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

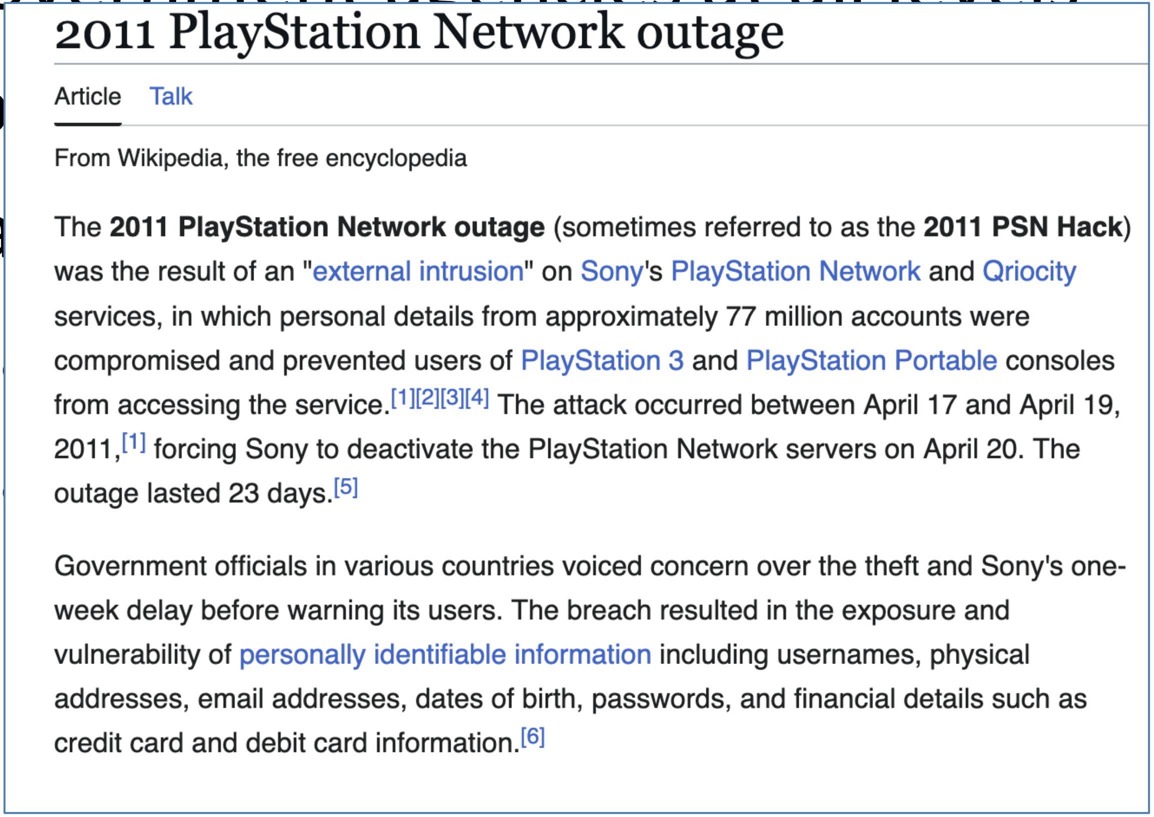
- From 2011, a loosely affiliated group or collection of groups, to expose sensitive info to public or interrupt services (DOS)
- A variety of hacking techniques
  - SQL injection, cross-site scripting, web service vulnerability exploits, social engineering (targeted spear-phishing, imitating employees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

Targets

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

Targets

- Government agencies at all levels
- So
- Ba
- M
- M



2011 PlayStation Network outage

Article Talk

From Wikipedia, the free encyclopedia

The **2011 PlayStation Network outage** (sometimes referred to as the **2011 PSN Hack**) was the result of an "external intrusion" on Sony's PlayStation Network and Qriocity services, in which personal details from approximately 77 million accounts were compromised and prevented users of PlayStation 3 and PlayStation Portable consoles from accessing the service.[1][2][3][4] The attack occurred between April 17 and April 19, 2011,[1] forcing Sony to deactivate the PlayStation Network servers on April 20. The outage lasted 23 days.[5]

Government officials in various countries voiced concern over the theft and Sony's one-week delay before warning its users. The breach resulted in the exposure and vulnerability of personally identifiable information including usernames, physical addresses, email addresses, dates of birth, passwords, and financial details such as credit card and debit card information.[6]

https://en.wikipedia.org/wiki/2011_PlayStation_Network_outage

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

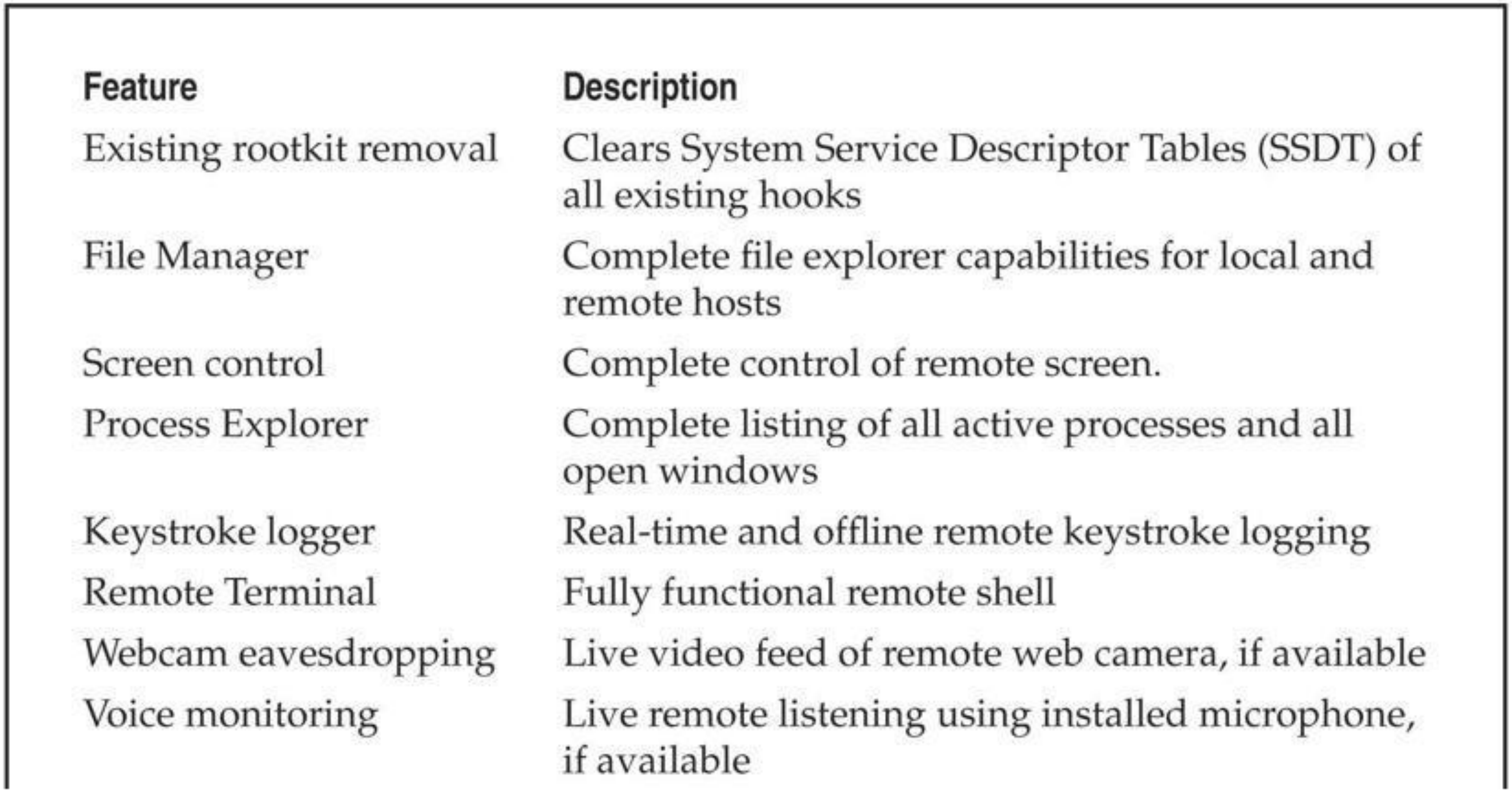
- Gh0st attack
- Malicious email

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)

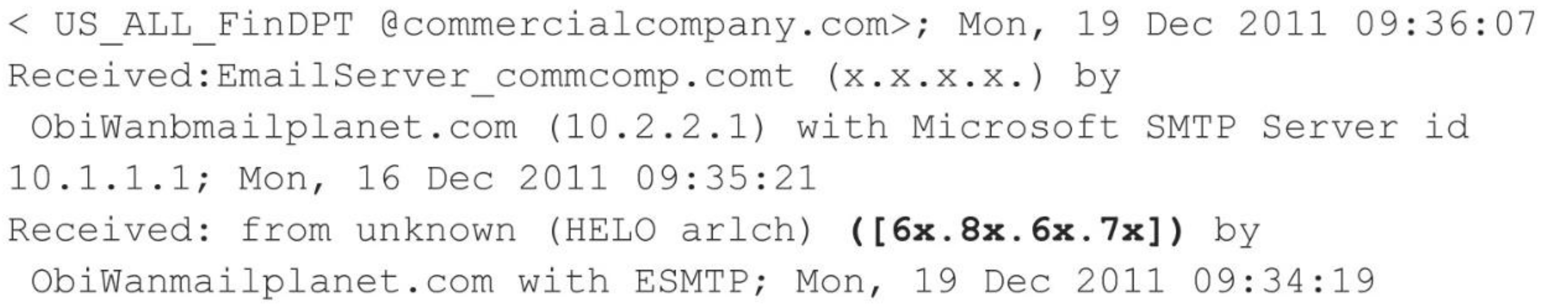
Dial-up profile cracking	Listing of dial-up profiles, including cracked passwords.
Remote screen blanking	Blanks compromised host screen, making computer unusable
Remote input blocking	Disables compromised host mouse and keyboard
Session management	Remote shutdown and reboot of host
Remote file downloads	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

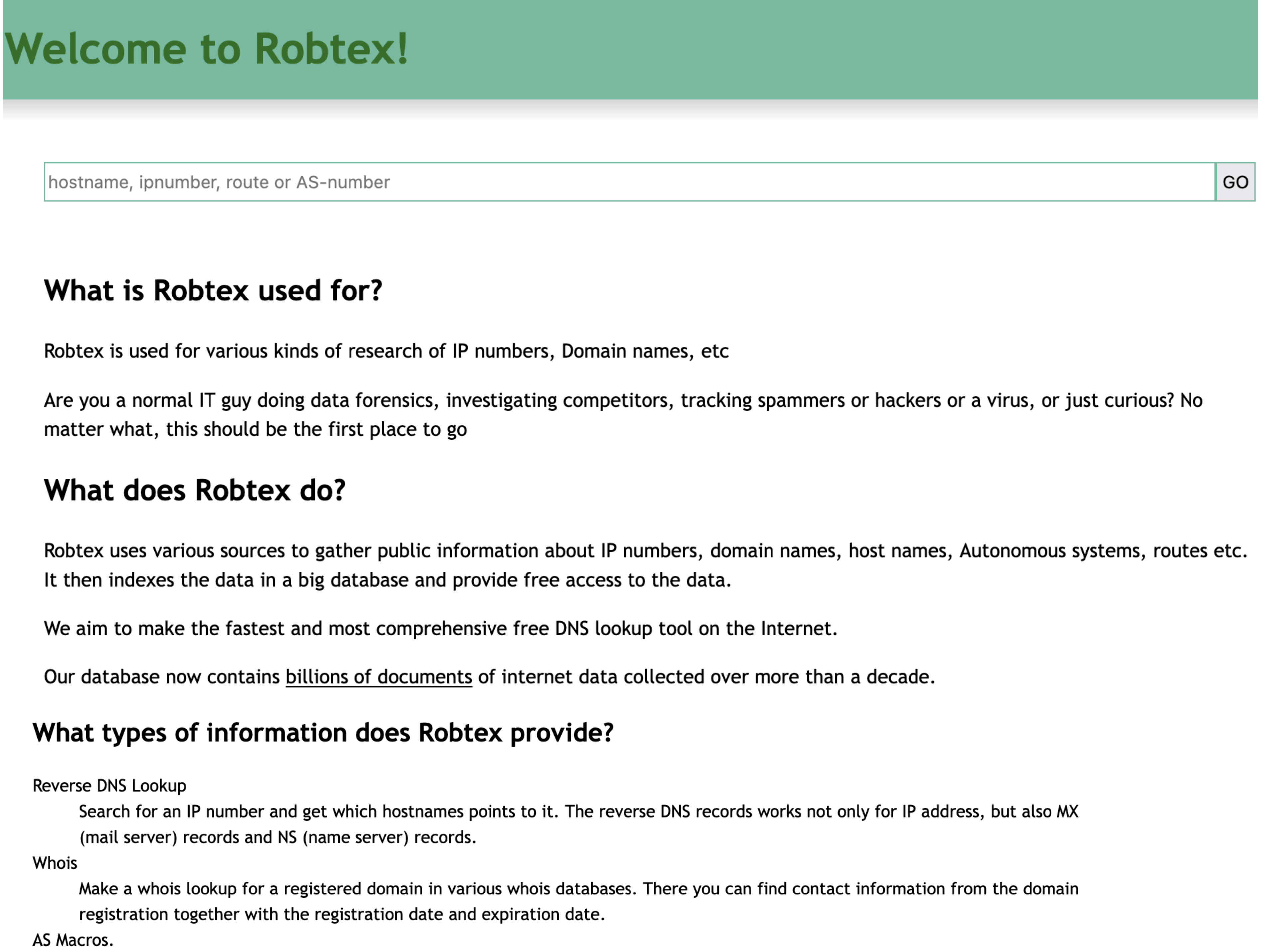
- Phishing email
- Backdoor placed when malicious link clicked
- Backdoor hides itself to survive a reboot
- Connection to C&C
- Check internal domain, create accounts, use Terminal Server to hop to other hosts (Event Logs)
- Add/modify some files (diff \System32)
- Look for documents and zip for exfiltration
- 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



```
< US_ALL_FinDPT @commercialcompany.com>; Mon, 19 Dec 2011 09:36:07
Received:EmailServer_commcomp.comt (x.x.x.x.) by
 ObiWanbmailplanet.com (10.2.2.1) with Microsoft SMTP Server id
10.1.1.1; Mon, 16 Dec 2011 09:35:21
Received: from unknown (HELO arlch) ([6x.8x.6x.7x]) by
 ObiWanmailplanet.com with ESMTP; Mon, 19 Dec 2011 09:34:19
```



Welcome to 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 matter what, 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 etc. It then 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.

What types of information does Robtex provide?

Reverse DNS Lookup

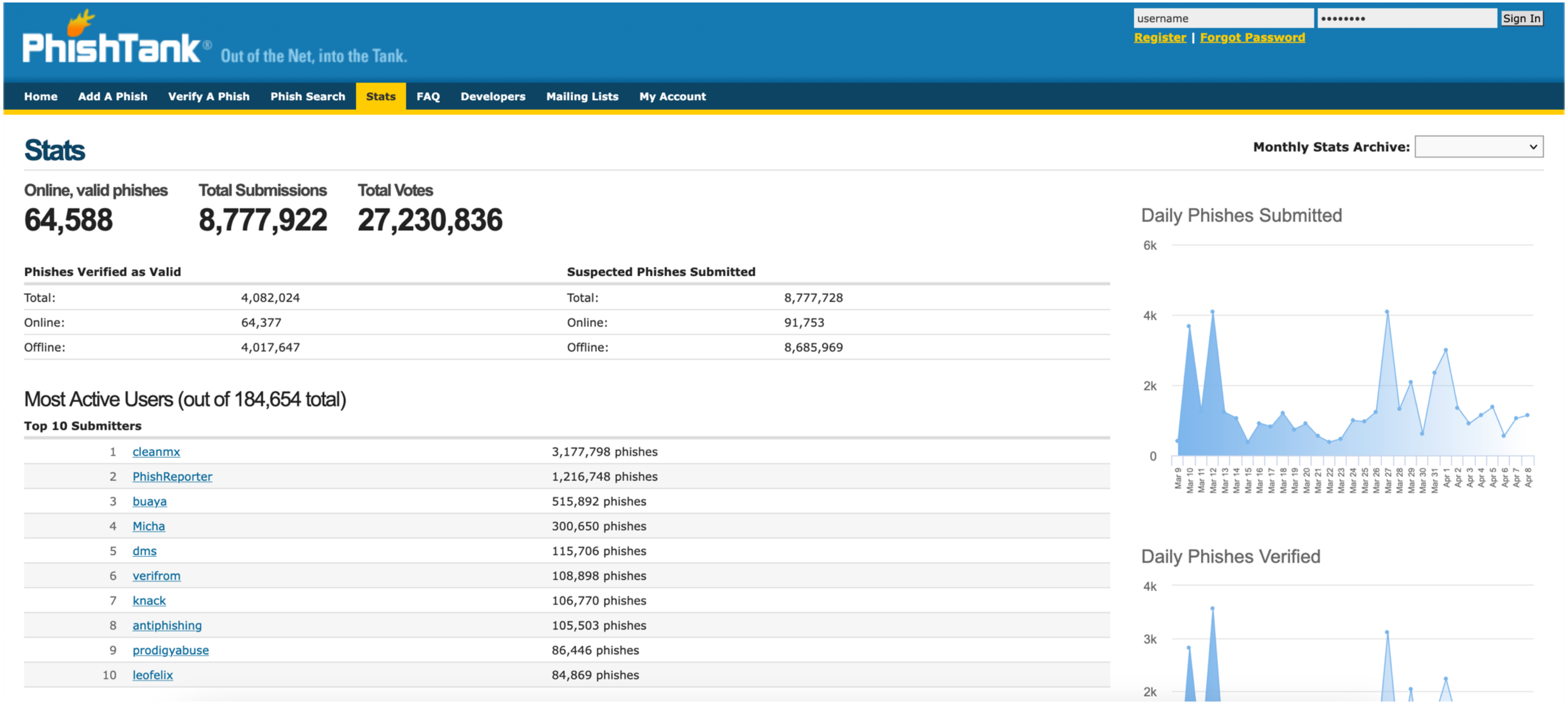
Search for an IP number and get which hostnames points to it. The reverse DNS records works not only for IP address, but also MX (mail server) records and NS (name server) records.

Whois

Make a whois lookup for a registered domain in various whois databases. There you can find contact information from the domain registration together with the registration date and expiration date.

AS Macros.

PhishTank



Stats

Online, valid phishes	Total Submissions	Total Votes
64,588	8,777,922	27,230,836

Phishes Verified as Valid		Suspected Phishes Submitted	
Total:	4,082,024	Total:	8,777,728
Online:	64,377	Online:	91,753
Offline:	4,017,647	Offline:	8,685,969

Most Active Users (out of 184,654 total)

Top 10 Submitters

1	cleanmx	3,177,798 phishes
2	PhishReporter	1,216,748 phishes
3	buaya	515,892 phishes
4	Micha	300,650 phishes
5	dms	115,706 phishes
6	verifrom	108,898 phishes
7	knack	106,770 phishes
8	antiphishing	105,503 phishes
9	prodigyabuse	86,446 phishes
10	leofelix	84,869 phishes

Daily Phishes Submitted

Daily Phishes Verified

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

Resource Center

Free Tool

Magnet DumpIt for Windows

GET FREE TOOL ↓

Share

DumpIt is a fast memory acquisition tool for Windows (x86, x64, ARM64). Generate full memory crash dumps of Windows machines.

Magnet DumpIt for Windows: What does it do?

Memory analysis (sometimes referred to as memory forensics) is a key part of the Digital Forensics and Incident Response (DFIR) process for analyzing malware and exploits, but also for troubleshooting issues.

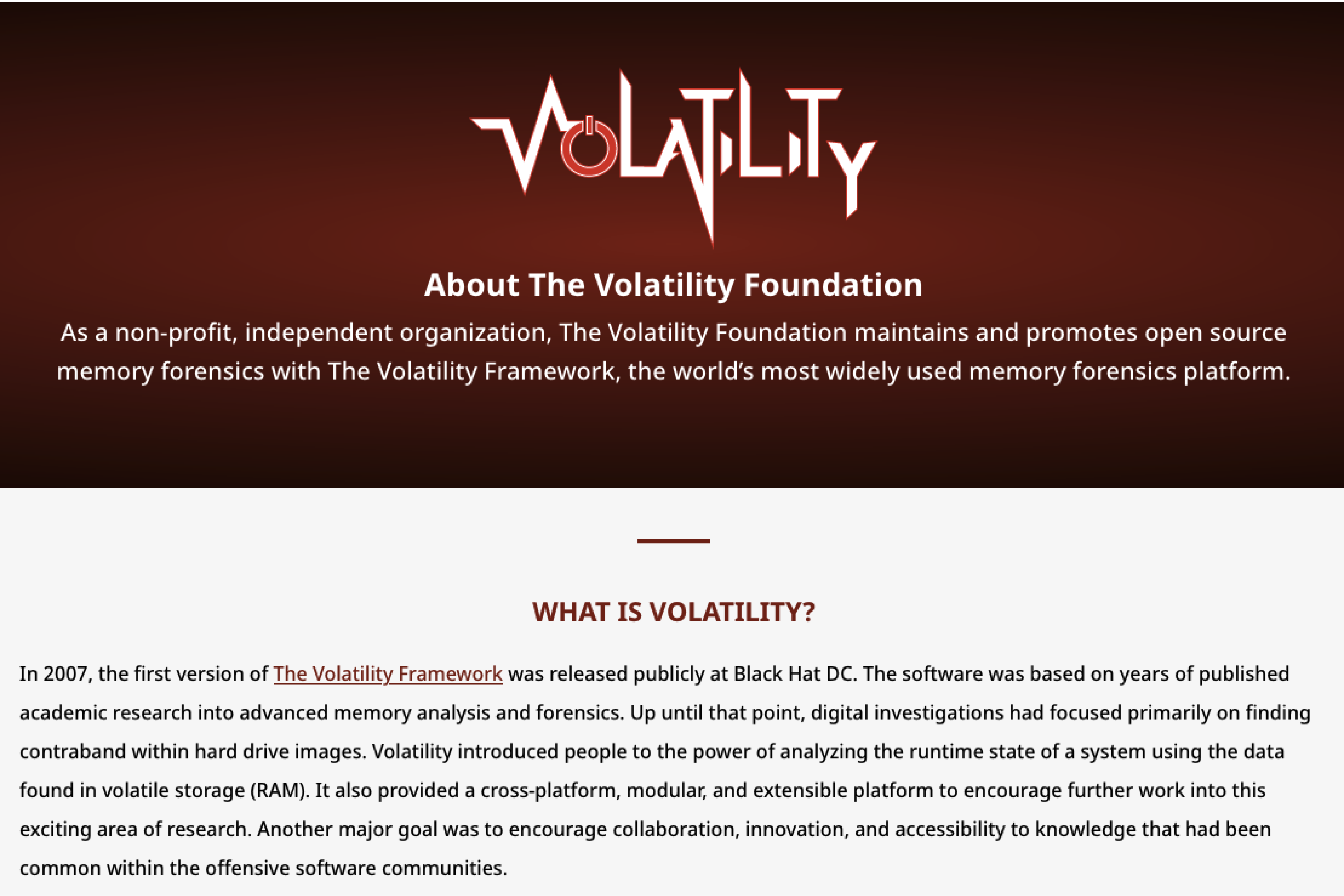
MAGNET DumpIt for Windows (created by Comae Technologies and acquired by Magnet Forensics in 2022) generates full memory crash dumps that are interoperable with multiple analysis tools and products such as WinDbg, Comae Platform.

Key Features & Benefits

- **Easy to Deploy:** No pre-installed agent is required. Machine states can be collected via DumpIt and its PowerShell interface to provide your organization with more flexibility.
- **Super Fast:** Every minute counts when investigating a security incident. Since its initial release 10 years ago, DumpIt has been known for its super fast speed of memory acquisition.
- **No BSOD**: Generate full memory Microsoft crash dumps on the fly without having to trigger a "Blue Screen of Death (BSOD)"

Memory Analysis

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



About The Volatility Foundation

As a non-profit, independent organization, The Volatility Foundation maintains and promotes open source memory forensics with The Volatility Framework, the world’s most widely used memory forensics platform.

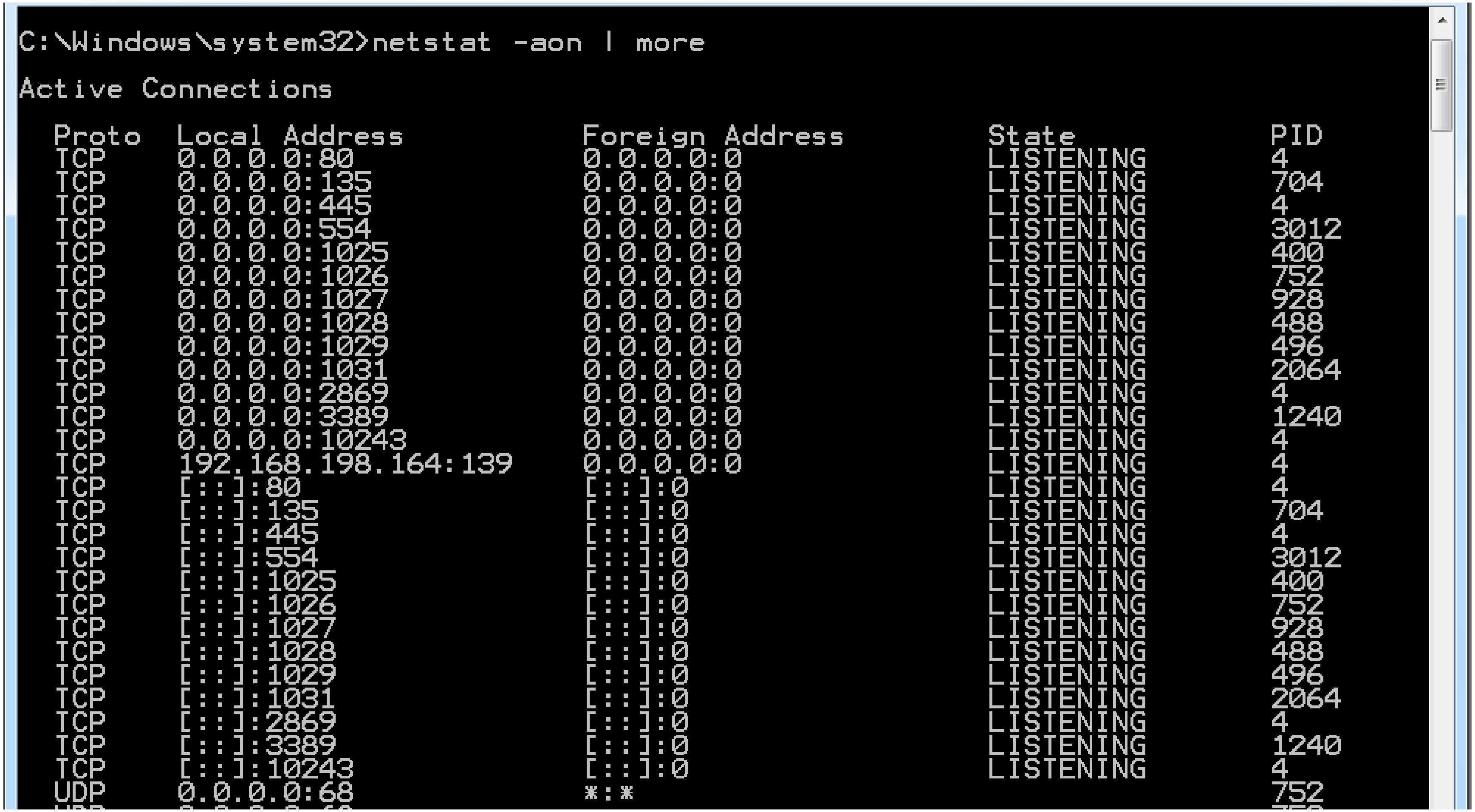
WHAT IS VOLATILITY?

In 2007, the first version of The Volatility Framework was released publicly at Black Hat DC. The software was based on years of published academic research into advanced memory analysis and forensics. Up until that point, digital investigations had focused primarily on finding contraband within hard drive images. Volatility introduced people to the power of analyzing the runtime state of a system using the data found in volatile storage (RAM). It also provided a cross-platform, modular, and extensible platform to encourage further work into this exciting area of research. Another major goal was to encourage collaboration, innovation, and accessibility to knowledge that had been common within the offensive software communities.

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

Netstat -aon

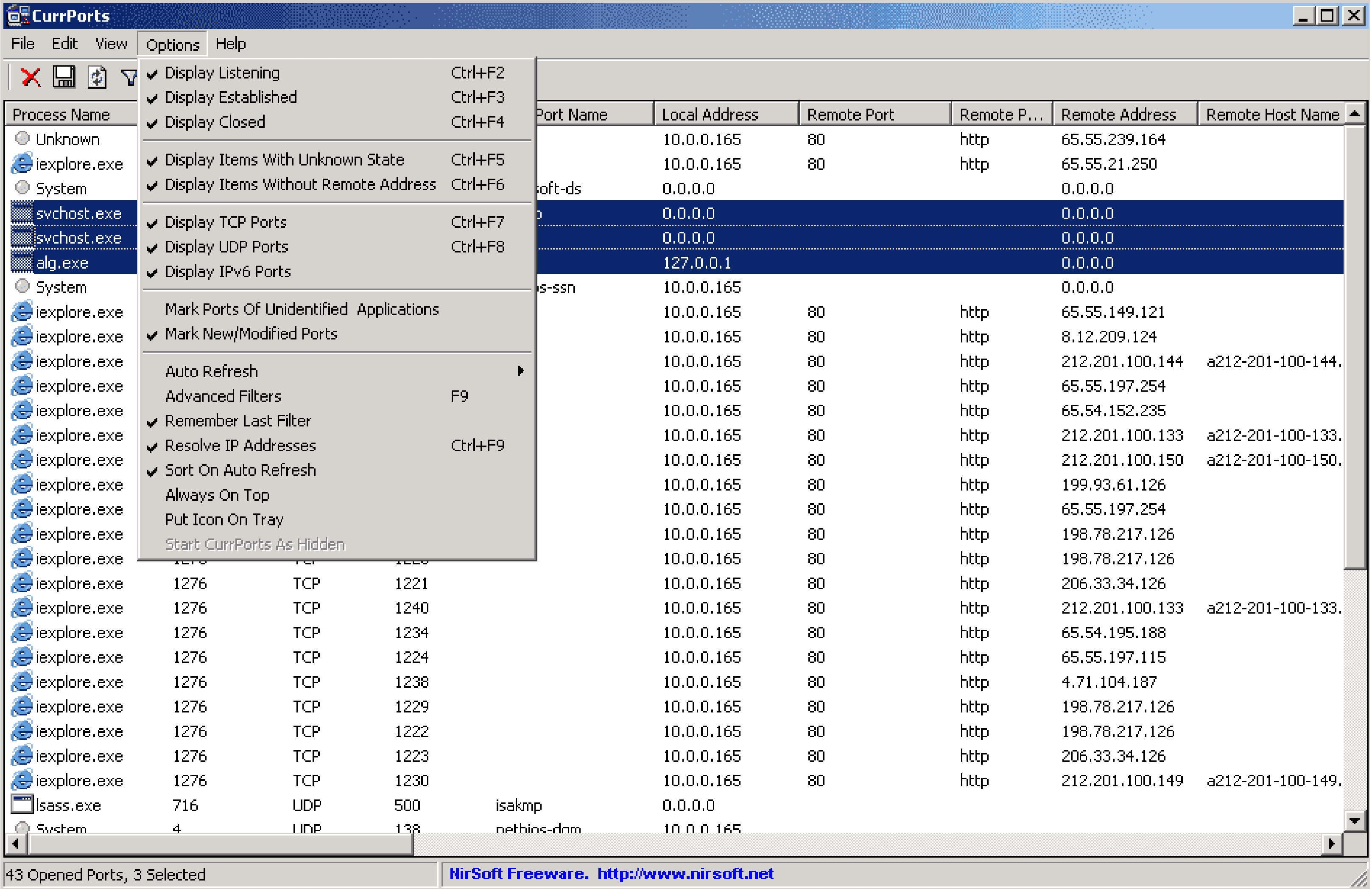


```
C:\Windows\system32>netstat -aon | more

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
```

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

CurrPorts

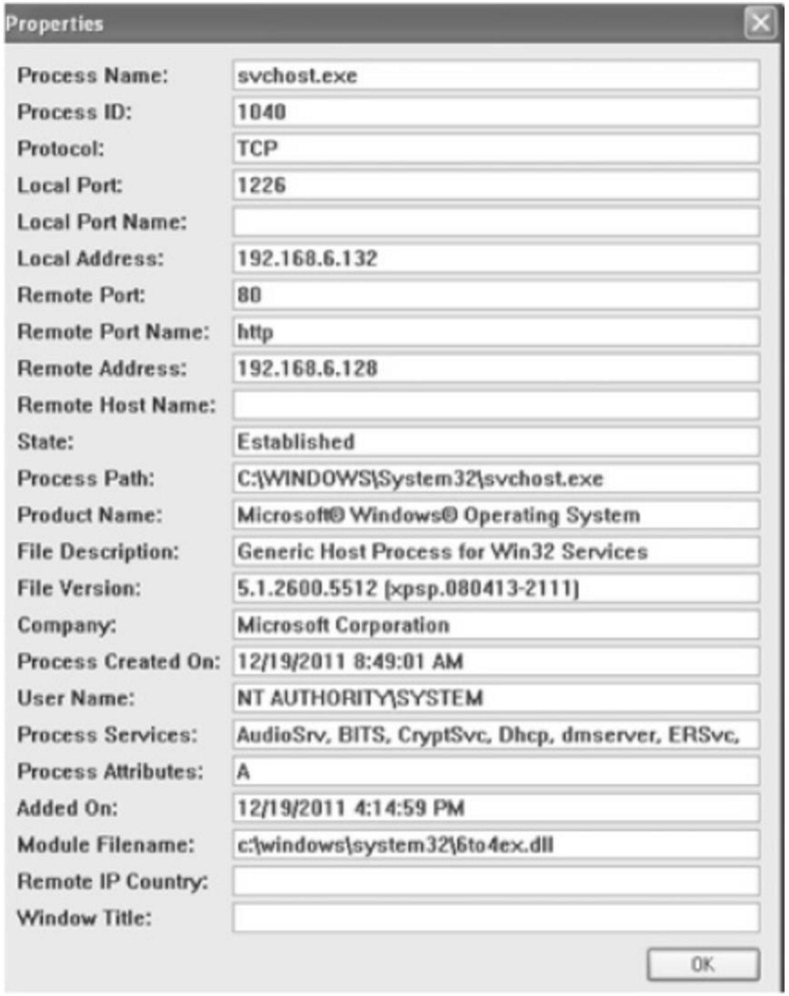

CurrPorts
File
Edit
View
Options
Help
✓ Display Listening Ctrl+F2
✓ Display Established Ctrl+F3
✓ Display Closed Ctrl+F4
✓ Display Items With Unknown State Ctrl+F5
✓ Display Items Without Remote Address Ctrl+F6
✓ Display TCP Ports Ctrl+F7
✓ Display UDP Ports Ctrl+F8
✓ Display IPv6 Ports
Mark Ports Of Unidentified Applications
✓ Mark New/Modified Ports
Auto Refresh
Advanced Filters F9
✓ Remember Last Filter
✓ Resolve IP Addresses Ctrl+F9
✓ Sort On Auto Refresh
Always On Top
Put Icon On Tray
Start CurrPorts As Hidden

Process Name				Port Name	Local Address	Remote Port	Remote P...	Remote Address	Remote Host Name
Unknown					10.0.0.165	80	http	65.55.239.164	
iexplore.exe					10.0.0.165	80	http	65.55.21.250	
System				oft-ds	0.0.0.0			0.0.0.0	
svchost.exe					0.0.0.0			0.0.0.0	
svchost.exe					0.0.0.0			0.0.0.0	
alg.exe					127.0.0.1			0.0.0.0	
System				s-ssn	10.0.0.165			0.0.0.0	
iexplore.exe					10.0.0.165	80	http	65.55.149.121	
iexplore.exe					10.0.0.165	80	http	8.12.209.124	
iexplore.exe					10.0.0.165	80	http	212.201.100.144	a212-201-100-144.
iexplore.exe					10.0.0.165	80	http	65.55.197.254	
iexplore.exe					10.0.0.165	80	http	65.54.152.235	
iexplore.exe					10.0.0.165	80	http	212.201.100.133	a212-201-100-133.
iexplore.exe					10.0.0.165	80	http	212.201.100.150	a212-201-100-150.
iexplore.exe					10.0.0.165	80	http	199.93.61.126	
iexplore.exe					10.0.0.165	80	http	65.55.197.254	
iexplore.exe					10.0.0.165	80	http	198.78.217.126	
iexplore.exe					10.0.0.165	80	http	198.78.217.126	
iexplore.exe	1276	TCP	1221		10.0.0.165	80	http	206.33.34.126	
iexplore.exe	1276	TCP	1240		10.0.0.165	80	http	212.201.100.133	a212-201-100-133.
iexplore.exe	1276	TCP	1234		10.0.0.165	80	http	65.54.195.188	
iexplore.exe	1276	TCP	1224		10.0.0.165	80	http	65.55.197.115	
iexplore.exe	1276	TCP	1238		10.0.0.165	80	http	4.71.104.187	
iexplore.exe	1276	TCP	1229		10.0.0.165	80	http	198.78.217.126	
iexplore.exe	1276	TCP	1222		10.0.0.165	80	http	198.78.217.126	
iexplore.exe	1276	TCP	1223		10.0.0.165	80	http	206.33.34.126	
iexplore.exe	1276	TCP	1230		10.0.0.165	80	http	212.201.100.149	a212-201-100-149.
lsass.exe	716	UDP	500	isakmp	0.0.0.0				
System	4	UDP	138	netbios-dgm	10.0.0.165				

43 Opened Ports, 3 Selected

NirSoft Freeware. http://www.nirsoft.net

CurrPorts

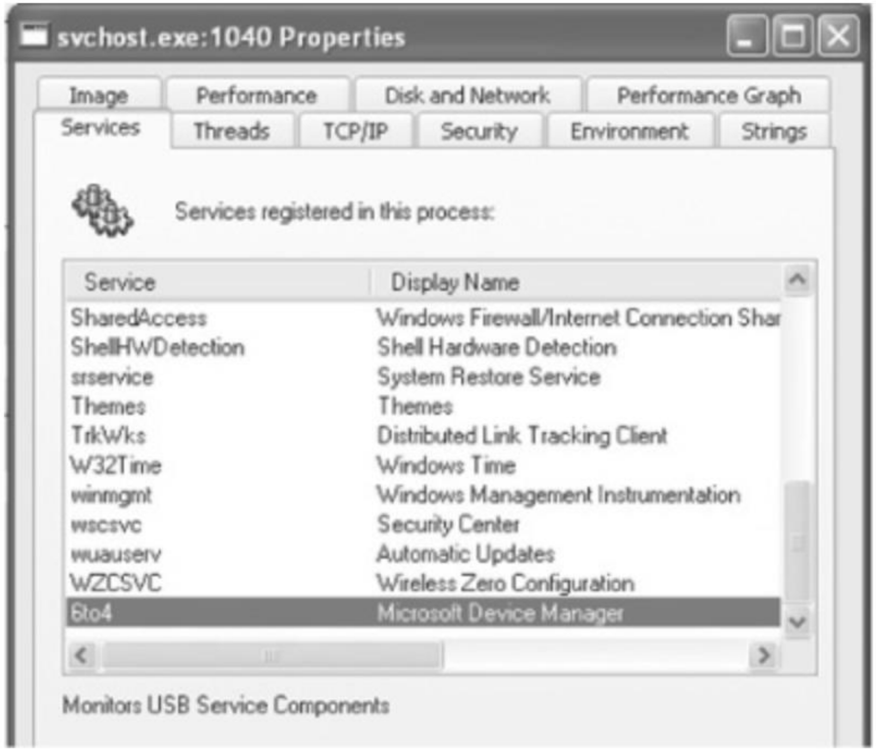


Process Name:	svchost.exe
Process ID:	1040
Protocol:	TCP
Local Port:	1226
Local Port Name:	
Local Address:	192.168.6.132
Remote Port:	80
Remote Port Name:	http
Remote Address:	192.168.6.128
Remote Host Name:	
State:	Established
Process Path:	C:\WINDOWS\System32\svchost.exe
Product Name:	Microsoft® Windows® Operating System
File Description:	Generic Host Process for Win32 Services
File Version:	5.1.2600.5512 (xpsp.080413-2111)
Company:	Microsoft Corporation
Process Created On:	12/19/2011 8:49:01 AM
User Name:	NT AUTHORITY\SYSTEM
Process Services:	AudioSrv, BITS, CryptSvc, Dhcp, dmserver, ERSvc,
Process Attributes:	A
Added On:	12/19/2011 4:14:59 PM
Module Filename:	c:\windows\system32\6to4ex.dll
Remote IP Country:	
Window Title:	

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

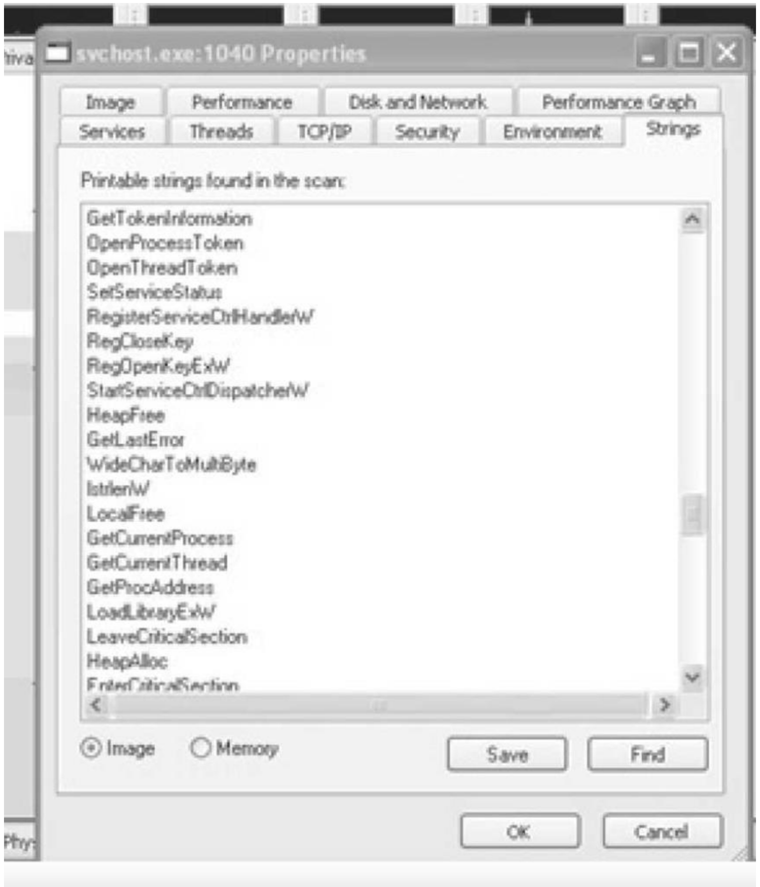
Process Explorer



Services registered in this process:

Service	Display Name
SharedAccess	Windows Firewall/Internet Connection Shar
ShellHWDetection	Shell Hardware Detection
srservice	System Restore Service
Themes	Themes
TrkWks	Distributed Link Tracking Client
W32Time	Windows Time
winmgmt	Windows Management Instrumentation
wscsvc	Security Center
wuauserv	Automatic Updates
WZCSVC	Wireless Zero Configuration
6to4	Microsoft Device Manager

Monitors USB Service Components

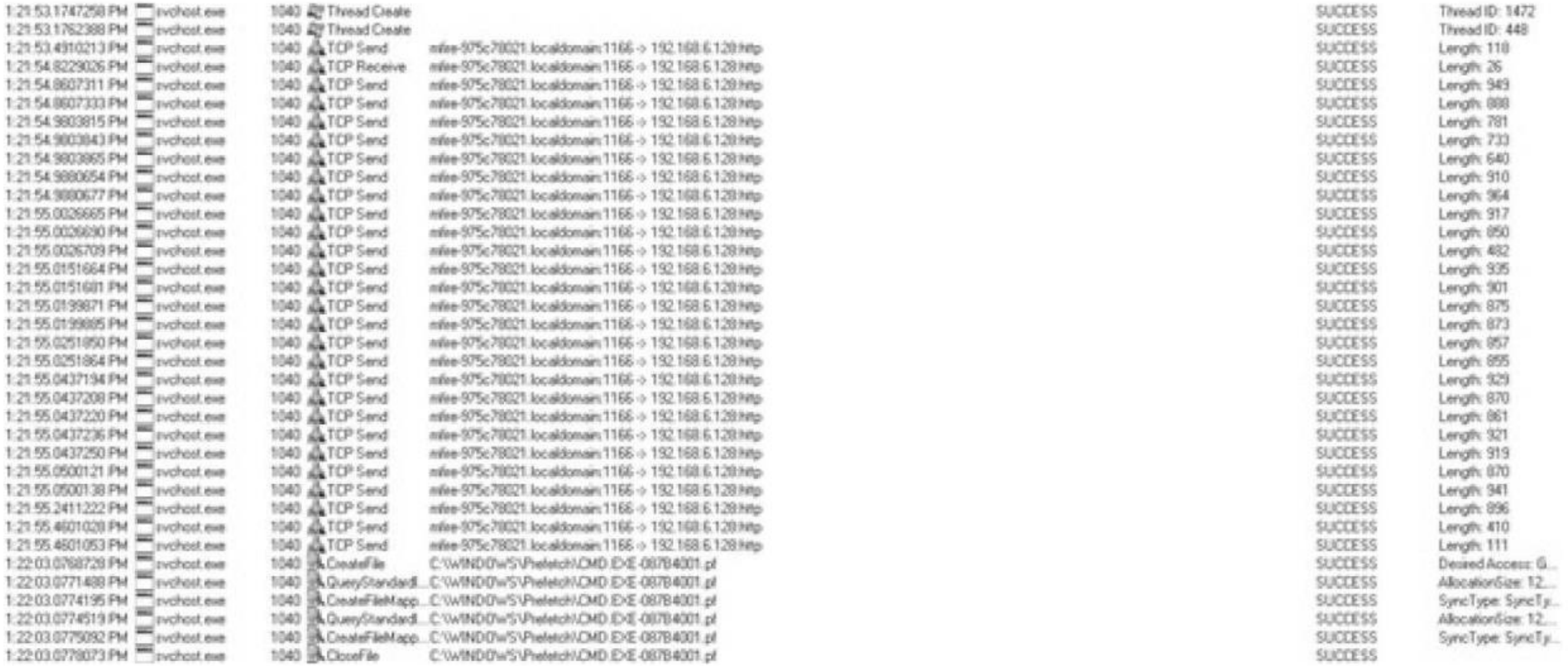


Printable strings found in the scan:

```
GetTokenInformation
OpenProcessToken
OpenThreadToken
SetServiceStatus
RegisterServiceCtrlHandlerW
RegCloseKey
RegOpenKeyExW
StartServiceCtrlDispatcherW
HeapFree
GetLastError
WideCharToMultiByte
lstrlenW
LocalFree
GetCurrentProcess
GetCurrentThread
GetProcAddress
LoadLibraryExW
LeaveCriticalSection
HeapAlloc
EnterCriticalSection
```

File/Process Capture (1/2)

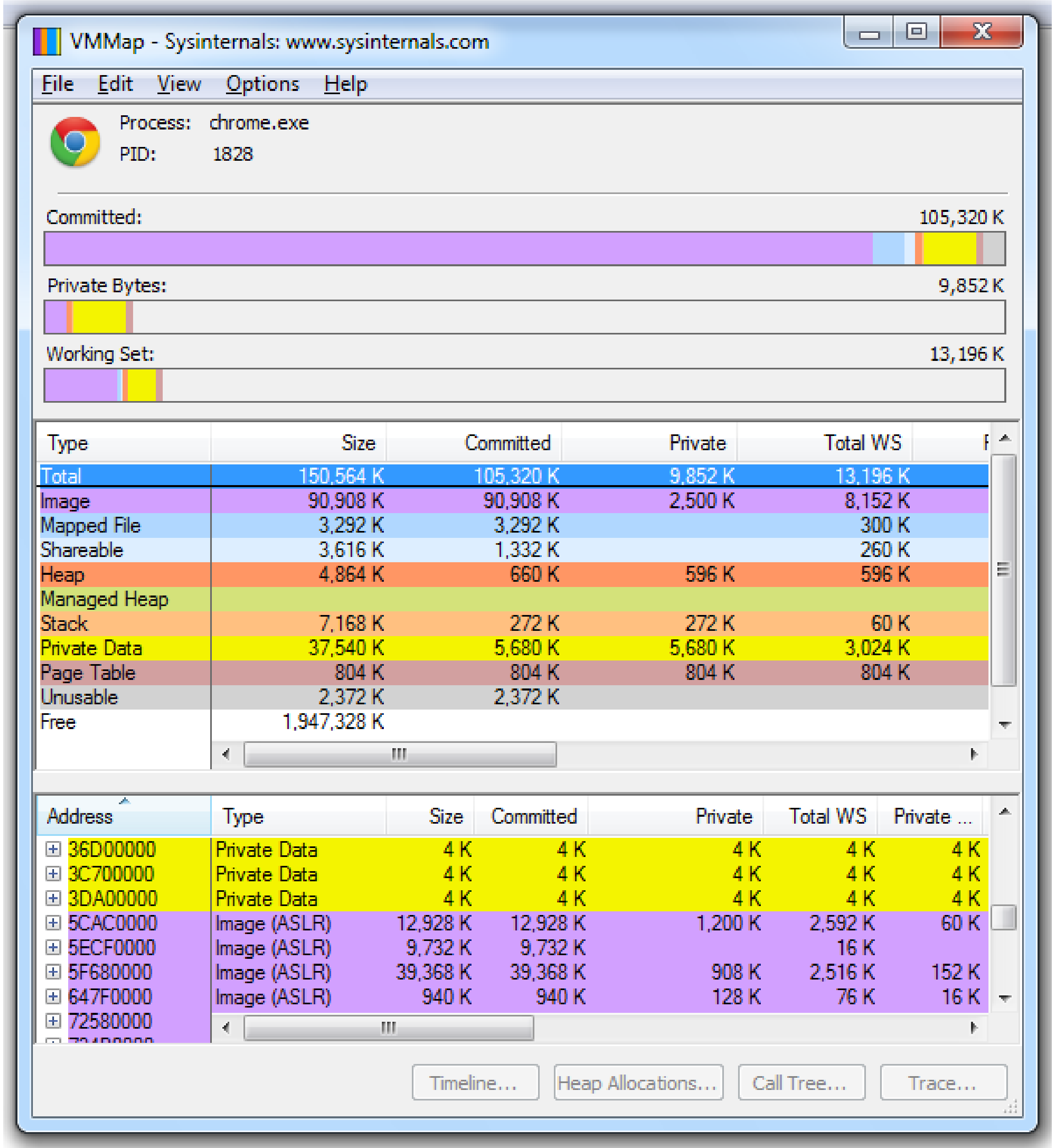
- Master File Table (MFT): metadata (filename, timestamp, file size, etc.), timeline is important
- Network/process/registry: netstat to find connections and process PID
- Host file: check any changes
- Currports: look into a current open port and its DLL
- Process Explorer: lookup a process, its DLL 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



```
1:21:53.1747258 PM  svchost.exe  1040  Thread Create                                                             SUCCESS  Thread ID: 1472
1:21:53.1762388 PM  svchost.exe  1040  Thread Create                                                             SUCCESS  Thread ID: 448
1:21:53.4910213 PM  svchost.exe  1040  TCP Send        mfee-975c78021.localdomain:1166 -> 192.168.6.128:http     SUCCESS  Length: 118
1:21:54.8229026 PM  svchost.exe  1040  TCP Receive     mfee-975c78021.localdomain:1166 -> 192.168.6.128:http     SUCCESS  Length: 26
1:21:54.8607311 PM  svchost.exe  1040  TCP Send        mfee-975c78021.localdomain:1166 -> 192.168.6.128:http     SUCCESS  Length: 949
1:21:54.8607333 PM  svchost.exe  1040  TCP Send        mfee-975c78021.localdomain:1166 -> 192.168.6.128:http     SUCCESS  Length: 888
1:21:54.9803815 PM  svchost.exe  1040  TCP Send        mfee-975c78021.localdomain:1166 -> 192.168.6.128:http     SUCCESS  Length: 781
1:21:54.9803843 PM  svchost.exe  1040  TCP Send        mfee-975c78021.localdomain:1166 -> 192.168.6.128:http     SUCCESS  Length: 733
1:21:54.9803865 PM  svchost.exe  1040  TCP Send        mfee-975c78021.localdomain:1166 -> 192.168.6.128:http     SUCCESS  Length: 640
1:21:54.9880654 PM  svchost.exe  1040  TCP Send        mfee-975c78021.localdomain:1166 -> 192.168.6.128:http     SUCCESS  Length: 910
1:21:54.9880677 PM  svchost.exe  1040  TCP Send        mfee-975c78021.localdomain:1166 -> 192.168.6.128:http     SUCCESS  Length: 964
1:21:55.0026665 PM  svchost.exe  1040  TCP Send        mfee-975c78021.localdomain:1166 -> 192.168.6.128:http     SUCCESS  Length: 917
1:21:55.0026690 PM  svchost.exe  1040  TCP Send        mfee-975c78021.localdomain:1166 -> 192.168.6.128:http     SUCCESS  Length: 850
1:21:55.0026709 PM  svchost.exe  1040  TCP Send        mfee-975c78021.localdomain:1166 -> 192.168.6.128:http     SUCCESS  Length: 482
1:21:55.0151664 PM  svchost.exe  1040  TCP Send        mfee-975c78021.localdomain:1166 -> 192.168.6.128:http     SUCCESS  Length: 935
1:21:55.0151681 PM  svchost.exe  1040  TCP Send        mfee-975c78021.localdomain:1166 -> 192.168.6.128:http     SUCCESS  Length: 901
1:21:55.0199871 PM  svchost.exe  1040  TCP Send        mfee-975c78021.localdomain:1166 -> 192.168.6.128:http     SUCCESS  Length: 875
1:21:55.0199885 PM  svchost.exe  1040  TCP Send        mfee-975c78021.localdomain:1166 -> 192.168.6.128:http     SUCCESS  Length: 873
1:21:55.0251850 PM  svchost.exe  1040  TCP Send        mfee-975c78021.localdomain:1166 -> 192.168.6.128:http     SUCCESS  Length: 857
1:21:55.0251864 PM  svchost.exe  1040  TCP Send        mfee-975c78021.localdomain:1166 -> 192.168.6.128:http     SUCCESS  Length: 855
1:21:55.0437194 PM  svchost.exe  1040  TCP Send        mfee-975c78021.localdomain:1166 -> 192.168.6.128:http     SUCCESS  Length: 929
1:21:55.0437208 PM  svchost.exe  1040  TCP Send        mfee-975c78021.localdomain:1166 -> 192.168.6.128:http     SUCCESS  Length: 870
1:21:55.0437220 PM  svchost.exe  1040  TCP Send        mfee-975c78021.localdomain:1166 -> 192.168.6.128:http     SUCCESS  Length: 861
1:21:55.0437236 PM  svchost.exe  1040  TCP Send        mfee-975c78021.localdomain:1166 -> 192.168.6.128:http     SUCCESS  Length: 921
1:21:55.0437250 PM  svchost.exe  1040  TCP Send        mfee-975c78021.localdomain:1166 -> 192.168.6.128:http     SUCCESS  Length: 919
1:21:55.0500121 PM  svchost.exe  1040  TCP Send        mfee-975c78021.localdomain:1166 -> 192.168.6.128:http     SUCCESS  Length: 870
1:21:55.0500138 PM  svchost.exe  1040  TCP Send        mfee-975c78021.localdomain:1166 -> 192.168.6.128:http     SUCCESS  Length: 941
1:21:55.2411222 PM  svchost.exe  1040  TCP Send        mfee-975c78021.localdomain:1166 -> 192.168.6.128:http     SUCCESS  Length: 896
1:21:55.4601028 PM  svchost.exe  1040  TCP Send        mfee-975c78021.localdomain:1166 -> 192.168.6.128:http     SUCCESS  Length: 410
1:21:55.4601053 PM  svchost.exe  1040  TCP Send        mfee-975c78021.localdomain:1166 -> 192.168.6.128:http     SUCCESS  Length: 111
1:22:03.0768728 PM  svchost.exe  1040  CreateFile      C:\WINDOWS\Prefetch\CMD.EXE-087B4001.pf                   SUCCESS  Desired Access: G...
1:22:03.0771488 PM  svchost.exe  1040  QueryStandardI...C:\WINDOWS\Prefetch\CMD.EXE-087B4001.pf                  SUCCESS  AllocationSize: 12...
1:22:03.0774195 PM  svchost.exe  1040  CreateFileMapp...C:\WINDOWS\Prefetch\CMD.EXE-087B4001.pf                  SUCCESS  SyncType: SyncTy...
1:22:03.0774519 PM  svchost.exe  1040  QueryStandardI...C:\WINDOWS\Prefetch\CMD.EXE-087B4001.pf                  SUCCESS  AllocationSize: 12...
1:22:03.0775092 PM  svchost.exe  1040  CreateFileMapp...C:\WINDOWS\Prefetch\CMD.EXE-087B4001.pf                  SUCCESS  SyncType: SyncTy...
1:22:03.0778073 PM  svchost.exe  1040  CloseFile       C:\WINDOWS\Prefetch\CMD.EXE-087B4001.pf                   SUCCESS
```

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



Process: chrome.exe
PID: 1828

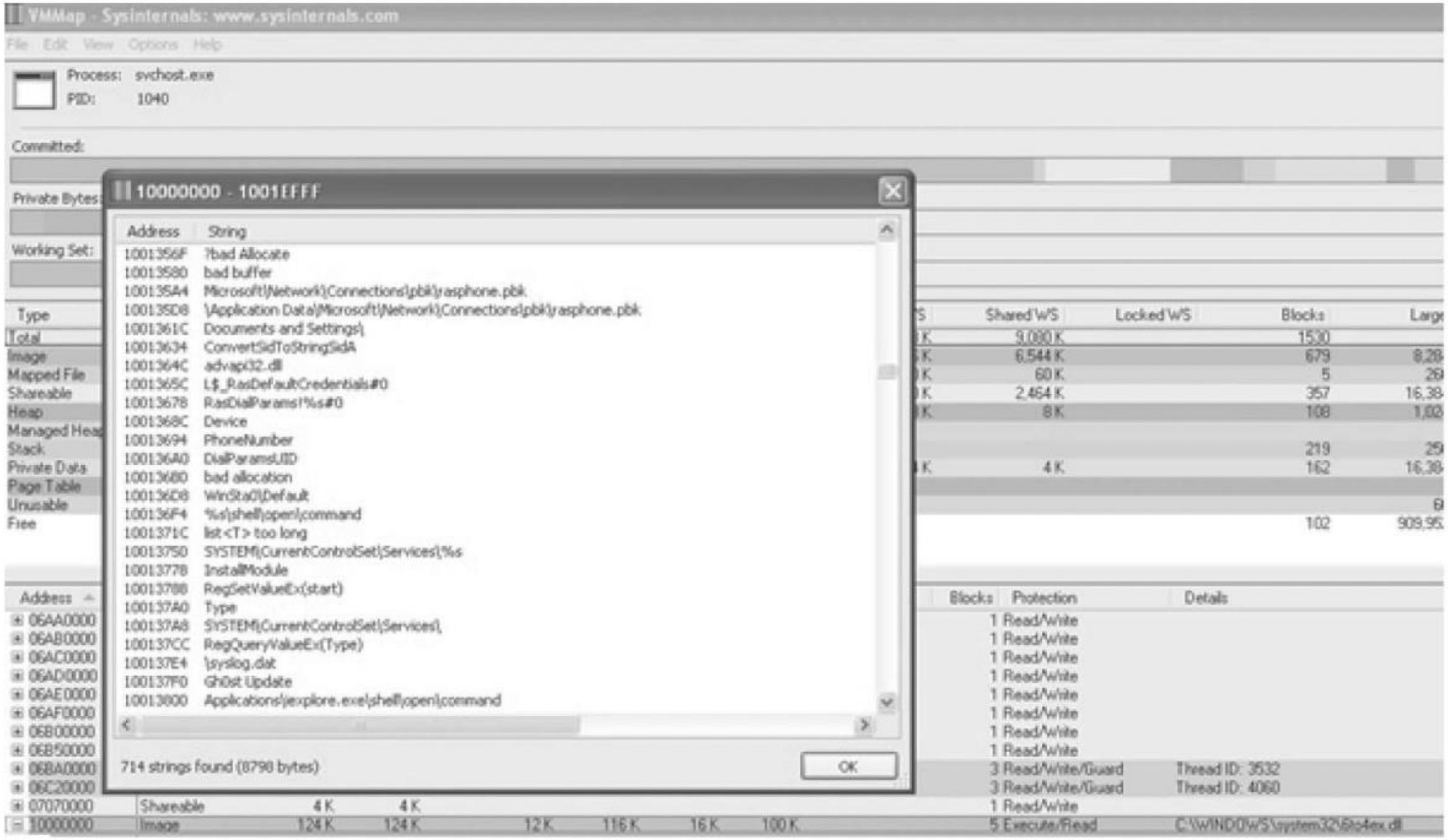
Committed: 105,320 K

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						



VMMap - Sysinternals: www.sysinternals.com
File Edit View Options Help

Process: svchost.exe
PID: 1040

Committed:
Private Bytes:
Working Set:

Type	Shared WS	Locked WS	Blocks	Larg
Total	9,000 K		1530	
Image	6,544 K		679	8,28
Mapped File	60 K		5	26
Shareable	2,464 K		357	16,38
Heap	8 K		108	1,02
Managed Hea				
Stack			219	25
Private Data	4 K		162	16,38
Page Table				
Unusable				6
Free			102	909,95

10000000 - 1001EFFF

```
Address   String
1001356F  ?bad Allocate
10013580  bad buffer
100135A4  Microsoft\Network\Connections\pbk\rasphone.pbk
100135D8  \Application Data\Microsoft\Network\Connections\pbk\rasphone.pbk
1001361C  Documents and Settings\
10013634  ConvertSidToStringSidA
1001364C  advapi32.dll
1001365C  L$_RasDefaultCredentials#0
10013678  RasDialParams!%s#0
1001368C  Device
10013694  PhoneNumber
100136A0  DialParamsUID
100136B0  bad allocation
100136D8  WinSta0\Default
100136F4  %s\shell\open\command
1001371C  list<T> too long
10013750  SYSTEM\CurrentControlSet\Services\%s
10013778  InstallModule
10013788  RegSetValueEx(start)
100137A0  Type
100137A8  SYSTEM\CurrentControlSet\Services\
100137CC  RegQueryValueEx(Type)
100137E4  \syslog.dat
100137F0  Gh0st Update
10013800  Applications\iexplore.exe\shell\open\command
```

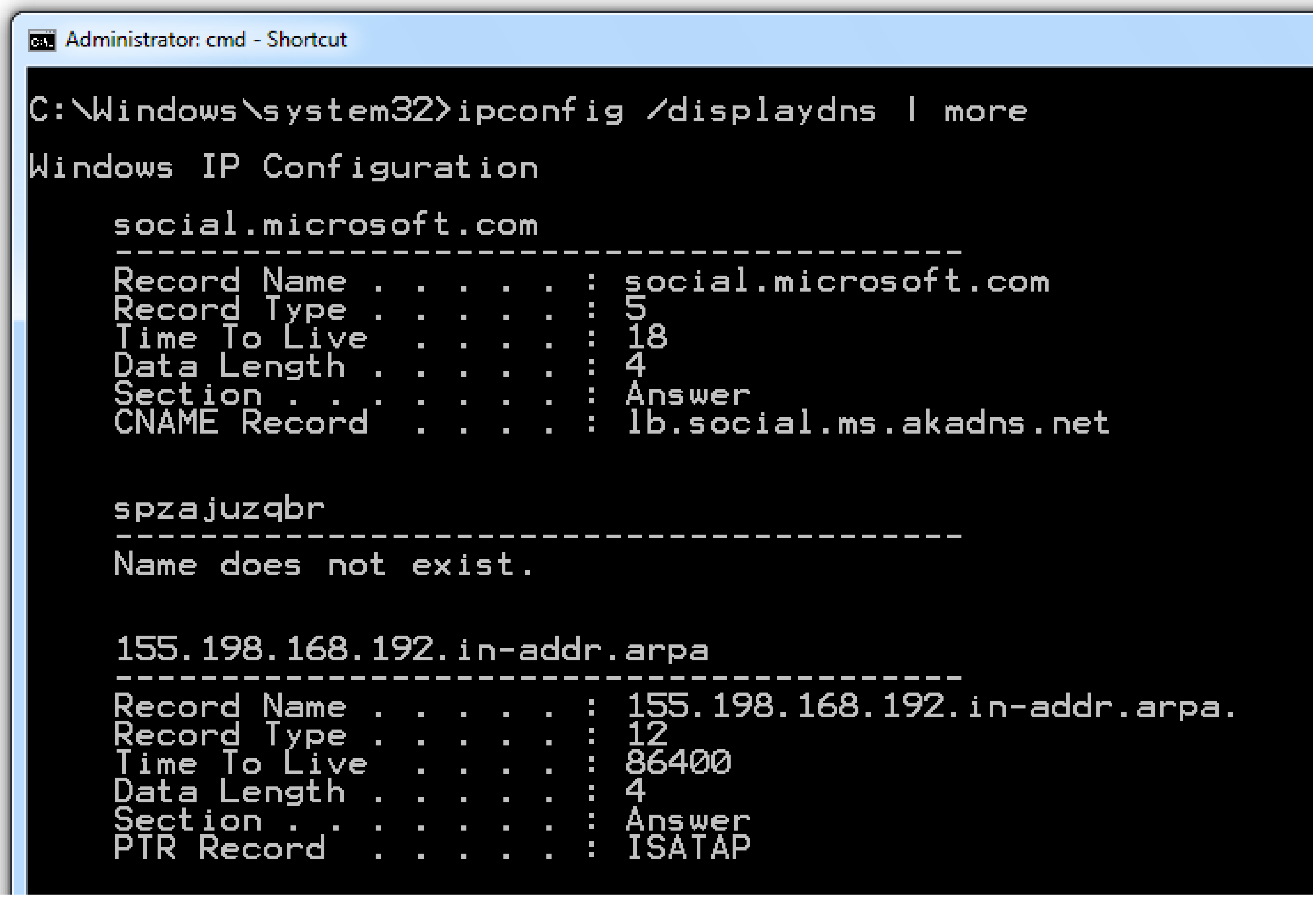
714 strings found (8798 bytes)

Address								Blocks	Protection	Details
06AA0000								1	Read/Write	
06AB0000								1	Read/Write	
06AC0000								1	Read/Write	
06AD0000								1	Read/Write	
06AE0000								1	Read/Write	
06AF0000								1	Read/Write	
06B00000								1	Read/Write	
06B50000								1	Read/Write	
06BA0000								3	Read/Write/Guard	Thread ID: 3532
06C20000								3	Read/Write/Guard	Thread ID: 4060
07070000	Shareable	4 K	4 K					1	Read/Write	
10000000	Image	124 K	124 K	12 K	116 K	16 K	100 K	5	Execute/Read	C:\WINDOWS\system32\6to4ex.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

DNS Cache

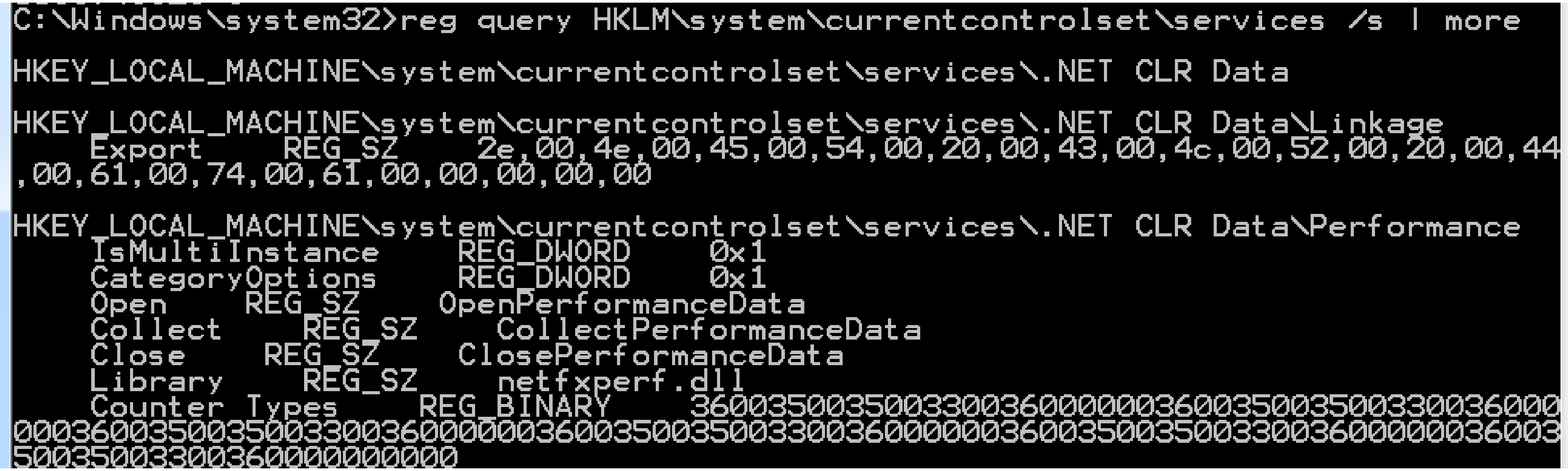


```
C:\Windows\system32>ipconfig /displaydns | more

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
```

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

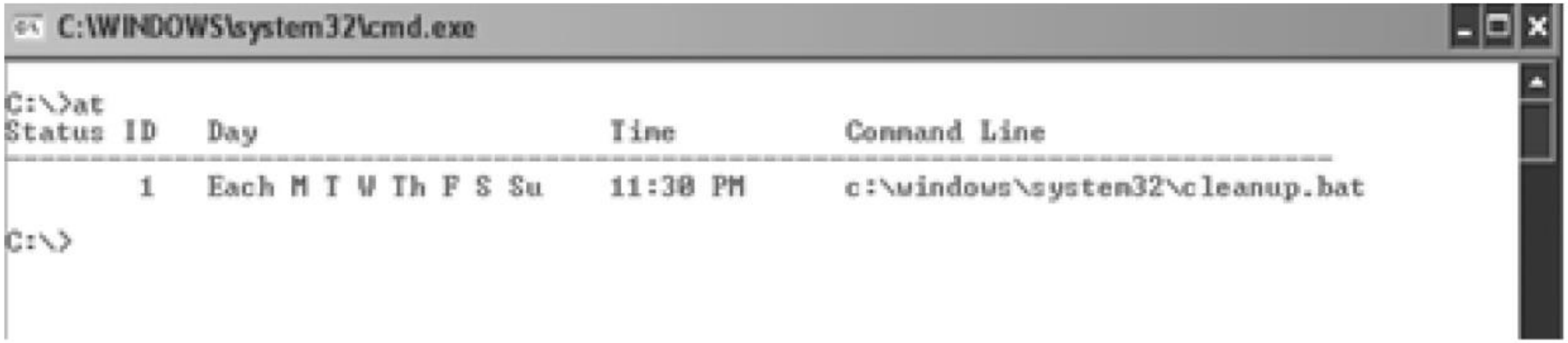
Registry Query for Run and RunOnce Keys



```
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
00036003500350033003600000036003500350033003600000036003500350033003600000036003
5003500330036000000000
```

File/Process Capture (2/2)

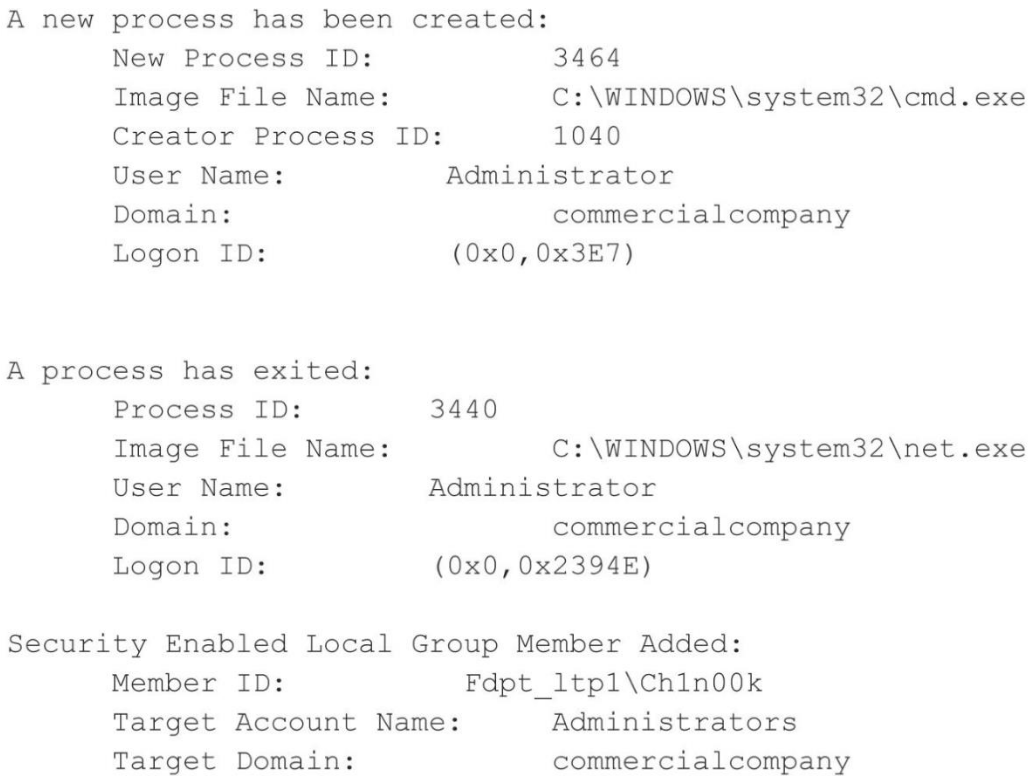
- Scheduled Tasks: at to find scheduled tasks



```
C:\>at
Status ID   Day                     Time          Command Line
-------------------------------------------------------------------------------
        1   Each M T W Th F S Su    11:30 PM      c:\windows\system32\cleanup.bat

C:\>
```

File/Process Capture (2/2)

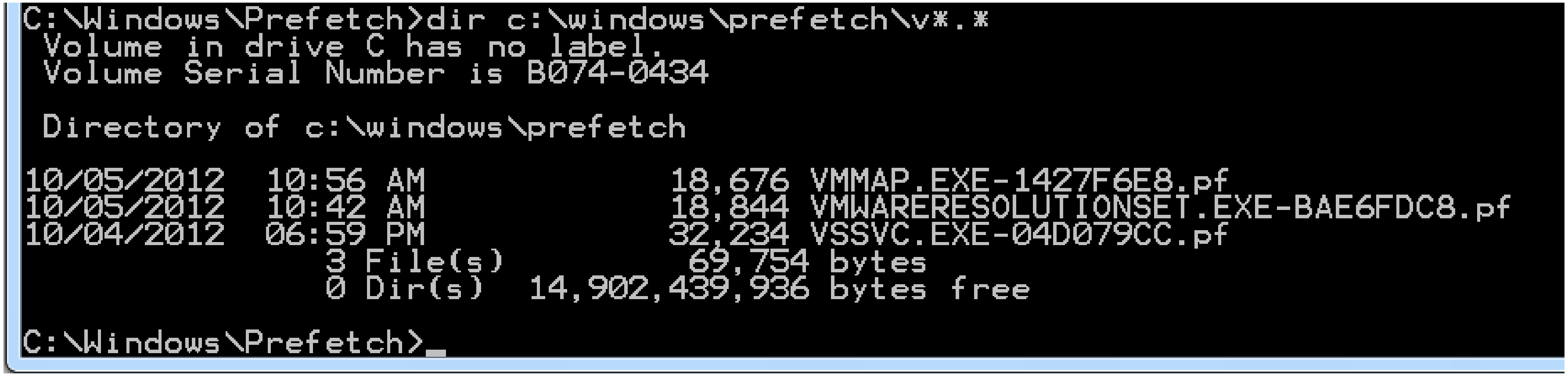
- Scheduled Tasks: at to find scheduled tasks
- Event Logs: psloglist to retrieve System and Security Event logs → commands issued by attackers



```
A new process has been created:
      New Process ID:          3464
      Image File Name:         C:\WINDOWS\system32\cmd.exe
      Creator Process ID:      1040
      User Name:         Administrator
      Domain:                  commercialcompany
      Logon ID:          (0x0,0x3E7)


A process has exited:
      Process ID:       3440
      Image File Name:         C:\WINDOWS\system32\net.exe
      User Name:        Administrator
      Domain:                  commercialcompany
      Logon ID:         (0x0,0x2394E)

Security Enabled Local Group Member Added:
      Member ID:          Fdpt_ltp1\Ch1n00k
      Target Account Name:     Administrators
      Target Domain:           commercialcompany
```

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

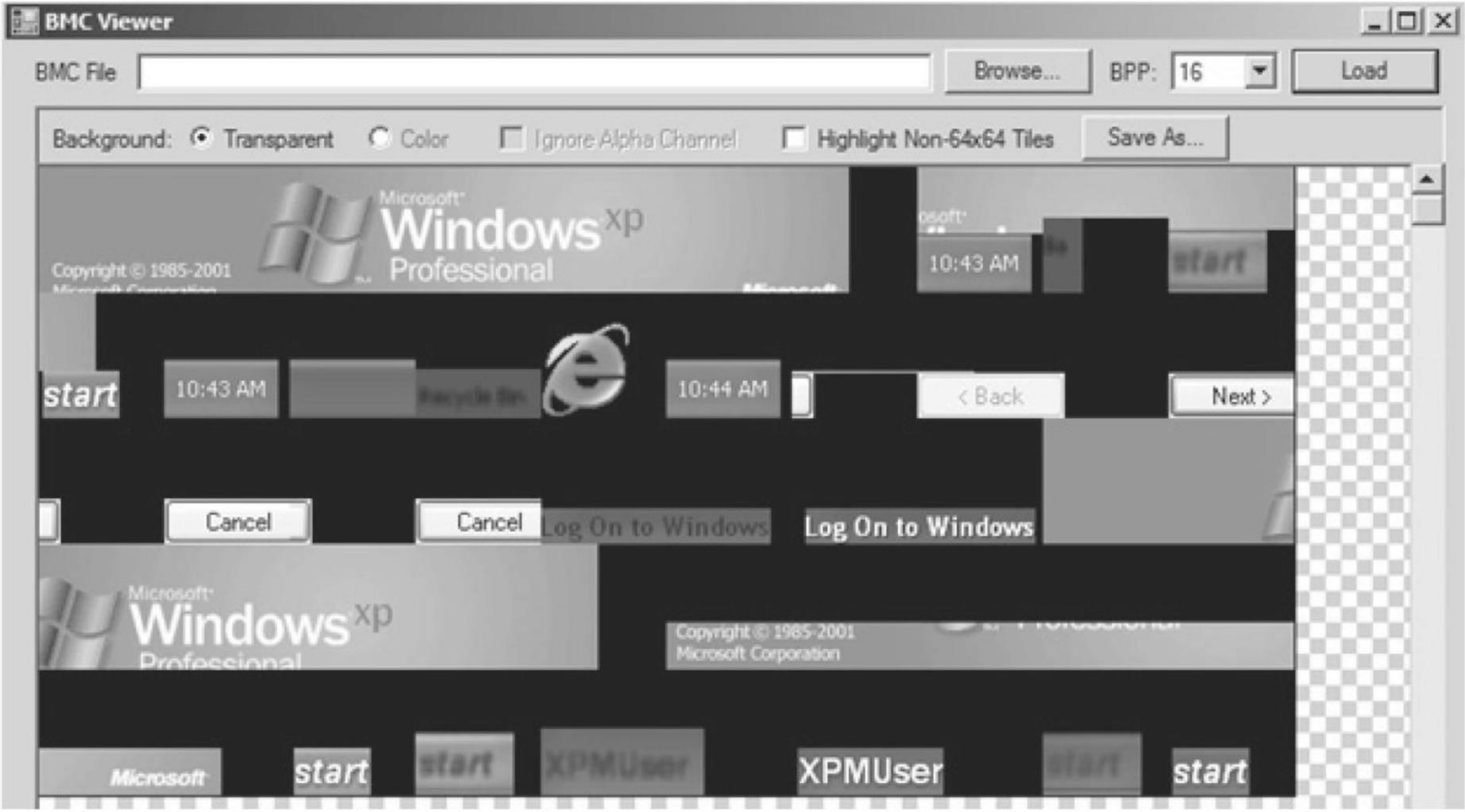


```
C:\Windows\Prefetch>dir c:\windows\prefetch\v*.*
 Volume in drive C has no label.
 Volume Serial Number is B074-0434

 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>_
```

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

File/Process Capture (2/2)



BMC Viewer

BMC File:

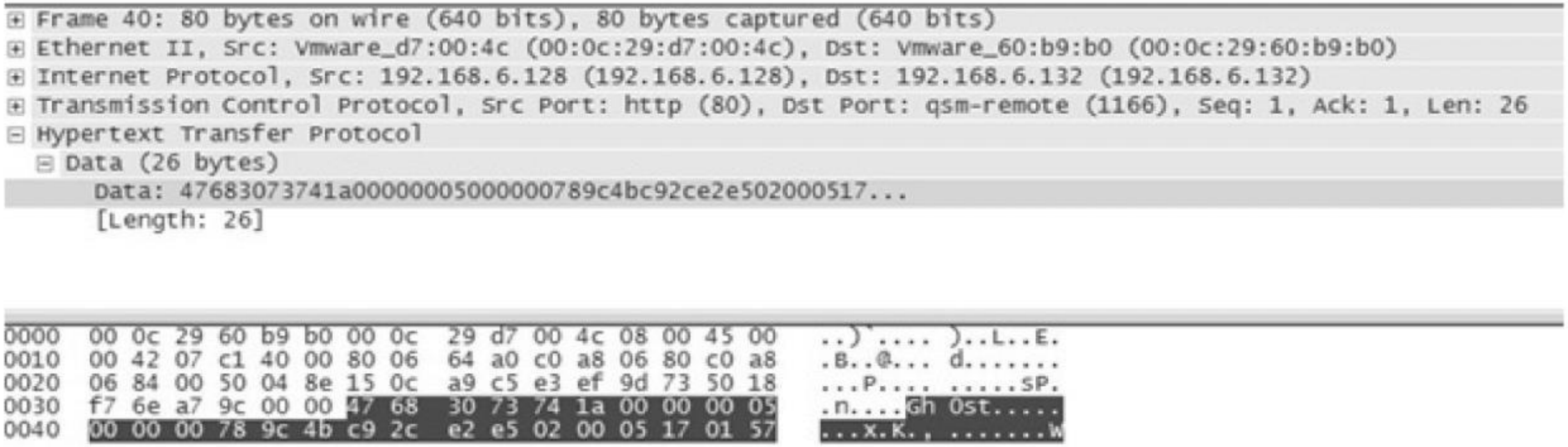
BPP: 16

Background: ● Transparent ○ Color □ Ignore Alpha Channel □ Highlight Non-64x64 Tiles

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

Wireshark



```
⊞ Frame 40: 80 bytes on wire (640 bits), 80 bytes captured (640 bits)
⊞ Ethernet II, Src: Vmware_d7:00:4c (00:0c:29:d7:00:4c), Dst: Vmware_60:b9:b0 (00:0c:29:60:b9:b0)
⊞ Internet Protocol, Src: 192.168.6.128 (192.168.6.128), Dst: 192.168.6.132 (192.168.6.132)
⊞ Transmission Control Protocol, Src Port: http (80), Dst Port: qsm-remote (1166), Seq: 1, Ack: 1, Len: 26
⊟ Hypertext Transfer Protocol
  ⊟ Data (26 bytes)
      Data: 47683073741a000000050000000789c4bc92ce2e502000517...
      [Length: 26]
```

```
0000   00 0c 29 60 b9 b0 00 0c  29 d7 00 4c 08 00 45 00   ..)`.... )..L..E.
0010   00 42 07 c1 40 00 80 06  64 a0 c0 a8 06 80 c0 a8   .B..@... d.......
0020   06 84 00 50 04 8e 15 0c  a9 c5 e3 ef 9d 73 50 18   ...P.... .....sP.
0030   f7 6e a7 9c 00 00 47 68  30 73 74 1a 00 00 00 05   .n....Gh 0st.....
0040   00 00 00 78 9c 4b c9 2c  e2 e5 02 00 05 17 01 57   ...x.K., .......W
```

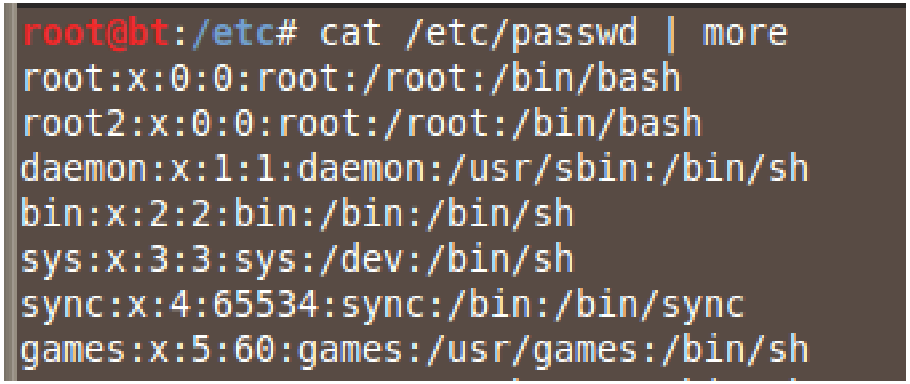
Antivirus Exclusions

- 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

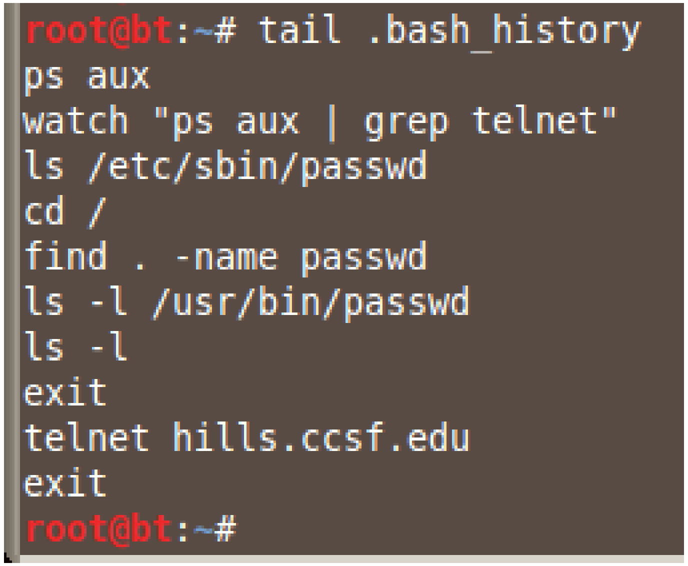
- Attackers upload a PHP backdoor
- Create a SUID root shell for getting root back in case a password is changed
- With Metaexploit Framework, compromised host used as a pivot host (without tools installed)
- Run shells like Meterpreter in memory without disk writes: leave little on the host

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

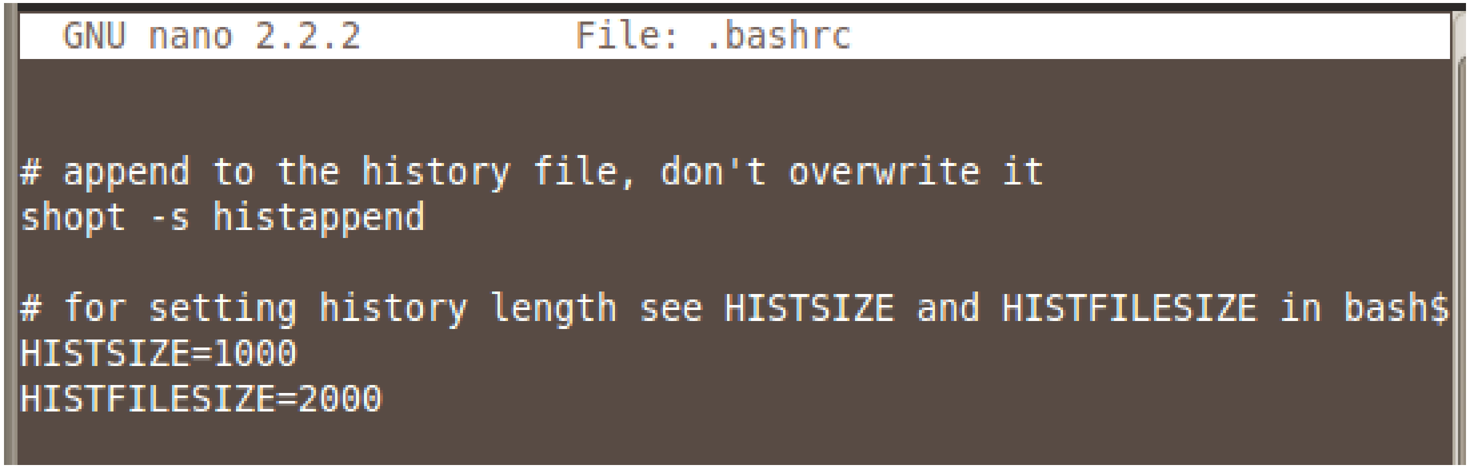
- In each user's home directory
- .bash_history
- Remembers the previous 2000 lines by default in BackTrack 5 R2



```
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



```
  GNU nano 2.2.2              File: .bashrc


# append to the history file, don't overwrite it
shopt -s histappend

# for setting history length see HISTSIZE and HISTFILESIZE in bash$
HISTSIZE=1000
HISTFILESIZE=2000
```

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

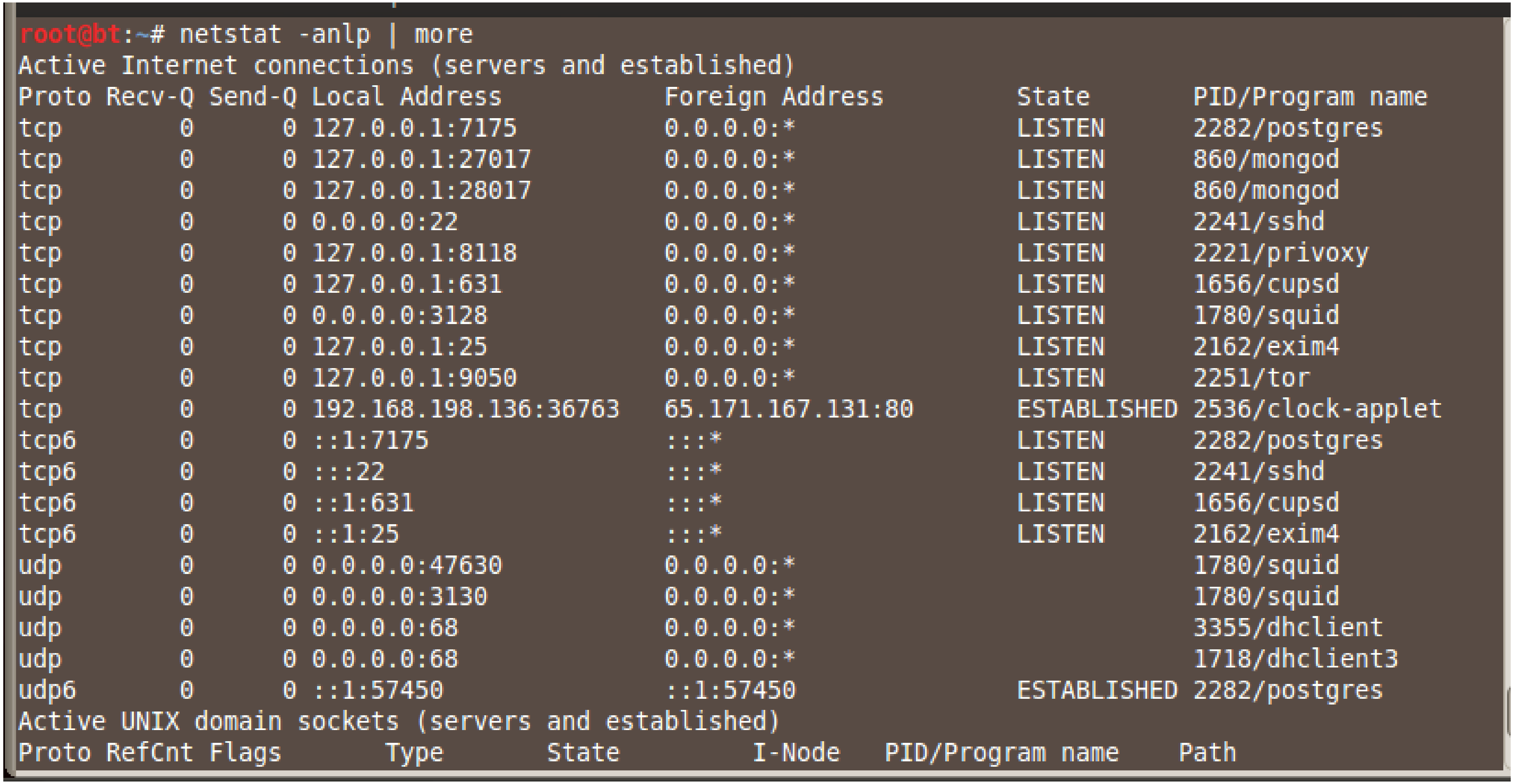
Commands to Check Network Connections

- To check network connections, use

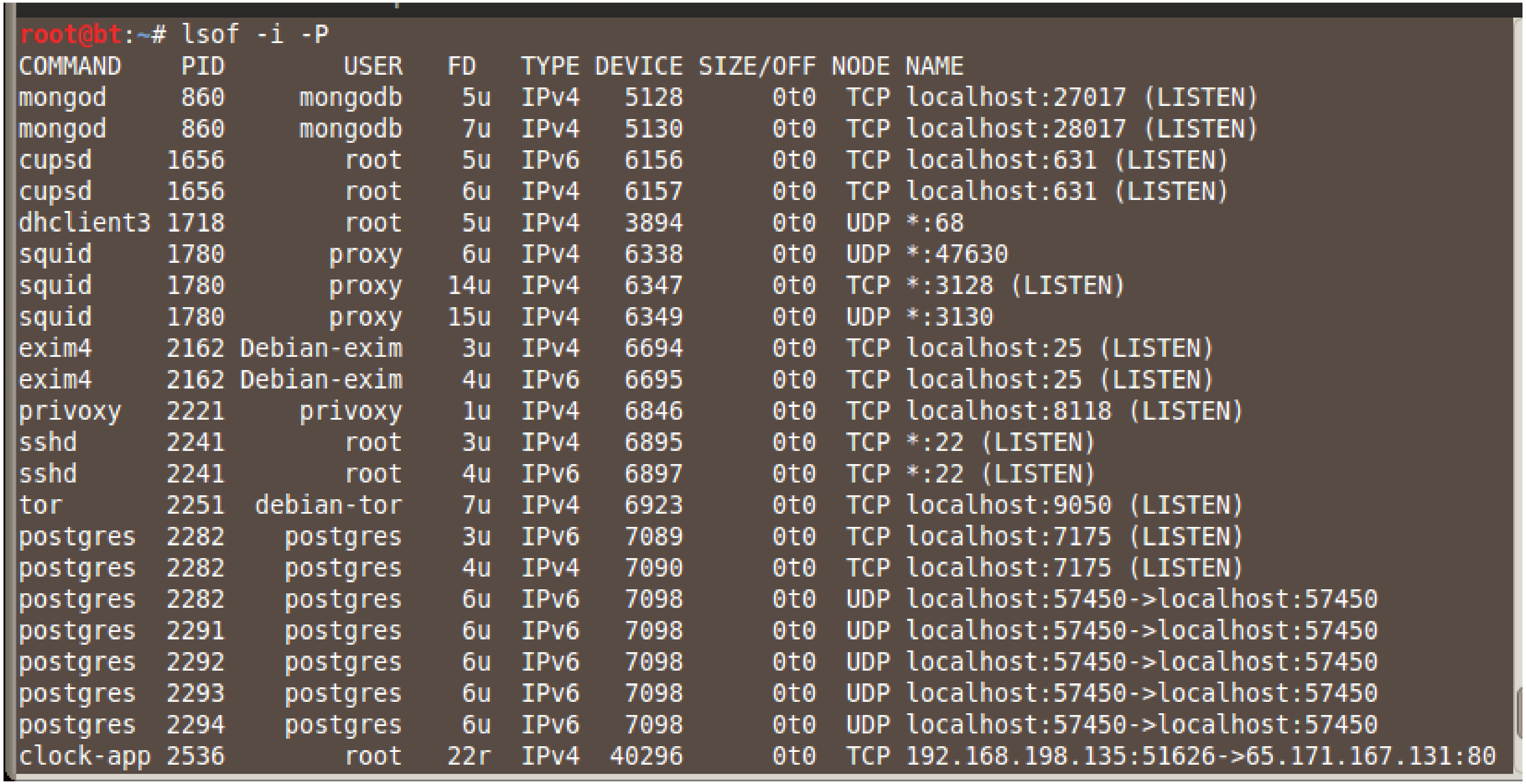
  ```
  netstat –anlp
  lsof –i -P
  ```

  - Shows all open files (and listening services)

- IMPORTANT: A rootkit could cause these programs to lie

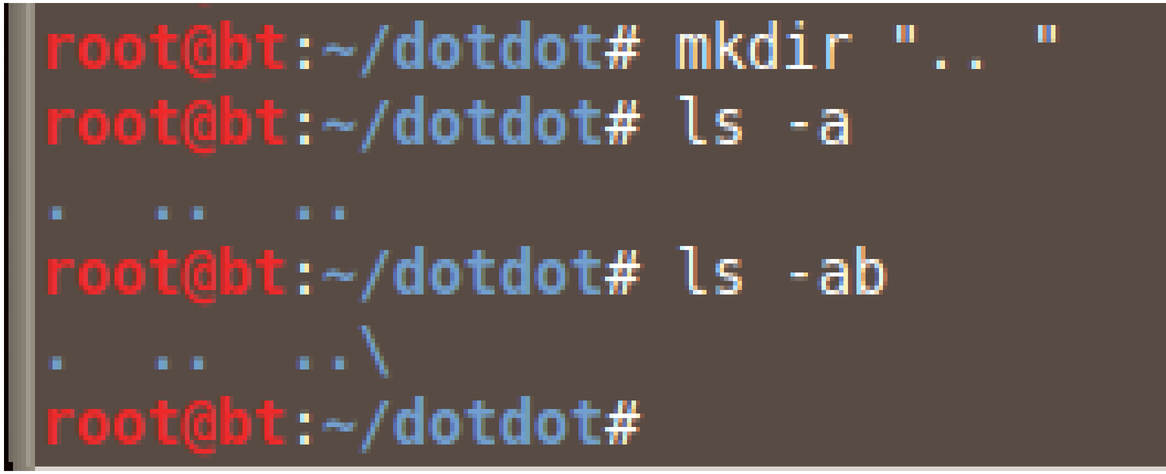


```
root@bt:~# netstat -anlp | more
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 127.0.0.1:7175          0.0.0.0:*               LISTEN      2282/postgres
tcp        0      0 127.0.0.1:27017         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



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

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

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/
```

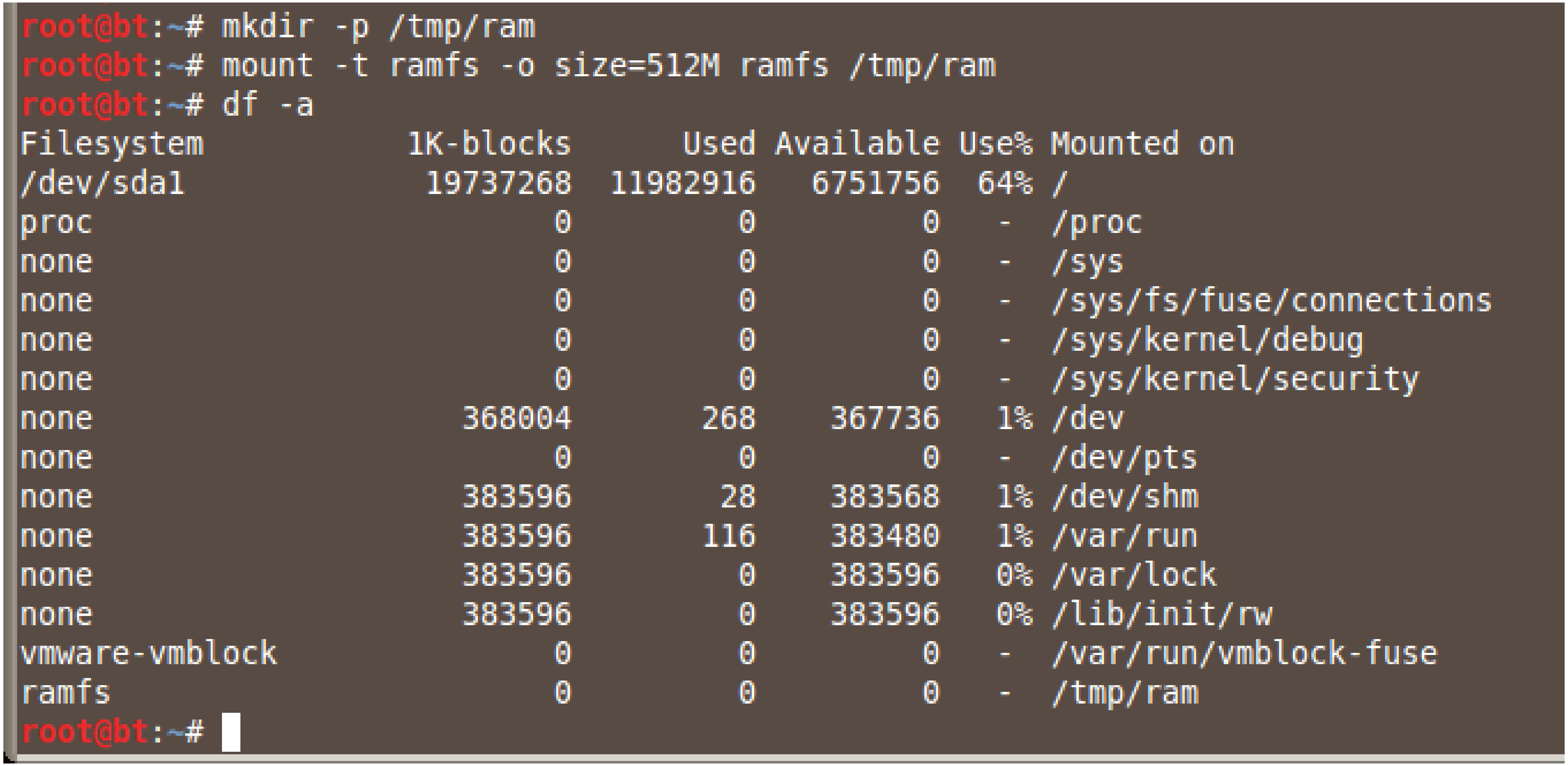
- To see Ram drives, use

```
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:~# 
```

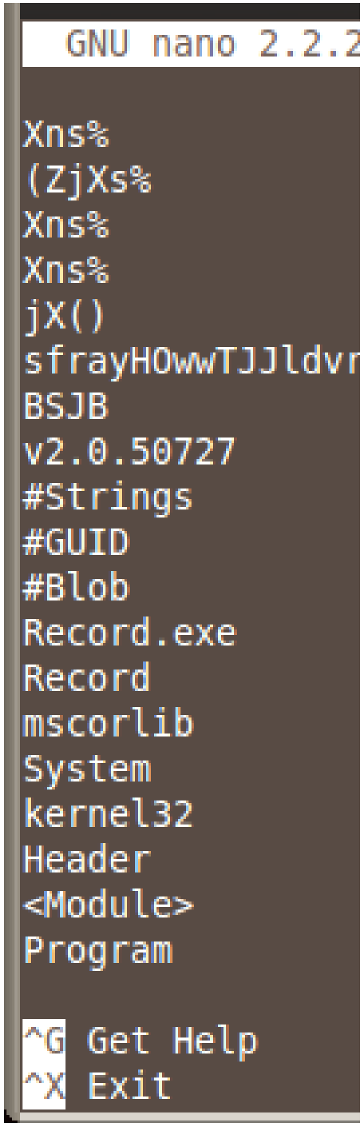
Strings command

- To get readable strings from a file

  strings malware.exe > malfile

- To view results

  nano malfile



```
  GNU nano 2.2.2

Xns%
(ZjXs%
Xns%
Xns%
jX()
sfrayHOwwTJJldvr
BSJB
v2.0.50727
#Strings
#GUID
#Blob
Record.exe
Record
mscorlib
System
kernel32
Header
<Module>
Program

^G Get Help
^X Exit
```

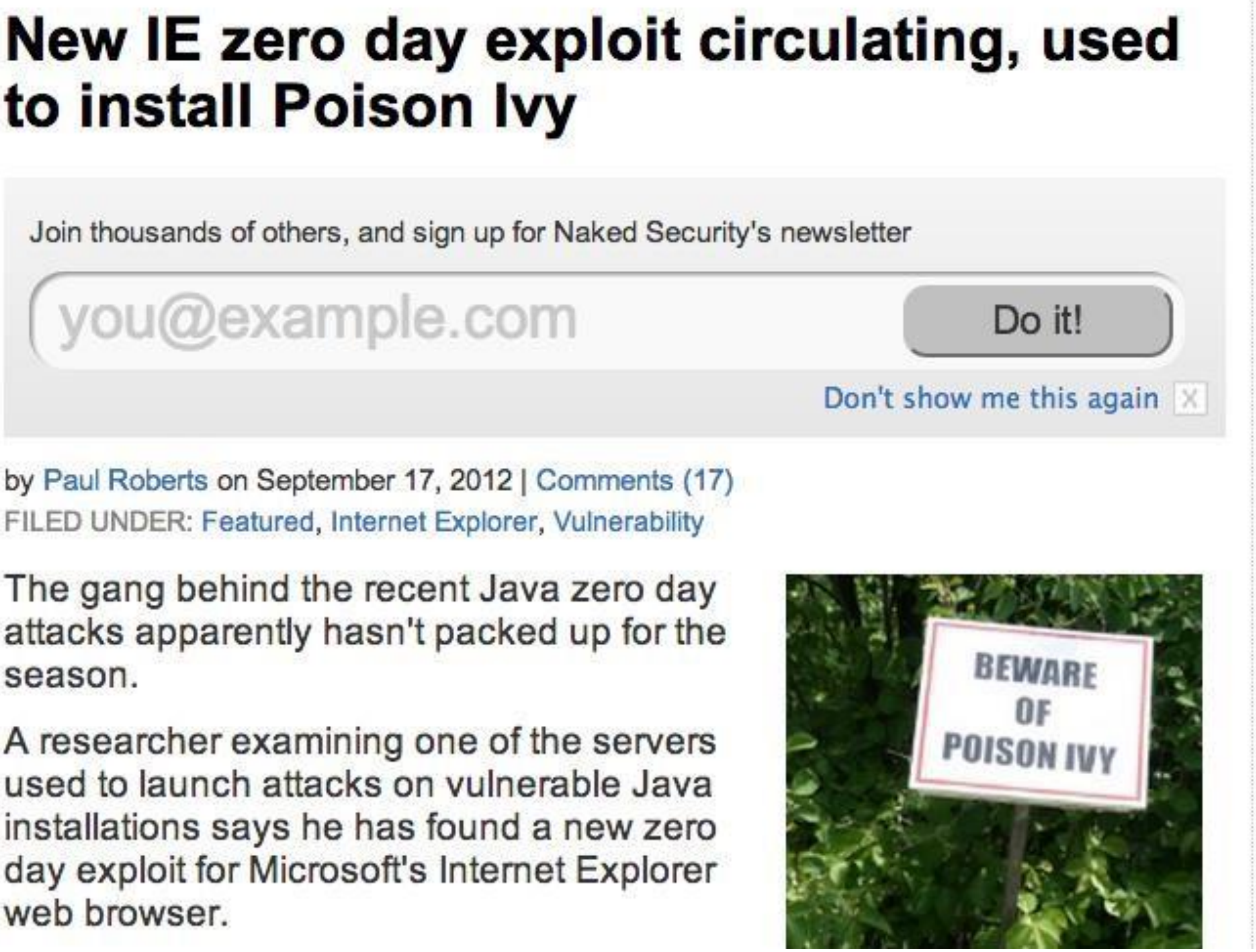
Poison Ivy

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



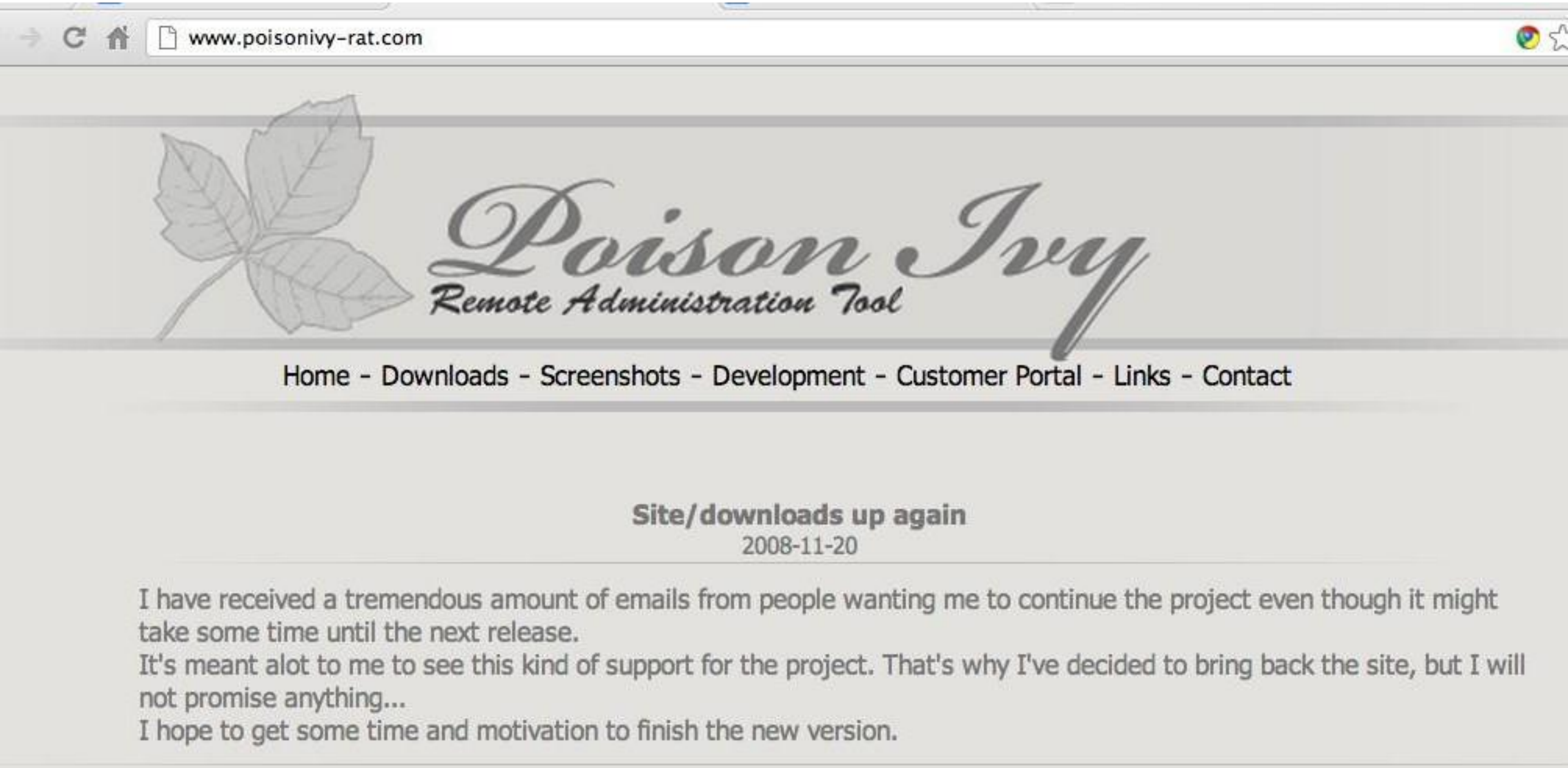
New IE zero day exploit circulating, used to install Poison Ivy

Join thousands of others, and sign up for Naked Security's newsletter

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 (to survive reboot)
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 user 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)