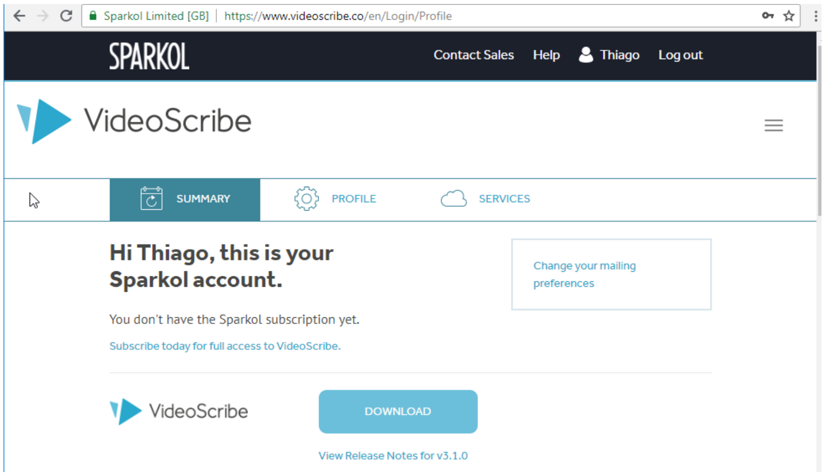
VideoScribe v3.1.0 Assessment

Date: July 30th, 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 a SQL injection attack or remote code execution, for example. Other constructive results show the presence of packed icon files in the *.msi file.

Sumário

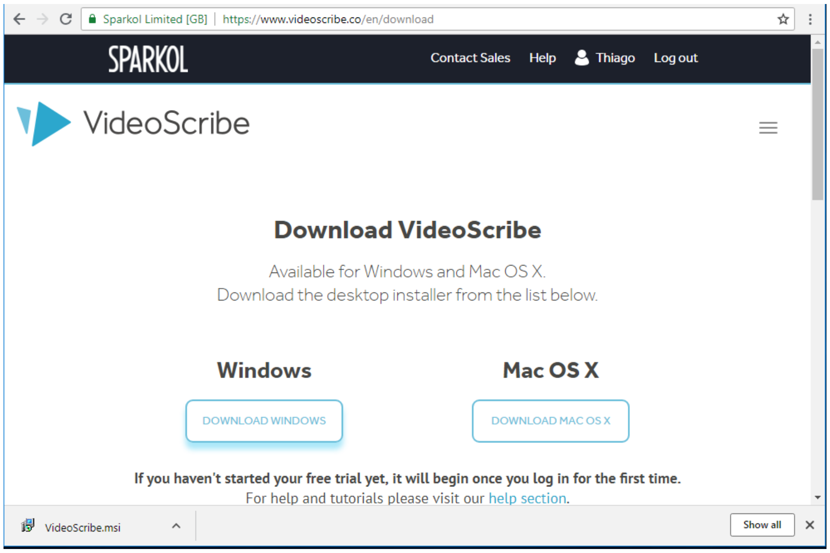
1. File Identification


Sparkol Limited [GB] | https://www.videoscribe.co/en/Login/Profile
SPARKOL
Contact Sales
Help
Thiago
Log out
VideoScribe
SUMMARY
PROFILE
SERVICES
Change your mailing preferences
VideoScribe
DOWNLOAD
View Release Notes for v3.1.0

Hi Thiago, this is your Sparkol account.

You don't have the Sparkol subscription yet.

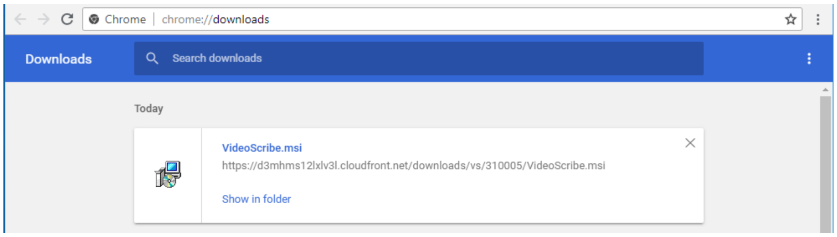
Subscribe today for full access to VideoScribe.



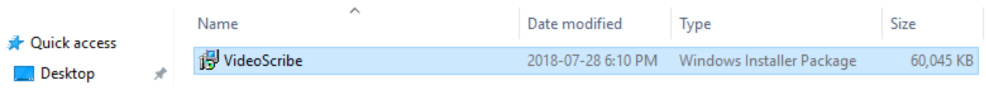
Download VideoScribe

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

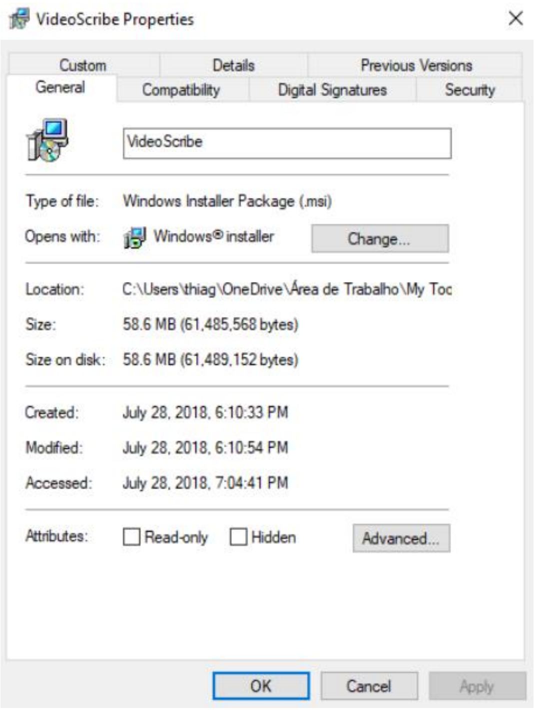
If you haven't started your free trial yet, it will begin once you log in for the first time.
For help and tutorials please visit our help section.



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



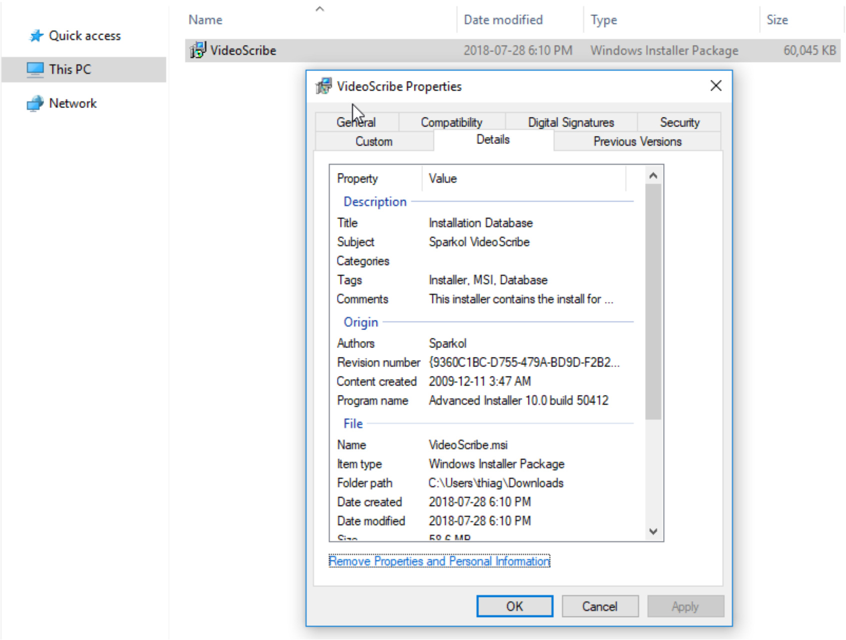
Name	Date modified	Type	Size
VideoScribe	2018-07-28 6:10 PM	Windows Installer Package	60,045 KB



VideoScribe

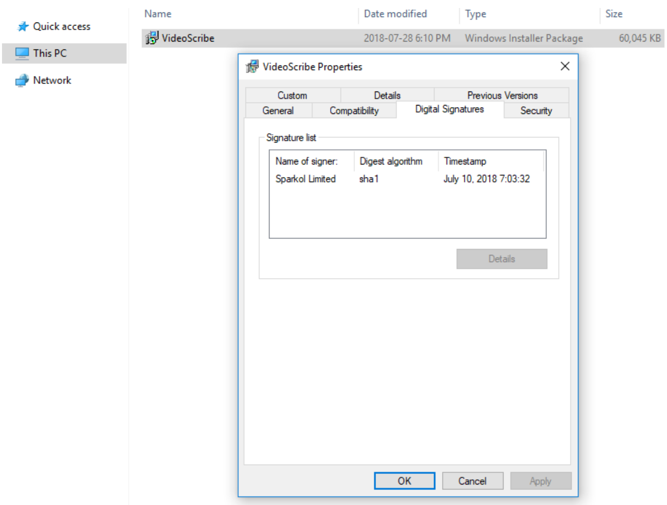
Type of file:	Windows Installer Package (.msi)
Opens with:	Windows® installer
Location:	C:\Users\thiag\OneDrive\Área de Trabalho\My Toc
Size:	58.6 MB (61,485,568 bytes)
Size on disk:	58.6 MB (61,489,152 bytes)
Created:	July 28, 2018, 6:10:33 PM
Modified:	July 28, 2018, 6:10:54 PM
Accessed:	July 28, 2018, 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

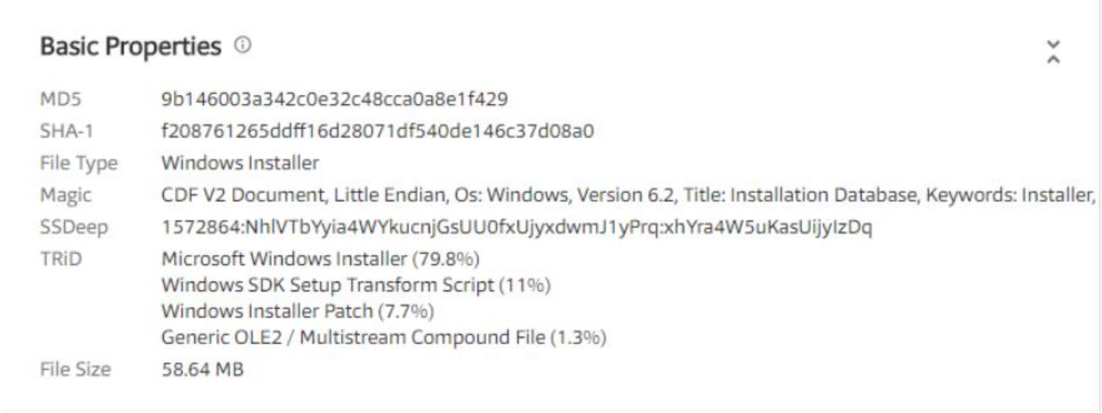
Property	Value
Description	
Title	Installation Database
Subject	Sparkol VideoScribe
Categories	
Tags	Installer, MSI, Database
Comments	This installer contains the install for ...
Origin	
Authors	Sparkol
Revision number	{9360C1BC-D755-479A-BD9D-F2B2...
Content created	2009-12-11 3:47 AM
Program name	Advanced 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

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

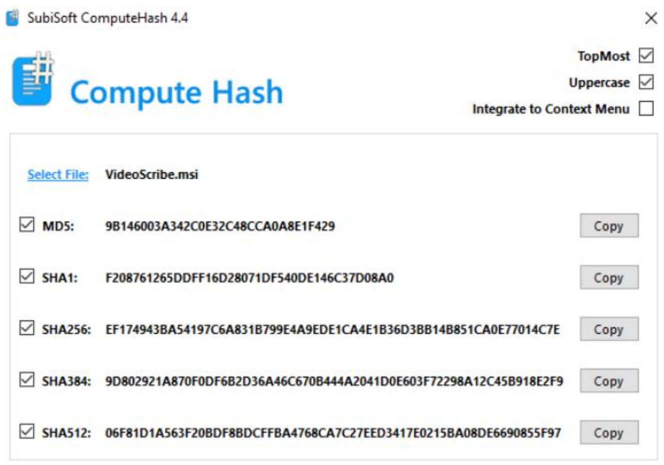
2. File Properties



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:xhYra4W5uKasUijylzDq
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

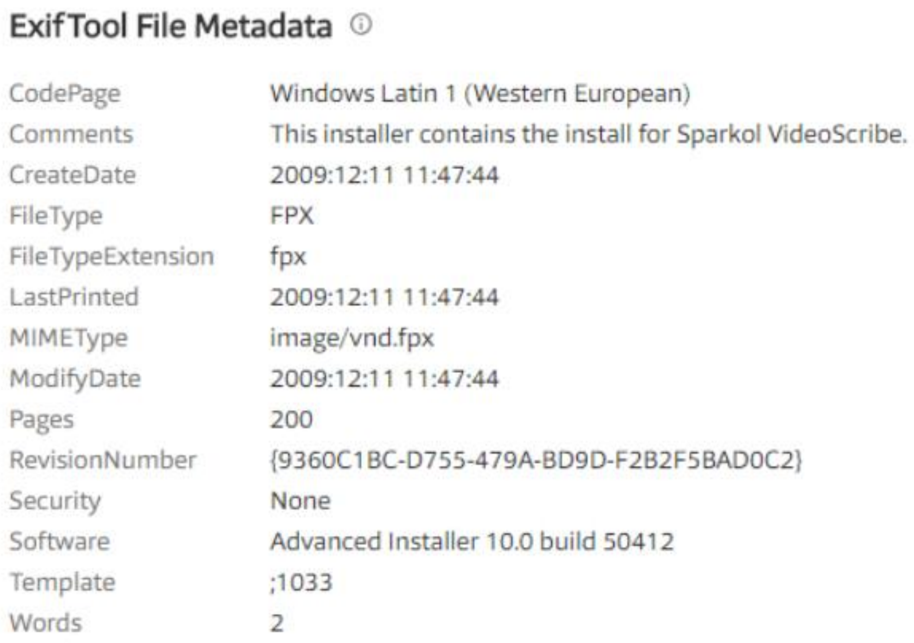
Source: www.virustotal.com



Select File: VideoScribe.msi

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

Source: Compute Hash

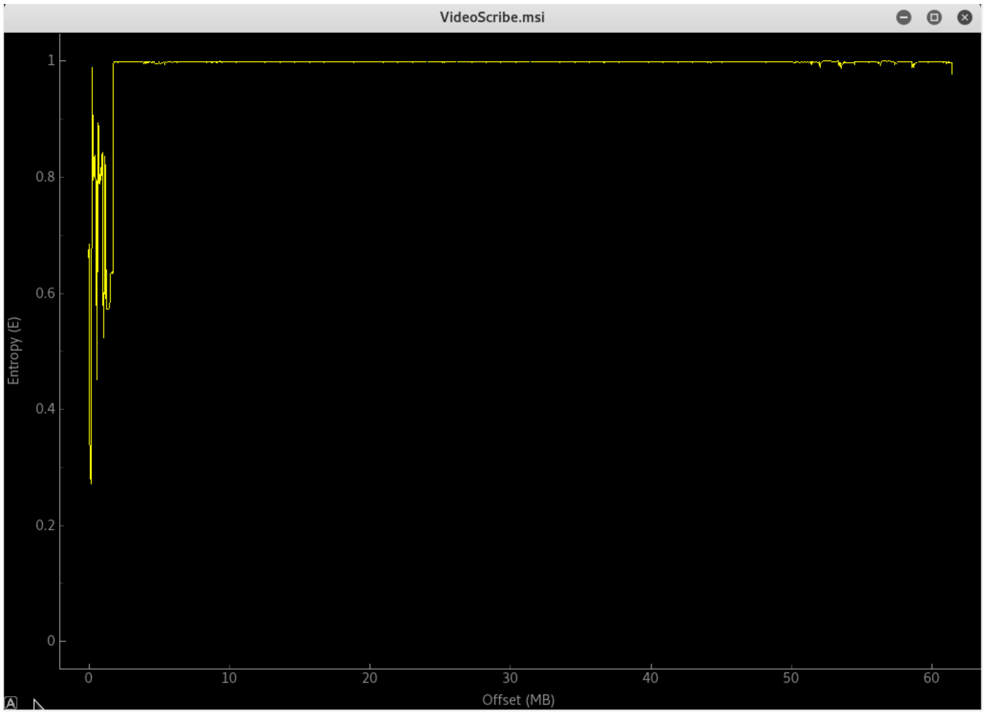


ExifTool File Metadata

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

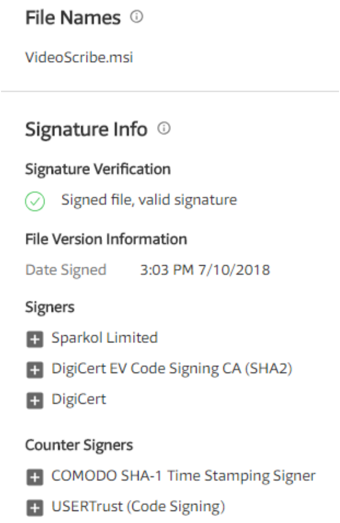
Source: www.virustotal.com

The entropy test below confirms the presence of compressed files.



Source: kali linux.

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

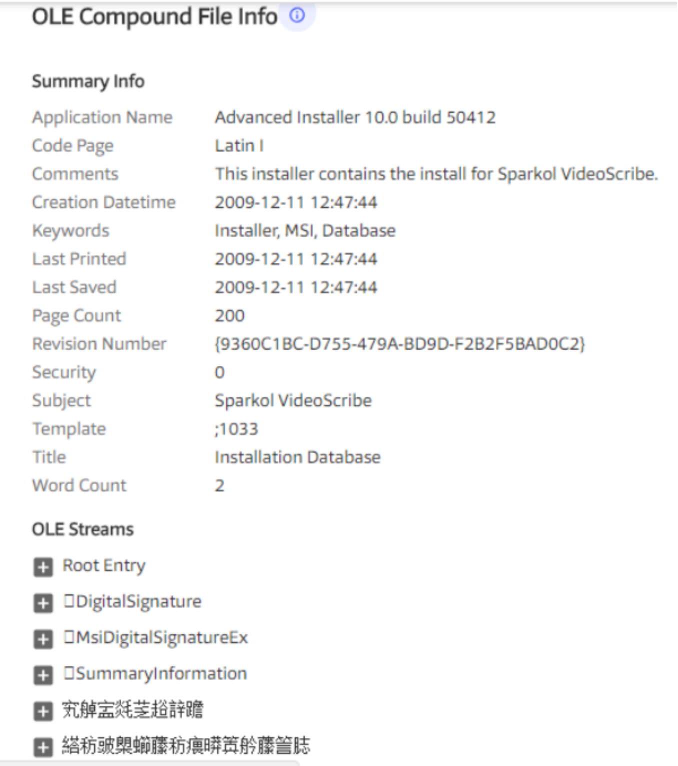
- ⊞ Sparkol Limited
- ⊞ DigiCert EV Code Signing CA (SHA2)
- ⊞ DigiCert

Counter Signers

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

Source: www.virustotal.com

4. Object Linking and Embedding (OLE) streams



OLE Compound File Info ⓘ

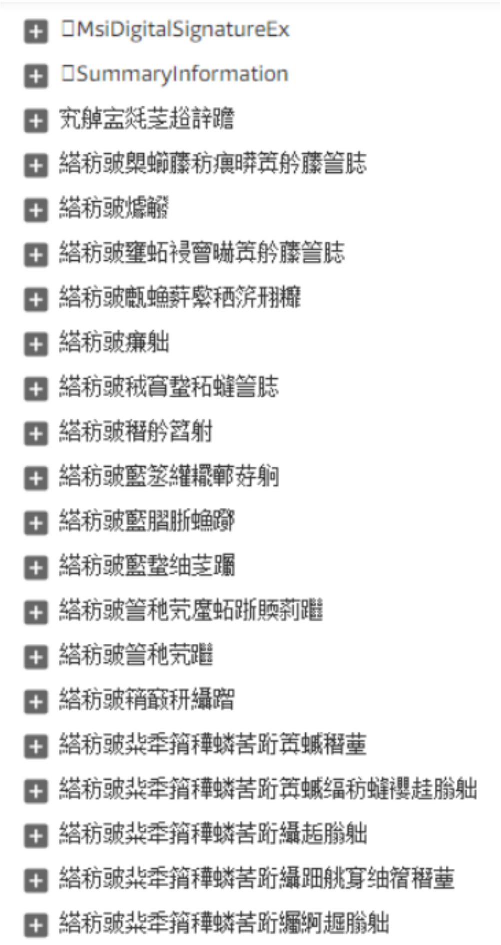
Summary Info

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
- ⊞ 宄艀宖焼茎趦詳矙
- ⊞ 緒秎琥槼蛐藤秎癀畊萁舲藤筥眬

Source: www.virustotal.com



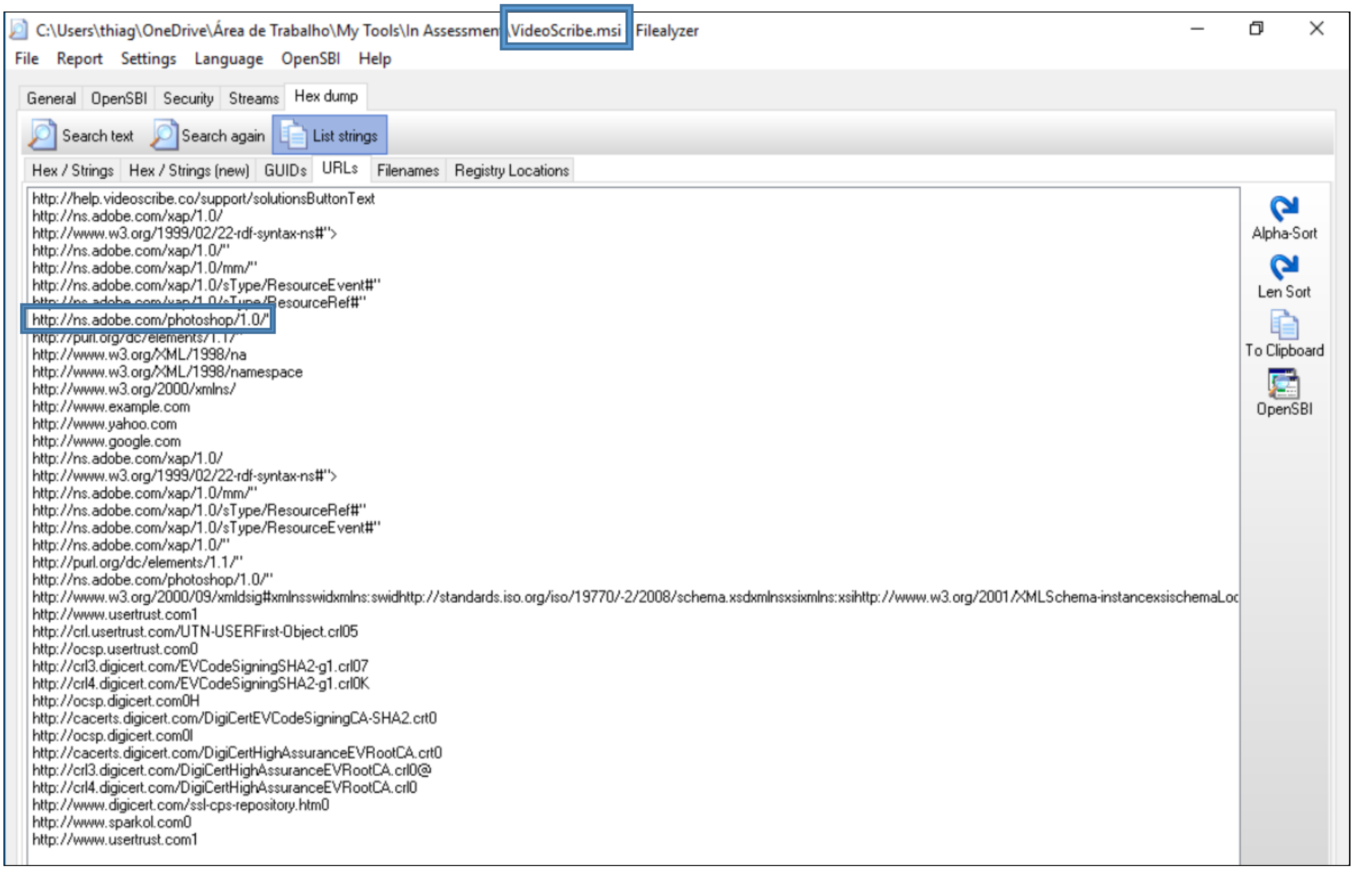
⊞ □MsiDigitalSignatureEx
⊞ □SummaryInformation
⊞ 究艡宖㶶茎趍詳瓣
⊞ 緒秎號槧蝙藤秎瘨暺筭舲藤管䏜
⊞ 緒秎號爈鼶
⊞ 緒秎號䨏蛞袩窨蝴筭舲藤管䏜
⊞ 緒秎號甋蝩薢鮤秞涾䎃欟
⊞ 緒秎號癛舭
⊞ 緒秎號秡萺蝵秥鰚管䏜
⊞ 緒秎號稭舲窰躲
⊞ 緒秎號藍箋繬糶鄬㤉躹
⊞ 緒秎號藍膶腁蝩蹸
⊞ 緒秎號藍蝵䌷茎躅
⊞ 緒秎號管秜茺㲨蛞跡睓䓣䟋
⊞ 緒秎號管秜茺䟋
⊞ 緒秎號䆊萩䎋繡䠞
⊞ 緒秎號㸀秊揥䆾蟒苦䟎筭蜮稭䕂
⊞ 緒秎號㸀秊揥䆾蟒苦䟎筭蜮缁秎蟕䙒趌腳舭
⊞ 緒秎號㸀秊揥䆾蟒苦䟎繡趏腳舭
⊞ 緒秎號㸀秊揥䆾蟒苦䟎繡䟃䑿䝼䌷䆿稭䕂
⊞ 緒秎號㸀秊揥䆾蟒苦䟎䥸䋿趧腳舭

Source: www.virustotal.com

5. Suspicious Websites

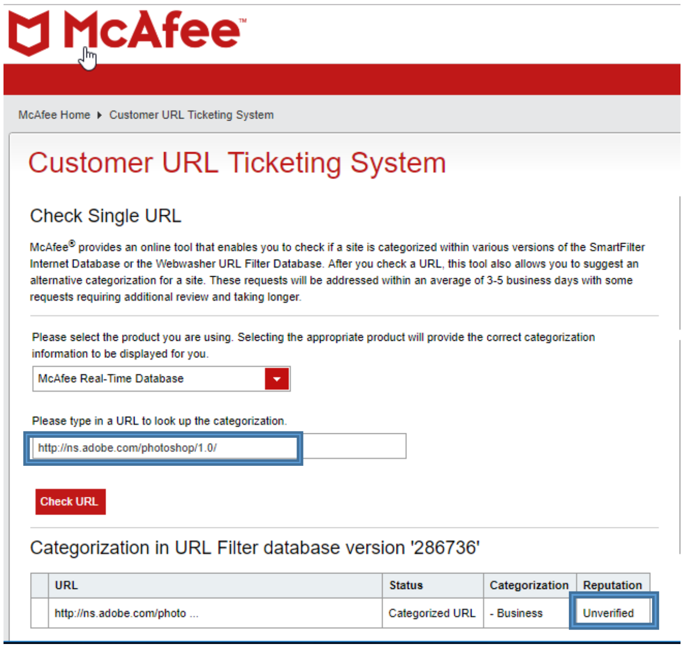
Suspicious websites were identified among acceptable ones such as www.google.com, for example. One website was selected for follow-up and demonstration.

- 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



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.

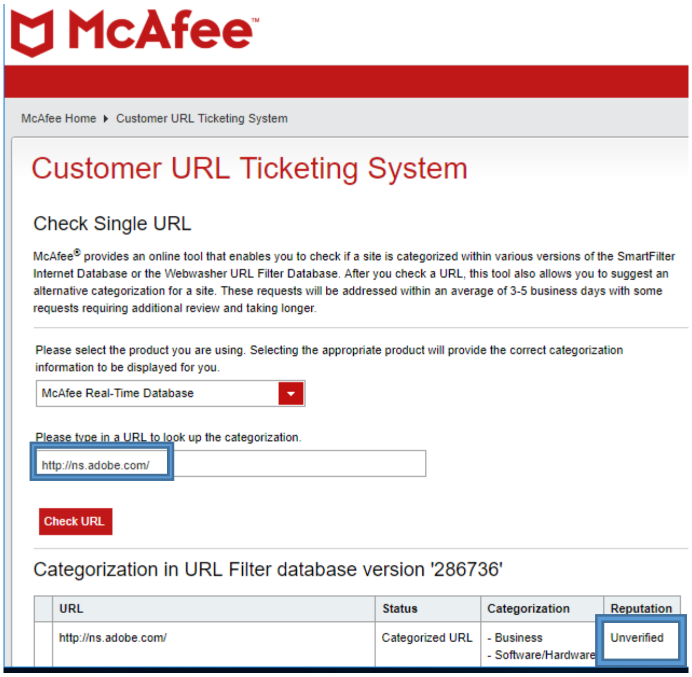
McAfee Real-Time Database

Please type in a URL to look up the categorization.

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

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

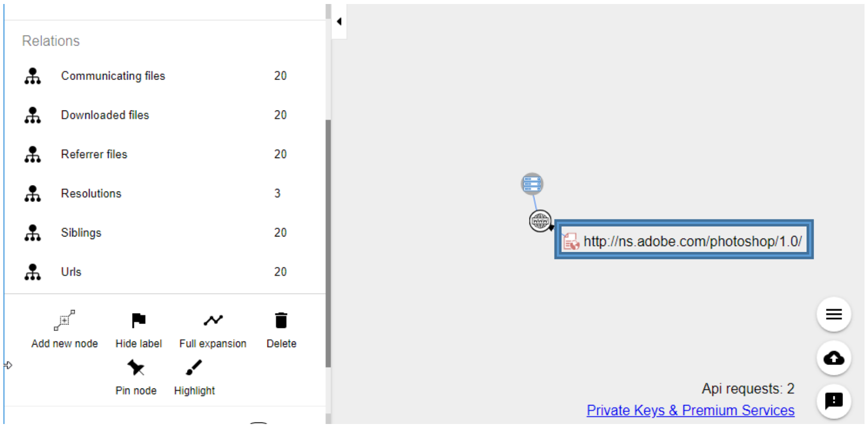
Please type in a URL to look up the categorization.

http://ns.adobe.com/

Categorization in URL Filter database version '286736'

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

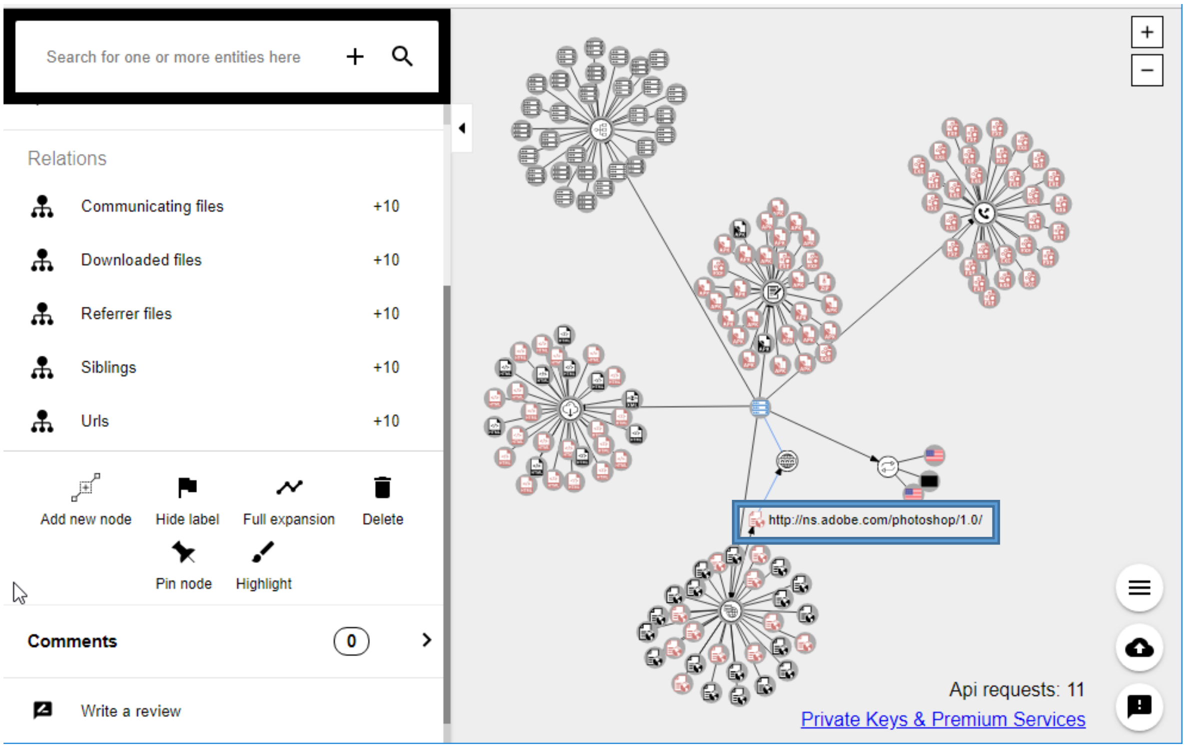
Source: www.trustedsource.org



Relations

Communicating files	20
Downloaded files	20
Referrer files	20
Resolutions	3
Siblings	20
Urls	20

Source: www.virustotal.com



Relations

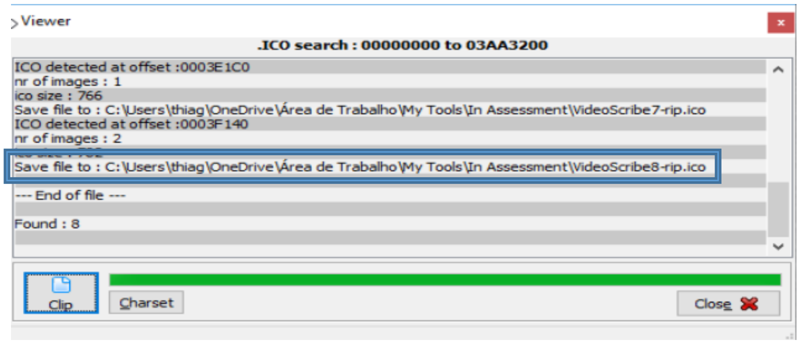
Communicating files	+10
Downloaded files	+10
Referrer files	+10
Siblings	+10
Urls	+10

Search for one or more entities here
Add new node
Hide label
Full expansion
Delete
Pin node
Highlight
Comments
0
Write a review
http://ns.adobe.com/photoshop/1.0/
Api requests: 11
Private Keys & Premium Services

Source: www.virustotal.com

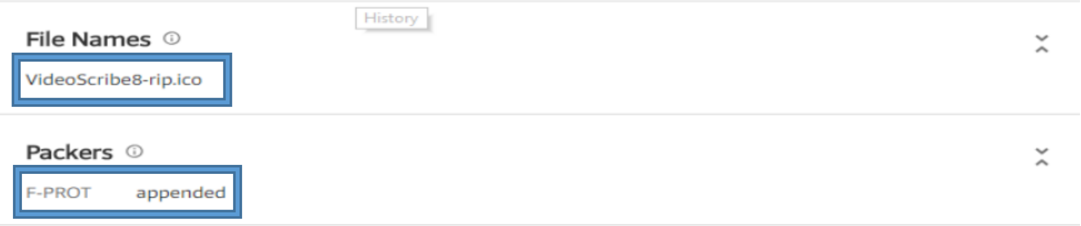
6. Other results

There were 08 hidden icons found. Note that these files were packed. Once unpacked they show a 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).



```
.ICO search : 00000000 to 03AA3200
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\thiag\OneDrive\Área de Trabalho\My Tools\In Assessment\VideoScribe8-rip.ico
--- End of file ---
Found : 8
```

Source: Exeinfo PE



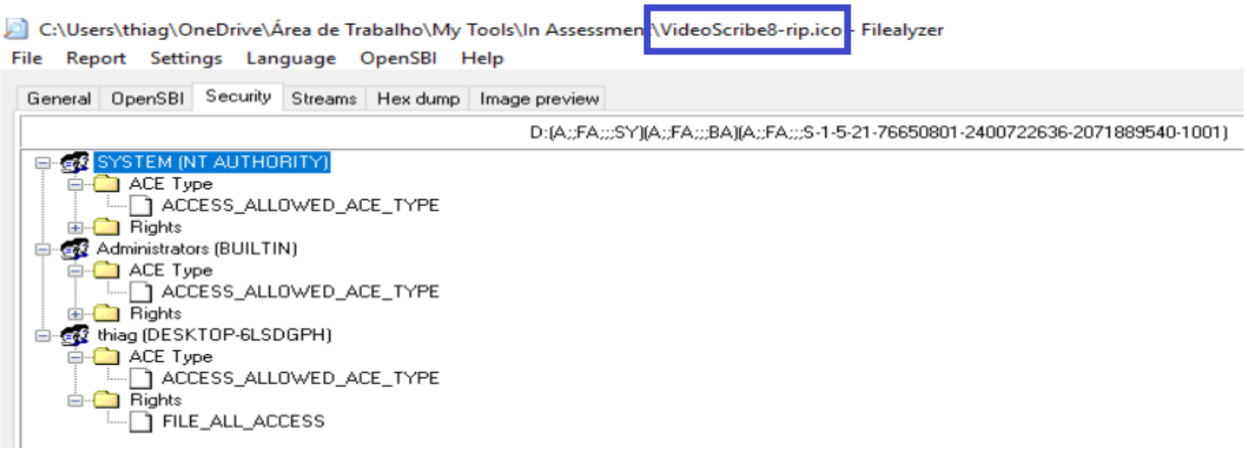
File Names

VideoScribe8-rip.ico

Packers

F-PROT appended

Source: www.virustotal.com


C:\Users\thiag\OneDrive\Área de Trabalho\My Tools\In Assessmen\VideoScribe8-rip.ico - Filealyzer
File
Report
Settings
Language
OpenSBI
Help
General
OpenSBI
Security
Streams
Hex dump
Image preview

```
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