Vault 7: CIA Hacking Tools Revealed

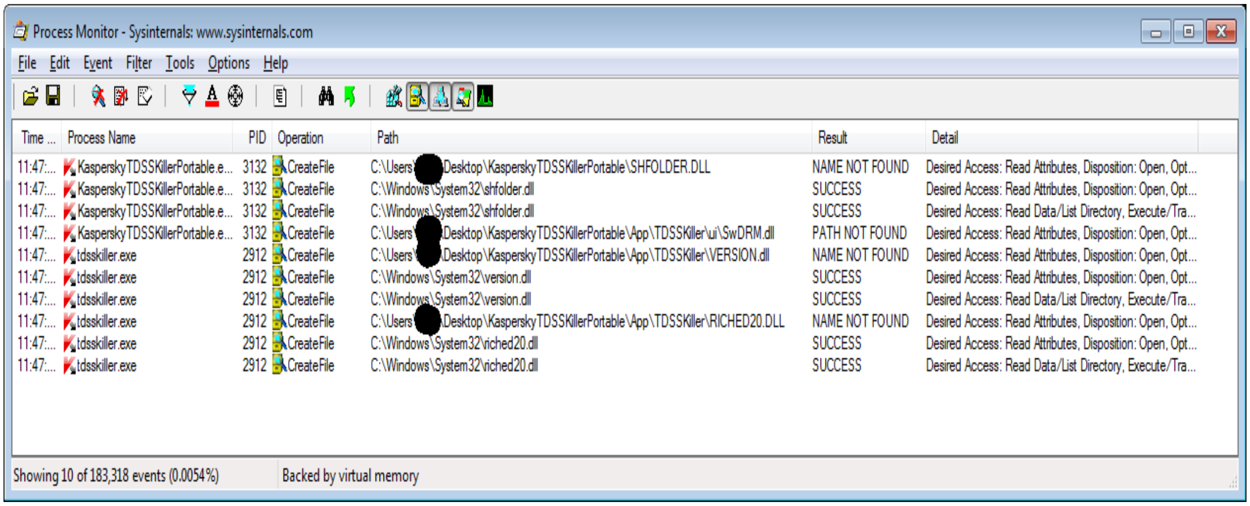
Releases ▼ (../index.html) **Documents ▼** (index.html)

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:...	KasperskyTDSSKillerPortable.e...	3132	CreateFile	C:\Users\[redacted]\Desktop\KasperskyTDSSKillerPortable\SHFOLDER.DLL	NAME NOT FOUND	Desired Access: Read Attributes, Disposition: Open, Opt...
11:47:...	KasperskyTDSSKillerPortable.e...	3132	CreateFile	C:\Windows\System32\shfolder.dll	SUCCESS	Desired Access: Read Attributes, Disposition: Open, Opt...
11:47:...	KasperskyTDSSKillerPortable.e...	3132	CreateFile	C:\Windows\System32\shfolder.dll	SUCCESS	Desired Access: Read Data/List Directory, Execute/Tra...
11:47:...	KasperskyTDSSKillerPortable.e...	3132	CreateFile	C:\Users\[redacted]\Desktop\KasperskyTDSSKillerPortable\App\TDSSKiller\ui\SwDRM.dll	PATH NOT FOUND	Desired Access: Read Attributes, Disposition: Open, Opt...
11:47:...	tdsskiller.exe	2912	CreateFile	C:\Users\[redacted]\Desktop\KasperskyTDSSKillerPortable\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\[redacted]\Desktop\KasperskyTDSSKillerPortable\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 odes 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)

Top