



Debugging.TV

Frame 0x1C

Presenter: Dmitry Vostokov

SOFTWARE DIAGNOSTICS SERVICES

www.PatternDiagnostics.com

Including Memory Dump and Software Trace Analysis Audit, Seminars,
Certification and Training

Sponsors

OPENTASK
Iterative and Incremental Publishing

A world map in shades of blue and black, serving as a background for the Opentask logo.

Topics

- The life without LSASS
- Fibre bundle memory dumps
- Zero threads on Windows 8.1
- Windows 8.1 File Explorer threads

Fibre Bundle

Kernel Virtual Space

Process Virtual User Space

Process Virtual User Space

Process Virtual User Space

Process Virtual User Space

Zero Threads

THREAD fffffe000006f4880 Cid 0214.063c Teb: 00007ff70c1a4000 Win32Thread: 0000000000000000 WAIT: (Suspended) KernelMode Non-Alertable

SuspendCount 1

```
fffffe000006f4b60 NotificationEvent
Not impersonating
DeviceMap fffffc00001c145c0
Owning Process fffffe000021fd900 Image: explorer.exe
Attached Process N/A Image: N/A
Wait Start TickCount 255497 Ticks: 32955 (0:00:08:34.921)
Context Switch Count 2 IdealProcessor: 0
UserTime 00:00:00.000
KernelTime 00:00:00.000
Win32 Start Address 0x00007ffe14aed6bc
Stack Init fffffd00022119dd0 Current fffffd00022119500
Base fffffd0002211a000 Limit fffffd00022114000 Call 0
Priority 10 BasePriority 8 UnusualBoost 0 ForegroundBoost 0 IoPriority 2 PagePriority 5
Child-SP RetAddr Call Site
ffffd000`22119540 fffff802`c572c90e nt!KiSwapContext+0x76
ffffd000`22119680 fffff802`c572c3a7 nt!KiSwapThread+0x14e
ffffd000`22119720 fffff802`c56c39a8 nt!KiCommitThreadWait+0x127
ffffd000`22119780 fffff802`c577ce64 nt!KeWaitForSingleObject+0x248
ffffd000`22119820 fffff802`c572e289 nt!KiSchedulerApc+0x94
ffffd000`22119880 fffff802`c57daa23 nt!KiDeliverApc+0x209
ffffd000`22119900 fffff802`c5ac325c nt!KiApcInterrupt+0xc3 (TrapFrame @ fffffd000`22119900)
ffffd000`22119a90 fffff802`c57dc3f5 nt!PspUserThreadStartup+0x18
ffffd000`22119b00 fffff802`c57dc377 nt!KiStartUserThread+0x16
ffffd000`22119c40 00007ffe`1e2a43b4 nt!KiStartUserThreadReturn (TrapFrame @ fffffd000`22119c40)
00000000`0d49fcb8 00000000`00000000 0x00007ffe`1e2a43b4
```

74 Id: 214.63c Suspend: 1 Teb: 00007ff7`0c1a4000 Unfrozen

```
Child-SP RetAddr Call Site
00000000`0d49fcb8 00000000`00000000 ntdll!RtlUserThreadStart
```

When CPU Spike is Normal

```
T0:000> !runaway
```

```
User Mode Time
```

```
Thread      Time
44:1ec      0 days 0:00:20.312
32:790      0 days 0:00:02.640
```

```
[...]
```

```
0:000> ~44kc
```

```
Call Site
```

```
gdi32!NtGdiStretchBlt
gdi32!StretchBlt
GdiPlus!EpScanGdiDci::ProcessBatch_Gdi_Batch
GdiPlus!EpScanGdiDci::EmptyBatch
GdiPlus!EpScanBufferNative<unsigned long>::~EpScanBufferNative<unsigned long>
GdiPlus!DpDriver::FillPath
GdiPlus!DriverGdi::FillPath
GdiPlus!GpGraphics::DrvFillPath
GdiPlus!GpGraphics::RenderFillPath
GdiPlus!GpGraphics::FillPolygon
GdiPlus!GdipFillPolygon
GdiPlus!GdipFillPolygonI
chartv!CvPaintSurface::Polyline
chartv!CvLine::Render
chartv!CvLineChart::Render
chartv!CvWindow::WindowMessages
user32!UserCallWinProcCheckWow
user32!CallWindowProcW
duser!WndBridge::RawWndProc
user32!UserCallWinProcCheckWow
user32!SendMessageWorker
user32!SendMessageW
shell32!COperationStatusTileRateChart::_DrawChart
shell32!COperationStatusTileRateChart::_PaintOverlay
shell32!COperationStatusTileRateChart::_OverlayBufferedPaint
shell32!COperationStatusTileRateChart::_OverlayWindowProcedure
shell32!COperationStatusTileRateChart::s_OverlayWindowProcedure
```

```
[...]
```

WRL

```
0:000> ~1kc ; Windows 8.0
```

```
Call Site
```

```
user32!NtUserWaitAvailableMessageEx
```

```
explorer!CTray::_MessageLoop
```

```
explorer!CTray::MainThreadProc
```

```
SHCore!COplockFileHandle::v_GetHandlerCLSID
```

```
kernel32!BaseThreadInitThunk
```

```
ntdll!RtlUserThreadStart
```

```
0:000> ~2kc ; Windows 8.1 - coincidental symbolic information
```

```
Call Site
```

```
user32!NtUserWaitAvailableMessageEx
```

```
explorer!CTray::_MessageLoop
```

```
explorer!CTray::MainThreadProc
```

```
SHCore!Microsoft::WRL::Details::ImplementsHelper<Microsoft::WRL::RuntimeClassFlags  
<3>,Microsoft::WRL::Details::InterfaceList<Microsoft::WRL::CloakedId<IInputStream  
Priv>,Microsoft::WRL::Details::InterfaceList<Microsoft::WRL::CloakedId<CFTMCrossP  
rocServer>,Microsoft::WRL::Details::Nil> >,1,0>::CanCastTo
```

```
kernel32!BaseThreadInitThunk
```

```
ntdll!RtlUserThreadStart
```

!Ad Hardcore Software Diagnostics Training

| | |
|----------------------|---|
| 2014 | <u>Psychology of Software Diagnostics</u> (FREE) <u>Semiotics of Debugging</u> (FREE) <u>Generative Software Narratology</u> (FREE) <u>Software Diagnostics: Requirements, Architecture, Design, Implementation and Improvement</u> (FREE) |
| December 6-9, 2013 | <u>Advanced Windows Memory Dump Analysis with Data Structures</u> |
| December 13-16, 2013 | <u>Deep Down C++</u> |
| January 6, 2014 | <u>Pattern-Oriented Software Forensics</u> |

Debugging.TV

Now on YouTube!

<http://www.youtube.com/DebuggingTV>