

[Full-disclosure] Multi-Languages OPcodes DB

Source: <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2005-08/0892.html>

From: Jerome Athias (*jerome.athias_at_free.fr*)

Date: 08/26/05

Date: Fri, 26 Aug 2005 11:37:04 +0200

To: "framework@metasploit.com" <framework@metasploit.com>, "full-disclosure@lists.grok.org.uk" <f

Hi,

as you probably all know, Windows DLLs have different base addresses across Windows/SP/languages so i think it could be usefull to try to build a multi-lang opcodes database, isn't it? so, i have done VERY QUICKLY a little package based on a .BAT and some tools :

Files included in the package:

* OPCODES_LIST.bat : (horrible) Main batch file

MD5: c43d4167f7352c211a97f8cf21cd0458

SHA1: eb2f62912c9311351540dfc0237000e7bf090070

* Psinfo.exe : tool from sysinternals.com to retrieve windows system informations ans the list of installed hotfixs (trying also to use the Windows 2003 "wmic qfe" command) (could be long...)

MD5: 2c18e62e9902b0a258e6a64ab812f02c

SHA1: 0188d8836ba6a2a198abcfee9ae730b4ce0521aa

pdh.dll

MD5: 8542b31187bd1035a2311324c23e66b1

SHA1: ecc77cd54061745273af9750c55c1434c24bcd74

* reg.exe : tool present on XP but not on all 2000... used to retrieve the OS language (languages codes list included in the bat)

MD5: 5bc49b61651edbc0a80d2de16d7f422c

SHA1: 7a778b97bf7b68247e0b212a81c952118c1ba45a

* Findjmp2.exe : tool by Class101 to retrieve the opcodes in memory

(DLLs searched : KERNEL32.DLL, NTDLL.DLL, USER32.DLL, SHELL32.DLL, GDI32.DLL, WS2_32.DLL, WS2HELP.DLL)

(registers searched : EAX, EBX, ECX, EDX, ESI, EDI, ESP, EBP)

MD5: 3909e20cb55ea82b01a3b593d0cc59b6

SHA1: 174169d18b039fcd11ee1507d0a7f8e4230ed717

Full-Disclosure: [Full-disclosure] Multi-Languages OPcodes DB

* LISTDLLS.exe : tool from sysinternals.com used to retrieve the versions of DLLs

MD5: bb5f0e1d03f4e32261bb0964fc3b0e9d

SHA1: c6081622207ec53f6400a6312a87cf350333996b

* mycrc.exe : tool by Luigi Auriemma to check files checksums (MD5, SHA1, ...)

MD5: 5473219dd371630c1e7d7e7fa1ddd53f

SHA1: 37c71403ed231dd9cb9a6e97c869e7275372ba12

* grep.exe : used to parse a little bit the output

MD5: 9e05a9c264c8a908a8e79450fcbff047

SHA1: 0ab5c2b1c3c637cbe82564d6d9ed34a78c901cb7

* uniq.exe : used to parse a little bit the output

PLEASE NOTE :

1) we can do better and more simple!!!, so if you want: JUST DO IT and please don't flame!

2) the output is far to be clean! but could be easily parsed with a simple script...

For guy who want to help; please send me the resulting

"OPCODES_LIST.TXT" file

(PLEASE REMOVE ALL PERSONAL DATA IN THE FILE! ;).

Then i'll try to check all the files and start to build something, of course publicly available.

The package is available for download at:

http://www.athias.fr/OPCODES_LIST.RAR

MD5: c4a7d4eba31afafb67ef488dda7cf19e

SHA1: c99a98741a8365fe6872a2347d0b05891188c584

Please let me know missing things...

Thank you.

/JA

Full-Disclosure – We believe in it.

Charter: <http://lists.grok.org.uk/full-disclosure-charter.html>

Hosted and sponsored by Secunia – <http://secunia.com/>

Full-Disclosure: [Full-disclosure] Multi-Languages OPcodes DB

- application/x-pkcs7-signature attachment: S/MIME Cryptographic Signature