Legacy Windows Debugging

with Memory Dumps

Dmitry Vostokov
Software Diagnostics Services

Prerequisites

Legacy Windows Programming

Agenda

- Accelerated Windows Memory Dump Analysis (up to 8 hours)
- Accelerated .NET Memory Dump Analysis (up to 4 hours)
- Advanced Windows Memory Dump Analysis (up to 4 hours)
- Special Topics (customized)

Training Goals

- Review fundamentals
- Learn how to analyze process, kernel and complete memory dumps
- Learn specialized analysis techniques and commands
- Learn Windows data structures and their navigation

Training Principles

- Talk only about what I can show
- Lots of pictures
- Lots of examples
- Original content and examples

Special Topics

Process Dump Generation

- Crash or Hang, … ?

  PID in Task Manager

- Windows XP / W2K3
  - Crash: set default debugger or Userdump monitoring
  - Hang / Leak / Spike: userdump.exe
- Windows Vista / W2K8 / W7 / W8 / W10
  - Crash: LocalDumps
  - Hang / Leak / Spike: Task Manager, procdump -ma

Complete Dump Setup

- Control Panel

  System \ Advanced system settings \ Startup and Recovery

- Page file size should be greater than the amount of physical memory by 100 MB
- DedicatedDumpFile (KB969028)

Complete Dump Generation

- Keyboard (KB972110, Step 6), NMI button
- Tools: NotMyFault
- VMware memory snapshot + vmss2core

Common Issues

- 32-bit vs. x64 (process dumps)

  32-bit Task Manager (from \Windows\SysWOW64) vs. 64-bit Task Manager

- Truncated complete dumps
- No complete memory dumps saved (+W7)

  WER services blog

- No “Complete memory dump” option

  HKLM \ SYSTEM \ CurrentControlSet \ Control \ CrashControl
  CrashDumpEnabled = 1 (DWORD)