Home   Services   Products & Freebies   ⬚ Search

Case Studies   Contact Us

Posted on **2018-04-24**   ← **Previous**   **Next** →

ExtExport – yet another LOLBin

This is a quick & dirty recipe how to load a DLL of your choice using a built-in tool ExtExport.exe that can be found inside the Internet Explorer directory:

Method #1

- Drop a file named like one of these:
    - mozcrt19.dll
    - mozsqlite3.dll
    - sqlite3.dll
      inside the c:\test folder
- Now run:
    - "C:\Program Files\Internet Explorer\ExtExport.exe" c:\test foo bar

This will load one (or all) of these DLLs.

Method #2

The tool has more arbitrary DLL loading possibilities that allow to specify the name of the library directly from a command line.

This method requires providing more arguments e.g.:

- ExtExport.exe c:\Test\test.dll 2 3 4 FIREFOX {00000000-0000-0000-0000-000000000000}

I have not explored what other arguments mean but you can swap them with whatever you want to evade static detection; what matters is that the first argument must be a DLL name we want to load and the last argument must be a valid GUID presented in a form shown in a syntax above (acceptable by the IIDFromString function).

Method #3

It's actually a variant of the method 2 – we just need to swap 'FIREFOX' with '360SE':

- ExtExport.exe c:\Test\test.dll 2 3 4 360SE {00000000-0000-0000-0000-000000000000}

This entry was posted in **Living off the land**, **LOLBins** by **adam**. Bookmark the **permalink**.

Privacy Policy | **Proudly powered by WordPress**