Update: oledump & MSI Files

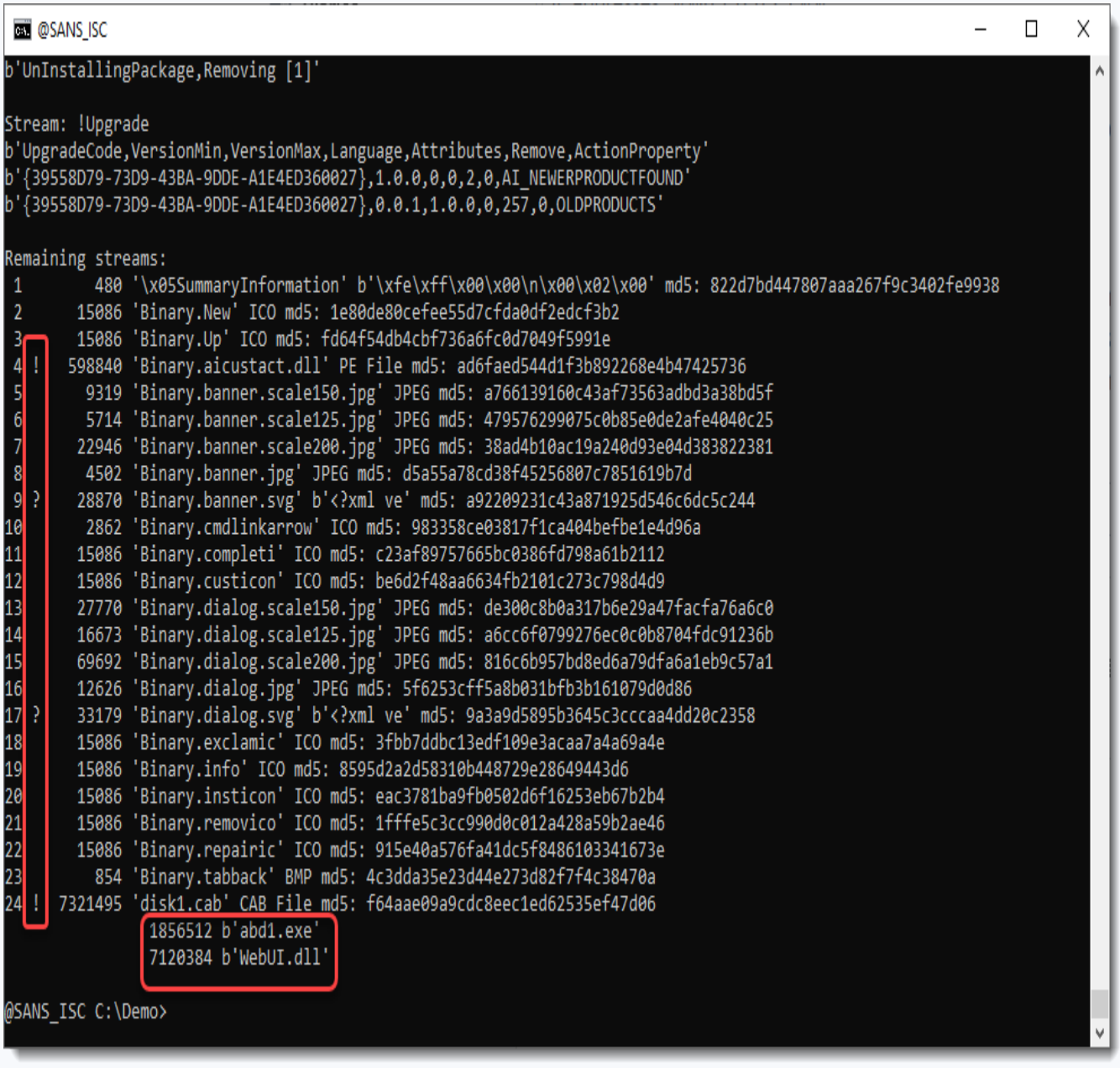
Published: 2023-04-02
Last Updated: 2023-04-02 08:32:42 UTC
by Didier Stevens (Version: 1)

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:



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