

# Update: oledump & MSI Files

Published: 2023-04-02

Last Updated: 2023-04-02 08:32:42 UTC

by [Didier Stevens](#) (Version: 1)



0 comment(s)

I wrote about my new oledump plugin [plugin\\_msi\\_info](#) that analyzes MSI files (MSI files are OLE files) in diary entry "[oledump & MSI Files](#)".

I have a new release that brings some changes to the output.

Let me illustrate with this [sample from MalwareBazaar](#):

```
@SANS_JSC
b'UnInstallingPackage,Removing [1]'

Stream: !Upgrade
b'UpgradeCode,VersionMin,VersionMax,Language,Attributes,Remove,ActionProperty'
b'{39558D79-73D9-43BA-9DDE-A1E4ED360027},1.0.0,0,0,2,0,AI_NEWERPRODUCTFOUND'
b'{39558D79-73D9-43BA-9DDE-A1E4ED360027},0.0.1,1.0.0,0,257,0,OLDPRODUCTS'

Remaining streams:
1      480 '\x05SummaryInformation' b'\xfe\xff\x00\x00\n\x00\x02\x00' md5: 822d7bd447807aaa267f9c3402fe9938
2      15086 'Binary.New' ICO md5: 1e80de80cefee55d7cfdaf2edcf3b2
3      15086 'Binary.Up' ICO md5: fd64f54db4cbf736a6fc0d7049f5991e
4 !    598840 'Binary.aicustact.dll' PE File md5: ad6faed544d1f3b892268e4b47425736
5      9319 'Binary.banner.scale150.jpg' JPEG md5: a766139160c43af73563adbd3a38bd5f
6      5714 'Binary.banner.scale125.jpg' JPEG md5: 479576299075c0b85e0de2afe4040c25
7      22946 'Binary.banner.scale200.jpg' JPEG md5: 38ad4b10ac19a240d93e04d383822381
8      4502 'Binary.banner.jpg' JPEG md5: d5a55a78cd38f45256807c7851619b7d
9 ?    28870 'Binary.banner.svg' b'<?xml ve' md5: a92209231c43a871925d546c6dc5c244
10     2862 'Binary.cmdlinkarrow' ICO md5: 983358ce03817f1ca404befbe1e4d96a
11     15086 'Binary.completi' ICO md5: c23af89757665bc0386fd798a61b2112
12     15086 'Binary.custicon' ICO md5: be6d2f48aa6634fb2101c273c798d4d9
13     27770 'Binary.dialog.scale150.jpg' JPEG md5: de300c8b0a317b6e29a47facfa76a6c0
14     16673 'Binary.dialog.scale125.jpg' JPEG md5: a6cc6f0799276ec0c0b8704fdc91236b
15     69692 'Binary.dialog.scale200.jpg' JPEG md5: 816c6b957bd8ed6a79dfa6a1eb9c57a1
16     12626 'Binary.dialog.jpg' JPEG md5: 5f6253cff5a8b031bfb3b161079d0d86
17 ?    33179 'Binary.dialog.svg' b'<?xml ve' md5: 9a3a9d5895b3645c3cccaa4dd20c2358
18     15086 'Binary.exclamic' ICO md5: 3fbb7ddbc13edf109e3acaa7a4a69a4e
19     15086 'Binary.info' ICO md5: 8595d2a2d58310b448729e28649443d6
20     15086 'Binary.insticon' ICO md5: eac3781ba9fb0502d6f16253eb67b2b4
21     15086 'Binary.removico' ICO md5: 1fffe5c3cc990d0c012a428a59b2ae46
22     15086 'Binary.repairic' ICO md5: 915e40a576fa41dc5f8486103341673e
23      854 'Binary.tabback' BMP md5: 4c3dda35e23d44e273d82f7f4c38470a
24 !   7321495 'disk1.cab' CAB File md5: f64aae09a9cdc8eec1ed62535ef47d06
      1856512 b'abd1.exe'
      7120384 b'WebUI.dll'

@SANS_ISC C:\Demo>
```

At the end of the report (Remaining streams), I've added an indicator.

! indicates PE files and CAB files.

? indicates files that are not images (PNG, JPEG, BMP), neither PE or CAB files.

In this example, a SVG file (image) is marked with indicator ?.

I parse CAB files to list their content.

And you can change the hash algorithm with environment variable  
DSS\_DEFAULT\_HASH\_ALGORITHMS.

Didier Stevens

Senior handler

Microsoft MVP

[blog.DidierStevens.com](https://blog.didierstevens.com)