

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

Kaspersky TDSS Killer Portable DLL Hijack

The following is a screenshot of a selected number of DLL misses from Kaspersky TDSS Killer Portable:

Time ...	Process Name	PID	Operation	Path	Result	Detail
11:47:...	Kaspersky TDSSKillerPortable.e...	3132	CreateFile	C:\Users\...\Desktop\Kaspersky TDSSKillerPortable\SHFOLDER.DLL	NAME NOT FOUND	Desired Access: Read Attributes, Disposition: Open, Opt...
11:47:...	Kaspersky TDSSKillerPortable.e...	3132	CreateFile	C:\Windows\System32\shfolder.dll	SUCCESS	Desired Access: Read Attributes, Disposition: Open, Opt...
11:47:...	Kaspersky TDSSKillerPortable.e...	3132	CreateFile	C:\Windows\System32\shfolder.dll	SUCCESS	Desired Access: Read Data/List Directory, Execute/Tra...
11:47:...	Kaspersky TDSSKillerPortable.e...	3132	CreateFile	C:\Users\...\Desktop\Kaspersky TDSSKillerPortable\App\TDSSKiller\ui\SwDRM.dll	PATH NOT FOUND	Desired Access: Read Attributes, Disposition: Open, Opt...
11:47:...	tdsskiller.exe	2912	CreateFile	C:\Users\...Desktop\Kaspersky TDSSKillerPortable\App\TDSSKiller\VERSION.dll	NAME NOT FOUND	Desired Access: Read Attributes, Disposition: Open, Opt...
11:47:...	tdsskiller.exe	2912	CreateFile	C:\Windows\System32\version.dll	SUCCESS	Desired Access: Read Attributes, Disposition: Open, Opt...
11:47:...	tdsskiller.exe	2912	CreateFile	C:\Windows\System32\version.dll	SUCCESS	Desired Access: Read Data/List Directory, Execute/Tra...
11:47:...	tdsskiller.exe	2912	CreateFile	C:\Users\...Desktop\Kaspersky TDSSKillerPortable\App\TDSSKiller\RICHED20.DLL	NAME NOT FOUND	Desired Access: Read Attributes, Disposition: Open, Opt...
11:47:...	tdsskiller.exe	2912	CreateFile	C:\Windows\System32\riched20.dll	SUCCESS	Desired Access: Read Attributes, Disposition: Open, Opt...
11:47:...	tdsskiller.exe	2912	CreateFile	C:\Windows\System32\riched20.dll	SUCCESS	Desired Access: Read Data/List Directory, Execute/Tra...

Showing 10 of 183,318 events (0.0054%) Backed by virtual memory

Although `\app\TDSSKiller\ui\SwDRM.dll` is a miss for the Portable splash EXE, placing a DLL here does not result in code execution.

"SHFOLDER.dll" will load and can return FALSE from `PROCESS_ATTACH`, `"riched20.dll"`

and "version.dll" require function forwarding

Attachments:

kasp procmon.png (files/kasp%20procmon.png)



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>)