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: User #71468 [redacted]

Notepad++ DLL Hijack

The following DLL hijack works for both the portable and non-portable variants of Notepad++

Notepad++ loads Scintilla, a "code editing component" (and seperate project), from a DLL adjacent to its EXE called "**SciLexer.dll**". This DLL exports only one funciton named "**Scintilla_DirectFunction**" at ordinal #1

The DLL does a lot of "set up" in ProcessAttach, so it is important to load the true DLL as soon as the hijack is loaded.

The exported function has the following prototype definition, according to the open source for Notepad++ online:

```
    sptr_t __stdcall Scintilla_DirectFunction(ScintillaWin * sci, UINT iMessage, uptr_t
```

wParam, sptr_t lParam)

For the life of me, I couldn't get this function to be called – I even installed additional plugins that were supposed to interact with Scintilla directly. Considering we have the prototype, this shouldn't be that big of a deal, but its worth noting.

<u>Languages Available:</u>

Languages	**%PAL:LanguageCustom% Replacement**
Arabic	arabic
Bengali	bengali
Chinese (Simplified)	chinese
Chinese (Traditional)	chineseSimplified
Dutch	dutch
English	english
French	french
Farsi	farsi
German	german
Hindi	hindi
Italian	italian
Japanese	japanese
Korean	korean
Portuguese	prtuguese
Portuguese (Brazilian)	brazilian_portugese
Russian	russian
Spanish	spanish

Turkish	turkish
Urdu	urdu

Previous versions:

| 1 (page_26968092.html) | 2 (page_28803118.html) | 3 (page_28803124.html) |

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.org/)

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)