Volatility Development Team

- Core Developers:
  - Mike Auty (ikelos)
  - Andrew Case (attc)
  - Brendan Dolan-Gavitt (moyix)
  - Michael Hale Ligh (MHL)
  - Jamie Levy (gleeda)
  - AAron Walters (labarum)

- The Volatility Community (OOV)
  - Numerous research collaborators/testing/bugs
  - Academia, government, industry
  - Mailing lists, blogs, irc (#volatility)
  - Moved: https://github.com/volatilityfoundation/volatility
  - @volatility

Thank You!
Volatility Foundation

• Volatility development is supported by an independent foundation
  • US 501(c)(3) Nonprofit

• The Volatility Foundation was established:
  • to support the development of Volatility
  • to promote the use of Volatility and memory analysis in the forensics community
  • to protect the intellectual property and the framework's long-term viability
  • to advance the state of the art in memory analysis research.

• But….development driven by Volatility community
Opaque Systems/Enterprise

- Opaque components of information infrastructure
- Can your systems be trusted? (patches, malware)
Adversaries Challenges

• Adversaries Challenges
  • They want to remain undetected (stealthy)
  • They want to execute a mission
  • They rely on components of the operating system

• Consume system resources
  • Memory (stack, heap, pool)
  • Objects (thread, process, mutex, driver)

• Modify control flow (execution) of the system
  • Hide the allocated resources
  • Perform mission
What is Memory Forensics?

• Memory forensics is the process of acquiring and analyzing physical memory (RAM) in order to find artifacts and evidence
  • Analysis does not depend on OS (trust)
  • Unconstrained analysis (entire state of OS/historical)
  • Removes the active adversary

• Usually performed in conjunction with disk and network forensics (memory only artifacts)

• Rapid triage/analysis leads (sandbox)
Volatility Framework

- Volatile memory artifact extraction utility framework
- Completely open source (GPLv2/Python)
- Cross platform (Python)
- Single, cohesive analysis framework
  - Windows, Mac, Linux, Android, …
- Command-line tools/scriptable
- Modular architecture
- Unparalleled features!
- Active Community
  - Industry, academics, government, law enforcement
Volatility 2.4: AMF
Volatility 2.4: Highlights

- Released: August 2014 at Black Hat Arsenal
- Address Spaces (3 new AS/17)
  - QEMU virtual machine memory samples
  - “split” VMware files (vmem, vmss, vmsn)
  - Windows BitMap crash dumps (Windows 8/2012)
- Mac OSX (30 new plugins/62)
  - Mavericks through 10.9.4
  - Mac string translation
  - Adium message (OTR)/Contact records/Notes artifacts
  - Apple Keychain encryption keys/clear-text PGP emails
  - API hooks in kernel and process memory
  - IP and socket filters
  - Suspicious process mappings (injected code)
  - Hidden kernel extensions (extraction)
  - Recovered files cached in memory
Application Artifacts
Volatility 2.4: Highlights

- Linux/Android (24 new plugins/66)
  - Linux kernels through 3.16
  - Linux string translation
  - API hooks (kernel/userland)
  - GOT/PLT overwrites
  - Hollowed executables
  - Suspicious process mappings (injected code)
  - Library listing using the loader’s data structures
  - Extract process ELF executables and libraries
  - Network interfaces in promiscuous mode
  - Processes that are using raw sockets
  - Hidden kernel modules
  - Netfilter hooks
  - Cached TrueCrypt passphrases
Volatility 2.4: Highlights

- Windows (14 new plugins/108)
  - Windows 8/2012 support
  - TrueCrypt plugins (summary, cached pass, master keys)
  - Apihooks (64-bit/JMP FAR)
  - hashdump, cachedump, and lsadump (x64/Win8/2012)
  - callbacks and timers (64-bit)
  - mftparser (ADS, extract MFT resident blocks)
  - Single pass executive object scanning
  - verinfo plugin (PE version info)
  - auditpol plugin (audit policies)
  - cmdline plugin (process command line arguments)
  - pooltracker plugin (kernel pool tag statistics)
  - bigpools plugin (big page pool allocations)
  - Notepad plugin (application heap)
  - svcscan enumerates service start type
TrueCrypt

Passphrase unlocks the header

Host Disk

C:\Users\Mike\Documents\lease.pdf

Master keys

Cached password

Cached file(s)

Encrypted
Un-encrypted
Decrypted

RAM
Notepad’s Heap

List of targets:
Jim James
Bobby Knight
Peter Silver
Amy Christoph

Plan:
Get their cell phone numbers
Text with a place to meet
Blackmail with pictures
Collect money and profit

2011 TIME: 06:56 pm

Try value returned 2, dwv:
Try value default to 0
Value = 0
T = dtc Subcomponent = dtc
-I, R-
V = 0
TATE Component = dtc Subcomp
C+, R-
TATE Return Value = 1
TATE Component = dtc Subcomp
C+, R-
DTC Setup[6:57:21]: Start OC_QUERY_CHANGE_SEL_STATE Component = dtc Subcomp
DTC Setup[6:57:21]: Subcomponent dtc state: O-, C+, R-
DTC Setup[6:57:21]: End OC_QUERY_CHANGE_SEL_STATE Return Value = 1
DTC Setup[6:57:21]: Start OC_CALC_DISK_SPACE Component = dtc Subcomponent =
DTC Setup[6:57:21]: End OC_CALC_DISK_SPACE Return Value = 0
DTC Setup[6:57:43]: Start OC_QUEUE_FILE_OPS Component = dtc Subcomponent =
DTC Setup[6:57:43]: End OC_QUEUE_FILE_OPS Return Value = 0
DTC Setup[6:57:43]: Start OC_QUEUE_FILE_OPS Component = dtc Subcomponent =
DTC Setup[6:57:43]: Subcomponent dtc state: O-, C+, R-
DTC Setup[6:57:43]: Reading persistent registry values
Volatility 2.4: Resources

• Official Volatility Memory Analysis Cheat Sheet
  • Windows, Linux, Mac OS X
  • RTFM-style insert for Windows
    • http://downloads.volatilityfoundation.org/releases/2.4/CheatSheet_v2.4.pdf

• Volatility demo videos
  • Defeating Truecrypt Disk Encryption
  • Reverse Engineering Rootkits
  • Tracking Mac OS X Activity
    • https://www.youtube.com/channel/UC3AsZ6DGlqZ1aPqx6tXgAA
Volatility Roadmap

- **Volatility 2.5 (November 2014)**
  - Bug fixes
  - Unified plugin output format
- **Volatility 3.0 (2015)**
  - “Big Changes”: Refactor/Cleanup/API
  - Unicode improvement/Python 3.0
  - *Performance*
Compressed RAM/Swap

- virtual address to slot mapping
- cpgr_slots
- compressor_pager (per vm_map_entry object)
- c_size
- c_offset
- c_slots
- c_buffer
- c_segments
- compressor
- compressed pages
Social Media Artifacts

volatility social media plugins
ssl everywhere causes browsers to limit disk storage
memory is where it's at!

```
$vol.py --profile=Win/SP1x64 --f briner/memimages/win/chrometwitter twitter
Volatile Systems Volatility Framework 2.3_alpha
searching for browser processes...
found browser pid: 2708, chrome.exe
examining 109010118 bytes
found browser pid: 1800, chrome.exe
examining 127633456 bytes
profile: @0wulabs, 3,477 Tweets 921 Following 1,160 Followers
profile: @0wulabs, 3,477 Tweets 921 Following 1,160 Followers
6:46 PM - 20 Jul 13 (3m)  #obscuresec Chris
@CarlosPerez @aattifikation @JosephBialek also, did you try HTTP/HTTPS interpreter?
6:19 PM - 20 Jul 13 (3m)  #VinylMuseum Vinyl Music Hall
LIVING COLOUR tonight at Vinyl with special guests LUGOSI Doors, just opened...LUGOSI hits at
9pm! Tickets still available at the door!
6:47 PM - 20 Jul 13 (3m)  #CarlosPerez Darkoperator
#obscuresec tcp from shell I just execute powershell.exe -nologo
```
Dalvik Inspector

http://www.504ensics.com/blog/
2nd Volatility Plugin Contest

- (Inspired by the Hex-Rays IDA plugin contest)
- Create an innovative and useful extension to Volatility and win the contest!
- **Facebook doubled the prize money!**
- Prizes awarded for top 5 submissions:
  - 1: $2500, 2: $1250, 3: $750, 4-5: Volatility swag
- Core development team judges
  - creativity, usefulness, effort, completeness, submission date, and clarity of documentation.
- 12 submissions worldwide (>30 new plugins!)
- Trend: Application analysis/context
1st Place: Dave Lasalle

- Dave submitted 14 plugins ("Forensic Suite")
- Recovering Firefox and Chrome artifacts
  - Firefox (3 plugins)
    - History, cookies, downloads
  - Chrome (6 plugins)
    - History, cookies, downloads, visits, search terms
- Java IDX files: Download history of Java archives
- Office TrustRecords: Office files from untrusted src
- Fuzzy hashing to whitelist injected code/API hooks
  - ssdeepscan, malfinddeep, apihooksdeep
Chrome History

$ python vol.py -f voltest.dmp chromehistory --output=csv > output.csv

<table>
<thead>
<tr>
<th>index</th>
<th>url</th>
<th>title</th>
<th>visits</th>
<th>typed</th>
<th>last_visit</th>
<th>hidden</th>
<th>favicon_id</th>
</tr>
</thead>
<tbody>
<tr>
<td>15</td>
<td><a href="https://www.google.com/webhp?sourceid=chrome-instant&amp;ion=1&amp;espv=2&amp;ie=UTF-8&amp;q=What%20Is%20Google">https://www.google.com/webhp?sourceid=chrome-instant&amp;ion=1&amp;espv=2&amp;ie=UTF-8&amp;q=What%20Is%20Google</a></td>
<td>Welcome to Google - Log In, Sign Up</td>
<td>1</td>
<td>0</td>
<td>09:30.1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>13</td>
<td><a href="http://www.ubuntu.com/download/desktop/thank-you/?version=14">http://www.ubuntu.com/download/desktop/thank-you/?version=14</a></td>
<td>Thanks for downloading Ubuntu Desktop</td>
<td>1</td>
<td>0</td>
<td>56:08.0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>14</td>
<td><a href="http://www.ubuntu.com/download/desktop/thank-you?country=US">http://www.ubuntu.com/download/desktop/thank-you?country=US</a></td>
<td>Thanks for downloading Ubuntu Desktop</td>
<td>1</td>
<td>0</td>
<td>56:08.0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>12</td>
<td><a href="http://www.ubuntu.com/download/desktop/contribute/?version=14">http://www.ubuntu.com/download/desktop/contribute/?version=14</a></td>
<td>Contribute to Ubuntu</td>
<td>1</td>
<td>0</td>
<td>56:04.5</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>11</td>
<td><a href="http://www.ubuntu.com/download/desktop">http://www.ubuntu.com/download/desktop</a></td>
<td>Download Ubuntu Desktop</td>
<td>1</td>
<td>0</td>
<td>56:01.8</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>9</td>
<td><a href="https://www.google.com/webhp?sourceid=chrome-instant&amp;ion=1&amp;ie=UTF-8&amp;q=Ubuntu%20Desktop">https://www.google.com/webhp?sourceid=chrome-instant&amp;ion=1&amp;ie=UTF-8&amp;q=Ubuntu%20Desktop</a></td>
<td>Welcome to Google - Log In, Sign Up</td>
<td>1</td>
<td>0</td>
<td>55:46.2</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>5</td>
<td><a href="http://www.facebook.com/">http://www.facebook.com/</a></td>
<td>Welcome to Facebook - Log In, Sign Up</td>
<td>2</td>
<td>2</td>
<td>09:50.6</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>7</td>
<td><a href="http://www.cnn.com/">http://www.cnn.com/</a></td>
<td>Welcome to CNN.com - Breaking News, U.S., World News</td>
<td>1</td>
<td>1</td>
<td>55:33.5</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>6</td>
<td><a href="https://www.facebook.com/">https://www.facebook.com/</a></td>
<td>Welcome to Facebook - Log In, Sign Up</td>
<td>2</td>
<td>0</td>
<td>09:50.6</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>10</td>
<td><a href="http://www.ubuntu.com/download">http://www.ubuntu.com/download</a></td>
<td>Get Ubuntu</td>
<td>1</td>
<td>0</td>
<td>55:54.3</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>4</td>
<td><a href="http://www.foxnews.com/">http://www.foxnews.com/</a></td>
<td>Fox News - Breaking News Update</td>
<td>1</td>
<td>1</td>
<td>55:04.1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td><a href="http://tools.google.com/chrome/intl/en/welcome.html">http://tools.google.com/chrome/intl/en/welcome.html</a></td>
<td>Getting Started</td>
<td>1</td>
<td>0</td>
<td>53:54.4</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>3</td>
<td><a href="https://www.google.com/">https://www.google.com/</a></td>
<td>Google</td>
<td>1</td>
<td>1</td>
<td>54:43.9</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td><a href="https://www.google.com/intl/en/chrome/browser/welcome.html">https://www.google.com/intl/en/chrome/browser/welcome.html</a></td>
<td>Getting Started</td>
<td>1</td>
<td>0</td>
<td>53:54.4</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
IDX Parser

$ python vol.py –f voltest.dmp idxparses

[*] Section 2 (Download History) found:
URL: http://javagameplay.com/offroadrally/inthejar.jar
IP: 209.188.88.156
<null>: HTTP/1.1 200 OK
content-length: 61699
last-modified: Fri, 10 Oct 2008 20:25:10 GMT
content-type: text/plain
date: Sat, 30 Aug 2014 19:53:56 GMT
server: Apache/2.2.8 (Unix) mod_ssl/2.2.8 OpenSSL/0.9.8e-fips-rhel5 DAV/2 mod_auth_passthrough/2.1 mod_bwlimited/1.4 FrontPage/5.0.2.2635 PHP/5.2.6
deploy-request-content-type: application/x-java-archive
• Create the whitelist:

$ vol.py -f D5XLBY3J-bf977e52_lookIE_pid_860.vmss --profile=WinXPSP2x86 vaddump -p 860 -b 0x71590000 -D dumps

[snip]

860 iexplore.exe 0x71590000 0x71608fff dumps/iexplore.exe.
24296b8.0x71590000-0x71608fff.dmp

$ python hash_by_page.py -n AcLayers.DLL -f dumps/iexplore.exe.
24296b8.0x71590000-0x71608fff.dmp

('AcLayers.DLL', '6:idqLvVg3F+X32xbQ7esfGkxNPWgwh9lorlclfMfEtj/lkwSM0E/mh6l+tgdwL:eqGSGfP0FWgO9arlclrUpEec1w'),

('AcLayers.DLL', '96:1SxccXfBWrvZnxbZ3IX26dZC6FsEzSVr6y616GpIHoib8u:uvBWrpxbxGpWEcr3UTpIHPb8u'),

[snip]
Now those hooks are not shown:

```
$ vol.py -f D5XLBY3J-bf977e52_lookIE_pid_860.vmss --profile=WinXPSP2x86 apihooksdeep -p 860
```

Process: 860 (iexplore.exe)
Hook at 0x715b9e59 in page 0x715b9000 is 100% similar to whitelist hook AcLayers.DLL

Process: 860 (iexplore.exe)
Hook at 0x715ba067 in page 0x715ba000 is 100% similar to whitelist hook AcLayers.DLL
2\textsuperscript{nd} Place: dm\_dump

- Submitted by Curtis Carmony
- dm-crypt is used on Linux and Android for FDE
- Keying material in physical memory (RAM)
- dm\_dump plugin recovers dm-crypt keys from memory and prints commands that can be copy/pasted to mount the volumes
- Will be incorporated into core Volatility soon

Volatility Foundation Volatility Framework 2.4

sda5_crypt: 0 16269312 crypt aes-xts-plain64
c2ca0a6a52980952016936047ab46fba961397978f6bf3219ca39f6fde3b46e2b6348daa09d09335113288c8258bc6bd3c3d57afab2d6bc3cac7cfde436939b 0 /dev/sda5 4096

ubuntu--vg-swap_1: 0 1040384 linear /dev/dm-0 15163776

ubuntu--vg-root: 0 15163392 linear /dev/dm-0 384

$ dmsetup create volatility --table “0 16269312 crypt aes-xts-plain64
c2ca0a6a52980952016936047ab46fba961397978f6bf3219ca39f6fde3b46e2b6348daa09d09335113288c8258bc6bd3c3d57afab2d6bc3cac7cfde436939b 0 /dev/sda5 4096”
3rd Place: editbox

- Written by Adam Bridge “Bridgey The Geek”
- This plugin extracts text from the edit, combo, and list boxes of GUI applications that run on Windows
- Includes, but is not limited to:
  - Notepad window
  - Run dialog
  - Username and server name fields of Remote Desktop Connection
  - Address bar and search bar of Internet Explorer
  - Search bar of Windows Media Player
  - Username field of Create New Account wizard
  - Password of Change Password dialog
editbox
$ python vol.py --profile=Win7SP1x64 -f WIN7SP1X64-20140929-225403.raw

editbox

Volatility Foundation Volatility Framework 2.4
*******************************************************
Wnd context          : 1\WinSta0\Default
pid                  : 2244
imageFileName        : mstsc.exe
wow64                : No
atom_class           : 6.0.7601.17514!Edit
isPwdControl         : No
*******************************************************
Wnd context          : 1\WinSta0\Default
pid                  : 1748
imageFileName        : explorer.exe
wow64                : No
atom_class           : 6.0.7601.17514!Edit
isPwdControl         : Yes
pwdChar              : 0x25cf
monkey

monkey
screenshot + editbox
screenshot + editbox

Type the name of a program, folder, document, or Internet

Open: \\
crashoverride\pwn_acidburn.exe

OK Cancel &Browse...
Volatility 2014 Plugin Contest

• 4th Place:
  • Thomas Chopitea: Autoruns – Finding persistence

• 5th Place:
  • Takahiro Haruyama: OpenIOC Scan

• Submissions:
  • Monnappa KA: Gh0stRat Decryption
  • Jamaal Speights: MsDecompress
  • Cem Gurkok: Mac Rootkit and Bitcoin
  • Csaba Barta: Malware Analysis (Baselines)
  • Philip Huppert: OpenVPN
  • Wyatt Roersma: Hyper-V Tools
OMFW 2014

• OMFW first held 2008
• Highly technical venue for digital investigators
• 100% of the proceeds are donated to charity
• What makes OMFW unique:
  • Workshop size
  • Technical content
  • Researchers and developers
  • Peer relationships
  • Cost
  • Lightning talks
• 8 Memory forensics presentations
<table>
<thead>
<tr>
<th>Time</th>
<th>Session Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>1300PM</td>
<td>The State of Volatility</td>
</tr>
<tr>
<td>1330PM</td>
<td>Careto: Accomplishing in 7 Minutes What AV Couldn’t Do in 7 yrs</td>
</tr>
<tr>
<td>1400PM</td>
<td>Restructuring Memory: Extracting Results in a Reusable Way</td>
</tr>
<tr>
<td>1430PM</td>
<td>Science, Sharing, and Repeatability in Memory Forensics</td>
</tr>
<tr>
<td>1500PM</td>
<td>Break</td>
</tr>
<tr>
<td>1530PM</td>
<td>Many Ways to Skin a RAT: Let’s Start with the Tail</td>
</tr>
<tr>
<td>1600PM</td>
<td>Memory Forensics for IR: Leveraging Volatility to Hunt Adv Actors</td>
</tr>
<tr>
<td>1630PM</td>
<td>Memory Tracing: Forensic Reverse Engineering</td>
</tr>
<tr>
<td>1700PM</td>
<td>DAMM: A Tool for Differential Analysis of Malware in Memory</td>
</tr>
<tr>
<td>1730PM</td>
<td>Closing Comments/Reception</td>
</tr>
</tbody>
</table>
### Volatility Unified Output

#### List/Tree Hybrid

<table>
<thead>
<tr>
<th></th>
<th>A (int)</th>
<th>B (unicode)</th>
<th>C (float)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Careto: Memory vs. AV

Memory Tracing

"Traditional" memory forensics

Memory tracing
- Memory trace = series of memory snapshots
Volatility Training/Certification

- Learn from the actual researchers and developers
- Show your support for open source developers
- Courses
  - Windows Memory Forensics & Malware Analysis
  - Memory Forensics Essentials
  - Mac Memory Forensics & Malware Analysis
  - Linux Memory Forensics & Malware Analysis
- Certifications
  - Memory Forensics Examiner
  - Memory Forensics Professional (Win/Mac/Lin)
- Information: www.memoryanalysis.net
Download Volatility 2.4

https://github.com/volatilityfoundation/volatility
http://volatility-labs.blogspot.com/
@volatility

Join the community!