Vault 7: CIA Hacking Tools Revealed

Releases ▼ (../index.html) **Documents ▼** (index.html)

Navigation: » Directory (index.html) » Operational Support Branch (OSB) (space_1736706.html) » OSB Home (page_1179757.html) » Projects (page_2621693.html) » Fine Dining (page_20251096.html) » Fine Dining Tool Module Lists (page_20251107.html)

Owner: [redacted]

Chrome Portable DLL Hijack

Similar to others prior...

Chromelooks for "**DWrite.dll**", a system DLL, adjacent to itself (under \app\Chrome-bin) before correctly finding it

This DLL is ideal for hijacking as it only exports one function (at ordinal **#1**) with the following prototype:

HRESULT DWriteCreateFactory(DWRITE_FACTORY_TYPE, REFIID, IUnknown)**

The DWRITE_FACTORY_TYPE is an enum defined in Dwrite.h, however we cannot #include this header as doing so will declare the function as an extern.

Instead, we can either create a dummy enum with only two values (as the real DWRITE_FACTORY_TYPE only has two options) or simply use a INT variable in its place.

Chrome does not appear to have the race-condition crash report that Thunderbird had

Top

WL Research Community - user contributed research based on documents published by WikiLeaks.

(https://our.wikileaks.org)

Tor is an encrypted anonymising network that makes it harder to intercept internet communications, or see where communications are coming from or going to.

(https://www.torproject

Tails is a live operating system, that you can start on almost any computer from a DVD, USB stick, or SD card. It aims at preserving your privacy and anonymity.

(https://tails.boum.org/)

The Courage Foundation is an international organisation that supports those who risk life or liberty to make significant contributions to the historical record.

(https://www.couragefound.org/)

Bitcoin uses peer-to-peer technology to operate with no central authority or banks; managing transactions and the issuing of bitcoins is carried out collectively by the network.

(https://www.bitcoin.org/)

(https://www.facebook.com/wikileaks) (https://twitter.com/wikileaks)