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”
- Chosen as a SANS “Thought Leader” in Digital Forensics
- Member of the USSS Electronic Crimes Task Force
- Speaker @ SANS “What Works in Incident Response” ’09 and ’10, The Computer Forensics Show ’09 and ’10, Direct Response Forum ’09, SecTor ’09 and ’10, USSS ECTF - Miami Conference, The Next HOPE ’10, BSIDESLV ’10, DEF CON 18.
- Former US Army Signal Corps Warrant Officer
Thank You Dan Christensen!

SNIPER FORENSICS

http://dcdrawings.blogspot.com/
Thank You MAJ Carole Newell...I think...

Twitter handle: @cpbeefcake
Sunday, October 24, 2010

SecTor 2010 – Debuting SF2

I will be debuting the second version of Sniper Forensics, titled, "Target Acquisition" at SecTor in Toronto, Ontario, Canada on October 27th. It’s a great conference and I couldn’t be more excited!

Here are some quotes about what others are saying about SF2!

"As environments continue to grow in size and complexity, incident response teams entrenched in the "image everything" methodology will find themselves not able to understand the situation as fast as the threat is evolving within a target environment. Adopting the Sniper Forensics Methodology, will decrease the cost of the investigations while providing results many times faster over traditional approaches when applied to modern environments."
Agenda

- Recap – What is Sniper Forensics?
- The Evolution of Sniper Forensics
- What are the benefits of using Sniper Forensics?
- Testimonials
- Target Acquisition
- Trigger Squeeze
- Rounds down range
- Analysis
- Case Studies
- Conclusion
The Evolution of: Sniper Forensics

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

- Create an investigation plan
- Apply sound logic
  - Locard’s Exchange Principle
  - Occam’s Razor
  - The Alexiou Principle
- Extract what needs to be extracted, nothing more
- Allow the data to provide the answers
- Report on what was done
- Answer the questions
Sniper Forensics V2.0: Target Acquisition

- What do I snipe?
- How do I actually DO that?
- How do I interpret the data?
- Examples: Some Secret Sauce
Sniper Forensics V3.0: Black Ops

- Using hacking techniques to facilitate forensic investigations
- Is it legal?
- Any different than Law Enforcement buying drugs?
- Burden of proof
- Endgame
Benefits...Don’t Take My Word For it!

“As environments continue to grow in size and complexity, incident response teams entrenched in the “image everything” methodology will find themselves not able to understand the situation as fast as the threat is evolving within a target environment. Adopting the Sniper Forensics Methodology, will decrease the cost of the investigations while providing results many times faster over traditional approaches when applied to modern environments.”

- Nick Percoco
  - Senior Vice President, Trustwave SpiderLabs
Benefits...Don’t Take My Word For it!

“Sniper Forensic rocks because it's foundations lies in logic. Try it, you will thank us later! “

- Jibran Ilyas
  - Senior Security Consultant, Trustwave SpiderLabs
Benefits...Don’t Take My Word For it!

“If you have a specific goal, you are much more likely to achieve it. Knowing what you want out of an investigation, before you start, will help you know when you're finished.”

- Jesse Kornblum
  - Computer Forensics Research Guru, Kyrus Technology

- "Using F-Response as part of the "Sniper Forensics" model is the perfect logical extension of our original mission. Get answers, not just information."

- Matt Shannon
  - Founder, F-Response
"Sniper Forensics: Target Acquisition' walks up to an analyst and slaps him right in the face! Here are targeted tools and techniques, straight from successful field ops, that every analyst needs to know!

Once you've defined your target, go grab the data you need, and optimize your time and resources to get the job done!"

- **Harlan Carvey**
  - Vice President of Advanced Technical Projects, Terremark Worldwide
  - Author of “Windows Forensic Analysis 2nd Edition”
  - Author of the Blog, “WindowsIR.blogspot.com”
Benefits…Don’t Take My Word For it!

“During a major breach, there is no plan B. Chris's presentation on Sniper Forensics are the result from his time spent on the front lines in the field. If you are looking to equip your team with what they really need, Sniper Forensics details special ops TTPs that make a clear difference. “

- Rob Lee
  - Director, Mandiant
  - Curriculum Lead, SANS Institute

* TTP = Tactics, Techniques, and Procedures
Target Acquisition

• What do I “snipe”?  
• How do I “snipe” it?  
• What do I do with the information once I have it?
Target Acquisition

What do I snipe?

• Registry hives (SAM, System, Security)
• NTUSER.dat files
• Timelines
• $MFT
• Volatile data
• RAM
Target Acquisition

How do I snipe it?

• Follow the “Order of Volatility” (RFC 3227)
  http://www.faqs.org/rfcs/rfc3227.html

• Script this! So you don’t have to remember it!

• Dump contents into predefined output files.
Target Acquisition

• **F-Response is the Biggity Bomb!**
  - Deploy remote agent
  - Connect to your forensic workstation
  - Issue Discovery Request
  - Mount the target drive as a Read Only share (PHAT!)

• You now have a RO drive mapping to the remote drive(s) on the target system. WHILE you image (imaging method is irrelevant), you can begin to extract meaningful data!
Target Acquisition

FTK Imager v3.00 allows you to copy protected files from the F-Response mounted RO drive!

- SAM
- System
- Security
- Software
- SysEvent.evt(x)
- SecEvent.evt(x)
- AppEvent.evt(x)
- NTUSER.dat

- Hives and event logs are located in `C:\Windows\system32\config`
- NTUSER.dat files are located in `C:\Document and Settings\<user>`
Target Acquisition

Prepare your workstation

• **Create Directories**
  • Registry
    • Will contain your registry hives and event logs
  • NTUSER
    • Will contain all of your ntuser.dat files
  • Timeline
    • Will contain your bodyfiles and timelines
  • Malware
    • Will contain any malware you find
    • Make sure you create an exception for this directory in your AV program
  • Ripped
    • Will contain your parsed registry hives and ntuser.dat files
  • RAM
    • Will contain your RAM dumps
  • Vol
    • Will contain your volatile data dumps
Target Acquisition

Rinse, Repeat, Rip

• Repeat file creation for all affected systems
  • Separate by hostname

• Open three command windows
  • The command line is your friend...do not fear him...

• Get ready to snipe!
Use RegRipper to rip the registry hives and ntuser.dat files

Like this...

C:\tools\RegRipper\rip.exe \-r c:\cases\customerX\registry\SAM \-f SAM > c:\cases\ripped\systemY_Sam_ripped.txt

C:\tools\RegRipper\rip.exe \-r c:\cases\customerX\registry\system \-f System\> c:\cases\ripped\systemY_system_ripped.txt

C:\tools\RegRipper\rip.exe \-r c:\cases\customerX\registry\ntuser.dat \-f ntuser\> c:\cases\ripped\systemY_ntuser.dat.userX_ripped.txt

Repeat Rips for all hives and make sure the output files all go to the same directory with a .txt extension.
If you don’t want to run your binaries (like RegRipper, or TSK) from the tools directory, you can add their location to your default path...like this...

The path is now managed by Windows 2000 / Windows XP and not the autoexec.bat or autoexec.nt files. To change the system environment variables, follow the below steps.

1. From the desktop, right-click My Computer and click Properties.
2. In the System Properties window, click on the Advanced tab.
3. In the Advanced section, click the Environment Variables button.
4. Finally, in the Environment Variables window (as shown below), highlight the Path variable in the Systems Variable section and click the Edit button. Add or modify the path lines with the paths you wish the computer to access. Each different directory is separated with a semicolon as shown below.

C:\Program Files;C:\Winnt;C:\Winnt\System32
Trigger Squeeze

Generate timelines while images are burning!!!*

Like this...

C:\tools\TSK\fls -m 'C:/’ –f ntfs -r \\.\F: >
  c:\cases\customerX\timelines\systemY_bodyfile

Perl C:\tools\TSK\mactime.pl –d –b
  C:\cases\customerX\timelines\systemY_bodyfile\systemY_timeline.csv

This will cook while you wait! It will not hurt the image since F-Response mounts the remote physical device as “read-only”!

***If your local system clock is in a different timezone than the affected system(s) make sure to use the –z <TIMEZONE> option or your timeline will be in the WRONG TIMEZONE!

• Repeat for all affected systems.
• Drive letter “F:” was chosen at random...could be any letter

* You gotta love F-Response!
Supertimelines

- You can add logs to your bodyfile with Log2Timeline
  - C:\>Perl C:\Perl\bin\Log2timeline –t <log type> >>
    c:\cases\customerX\timelines\systemY_bodyfile
- You can hives and NTUSER.dat files to your bodyfile with regtime
  - C:\>Perl C:\tools\bin\regtime.pl –m HKLM/system –r
    c:\cases\customerX\hives\system >>
    \c:\cases\customerX\timelines\systemY_bodyfile
  - Repeat for each hive or ntuser file you want to add
  - Make sure you append with the double “>>”
Trigger Squeeze

Convert evt logs to txt (this is optional at this point)

I use Event Log Explorer or DUMPEL

http://www.eventlogxp.com/

Trigger Squeeze

Rip the $MFT

- I use Harlan Carvey’s “PARSEMFT.pl”
  - Because we’re cool like that
- YOU can use “analyzeMFT”
- Look at the $Standard_Information and $File_Name attributes
  - The system and user can interact with the $S_I attribute
  - The Kernel is the ONLY thing that interacts with the $F_N attribute
  - Anti-Forensics WILL NOT affect the $F_N attribute
  - Makes attempts seem silly...VERY obvious!
Rounds Down Range

Now that you have your ripped Registry hives, NTUSER.dat files, timeline, $MFT, you can begin analysis:

• Search for suspect keywords
  • C:\cases\customerX\ripped>strings *.txt | grep –i <keyword>
  • C:\cases\customerX\timeline>strings *.csv | grep –i <keyword>

• Search for suspect timeframe
  • C:\cases\customerX\ripped>strings *.txt | grep –i <date>
  • C:\cases\customerX\timeline>strings *.csv | grep –i <date>
Rounds Down Range

Know how to stack your searches! CRITICAL!!!

- Grep –i <keyword> | grep –i <date>
- Grep –i <year> | grep –i <month> | grep –i <time>
- Grep –o <keyword or date>
- Gawk "{print $#}"
- Cut –d<delimiter> -f#

- You can stack your searches and delimiters one after another on the same command string, or in subsequent strings. This ability is critical when performing searches, and is VERY POWERFUL! If you are not familiar with how to use grep, gawk, and cut you seriously need to download them and start familiarizing yourself with them!
Analysis

Search for suspected date, all files “born” on that date.

C:\cases\customerX\timeline>strings_hostname_timeline.csv | grep -i "may 26 2010" | grep "..b,r"

Wed May 26 2010 12:08:31,9488,...b,r/rrwxrwxrwx,0,0,18914-128-3,'C:\/WINDOWS/system32/Kill.exe
Wed May 26 2010 12:10:44,28802,...b,r/rrwxrwxrwx,0,0,19142-128-3,'C:\/WINDOWS/system32/ANSI.dll
Wed May 26 2010 12:10:50,32883,...b,r/rrwxrwxrwx,0,0,19143-128-3,'C:\/WINDOWS/system32/API.dll
Wed May 26 2010 12:10:57,20573,...b,r/rrwxrwxrwx,0,0,19163-128-3,'C:\/WINDOWS/system32/cwd.dll
Wed May 26 2010 12:12:14,28772,...b,r/rrwxrwxrwx,0,0,28146-128-3,'C:\/WINDOWS/system32/Util.dll
Wed May 26 2010 12:12:24,41057,...b,r/rrwxrwxrwx,0,0,28148-128-3,'C:\/WINDOWS/system32/Win32.dll
Wed May 26 2010 12:12:34,374784,...b,r/rrwxrwxrwx,0,0,29347-128-3,'C:\/WINDOWS/system32/p2x588.dll
Wed May 26 2010 12:13:20,501052,...b,r/rrwxrwxrwx,0,0,29356-128-3,'C:\/WINDOWS/system32/lanst.exe
Wed May 26 2010 16:33:18,37376,...b,r/rrwxrwxrwx,0,0,30913-128-4,'C:\/WINDOWS/system32/netshares.exe
Wed May 26 2010 16:33:24,56320,...b,r/rrwxrwxrwx,0,0,30914-128-3,'C:\/WINDOWS/system32/starter.exe
Wed May 26 2010 16:33:29,53760,...b,r/rrwxrwxrwx,0,0,30992-128-3,'C:\/WINDOWS/system32/compenum.exe
Wed May 26 2010 16:33:34,53248,...b,r/rrwxrwxrwx,0,0,30993-128-4,'C:\/WINDOWS/system32/shareenum.exe
String search in timeline for known malware. Notice the birth date...hrm...something seems amiss here...2003???...let’s compare this date to the $MFT.

C:\cases\customerX\timeline>strings_hostname_timeline.csv | grep -i inetmgr.exe

Mon Jun 23 2003 07:28:52,1301333,m..b,r/rrwxrwxrwx,0,0,32324-128-3,'C:/WINDOWS/system32/inetmgr.exe
Analysis

BAM! Anti-Forensics – Schmanti-Schmorensics...

32324 FILE 348 1 0x38 4 1
0x0010 96 0 0x0000 0x0000
A: Tue Sep 28 21:34:57 2010 Z
C: Tue Sep 28 00:18:58 2010 Z

**B: Mon Jun 23 12:28:52 2003 Z** ← **Modified** birth date
0x0030 112 0 0x0000 0x0000
FN: inetmgr.exe Parent Ref: 29 Parent Seq: 1
C: Wed Jun 2 17:51:20 2010 Z

**B: Wed Jun 2 17:51:20 2010 Z** ← **Accurate** birth date
0x0080 72 1 0x0000 0x0000
Analysis

Analyzing RAM dumps is a great way to see what is going on RIGHT NOW!
Memoryze is a GREAT tool! Gives you a nice clean GUI…very easy to use.
Established network connection to CHINA? Not good!

* There are detailed instructions on how to use Memoryze on The Digital Standard.
Analysis

You cannot fool the registry! Check out this activity from “Oct 9 2009”…

Fri Oct 9 05:53:57 2009 Z
UEME_RUNPATH:C:\WINDOWS\system32\rpcproxy\1022.exe (1)
Subkey: exe
LastWrite Time Tue Mar 30 15:58:10 2010 (UTC)
d -> C:\WINDOWS\system32\rpcproxy\svchost.exe

Mon Apr 19 13:12:33 2010Z,DfSCC,Distributed File System
Cilent,C:\Windows\system32\rpcproxy\svchost.exe –service,272,Auto
Start,LocalSystem

Fri Oct 9 06:00:05 2009 Z
UEME_RUNPATH:C:\WINDOWS\system32\rpcproxy\1022.exe (1)

Mon Jun 7 21:32:00 2010Z,DfSCC,Distributed File System
Cilent,C:\Windows\system32\rpcproxy\svchost.exe –service,272,Auto
Start,LocalSystem
Analysis

Event logs confirm activity...busy busy busy...
Case Studies

• Wholly Crap That’s Good Malware

• All Your Config Files are Belong to Me

• Seriously, at Least TRY!
Wholly Crap! That’s Good Malware!
Wholly Crap! That’s Good Malware!

<table>
<thead>
<tr>
<th>Time</th>
<th>Process Name</th>
<th>PID</th>
<th>Operation</th>
<th>Path</th>
<th>Result</th>
<th>Detail</th>
</tr>
</thead>
<tbody>
<tr>
<td>2:34:3</td>
<td>inetmgr.exe</td>
<td>2540</td>
<td>CreateFile</td>
<td>C:\WINDOWS\system32\memdump</td>
<td>IS DIRECTORY</td>
<td>Desired Access: R...</td>
</tr>
<tr>
<td>2:34:3</td>
<td>inetmgr.exe</td>
<td>2540</td>
<td>CreateFile</td>
<td>C:\WINDOWS\system32</td>
<td>SUCCESS</td>
<td>Desired Access: R...</td>
</tr>
<tr>
<td>2:34:3</td>
<td>inetmgr.exe</td>
<td>2540</td>
<td>CreateFile</td>
<td>C:\WINDOWS\system32\memdump</td>
<td>SUCCESS</td>
<td>Filter: memdump, 1:...</td>
</tr>
<tr>
<td>2:34:3</td>
<td>inetmgr.exe</td>
<td>2540</td>
<td>CreateFile</td>
<td>C:\WINDOWS\system32\memdump</td>
<td>SUCCESS</td>
<td>Desired Access: R...</td>
</tr>
<tr>
<td>2:34:3</td>
<td>inetmgr.exe</td>
<td>2540</td>
<td>QueryDirectory</td>
<td>C:\WINDOWS\system32\memdump</td>
<td>SUCCESS</td>
<td>CreationTime: 6/2/...</td>
</tr>
<tr>
<td>2:34:3</td>
<td>inetmgr.exe</td>
<td>2540</td>
<td>CloseFile</td>
<td>C:\WINDOWS\system32\memdump</td>
<td>SUCCESS</td>
<td>Desired Access: R...</td>
</tr>
<tr>
<td>2:34:3</td>
<td>inetmgr.exe</td>
<td>2540</td>
<td>CreateFile</td>
<td>C:\WINDOWS\system32\memdump</td>
<td>IS DIRECTORY</td>
<td>Desired Access: R...</td>
</tr>
<tr>
<td>2:34:3</td>
<td>inetmgr.exe</td>
<td>2540</td>
<td>CreateFile</td>
<td>C:\WINDOWS\system32\memdump</td>
<td>SUCCESS</td>
<td>Desired Access: R...</td>
</tr>
<tr>
<td>2:34:3</td>
<td>inetmgr.exe</td>
<td>2540</td>
<td>QueryDirectory</td>
<td>C:\WINDOWS\system32\memdump</td>
<td>SUCCESS</td>
<td>Filter: memdump, 1:...</td>
</tr>
<tr>
<td>2:34:3</td>
<td>inetmgr.exe</td>
<td>2540</td>
<td>CloseFile</td>
<td>C:\WINDOWS\system32\memdump</td>
<td>SUCCESS</td>
<td>Desired Access: R...</td>
</tr>
<tr>
<td>2:34:3</td>
<td>inetmgr.exe</td>
<td>2540</td>
<td>CreateFile</td>
<td>C:\WINDOWS\system32\memdump</td>
<td>IS DIRECTORY</td>
<td>Desired Access: R...</td>
</tr>
<tr>
<td>2:34:3</td>
<td>inetmgr.exe</td>
<td>2540</td>
<td>CreateFile</td>
<td>C:\WINDOWS\system32\memdump</td>
<td>SUCCESS</td>
<td>Desired Access: R...</td>
</tr>
<tr>
<td>2:34:3</td>
<td>inetmgr.exe</td>
<td>2540</td>
<td>QueryDirectory</td>
<td>C:\WINDOWS\system32\memdump</td>
<td>SUCCESS</td>
<td>Filter: memdump, 1:...</td>
</tr>
<tr>
<td>2:34:3</td>
<td>inetmgr.exe</td>
<td>2540</td>
<td>CloseFile</td>
<td>C:\WINDOWS\system32\memdump</td>
<td>SUCCESS</td>
<td>Desired Access: R...</td>
</tr>
<tr>
<td>2:34:3</td>
<td>inetmgr.exe</td>
<td>2540</td>
<td>CreateFile</td>
<td>C:\WINDOWS\system32\memdump</td>
<td>IS DIRECTORY</td>
<td>Desired Access: R...</td>
</tr>
<tr>
<td>2:34:3</td>
<td>inetmgr.exe</td>
<td>2540</td>
<td>CreateFile</td>
<td>C:\WINDOWS\system32\memdump</td>
<td>SUCCESS</td>
<td>Desired Access: R...</td>
</tr>
<tr>
<td>2:34:3</td>
<td>inetmgr.exe</td>
<td>2540</td>
<td>QueryDirectory</td>
<td>C:\WINDOWS\system32\memdump</td>
<td>SUCCESS</td>
<td>Filter: memdump, 1:...</td>
</tr>
<tr>
<td>2:34:3</td>
<td>inetmgr.exe</td>
<td>2540</td>
<td>CloseFile</td>
<td>C:\WINDOWS\system32\memdump</td>
<td>SUCCESS</td>
<td>Desired Access: R...</td>
</tr>
<tr>
<td>2:34:3</td>
<td>inetmgr.exe</td>
<td>2540</td>
<td>CreateFile</td>
<td>C:\WINDOWS\system32\memdump</td>
<td>IS DIRECTORY</td>
<td>Desired Access: R...</td>
</tr>
<tr>
<td>2:34:3</td>
<td>inetmgr.exe</td>
<td>2540</td>
<td>CreateFile</td>
<td>C:\WINDOWS\system32\memdump</td>
<td>SUCCESS</td>
<td>Desired Access: R...</td>
</tr>
<tr>
<td>2:34:3</td>
<td>inetmgr.exe</td>
<td>2540</td>
<td>QueryDirectory</td>
<td>C:\WINDOWS\system32\memdump</td>
<td>SUCCESS</td>
<td>Filter: memdump, 1:...</td>
</tr>
<tr>
<td>2:34:3</td>
<td>inetmgr.exe</td>
<td>2540</td>
<td>CloseFile</td>
<td>C:\WINDOWS\system32\memdump</td>
<td>SUCCESS</td>
<td>Desired Access: R...</td>
</tr>
<tr>
<td>2:34:3</td>
<td>inetmgr.exe</td>
<td>2540</td>
<td>CreateFile</td>
<td>C:\WINDOWS\system32\memdump</td>
<td>IS DIRECTORY</td>
<td>Desired Access: R...</td>
</tr>
</tbody>
</table>

Showing 126,293 of 251,345 events (50%) Backed by page file
Wholly Crap! That’s Good Malware!
Wholly Crap! That’s Good Malware!

The malware even stomps it’s creation time...

C:\cases\timeline>strings BOH_Server_timeline.csv | grep -i inetmgr.exe
Tue Feb 25 2003 15:23:48,74752,m..b,r/rrwrxrwxrwx,0,0,32321-128-3,'C://WINDOWS/system32/inetmgr.exe

Where have I heard this before…..?

But...thanks to the fact that I know a little something something about the $MFT...
Wholly Crap! That’s Good Malware!

• While the $S_I$ can be accessed by both the operating system and the end user, the $F_N$ cannot be accessed by anything except the kernel.

• This means that it is currently not possible for the $F_N$ timestamps to be modified in anyway, by anyone.

• In the example provided on the next slide for “inetmgr.exe”, notice how the $S_I$ birth date has been modified to read June 23, 2003, while the $F_N$ birth date shows the unmodified date of June 2, 2010.
Wholly Crap! That’s Good Malware!

32324 FILE 348 1 0x38 4 1
0x0010 96 0 0x0000 0x0000
A: Tue Sep 28 21:34:57 2010 Z
C: Tue Sep 28 00:18:58 2010 Z

**B: Mon Jun 23 12:28:52 2003 Z** ← Modified birth date
0x0030 112 0 0x0000 0x0000
FN: inetmgr.exe Parent Ref: 29 Parent Seq: 1
C: Wed Jun 2 17:51:20 2010 Z

**B: Wed Jun 2 17:51:20 2010 Z** ← Accurate birth date
0x0080 72 1 0x0000 0x0000
All Your Config Files are Belong to Me!
All Your Config Files are Belong to Me!

Found “rpcsrv.exe” which is a known memory dumper... but wait... where is the dump file?

C:\cases\timeline\> strings boh_timeline.csv | grep -i "rpcsrv.exe"

Mon Feb 15 2010 07:10:34,128000,...b,r/rrwxrwxrwx,0,0,10140-128-3,'C:/'/WINDOWS/system32/rpcsrv.exe

Thu Feb 18 2010 02:01:04,128000,m...,r/rrwxrwxrwx,0,0,10140-128-3,'C:/'/WINDOWS/system32/rpcsrv.exe

Wed Oct 06 2010 13:02:35,128000,.c.,r/rrwxrwxrwx,0,0,10140-128-3,'C:/'/WINDOWS/system32/rpcsrv.exe

Wed Oct 06 2010 18:15:51,128000,a..,r/rrwxrwxrwx,0,0,10140-128-3,'C:/'/WINDOWS/system32/rpcsrv.exe
All Your Config Files are Belong to Me!

Ah...there’s the dump file...

C:\cases\timeline\> strings boh_timeline.csv | grep -i "bios12.rom"

Thu Feb 18 2010 02:04:01,21278,...b,r/rrwxrwxrwx,0,0,5475-128-3,'C:\'\WINDOWS\system32\bios12.rom

Fri Sep 24 2010 19:06:36,21278,m.c.,r/rrwxrwxrwx,0,0,5475-128-3,'C:\'\WINDOWS\system32\bios12.rom

Wed Oct 06 2010 20:52:10,21278,.a..,r/rrwxrwxrwx,0,0,5475-128-3,'C:\'\WINDOWS\system32\bios12.rom
All Your Config Files are Belong to Me!

Well not wait a tick...what happened on the system on February 18th?

C:\cases\timeline\> strings boh_timeline.csv | grep -i "feb 18 2010" | grep -i ".b,r"

Thu Feb 18 2010 01:50:00,101326,m..b,r/rrwxrwxrwx,0,0,22056-128-3,'C:/WINDOWS/system32/log
Thu Feb 18 2010 02:04:01,21278,...b,r/rrwxrwxrwx,0,0,5475-128-3,'C:/WINDOWS/system32/bios12.rom
Thu Feb 18 2010 14:29:38,203776,...b,r/rrwxrwxrwx,0,0,18101-128-3,'C:/WINDOWS/system32/unrar.exe
Thu Feb 18 2010 14:29:58,274,...b,r/rrwxrwxrwx,0,0,18110-128-1,'C:/WINDOWS/system32/kb852310.dll  ***
Thu Feb 18 2010 14:29:58,61440,...b,r/rrwxrwxrwx,0,0,18113-128-3,'C:/WINDOWS/system32/Searcher.dll
Thu Feb 18 2010 14:29:58,60416,...b,r/rrwxrwxrwx,0,0,18115-128-3,'C:/WINDOWS/system32/srf.exe
Thu Feb 18 2010 14:38:40,200,...b,r/rrwxrwxrwx,0,0,18205-128-1,'C:/WINDOWS/system32/graph32.dll
Thu Feb 18 2010 14:38:40,59392,...b,r/rrwxrwxrwx,0,0,18230-128-4,'C:/WINDOWS/system32/pserver32.dll
Thu Feb 18 2010 14:38:40,317952,...b,r/rrwxrwxrwx,0,0,18231-128-3,'C:/WINDOWS/system32/Rar.exe
Thu Feb 18 2010 14:38:40,60928,...b,r/rrwxrwxrwx,0,0,18312-128-3,'C:/WINDOWS/system32/windll32.exe

*** Trying to disguise a file to look like a MS update file...well played...except...
All Your Config Files are Belong to Me!

Except for I found you sucka!

[Config]
time=2200
timeout=500
scancount=1000000000
r_cnt=1
r_time=60
f_passive=1
prlog=1
f_l=22789
f_log=0
f_p=gbpafkjhdgbpltwgbpltwgbfghsbplf ← This was changed from the original password.
f_h=192.168.192.168 ← This has been changed from the original IP.
p=gbplfgbpltwgbpltwgbf123gbplf
ln=c:\windows\system32\syssl.dll
an=aloh_6_%.rar ← What are you??
pr=Edcsvr.exe
stop=0
All Your Config Files are Belong to Me!

Ouch! 176 days of dump files! Dang dood!

```
C:\cases\timeline>strings boh_timeline.csv | grep -i "aloh_6" | grep -i "..b,r" | wc -l
    176
```

```
C:\cases\timeline>strings boh_timeline.csv | grep -i "aloh_6" | grep -i "..b,r" | tail -10
Sun Sep 12 2010 22:00:01,476,m.cb,r/rrwxrwxrwx,0,0,4812-128-1,'C:/WINDOWS/system32/aloh_6_912.rar
Mon Sep 13 2010 22:00:02,492,m.cb,r/rrwxrwxrwx,0,0,5710-128-1,'C:/WINDOWS/system32/aloh_6_913.rar
Tue Sep 14 2010 22:00:02,476,...b,r/rrwxrwxrwx,0,0,23873-128-1,'C:/WINDOWS/system32/aloh_6_914.rar
Wed Sep 15 2010 22:00:01,332,m.cb,r/rrwxrwxrwx,0,0,20625-128-1,'C:/WINDOWS/system32/aloh_6_915.rar
Thu Sep 16 2010 22:00:03,348,m.cb,r/rrwxrwxrwx,0,0,17535-128-1,'C:/WINDOWS/system32/aloh_6_916.rar
Fri Sep 17 2010 22:00:00,364,...b,r/rrwxrwxrwx,0,0,20149-128-1,'C:/WINDOWS/system32/aloh_6_917.rar
Sat Sep 18 2010 22:00:01,316,...b,r/rrwxrwxrwx,0,0,11228-128-1,'C:/WINDOWS/system32/aloh_6_918.rar
Tue Sep 21 2010 22:00:01,364,m.cb,r/rrwxrwxrwx,0,0,2506-128-1,'C:/WINDOWS/system32/aloh_6_921.rar
Wed Sep 22 2010 22:00:02,396,m.cb,r/rrwxrwxrwx,0,0,11368-128-1,'C:/WINDOWS/system32/aloh_6_922.rar
Fri Sep 24 2010 22:00:00,396,m.cb,r/rrwxrwxrwx,0,0,20377-128-1,'C:/WINDOWS/system32/aloh_6_924.rar
```
Seriously, at Least Try!
Seriously, at Least Try!

User Information

--------------------
Username        : DEFAULT [1005]
Full Name       :
User Comment    :
Account Created : Fri May 2 17:18:47 2008 Z
Last Login Date : Tue Oct 19 16:16:10 2010 Z
Pwd Reset Date  : Sat Sep 4 11:24:24 2010 Z ← Although the password was reset on this date, it was still the default!
Pwd Fail Date   : Tue Sep 14 11:45:34 2010 Z
Login Count     : 1300
  --> Password does not expire ← No password expiration policy is in place.
  --> Normal user account

Although the password was reset on this date, it was still the default!
No password expiration policy is in place.
Seriously, at Least Try!

TypedURLs

Software\Microsoft\Internet Explorer\TypedURLs

LastWrite Time Thu Sep 23 10:48:17 2010 (UTC)
  url1 -> \term1\BOOTDRV\WINDOWS\security
  url2 -> \term3\BOOTDRV\WINDOWS\security
  url3 -> \term4\BOOTDRV\WINDOWS\security
  url4 -> \term5\BOOTDRV\WINDOWS\security
  url5 -> \term6\BOOTDRV\WINDOWS\security
  url6 -> \term7\BOOTDRV\WINDOWS\security

What? No GUI? That’s OK...net use works just fine...
Seriously, at Least Try!

Perfect Keylogger, running from it’s default location...

And Actual Spy Monitor...
Seriously, at Least Try!

Not shown: 998 filtered ports
PORT   STATE SERVICE VERSION
25/tcp  open  smtp   netqmail smtpd 1.04
1111/tcp open  tcpwrapped

Anybody wanna guess what the exfiltration mechanism was?
Conclusion

- Go after ONLY the data you need to go after
  - Get out of the “image everything” mindset
- Be consistent in your approach to each case
  - Build a methodology that works for you and follow it
  - Consistency builds efficiency and accuracy
- You can do multiple things at once
  - Don’t’ get stuck thinking “I have to wait for my images to complete”!
  - There is a LOT than can be done while images are burning
- Become familiar with the command line
  - Learn the switches for grep, gawk, and cut
  - Learn how to stack commands
Conclusion

• **Take good notes**
  • Good case notes will literally write your final report for you
  • Keeps you from forgetting what you did three days ago

• **Learn what data resides in which locations, and why it’s important**
  • Registry hives
  • NTUSER.dat
  • Timelines
  • $MFT
  • Event Logs

• **Get HOT! Time’s a wastin!**