Hacking Exposed 7
Network Security Secrets & Solutions

Chapter 6 Cybercrime and Advanced Persistent Threats

Cybercrime and Advanced Persistent Threats

- What is an APT?
  - Operation Aurora
  - Anonymous
  - RBN
- What APTs are not?
- Examples of popular APT tools and techniques
- Common APTs indicators (detection, forensics)

What is an APT?

Advanced Persistent Threat (APT)

- Advanced
  - Uses sophisticated methods, such as zero-day exploits, crafting custom exploits.
- Persistent
  - Attacker returns to target system over and over again
  - Attacker has a long-term goal
  - Attacker works to achieve goals without detection
- Threat: organized, funded, and motivated

APT Goals

- Non-APT Attacks
  - Non-APT attacks are against "targets of opportunity"— just find vulnerable systems
  - Non-APT attacks are brief: smash and grab
- APT
  - Used to steal large amounts of data from a corporation over a long period of time
  - **Long-term goals**

Crime v. Espionage

- Two types of APTs
  - Crime
    - Steal PII, financial information, or corporate data just to use it for fraud
  - Espionage – industry or state-sponsored
    - Gather intellectual property or trade secrets
    - To gain competitive advantage
- APT goal is to gain and maintain access to information

APT Attacks

- Don't destroy systems
- Don't interrupt normal operation
- Try to stay hidden and keep the stolen data flowing
- Most often starts from spear phishing
  - Trick a user into installing malware

Hiding APT Techniques

- Cut-outs
  - Attacks are routed through other compromised computers to conceal attacker's location
- Dropper delivery services
  - "Pay per install" or "Leased" campaigns

Other APT Techniques

- SQL injection to add malware to websites
- Infected USB stick "drops"
- Infected hardware or software
- Social engineering, impersonating users, etc
- Less often: compromised human insiders

APT Phases

- Targeting
  - Collect info about the target and test: vulnerability scanning, social engineering, spear-phishing
- Access/compromise
  - Gain access: ascertain host info, collect credentials for additional compromises, obfuscate intention by malware
- Reconnaissance
  - Enumerate networks and systems
- Lateral movement
  - Move through network to other hosts
- Data collection and exfiltration
  - Establish collection points and exfiltrate via proxy
- Administration and maintenance
  - Maintain access over time

Detecting APTs

- Email logs
- Lateral movement may leave artifacts from misuse of access credentials or identities
- Exfiltration may leave traces in
  - Firewall and IDS logs
  - Data Loss Prevention logs
  - Application history logs
  - Web server logs

Forensics

- Artifacts of APT may be found in
  - Live file systems (RAM)
  - Hard disk image

Historical APT Campaigns

Historical APT Attacks

- Aurora
- Nitro
- ShadyRAT
- Lurid
- Night Dragon
- Stuxnet
- DuQu

Operation Aurora

2009

Targets: U.S. Technology and Defense Industries

- Google
- Juniper
- Adobe
- At least 29 other companies lost data over a period as long as six months

Spear-Phishing and RAT

- Email with a link to a Taiwanese website with malicious JavaScript
  - Exploited Internet Explorer vunerability
  - Undetected by antivirus
- Trojan Downloaders placed on victim computers
- Installed a Backdoor Trojan Remote Administration Tool (RAT)
  - Accessed through SSL

Lateral Movement

- Network reconnaissance
- Compromised Active Directory credentials
- Access to computers and network shares with valuable intellectual property

China?

- Spear-phishing and downloader linked to Taiwan
- Backdoor Command & Control servers were traced to two schools in China
- Google blamed China
- No proof that Chinese government or industry sponsored or supported the attacks

Other APT Campaigns

- "Night Dragon" in 2010
- "RSA Breach" in 2011
- "Shady RAT" spanned several years
  - All commonly attributed to China, but not proven

- Commonly attributed APTs' C&C: China, India, Pakistan, Malaysia, Korea, UAE, Russia, USA, Mexico, Brazil.

Anonymous

2011

Anonymous

- From 2011, a loosely affiliated group or collection of groups, to expose sensitive info to public or interrupt services (DOS)
- A variety of hacking techniques
  - SQL injection, cross-site scripting, web service vulnerability exploits, social engineering (targeted spear-phishing, imitating employees like help desk personnel)

Targets

- Government agencies at all levels
- Sony
- Bay Area Rapid Transit (BART)
- Mastercard & Visa
- Many, many more

Techniques

- SQL injection
- Cross-site scripting
- Web service vulnerability exploits
- Social engineering

Goals

- Demonstrate that people can strike back at powerful organizations
- Expose corruption
- Primary goal: expose information
  - Not to use it for competitive or financial gain

RBN

RBN (Russian Business Network)

- From St. Petersburg to international cybercrime
- Operates several botnets for spamming, phishing, malware distribution
  - Identity or financial theft
  - Very sophisticated malware tools to remain persistent
  - A platform for subscribers to conduct activities
- Hosts pornographic subscription websites
- Main goal is identity theft and financial theft

APT Tools and Techniques

Examples of Tools and Techniques used in APT Campaigns

- Gh0st attack
- Malicious email

Investigate a potential “victim” system:

- Indicators of compromise
- Memory capture
- File/process capture
- Lost Linux host

Ghost Attack

- GhostRAT used in the "Ghostnet" attacks 2008-2010
- Targeted the Dalai Lama (Tibetan Government-in-Exile in India, London and New York City) and other Tibetan enterprises

Feature	Description
Existing rootkit removal	Clears System Service Descriptor Tables (SSDT) of all existing hooks
File Manager	Complete file explorer capabilities for local and remote hosts
Screen control	Complete control of remote screen.
Process Explorer	Complete listing of all active processes and all open windows
Keystroke logger	Real-time and offline remote keystroke logging
Remote Terminal	Fully functional remote shell
Webcam eavesdropping	Live video feed of remote web camera, if available
Voice monitoring	Live remote listening using installed microphone, if available

Table 6-1 Ghost RAT Capabilities (Courtesy of Michael Spohn, Foundstone Professional Services)

Dial-up profile cracking	Listing of dial-up profiles, including cracked passwords.
Remote screen blanking	Blanks compromised host screen, making computer unusable
Remote input blocking	Disables compromised host mouse and keyboard
Session management	Remote shutdown and reboot of host
Remote file downloads	Ability to download binaries from the Internet to remote host
Custom Gh0st server creation	Configurable server settings placed into custom binary

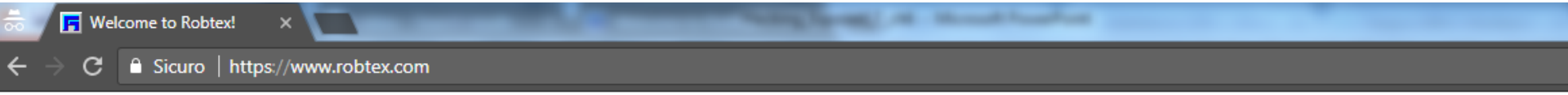
Summary of Gh0st Attack

- Phishing email
- Backdoor placed when malicious link clicked
- Backdoor hides itself to survive a reboot
- Connection to C&C
- Check internal domain, create accounts, use Terminal Server to hop to other hosts (Event Logs)
- Add/modify some files (diff \System32)
- Look for documents and zip for exfiltration
- Create a 2nd backdoor using netcat
- Create user account and execute FTP (Windows Security Event Log)
- Schedule a new job to clean logs everyday

GhostNET Phishing

- Attack started with an email from a server on several blacklists for spamming
- Tools used to research source of email
  - Whois
  - Robtex
  - Phishtank

Robtex



What is Robtex used for?

Robtex is used for various kinds of research of IP numbers, Domain names, etc

Are you a normal IT guy doing data forensics, investigating competitors, tracking spammers or hackers or a virus, or just curious? No m
this should be the first place to go

What does Robtex do?

Robtex uses various sources to gather public information about IP numbers, domain names, host names, Autonomous systems, routes e
indexes the data in a big database and provide free access to the data.

We aim to make the fastest and most comprehensive free DNS lookup tool on the Internet.

Our database now contains billions of documents of internet data collected over more than a decade.

How to use Robtex?

Enter an IP address or hostname in the field above, and click "GO" to look up technical information. From the resulting page you can na
between the different tabs

www.phishtank.com/stats.php

PhishTank is operated by OpenDNS, a free service that makes your Internet safer, faster, and smarter. Get started today!

PhishTank® Out of the Net, into the Tank.

username ••••••••• Sign In

Register | Forgot Password

Home | Add A Phish | Verify A Phish | Phish Search | Stats | FAQ | Developers | Mailing Lists | My Account

Stats

Monthly Stats Archive:

Online, valid phishes	Total Submissions	Total Votes
6,594	1,550,580	6,112,989

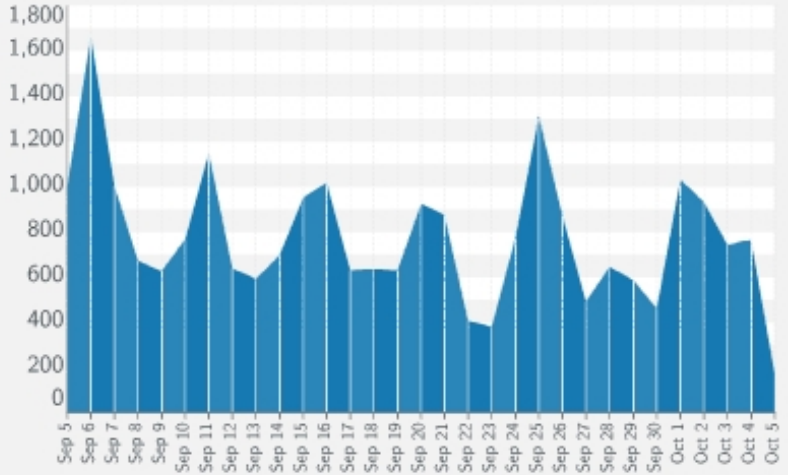
Phishes Verified as Valid		Suspected Phishes Submitted	
Total:	950,446	Total:	1,550,581
Online:	6,594	Online:	6,850
Offline:	943,852	Offline:	1,543,697

Most Active Users (out of 57,301 total)

Top 10 Submitters

1	PhishReporter	510,356 phishes
2	cleanmx	205,903 phishes
3	antiphishing	105,503 phishes
4	spamfighter	55,210 phishes

Daily Phishes Verified
chart created Oct 5 2012 17:26 UTC



Daily Phishes Submitted
chart created Oct 5 2012 17:26 UTC

Indicators of Compromise

- How to survive reboot:
  - Using various “Run” Registry keys
  - Creating a service
  - Hooking into an existing service
  - Using a scheduled task
  - Disguising communications as valid traffic
  - Overwriting the master boot record
  - Overwriting the system’s BIOS

Order of Volatility

- Memory
- Page or swap file
- Running process information
- Network data such as listening ports or existing connections to other systems
- System Registry (if applicable)
- System or application log files
- Forensic image of disk(s)
- Backup media

Forensic Tools copied to CD-ROM

- AccessData FTK Imager
- Sysinternals Autoruns
- Sysinternals Process Explorer
- Sysinternals Process Monitor
- WinMerge
- Currports
- Sysinternals Vmmap

Memory Dump Analysis

- Crucial for APT analysis because many APT methods use process injection or obfuscation
- Analyzing RAM data guarantees that the data are **unencrypted**

- **FTK Imager:** select the Capture Memory option, select an external mass-storage device as the output folder

Pagefile/Swapfile Analysis

- Virtual memory on pagefile.sys
- Also Hiberfil.sys
- Preferable to collect a forensic disk image of a compromised or suspicious computer
- Memory snapshot analysis Tools:
  - HBGary FDPro
  - Mandiant Memoryze
  - Volatility Framework - open source

Login - Comae Stardust

Sicuro | https://my.comae.io/login

STARDUST

By Comae BETA

Enterprise memory forensics for threat detection and hunting.

***Yes**, you are at the right place to download **DumpIt**. Sign up to continue.*

soon

Get Started

Email

Passw

Memory Analysis

- Using Volatility Framework Tool (open source) to analyze memory
  - Processes
  - Network connections
  - DLLS from suspicious process
  - Use strings on the DLL

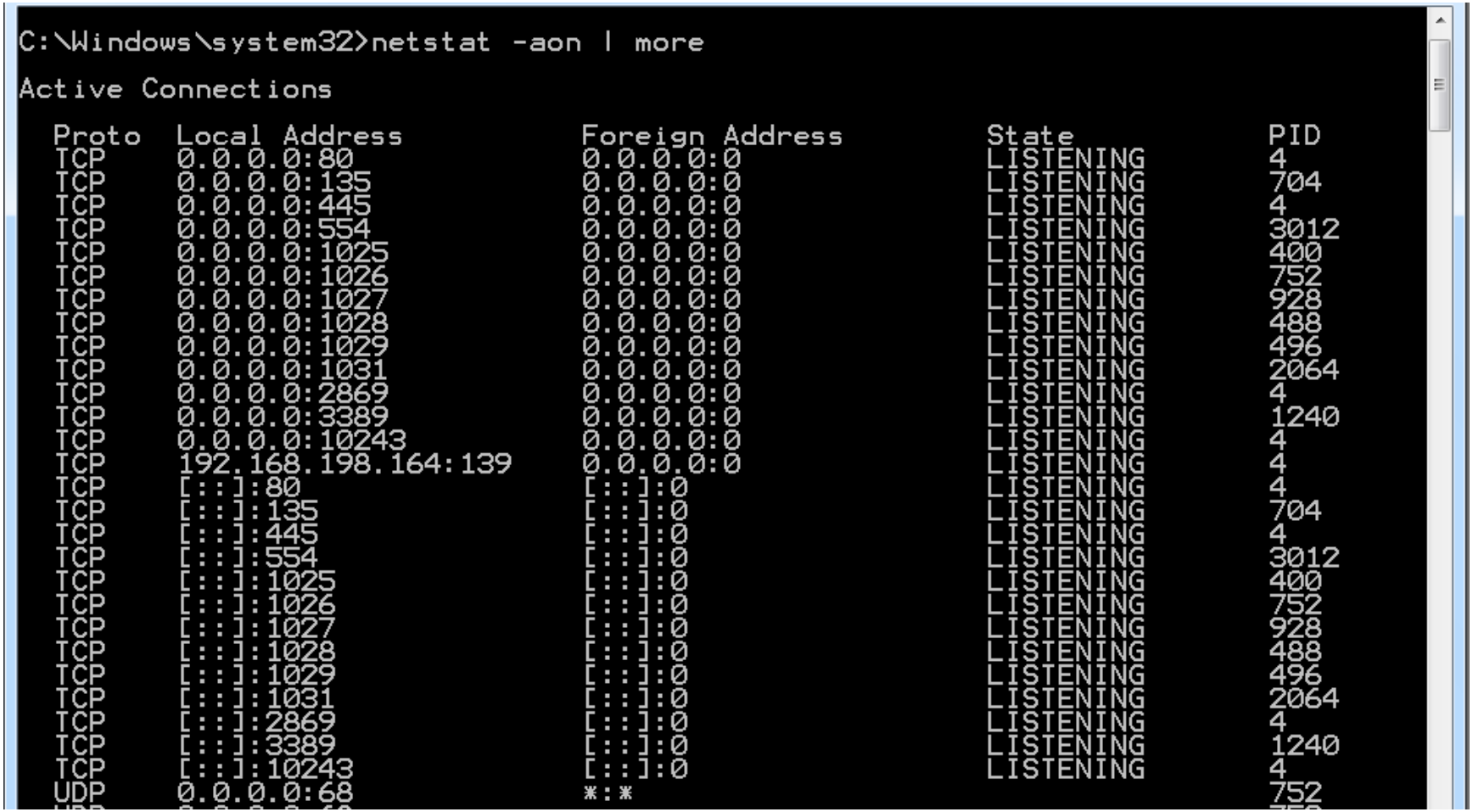
File/Process Capture (1/2)

- Master File Table (MFT): metadata (filename, timestamp, file size, etc.), timeline is important
- Network/process/registry: netstat to find connections and process PID
- Host file: check any changes
- Currports: look into a current open port and its DLL
- Process Explorer: lookup a process, its DLL references, and cmd.exe shell executions
- Process Monitor: lookup process-kernel interactions → understand how malware modifies a compromised system and provide indicators for detection tools
- VMMap: show virtual/physical memory map, check DLL strings → malware strings to imply RAT
- DNS Cache: find other possible infection hosts
- Registry Query: reg query to check for suspicious Registry entries of Run keys

File/Process Capture (2/2)

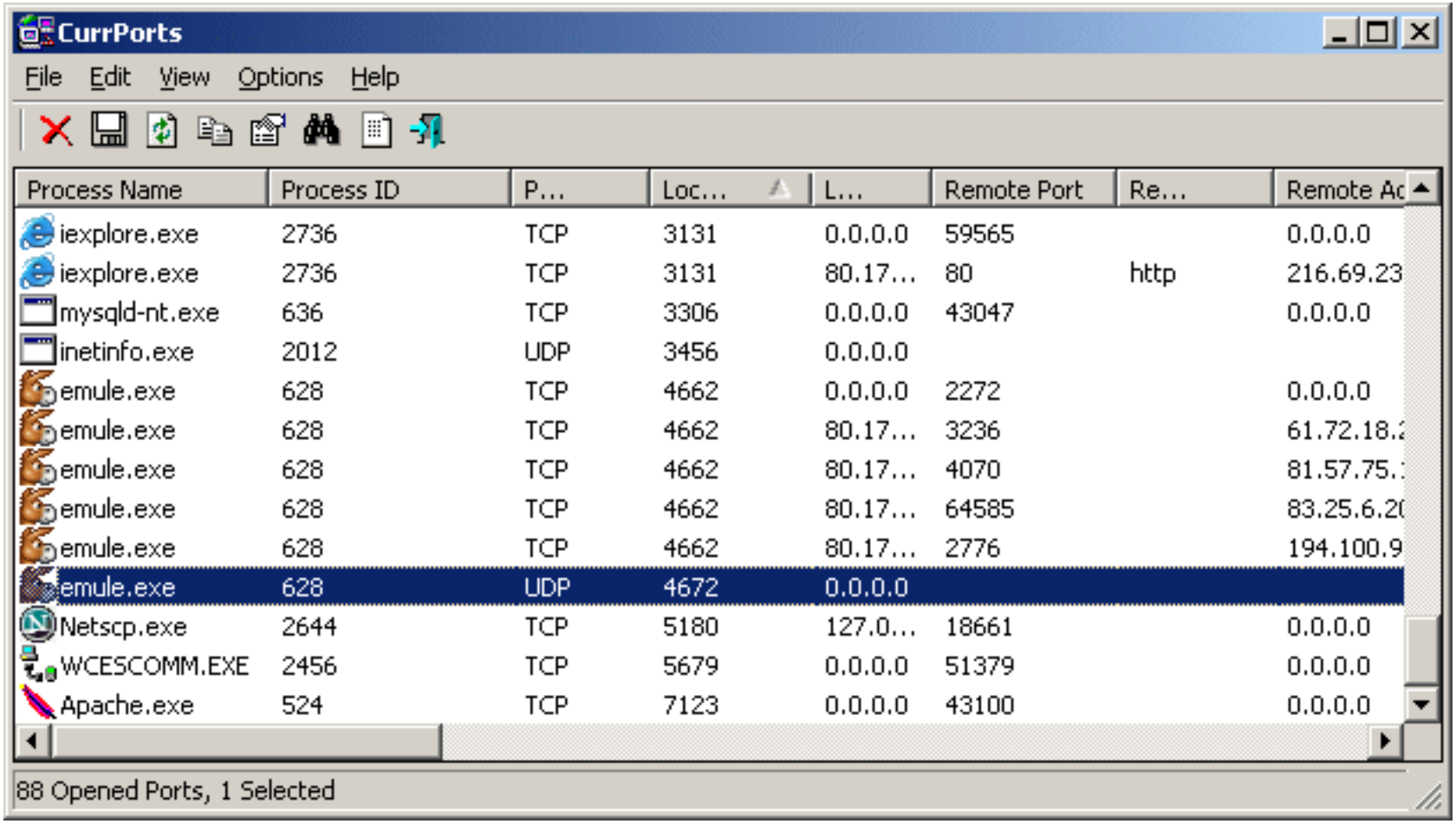
- Scheduled Tasks: at to find scheduled tasks
- Event Logs: psloglist to retrieve System and Security Event logs → commands issued by attackers
- Prefetch Directory: last 128 unique programs executed
- Collecting interesting files: ntuser.dat (user profile), index.dat (requested URLs), .rdp files (remote desktop session info), .bmc files (bit map to clients), antivirus log files (virus alerts)
- Analyzing RDP files: servers accessed, login info, etc. in XML → attackers use RDP to connect to other servers
- Analyzing BMC files: cached bitmap image for performance → BMC Viewer to find attacker's access to applications, files, network, credentials
- Investigating System 32 Directory for anomalies: diff system32 directory with cache directory to find files changed since installation → .dll, .bat, .rar, .txt
- Antivirus logs: check configurations that exclude detection of certain PUP (Potentially Unwanted Program), e.g. netcat/nc
- Network: analyze traffic between compromised host to C&C server → other targeted hosts → signatures for IDS

Netstat -aon

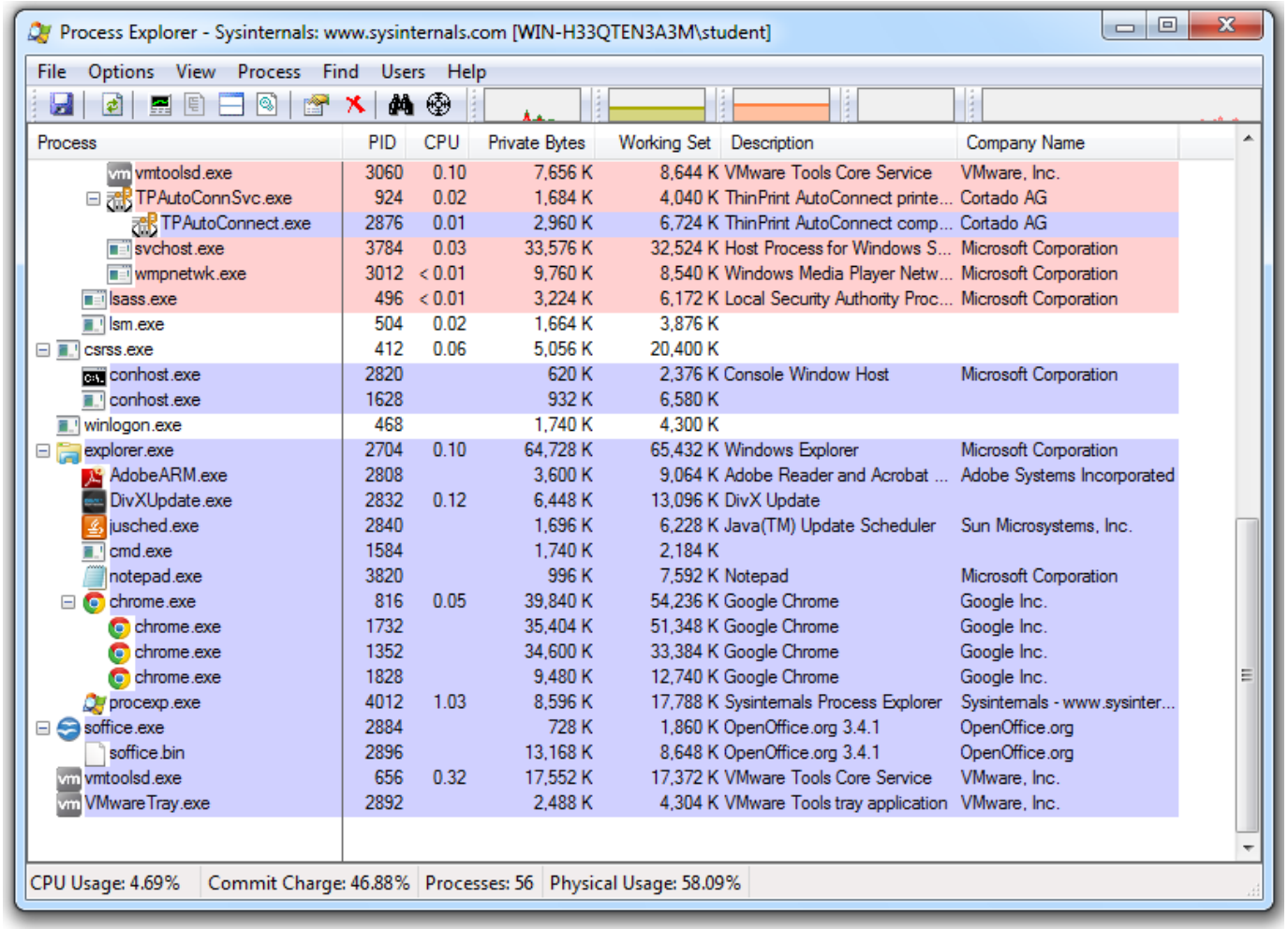


```
C:\Windows\system32>netstat -aon | more

Active Connections

  Proto  Local Address          Foreign Address        State           PID
  TCP    0.0.0.0:80             0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       704
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:554            0.0.0.0:0              LISTENING       3012
  TCP    0.0.0.0:1025           0.0.0.0:0              LISTENING       400
  TCP    0.0.0.0:1026           0.0.0.0:0              LISTENING       752
  TCP    0.0.0.0:1027           0.0.0.0:0              LISTENING       928
  TCP    0.0.0.0:1028           0.0.0.0:0              LISTENING       488
  TCP    0.0.0.0:1029           0.0.0.0:0              LISTENING       496
  TCP    0.0.0.0:1031           0.0.0.0:0              LISTENING       2064
  TCP    0.0.0.0:2869           0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:3389           0.0.0.0:0              LISTENING       1240
  TCP    0.0.0.0:10243          0.0.0.0:0              LISTENING       4
  TCP    192.168.198.164:139    0.0.0.0:0              LISTENING       4
  TCP    [::]:80                [::]:0                 LISTENING       4
  TCP    [::]:135               [::]:0                 LISTENING       704
  TCP    [::]:445               [::]:0                 LISTENING       4
  TCP    [::]:554               [::]:0                 LISTENING       3012
  TCP    [::]:1025              [::]:0                 LISTENING       400
  TCP    [::]:1026              [::]:0                 LISTENING       752
  TCP    [::]:1027              [::]:0                 LISTENING       928
  TCP    [::]:1028              [::]:0                 LISTENING       488
  TCP    [::]:1029              [::]:0                 LISTENING       496
  TCP    [::]:1031              [::]:0                 LISTENING       2064
  TCP    [::]:2869              [::]:0                 LISTENING       4
  TCP    [::]:3389              [::]:0                 LISTENING       1240
  TCP    [::]:10243             [::]:0                 LISTENING       4
  UDP    0.0.0.0:68             *:*                                    752
```

CurrPorts

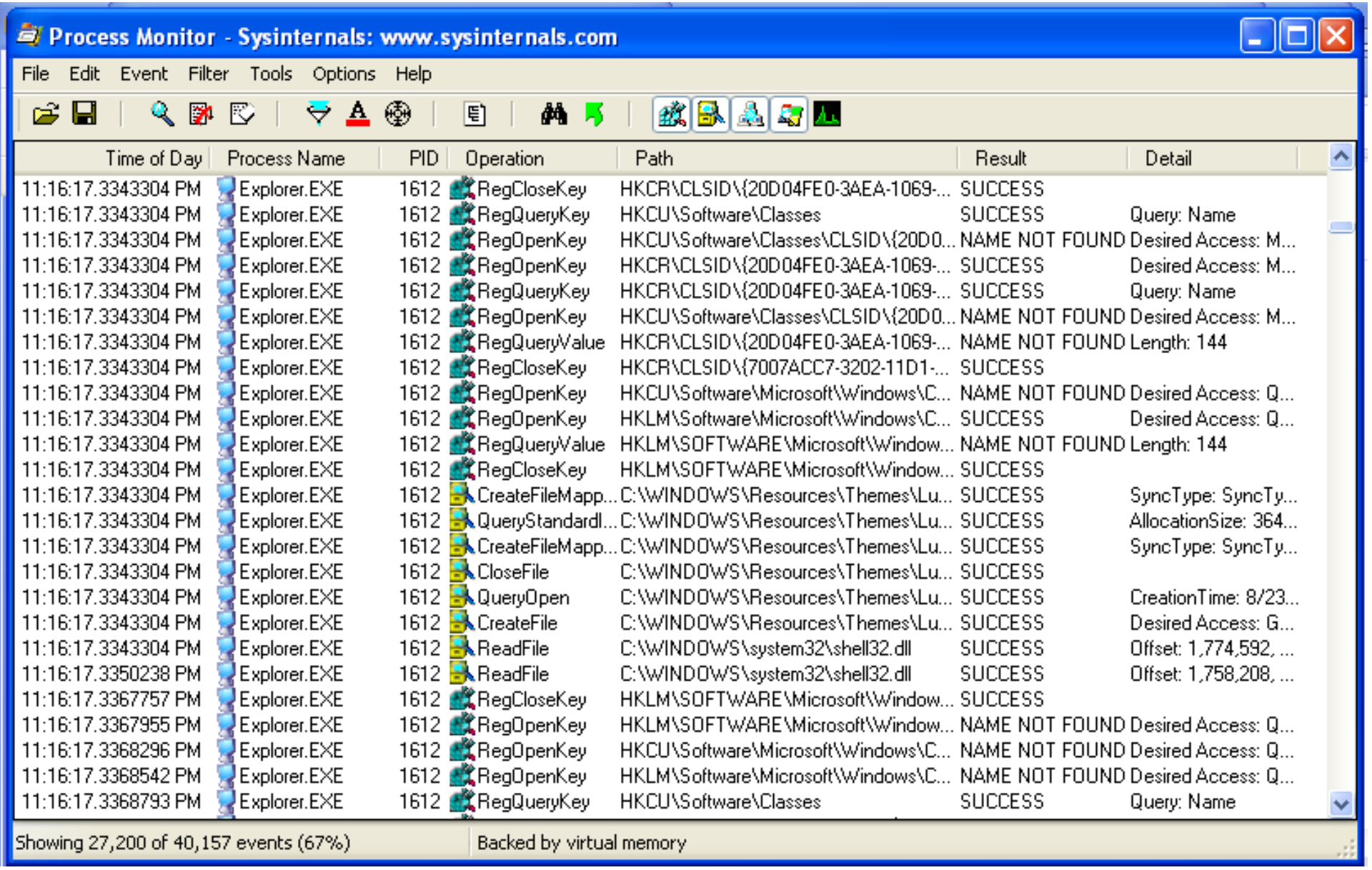

CurrPorts
File Edit View Options Help
Process Name | Process ID | P... | Loc... | L... | Remote Port | Re... | Remote Ac
iexplore.exe 2736 TCP 3131 0.0.0.0 59565 0.0.0.0
iexplore.exe 2736 TCP 3131 80.17... 80 http 216.69.23
mysqld-nt.exe 636 TCP 3306 0.0.0.0 43047 0.0.0.0
inetinfo.exe 2012 UDP 3456 0.0.0.0
emule.exe 628 TCP 4662 0.0.0.0 2272 0.0.0.0
emule.exe 628 TCP 4662 80.17... 3236 61.72.18.
emule.exe 628 TCP 4662 80.17... 4070 81.57.75.
emule.exe 628 TCP 4662 80.17... 64585 83.25.6.2
emule.exe 628 TCP 4662 80.17... 2776 194.100.9
emule.exe 628 UDP 4672 0.0.0.0
Netscp.exe 2644 TCP 5180 127.0... 18661 0.0.0.0
WCESCOMM.EXE 2456 TCP 5679 0.0.0.0 51379 0.0.0.0
Apache.exe 524 TCP 7123 0.0.0.0 43100 0.0.0.0
88 Opened Ports, 1 Selected

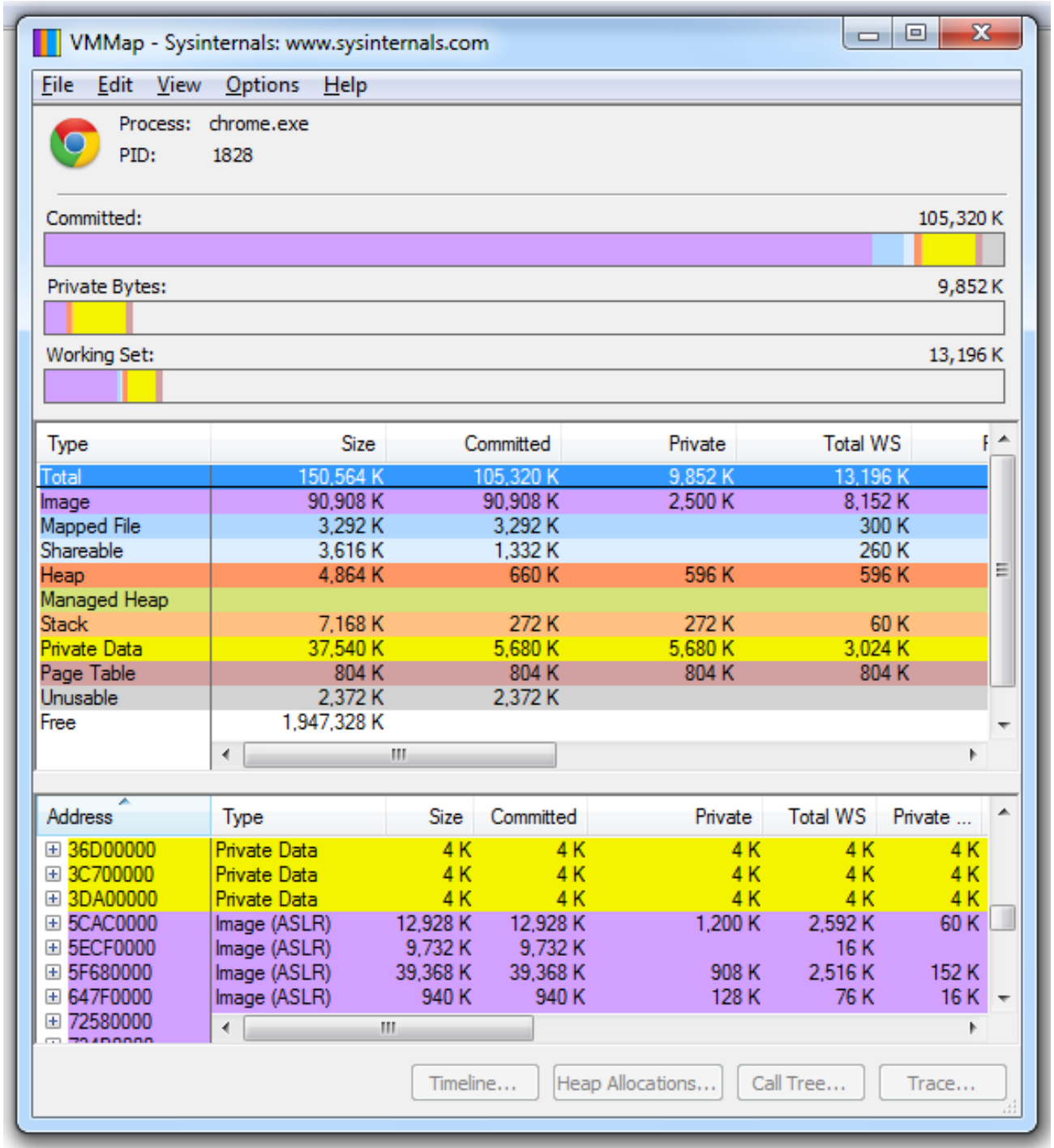
Process Explorer



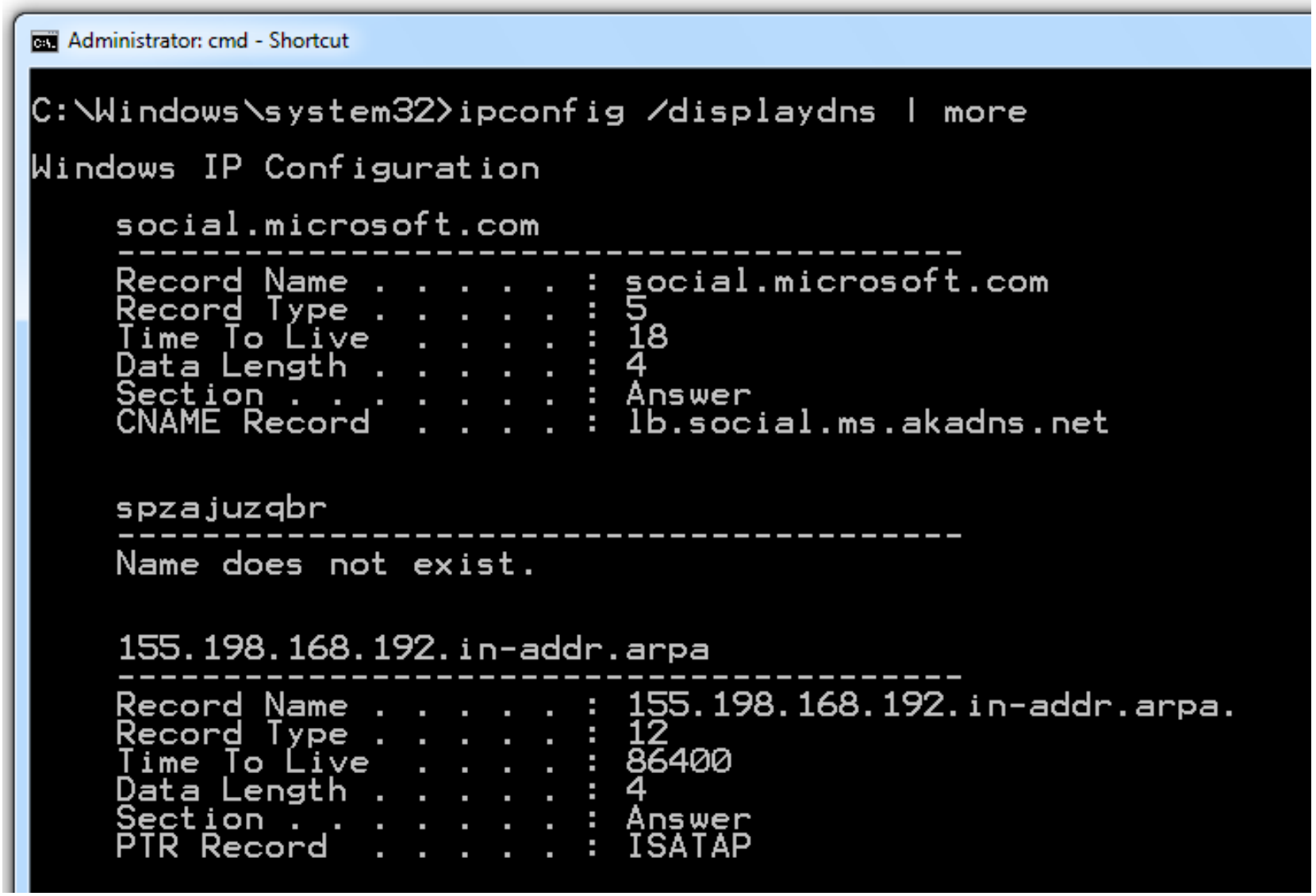
Other SysInternals Tools

- Process Monitor
  - View all kernel interactions that processes make as the system runs
  - Very useful to run during malware infection
- VMMap
  - Analyzes virtual memory and physical memory used by a process
  - Can extract strings from the processes


Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help
Time of Day Process Name PID Operation Path Result Detail
11:16:17.3343304 PM Explorer.EXE 1612 RegCloseKey HKCR\CLSID\{20D04FE0-3AEA-1069-... SUCCESS
11:16:17.3343304 PM Explorer.EXE 1612 RegQueryKey HKCU\Software\Classes SUCCESS Query: Name
11:16:17.3343304 PM Explorer.EXE 1612 RegOpenKey HKCU\Software\Classes\CLSID\{20D0... NAME NOT FOUND Desired Access: M...
11:16:17.3343304 PM Explorer.EXE 1612 RegOpenKey HKCR\CLSID\{20D04FE0-3AEA-1069-... SUCCESS Desired Access: M...
11:16:17.3343304 PM Explorer.EXE 1612 RegQueryKey HKCR\CLSID\{20D04FE0-3AEA-1069-... SUCCESS Query: Name
11:16:17.3343304 PM Explorer.EXE 1612 RegOpenKey HKCU\Software\Classes\CLSID\{20D0... NAME NOT FOUND Desired Access: M...
11:16:17.3343304 PM Explorer.EXE 1612 RegQueryValue HKCR\CLSID\{20D04FE0-3AEA-1069-... NAME NOT FOUND Length: 144
11:16:17.3343304 PM Explorer.EXE 1612 RegCloseKey HKCR\CLSID\{7007ACC7-3202-11D1-... SUCCESS
11:16:17.3343304 PM Explorer.EXE 1612 RegOpenKey HKCU\Software\Microsoft\Windows\C... NAME NOT FOUND Desired Access: Q...
11:16:17.3343304 PM Explorer.EXE 1612 RegOpenKey HKLM\Software\Microsoft\Windows\C... SUCCESS Desired Access: Q...
11:16:17.3343304 PM Explorer.EXE 1612 RegQueryValue HKLM\SOFTWARE\Microsoft\Window... NAME NOT FOUND Length: 144
11:16:17.3343304 PM Explorer.EXE 1612 RegCloseKey HKLM\SOFTWARE\Microsoft\Window... SUCCESS
11:16:17.3343304 PM Explorer.EXE 1612 CreateFileMapp... C:\WINDOWS\Resources\Themes\Lu... SUCCESS SyncType: SyncTy...
11:16:17.3343304 PM Explorer.EXE 1612 QueryStandardI... C:\WINDOWS\Resources\Themes\Lu... SUCCESS AllocationSize: 364...
11:16:17.3343304 PM Explorer.EXE 1612 CreateFileMapp... C:\WINDOWS\Resources\Themes\Lu... SUCCESS SyncType: SyncTy...
11:16:17.3343304 PM Explorer.EXE 1612 CloseFile C:\WINDOWS\Resources\Themes\Lu... SUCCESS
11:16:17.3343304 PM Explorer.EXE 1612 QueryOpen C:\WINDOWS\Resources\Themes\Lu... SUCCESS CreationTime: 8/23...
11:16:17.3343304 PM Explorer.EXE 1612 CreateFile C:\WINDOWS\Resources\Themes\Lu... SUCCESS Desired Access: G...
11:16:17.3343304 PM Explorer.EXE 1612 ReadFile C:\WINDOWS\system32\shell32.dll SUCCESS Offset: 1,774,592, ...
11:16:17.3350238 PM Explorer.EXE 1612 ReadFile C:\WINDOWS\system32\shell32.dll SUCCESS Offset: 1,758,208, ...
11:16:17.3367757 PM Explorer.EXE 1612 RegCloseKey HKLM\SOFTWARE\Microsoft\Window... SUCCESS
11:16:17.3367955 PM Explorer.EXE 1612 RegOpenKey HKLM\SOFTWARE\Microsoft\Window... NAME NOT FOUND Desired Access: Q...
11:16:17.3368296 PM Explorer.EXE 1612 RegOpenKey HKCU\Software\Microsoft\Windows\C... NAME NOT FOUND Desired Access: Q...
11:16:17.3368542 PM Explorer.EXE 1612 RegOpenKey HKLM\Software\Microsoft\Windows\C... NAME NOT FOUND Desired Access: Q...
11:16:17.3368793 PM Explorer.EXE 1612 RegQueryKey HKCU\Software\Classes SUCCESS Query: Name
Showing 27,200 of 40,157 events (67%)
Backed by virtual memory


VMMap - Sysinternals: www.sysinternals.com
File Edit View Options Help
Process: chrome.exe
PID: 1828
Committed: 105,320 K
Private Bytes: 9,852 K
Working Set: 13,196 K
Type Size Committed Private Total WS
Total 150,564 K 105,320 K 9,852 K 13,196 K
Image 90,908 K 90,908 K 2,500 K 8,152 K
Mapped File 3,292 K 3,292 K 300 K
Shareable 3,616 K 1,332 K 260 K
Heap 4,864 K 660 K 596 K 596 K
Managed Heap
Stack 7,168 K 272 K 272 K 60 K
Private Data 37,540 K 5,680 K 5,680 K 3,024 K
Page Table 804 K 804 K 804 K 804 K
Unusable 2,372 K 2,372 K
Free 1,947,328 K
Address Type Size Committed Private Total WS Private ...
36D00000 Private Data 4 K 4 K 4 K 4 K 4 K
3C700000 Private Data 4 K 4 K 4 K 4 K 4 K
3DA00000 Private Data 4 K 4 K 4 K 4 K 4 K
5CAC0000 Image (ASLR) 12,928 K 12,928 K 1,200 K 2,592 K 60 K
5ECF0000 Image (ASLR) 9,732 K 9,732 K 16 K
5F680000 Image (ASLR) 39,368 K 39,368 K 908 K 2,516 K 152 K
647F0000 Image (ASLR) 940 K 940 K 128 K 76 K 16 K
72580000
Timeline... Heap Allocations... Call Tree... Trace...

DNS Cache


Administrator: cmd - Shortcut
C:\Windows\system32>ipconfig /displaydns | more
Windows IP Configuration
social.microsoft.com
Record Name . . . . . : social.microsoft.com
Record Type . . . . . : 5
Time To Live . . . . . : 18
Data Length . . . . . : 4
Section . . . . . : Answer
CNAME Record . . . . . : lb.social.ms.akadns.net
spzajuzqbr
Name does not exist.
155.198.168.192.in-addr.arpa
Record Name . . . . . : 155.198.168.192.in-addr.arpa.
Record Type . . . . . : 12
Time To Live . . . . . : 86400
Data Length . . . . . : 4
Section . . . . . : Answer
PTR Record . . . . . : ISATAP

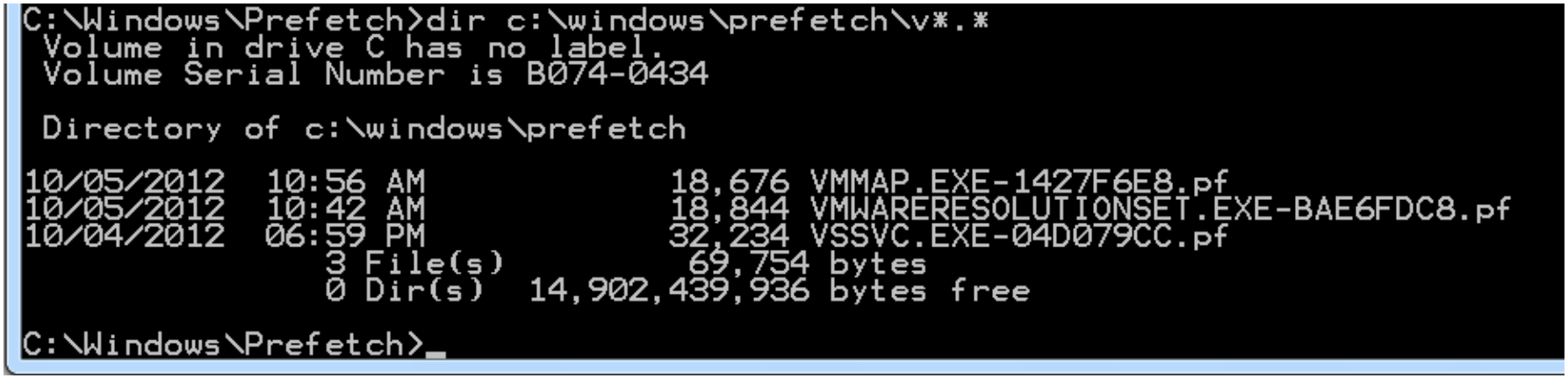
Registry Query for Run and RunOnce Keys

```
C:\Windows\system32>reg query HKLM\system\currentcontrolset\services /s | more

HKEY_LOCAL_MACHINE\system\currentcontrolset\services\.NET CLR Data

HKEY_LOCAL_MACHINE\system\currentcontrolset\services\.NET CLR Data\Linkage
    Export    REG_SZ    2e,00,4e,00,45,00,54,00,20,00,43,00,4c,00,52,00,20,00,44
,00,61,00,74,00,61,00,00,00,00,00

HKEY_LOCAL_MACHINE\system\currentcontrolset\services\.NET CLR Data\Performance
    IsMultiInstance    REG_DWORD    0x1
    CategoryOptions    REG_DWORD    0x1
    Open    REG_SZ    OpenPerformanceData
    Collect    REG_SZ    CollectPerformanceData
    Close    REG_SZ    ClosePerformanceData
    Library    REG_SZ    netfxperf.dll
    Counter Types    REG_BINARY    360035003500330036000000360035003500330036000
000360035003500330036000000360035003500330036000000360035003500330036000000360033
5003500330036000000000
```

Other Tests

- Scheduled Tasks
- Event Viewer
- Prefetch Directory
  - Records the last 128 "unique" programs executed on the system

Prefetch


C:\Windows\Prefetch>dir c:\windows\prefetch\v*.*
Volume in drive C has no label.
Volume Serial Number is B074-0434
Directory of c:\windows\prefetch
10/05/2012 10:56 AM 18,676 VMMAP.EXE-1427F6E8.pf
10/05/2012 10:42 AM 18,844 VMWARERESOLUTIONSET.EXE-BAE6FDC8.pf
10/04/2012 06:59 PM 32,234 VSSVC.EXE-04D079CC.pf
3 File(s) 69,754 bytes
0 Dir(s) 14,902,439,936 bytes free
C:\Windows\Prefetch>

Collecting Interesting Files

- **ntuser.dat** Contains the user's profile data
- **index.dat** Contains an index of requested URLs
- **.rdp files** Contains information around any remote desktop session(s)
- **.bmc files** Contains cached images of the RDC client
- **Antivirus log files** Contains virus alerts

Antivirus Exclusions

- The antivirus may have been reconfigured to allow the malware
- Packing the file is a common technique to evade antivirus

Linux APT Attack

Target Scenario

- Linux running Apache Tomcat with weak credentials, copied from an example page
- Exploit it with Metasploit through Tomcat
- cat /etc/passwd reveals usernames

```
root@bt:/etc# cat /etc/passwd | more
root:x:0:0:root:/root:/bin/bash
root2:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
```

Escalating to root

- One way: find a user with an obvious password; like their last name
- Crack superuser password

Backdoor

- Attackers upload a PHP backdoor
- Create a SUID root shell for getting root back in case a password is changed
- With Metaexploit Framework, compromised host used as a pivot host (without tools installed)
- Run shells like Meterpreter in memory without disk writes: leave little on the host

Diagnose Linux APT Attack

- Apache Tomcat server with weak credentials
- To diagnose the host
  - Block access by firewall
  - Check root account history, check added/modified files, check logs for sudo su – commands
  - Check listening ports and connections with netstat and lsof
  - Check hidden files in RAM drives, drive slack space, /dev, hard-to-see file or directory like ".. " (dot-dot-space), /tmp and /var/tmp

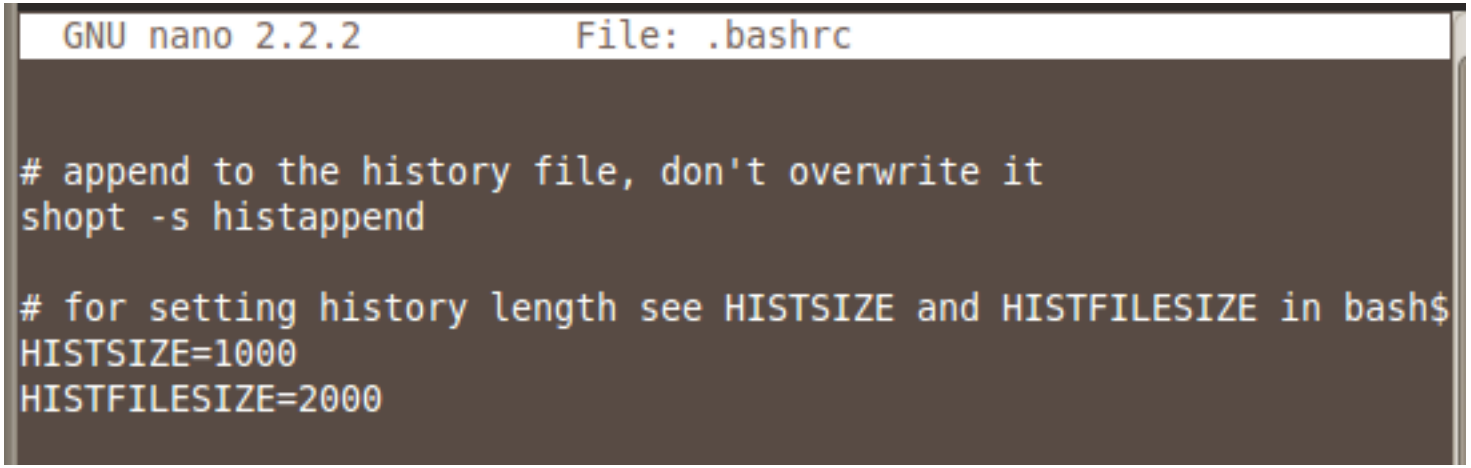
Bash History

- In each user's home directory
- .bash_history
- Remembers the previous 2000 lines by default in BackTrack 5 R2

```
root@bt:~# tail .bash_history
ps aux
watch "ps aux | grep telnet"
ls /etc/sbin/passwd
cd /
find . -name passwd
ls -l /usr/bin/passwd
ls -l
exit
telnet hills.ccsf.edu
exit
root@bt:~#
```

HISTFILESIZE

- Controlled by .bashrc in each user's home directory
  - HISTFILESIZE controls this
  - HISTSIZE is just a RAM buffer



Tomcat configured to log access requests

- Shows PUT being used to upload suspicious files

- PUT entries, someone [FROM THE INTERNET] has deployed an application on the server

Commands to Check Network Connections

- To check network connections, use

  netstat –anlp

  lsof –i -P

  - Shows all open files (and listening services)

- IMPORTANT: A rootkit could cause these programs to lie

```
root@bt:~# netstat -anlp | more
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 127.0.0.1:7175          0.0.0.0:*               LISTEN      2282/postgres
tcp        0      0 127.0.0.1:27017         0.0.0.0:*               LISTEN      860/mongod
tcp        0      0 127.0.0.1:28017         0.0.0.0:*               LISTEN      860/mongod
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      2241/sshd
tcp        0      0 127.0.0.1:8118          0.0.0.0:*               LISTEN      2221/privoxy
tcp        0      0 127.0.0.1:631           0.0.0.0:*               LISTEN      1656/cupsd
tcp        0      0 0.0.0.0:3128            0.0.0.0:*               LISTEN      1780/squid
tcp        0      0 127.0.0.1:25            0.0.0.0:*               LISTEN      2162/exim4
tcp        0      0 127.0.0.1:9050          0.0.0.0:*               LISTEN      2251/tor
tcp        0      0 192.168.198.136:36763   65.171.167.131:80       ESTABLISHED 2536/clock-applet
tcp6       0      0 ::1:7175                :::*                    LISTEN      2282/postgres
tcp6       0      0 :::22                   :::*                    LISTEN      2241/sshd
tcp6       0      0 ::1:631                 :::*                    LISTEN      1656/cupsd
tcp6       0      0 ::1:25                  :::*                    LISTEN      2162/exim4
udp        0      0 0.0.0.0:47630           0.0.0.0:*                           1780/squid
udp        0      0 0.0.0.0:3130            0.0.0.0:*                           1780/squid
udp        0      0 0.0.0.0:68              0.0.0.0:*                           3355/dhclient
udp        0      0 0.0.0.0:68              0.0.0.0:*                           1718/dhclient3
udp6       0      0 ::1:57450               ::1:57450               ESTABLISHED 2282/postgres
Active UNIX domain sockets (servers and established)
Proto RefCnt Flags       Type       State         I-Node   PID/Program name    Path
```

```
root@bt:~# lsof -i -P
COMMAND    PID        USER   FD   TYPE DEVICE SIZE/OFF NODE NAME
mongod     860     mongodb    5u  IPv4   5128      0t0  TCP localhost:27017 (LISTEN)
mongod     860     mongodb    7u  IPv4   5130      0t0  TCP localhost:28017 (LISTEN)
cupsd     1656        root    5u  IPv6   6156      0t0  TCP localhost:631 (LISTEN)
cupsd     1656        root    6u  IPv4   6157      0t0  TCP localhost:631 (LISTEN)
dhclient3 1718        root    5u  IPv4   3894      0t0  UDP *:68
squid     1780       proxy    6u  IPv4   6338      0t0  UDP *:47630
squid     1780       proxy   14u  IPv4   6347      0t0  TCP *:3128 (LISTEN)
squid     1780       proxy   15u  IPv4   6349      0t0  UDP *:3130
exim4     2162 Debian-exim    3u  IPv4   6694      0t0  TCP localhost:25 (LISTEN)
exim4     2162 Debian-exim    4u  IPv6   6695      0t0  TCP localhost:25 (LISTEN)
privoxy   2221     privoxy    1u  IPv4   6846      0t0  TCP localhost:8118 (LISTEN)
sshd      2241        root    3u  IPv4   6895      0t0  TCP *:22 (LISTEN)
sshd      2241        root    4u  IPv6   6897      0t0  TCP *:22 (LISTEN)
tor       2251  debian-tor    7u  IPv4   6923      0t0  TCP localhost:9050 (LISTEN)
postgres  2282    postgres    3u  IPv6   7089      0t0  TCP localhost:7175 (LISTEN)
postgres  2282    postgres    4u  IPv4   7090      0t0  TCP localhost:7175 (LISTEN)
postgres  2282    postgres    6u  IPv6   7098      0t0  UDP localhost:57450->localhost:57450
postgres  2291    postgres    6u  IPv6   7098      0t0  UDP localhost:57450->localhost:57450
postgres  2292    postgres    6u  IPv6   7098      0t0  UDP localhost:57450->localhost:57450
postgres  2293    postgres    6u  IPv6   7098      0t0  UDP localhost:57450->localhost:57450
postgres  2294    postgres    6u  IPv6   7098      0t0  UDP localhost:57450->localhost:57450
clock-app 2536        root   22r  IPv4  40296      0t0  TCP 192.168.198.135:51626->65.171.167.131:80
```

Where to Hide Files

- RAM drives (disappear)
- Drive slack space
- /dev
- Directories named ".. " (dot-dot-space)
- /tmp and /var/tmp

```
root@bt:~/dotdot# mkdir ".. "
root@bt:~/dotdot# ls -a
.   ..   ..
root@bt:~/dotdot# ls -ab
.   ..   ..\
root@bt:~/dotdot#
```

RAM Drives

- /dev/shm is already mounted by default
- You can make your own with

  mkdir -p /tmp/ram

  sudo mount -t ramfs -o size=512M ramfs /tmp/ram/
- To see Ram drives, use

  df -a

Linux Mount

- mount -t *type device dir*
- the kernel attaches the filesystem found on **device** (which is of type **type**) at the directory **dir**

Mount RAMDISK

```
root@bt:~# mkdir -p /tmp/ram
root@bt:~# mount -t ramfs -o size=512M ramfs /tmp/ram
root@bt:~# df -a
Filesystem           1K-blocks      Used Available Use% Mounted on
/dev/sda1             19737268  11982916   6751756  64% /
proc                         0         0         0   -  /proc
none                         0         0         0   -  /sys
none                         0         0         0   -  /sys/fs/fuse/connections
none                         0         0         0   -  /sys/kernel/debug
none                         0         0         0   -  /sys/kernel/security
none                    368004       268    367736   1% /dev
none                         0         0         0   -  /dev/pts
none                    383596        28    383568   1% /dev/shm
none                    383596       116    383480   1% /var/run
none                    383596         0    383596   0% /var/lock
none                    383596         0    383596   0% /lib/init/rw
vmware-vmblock               0         0         0   -  /var/run/vmblock-fuse
ramfs                        0         0         0   -  /tmp/ram
root@bt:~#
```

Strings command

- To get readable strings from a file

  strings malware.exe > malfile

- To view results

  nano malfile

Poison Ivy

http://www.poisonivy-rat.com/
Source code available

Very Common

- Poison Ivy is a RAT used very often in APT attacks
- Used in
  - Aurora, 2009
  - RSA attacks, 2011
  - Nitro, April-October 2011

New IE zero day exploit circulating, used to install Poison Ivy

by Paul Roberts on September 17, 2012 | Comments (17)

FILED UNDER: Featured, Internet Explorer, Vulnerability

The gang behind the recent Java zero day attacks apparently hasn't packed up for the season.

A researcher examining one of the servers used to launch attacks on vulnerable Java installations says he has found a new zero day exploit for Microsoft's Internet Explorer web browser.

www.poisonivy-rat.com

Poison Ivy

Remote Administration Tool

Home - Downloads - Screenshots - Development - Customer Portal - Links - Contact

Site/downloads up again

2008-11-20

I have received a tremendous amount of emails from people wanting me to continue the project even though it might take some time until the next release.
It's meant alot to me to see this kind of support for the project. That's why I've decided to bring back the site, but I will not promise anything...
I hope to get some time and motivation to finish the new version.

TDSS (TLD1-4)

TDSS

- A botnet with 5 million compromised hosts
- Sophisticated malware
  - Rootkit
  - Encrypted files and communications
  - Many C&C servers
  - Variants: TDL 1, 2, 3, 4
  - Derivatives: *Zero Access*, *Purple Haze…*

Malware as a Service

- TDSS botnet rented to criminals
  - DDoS attacks
  - Click fraud
  - To install Trojans

Common APT Indicators

APT Method of Attack

1. Spear-phishing email
2. User clicks link; opens an application and redirects to a hidden address
3. Hidden address is a Dropsite; detect browser vulnerabilities, and drops a Trojan downloader

APT Method of Attack

4. Downloader sends a base64-encoded instruction to a different dropsite, which installs a Trojan backdoor
5. Trojan backdoor installed in c:\windows\system32 and registers in NETSVCS
6. Trojan backdoor uses a filename slightly different from Windows filenames
7. Uses SSL communication with C&C server

APT Method of Attack

8. Attacker interacts via cutouts with Trojan with SSL-encrypted traffic
9. Attacker lists Computername and User Accounts; uses pass-the-hash, gets local and Active Directory account information
10. Service privilege escalation to network reconnaissance
11. Offline password hash cracking

APT Method of Attack

12. Lateral movement by using RDP (Terminal Services), SC.exe (to create services), or NET commands (to connect to shares)
13. Installs additional backdoor Trojans, and egress point
14. Stolen files are packaged in ZIP or RAR packages, renamed as GIFs

Detecting APTs

- Audit changes to the file system
- SMS alerts on administrative logins
- Firewalls that monitor inbound RDP/VNC/CMD.EXE
- AV, HIPS, file system integrity checking
- NIDS, NIPS; Snort
- Security Information/Events Management (SIEM)