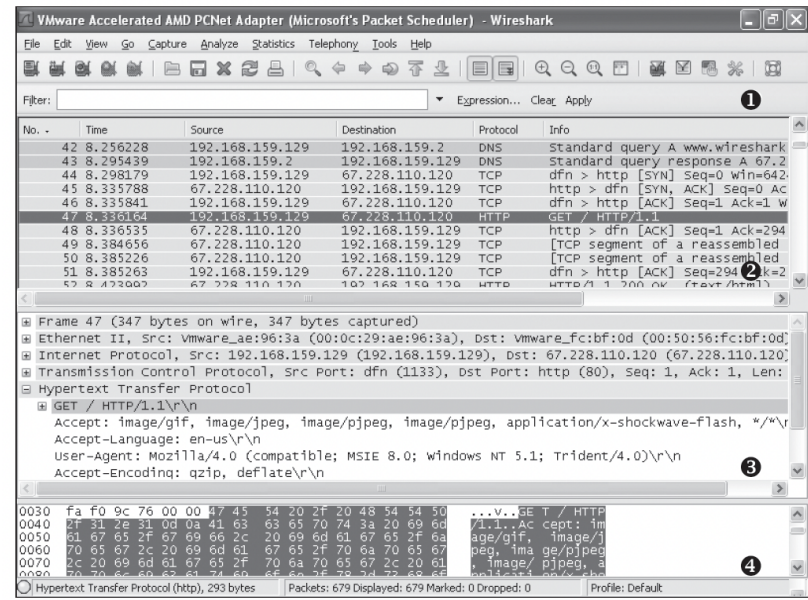


Practical Malware Analysis

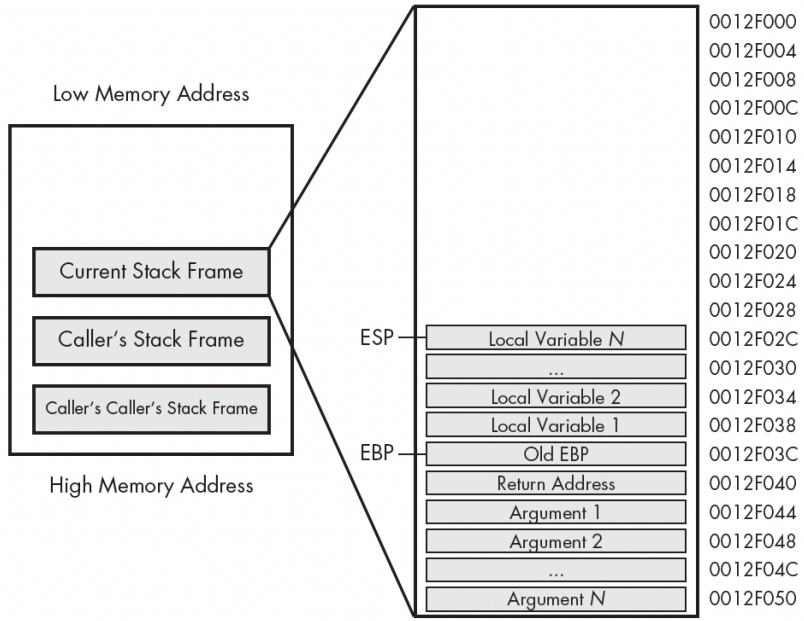
The Hands-On Guide to Dissecting Malicious Software

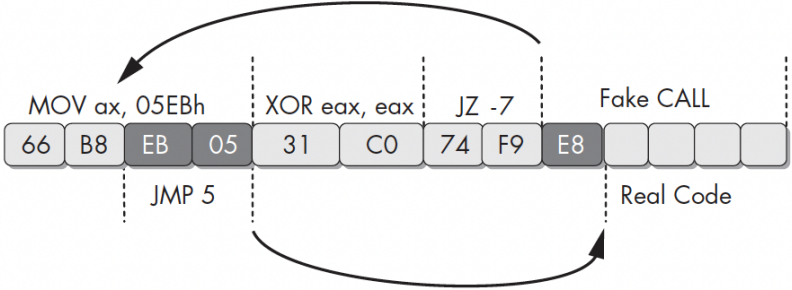
by Michael Sikorski & Andrew Honig

errata updated to print 16

Page	Error	Correction	Print corrected
10	373e7a863a1a345c60edb9e20ec3231	373e7a863a1a345c60edb9e20ec3231 ¹	Print 2
54	Figure replacement	 <p>Figure 3-10: Wireshark DNS and HTTP example</p>	Print 6

Page	Error	Correction	Print corrected
66	Figure replacement	<p>Malware Author High-Level Language</p> <pre>int c; printf("Hello.\n"); exit(0);</pre> <p>Compiler</p> <p>CPU Machine Code</p> <pre>55 8B EC 8B EC 40</pre> <p>Disassembler</p> <p>Malware Analyst Low-Level Language</p> <pre>push ebp mov ebp, esp sub esp, 0x40</pre> <p><i>Figure 4-1: Code level examples</i></p>	Print 2
74	... instruction such as <code>lea ebx, [eax*5+5]</code> , where <code>eax</code> is a number, rather than a memory address. This instruction is the functional equivalent of <code>ebx = (eax+1)*5</code> , but the former is shorter or more efficient for the compiler to use instead of a total of four instructions (for example <code>inc eax; mov ecx, 5; mul ecx; mov ebx, eax</code>).	... instruction such as <code>lea ebx, [eax*4+4]</code> , where <code>eax</code> is a number, rather than a memory address. This instruction is the functional equivalent of <code>ebx = (eax+1)*4</code> , but the former is shorter or more efficient for the compiler to use instead of a total of four instructions (for example <code>inc eax; mov ecx, 4; mul ecx; mov ebx, eax</code>).	Print 14
76	The instruction <code>nop</code> is actually a pseudonym for <code>xchg eax, eax</code> ...	The instruction <code>nop</code> is actually a pseudonym for <code>xchg eax, eax</code> ...	Print 7

Page	Error	Correction	Print corrected
79	Figure replacement	 <p>Figure 4-8: Individual stack frame</p>	Print 8
82	This works in the same way as cmpsb, but it compares the byte located at address ESI to AL, rather than to EDI .	This works in the same way as cmpsb, but it compares the byte located at address EDI to AL, rather than to ESI .	Print 8
84	Table 4-12	Listing 4-2	Print 10
101, 102	<pre>printf("total = %d\n", x);</pre>	<pre>printf("Total = %d\n", x);</pre>	Print 4
111, 112	<pre>00401006 mov dword ptr [ebp-4], 0 0040100D mov dword ptr [ebp-8], 1</pre>	<pre>00401006 mov dword ptr [ebp-4], 1 0040100D mov dword ptr [ebp-8], 2</pre>	Print 2
148	The lpStartupInfo structure for the process stores the standard output ❶, standard input ❷, and standard error ❸ that will be used for the new process.	The lpStartupInfo structure for the process stores the standard output ❷, standard input ❸, and standard error ❶ that will be used for the new process.	Print 2
178	... and 0x41100 1 if the language is Chinese.	... and 0x41100 A if the language is Chinese.	Print 7
258	<pre>CreateProcess(...,"svchost.exe",...,CREATE_SUSPEND,...);</pre>	<pre>CreateProcess(...,"svchost.exe",...,CREATE_SUSPENDED,...);</pre>	Print 2

Page	Error	Correction	Print corrected
263	Every thread has a queue of APCs attached to it, and these are processed when the thread is in an alertable state, such as when they call functions like WaitForSingleObjectEx, WaitForMultipleObjectsEx, and Sleep.	Every thread has a queue of APCs attached to it, and these are processed when the thread is in an alertable state, such as when they call functions like WaitForSingleObjectEx, WaitForMultipleObjectsEx, and Sleep Ex .	Print 2
263	<pre>cbuf = f.read()</pre>	<pre>cbuf = cfile.read()</pre>	Print 5
338	Figure replacement	 <p>Figure 15-5: Multilevel inward-jumping sequence</p>	Print 2
338	<pre>74 F9 jz short near ptr sub_4011C0+1</pre>	<pre>74 FA jz short near ptr sub_4011C0+2</pre>	Print 2
339	<pre>F9 db 0F9h</pre>	<pre>FA db 0FAh</pre>	Print 2
363	Because INT 0x2D is the way that kernel debuggers set breakpoints, the method shown in Listing 16-10 applies.	Because INT 0x2D is the way that kernel debuggers set breakpoints, the method shown in Listing 16-9 applies.	Print 2
376	0x5668 (vx)	0x5658 (vx)	Print 14
440	3. At 0x4036F0, there is a function call that takes the string Config error, followed a few instructions later by a call to CxxThrowException.	3. The function 0x4036F0 is called multiple times and each time it takes the string Config error, followed a few instructions later by a call to CxxThrowException.	Print 6
447	\WOW64	\SysWOW64	Print 12
448	C:\Windows\WOW64	C:\Windows\SysWOW64	Print 12
471	URL update	You can download PEview from http://wjradsburn.com/software/	Print 2
499	View ► Graphs ► Xrefs From	View ► Graphs ► User Xrefs Chart	Print 2
514	If the call fails, the program exits.	If the call succeeds, the program exits.	Print 2

Page	Error	Correction	Print corrected
523	... if so, it calls the Sleep function to sleep for 60 seconds.	... if so, it calls the Sleep function to sleep for about 394 seconds.	Print 6
533	<i>If you perform a full analysis of 0x4025120...</i>	<i>If you perform a full analysis of 0x402510...</i>	Print 7
649	The two functions (sub_401 2F2 and sub_4013 69)...	The two functions (sub_401 30F and sub_4013 86)...	Print 2
675	The malware is querying the I/O communication port (0x56 68)...	The malware is querying the I/O communication port (0x56 58)...	Print 14
680	... as described in “Searching for Vulnerable Instructions” on page 67 0 as described in “Searching for Vulnerable Instructions” on page 67 8 .	Print 6