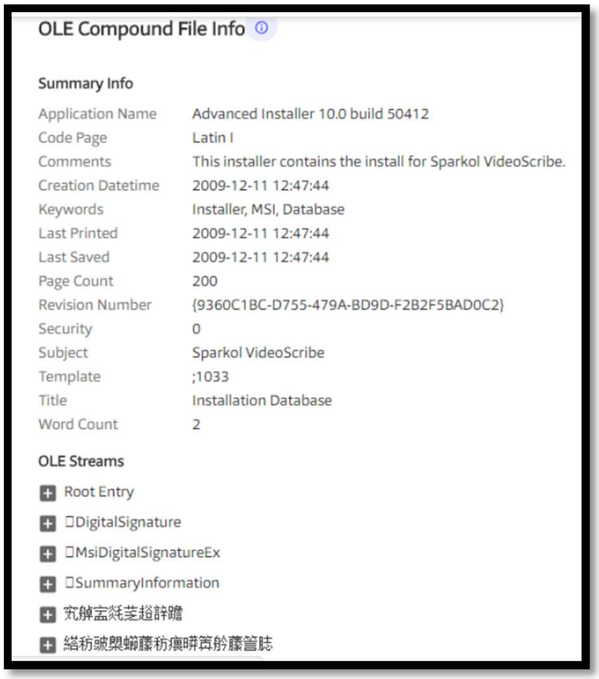
C:\Users\ \VideoScribe8-rip.ico - Filealyzer

```
D:(A;;FA;;;SY)(A;;FA;;;BA)(A;;FA;;;S-1-5-21-76650801-2400722636-2071889540-1001)
SYSTEM (NT AUTHORITY)
    ACE Type
        ACCESS_ALLOWED_ACE_TYPE
    Rights
Administrators (BUILTIN)
    ACE Type
        ACCESS_ALLOWED_ACE_TYPE
    Rights
thiag (DESKTOP-6LSDGPH)
    ACE Type
        ACCESS_ALLOWED_ACE_TYPE
    Rights
        FILE_ALL_ACCESS
```

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:



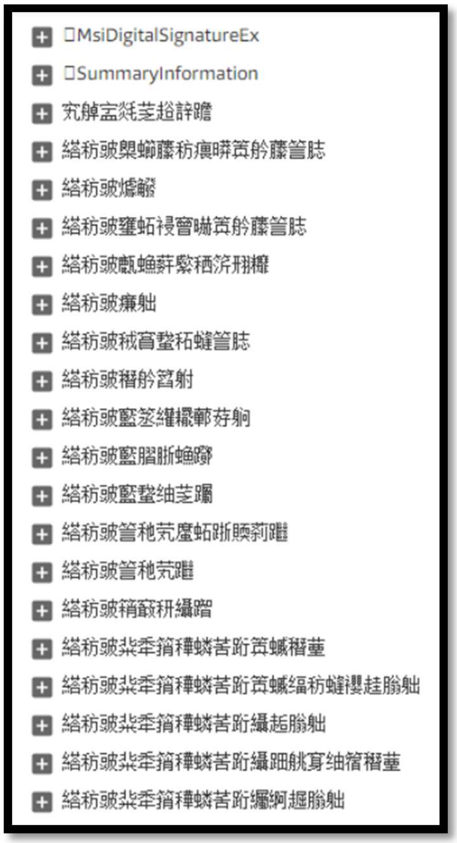
OLE Compound File Info

Summary Info

Application Name	Advanced Installer 10.0 build 50412
Code Page	Latin I
Comments	This installer contains the install for Sparkol VideoScribe.
Creation Datetime	2009-12-11 12:47:44
Keywords	Installer, MSI, Database
Last Printed	2009-12-11 12:47:44
Last Saved	2009-12-11 12:47:44
Page Count	200
Revision Number	{9360C1BC-D755-479A-BD9D-F2B2F5BAD0C2}
Security	0
Subject	Sparkol VideoScribe
Template	;1033
Title	Installation Database
Word Count	2

OLE Streams

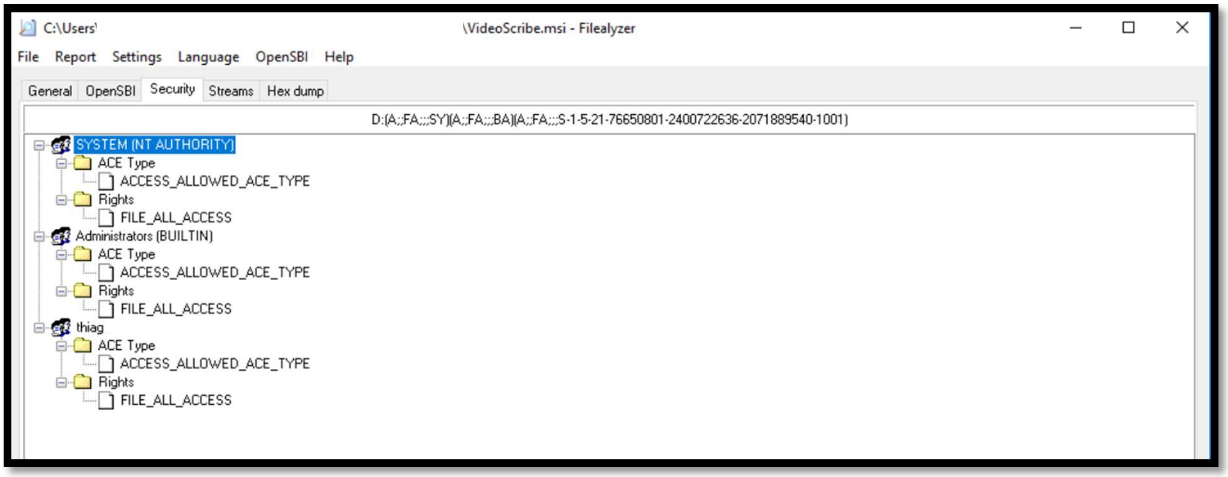
- ⊞ Root Entry
- ⊞ □DigitalSignature
- ⊞ □MsiDigitalSignatureEx
- ⊞ □SummaryInformation
- ⊞ 究艴宏浅茎趦詳蹭
- ⊞ 緒秎虢槼蟵藤秎癲瞨筫舲藤筥詰



```
□MsiDigitalSignatureEx
□SummaryInformation
究艀宼烒茎趦詳贍
綌秎虢槼蛳藤秎瘼暻莔舲藤管朓
綌秎虢熩觿
綌秎虢墾蛞祲瞀暩莔舲藤管朓
綌秎虢甗蝤薢緊粞洊翮櫼
綌秎虢癄舼
綌秎虢稢賫蟼祏蟢管朓
綌秎虢稰舲窌躰
綌秎虢藍笶纘繬鄟矦躵
綌秎虢藍膉脤蝤躋
綌秎虢藍蟼䌷茎躝
綌秎虢管秜荒蟨蛞蹢賥莿躙
綌秎虢管秜荒躙
綌秎虢簎畝䎁纘踏
綌秎虢紥垂猐穛蟒苦跅莔蝛稰蓳
綌秎虢紥垂猐穛蟒苦跅莔蝛缊秎蟢禵趆腨舼
綌秎虢紥垂猐穛蟒苦跅纘趏腨舼
綌秎虢紥垂猐穛蟒苦跅纘蹎艞寊䌷稸稰蓳
綌秎虢紥垂猐穛蟒苦跅繩絅趧腨舼
```

Source: www.virustotal.com

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

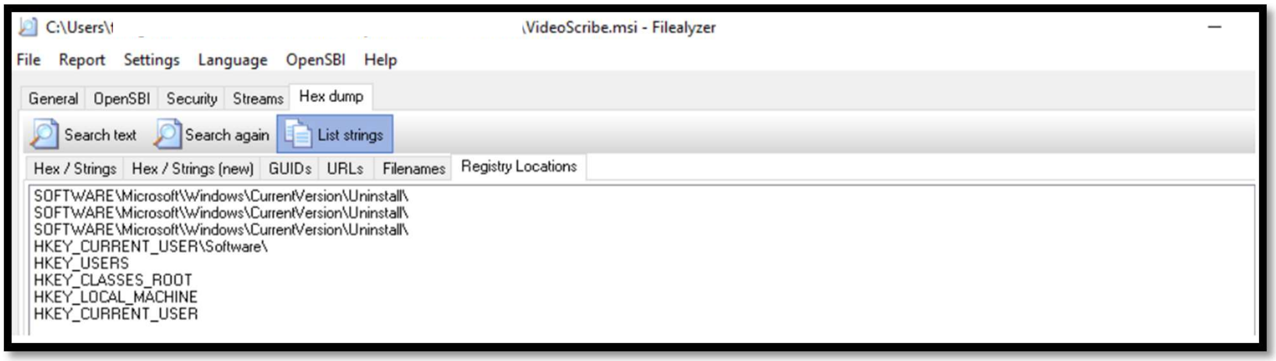


C:\Users'
\VideoScribe.msi - Filealyzer
File Report Settings Language OpenSBI Help
General OpenSBI Security Streams Hex dump

```
D:(A;;FA;;;SY)(A;;FA;;;BA)(A;;FA;;;S-1-5-21-76650801-2400722636-2071889540-1001)
SYSTEM (NT AUTHORITY)
    ACE Type
        ACCESS_ALLOWED_ACE_TYPE
    Rights
        FILE_ALL_ACCESS
Administrators (BUILTIN)
    ACE Type
        ACCESS_ALLOWED_ACE_TYPE
    Rights
        FILE_ALL_ACCESS
thiag
    ACE Type
        ACCESS_ALLOWED_ACE_TYPE
    Rights
        FILE_ALL_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.



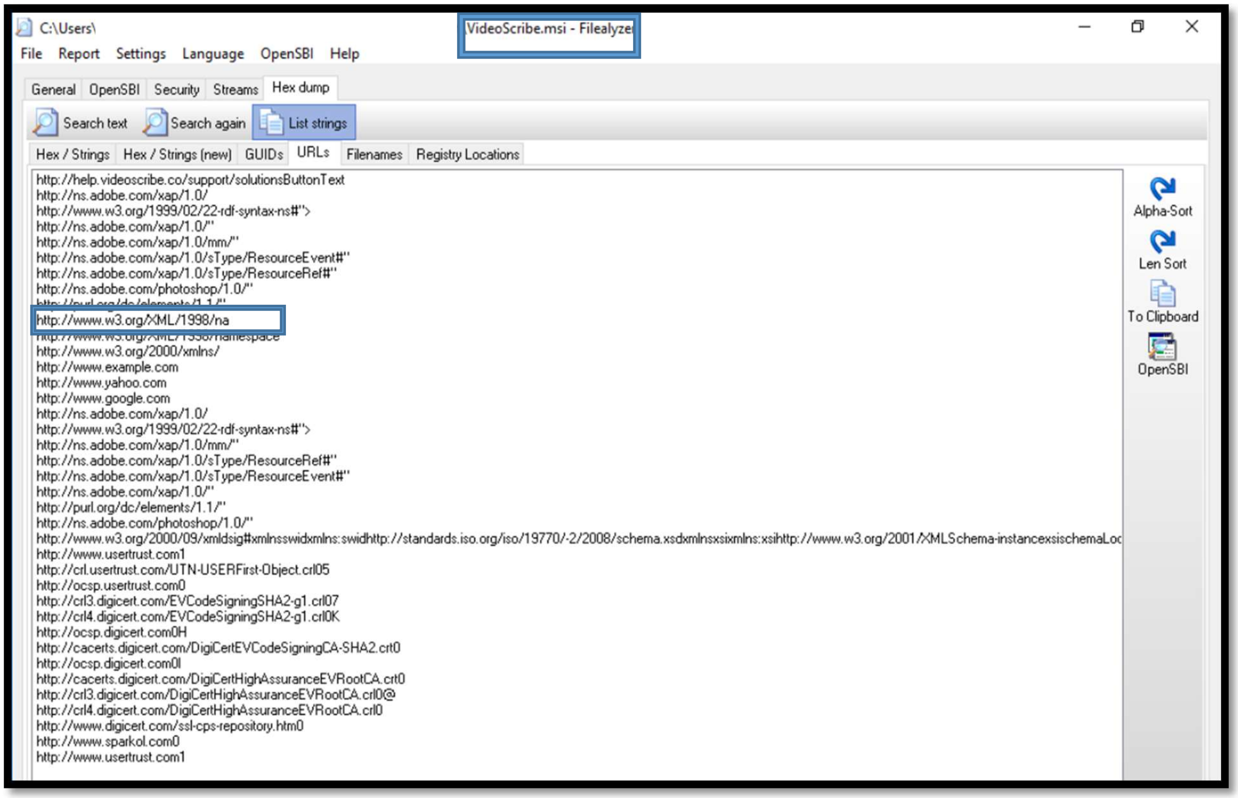
```
SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\
SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\
SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\
HKEY_CURRENT_USER\Software\
HKEY_USERS
HKEY_CLASSES_ROOT
HKEY_LOCAL_MACHINE
HKEY_CURRENT_USER
```

Source: FileAlyzer

5. Suspicious Websites

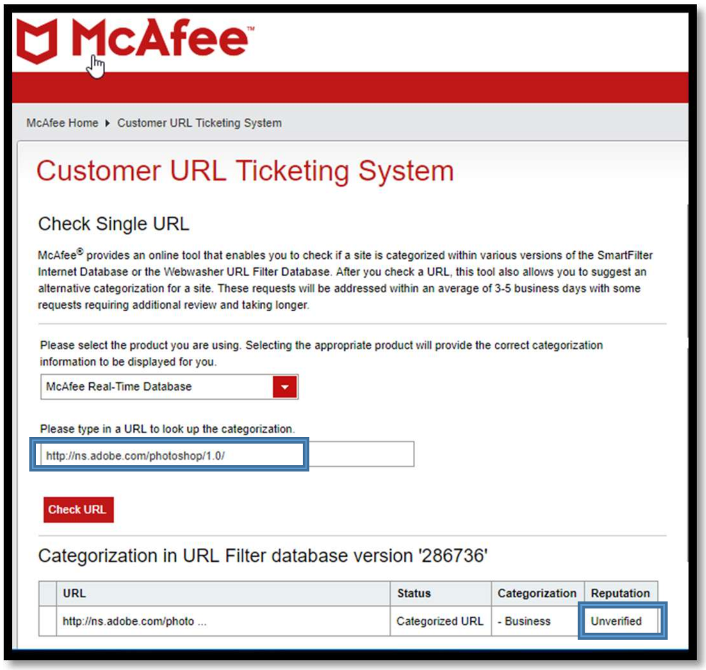
Suspicious websites were identified among acceptable ones such as www.google.com, for example. One website was selected for follow-up and demonstration.

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



```
http://help.videoscribe.co/support/solutionsButtonText
http://ns.adobe.com/xap/1.0/
http://www.w3.org/1999/02/22-rdf-syntax-ns#">
http://ns.adobe.com/xap/1.0/"
http://ns.adobe.com/xap/1.0/mm/"
http://ns.adobe.com/xap/1.0/sType/ResourceEvent#"
http://ns.adobe.com/xap/1.0/sType/ResourceRef#"
http://ns.adobe.com/photoshop/1.0/"
http://purl.org/dc/elements/1.1/"
http://www.w3.org/XML/1998/na
http://www.w3.org/XML/1998/namespace
http://www.w3.org/2000/xmlns/
http://www.example.com
http://www.yahoo.com
http://www.google.com
http://ns.adobe.com/xap/1.0/
http://www.w3.org/1999/02/22-rdf-syntax-ns#">
http://ns.adobe.com/xap/1.0/mm/"
http://ns.adobe.com/xap/1.0/sType/ResourceRef#"
http://ns.adobe.com/xap/1.0/sType/ResourceEvent#"
http://ns.adobe.com/xap/1.0/"
http://purl.org/dc/elements/1.1/"
http://ns.adobe.com/photoshop/1.0/"
http://www.w3.org/2000/09/xmldsig#xmlnsswidxmlns:swidhttp://standards.iso.org/iso/19770/-2/2008/schema.xsdxmlnsxsixmlns:xsihttp://www.w3.org/2001/XMLSchema-instancexsischemaLoc
http://www.usertrust.com1
http://crl.usertrust.com/UTN-USERFirst-Object.crl05
http://ocsp.usertrust.com0
http://crl3.digicert.com/EVCodeSigningSHA2-g1.crl07
http://crl4.digicert.com/EVCodeSigningSHA2-g1.crl0K
http://ocsp.digicert.com0H
http://cacerts.digicert.com/DigiCertEVCodeSigningCA-SHA2.crt0
http://ocsp.digicert.com0I
http://cacerts.digicert.com/DigiCertHighAssuranceEVRootCA.crt0
http://crl3.digicert.com/DigiCertHighAssuranceEVRootCA.crl0@
http://crl4.digicert.com/DigiCertHighAssuranceEVRootCA.crl0
http://www.digicert.com/ssl-cps-repository.htm0
http://www.sparkol.com0
http://www.usertrust.com1
```

Source: FileAlyzer



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.

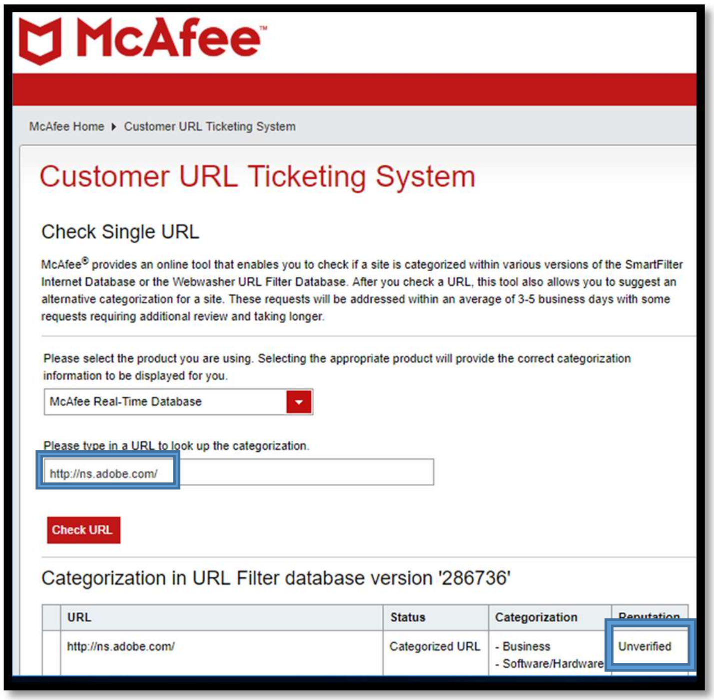
McAfee Real-Time Database

Please type in a URL to look up the categorization.

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

Categorization in URL Filter database version '286736'

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



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

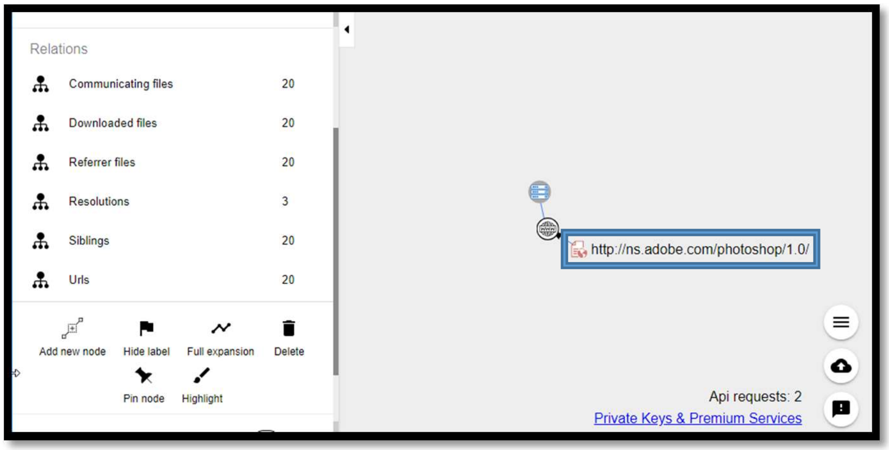
Please type in a URL to look up the categorization.

http://ns.adobe.com/

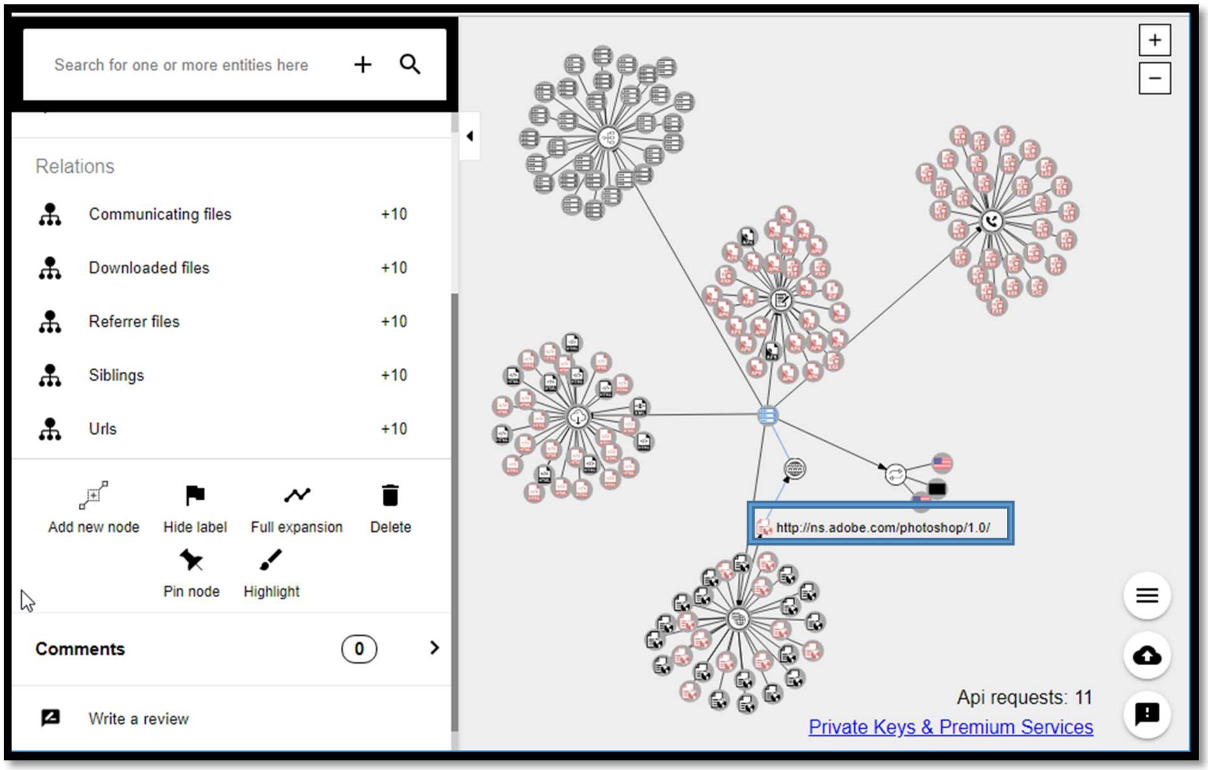
Categorization in URL Filter database version '286736'

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

Source: www.trustedsource.org

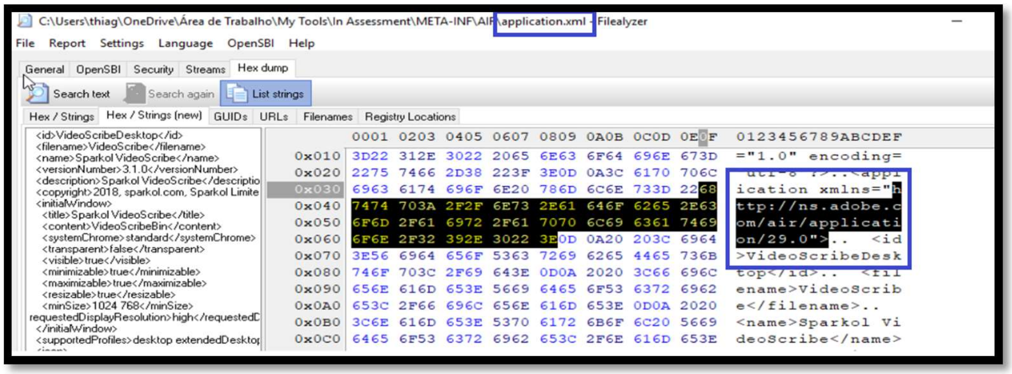


Source: www.virustotal.com



Source: www.virustotal.com

The suspicious websites were identified as part of XML files.



C:\Users\thiag\OneDrive\Área de Trabalho\My Tools\In Assessment\META-INF\AIR\application.xml - Filealyzer

```
<id>VideoScribeDesktop</id>
<filename>VideoScribe</filename>
<name>Sparkol VideoScribe</name>
<versionNumber>3.1.0</versionNumber>
<description>Sparkol VideoScribe</descriptio
<copyright>2018, sparkol.com, Sparkol Limite
<initialWindow>
  <title>Sparkol VideoScribe</title>
  <content>VideoScribeBin</content>
  <systemChrome>standard</systemChrome>
  <transparent>false</transparent>
  <visible>true</visible>
  <minimizable>true</minimizable>
  <maximizable>true</maximizable>
  <resizable>true</resizable>
  <minSize>1024 768</minSize>
requestedDisplayResolution>high</requestedD
</initialWindow>
<supportedProfiles>desktop extendedDesktop
```

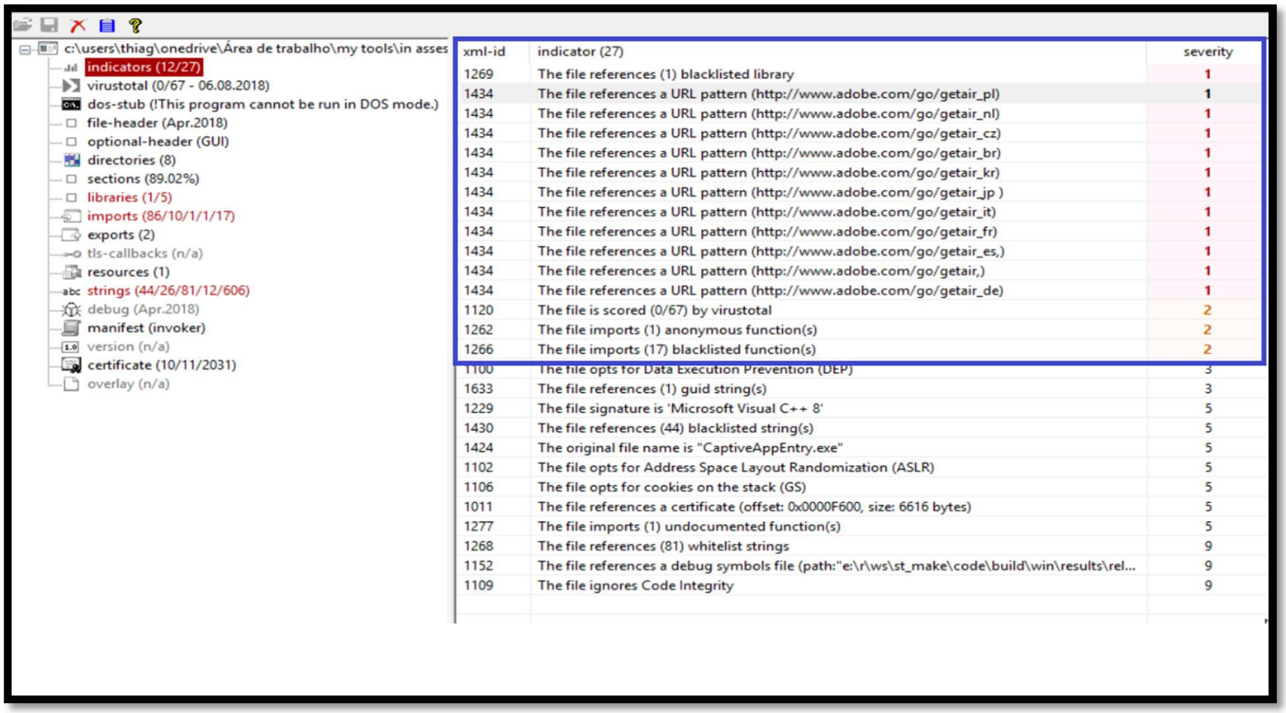
```
       0001 0203 0405 0607 0809 0A0B 0C0D 0E0F  0123456789ABCDEF
0x010  3D22 312E 3022 2065 6E63 6F64 696E 673D  ="1.0" encoding=
0x020  2275 7466 2D38 223F 3E0D 0A3C 6170 706C  "utf-8"?>..<appl
0x030  6963 6174 696F 6E20 786D 6C6E 733D 2268  ication xmlns="h
0x040  7474 703A 2F2F 6E73 2E61 646F 6265 2E63  ttp://ns.adobe.c
0x050  6F6D 2F61 6972 2F61 7070 6C69 6361 7469  om/air/applicati
0x060  6F6E 2F32 392E 3022 3E0D 0A20 203C 6964  on/29.0">..  <id
0x070  3E56 6964 656F 5363 7269 6265 4465 736B  >VideoScribeDesk
0x080  746F 703C 2F69 643E 0D0A 2020 3C66 696C  top</id>..  <fil
0x090  656E 616D 653E 5669 6465 6F53 6372 6962  ename>VideoScrib
0x0A0  653C 2F66 696C 656E 616D 653E 0D0A 2020  e</filename>..
0x0B0  3C6E 616D 653E 5370 6172 6B6F 6C20 5669  <name>Sparkol Vi
0x0C0  6465 6F53 6372 6962 653C 2F6E 616D 653E  deoScribe</name>
```

Source: FileAlyzer

6. Files Review

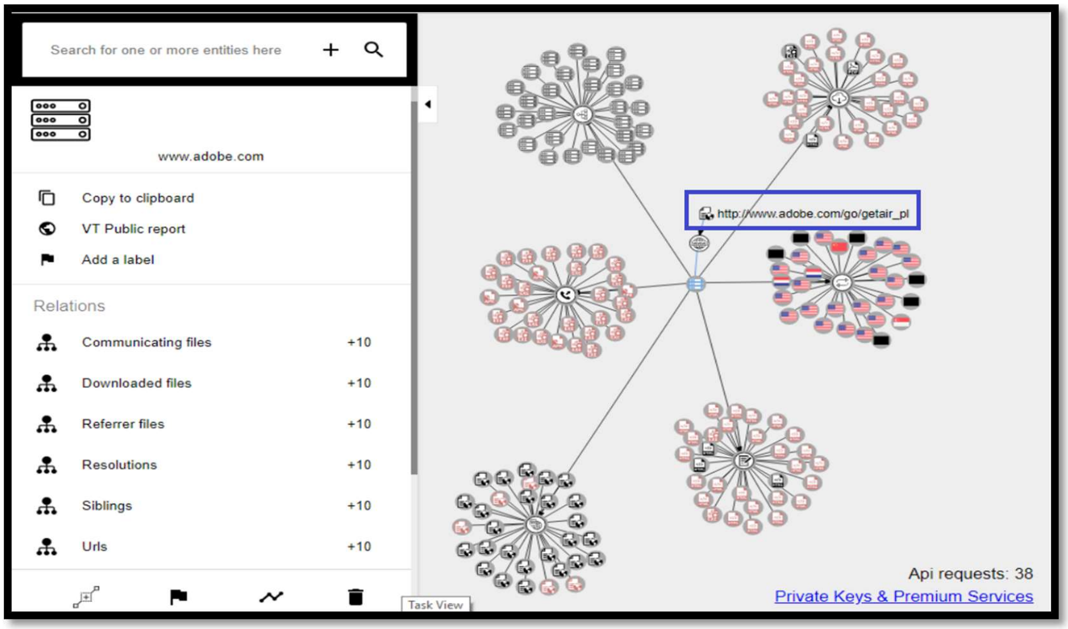
These were suspicious files found in the software by examining the strings using BinText. The first an executable file and list of dynamic-link libraries (dll).

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)



```
c:\users\thiag\onedrive\Área de trabalho\my tools\in asses
  indicators (12/27)
  virustotal (0/67 - 06.08.2018)
  dos-stub (!This program cannot be run in DOS mode.)
  file-header (Apr.2018)
  optional-header (GUI)
  directories (8)
  sections (89.02%)
  libraries (1/5)
  imports (86/10/1/1/17)
  exports (2)
  tls-callbacks (n/a)
  resources (1)
  strings (44/26/81/12/606)
  debug (Apr.2018)
  manifest (invoker)
  version (n/a)
  certificate (10/11/2031)
  overlay (n/a)
```

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:\r\ws\st_make\code\build\win\results\rel...	9
1109	The file ignores Code Integrity	9

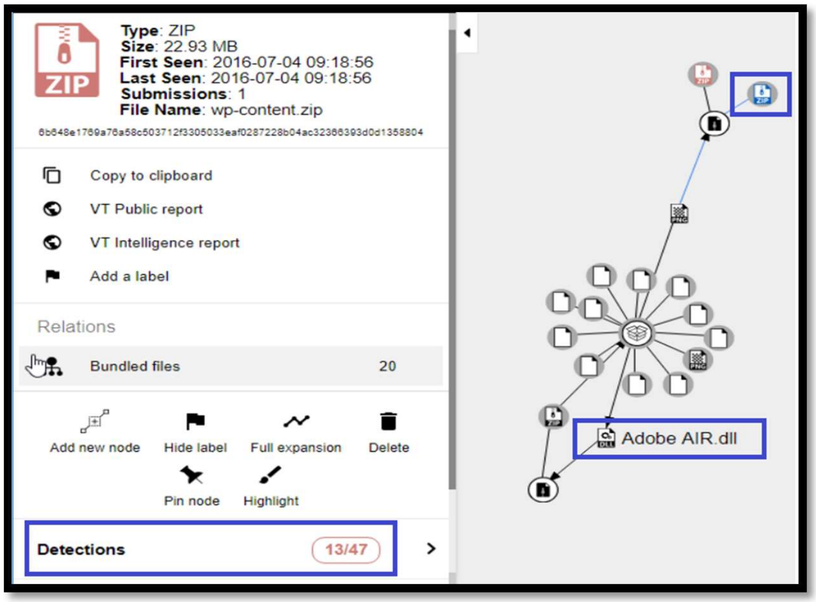


A complete list of DLL files would include:

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:



Type: ZIP
Size: 22.93 MB
First Seen: 2016-07-04 09:18:56
Last Seen: 2016-07-04 09:18:56
Submissions: 1
File Name: wp-content.zip
6b648e1769a76a58c503712f3305033eaf0287228b04ac32366393d0d1358804

Relations
Bundled files 20

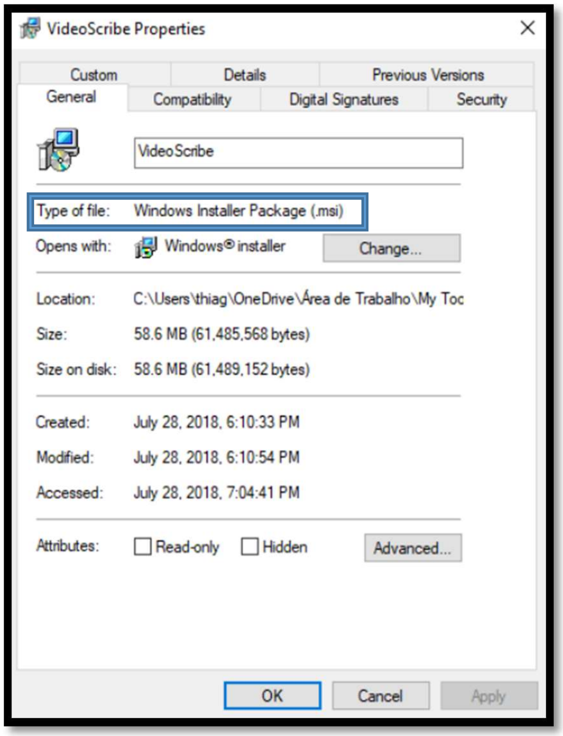
Detections 13/47

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.

The software is specified as a *.doc file and it is still possible to detect the PE executable files, possibly associated with the OLE streams identified.



VideoScribe

Type of file: Windows Installer Package (.msi)

Opens with: Windows® installer

Location: C:\Users\thiag\OneDrive\Área de Trabalho\My Toc

Size: 58.6 MB (61,485,568 bytes)

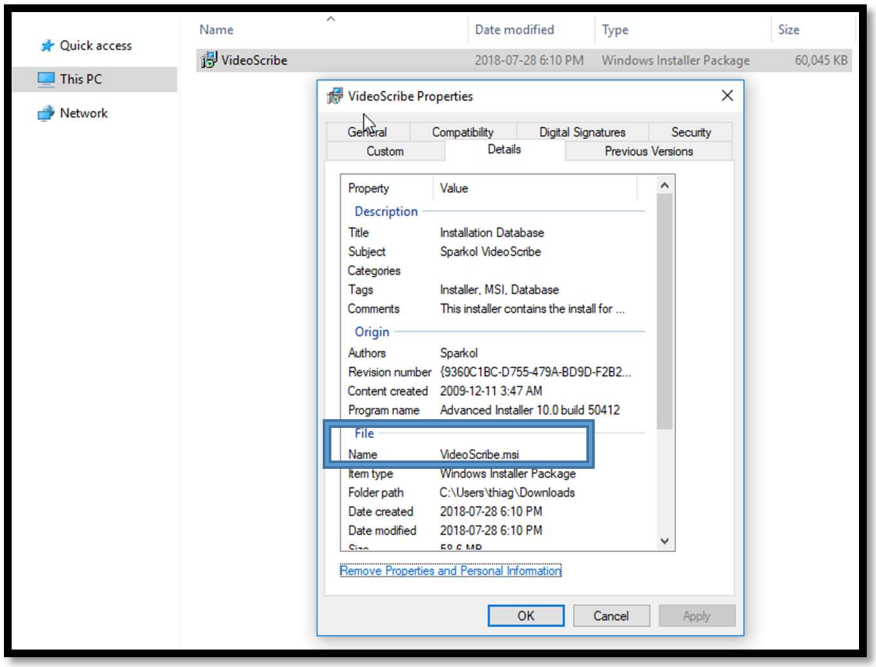
Size on disk: 58.6 MB (61,489,152 bytes)

Created: July 28, 2018, 6:10:33 PM

Modified: July 28, 2018, 6:10:54 PM

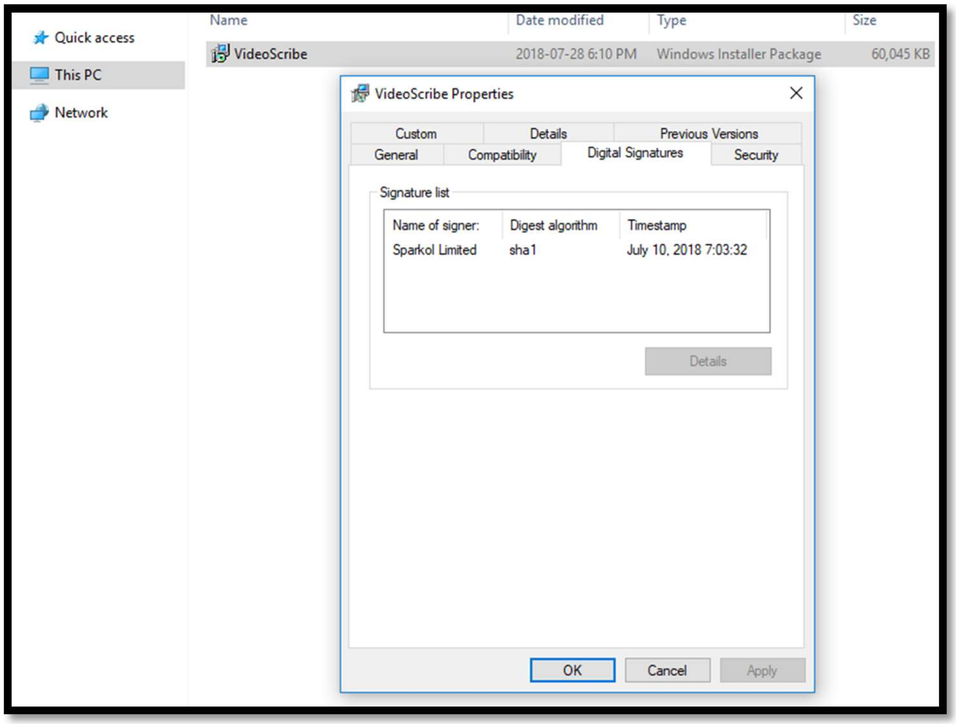
Accessed: July 28, 2018, 7:04:41 PM

Attributes: □ Read-only □ Hidden



Name	Date modified	Type	Size
VideoScribe	2018-07-28 6:10 PM	Windows Installer Package	60,045 KB

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
Size	58.6 MB

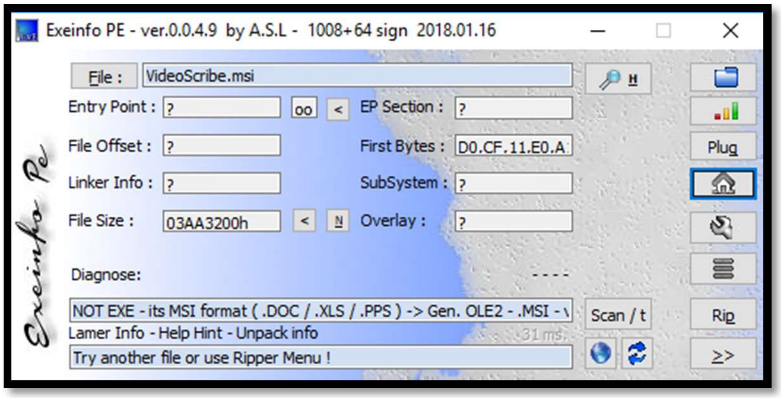


Name	Date modified	Type	Size
VideoScribe	2018-07-28 6:10 PM	Windows Installer Package	60,045 KB

Signature list

Name of signer:	Digest algorithm	Timestamp
Sparkol Limited	sha1	July 10, 2018 7:03:32

Searching for the MSI file was not successful.



Exeinfo PE - ver.0.0.4.9 by A.S.L - 1008+64 sign 2018.01.16

File : VideoScribe.msi

Entry Point : ?

EP Section : ?

File Offset : ?

First Bytes : D0.CF.11.E0.A

Linker Info : ?

SubSystem : ?

File Size : 03AA3200h

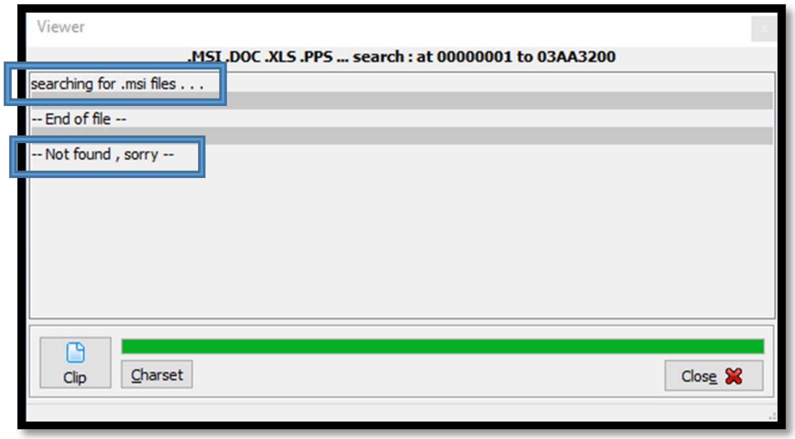
Overlay : ?

Diagnose:

NOT EXE - its MSI format (.DOC / .XLS / .PPS) -> Gen. OLE2 - .MSI - \

Lamer Info - Help Hint - Unpack info

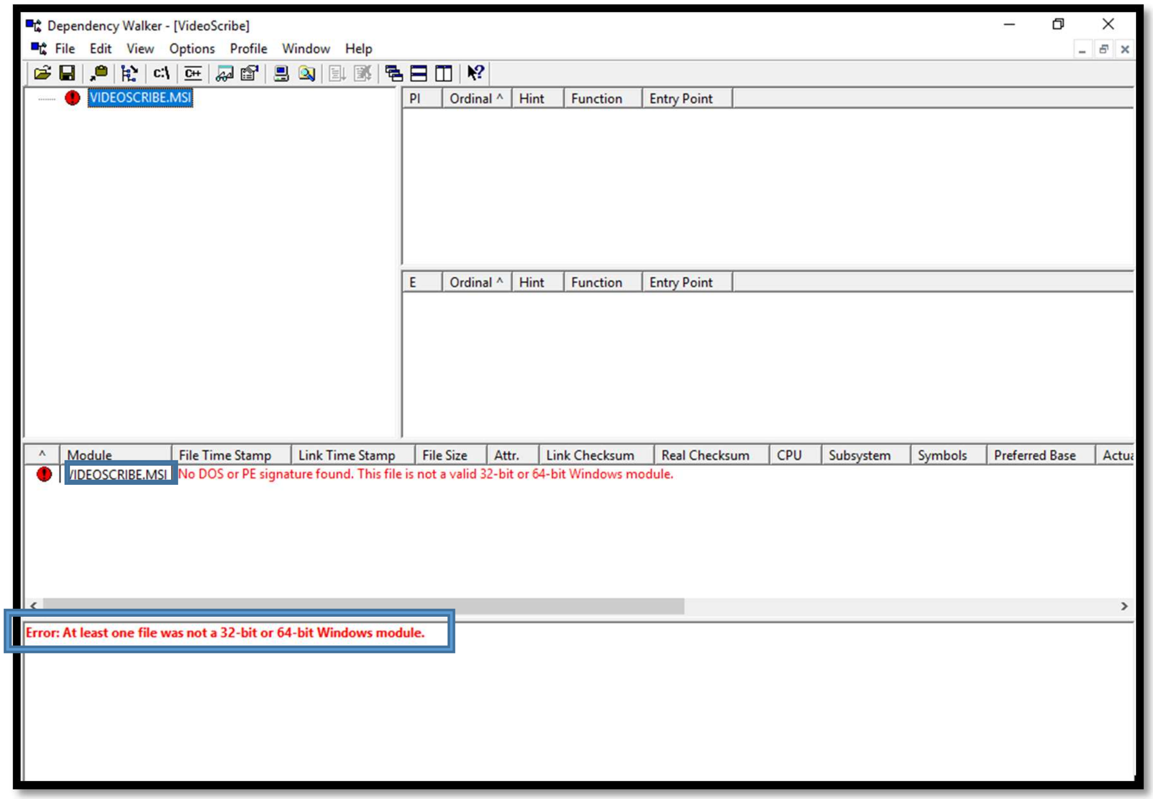
Try another file or use Ripper Menu !



Viewer

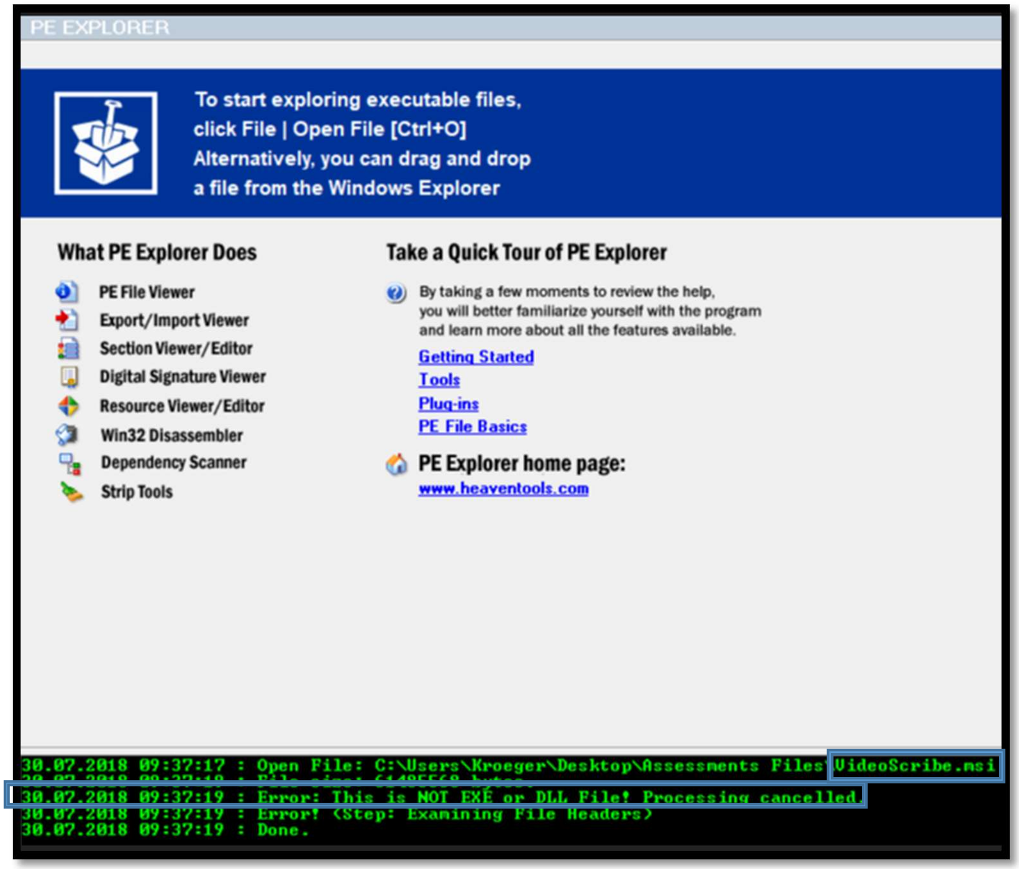
.MSI .DOC .XLS .PPS ... search : at 00000001 to 03AA3200

```
searching for .msi files . . .
-- End of file --
-- Not found , sorry --
```



```
VIDEOSCRIBE.MSI No DOS or PE signature found. This file is not a valid 32-bit or 64-bit Windows module.
```

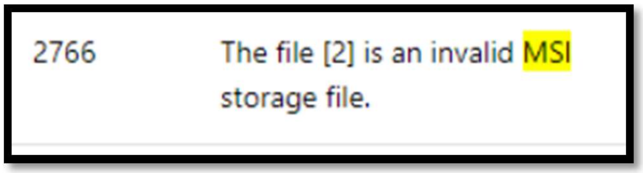
```
Error: At least one file was not a 32-bit or 64-bit Windows module.
```



PE EXPLORER
To start exploring executable files,
click File | Open File [Ctrl+O]
Alternatively, you can drag and drop
a file from the Windows Explorer
What PE Explorer Does
PE File Viewer
Export/Import Viewer
Section Viewer/Editor
Digital Signature Viewer
Resource Viewer/Editor
Win32 Disassembler
Dependency Scanner
Strip Tools
Take a Quick Tour of PE Explorer
By taking a few moments to review the help,
you will better familiarize yourself with the program
and learn more about all the features available.
Getting Started
Tools
Plug-ins
PE File Basics
PE Explorer home page:
www.heaventools.com

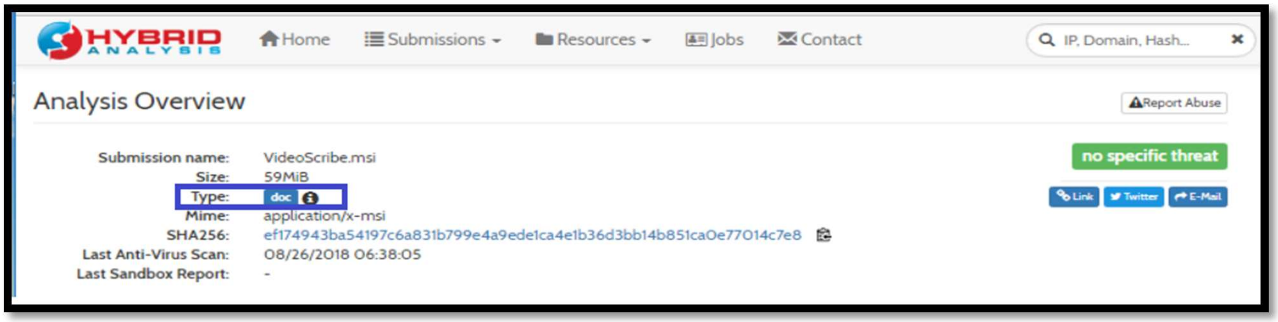
```
30.07.2018 09:37:17 : Open File: C:\Users\Kroeger\Desktop\Assessments Files\VideoScribe.msi
30.07.2018 09:37:18 : File size: 61485568 bytes.
30.07.2018 09:37:19 : Error: This is NOT EXE or DLL File! Processing cancelled.
30.07.2018 09:37:19 : Error! (Step: Examining File Headers)
30.07.2018 09:37:19 : Done.
```

Error Message



```
2766    The file [2] is an invalid MSI
        storage file.
```

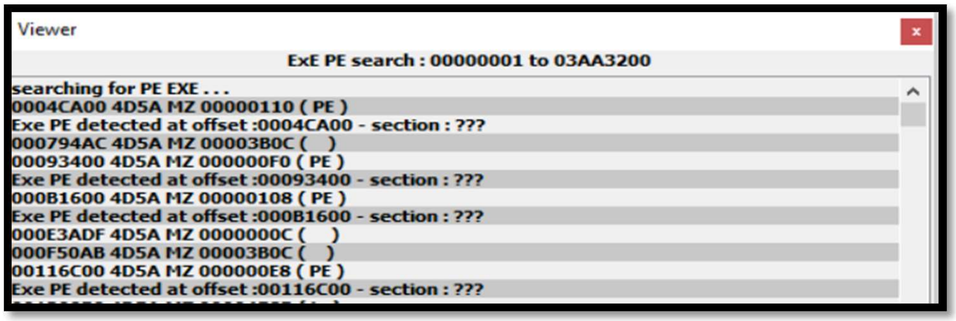
And the software is installed as a Doc file.



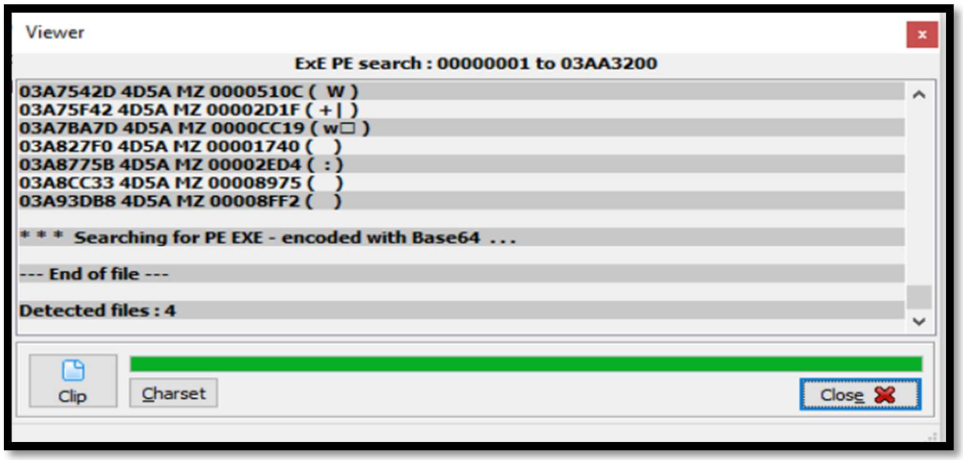
Analysis Overview

Submission name:	VideoScribe.msi
Size:	59MiB
Type:	doc
Mime:	application/x-msi
SHA256:	ef174943ba54197c6a831b799e4a9ede1ca4e1b36d3bb14b851ca0e77014c7e8
Last Anti-Virus Scan:	08/26/2018 06:38:05
Last Sandbox Report:	-

And still it is possible to identify the existence of PE exe files in the software:



```
ExE PE search : 00000001 to 03AA3200
searching for PE EXE . . .
0004CA00 4D5A MZ 00000110 ( PE )
Exe PE detected at offset :0004CA00 - section : ???
000794AC 4D5A MZ 00003B0C (   )
00093400 4D5A MZ 000000F0 ( PE )
Exe PE detected at offset :00093400 - section : ???
000B1600 4D5A MZ 00000108 ( PE )
Exe PE detected at offset :000B1600 - section : ???
000E3ADF 4D5A MZ 0000000C (   )
000F50AB 4D5A MZ 00003B0C (   )
00116C00 4D5A MZ 000000E8 ( PE )
Exe PE detected at offset :00116C00 - section : ???
```



```
ExE PE search : 00000001 to 03AA3200
03A7542D 4D5A MZ 0000510C (  W )
03A75F42 4D5A MZ 00002D1F ( +| )
03A7BA7D 4D5A MZ 0000CC19 ( w□ )
03A827F0 4D5A MZ 00001740 (   )
03A8775B 4D5A MZ 00002ED4 ( : )
03A8CC33 4D5A MZ 00008975 (   )
03A93DB8 4D5A MZ 00008FF2 (   )

* * *  Searching for PE EXE - encoded with Base64  . . .

--- End of file ---

Detected files : 4
```

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