Software Trace and Memory Dump Analysis

PATTERNS, TOOLS, PROCESSES AND BEST PRACTICES

Presenter: Dmitry Vostokov
Memory Dump Analysis Services
Prerequisites

Experience in software troubleshooting and reading software logs

Advantage: Citrix CDF and Microsoft ETW trace analysis including Process Monitor logs
Agenda

- Memory Dump Analysis Services
- Root Cause Analysis Methodology
- Software Traces and Memory Dumps
- Examples
MDA Services

- Memory Dump Analysis Audit
- Software Trace Analysis Audit (New)
- Software Error Reporting Audit
- Remote Training
- Debugging Bureau
- Tool Objects and EasyDbg

Powered by DA+TA

DumpAnalysis.org + TraceAnalysis.org
A.C.P. Root Cause Analysis

Checklists and patterns as best practices

Iterative and Incremental
DA+TA

- DA: Dump Artifact / Dump Analysis
  Memory snapshots: process, kernel, physical memory dumps

- TA: Trace Artifact / Trace Analysis
  Software traces: Event Tracing for Windows, logs
Spatiality vs. Narrativity

Software trace as software narrative, the story of a computation
Tools for Artifact Analysis

Memory dumps:
- WinDbg from Debugging Tools for Windows
- Notepad (textual debugger logs)

Software traces:
- CDFAnalyzer* / CDFControl from Citrix
- Process Monitor* from Microsoft

* supports adjoint threads
Checklists for Analysis

Memory dumps:


Software traces:

http://www.dumpanalysis.org/blog/index.php/2011/03/10/software-trace-analysis-checklist/
Software Behavior Patterns

- Memory dump and software trace
- Examples: Spiking Thread, Discontinuity
- +200 patterns (DA+TA)
- DumpAnalysis.org

Patterns for Structural and Behavioral Analysis of Software

Software Behavior Patterns

© 2011 Memory Dump Analysis Services
DA: Software Behavior

- Memory dump: a memory snapshot
- Definition, partial classification and historical list
- Pattern identification case studies
“Imagine you got a software trace from hundreds of modules you haven’t written or haven’t seen source code of...”

- Software trace: a sequence of memory fragments ordered in time
- Definition, and historical list
- Pattern identification case studies
CDFAnalyzer Filters
Threads

Time

# PID TID Time Message

Time

# PID TID Time Message

© 2011 Memory Dump Analysis Services
Adjoint Threads

Time
# PID TID Time Message

Time
# PID TID Time Message (ATID)
Significant Event

csrss.exe
winlogon.exe
LogonUI.exe
userinit.exe
...

Custom events: CDFMarker
Discontinuity

...  
14:23:02.146  
14:23:02.345  
14:31:10.254  
14:31:10.341  
...
No Activity

Expecting messages from Module X

Absence of such messages may suggest that a process or a thread was hang / blocked
Guest Component

Sudden appearance of an unexpected module, for example, werfault.exe or faultrep.dll
Statement Current

The flood of messages

Normal case: 15 msg/s
Abnormal case: 3500 msg/s

May point to a CPU spike
Resources

- DumpAnalysis.org
- Pattern-Driven Memory Dump Analysis
- Memory Dump and Trace Analysis: A Unified Pattern Approach
- Introduction to Pattern-Driven Software Problem Solving
- Advanced Software Debugging Reference:

- OpenTask publishes this talk with extra case studies
  (ISBN: 978-1908043238)
More Resources

August remote training season:

- Accelerated Windows Memory Dump Analysis
- Complete Physical Memory Dump Analysis

Visit Memory Dump Analysis Services for registration details:

www.DumpAnalysis.com
Free Summer Webinars

- The Old New Crash: Cloud Memory Dump Analysis (June 6th)
- Cyber Warfare Memory Dump Analysis (forthcoming in July-August)

Visit Memory Dump Analysis Services for registration details:

www.DumpAnalysis.com
Q&A

Please send your feedback using the contact form on DumpAnalysis.com
Thank you!

Join DA+TA Facebook Group