n C I r c l e°

64-bit Imports Rebuilding and Unpacking

Sebastien Doucet <sdoucet@ncircle.com>

© nCircle 2010. All rights reserved.



- Security Research Engineer at nCircle in Toronto
- My accent is from Montreal
- Used to be involved in the online reverse-engineering community
 - Moderator at reverse-engineering.net forum
 - Co-founder of video.reverse-engineering.net (defunct)
 - Most evil moderator at crackmes.de
 - Member of ARTeam





- Used to be a 60-minutes presentation
- Had to take away all the jokes
- Only dry technical stuff left
- Focus is on the unpacking process instead of the tool
- For more information or the full deck of slides, come see me at the nCircle booth



Looking at the Bigger Picture

- More 64-bit malware is appearing every day
- Next generation of Windows will probably be 64-bit only like Windows Server 2008 R2
- Programming languages limited to a specific architecture like C and C++ increase the difficulty in dealing with cross-architecture tasks like unpacking
- Platform-independent languages like Python simplify things but still require you to know what you are doing when dealing with the PE format and headers
- If I had to redo it today, I would do it in C#

Overview

- Part 1: What is unpacking?
- Part 2: What is ImpREC? (original tool)
- Part 3: What is CHimpREC? (my tool)
- Part 4: Inner workings of an imports rebuilder

• Part 5: Live 64-bit unpacking session

Part 1: What is unpacking?

- Packers are designed to protect the content of an executable binary or library
 - Commercial software (game copy protection)
 - Malware
- Most packers use encryption or compression
- Original assembly code not accessible
- Make static analysis impossible or at least, very hard

• Called a "shell" in Chinese

How simple packers work







General unpacking theory



8

Part 2: What is ImpREC?

- 32-bit only imports rebuilder
- Saves a lot of time over the manual rebuilding method
- Wasn't designed to deal with "features" of Vista
- No documentation or source code was available
- It did its job really well though

Part 2: What is ImpREC?

| At | tach to an Active Process | |
|---------------------------------|----------------------------|---------------|
| | | Pick DLL |
| Imported Fur | nctions Found | 1.17 |
| | | Show Invalid |
| | | |
| | | Show Suspect |
| | | Auto Trace |
| | | L Auto made |
| | | Clear Imports |
| | | |
| L | og | |
| | | ClearLog |
| | | |
| | | |
| IAT Infos needed | | Options |
| OEP 00000000 IAT AutoSearch | BVA 00000000 Size 00000000 | |
| | | About |
| 117A 1000000 312E 100001000 | Add new section | Exit |
| Load Tree Save Tree Get Imports | Fix Dump | |

10 © nCircle 2010 All rights reserved.

Why do this project?

- ImpREC was getting older.
- There were no public 64-bit imports rebuilder freely available on the internet at the time.
- Some functionality was missing (process dumper)
- I was curious.

I am a reverser. It's what I do.

Got tired of waiting for somebody else to do it.
 So I made it by myself.



Part 3: What is CHimpREC?

- 32 and 64-bit imports rebuilder
- Improved version of ImpREC
- Fixes many existing bugs
- Introduces new features
- Made especially for WoW64 compatibility
- Allows for an all-in-one version
- Chinese version available (unexpectedly)
- Done entirely through black box reverse-engineering
- Done by making up equivalent operations that yield exactly the same results in all possible scenarios

Part 3: What is CHimpREC?



n Cırcle°

What is CHimpREC? (Chinese)



XP or Vista w/o ASLR

| 🔮 Import REConstructor 🖬 .6 FINAL (C) 2001-2003 MackT/uCF | _ 🗆 🗙 |
|--|---------------|
| Attach to an Active Process | |
| c:\program files\mozilla firefox\firefox.exe (00000718) | Pick DLL |
| Imported Functions Found | |
| IT: advapi32.dll FThunk:004AA000 NbFunc:11 (decimal:17) valid:YES | Show Involid |
| ⊕ gdi32.dll FThunk:004AA048 NbFunc:51 (decimal:81) valid:YES | Show mvaliu |
| 🗄 kernel32.dll FThunk:004AA190 NbFunc:43 (decimal:67) valid:YES | Show Suspect |
| 🗄 ·· msvcrt.dll FThunk:004AA2A0 NbFunc:69 (decimal:105) valid:YES | |
| 🖶 · oleaut32.dll FThunk:004AA448 NbFunc:16 (decimal:22) valid:YES | |
| i≣∾ shell32.dll FThunk:004AA4A4 NbFunc:7 (decimal:7) valid:YES | Auto Trace |
| ⊕ user32.dll FThunk:004AA4C4 NbFunc:8C (decimal:140) valid:YES | |
| tersion.dll FThunk:004AA6F8 NbFunc:3 (decimal:3) valid:YES | Clear Imports |
| I I I winspool.drv FT hunk:004AA708 NbFunc:4 (decimal:4) valid:YES | |
| Log | |
| rva:0044A268 forwarded from mod:ntdll.dll.ord:013D.name:BtlBestoreLastWin32Error | |
| rva:004AA280 forwarded from mod:ntdll.dll ord:021E name:RtlDeleteCriticalSection | |
| Construction of the second sec | Clear Log |
| 14 (decimal: 20) valid module(s) (added: +14 (decimal: +20)) | |
| 7D7 (decimal:2007) imported function(s). (added: +7D7 (decimal:+2007)) | |
| | Options |
| IAT Infos needed New Import Infos (IID+ASCII+LOADER) | |
| 0EP 004A66CC IAT AutoSearch RVA 00000000 Size 0001203E | |
| | About |
| RVA 1004A4000 Size 100001FAC | |
| Load Tree Save Tree Get Imports Fix Dump | |
| | |

Vista ASLR

| MarkT/uCF | |
|---|---------------|
| Attach to an Active Proce | |
| c:\program files (x86)\mozilla firefox\firefox.exe (00000384) | Pick DLL |
| Imported Functions Found | |
| E = advapi32.dll F i nunk:0056D000 NDFunc:E (decima: 14) valid:YES A | Show Invalid |
| | Show Suspect |
| ⊕ oleaut32.dll FThunk:0056D4F0 NbFunc:16 (decimal:22) valid | |
| the shell32.dll FThunk:0056D54C NbFunc:C (decimal:12) valid: | Auto Trace |
| 🗄 🤄 ? FThunk:0056D580 NbFunc:8F (decimal:143) valid:ND | |
| ⊕ version.dll FThunk:0056D7C0 NbFunc:3 (decimal:3) valid:YES | Clear Importe |
| I I IIII IIIII IIIIIIIIIIIIIIIIIIIIII | clear imports |
| Log | |
| IAT read successfully. | |
| Constituents | ClearLog |
| 11 (decimal: 17) valid module(s) | |
| 898 (decimal: 2200) imported function(s). | |
| [EF [decimal:239] unresolved pointer(s)] | |
| IAT Infos needed New Import Infos (IID+ASCII+LOADER) | Options |
| UEP 0005690C2 IAT AutoSearch RVA 00000000 Size 0000EA9C | About |
| RVA 0056D000 Size 00002280 | About |
| | Exit |
| Load Tree Get Imports Fix Dump | |
| | |

16 © nCircle 2010 All rights reserved.

Vista ASLR

| MarkT/uCF | |
|--|---------------|
| Attach to an Active Process | |
| c:\program files (x86)\mozilla firefox\firefox.exe (00000384) | Pick DLL |
| | |
| Imported Functions Found | |
| ···· rva:0056D278 mod:ker 22 dll and 01E4 name: CatEullPathNameW | Show Invalid |
| m rva:UU56D/27C mod:K | |
| ······································ | Show Suspect |
| | |
| rva:0056D/28C mod:kernel32 dll ord:02C9 name:InterlockedIncrement | Auto Trace |
| rva:0056D 290 pt: 778035C0 | |
| - rva:0056D294 mod:kernel32.dll ord:0257 name:GetSystemTimeAsFileTime | |
| rva:0056D298 mod:kernel32.dll ord:0442 name:TIsSetValue 🔹 | Clear Imports |
| | |
| Log | |
| IAT read successfully. | |
| Current imports: | Clear Log |
| 11 (decimal:17) valid module(s) (added: +11 (decimal:+17)) | |
| 898 (decimal: 2200) imported function(s). (added: +898 (decimal: +2200)) | |
| LEF (decimal:239) unresolved pointer(s)) (added: +EF (decimal:+239)) | |
| IAT Infos needed | Options |
| | |
| RVA UUUUUUUUU Size UUUUEASC | About |
| RVA 0056D000 Size 00002280 | |
| | Exit |
| Load Tree Get Imports Fix Dump | |
| | |

Vista ASLR

GDI32

KERNEL32

USER32

| 국 gdi32.dll 국 gdi32.dll 국 gdi32.dll 국 gdi32.dll | 77F10000 77F11000 77F53000 77F54000 | 77F11000 77F53000 77F54000 77F57000 | R R . X R W R | D . D . D . D . | ə kernel32.dll ə kernel32.dll ə kernel32.dll ə kernel32.dll | 7C800000 7C801000 7C883000 7C886000 | 7C801000 7C883000 7C886000 7C888000 7C888000 | R R . X R W R W | D. D. D. D. | - ar user32.dll - ar user32.dll - ar user32.dll - ar user32.dll - ar user32.dll - ar user32.dll | 77D 40000 77D 41000 77D A0000 77D A1000 77D A2000 | 77D41000 77DA0000 77DA1000 77DA2000 | R R . X R W R W | D. D. D. D. |
|--|--|--|------------------------|--------------------------|--|--|--|--------------------------|----------------------|--|---|--|--------------------------|----------------------|
| _ | | | | | | 1000000 | 10014000 | | υ. | | 7050000 | 70501000 | | - |
| 🗗 gdi32.dll | 77100000 | 77101000 | R | D . | 🗗 kernel 32. dll | 76590000 | 76591000 | R | D. | ⊟Puser32.dll | 76F80000 | 76F81000 | н | , D |
| 🗗 gdi32.dll | 77110000 | 77157000 | R. X | D. | 🗗 kernel32.dll | 765A0000 | 76665000 | в. X | D. | Huser32.dll | 76F90000 | 76FFD000 | н. х | . U |
| 🗇 gdi32.dll | 77160000 | 77162000 | RW. | D. | 🗇 kernel32.dll | 76670000 | 76673000 | RW. | D. | 🗗 user32.dll | 77000000 | 77002000 | RW. | D |
| 🗇 gdi32.dll | 77170000 | 77171000 | Β | D . | न kernel 32. dll | 76680000 | 76681000 | Β | D . | 🗇 user32.dll | 77010000 | 7703E000 | Β | D |
| 🗇 odi32.dll | 77180000 | 77182000 | B | D . | 🗇 kemel32.dll | 76690000 | 7669A000 | B | D . | 🗇 user32.dll | 77040000 | 77044000 | Β | D |



Buffer Overflow Vulnerabilities

| Image Base Image Base Image Base I | CHimpREC - IT Underg | Attach to an Active Process | |
|--|------------------------------|------------------------------|----------------|
| Import EDITOR Image Base Current implication 1 (decimal: 2 (decimal: 0 (decimal: 0 (decimal: <td>dlloader.ex</td> <td></td> <td></td> | dlloader.ex | | |
| Image Base Original IAT IAT read su Current imp 1 (decimal: 0 (decimal: | IMPO | RT EDITOR | |
| Image Base Original IAT Original IAT AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA | ⊡•kernel3 | | Dump |
| Image Base Original IAT Original IAT IMAL IAT readsu IMAL Current imp 1 (decimal: 2 (decimal: IMAL 0 (decimal: IMAL 0 (decimal: IMAL 0 (decimal: IMAL | <mark>rva</mark> : | | |
| Image Base Get Imports Original IAT Fix Dump IAT read st Clear Imports Current imp (decimal: 0 (decimal: AAAAAAAAAAAAAAAAAAAAAAAAAAAAAA 0 (decimal: OU0002062 0K Cancel | ···· rva: | | IAT AutoSearch |
| Image Base Show Invalid Image Base Fix Dump Original IAT Clear Imports IAT read su Clear Log Outcomain Options AAAAAAAAAAAAAAAAAAAAAAAAAAAA About Exit Exit | | | Get Imports |
| Image Base Original IAT IAT read su Current imp 1 (decimal: 2 (decimal: 0 (decimal: | | | Show Invalid |
| Image Base Original IAT Original IAT IAT read su Current imp 1 (decimal: 2 (decimal: AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA | | | Fix Dump |
| Image Base Original IAT IAT read su Current imp 1 (decimal: 2 (decimal: AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA | | | |
| Original IAT IAT read su Imports Clear Log Current imp 1 (decimal: 2 (decimal:) Imports Options Imports Options About Imports Imports Imports | Image Base | | |
| IAT read su Image: Clear Log Current imp 1 (decimal: 1 (decimal: AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA | Original IAT | | Clear Imports |
| Current imp 1 (decimal: 2 (decimal: 0 (decimal:) AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA | IAT read su | < | Clear Log |
| 2 (decimal: 0 (decimal:) 0 (de | Current imp 1 (decimal: 1 | | Options |
| 0 (declination 0 (decli | 2 (decimal: | ΑΔΑΔΑΔΑΔΑΔΑΔΑΔΑΔΑΔΑΔΑΔΑΔΑ | About |
| 00002062 OK Cancel | o (decimal.) | | Evit |
| | | 00002062 OK Cancel | |
| | | | |
| | OEP RVA: | | |
| | 00001000 | 100002062 10000008 100000052 | |





Buffer Overflow Vulnerabilities

| MarkT/uCF | |
|---|---------------|
| Attach to an Active Process | |
| c:\users\tiga\appdata\local\temp\rar\$ex57.093\dllloader.exe (00001434) | Pick DLL |
| Imported Functions Found | |
| | Show Invalid |
| | Show Suspect |
| Microsoft Windows | |
| ImportREC Wow64 ave has stopped working | Auto Trace |
| ImportKeC_wowo4.exe has stopped working | Clear Imports |
| A problem caused the program to stop working correctly. Windows will close the program and notify you if a solution is | |
| available. | |
| Module loaded: c: | Clear Log |
| Module loaded: c: Debug Close program | |
| Module loaded: c:\windows\syswow64\usp10.dll | |
| IAT Infos needed New Import Infos (IID+ASCII+LOADER) | Options |
| OEP 00000000 IAT AutoSearch RVA 00000000 Size 00000000 | About |
| RVA 00000000 Size 00001000 M Add new section | About |
| Load Tree Save Tree Get Imports Fix Dump | Exit |
| | |





Part 4: Inner workings of an import rebuilder

- API families: Toolhelp32 vs. PSAPI
- How planning efficiently can save time
- 5-steps of the process:
 - Dump
 - IAT AutoSearch
 - Get Imports (Unforwarding)
 - Show Invalid
 - Fix Dump



Toolhelp32 vs. PSAPI

- Toolhelp32 APIs
 - CreateToolhelp32Snapshot
 - Process32First
 - Process32Next
 - Module32First
 - Module32Next
 - ToolHelp32ReadProcessMemory



Toolhelp32 vs. PSAPI

- PSAPI APIs
 - EnumProcesses
 - EnumProcessModules
 - EnumProcessModulesEx
 - GetModuleInformation
 - GetModuleBaseName
 - GetModuleFileNameEx



Toolhelp32 vs. PSAPI

Windows Version Compatibility

| | 95 | 98 | Ме | NT4 | 2000 | 2003 | ХР | Vista |
|--------------------------|----|----|----|-----|------|------|----|-------|
| CreateToolhelp32Snapshot | Х | Х | Х | | Х | Х | Х | Х |
| EnumProcessModules | | | | Х | Х | Х | Х | Х |
| EnumProcessModulesEx | | | | | | | | Х |



How planning efficiently can save time

- 2 Single-Architecture versions (x86 OR x64)
 - To each his own
 - APIs: CreateToolhelp32Snapshot
 - Best OS compatibility range
 - Allows for common project source and headers
 - Coded in 32-bit then ported to 64-bit
- Cross-Architecture All-in-one version (x86 AND x64)

- Made from a different x64 project
- Requires 64-bit OS
- EnumProcessModules & Ex
- Runs on Vista x64 and Windows 7 only (not XP)

- Copying the memory area of a process to a file
- When the process has reached its Original Entry Point
- Each section is dumped individually
- Each section RawSize must be realigned from FileAlignment to SectionAlignment
- RawAddress matches VirtualAddress
- All sections are made writable by adding the flag:
 IMAGE_SCN_MEM_WRITE
- VirtualProtectEx to change the process memory to:
 PAGE_EXECUTE_READWRITE

Step 1: Dump

| Name | Virtual Size | Virtual Address | Raw Size | Raw Address | Reloc Address | Linenumbers | Relocations N | Linenumbers | Characteristics |
|---------|--------------|-----------------|----------|-------------|---------------|-------------|---------------|-------------|-----------------|
| | | | | | | | | | |
| Byte[8] | Dword | Dword | Dword | Dword | Dword | Dword | Word | Word | Dword |
| UPX0 | 00005000 | 00001000 | 0000000 | 00000400 | 0000000 | 0000000 | 0000 | 0000 | E0000080 |
| UPX1 | 00001000 | 00006000 | 00000600 | 00000400 | 0000000 | 0000000 | 0000 | 0000 | E0000040 |
| .rsrc | 00001000 | 00007000 | 00000200 | 00000A00 | 0000000 | 0000000 | 0000 | 0000 | C0000040 |



| Name | Virtual Size | Virtual Address | Raw Size | Raw Address | Reloc Address | Linenumbers | Relocations N | Linenumbers | Characteristics |
|---------|--------------|-----------------|----------|-------------|---------------|-------------|---------------|-------------|-----------------|
| | | | | | | | | | |
| Byte[8] | Dword | Dword | Dword | Dword | Dword | Dword | Word | Word | Dword |
| UPX0 | 00005000 | 00001000 | 00005000 | 00001000 | 0000000 | 0000000 | 0000 | 0000 | E0000080 |
| UPX1 | 00001000 | 00006000 | 00001000 | 00006000 | 0000000 | 0000000 | 0000 | 0000 | E0000040 |
| .rsrc | 00001000 | 00007000 | 00001000 | 00007000 | 0000000 | 0000000 | 0000 | 0000 | C0000040 |



• Binary search looking for indirect call opcodes:

- 8B0D MOV ECX,[ADDRESS]
- 8B15 MOV EDX,[ADDRESS]
- 8B1D MOV EBX,[ADDRESS]
- 8B25 MOV ESP,[ADDRESS]
- 8B2D MOV EBP,[ADDRESS]
- 8B35 MOV ESI,[ADDRESS]
- 8B3D MOV EDI,[ADDRESS]
- A1 MOV EAX,[ADDRESS]

- Binary search looking for direct call opcodes:
 - FF15 CALL [ADDRESS]
 - FF25 JMP [ADDRESS]
 - FF35 PUSH [ADDRESS]
- Binary search ignores relative calls in 32-bit
- Starting from ImageBase or EntryPoint
- Found call must lead to a valid import
- Search up for the beginning of the IAT
- Search down for the end of the IAT
- Just like trying to identify a weird object in the dark

| \times |
|----------|
|----------|

| | | | | | | public start | start proc ne | ar | | |
|----|----|----|----|----|----|-----------------|------------------|---------|-------|----------------|
| 6A | 00 | | | | | push | 0 | | : | 1pModuleName |
| E8 | 81 | 00 | 00 | 00 | | call | GetMo | duleHan | dleA | 1 |
| A3 | 04 | 30 | 40 | 00 | | mov | hInst | ance, e | ax | |
| 6A | 00 | | | | | push | 0 | | ; | dwInitParam |
| 68 | 29 | 10 | 40 | 00 | | push | offse | t Dialo | gFunc | ; 1pDialogFunc |
| 6A | 00 | | | | | push | 0 | | ī; | hWndParent |
| 6A | 65 | | | | | push | 65h | | ; | 1pTemplateName |
| FF | 35 | 04 | 30 | 40 | 00 | push | hInst | ance | ; | hInstance |
| E8 | 54 | 00 | 00 | 00 | | call | Dialo | gBoxPar | amA 👘 | |
| 6A | 00 | | | | | push | 6 | - | ; | uExitCode |
| E8 | 59 | 00 | 00 | 00 | | call | ExitP | rocess | | |
| | | | | | | start | endp | | | |
| | | | | | | | - | | | |



| .idata:00402000 | ; Imports from kernel32.dll |
|-----------------|---|
| .idata:00402000 | ; · · · |
| .idata:00402000 | |
| .idata:00402000 | |
| .idata:00402000 | ; Segment type: Externs |
| .idata:00402000 | ; idata |
| .idata:00402000 | ; HMODULE |
| .idata:00402000 | extrn imp_GetModuleHandleA:dword |
| .idata:00402000 | ; DATA XREF: GetModuleHandleA1r |
| .idata:00402004 | ; voidstdcall ExitProcess(UINT uExitCode) |
| .idata:00402004 | <pre>extrn imp_ExitProcess:dword ; DATA XREF: ExitProcess1r</pre> |
| .idata:00402008 | |
| .idata:0040200C | ; |
| .idata:0040200C | ; Imports from user32.dll |
| .idata:0040200C | ; |
| .idata:0040200C | ; BOOLstdcall EndDialog(HWND hDlg, INT_PTR nResult) |
| .idata:0040200C | <pre>extrnimp_EndDialog:dword ; DATA XREF: EndDialog¹r</pre> |
| .idata:00402010 | ; INT_PTRstdcall DialogBoxParamA(HINSTANCE hInstance, LPCSTR lpTemplateName, HWND hWndParent, |
| .idata:00402010 | extrnimp_DialogBoxParamA:dword |
| .idata:00402010 | ; DATA XREF: DialogBoxParamAîr |
| .idata:00402010 | |
| .rdata:00402014 | |



Step 3: Get Imports

• Identify the elements of the IAT in the specified range

- Exactly the contrary of GetProcAddress
- Using custom-made reusable functions:
 - GetProcModuleName
 - GetProcName
 - GetProcOrdinal
 - GetProcNameAndOrdinal
 - GetProcInfo
 - Unforward



- The Entry Point of the function is not code but a string
- Imports are forwarded for compatibility between all the different versions of Windows
- If an import can be unforwarded, it doesn't mean that it really was forwarded

- There are many false-positives
- Must analyze the context with some fuzzy logic
- Could be called guessing too

| MarkT/uCF | | | | | | |
|--|---------------|--|--|--|--|--|
| Attach to an Active Process | | | | | | |
| c:\program files (x86)\mozilla firefox\firefox.exe (000011D8) | Pick DLL | | | | | |
| Imported Functions Found | | | | | | |
| rva:0056D780 mod:user32.dll ord:0299 name:SetSysColors rva:0056D784 mod:user32.dll ord:02AC name:SetWindowTextA | Show Invalid | | | | | |
| rva:0056D788 mod:user32.dll ord:0120 name:GetDlgltem rva:0056D78C mod:user32.dll ord:011D name:GetDesktopWindow | Show Suspect | | | | | |
| rva:0056D790 mod:ntdll.dll ord:023D name:NtdllDefWindowProc_W rva:0056D794 mod:user32.dll ord:001E name:CallWindowProcW rva:0056D798 mod:user32.dll ord:02A6 name:SetWindowLongW | Auto Trace | | | | | |
| rva:0056D79C mod:user32.dll ord:0183 name:GetWindowLongW rva:0056D7A0 mod:user32.dll ord:0264 name:SendMessageW | Clear Imports | | | | | |
| Log | | | | | | |
| rva:0056D2C4 forwarded from mod:ntdll.dll ord:022A name:RtlAllocateHeap rva:0056D30C forwarded from mod:ntdll.dll ord:033D name:RtlDeleteCriticalSection | Clear Log | | | | | |
| Current imports: 13 (decimal: 19) valid module(s) (added: +13 (decimal:+19)) 898 (decimal: 2200) imported function(s). (added: +898 (decimal:+2200)) | | | | | | |
| IAT Infos needed New Import Infos (IID+ASCII+LOADER) | Options | | | | | |
| UEP U005690C2 IAT AutoSearch RVA 00000000 Size 0000F6EE RVA 0056D000 Size 00002280 Image: Add new section Image: Add new section | About | | | | | |
| Load Tree Save Tree Get Imports Fix Dump | Exit | | | | | |

n Cırcle°

| Ordinal | Function RVA | Name Ordinal | Name RVA | Name |
|--------------|--------------|--------------|----------|----------------|
| N/A | 000029DC | 00004106 | 00003608 | 0000500E |
| (nFunctions) | Dword | Word | Dword | szAnsi |
| 00000096 | 0001751E | 0095 | 00014BF0 | DefWindowProcA |
| 00000097 | 00017539 | 0096 | 00014BFF | DefWindowProcW |

user32.dll:76460000 assume cs:user32_dll
user32.dll:76460000 assume cs:user32_dll
user32.dll:76460000 ;org 76460000h
user32.dll:764774E8 aNtdll_ntdlld_1 db 'NTDLL.NtdllDialogWndProc_A',0
user32.dll:76477503 aNtdll_ntdlldia db 'NTDLL.NtdllDialogWndProc_A',0
user32.dll:7647751E aNtdll_ntdlldef db 'NTDLL.NtdllDefWindowProc_A',0
user32.dll:76477539 aNtdll_ntdlld_0 db 'NTDLL.NtdllDefWindowProc_W',0

.idata:0096D790 ; LRESULT __stdcall DefWindowProcW(HWND hWnd, UINT Msg, WPARAM wParam, LPARAM 1Param) .idata:0096D790 4D 3D 84 77 DefWindowProcW dd offset ntdll_Ntdl1DefWindowProc_W

False-positives

| xport | Viewer | |
|-------|---|---|
| | | _ |
| | firefox.exe (000011D8) | • |
| | shlwapi.dll | - |
| | Ordinal | * |
| | ord:0167 name: <none> address:0002526E - F - KERNEL32.OpenEventW</none> | |
| | ord:0169 name: <none>address:00025282 - F - KERNEL32.RemoveDirectoryW ord:0169 name:<none>address:0002529C - F - KERNEL32.GetShortPathNameW</none></none> | |
| | ord:016A name: <none> address:000252B7 - F - ADVAPI32.GetUserNameW</none> | |
| | ord:016B name: <none> address:00040897 ord:016C name:<none> address:00035E16</none></none> | |
| | ord:016D name: <none>address:00020A49</none> | |
| | ord:016E name: <none> address:000252CD - F - ADVAPI32.RegEnumValueW</none> | |
| | ord:0170 name: <none> address:0002532E4 = 1 = KERNEL32.GetPrivateProfileStru ord:0170 name:<none> address:00025308 - F - KERNEL32.GetPrivateProfileStru</none></none> | |
| | ord:0171 name: <none> address:0002532A - F - KERNEL32.CreateProcessW</none> | Ŧ |
| | < > | |
| | Evit | |
| | LXIL | |

n Cırcle°

Forwarding by ordinal

| xport Viewer | | | | |
|--|---|--|--|--|
| | | | | |
| firefox.exe (000011D8) | - | | | |
| shlwapi.dll | • | | | |
| Ordinal | * | | | |
| <pre>ord:0225 name:<none> address:00046B3B ord:0226 name:<none> address:000255EA - F - SHUNIMPL.#174 ord:0227 name:<none> address:000255F8 - F - SHUNIMPL.#175 ord:0228 name:<none> address:00025606 - F - SHUNIMPL.#176 ord:0229 name:IsInternetESCEnabled address:0003F81F ord:022A name:<none> address:00025614 - F - SHUNIMPL.#177 ord:022B name:<none> address:00025614 - F - SHUNIMPL.#178 ord:022B name:<none> address:00025624 - F - SHUNIMPL.#178 ord:022B name:<none> address:00025629 - F - SHUNIMPL.#178</none></none></none></none></none></none></none></none></pre> | | | | |
| ord:022C name: <none> address:0002563E - F - SHUNIMPL.#179 ord:022D name:<none> address:0002563E - F - SHUNIMPL.#180 ord:022E name:<none> address:0002564C - F - SHUNIMPL.#181 ord:022F name:<none> address:000185D9</none></none></none></none> | + | | | |
| Exit | F | | | |

37 © nCircle 2010 All rights reserved.

n Cırcle°

Step 4: Show Invalid

- Display unidentified IAT entries
- Text search through the interface
- Check all imports one by one for validity

n Cırcle[°]

• Simplest step to implement

Step 5: Fix dump

- Recreate the Import Directory to satisfy the loader
- Restore the original IAT
- Assemble structures that point to each other
 - IMAGE_IMPORT_DESCRIPTOR
 - IMAGE_IMPORT_BY_NAME
- Like gears in a clock



Changes from PE to PE32+ format

- All registers extended to QWORDs
 - EAX -> RAX
 - ESP -> RSP
- New registers
 - R8X-R15X
- All DLLs used must be 64-bit
- BaseOfData has disappeared
- New calling convention for APIs



Changes in the imports rebuilding process

- IAT elements are QWORDs
- Pointer to Original First Thunk is a QWORD
- ImageBase is a QWORD
- Exception Handlers are now stored as structures in the new PE32+ Exception Directory

Part 5: Live 64-bit unpacking session

- Tools used:
 - IDA Pro Advanced 64
 - CHimpREC-64
- Example: MPRESS 1.07
 - Simple UPX-like packer



Do you have any questions?

n C I r c l e°

© nCircle 2010. All rights reserved.

For more information or the full deck of slides, come see me at the nCircle booth.

n C I r c l e°

© nCircle 2010. All rights reserved.