Vault 7: CIA Hacking Tools Revealed

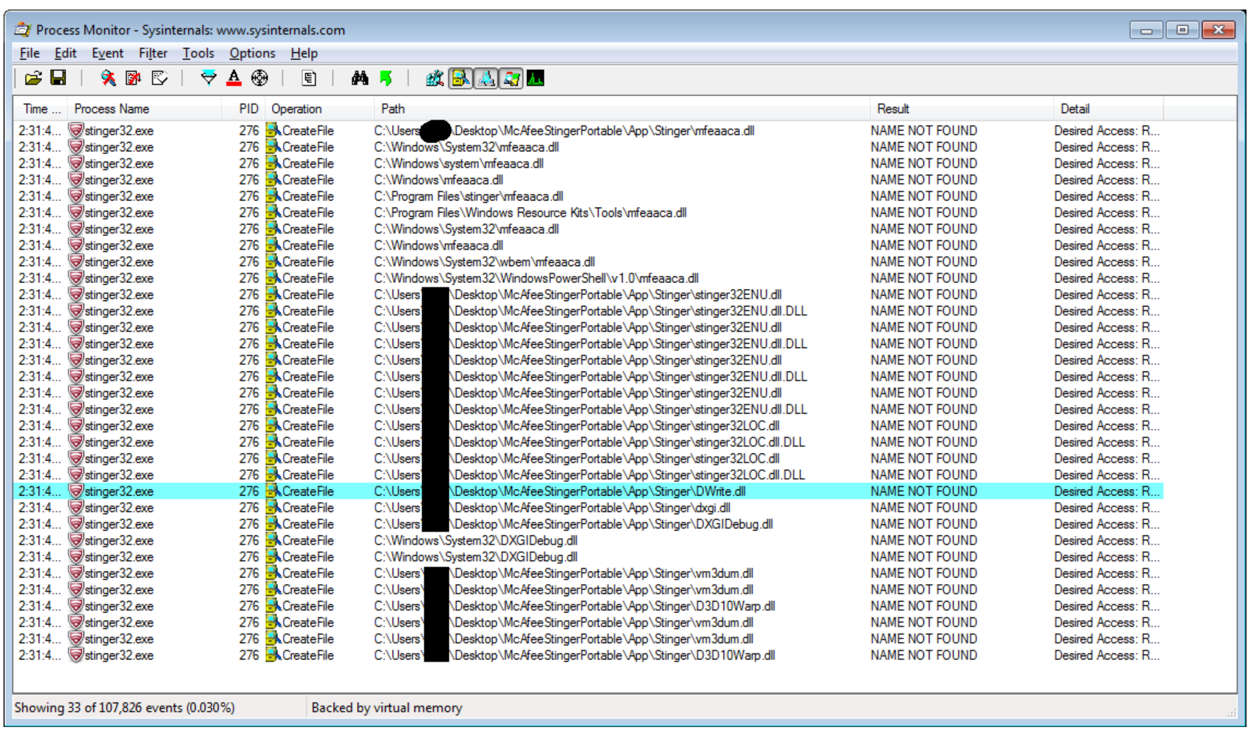
Releases ▼ (../index.html) **Documents ▼** (index.html)

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 protential DLL options:



Time ...	Process Name	PID	Operation	Path	Result	Detail
2:31:4...	stinger32.exe	276	CreateFile	C:\Users[redacted]\Desktop\McAfeeStingerPortable\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[redacted]\Desktop\McAfeeStingerPortable\App\Stinger\stinger32ENU.dll	NAME NOT FOUND	Desired Access: R...
2:31:4...	stinger32.exe	276	CreateFile	C:\Users[redacted]\Desktop\McAfeeStingerPortable\App\Stinger\stinger32ENU.dll.DLL	NAME NOT FOUND	Desired Access: R...
2:31:4...	stinger32.exe	276	CreateFile	C:\Users[redacted]\Desktop\McAfeeStingerPortable\App\Stinger\stinger32ENU.dll	NAME NOT FOUND	Desired Access: R...
2:31:4...	stinger32.exe	276	CreateFile	C:\Users[redacted]\Desktop\McAfeeStingerPortable\App\Stinger\stinger32ENU.dll.DLL	NAME NOT FOUND	Desired Access: R...
2:31:4...	stinger32.exe	276	CreateFile	C:\Users[redacted]\Desktop\McAfeeStingerPortable\App\Stinger\stinger32ENU.dll	NAME NOT FOUND	Desired Access: R...
2:31:4...	stinger32.exe	276	CreateFile	C:\Users[redacted]\Desktop\McAfeeStingerPortable\App\Stinger\stinger32ENU.dll.DLL	NAME NOT FOUND	Desired Access: R...
2:31:4...	stinger32.exe	276	CreateFile	C:\Users[redacted]\Desktop\McAfeeStingerPortable\App\Stinger\stinger32ENU.dll	NAME NOT FOUND	Desired Access: R...
2:31:4...	stinger32.exe	276	CreateFile	C:\Users[redacted]\Desktop\McAfeeStingerPortable\App\Stinger\stinger32ENU.dll.DLL	NAME NOT FOUND	Desired Access: R...
2:31:4...	stinger32.exe	276	CreateFile	C:\Users[redacted]\Desktop\McAfeeStingerPortable\App\Stinger\stinger32LOC.dll	NAME NOT FOUND	Desired Access: R...
2:31:4...	stinger32.exe	276	CreateFile	C:\Users[redacted]\Desktop\McAfeeStingerPortable\App\Stinger\stinger32LOC.dll.DLL	NAME NOT FOUND	Desired Access: R...
2:31:4...	stinger32.exe	276	CreateFile	C:\Users[redacted]\Desktop\McAfeeStingerPortable\App\Stinger\stinger32LOC.dll	NAME NOT FOUND	Desired Access: R...
2:31:4...	stinger32.exe	276	CreateFile	C:\Users[redacted]\Desktop\McAfeeStingerPortable\App\Stinger\stinger32LOC.dll.DLL	NAME NOT FOUND	Desired Access: R...
2:31:4...	stinger32.exe	276	CreateFile	C:\Users[redacted]\Desktop\McAfeeStingerPortable\App\Stinger\DWrite.dll	NAME NOT FOUND	Desired Access: R...
2:31:4...	stinger32.exe	276	CreateFile	C:\Users[redacted]\Desktop\McAfeeStingerPortable\App\Stinger\dxgi.dll	NAME NOT FOUND	Desired Access: R...
2:31:4...	stinger32.exe	276	CreateFile	C:\Users[redacted]\Desktop\McAfeeStingerPortable\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[redacted]\Desktop\McAfeeStingerPortable\App\Stinger\vm3dum.dll	NAME NOT FOUND	Desired Access: R...
2:31:4...	stinger32.exe	276	CreateFile	C:\Users[redacted]\Desktop\McAfeeStingerPortable\App\Stinger\vm3dum.dll	NAME NOT FOUND	Desired Access: R...
2:31:4...	stinger32.exe	276	CreateFile	C:\Users[redacted]\Desktop\McAfeeStingerPortable\App\Stinger\D3D10Warp.dll	NAME NOT FOUND	Desired Access: R...
2:31:4...	stinger32.exe	276	CreateFile	C:\Users[redacted]\Desktop\McAfeeStingerPortable\App\Stinger\vm3dum.dll	NAME NOT FOUND	Desired Access: R...
2:31:4...	stinger32.exe	276	CreateFile	C:\Users[redacted]\Desktop\McAfeeStingerPortable\App\Stinger\vm3dum.dll	NAME NOT FOUND	Desired Access: R...
2:31:4...	stinger32.exe	276	CreateFile	C:\Users[redacted]\Desktop\McAfeeStingerPortable\App\Stinger\D3D10Warp.dll	NAME NOT FOUND	Desired Access: R...

Showing 33 of 107,826 events (0.030%) Backed by virtual memory

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 McAffe crashing when returning FALSE from PROCSESS_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

(https://our.wikileaks.org/)

communications are coming from or going to.

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

preserving your privacy and anonymity.

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

significant contributions to the historical record.

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

the issuing of bitcoins is carried out collectively by the network.

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

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