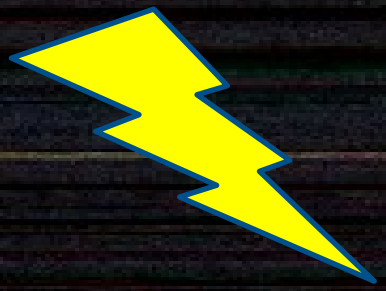
Debugging TV

Frame 0x01

Presenter: Dmitry Vostokov



TestWER.exe.2356.dmp

```
10000011 11000100 00000100 11000010 00010100 00000000 10010000 10111000
01011001 00000000 00000000 00000000 00110011 11001001 10001101 01010100
00100100 00000100 01100100 11111111 00010101 11000000 00000000 00000000
00000000 10000011 11000100 00000100 11000010 00010000 00000000 10111000
01011010 00000000 00000000 00000000 00110011 11001001 10001101 01010100
00100100 00000100 01100100 11111111 00010101 11000000 00000000 00000000
00000000 10000011 11000100 00000100 11000010 00001000 00000000 10111000
01011011 00000000 00000000 00000000 00110011 11001001 10001101 01010100
00100100 00000100 01100100 11111111 00010101 11000000 00000000 00000000
00000000 10000011 11000100 00000100 11000010 00010000 00000000 10111000
01011100 00000000 00000000 00000000 00110011 11001001 10001101 01010100
00100100 00000100 01100100 11111111 00010101 11000000 00000000 00000000
00000000 10000011 11000100 00000100 11000010 00010100 00000000 10111000
01011101 00000000 00000000 00000000 00110011 11001001 10001101 01010100
00100100 00000100 01100100 11111111 00010101 11000000 00000000 00000000
00000000 10000011 11000100 00000100 11000010 00011000 00000000 10111000
01011110 00000000 00000000 00000000 10111001 00000111 00000000 00000000
00000000 10001101 01010100 00100100 00000100 01100100 11111111 00010101
```

http://support.citrix.com/article/CTX111901

Σψμβολσ

```
0:000> k
ChildEBP RetAddr
WARNING: Stack unwind information not available. Following frames may be wrong.
0018f234 76ce162d ntdll!NtWaitForMultipleObjects+0x15
0018f27c 76ce1921 kernel32!WaitForMultipleObjectsEx+0x8e
0018f298 76d09b2d kernel32!WaitForMultipleObjects+0x18
0018f304 76d09bca kernel32!CheckForReadOnlyResource+0x175
0018f318 76d098f8 kernel32!CheckForReadOnlyResource+0x212
0018f328 76d09875 kernel32!UnhandledExceptionFilter+0x163
0018f3b4 77bc0df7 kernel32!UnhandledExceptionFilter+0xe0
0018ffd4 77b89ed5 ntdll!RtlKnownExceptionFilter+0xb7
0018ffec 00000000 ntdll!RtlInitializeExceptionChain+0x36

0:000> !teb
TEB at 7efdd000
************************************************************************
***                                                                  ***
***                                                                  ***
***    Your debugger is not using the correct symbols                ***
***                                                                  ***
***    In order for this command to work properly, your symbol path  ***
***    must point to .pdb files that have full type information.     ***
***                                                                  ***
***    Certain .pdb files (such as the public OS symbols) do not     ***
***    contain the required information.  Contact the group that     ***
***    provided you with these symbols if you need this command to   ***
***    work.                                                         ***
***                                                                  ***
***    Type referenced: nt!_TEB                                      ***
***                                                                  ***
************************************************************************
error InitTypeRead( TEB )...
```

```
Symbols from PE tables:

...
symbolA                    address1
symbolB                    address2
CheckForReadOnlyResource   76d099b8
...

0:000> x kernel32!CheckForReadOnlyResource
76d099b8 kernel32!CheckForReadOnlyResource
(<no parameter info>)
0:000> ? 76d099b8+175
Evaluate expression: 1993382701 = 76d09b2d
0:000> ln 76d09b2d
(76d099b8)
kernel32!CheckForReadOnlyResource+0x175   |
(76d09daa)
kernel32!GetThreadSelectorEntry
```

Symβολσ

```
0:000> .symfix c:\mss
0:000> .reload
.....................
0:000> k
ChildEBP RetAddr
0018f198 75670bdd ntdll!NtWaitForMultipleObjects+0x15
0018f234 76ce162d KERNELBASE!WaitForMultipleObjectsEx+0x100
0018f27c 76ce1921 kernel32!WaitForMultipleObjectsExImplementation+0xe0
0018f298 76d09b2d kernel32!WaitForMultipleObjects+0x18
0018f304 76d09bca kernel32!WerpReportFaultInternal+0x186
0018f318 76d098f8 kernel32!WerpReportFault+0x70
0018f328 76d09875 kernel32!BasepReportFault+0x20
0018f3b4 77bc0df7 kernel32!UnhandledExceptionFilter+0x1af
0018f3bc 77bc0cd4 ntdll!__RtlUserThreadStart+0x62
0018f3d0 77bc0b71 ntdll!_EH4_CallFilterFunc+0x12
0018f3f8 77b96ac9 ntdll!_except_handler4+0x8e
0018f41c 77b96a9b ntdll!ExecuteHandler2+0x26
0018f4cc 77b6010f ntdll!ExecuteHandler+0x24
0018f4cc 0041ff21 ntdll!KiUserExceptionDispatcher+0xf
*** ERROR: Module load completed but symbols could not be loaded for TestWER.exe
WARNING: Stack unwind information not available. Following frames may be wrong.
0018f850 00403620 TestWER+0x1ff21
0018f860 0040382f TestWER+0x3620
0018f890 00402df6 TestWER+0x382f
0018f8b4 00409ef8 TestWER+0x2df6
[...]
0018ff88 76ce3677 TestWER+0xfc3e
0018ff94 77b89f02 kernel32!BaseThreadInitThunk+0xe
0018ffd4 77b89ed5 ntdll!__RtlUserThreadStart+0x70
0018ffec 00000000 ntdll!_RtlUserThreadStart+0x1b
```

Compare before and after MSS:

```
0:000> x kernel32!*
[...]
0:000> .symfix c:\mss
0:000> .reload
.....................
0:000> x kernel32!*
[...]
```

Symbols

```
0:000> .sympath+ C:\TestWER\x86
Symbol search path is: srv*;C:\TestWER\x86
Expanded Symbol search path is: SRV*c:\mss*http://msdl.microsoft.com/download/symbols;c:\testwer\x86

0:000> .reload
.....................

0:000> kL
ChildEBP RetAddr
0018f198 75670bdd ntdll!NtWaitForMultipleObjects+0x15
0018f234 76ce162d KERNELBASE!WaitForMultipleObjectsEx+0x100
0018f27c 76ce1921 kernel32!WaitForMultipleObjectsExImplementation+0xe0
0018f298 76d09b2d kernel32!WaitForMultipleObjects+0x18
0018f304 76d09bca kernel32!WerpReportFaultInternal+0x186
0018f318 76d098f8 kernel32!WerpReportFault+0x70
0018f328 76d09875 kernel32!BasepReportFault+0x20
0018f3b4 77bc0df7 kernel32!UnhandledExceptionFilter+0x1af
0018f3bc 77bc0cd4 ntdll!__RtlUserThreadStart+0x62
0018f3d0 77bc0b71 ntdll!_EH4_CallFilterFunc+0x12
0018f3f8 77b96ac9 ntdll!_except_handler4+0x8e
0018f41c 77b96a9b ntdll!ExecuteHandler2+0x26
0018f4cc 77b6010f ntdll!ExecuteHandler+0x24
0018f4cc 0041ff21 ntdll!KiUserExceptionDispatcher+0xf
0018f850 00403620 TestWER!CTestDefaultDebuggerDlg::OnBnClickedButton1+0xb1
0018f860 0040382f TestWER!_AfxDispatchCmdMsg+0x45
0018f890 00402df6 TestWER!CCmdTarget::OnCmdMsg+0x11c
0018f8b4 00409ef8 TestWER!CDialog::OnCmdMsg+0x1d
[...]
0018ff88 76ce3677 TestWER!__tmainCRTStartup+0x112
0018ff94 77b89f02 kernel32!BaseThreadInitThunk+0xe
0018ffd4 77b89ed5 ntdll!__RtlUserThreadStart+0x70
0018ffec 00000000 ntdll!_RtlUserThreadStart+0x1b
```

Compare before and after loading TestWER PDB file:

```
0:000> x TestWER!*
[...]
0:000> .sympath+ C:\TestWER\x86
0:000> .reload
.....................
0:000> x TestWER!*
[...]
```

Symβols

```
0:000> !teb
TEB at 7efdd000
    ExceptionList:        0018f224
    StackBase:            00190000
    StackLimit:           0018d000
[...]

0:000> dps 0018d000 00190000
0018d000  00000000
[...]
0018deec  00000000
0018def0  7524a010 CRYPTBASE!g_AesCtrSafeCtx+0x924
0018def4  0018df0c
[...]
0018df04  0018df24
0018df08  77b7fa19 ntdll!LdrpFindLoadedDllByName+0x68
0018df0c  0018e004
[...]

0:000> ub 7524a010
CRYPTBASE!g_AesCtrSafeCtx+0x914:
7524a000 0000            add     byte ptr [eax],al
7524a002 0000            add     byte ptr [eax],al
7524a004 0000            add     byte ptr [eax],al
7524a006 0000            add     byte ptr [eax],al

0:000> ub 77b7fa19
ntdll!LdrpFindLoadedDllByName+0x77:
[...]
77b7fa10 50              push    eax
77b7fa11 ff7508          push    dword ptr [ebp+8]
77b7fa14 e8faedffff      call    ntdll!RtlEqualUnicodeString (77b7e813)
```

```
* ASCII or UNICODE fragments *
[...]
0018f6f4  00000000
0018f6f8  00000000
0018f6fc  00000000
0018f700  9f43baaa
0018f704  678f805c
0018f708  00010010
0018f70c  00000000
0018f710  006f0043
0018f714  00720072
0018f718  00630065
0018f71c  00690074
0018f720  00000000
0018f724  00000000
[...]

0:000> du 0018f710
0018f710  "Correcti"
```

Patterns

No Component Symbols

Coincidental Symbolic Information

Incorrect Symbolic Information

Debugging.TV