Snagit 19.1.0.2653

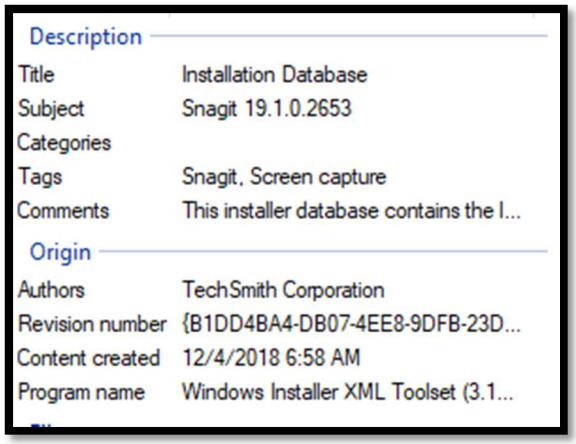
March 30th, 2019.

1. Description

The Snagit[1] 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 result[3] shows the possible negative impact over Microsoft components such as the msiexec[4].exe, Internet Explorer and the Snagit printer installers (SnagitPI[5] and SnagitPI64[6]).

The software also could weaken security settings by misusing privileges[7] such as (SeBackupPrivilege, SeChangeNotifyPrivilege, SeRestorePrivilege, SeShutdownPrivilege and SeDebugPrivilege).

2. File identification



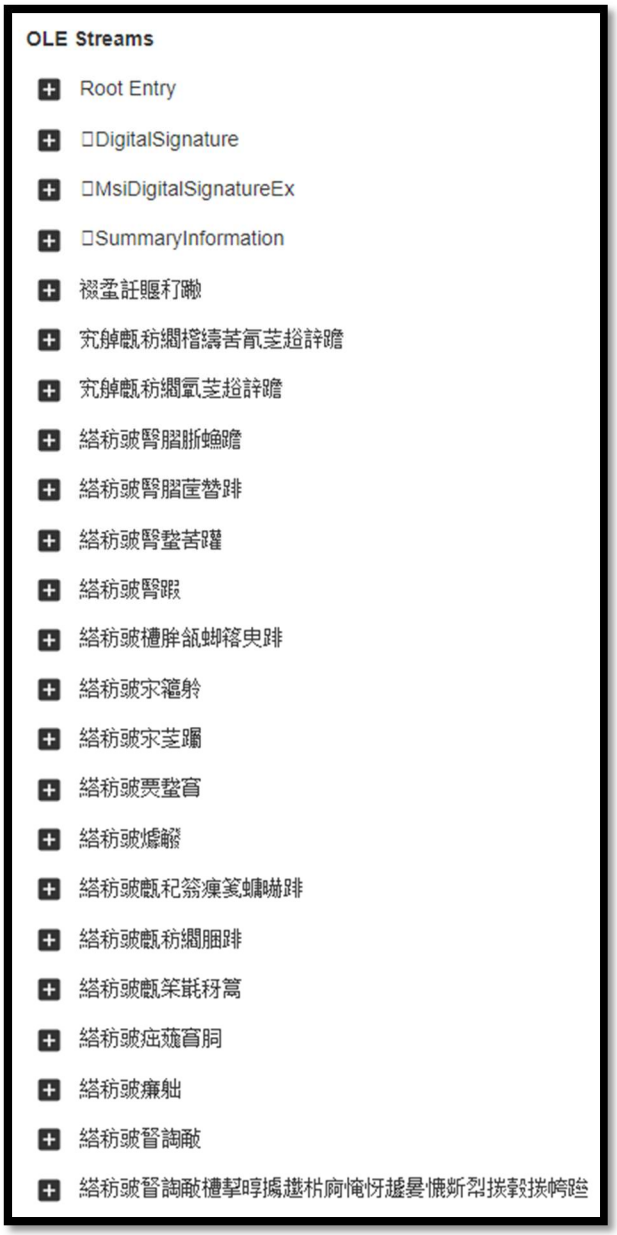
[1] https://www.virustotal.com/gui/file/3ac3c568a515d375eafe33dd712061ccb1814839dcf7e0070e3ea56fab969cb2/detection
[2] https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-oleds/2677fcf2-ad48-4386-ba8f-b1b7baf4c02f
[3] https://any.run/report/21eae0859c24faadbfd93be6b809b0c465f7a55f5e8aaa54fb274b9fa1410318/72a13352-5c47-44b9-b063-4f63ca4800bf#files
[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

```
MD5:    000AC66E850C1F2ECB8A38B1C890722F

SHA1:   BEEBCE29E8A2C82D1DAF1C543C09A3287DCE2889

SAH256: 3AC3C568A515D375EAFE33DD712061CCB1814839DCF7E0070E3EA56FAB969CB2
```

3. OLE Streams



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 (d41d8cd98f00b204e9800998ecf8427e[8]):

The hash above is associated with several malicious execution parents and PE resources parents (Win32) and could drop[9] malicious files.

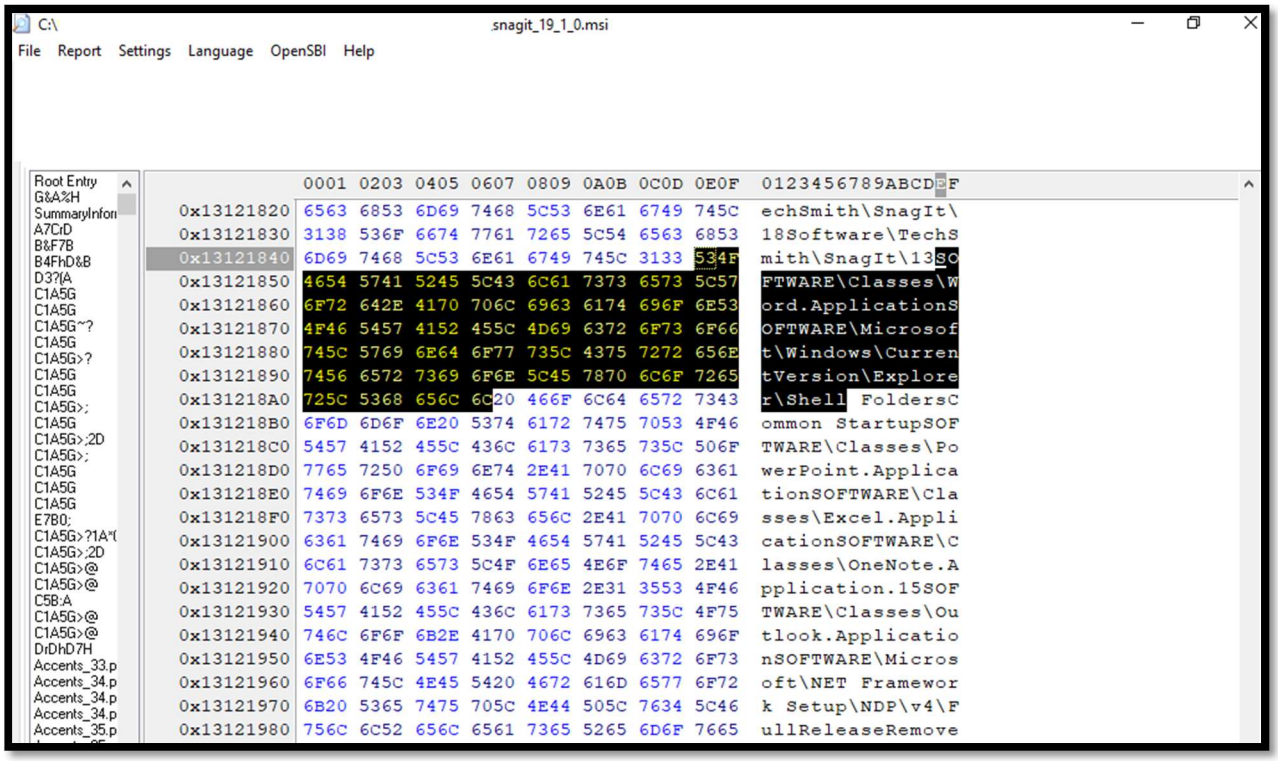
[8] https://www.virustotal.com/gui/file/e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855/relations

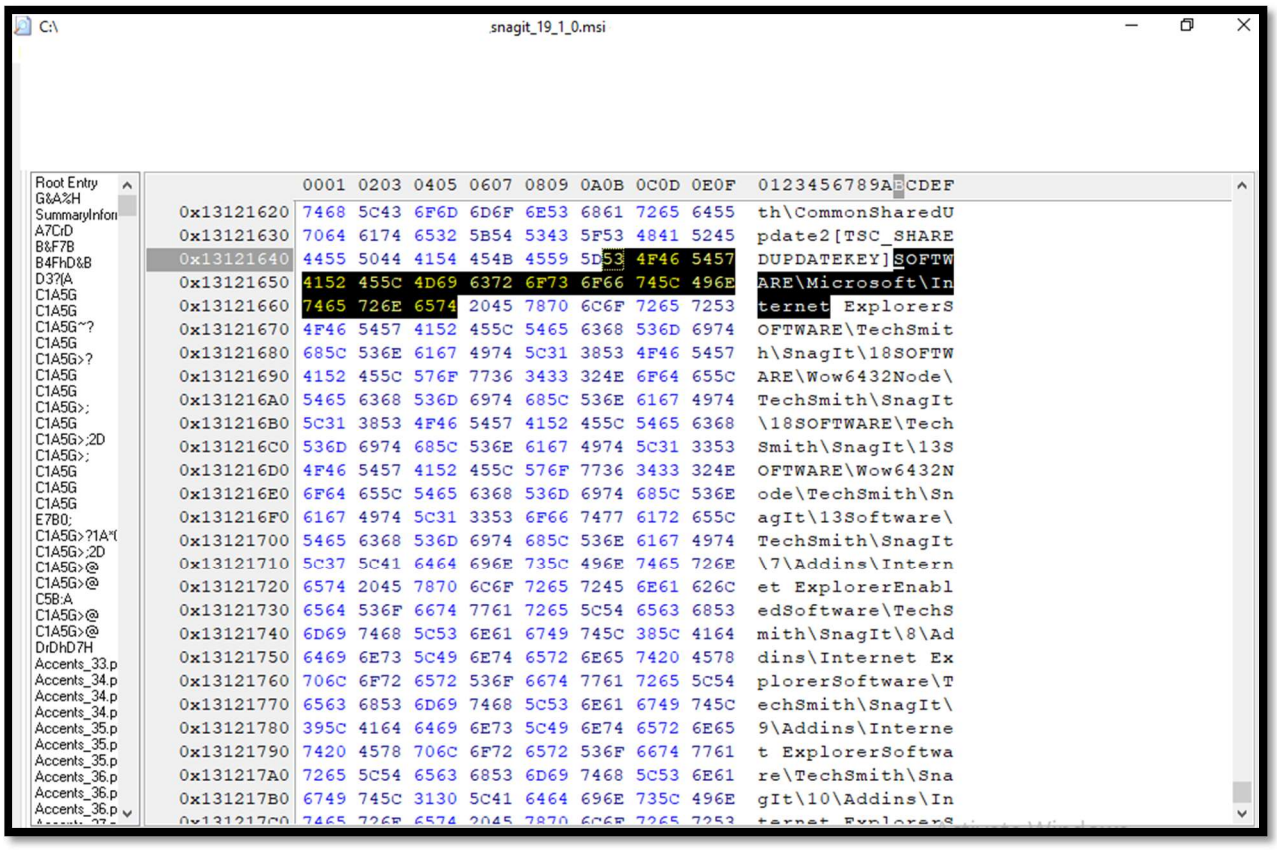
[9] https://www.virustotal.com/gui/file/8c212b6b8c5c643335165ae05ea776f074cfe09dcb29c1f0cfabb59fd2726da7/details

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

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

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





Privileges strings