

Snagit 19.1.0.2653

March 30th, 2019.

1. Description

The Snagit¹ version 19.1.0.2653 has an extensive use of Object Linking and Embedding (OLE)² streams combined with compression (*.cab) in the Microsoft Installer file (*.msi). This design could allow adversaries to drop unwanted files undetected by antivirus tools. To identify the potential malicious behavior of those OLEs, each of them had to be reviewed in order to identify the unwanted components. By extracting these OLEs, it was possible to identify the record used to drop other files searching by its hash. The final result³ shows the possible negative impact over Microsoft components such as the msixec⁴.exe, Internet Explorer and the Snagit printer installers (SnagitPI⁵ and SnagitPI64⁶).

The software also could weaken security settings by misusing privileges⁷ such as (SeBackupPrivilege, SeChangeNotifyPrivilege, SeRestorePrivilege, SeShutdownPrivilege and SeDebugPrivilege).

2. File identification

Description	
Title	Installation Database
Subject	Snagit 19.1.0.2653
Categories	
Tags	Snagit, Screen capture
Comments	This installer database contains the l...
Origin	
Authors	TechSmith Corporation
Revision number	{B1DD4BA4-DB07-4EE8-9DFB-23D...
Content created	12/4/2018 6:58 AM
Program name	Windows Installer XML Toolset (3.1...

¹<https://www.virustotal.com/gui/file/3ac3c568a515d375cafe33dd712061ccb1814839dcf7e0070c3ea56fab969cb2/detection>

² https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-oleds/2677fcf2-ad48-4386-ba8f-b1b7baf4c02f

³ <https://any.run/report/21eae0859c24faadbfd93be6b809b0c465f7a55f5e8aaa54fb274b9fa1410318/72a13352-5c47-44b9-b063-4f63ca4800bf#files>

⁴ <https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/msiexec>

⁵ <https://www.virustotal.com/gui/file/7c2ff6cb7d859e89fe6faa3cd834a523913a0f1be16f51e0b61f0f6a4a39ab88/relations>

⁶ <https://www.virustotal.com/gui/file/cf6f6bb904bc8897e7de57337f0d1389b4f5f0518574f7eb11c3f94ca3f9f31c/relations>

⁷ <https://docs.microsoft.com/en-us/windows-hardware/drivers/ifs/privileges>

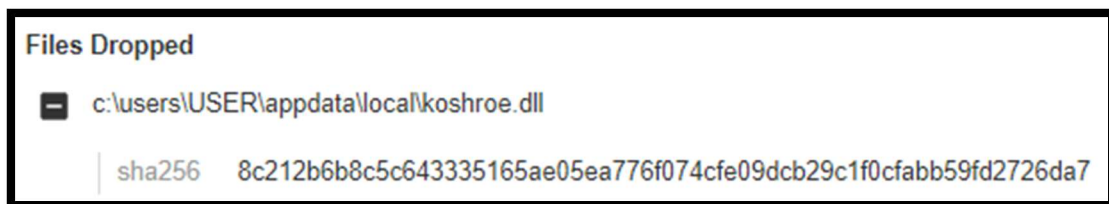
SAH256: 3AC3C568A515D375EAFE33DD712061CCB1814839DCF7E0070E3EA56FAB969CB2

- + Root Entry
- + □DigitalSignature
- + □MsiDigitalSignatureEx
- + □SummaryInformation
- + 襍盞託腰打嗽
- + 究舛齷舂縹櫓譎苦氘苙趁許瞻
- + 究舛齷舂縹氣苙趁許瞻
- + 綰舂皺腎腦駝蜃瞻
- + 綰舂皺腎腦莖替跽
- + 綰舂皺腎璫苦躡
- + 綰舂皺腎暇
- + 綰舂皺檀脾瓠蚱茀史跽
- + 綰舂皺朶籊舂
- + 綰舂皺朶苙躡
- + 綰舂皺璽璽膏
- + 綰舂皺燐驪
- + 綰舂皺齷紀箴瘵箋蟬蚱跽
- + 綰舂皺齷舂縹脚跽
- + 綰舂皺齷笨戔舂篙
- + 綰舂皺症菴膏胴
- + 綰舂皺瘳舂
- + 綰舂皺胥詢敵
- + 綰舂皺胥詢敵禮挈曄搗蕤枋痾愀忸越曇懣斯裂拔穀揆崕踟

The Extraction of the OLEs (e.g. 294752649 and 243619) allows to identify that several of them had embedded the following file with the hash value (d41d8cd98f00b204e9800998ecf8427e⁸):

```
root@snagit_19_1_0.msi
String 1: L  
M  
N  
O  
P  
Q  
R  
S  
T  
U  
V  
W  
X  
Y  
Z  
[  
\  
]  
^  
~  
~~~~~  
String 2:  
String 3:  
Size embedded file: 0  
MD5 embedded file: d41d8cd98f00b204e9800998ecf8427e  
MAJIC:  
Header:
```

The hash above is associated with several malicious execution parents and PE resources parents (Win32) and could drop⁹ malicious files.



⁸<https://www.virustotal.com/gui/file/e3b0c44298fc1c149afb4c8996fb92427ae41e4649b934ca495991b7852b855/relations>

<https://www.virustotal.com/gui/file/8c212b6b8c5c643335165ae05ea776f074cfe09dcb29c1f0cfabb59fd2726da7/details>

In the analysis was also found a potentially unwanted file with the following hash (OLE 107214):

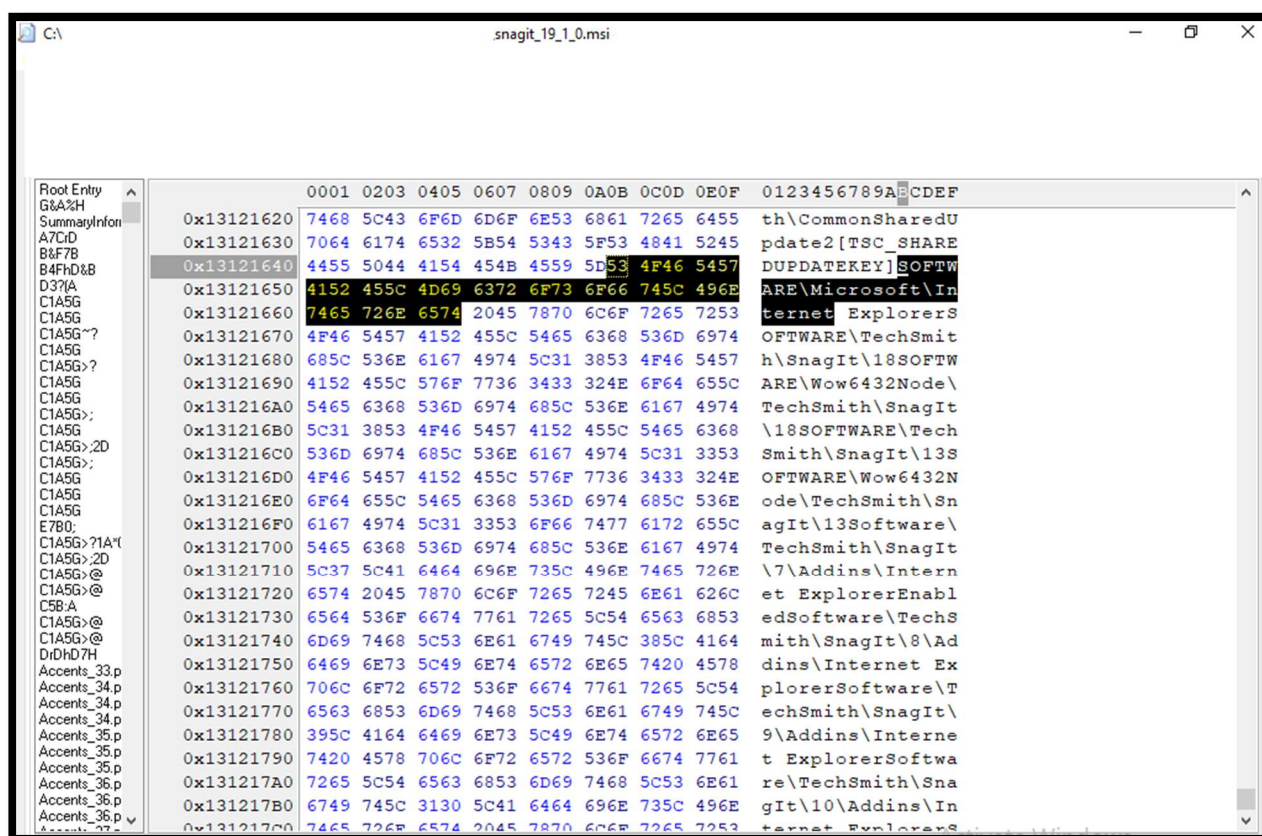
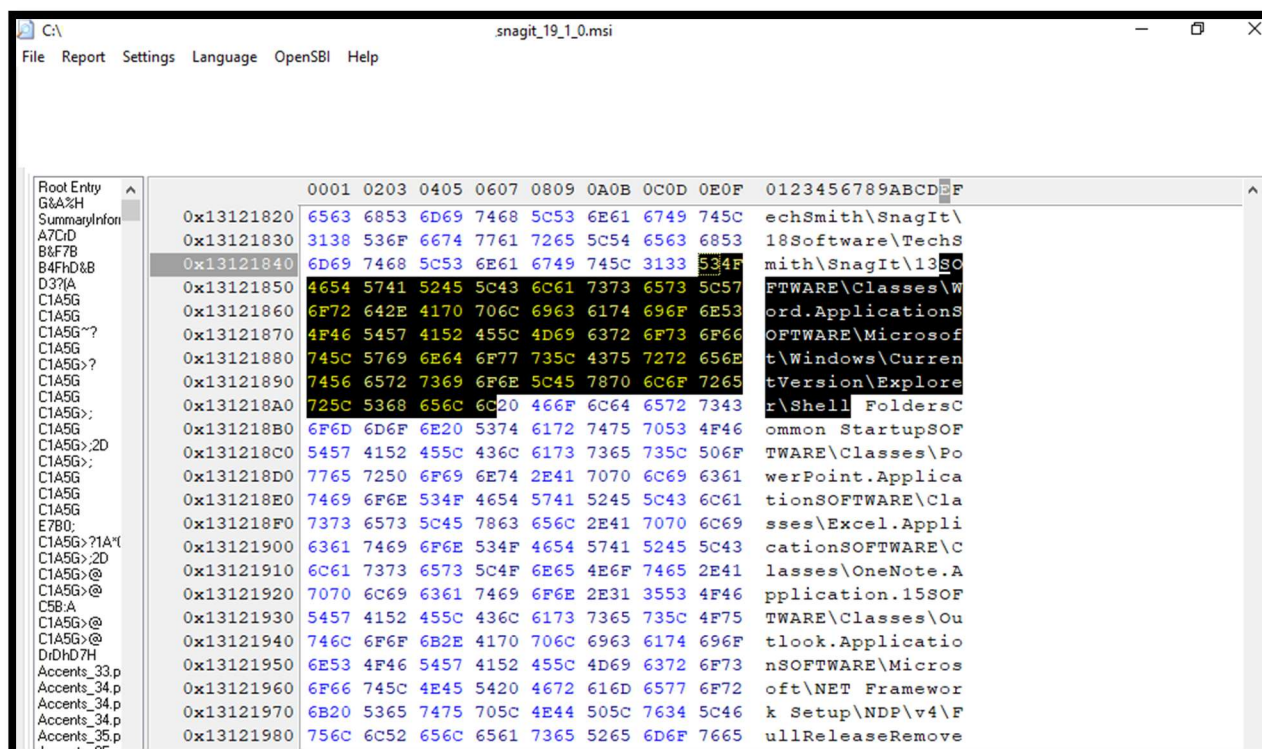
```
root@                                     snagit_19_1_0.msi
String 1:
String 2:
String 3:
Size embedded file: 96000
MD5 embedded file: db613ceacf95a7580ee6829a08d180c0
MAGIC: 005f0000 ._.
Header: 005f0000000100180000000000000000 . . . . .
```

Unfortunately the search of the MD5 (db613ceacf95a7580ee6829a08d180c0) and the further analysis of the OLE (107214) hexadecimal codes below were not conclusive:

```
inc edx
dec ebp
into
mov [0x1],al
add [eax],al
add ss:[eax],al
add [eax],ch
add [eax],al
add [edi+0x1],dh
add [eax],al
pop edi
add [eax],al
add [ecx],al
add [eax],bl
add [eax],al
add [eax],al
add [eax],al
add [eax],al
add [ebx],dl
or eax,[eax]
add [ebx],dl
or eax,[eax]
add [eax],al
add [eax],al
add [eax],al
add [eax],al
add bh,bh
```

11969000	42 4D CE A2 01 00 00 00	00 00 36 00 00 00 28 00	BM.....6... (. .
11969010	00 00 77 01 00 00 5F 00	00 00 01 00 18 00 00 00	. . w . . _
11969020	00 00 00 00 00 00 13 0B	00 00 13 0B 00 00 00 00
11969030	00 00 00 00 00 00 FF FF	FF FF FF FF FF FF FF FF
11969040	FF FF FF FF FF FF FF FF	FF FF FF FF FF FF FF FF
11969050	FF FF FF FF FF FF FF FF	FF FF FF FF FF FF FF FF
11969060	FF FF FF FF FF FF FF FF	FF FF FF FF FF FF FF FF
11969070	FF FF FF FF FF FF FF FF	FF FF FF FF FF FF FF FF
11969080	FF FF FF FF FF FF FF FF	FF FF FF FF FF FF FF FF
11969090	FF FF FF FF FF FF FF FF	FF FF FF FF FF FF FF FF
119690A0	FF FF FF FF FF FF FF FF	FF FF FF FF FF FF FF FF
119690B0	FF FF FF FF FF FF FF FF	FF FF FF FF FF FF FF FF
119690C0	FF FF FF FF FF FF FF FF	FF FF FF FF FF FF FF FF

The software could introduce vulnerabilities through changes in the Internet Explorer settings:



Privileges strings

<u>SeBackupPrivilege</u>
<u>SeChangeNotifyPrivilege</u>
<u>SeDebugPrivilege</u>
<u>SeRestorePrivilege</u>
<u>SeShutdownPrivilege</u>
<u>SeShutdownPrivilege</u>