

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

McAfee Stinger Portable DLL Hijack

Procmon screenshot of potential DLL options:

Time	Process Name	PID	Operation	Path	Result	Detail
2:31:4...	stinger32.exe	276	CreateFile	C:\Users\... Desktop\McAfee Stinger Portable\App\Stinger\mfeaaca.dll	NAME NOT FOUND	Desired Access: R...
2:31:4...	stinger32.exe	276	CreateFile	C:\Windows\System32\mfeaaca.dll	NAME NOT FOUND	Desired Access: R...
2:31:4...	stinger32.exe	276	CreateFile	C:\Windows\system\mfeaaca.dll	NAME NOT FOUND	Desired Access: R...
2:31:4...	stinger32.exe	276	CreateFile	C:\Windows\mfeaaca.dll	NAME NOT FOUND	Desired Access: R...
2:31:4...	stinger32.exe	276	CreateFile	C:\Program Files\stinger\mfeaaca.dll	NAME NOT FOUND	Desired Access: R...
2:31:4...	stinger32.exe	276	CreateFile	C:\Program Files\Windows Resource Kits\Tools\mfeaaca.dll	NAME NOT FOUND	Desired Access: R...
2:31:4...	stinger32.exe	276	CreateFile	C:\Windows\System32\mfeaaca.dll	NAME NOT FOUND	Desired Access: R...
2:31:4...	stinger32.exe	276	CreateFile	C:\Windows\mfeaaca.dll	NAME NOT FOUND	Desired Access: R...
2:31:4...	stinger32.exe	276	CreateFile	C:\Windows\System32\wbem\mfeaaca.dll	NAME NOT FOUND	Desired Access: R...
2:31:4...	stinger32.exe	276	CreateFile	C:\Windows\System32\WindowsPowerShell\v1.0\mfeaaca.dll	NAME NOT FOUND	Desired Access: R...
2:31:4...	stinger32.exe	276	CreateFile	C:\Users\... Desktop\McAfee Stinger Portable\App\Stinger\stinger32ENU.dll	NAME NOT FOUND	Desired Access: R...
2:31:4...	stinger32.exe	276	CreateFile	C:\Users\... Desktop\McAfee Stinger Portable\App\Stinger\stinger32ENU.dll.DLL	NAME NOT FOUND	Desired Access: R...
2:31:4...	stinger32.exe	276	CreateFile	C:\Users\... Desktop\McAfee Stinger Portable\App\Stinger\stinger32ENU.dll	NAME NOT FOUND	Desired Access: R...
2:31:4...	stinger32.exe	276	CreateFile	C:\Users\... Desktop\McAfee Stinger Portable\App\Stinger\stinger32ENU.dll.DLL	NAME NOT FOUND	Desired Access: R...
2:31:4...	stinger32.exe	276	CreateFile	C:\Users\... Desktop\McAfee Stinger Portable\App\Stinger\stinger32ENU.dll	NAME NOT FOUND	Desired Access: R...
2:31:4...	stinger32.exe	276	CreateFile	C:\Users\... Desktop\McAfee Stinger Portable\App\Stinger\stinger32ENU.dll.DLL	NAME NOT FOUND	Desired Access: R...
2:31:4...	stinger32.exe	276	CreateFile	C:\Users\... Desktop\McAfee Stinger Portable\App\Stinger\stinger32LOC.dll	NAME NOT FOUND	Desired Access: R...
2:31:4...	stinger32.exe	276	CreateFile	C:\Users\... Desktop\McAfee Stinger Portable\App\Stinger\stinger32LOC.dll.DLL	NAME NOT FOUND	Desired Access: R...
2:31:4...	stinger32.exe	276	CreateFile	C:\Users\... Desktop\McAfee Stinger Portable\App\Stinger\stinger32LOC.dll	NAME NOT FOUND	Desired Access: R...
2:31:4...	stinger32.exe	276	CreateFile	C:\Users\... Desktop\McAfee Stinger Portable\App\Stinger\stinger32LOC.dll.DLL	NAME NOT FOUND	Desired Access: R...
2:31:4...	stinger32.exe	276	CreateFile	C:\Users\... Desktop\McAfee Stinger Portable\App\Stinger\DWrite.dll	NAME NOT FOUND	Desired Access: R...
2:31:4...	stinger32.exe	276	CreateFile	C:\Users\... Desktop\McAfee Stinger Portable\App\Stinger\dxgi.dll	NAME NOT FOUND	Desired Access: R...
2:31:4...	stinger32.exe	276	CreateFile	C:\Users\... Desktop\McAfee Stinger Portable\App\Stinger\DXGIDebug.dll	NAME NOT FOUND	Desired Access: R...
2:31:4...	stinger32.exe	276	CreateFile	C:\Windows\System32\DXGIDebug.dll	NAME NOT FOUND	Desired Access: R...
2:31:4...	stinger32.exe	276	CreateFile	C:\Windows\System32\DXGIDebug.dll	NAME NOT FOUND	Desired Access: R...
2:31:4...	stinger32.exe	276	CreateFile	C:\Users\... Desktop\McAfee Stinger Portable\App\Stinger\vm3dum.dll	NAME NOT FOUND	Desired Access: R...
2:31:4...	stinger32.exe	276	CreateFile	C:\Users\... Desktop\McAfee Stinger Portable\App\Stinger\vm3dum.dll	NAME NOT FOUND	Desired Access: R...
2:31:4...	stinger32.exe	276	CreateFile	C:\Users\... Desktop\McAfee Stinger Portable\App\Stinger\D3D10Warp.dll	NAME NOT FOUND	Desired Access: R...
2:31:4...	stinger32.exe	276	CreateFile	C:\Users\... Desktop\McAfee Stinger Portable\App\Stinger\vm3dum.dll	NAME NOT FOUND	Desired Access: R...
2:31:4...	stinger32.exe	276	CreateFile	C:\Users\... Desktop\McAfee Stinger Portable\App\Stinger\vm3dum.dll	NAME NOT FOUND	Desired Access: R...
2:31:4...	stinger32.exe	276	CreateFile	C:\Users\... Desktop\McAfee Stinger Portable\App\Stinger\vm3dum.dll	NAME NOT FOUND	Desired Access: R...
2:31:4...	stinger32.exe	276	CreateFile	C:\Users\... Desktop\McAfee Stinger Portable\App\Stinger\D3D10Warp.dll	NAME NOT FOUND	Desired Access: R...

McAfee attempts to load "mfeaaca.dll" several times, including when it runs a scan, and thus may not be the best candidate.

the stinger32ENU.dll and stinger32LOC.dll locations resulted in McAfee crashing when returning FALSE from PROCESS_ATTACH. "vm3dum.dll" was never loaded

"DWrite.dll" worked fine when calls were forwarded to the proper system DLL

"DXGIDebug.dll" did not cause problems when returning FALSE from PROCESS_ATTACH (and thus no calls were forwarded)

Languages Available:

English only

Attachments:

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

Previous versions:

| 1 (page_27492402.html) | 2 (page_28803116.html) |

Top



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



Tor is an encrypted anonymising network that makes it harder to intercept internet communications, or see where



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



The Courage Foundation is an international organisation that supports those who risk life or liberty to make



Bitcoin uses peer-to-peer technology to operate with no central authority or banks; managing transactions and

(<https://our.wikileaks.org>) communications preserving your significant the issuing of
 are coming from or privacy and contributions to the bitcoins is carried
 going to. anonymity. historical record. out collectively by
 (<https://www.torproject.org>) (<https://tails.boum.org/>) (<https://www.couragefound.org/>) the network.
 (<https://www.bitcoin.org/>)

 (<https://www.facebook.com/wikileaks>)

 (<https://twitter.com/wikileaks>)