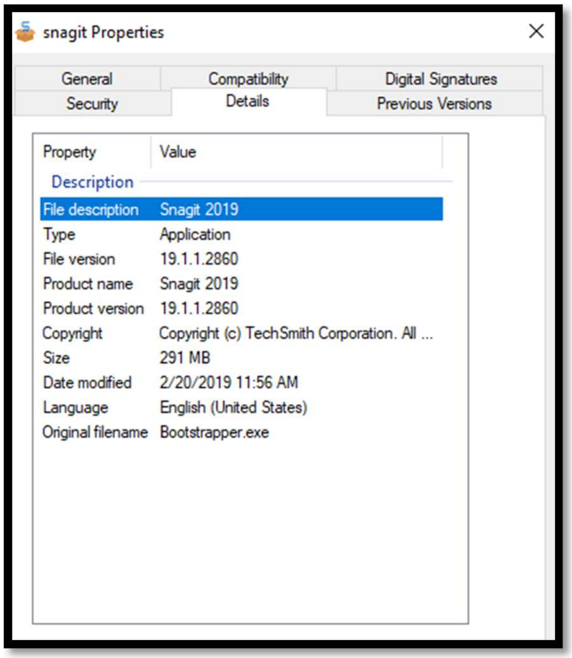
Snagit V.19.1.1.2860

March 2nd, 2019.

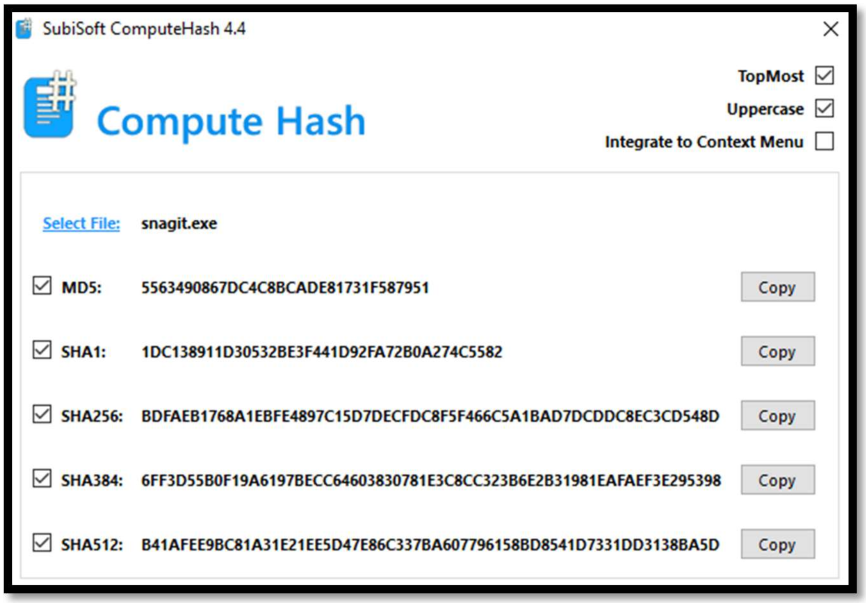
Description: This is a review of Snagit version 19.1.1.2860. The software relies in the use of the Windows installer XML (WiX) toolset which is vulnerable to elevation of privilege by loading dynamic link libraries (CVE-2016-0014). The same file structure from this known vulnerability was found in the software. In addition, it was identified security risks due to compressed parent referred files associated with the dynamic link libraries (*.dll) files in use by the software.

Contents

File identification



Property	Value
Description	
File description	Snagit 2019
Type	Application
File version	19.1.1.2860
Product name	Snagit 2019
Product version	19.1.1.2860
Copyright	Copyright (c) TechSmith Corporation. All ...
Size	291 MB
Date modified	2/20/2019 11:56 AM
Language	English (United States)
Original filename	Bootstrapper.exe



TopMost ☑

Uppercase ☑

Integrate to Context Menu □

Select File: snagit.exe

☑ MD5: 5563490867DC4C8BCADE81731F587951

☑ SHA1: 1DC138911D30532BE3F441D92FA72B0A274C5582

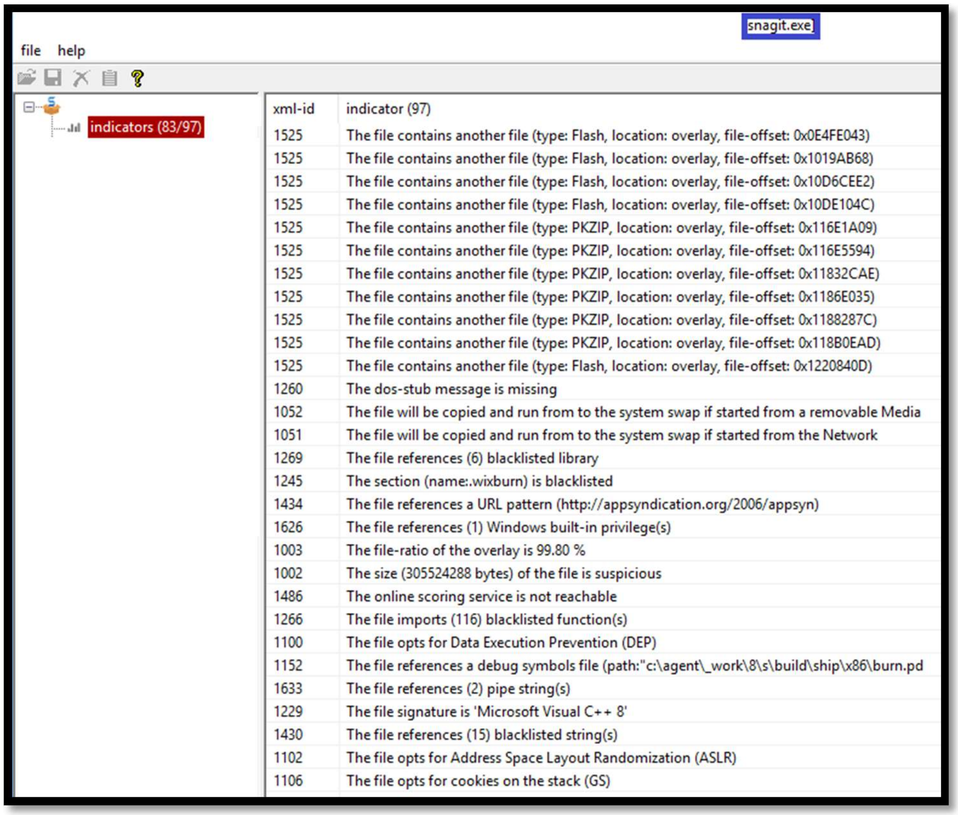
☑ SHA256: BDFAEB1768A1EBFE4897C15D7DECFDC8F5F466C5A1BAD7DCDDC8EC3CD548D

☑ SHA384: 6FF3D55B0F19A6197BECC64603830781E3C8CC323B6E2B31981EAFAEF3E295398

☑ SHA512: B41AFEE9BC81A31E21EE5D47E86C337BA607796158BD8541D7331DD3138BA5D

General Security Assessment

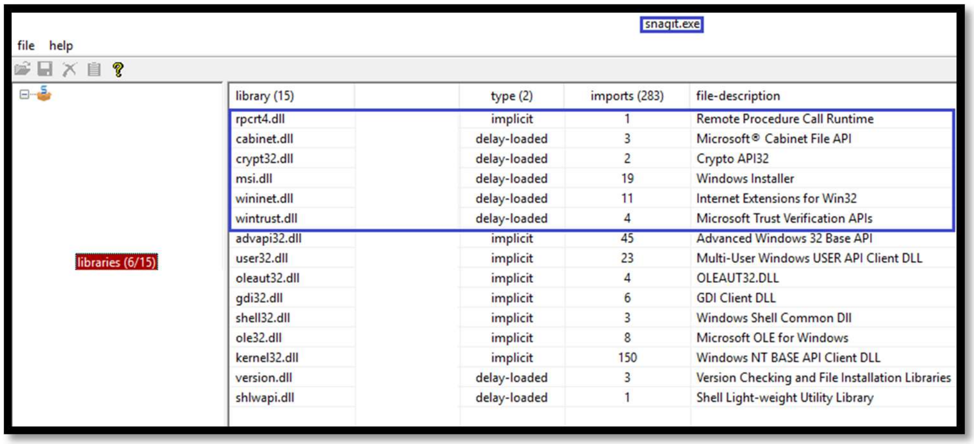
These were some events identified initially while checking security risks. It is possible to see aspects of compression (zip file and file-ratio outlay), use of blacklisted libraries, suspicious file size and the section “wixburn” which is related to the Windows installer XML toolset (WiX[1]).



xml-id	indicator (97)
1525	The file contains another file (type: Flash, location: overlay, file-offset: 0x0E4FE043)
1525	The file contains another file (type: Flash, location: overlay, file-offset: 0x1019AB68)
1525	The file contains another file (type: Flash, location: overlay, file-offset: 0x10D6CEE2)
1525	The file contains another file (type: Flash, location: overlay, file-offset: 0x10DE104C)
1525	The file contains another file (type: PKZIP, location: overlay, file-offset: 0x116E1A09)
1525	The file contains another file (type: PKZIP, location: overlay, file-offset: 0x116E5594)
1525	The file contains another file (type: PKZIP, location: overlay, file-offset: 0x11832CAE)
1525	The file contains another file (type: PKZIP, location: overlay, file-offset: 0x1186E035)
1525	The file contains another file (type: PKZIP, location: overlay, file-offset: 0x1188287C)
1525	The file contains another file (type: PKZIP, location: overlay, file-offset: 0x118B0EAD)
1525	The file contains another file (type: Flash, location: overlay, file-offset: 0x1220840D)
1260	The dos-stub message is missing
1052	The file will be copied and run from to the system swap if started from a removable Media
1051	The file will be copied and run from to the system swap if started from the Network
1269	The file references (6) blacklisted library
1245	The section (name:.wixburn) is blacklisted
1434	The file references a URL pattern (http://appsyndication.org/2006/appsyn)
1626	The file references (1) Windows built-in privilege(s)
1003	The file-ratio of the overlay is 99.80 %
1002	The size (305524288 bytes) of the file is suspicious
1486	The online scoring service is not reachable
1266	The file imports (116) blacklisted function(s)
1100	The file opts for Data Execution Prevention (DEP)
1152	The file references a debug symbols file (path:"c:\agent_work\8\s\build\ship\x86\burn.pd
1633	The file references (2) pipe string(s)
1229	The file signature is 'Microsoft Visual C++ 8'
1430	The file references (15) blacklisted string(s)
1102	The file opts for Address Space Layout Randomization (ASLR)
1106	The file opts for cookies on the stack (GS)

Executable File Review

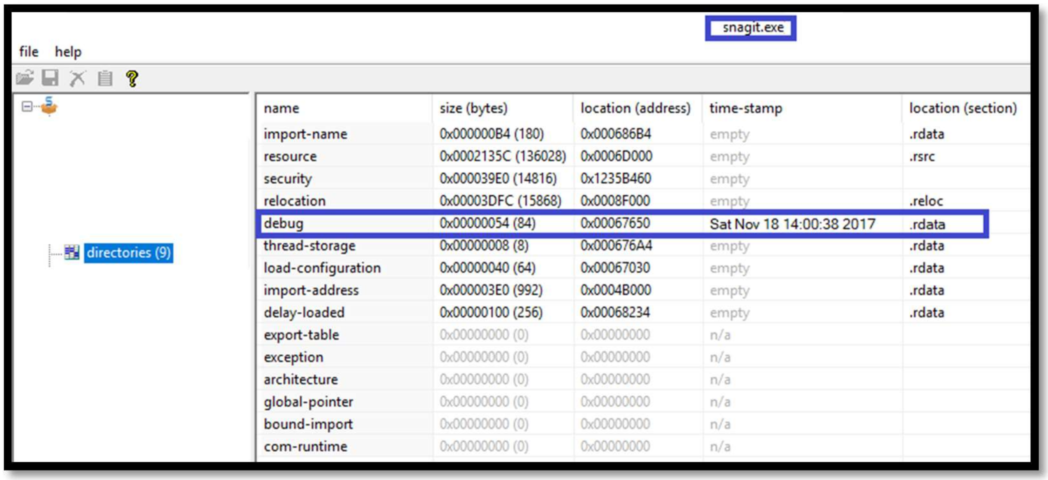
The software has some dynamic link libraries with a delay-loaded[2] behavior.



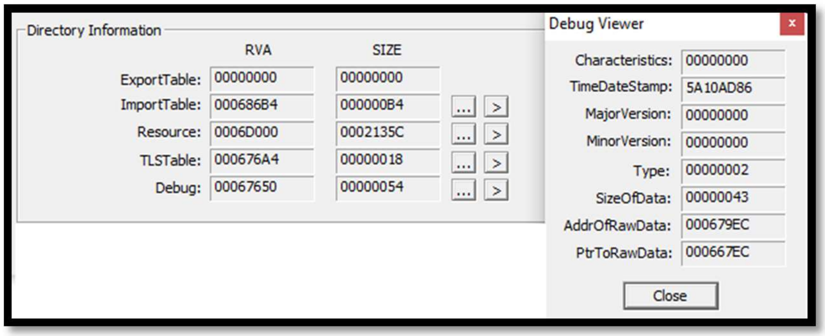
library (15)	type (2)	imports (283)	file-description
rpcrt4.dll	implicit	1	Remote Procedure Call Runtime
cabinet.dll	delay-loaded	3	Microsoft® Cabinet File API
crypt32.dll	delay-loaded	2	Crypto API32
msi.dll	delay-loaded	19	Windows Installer
wininet.dll	delay-loaded	11	Internet Extensions for Win32
wintrust.dll	delay-loaded	4	Microsoft Trust Verification APIs
advapi32.dll	implicit	45	Advanced Windows 32 Base API
user32.dll	implicit	23	Multi-User Windows USER API Client DLL
oleaut32.dll	implicit	4	OLEAUT32.DLL
gdi32.dll	implicit	6	GDI Client DLL
shell32.dll	implicit	3	Windows Shell Common Dll
ole32.dll	implicit	8	Microsoft OLE for Windows
kernel32.dll	implicit	150	Windows NT BASE API Client DLL
version.dll	delay-loaded	3	Version Checking and File Installation Libraries
shlwapi.dll	delay-loaded	1	Shell Light-weight Utility Library

[1] http://wixtoolset.org/
[2] https://docs.microsoft.com/en-us/cpp/build/reference/linker-support-for-delay-loaded-dlls?view=vs-2017

An interesting result found was the capacity of the debug section hide or disable the visibility of the other sections and info, including itself, if we try to access it. Most of the information were encrypted.



name	size (bytes)	location (address)	time-stamp	location (section)
import-name	0x000000B4 (180)	0x000686B4	empty	.rdata
resource	0x0002135C (136028)	0x0006D000	empty	.rsrc
security	0x000039E0 (14816)	0x1235B460	empty	
relocation	0x00003DFC (15868)	0x0008F000	empty	.reloc
debug	0x00000054 (84)	0x00067650	Sat Nov 18 14:00:38 2017	.rdata
thread-storage	0x00000008 (8)	0x000676A4	empty	.rdata
load-configuration	0x00000040 (64)	0x00067030	empty	.rdata
import-address	0x000003E0 (992)	0x0004B000	empty	.rdata
delay-loaded	0x00000100 (256)	0x00068234	empty	.rdata
export-table	0x00000000 (0)	0x00000000	n/a	
exception	0x00000000 (0)	0x00000000	n/a	
architecture	0x00000000 (0)	0x00000000	n/a	
global-pointer	0x00000000 (0)	0x00000000	n/a	
bound-import	0x00000000 (0)	0x00000000	n/a	
com-runtime	0x00000000 (0)	0x00000000	n/a	

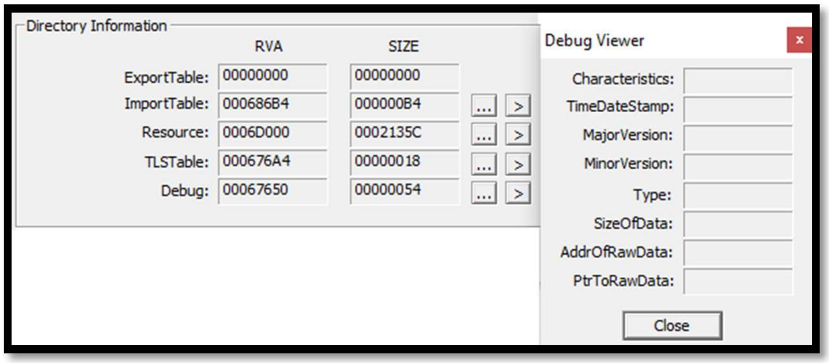


Directory Information

	RVA	SIZE
ExportTable:	00000000	00000000
ImportTable:	000686B4	000000B4
Resource:	0006D000	0002135C
TLSTable:	000676A4	00000018
Debug:	00067650	00000054

Debug Viewer

Characteristics:	00000000
TimeDateStamp:	5A10AD86
MajorVersion:	00000000
MinorVersion:	00000000
Type:	00000002
SizeOfData:	00000043
AddrOfRawData:	000679EC
PtrToRawData:	000667EC



Directory Information

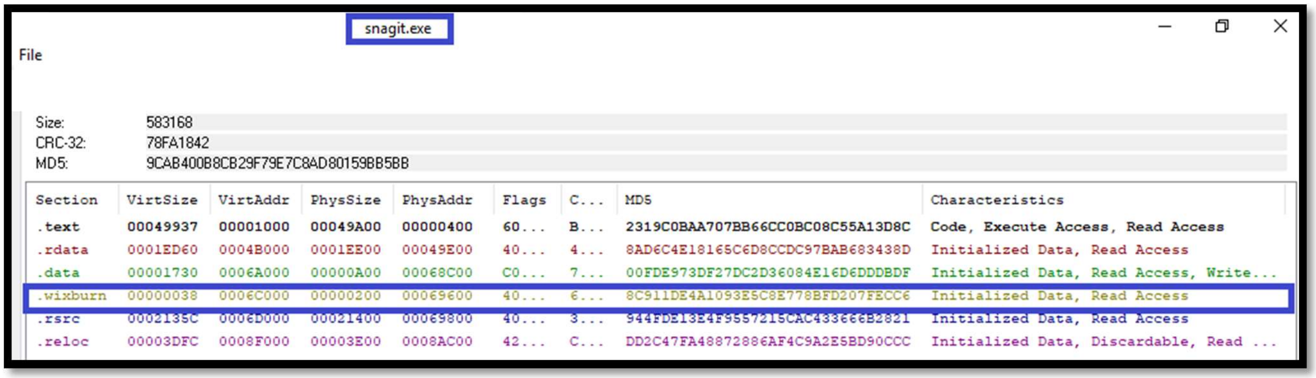
	RVA	SIZE
ExportTable:	00000000	00000000
ImportTable:	000686B4	000000B4
Resource:	0006D000	0002135C
TLSTable:	000676A4	00000018
Debug:	00067650	00000054

Debug Viewer

Characteristics:	
TimeDateStamp:	
MajorVersion:	
MinorVersion:	
Type:	
SizeOfData:	
AddrOfRawData:	
PtrToRawData:	

Software Components

As it was identified earlier, this is the section ".wixburn"



snagit.exe

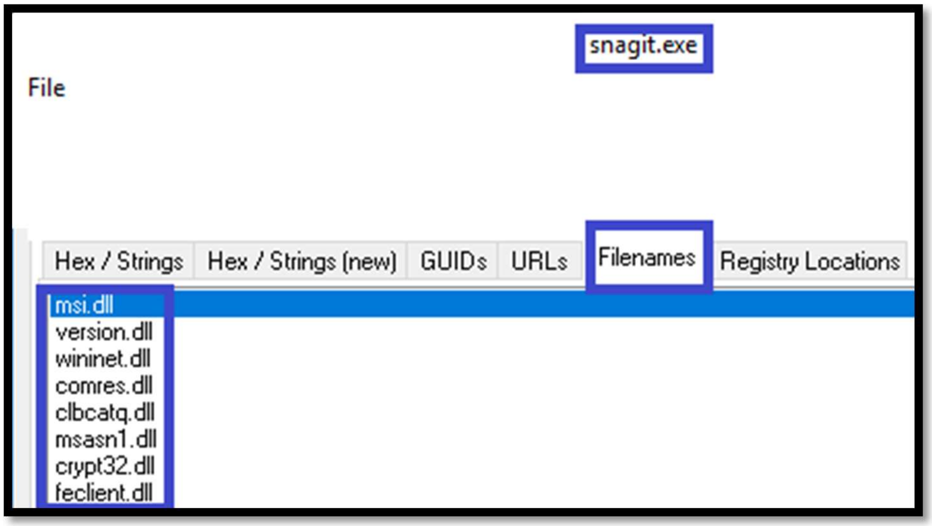
File

Size: 583168
CRC-32: 78FA1842
MD5: 9CAB400B8CB29F79E7C8AD80159BB5BB

Section	VirtSize	VirtAddr	PhysSize	PhysAddr	Flags	C...	MD5	Characteristics
.text	00049937	00001000	00049A00	00000400	60...	B...	2319C0BAA707BB66CC0BC08C55A13D8C	Code, Execute Access, Read Access
.rdata	0001ED60	0004B000	0001EE00	00049E00	40...	4...	8AD6C4E18165C6D8CCDC97BAB683438D	Initialized Data, Read Access
.data	00001730	0006A000	00000A00	00068C00	C0...	7...	00FDE973DF27DC2D36084E16D6DDDBDF	Initialized Data, Read Access, Write...
.wixburn	00000038	0006C000	00000200	00069600	40...	6...	8C911DE4A1093E5C8E778BFD207FECC6	Initialized Data, Read Access
.rsrc	0002135C	0006D000	00021400	00069800	40...	3...	944FDE13E4F9557215CAC433666B2821	Initialized Data, Read Access
.reloc	00003DFC	0008F000	00003E00	0008AC00	42...	C...	DD2C47FA48872886AF4C9A2E5BD90CCC	Initialized Data, Discardable, Read ...

By exploring the files inside the software, it is possible to identify the following dynamic link libraries (*.dll) files that has the same structure found in known vulnerabilities[3] related to the Wix Toolset[4]. In this case, the possibility of gain privilege via a crafted application.

It was possible to identify some common *.dll files:



snagit.exe

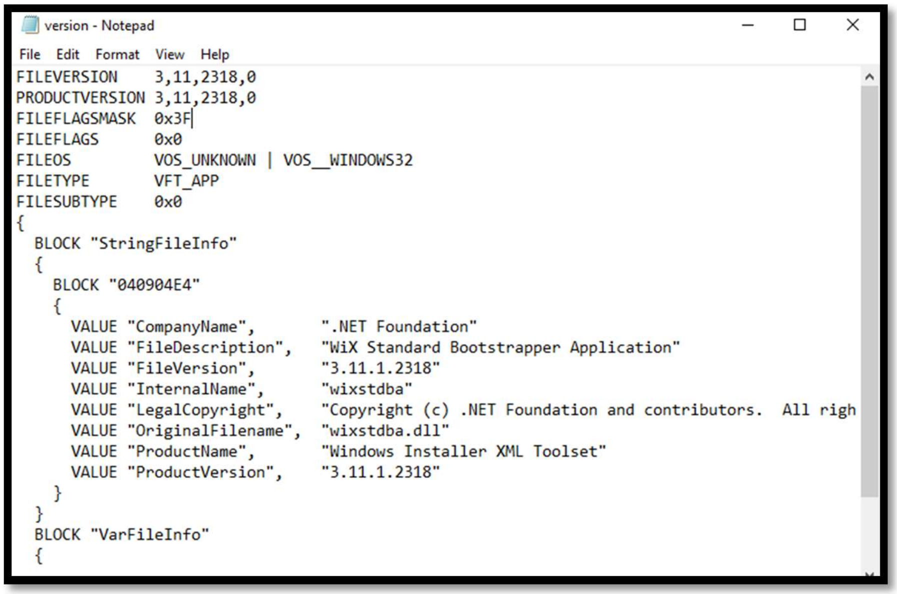
File

msi.dll
version.dll
wininet.dll
comres.dll
clbcatq.dll
msasn1.dll
crypt32.dll
feclient.dll

[3] https://nvd.nist.gov/vuln/detail/CVE-2016-0014

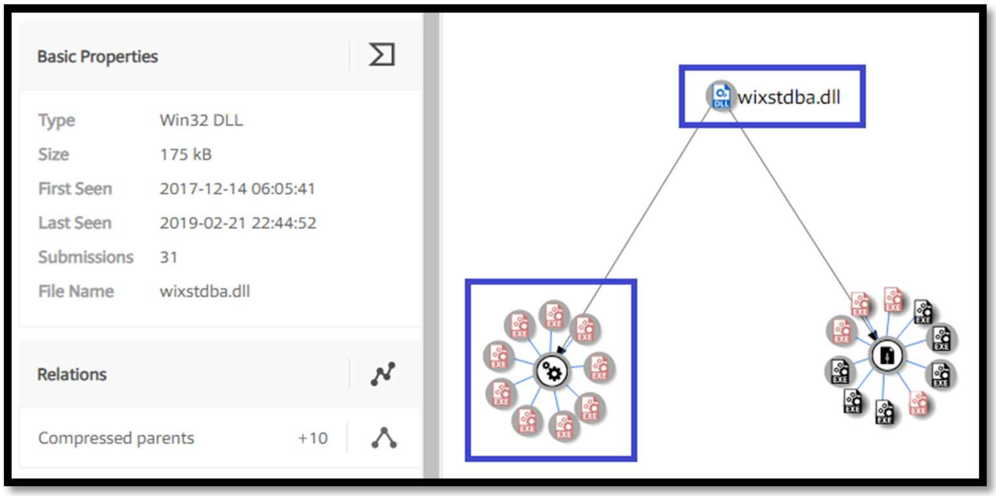
[4] https://www.securityfocus.com/archive/1/537344

Including the wixstdba.dll[5] (175 KB)



```
FILEVERSION    3,11,2318,0
PRODUCTVERSION 3,11,2318,0
FILEFLAGSMASK  0x3F
FILEFLAGS      0x0
FILEOS         VOS_UNKNOWN | VOS__WINDOWS32
FILETYPE       VFT_APP
FILESUBTYPE    0x0
{
  BLOCK "StringFileInfo"
  {
    BLOCK "040904E4"
    {
      VALUE "CompanyName",       ".NET Foundation"
      VALUE "FileDescription",   "WiX Standard Bootstrapper Application"
      VALUE "FileVersion",       "3.11.1.2318"
      VALUE "InternalName",      "wixstdba"
      VALUE "LegalCopyright",    "Copyright (c) .NET Foundation and contributors.  All righ
      VALUE "OriginalFilename",  "wixstdba.dll"
      VALUE "ProductName",       "Windows Installer XML Toolset"
      VALUE "ProductVersion",    "3.11.1.2318"
    }
  }
  BLOCK "VarFileInfo"
  {
```

This file refers to other several suspicious files:


Basic Properties

Type Win32 DLL

Size 175 kB

First Seen 2017-12-14 06:05:41

Last Seen 2019-02-21 22:44:52

Submissions 31

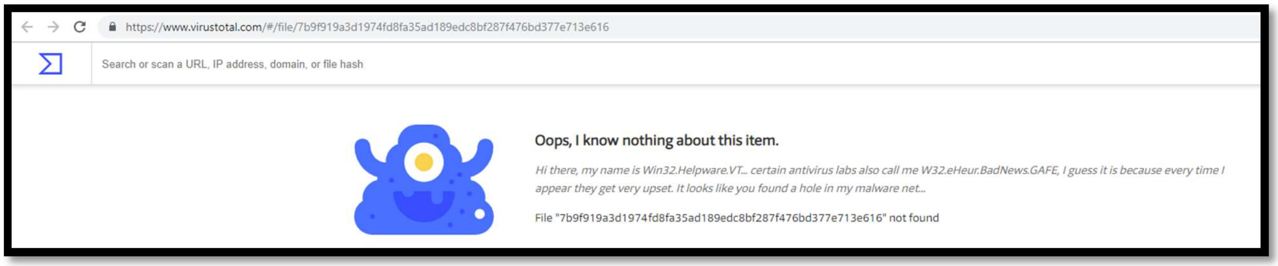
File Name wixstdba.dll

Relations

Compressed parents +10

[5] https://www.virustotal.com/#/file/7b9f919a3d1974fd8fa35ad189edc8bf287f476bd377e713e616b26864a4b0d3/relations

By accident, the analysis found an interesting result searching the hash of the wixstdba.dll file.



https://www.virustotal.com/#/file/7b9f919a3d1974fd8fa35ad189edc8bf287f476bd377e713e616

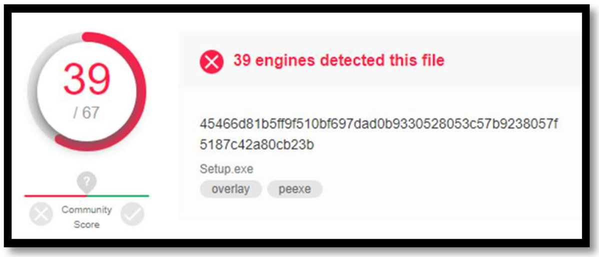
Search or scan a URL, IP address, domain, or file hash

Oops, I know nothing about this item.

Hi there, my name is Win32.Helpware.VT... certain antivirus labs also call me W32.eHeur.BadNews.GAFE, I guess it is because every time I appear they get very upset. It looks like you found a hole in my malware net...

File "7b9f919a3d1974fd8fa35ad189edc8bf287f476bd377e713e616" not found

A few example of compressed parent referred files include the setup.exe[6] and the flash_player_setup.exe[7] below:

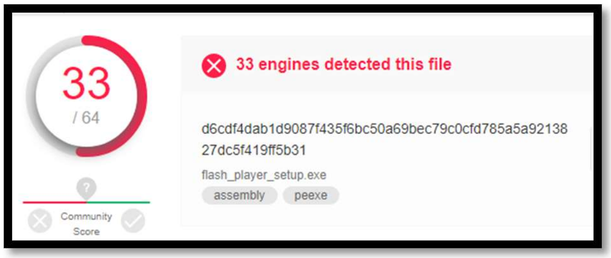


39 / 67

39 engines detected this file

45466d81b5ff9f510bf697dad0b9330528053c57b9238057f5187c42a80cb23b

Setup.exe



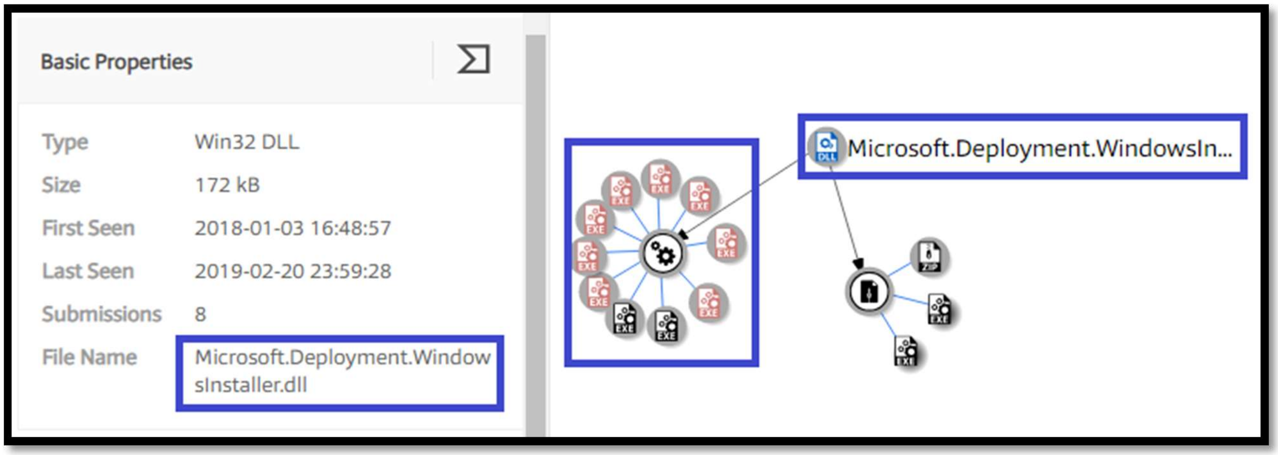
33 / 64

33 engines detected this file

d6cdf4dab1d9087f435f6bc50a69bec79c0cfd785a5a9213827dc5f419ff5b31

flash_player_setup.exe

Other libraries with suspicious behavior could also be found[8]:



Basic Properties

Type	Win32 DLL
Size	172 kB
First Seen	2018-01-03 16:48:57
Last Seen	2019-02-20 23:59:28
Submissions	8
File Name	Microsoft.Deployment.WindowsInstaller.dll

[6] https://www.virustotal.com/gui/file/45466d81b5ff9f510bf697dad0b9330528053c57b9238057f5187c42a80cb23b/detection

[7] https://www.virustotal.com/gui/file/d6cdf4dab1d9087f435f6bc50a69bec79c0cfd785a5a9213827dc5f419ff5b31/detection

[8] https://www.virustotal.com/#/file/cfed1841c76c9731035ebb61d5dc5656babf1beff6ed395e1c6b85bb9c74f85a/relations