Debugging.TV

Frame 0x07

Presenter: Dmitry Vostokov

Sponsors

Topics

- Detecting corruption in executable modules
- Aliases
- Image paths
- Troubleshoting image path problems
- When we need image paths?

Checking an Image

```
1: kd> !chkimg -d -v nt
Searching for module with expression: nt
Unable to open image file: C:\Program Files (x86)\Debugging Tools for Windows
(x86)\sym\ntkrpamp.exe\4549AE003a1000\ntkrpamp.exe
The system cannot find the file specified.

Error for nt: Could not find image file for the module. Make sure binaries are included in the symbol path.

1: kd> .sympath
Symbol search path is: srv*
Expanded Symbol search path is: SRV*c:\mss*http://msdl.microsoft.com/download/symbols

1: kd> .exepath+ SRV*c:\mss*http://msdl.microsoft.com/download/symbols
Executable image search path is: SRV*c:\mss*http://msdl.microsoft.com/download/symbols
Expanded Executable image search path is: srv*c:\mss*http://msdl.microsoft.com/download/symbols

1: kd> !chkimg -d -v nt
[...]
Scanning section:    .text
Size: 936109
Range to scan: 81801000-818e58ad
    81854019 - nt!PsGetCurrentProcess
               [ 64:24 ]
Total bytes compared: 936109(100%)
Number of errors: 1
[...]
```

Aliases

```
1: kd> !for_each_module al
  Alias            Value
  -------          -------
 $CurrentDumpArchiveFile
 $CurrentDumpArchivePath
 $CurrentDumpFile K:\AWMDA-Dumps\32-bit\Kernel\MEMORY-CodeOverwrite.DMP
 $CurrentDumpPath K:\AWMDA-Dumps\32-bit\Kernel
 $lowrite         C:\Users\Administrator\AppData\Local\Temp\Low
 $ntdllnsym
 $ntdllsym
 $ntdllwsym
 $ntnsym          nt
 $ntsym           nt
 $ntwsym
 $tmpwrite        C:\Users\ADMINI~1\AppData\Local\Temp
 @#Base           80200000
 @#Checksum       0000a38f
 @#End            8020a000
 @#FileDescription
 @#FileVersion
 @#Flags          00000004
 @#ImageName      \SystemRoot\system32\DRIVERS\BATTC.SYS
 @#ImageNameSize  00000027
 @#LoadedImageName
 @#LoadedImageNameSize 00000001
 @#MappedImageName
 @#MappedImageNameSize 00000001
 @#ModuleIndex    00
 @#ModuleName     BATTC
 @#ModuleNameSize 00000006
 @#ProductVersion
 @#Size           0000a000
 @#SymbolFileName BATTC.SYS
 @#SymbolFileNameSize 0000000a
 @#SymbolType     5
 @#TimeDateStamp  4549adb4
[...]
```

Checking All Modules

```
1: kd> !for_each_module -d -v @#ModuleName

[...]

Searching for module with expression: nt
Will apply relocation fixups to file used for comparison
Will ignore NOP/LOCK errors
Will ignore patched instructions
Image specific ignores will be applied
Comparison image path: C:\Program Files (x86)\Debugging Tools for Windows (x86)\sym\ntkrpamp.exe\4549AE003a1000\ntkrpamp.exe
No range specified

Scanning section:    .text
Size: 936109
Range to scan: 81801000-818e58ad
    81854019 - nt!PsGetCurrentProcess
               [ 64:24 ]
Total bytes compared: 936109(100%)
Number of errors: 1

[...]
```

Commands and Aliases

```
.exepath                    !chkimg

!for_each_module            @#ModuleName

al                          .sympath
```

!Ad Hardcore Technical Support Training

April 11-16, 2012: Accelerated Windows Memory Dump Analysis

April 20-23, 2012: Advanced Windows Memory Dump Analysis

April 27-30, 2012: Accelerated Software Trace Analysis

Forthcoming: Accelerated Mac OS X Core Dump Analysis

Training Schedule

Debugging.TV