Decade of Aggression

10 Years of Incident Response
Tips / Tricks
whoami

• IT professional with 18 years experience
  – Systems administration, Networking, Consulting, and Information Security
  – 10 years Incident Response (DoD & ISPs)

• Intrusion Detection & Analysis
• Digital Forensics
• Network Forensics
• Outdoor Enthusiast
In the Beginning...

• Worms
  – Sadmind
  – Welchia
  – Blaster

• Script Kiddies
  – Bandwidth
  – Disk space
  – Trading Warez
The more things change the more they stay the same...

- Who: Script kiddies
- What: Trading Warez
- When: ~30 days earlier
- How: WebChat vulnerability
  - PoC existed in the wild
  - Hiding in plain sight:
    - Renamed process of WSFTP server
    - Common looking service name
Reference System Configuration

• MacBook Pro OSX 10.6.8
  – 2.8Ghz Intel Core i7 (Dual Core w/Hyper-Threading)
  – 8 gig RAM
  – (2) Internal drives
    • Plextor PX-128M3 128gig SSD
    • Hitachi 500 gig 7200 rpm (system)
• (2) WD Caviar Black 2TB 7200 RPM
• (3) WD VelociRaptor 80GB 10,000 RPM
• Sonnet Tempo SATA Pro Express/34
Hard Drives (Physical)

• Mirror drives (where still applicable)
  – 100% reduction in imaging time
  – 0% downtime

• End users drive size
  – Bigger = Better
    • Maximizes recoverable artifacts over time
    • Increase Restore Point & Volume Shadow Copy size
  – Enforce remote storage vs. allowing local storage
    • Increases chances of having evidence on backups
Hard Drives (Virtual Storage)

- SANs / Network Storage
  - Maximize Snapshot retention
    - Multiple revisions of the file
    - Easily recover deleted artifacts / evidence
  - Ensure enough capacity to snapshot or clone your largest VM’s OS drive
Disk Imaging

- Use hardware mirroring, you can get (2) working copies per port
- Use dc3dd
  - Multiple drive output
  - Built-in hashing functions
  - Minimal overhead to run multiple hashes per image
- (2) drives per enclosure per port = (4) drives per laptop
- Speed of the output is limited by the speed of slowest drive
Disk Imaging Stats...

- FW800 -> RAID 1
  - 37 M/s with MD5 hash
- FW800 -> (2) eSATA drives via dc3dd
  - 55 M/s no hash
  - 52 M/s before hash, 35M/s after MD5
  - 50 M/s before hash, 34 M/s after SHA-1 & MD5
Know what you know...

• Getting the most bang for your buck
  – Capacity planning
  – Budgeting
  – Resource allocation
Performance Testing Tools Linux

• Linux
  – vmstat
    • Memory allocation stats
  – iostat
    • Drive throughput
    • CPU usage
  – top (general system / process stats)
  – Graphical monitoring
Performance Testing Tools OS X

• OS X
  – vm_stat (similar to vmstat on Linux)
    • Memory allocation stats
  – iostat
    • Drive throughput
    • CPU usage
  – top (general system / process stats)
  – Activity Monitor
    • Throughput
      – Network
      – Disk
    • CPU usage (process breakdown)
Testing Made Simple...

• Write throughput tests:
  – dc3dd wipe=/dev/sdX

• Read throughput tests:
  – dc3dd if=/dev/sdX of=/dev/null
    (tests speed from device)
  – MD5 & SHA1sum
That sounds good in theory…

- FW800 = 100 MB/s
- FW400 = 50 MB/s
- USB 2.0 = 60 MB/s
- USB 3.0 = 625 MB/s
- SATA 2.0 = 300 MB/s
- SATA 3.0 = 600 MB/s
Welcome to the real world...

- Linux desktop write blocker testing:
  - `dc3dd 7.1.614 of=/dev/null, no hash`
  - **Vendor A**
    - eSATA = 85 MB/s
    - eSATA = 99 MB/s (w/Advanced Host Controller Interface enabled)
    - FW800 = 58 MB/s
    - FW400 = 27 MB/s
    - USB 2.0 = 30 MB/s
  - **Vendor B**
    - eSATA = 62 MB/s
    - FW800 = 52 MB/s
    - FW400 = 30 MB/s
    - USB 2.0 = 25 MB/s
Not all things are created equal...

- Factors to consider:
  - Manufacturer / Model
  - Driver
  - Chipset

- Example: MBP Read testing
  - Card A:
    - Single Drive testing, 125 MB/s
    - Two Drive testing, 75 MB/s
  - Card B:
    - Single Drive testing, 135 MB/s
    - Two Drive testing, 99 MB/s
Work smarter, not harder...

- Not all Tools are created equal
  - File Carving
    - Scalpel
    - Foremost
  - String Searching
    - Scalpel
    - srch_strings and grep
Foremost File Carving

• 93 GB evidence image
• Results written to internal drive
• Simple scenario, search for:
  – PST, OST
  – DBX, IDX, MBX
• Results:
  – SSD:
    • 366 Mail files recovered, 6.5 GB in 11:57 min.
  – WD Caviar Black
    • 366 Mail files recovered, 6.5 GB in 17:59 min.
Scalpel File Carving

• 93 GB evidence image
• Results written to internal drive
• Simple scenario, search for:
  – PST, OST
  – DBX, IDX, MBX
• Results:
  – SSD:
    • 366 Mail files recovered, 34 GB in 13:23 min.
  – WD Caviar Black
    • 366 Mail files recovered, 34 GB in 20:55 min.
srch_strings

- 93 GB evidence image on SSD & WD Caviar Black
- Results written to internal drive
- Worst case scenario, strings entire image
- ASCII & Unicode
- Stats (nearly identical, only SSD listed):
  - Generate Strings:
    - ASCII: 21 GB, 39:55 min., ~40 MB/sec Read
    - Unicode: 424 MB, 20:32 min., ~77 MB/s Read
  - Search Strings 1 keyword: 13:23 min., 25 MB/sec Read
  - Total Time: 74:07 min.
Scalpel String Search

- 93 GB evidence image
- Results written to internal drive
- Worst case scenario, search entire image
- ASCII & Unicode
  - SSD:
    - Search String 1 Keyword: 5:45 min., 266 MB/s Read
  - WD Caviar Black
    - Search String 1 Keyword: 12:11 min., 132 MB/s Read

Andrew Case describes this method:
MacGyver Scaling

• Get creative / use your resources available
  – Boot SIFT on user workstations for extra processing nodes
    • Outfit these workstations for processing (install more RAM, FireWire cards, eSATA cards, etc...)

• Where applicable, make multiple working copies of the image.
MacGyver’s Processor Guidance

• One core per operation (depending on software’s multiprocessor capabilities)
• One core per HD
• Leave one core for the OS
  – Example:
    • Dual core MBP with HT can MD5 three drives simultaneously with CPU cycles left over
MacGyver’s I/O Guidance

• One operation type (read OR write) per HD
• Know your HD’s throughput numbers
  – Max. read, max. write
  – Average read, average write
• One read OR write function per physical card or device type (FireWire, eSATA, USB, etc...)
  – Example: Reference System could Read (FW800) and Write -> (2) eSATA drives on one physical card simultaneously, (4) SATA drives using mirroring enclosures
MacGyver Scaling Examples

• Reference System Optimal Usage:
  – Option #1
    • FW800 evidence results drive (Writing Only)
    • Evidence disks (2)
      – Disk #1 log2timeline processing (Read Only output to FW800)
      – Disk #2 anyone of the following: file carving, registry analysis, AV Scanning (Read Only output to FW800)
  – Option #2:
    • Use internal drive for results storage (Writing Only)
    • Add a third disk for evidence processing off of the FW800 port
  – Option #3:
    • Write results over the network
    • Add a fourth drive (internal) for evidence processing
Can I have that to go...

• Laptop requirements:
  – (2) Internal hard drives
  – ExpressCard slot for (2-3) additional ports
    • eSATA
    • FW800
    • USB 3.0
  – 8 gig of RAM
  – One external high speed connection built in
    • eSATA
    • FW800
    • USB 3.0
Don’t get cut by the bleeding edge...

• Standards are great, except when they impede security (consider the tradeoffs carefully)
  – If there isn’t a tool that can analyze the format, don’t adopt it.
  – Play to your strengths
  – Browser versions
  – Smartphones
    • Hardware
    • Software

• File Systems
  – Types (exFAT, ReiserFS, etc...)
Paint them into a corner...

- **System:**
  - Restrict Bios Access (No external boot options)
  - Restrict off network access
  - Disable Split tunneling
  - Force all devices through enterprise protections
- **Restrictive egress filtering**
- **Email**
  - Auto forwarding rules
  - Strict policy on personal email for business
- **Restrict BYOD (Personal / Professional Use)**
  - Tablets / eReaders
  - Smartphones
  - External media (USB, Hard Drives, etc...)
    - Restrict by manufacturer
Consider this...

• Hard Drives are so cheap they’re almost disposable:
  – Never reuse HDs
    • Shelf originals (especially during sudden separation / suspicious separation)
  – Wipe drives prior to reuse
    • Image and compress originals of important staff
Colocation, Collaboration, & Cohabitation != Cooperation

• Colocation / Shared Hosting Contract Notes:
  – Never let a third party have access to your system
  – Request for their system logs (Firewalls, Netflow, etc.) should not require a subpoena
  – Review their IR policies and procedures
  – If my site gets compromised, what are your processes and SLA?
You make me sick...

• Custom AV signatures:
  – You don’t want to tip your hand. (VirusTotal)
  – Can’t / Won’t submit targeted malware to your vendor
  – Need a detection mechanism for targeted malware
  – Scan for a handful of signatures instead of thousands
  – Search for traits to flag suspicious files for a deeper dive

• Cross platform supported tools:
  – ClamAV (Linux, BSD, Windows, OSX...)
  – YARA (anywhere Python, and Windows exe)
Crouching Vendor…
Hidden Vulnerability…

• Evil lurks within:
  – Printers and Vendor “Appliances”
    • Embedded OS
      – Linux
      – Microsoft
      – BSD
    • Poor patching support
      – Vendor maintained approved patches
  • Never hardened or hidden
  • Unknown threat surface
  • Treated as though they are model citizens
BCP... IR... and U...

• There may come a time when you realize... it really is that bad! And one of the few options you have left is to go DARK (aka Plan B)

• IR as part of your Business Continuity Plan (BCP)
  • Firewall / Router ACLs
  • Essential services and web apps. identified
Get out your tin foil hats...
Here comes Plan B...

• Stop using corp assets for communications
  – No VoIP
  – No corp email, encrypted or not

• In case of Emergency, Break Glass:
  – Backup consumer connection (Cable, DSL, etc.)
  – Secondary laptop
  – Setup a “Meta” network for response (site-to-site VPN)
  – Encrypt all communications traversing public networks
Well, I’ll never do that again...

• STOP
  – Do not disconnect a system from the network
    • Implement switch / firewall ACLs to block system
  – Do not AV scan a system until it is imaged
  – Never ship the original
    • Whenever possible, retain the original onsite
Things you always need but...

- **Full Packet Capture (FPC)**
  - When all else fails “Proof is in the packet!”

- **DNS Logging**
  - How will you know who asked for what?
  - Worst case turn logging on your MS servers

- **Proxy Servers**
  - Not for performance reasons!
    - URL’s requested, by whom
    - User Agent string
    - Blacklisting or better yet Whitelisting only
Free and Open Source Software (FOSS)

• Thank a FOSS developer or community contributor! There are plenty here!

Take your pick:

– Tools
– Scripts
– Authors (Blogs, Whitepapers, Books, etc...)
– Researchers
Forensified Investification
Questions ???

Christopher Witter
Twitter: mr_cwitter
Email: sparsefile:>gmail.com