Virtualization-Based Security: A Forensics Perspective

August 7, 2017

Jason Hale, MSc, CCE, GCFA
One Source Discovery
Windows 10 VBS/VSM

- User Mode
- Kernel Mode
- Hardware
Windows 10 VBS/VSM

User Mode

Kernel Mode

Hardware
Windows 10 VBS/VSM

- User Mode
- Kernel Mode
- Hypervisor
- Hardware
Windows 10 VBS/VSM

User Mode

Kernel Mode

Secure User Mode (Isolated User Mode)

Secure Kernel Mode

Hypervisor

Hardware
Windows 10 VBS/VSM

- **VTL 0**
  - User Mode
  - Kernel Mode
  - Hypervisor
  - Hardware

- **VTL 1**
  - Secure User Mode (Isolated User Mode)
  - Secure Kernel Mode
  - Hypervisor
  - Hardware
Technologies Using VBS

• Credential Guard
• Device Guard
• Hyper Guard
• Application Guard
• Exploit Guard
• Host Guardian and Shielded Fabric
VBS and Disk Forensics

System, Security, DeviceGuard event log
VBS and Disk Forensics

- No prefetch files for trustlets
- Shielded VMs – BitLocker encrypted
  - Attestation logs

VBS and Memory Forensics

• Acquisition currently the biggest hurdle
• Memory acquisition tools run in normal mode
• Normal kernel handles memory management
• VTL1 page allocations will be visible, but access to those pages may not be available
VBS and Memory Forensics
VBS and Memory Forensics
Your PC ran into a problem and needs to restart. We're just collecting some error info, and then we'll restart for you.

0% complete

For more information about this issue and possible fixes, visit http://windows.com/stopcode

If you call a support person, give them this info:
Stop Code: SYSTEM SERVICE EXCEPTION
What failed: pmeA766.tmp
## Memory Acquisition Test Results

<table>
<thead>
<tr>
<th>Tool</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>winpmem v1.6.2</td>
<td>BSOD</td>
</tr>
<tr>
<td>winpmem v2.1.post4</td>
<td>BSOD</td>
</tr>
<tr>
<td>DumpIt v1.3.2.20110401</td>
<td>BSOD</td>
</tr>
<tr>
<td>DumpIt v3.0.109.20161007</td>
<td>Load driver error*</td>
</tr>
<tr>
<td>Magnet RAM Capture v1.0.0.0034</td>
<td>BSOD</td>
</tr>
<tr>
<td>Magnet RAM Capture v1.1.1</td>
<td>BSOD</td>
</tr>
<tr>
<td>FTK Imager Lite v3.1.1</td>
<td>BSOD</td>
</tr>
</tbody>
</table>

-Tested on Windows 1607 and 1703

*Non-EV driver signed after July 29, 2015
Belkasoft RAM Capturer

Select output folder path:

D:\Belkasoft RAM Capturer\RamCapturer_64-bit

Physical Memory Page Size = 4096
Total Physical Memory Size = 16870 MB
Memory dump completed. Total memory dumped = 16870 MB
Analyze memory dumps with Belkasoft Forensic Studio. Download at www.belkasoft.com

Capture!  Cancel  Close
DumpIt v3.0.20170620

Destination path:  \??\E:\LENOVO-20170705-211411.dmp
Computer name:    LENOVO

--> Proceed with the acquisition? [y/n] y

[+] Information:
Dump Type:        Microsoft Crash Dump

[+] Machine Information:
Windows version:  10.0.15063
MachineId:        58EB7381-52A8-11CB-9C70-ED069E383733
TimeStamp:        131437628531654104
Cr3:              0x1aa000
KdCopyDataBlock:  0xffffffff8011647d8dc
KdDebuggerData:   0xffffffff801165bd4f0
KdpDataBlockEncoded:  0xffffffff801165f04b0
Current date/time: [2017-07-05 (YYYY-MM-DD) 21:14:13 (UTC)]
+ Processing... Done.

Acquisition finished at: [2017-07-05 (YYYY-MM-DD) 21:28:24 (UTC)]
Time elapsed:        14:11 minutes:seconds (851 secs)
Created file size:   16843382784 bytes (16063 Mb)
osforensics v5.1.1001
VBS and Memory Forensics
Future/Additional Work

• Windows Defender Application Guard
  – Is web history, cache, etc. of protected pages available?
  – What information related to WDAG is available from a memory dump?
Thank You!

jhale@onesourcediscovery.com
@jasonshale