Building A

NO-FRILLS

Malware Lab

Robert.Pitcher@ps-sp.gc.ca

Andre.Cormier@ps-sp.gc.ca

Cyber Incident Response Centre (CCIRC)

- **Located in the nation's capital of Ottawa, the CCIRC is the national focal point for dealing with cyber based threats to Canada's Critical Infrastructure.**
- **Provides a stable, 24/7 coordination and support across the Government of Canada (GoC), and to key national players in the event of cyber based emergencies**
- **Participation in operational working groups and strategic partnerships that include domestic and international partners**

Cyber Incident Response Centre (CCIRC)

- National operations centre with the following mandates:
  - Focal point for reporting of real or imminent threats, vulnerabilities and incidents against the GoC
  - Threat and vulnerability identification and analysis
  - Distribution of cyber based publications (Alerts/Advisories/Cyber Flashes/Information notes)
  - Technical analysis, investigations, and coordination

Cyber Incident Response Centre (Malware Analysis)

CCIRC Malware Analysis Technical Capabilities

- In support of its mandate, CCIRC has a fully functioning malware analysis lab performing the following tasks:
  - Malware reverse engineering
  - Malware detection
  - Behavior mapping of malcode
  - Technical analysis and research papers

- CCIRC also enjoys strategic partnerships with other government agencies and services responsible for malware investigations:
  - National Defense, National Intelligence, Federal/Provincial Law Enforcement

Sun Tzu: The Art of “Malware”

The art of war teaches us to rely not on the likelihood of the enemy's not coming, but on our own readiness to receive him; not on the chance of his not attacking, but rather on the fact that we have made our position unassailable.

- Sun Tzu

What is Malware?

Traditionally, the term Malware was used as a synonym for computer viruses

The term has since evolved to cover multiple vectors of computer infection and exploitation, including, but not limited to:

- **Adware**
- **Keyloggers**
- **RootKits**
- **Trojans**
- **Browser compromise**
- **Worm**
- **Botnets**
- **etc…**

The goal of Malware is still the same: Software designed to intentionally cause damage or disruption to a computer system, usually in such a way as to remain hidden to the user.

The goal of a CERT should mimic the goal of malware, but in reverse: An organization designed to prevent the damage and disruption to the computer systems they service.

An effective functioning CERT should therefore possess the ability to analyze the malware it receives

Q…. So Why Build a Malware Lab?

- **Better to be pro-active, than reactive in times of emergency…**
- **You can't protect against what you do not understand.**
- **CCIRC has received and analyzed multiple pieces of malicious software that were unknown to antivirus vendors.**
- **It is therefore up to the investigating organization to perform a forensic examination of the device or piece of malware to determine the malicious capabilities.**
- **To achieve this, you have multiple options:**
  - **An "off the shelf" product**
  - **Outsourcing**
  - **A customized creation**

Off the Shelf Products

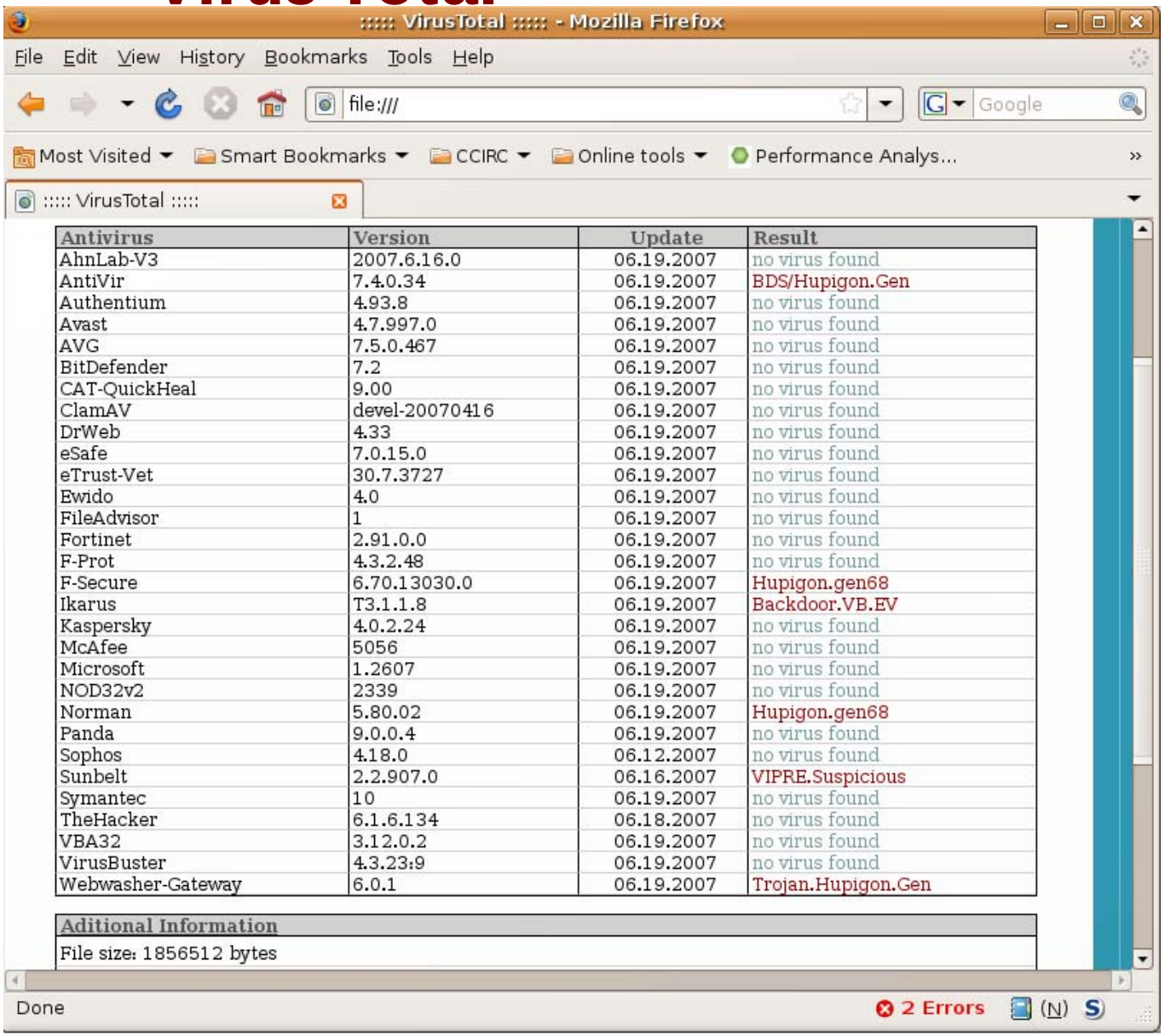
Malware Vendors:

- **Symantec:**http://www.symantec.com
- **McAfee:** http://www.mcafee.com
- **Trend Micro:**http://www.trendmicro.com
- **AVG:** http://www.grisoft.com/
- **Panda Software:**http://www.pandasoftware.com/
- **Sophos:** http://www.sophos.com

Online Resources:

- **Virus Total:** http://www.virustotal.com
- **Anubis:** http://anubis.iseclab.org/index.php
- **Sunbelt:** http://research.sunbelt-software.com/Submit.aspx

Virus Total

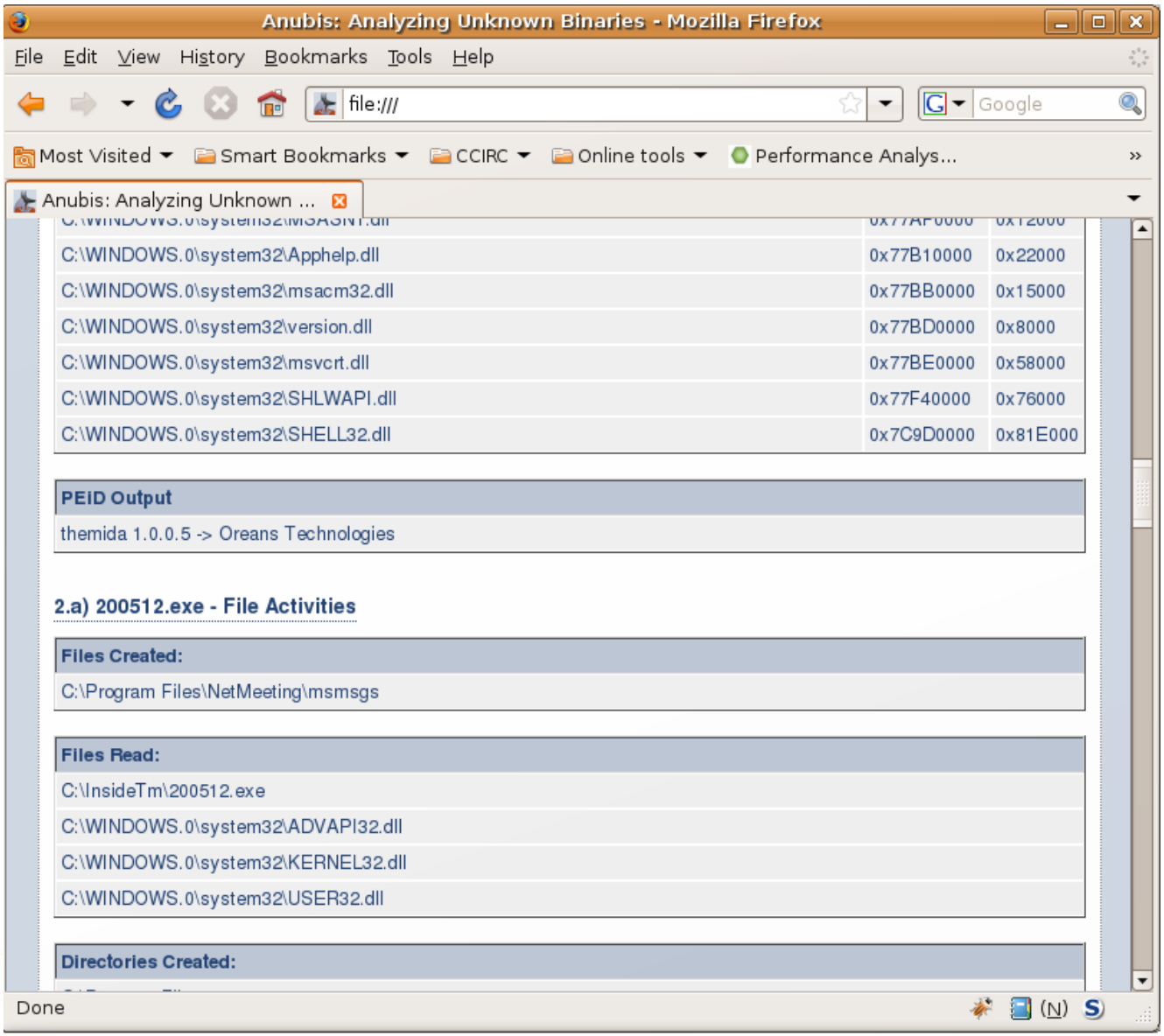


Antivirus	Version	Update	Result
AhnLab-V3	2007.6.16.0	06.19.2007	no virus found
AntiVir	7.4.0.34	06.19.2007	BDS/Hupigon.Gen
Authentium	4.93.8	06.19.2007	no virus found
Avast	4.7.997.0	06.19.2007	no virus found
AVG	7.5.0.467	06.19.2007	no virus found
BitDefender	7.2	06.19.2007	no virus found
CAT-QuickHeal	9.00	06.19.2007	no virus found
ClamAV	devel-20070416	06.19.2007	no virus found
DrWeb	4.33	06.19.2007	no virus found
eSafe	7.0.15.0	06.19.2007	no virus found
eTrust-Vet	30.7.3727	06.19.2007	no virus found
Ewido	4.0	06.19.2007	no virus found
FileAdvisor	1	06.19.2007	no virus found
Fortinet	2.91.0.0	06.19.2007	no virus found
F-Prot	4.3.2.48	06.19.2007	no virus found
F-Secure	6.70.13030.0	06.19.2007	Hupigon.gen68
Ikarus	T3.1.1.8	06.19.2007	Backdoor.VB.EV
Kaspersky	4.0.2.24	06.19.2007	no virus found
McAfee	5056	06.19.2007	no virus found
Microsoft	1.2607	06.19.2007	no virus found
NOD32v2	2339	06.19.2007	no virus found
Norman	5.80.02	06.19.2007	Hupigon.gen68
Panda	9.0.0.4	06.19.2007	no virus found
Sophos	4.18.0	06.12.2007	no virus found
Sunbelt	2.2.907.0	06.16.2007	VIPRE.Suspicious
Symantec	10	06.19.2007	no virus found
TheHacker	6.1.6.134	06.18.2007	no virus found
VBA32	3.12.0.2	06.19.2007	no virus found
VirusBuster	4.3.23:9	06.19.2007	no virus found
Webwasher-Gateway	6.0.1	06.19.2007	Trojan.Hupigon.Gen

Aditional Information
File size: 1856512 bytes

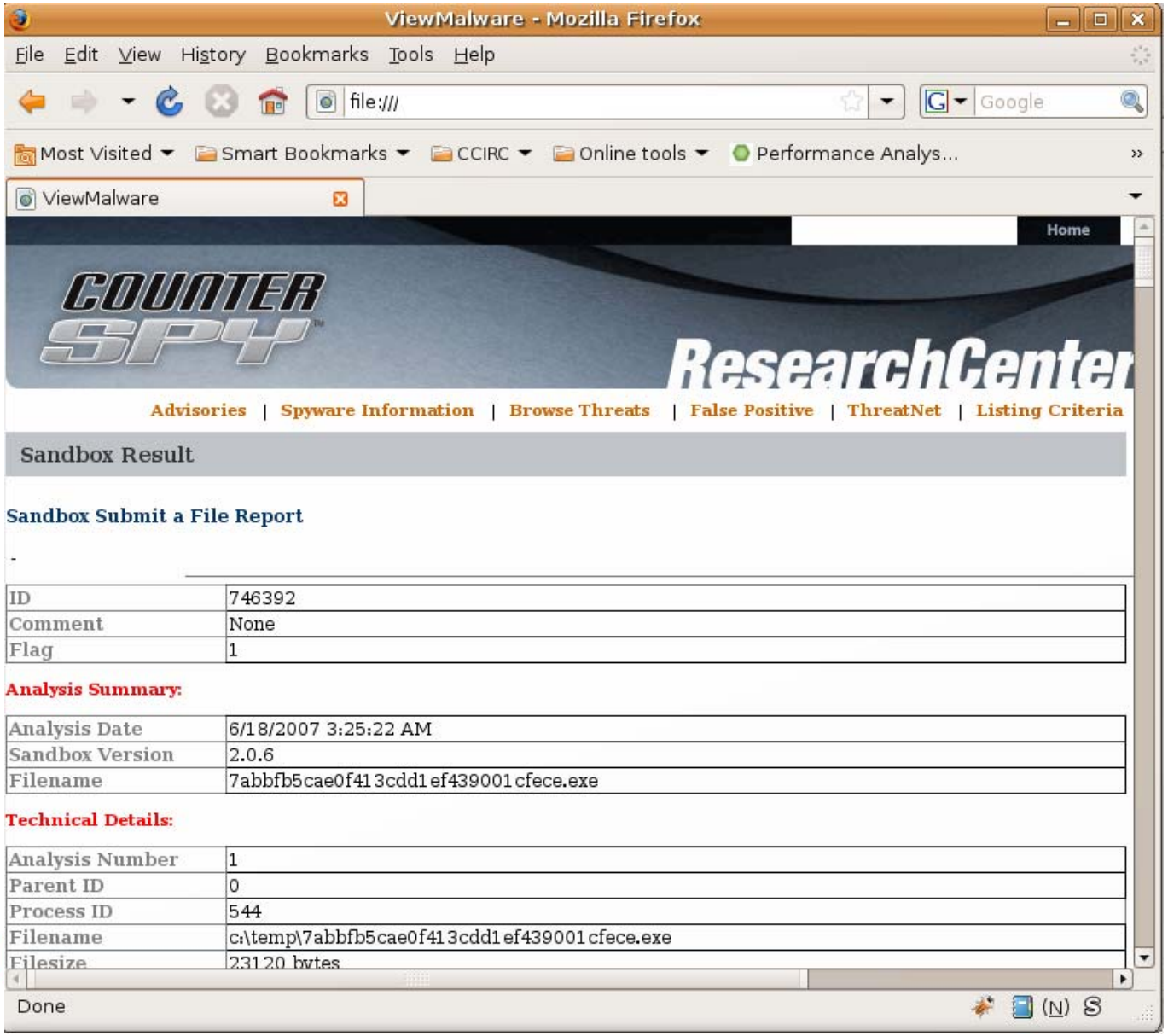
Canada

Anubis



Canada

Sunbelt



Canada

Outsourcing

Private Sector Alliances

- **Microsoft**
- **Contracted agencies**

Public/Government Sector Alliances

- **Military**
- **Law Enforcement**
- **Intelligence Agencies**

A Customized Creation!

- **Building a customized malware lab that is tailored to the needs, and capabilities of an organization**
- **Combines the best of both worlds, at a fraction of the cost**
- **Many CERT are also sometimes under financial and operation restrictions in the performance of their duties.**

The Good, the Bad, the Expensive!

1.“Off the Shelf”

Pros: Proven track record, variety of tools, latest technologies, constantly updated, industry leaders

Cons: Typically not customized, detection based on known patterns, *Expensive*, have to submit malware that may be sensitive

2. Outsourcing

Pros: Customizable environments, access to various vendor tools and agreements, experienced staff, pre-established infrastructure and methods of operations

Cons: *Expensive*, security clearances, timelines and lifecycles

3. Customized Product

Pros: Customized, *CHEAP* (free), familiar technologies and tools, expansion capabilities

Cons: Open source tools dependence, unfamiliar technologies, responsibility to remain current, defence is only as good as the builders knowledge

Goals of Malware Analysis

The primary goals of malware analysis

- Detection / Eradication
- Mitigation / Protection
- Education / Profiling

Detection / Eradication

- Analyzing Software and hardware to detect patterns and behavior to determine appropriate responses to remove the identified threat.
- Occurs when you have confirmation or suspicion of the presence of malware on a device
- Techniques
  - Establishing a baseline, infecting, analyzing the Delta
  - Redirecting malware beaconing to emulated locations
  - Simulating beacon calls
  - Passing in command and control commands
  - Breaking encryption algorithms (basic)
  - Using a Sandbox

Detection / Eradication

- Eradication
  - Removing registry key hooks
  - Removal of key loggers, image capture devices, or related malicious s/w
  - Reduction of privileges on infected machines
  - Restoration to baseline

Mitigation / Protection

- **Once a threat has been isolated, countermeasures must be developed to ensure protection**

- **Countermeasures:**
  - **Blocking IP addresses imbedded in the malware**
  - **Closing ports used by the software**
  - **Development of signatures (SNORT) to assist in detection and identification**
  - **Network scans to detect signatures to locate other infected machines**
  - **Review of corporate network to ensure conformity to security best-practices.**

Education / Profiling

Analyzing malware can not only provide insight into the modus operandi of those you are trying to fight, but you can also learn the weaknesses of your own organization.

Examples: Security holes/Best practices breaches

- **Ability to download and install executables**
- **Administrator rights on individual machines**
- **Failure to block malicious sites**
- **Blocking spoofed emails**

Analysis is not just about the code, but determining the methods an attacker is using.

By performing both behavioral analysis and code analysis, an investigator can develop intelligence and tactical data on the attacking agent and their tools and techniques, and use this information to assist in attacker agent and threat mitigation.

Final Thoughts… Sun Tzu

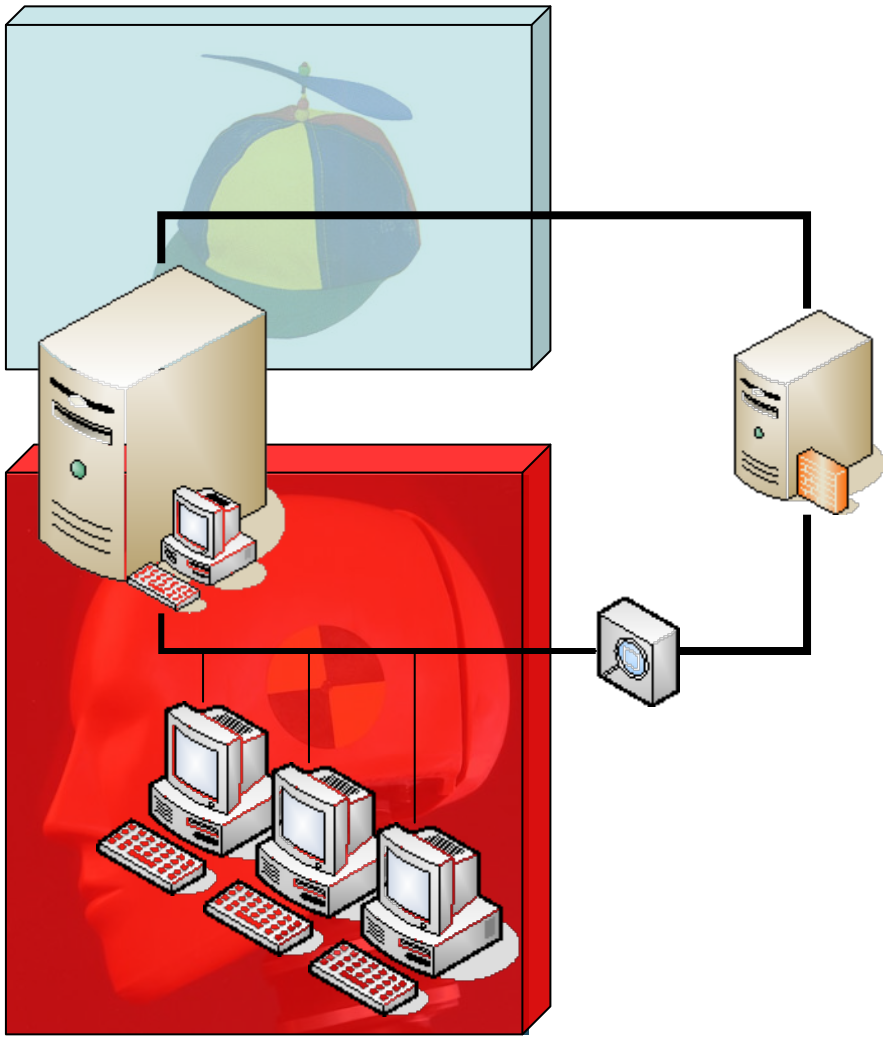
If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle.

- Sun Tzu

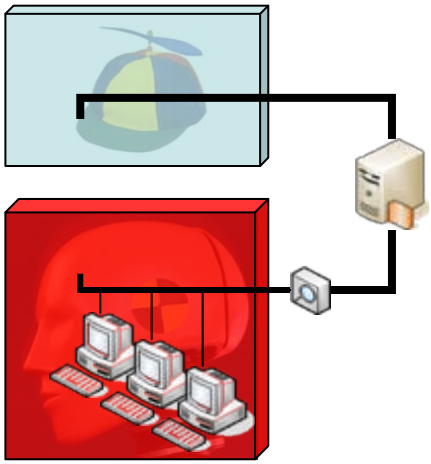
General overview of CCIRC's Malware Lab

Image used with permission from Adam Dorman
http://www.adamdorman.com

Bird’s eye view



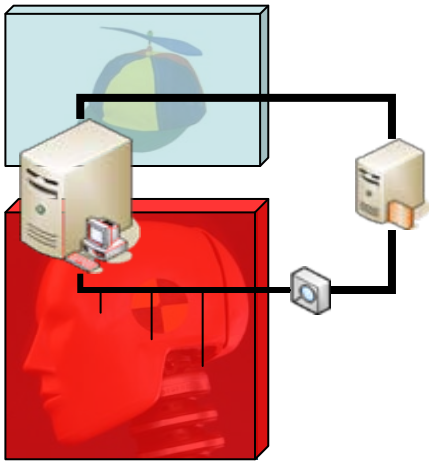
Analysis station using Virtualisation



Windows XP Pro

- **VMWare Workstation**
- **Several Guest Host versions**
- **Guests OS bridge to the testing zone or Host only network**

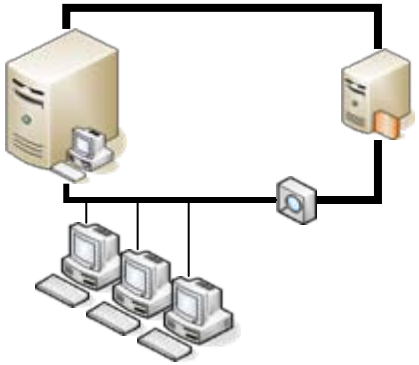
Analysis environment using physical devices



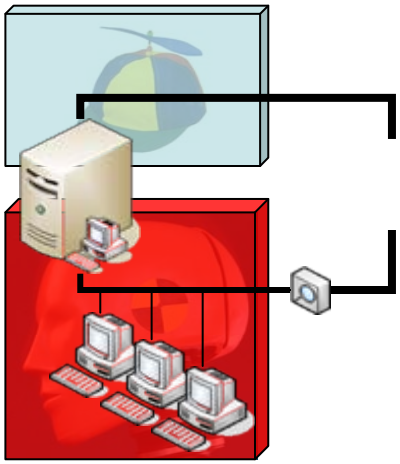
Windows XP Pro

- **3 main images at various patching stages**
- **Microsoft Office installed**

The Network



The Firewall



Ubuntu

- **Firewall**
- **Network monitoring**
- **Fake DNS server**
- **Fake network services**
- **Proxy**
- **Disk image server**

The Virtual Machines Host

- Using Virtual Machines (VM) is convenient.
  - Setting a test environment is quick
  - Moving data between Host and guest is easy
  - We can save the state of a machine and revert back to it later (Snapshots)
  - We can run more than one VM at the same time and simulate a whole network with one physical machine
  - Network monitoring is easy.

The Virtual Machines Host

- Using Virtual Machines (VM) has its drawbacks.
  - Advanced Malware will not run in VM
  - Running several VMs needs a lot of resources: RAM, CPU and disks.

The Virtual Machines Host

- Windows XP Pro
  - With the latest patches
- Lots of RAM (At 1Gig, 2 is better)
- Lots of disk space (>100Gigs)
- Good CPU (>2Ghz)

Required Software

- Virtualization Software
  - VMWare
    - VMWare Workstation is preferable. Snapshots are important and only VMWare Workstation allows multiple snapshots. VMWare server only allows one snapshot per VM.
  - VirtualBox
    - VirtualBox OSE (Open Source Edition)
      - Allows multiple snapshots.
      - No USB support. If you need it go for VirtualBox closed source. Make sure you understand the license agreement.

Setting up the dummy VMs

- Multiple VMs are required.
  - Build VMs at various patching levels of Windows XP, 2k3 or Vista
    - SP1, SP2, IE6, IE7, Office 2000, XP, 2003, 2007…
  - Build VM for network services
    - Typically a Linux firewall with 2 virtual interfaces. One Host Only and one bridged.

Networking

- Use Internal Host networking between VM
  - Easy with VMWare
  - Needs some tweaking with VirtualBox under Linux (use bridged interfaces)
- Do not allow direct connectivity with the Internet.
  - When the Internet is needed, it should go through the firewall

Hard disks

- Use auto-expanding disks to save space
- Create disks as big as the average workstation disk in your organization
  - With auto-expanding disks, on a disk partition of 80Gigs the OS will see the full partition size but the host will use only the space needed for the installation.

Analysis environment using physical devices

- Using physical devices is not really convenient:
  - Setting a test environment is slower
  - Saving the state of the machine and reverting back to it later is much slower
  - We need one computer per host

Analysis environment using physical devices

- Using physical devices is necessary in some cases:
  - Advanced Malware will not run in VM
- When the malware does not run as we expected in VM, we need to fallback on real computers

Analysis environment using physical devices

- Use decommissioned PCs from your organization

- Our PCs are:
  - Intel Pentium 4 3.2Ghz, 2GB RAM
  - 2 x 163GB hard drives

Analysis environment using physical devices

Hard disks

- Setup several partitions
  - The boot partition
  - The Analysis partition
  - The disk imaging partition

Analysis environment using physical devices

- Snapshots with physical devices
  - Using disk imaging utilities.
  - Disk images stored:
    - On a server to preserve integrity
    - On a separate partition for increased speed and convenience.
- Multiple disk images are required for the Analysis partition.
  - Build VMs at various patching levels of Windows XP, 2k3 or Vista
    - SP1, SP2, IE6, IE7, Office 2000, XP, 2003, 2007…

Analysis environment using physical devices

- Boot partition is using grub
- Disk-imaging partition is Linux-based
- The Analysis partition is … well variable

The Network

- Fake DNS server
  - Will redirect any query to a known IP which runs fake services
- Fake network services
  - Will capture first interactions with the server. This is key to understanding what is the real protocol used with the server.

The Network

- Network is supported by an ethernet switch with VLAN and port forwarding features
  - 2 VLANS (One for management and one for testing)
- Network Isolation – Firewall
  - Linux based IPTables
  - Proxying for granular control
- Network monitoring station
  - Switch setup with port forwarding for test VLAN ports
  - Network recording with tcpdump (Always record all packets to a binary file)
    tcpdump –ni *if* –s 0 –w *outputfile*

The Network

- Setup a Fake DNS server
  - Bind9
  - Setup a “Catch All” zone

This will enable you to redirect all DNS requests to a single IP running fake network services.

The Network

Change named.conf

Before:

```
zone "." {
    type hint;
    file "/etc/bind/db.root";
};
```

After:

```
zone "." {
    type master;
    file "/etc/bind/catchall";
};
```

The Network

Create the “catchall” zone (/etc/bind/catchall):

```
$TTL    86400
@       IN      SOA     localhost. root.localhost. (
                              1             ; Serial
                         604800             ; Refresh
                          86400             ; Retry
                        2419200             ; Expire
                          86400 )       ; Negative Cache TTL
;
@               IN      NS      localhost.

*.      14400   IN      A       192.168.101.2
```

The Network

Test your fake DNS server:

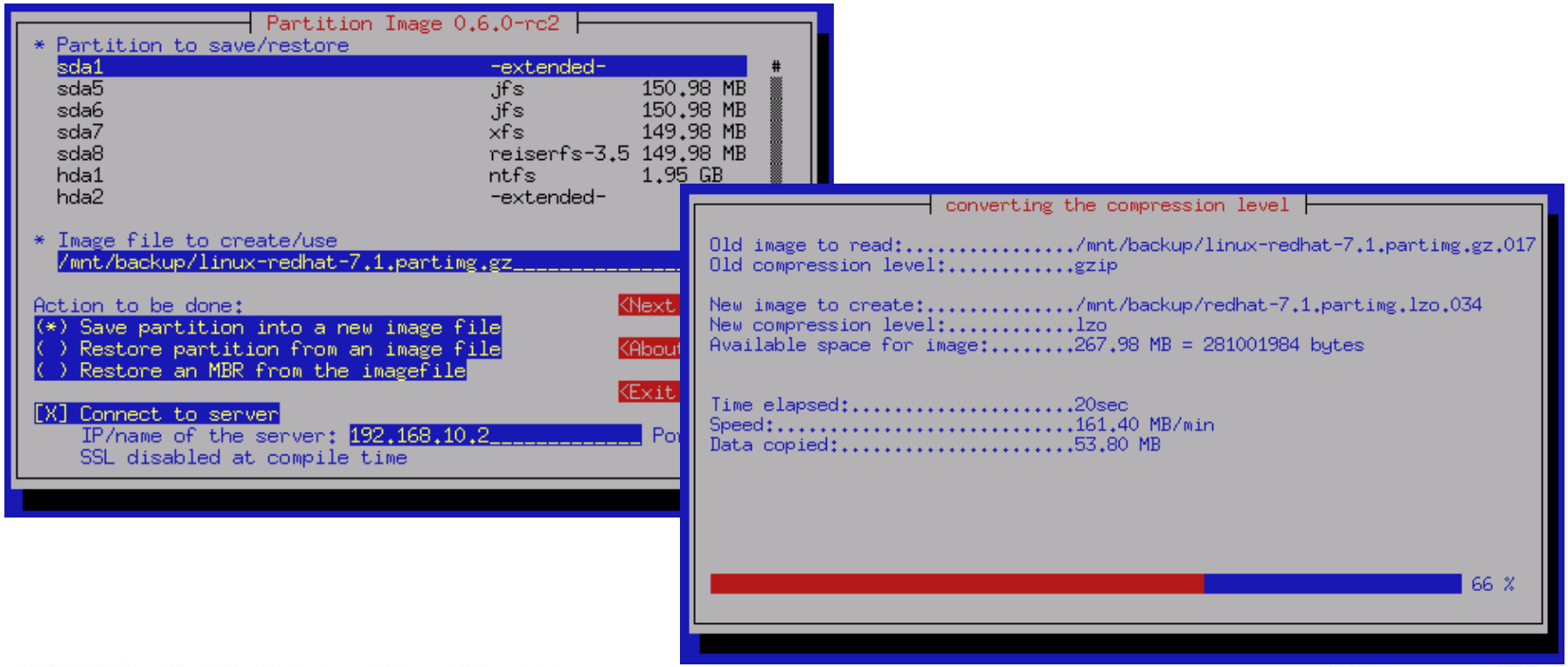
```
$ dig @127.0.0.1 test.vancouver.com.

; <<>> DiG 9.4.2 <<>> @127.0.0.1 test.vancouver.com.
; (1 server found)
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 29368
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 2

;; QUESTION SECTION:
;test.vancouver.com.                    IN          A

;; ANSWER SECTION:
test.vancouver.com.         14400    IN        A         192.168.101.2

;; AUTHORITY SECTION:
.                                      86400       IN          NS          localhost.

;; ADDITIONAL SECTION:
localhost.                604800       IN          A           127.0.0.1
localhost.                604800       IN          AAAA        ::1

;; Query time: 0 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Wed Jun 18 15:52:31 2008
;; MSG SIZE  rcvd: 119
```

The Network

- Fake network services
  - Netcat and iptables
  - Will capture first interactions with the server. This is key to understand what is the real protocol used with the server.
  - To use netcat
    - `iptables -t nat -A PREROUTING -i eth0 -p tcp -d ! 192.168.101.2 -j DNAT --to-destination 192.168.101.2:81`
    - `nc -l –n -p 81 –o dump`

The Network services

- Disk image server
  - Partimage server
- Hosts all the original images to preserve integrity



The Network services

- Internet Access
  - DO NOT:
    - USE COPORATE INTERNET ACCESS
    - Connect your malware network to your corporate network.
  - Acquire an anonymous Internet access like a DSL link.
- Only allow infected hosts to access the Internet if necessary for the analysis.

Test machine setup

- Setup the disk partitions

First drive

  - 1 x 15GB for test environment (Windows)
  - 1 x 4GB for Linux image manager
- Second drive
  - 1 x 163GB Linux partition for snapshots and images

Test machine setup

First things to do:

- Install Linux on the 4 GB partition.
- Use a swapfile instead of a swap partition (easier to re-image)
- Install partimage
- Install Grub
  - Default to windows partition
- Take a disk image of boot sector and Linux partition

Test machine setup

- What type of images are needed?
  - Since desktop is the most likely target these days, workstation images are needed
- Pick the most common workstation configuration for your organization
  - Typically, Windows OS, Office Suite, Acrobat reader.
  - Software used in your corporation
- To understand what the malware does in YOUR environment and corporate setting your test machines should replicate that environment.

Test machine setup

- At a minimum you will need 3 images.
  - From original media plus office apps.
  - Plus SP2 applied
  - Fully patched
- Ideally, you will want several images to test malware under various conditions
  - IE6 vs IE7…

Test machine setup

- Install the OS in the same manner that you would do for your organization using common features.
  - If your workstations use AD for authentication, use the same setup. You do not need to duplicate an AD in your lab. Log in locally.
- Do a vanilla OS install

Test machine setup

- Install the OS from the original media
  - Windows XP SP1, IE6
  - Install TightVNC
- Do a snapshot (disk image)
  - Install Office
- Do another snapshot

Test machine setup

- List of images required:
  - Windows XP SP1, Office, IE6
  - Windows XP SP2, Office, IE6
  - Windows XP SP2, Office, IE7
  - Windows XP SP3, Office, IE6
  - Windows XP SP2 – Fully patched, Office, IE6
  - Windows XP SP2 – Fully patched, Office, IE7

Test machine setup

- Install all the tools in an other directory
  - Ideally on a network or an other partition that you bring up when needed
  - Copy the following Windows native commands to that directory:
    - From C:\WINDOWS\SYSTEM32
      REG.EXE, TASKLIST.EXE, SC.EXE, NETSTAT.EXE, ATTRIB.EXE
    - From C:\WINDOWS\SYSTEM32\WBEM
      WMIC
      - WMIC also requires:
        - » Framedyn.dll

Test machine setup

Install Symbol package

- These are essential to help understand what the malware does
  - They will help identify many DLL calls
- Many tools use them
  - Debuggers
  - Dissassemblers
  - SysInternals tools

http://www.microsoft.com/whdc/DevTools/Debugging/symbolpkg.mspx

Test machine setup

Open files monitor

- Enable the open files monitor in XP. This feature allows to identify files opened by processes.

```
openfiles /Local ON
```

Note: You will have to reboot you system for this command to take effect.

Analysis Tools

Live Monitoring tools

- SySAnalyzer
- RegShot

- PROCEXP.EXE
- REGMON.EXE
- FILEMON.EXE

Low footprint monitoring

- REG
- TASKLIST
- SC
- ATTRIB
- NETSTAT
- WMIC

- AUTORUNS
- PSLIST
- PSSERVICE
- FPORT
- MD5SUMS
- KDIFF3

Live Monitoring Tools

SysInternals tools

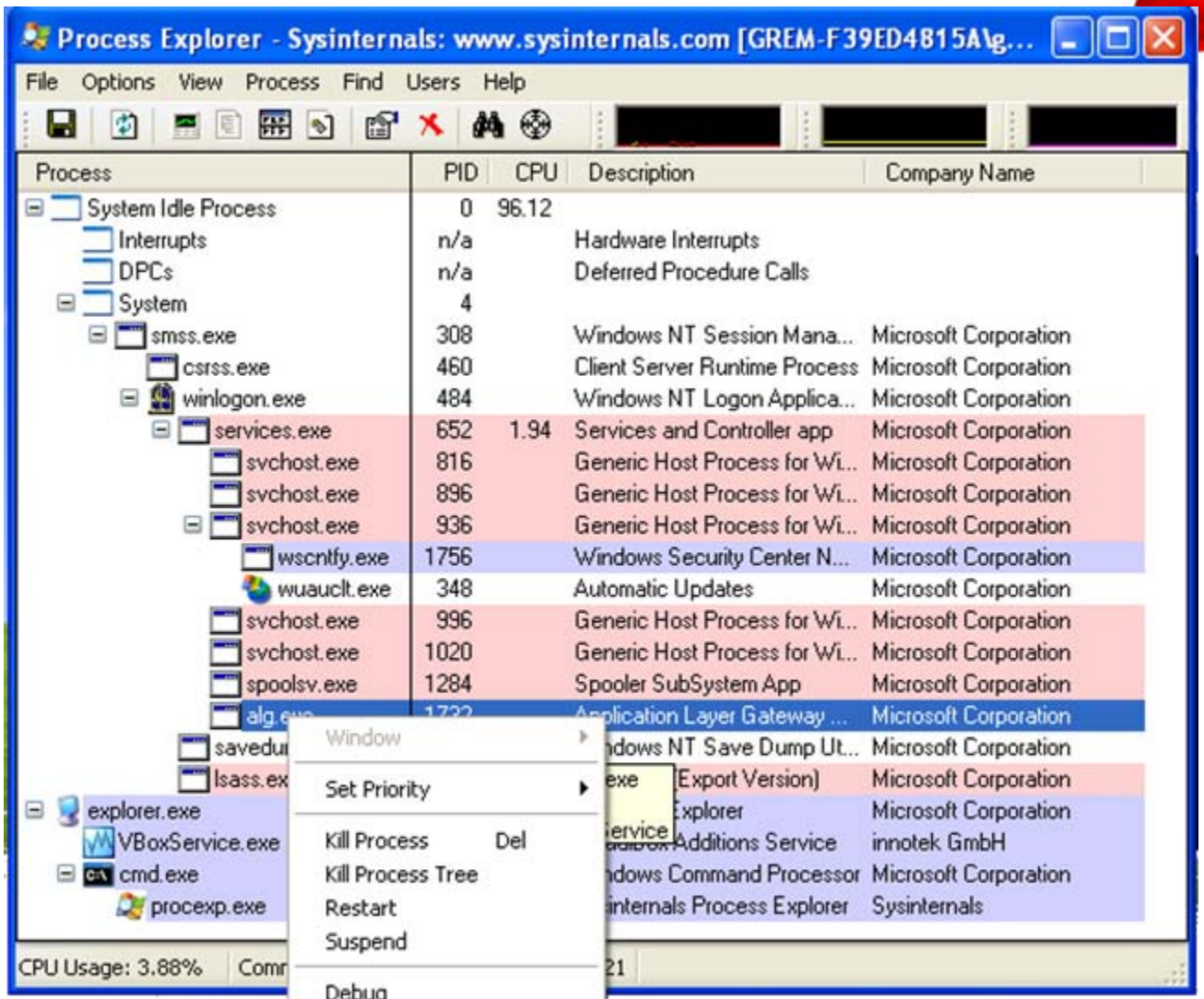
- PROCEXP.EXE
- FILEMON.EXE
- REGMON.EXE
- TCPVIEW.EXE

Other tools

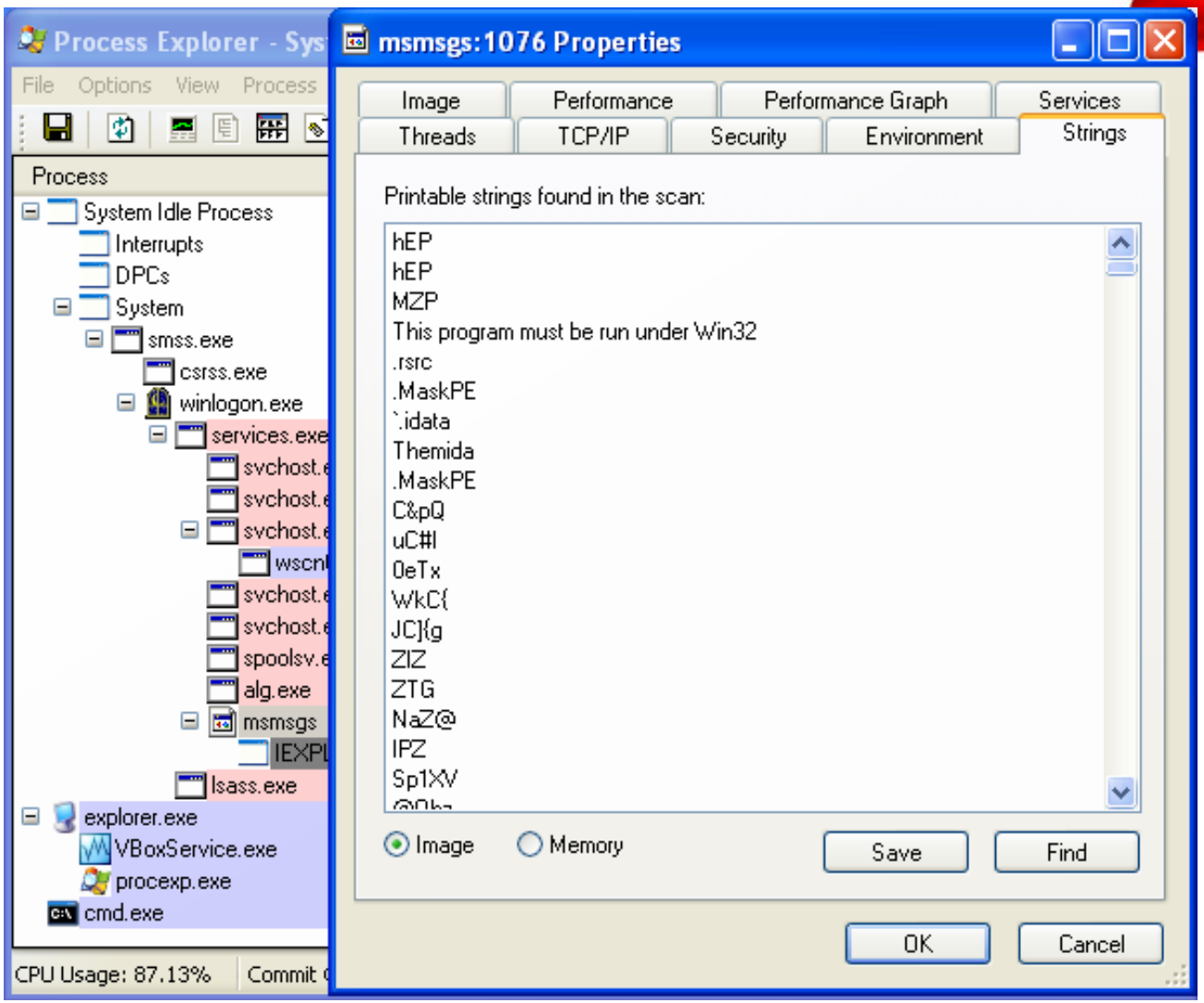
- RegShot
- SysAnalyzer

When the malware does not check for the presence of these programs, you should have the most complete picture of the malware behaviour.

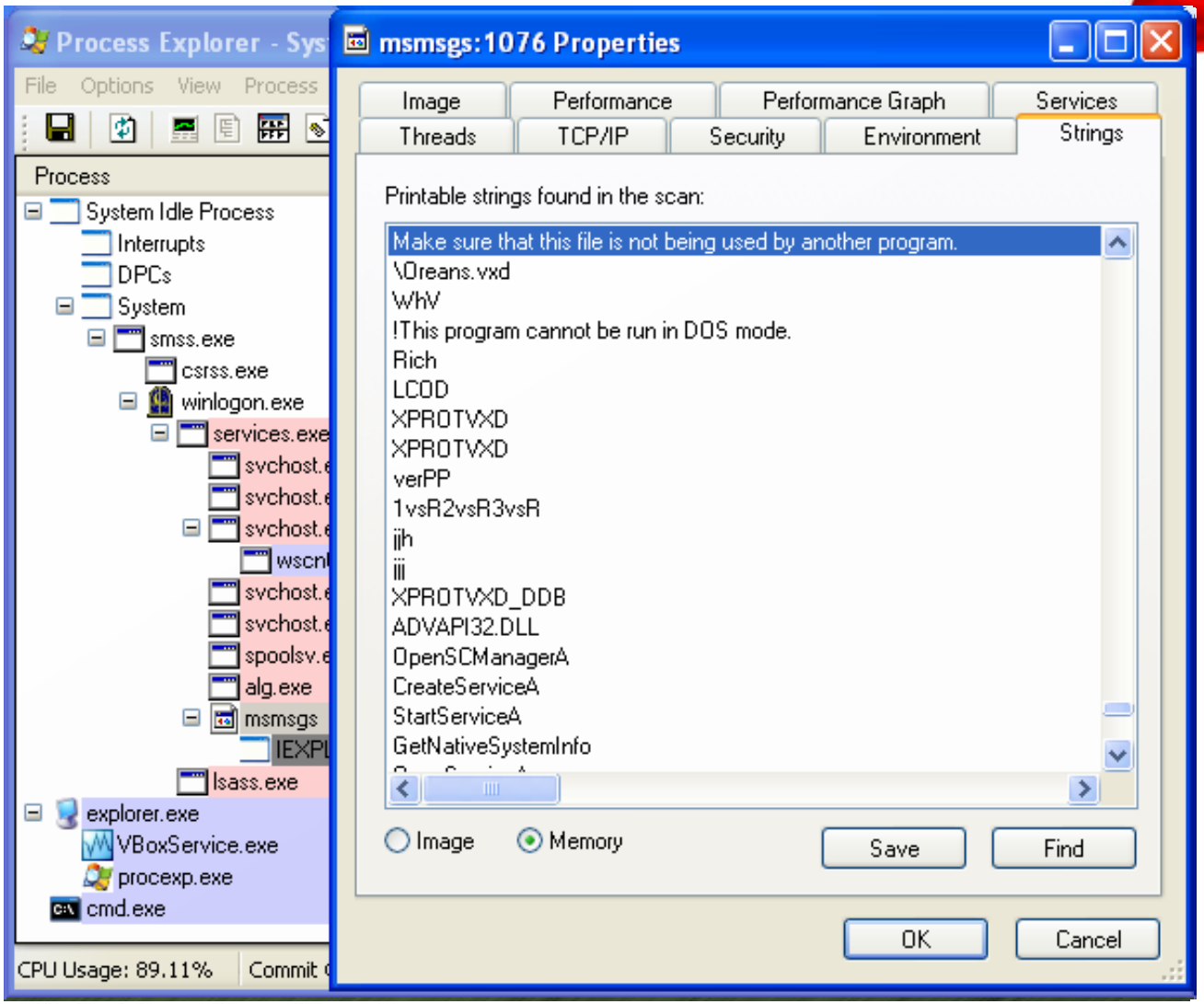
PROCEXP.EXE – Process Explorer



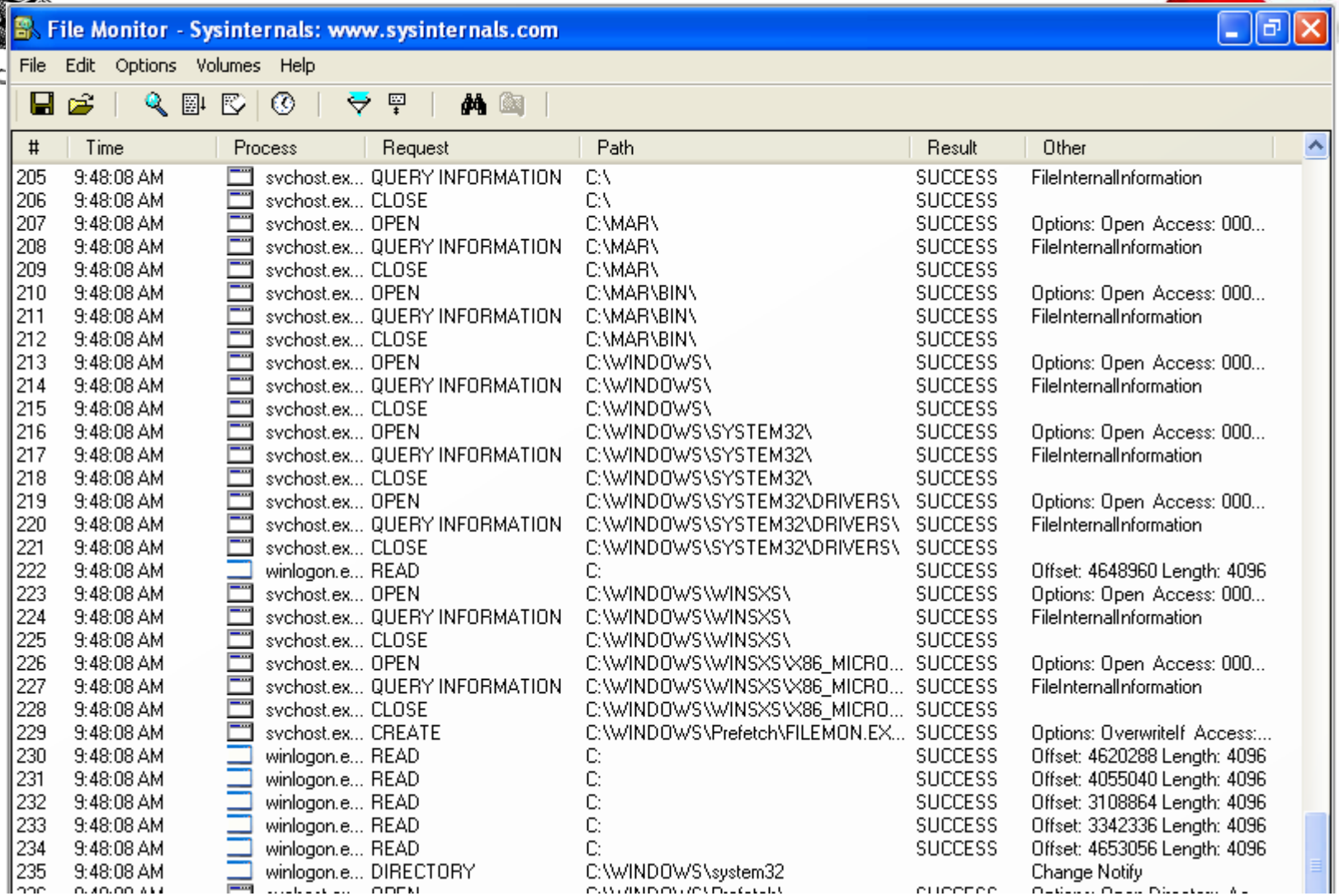
PROCEXP.EXE – Process Explorer



PROCEXP.EXE – Process Explorer

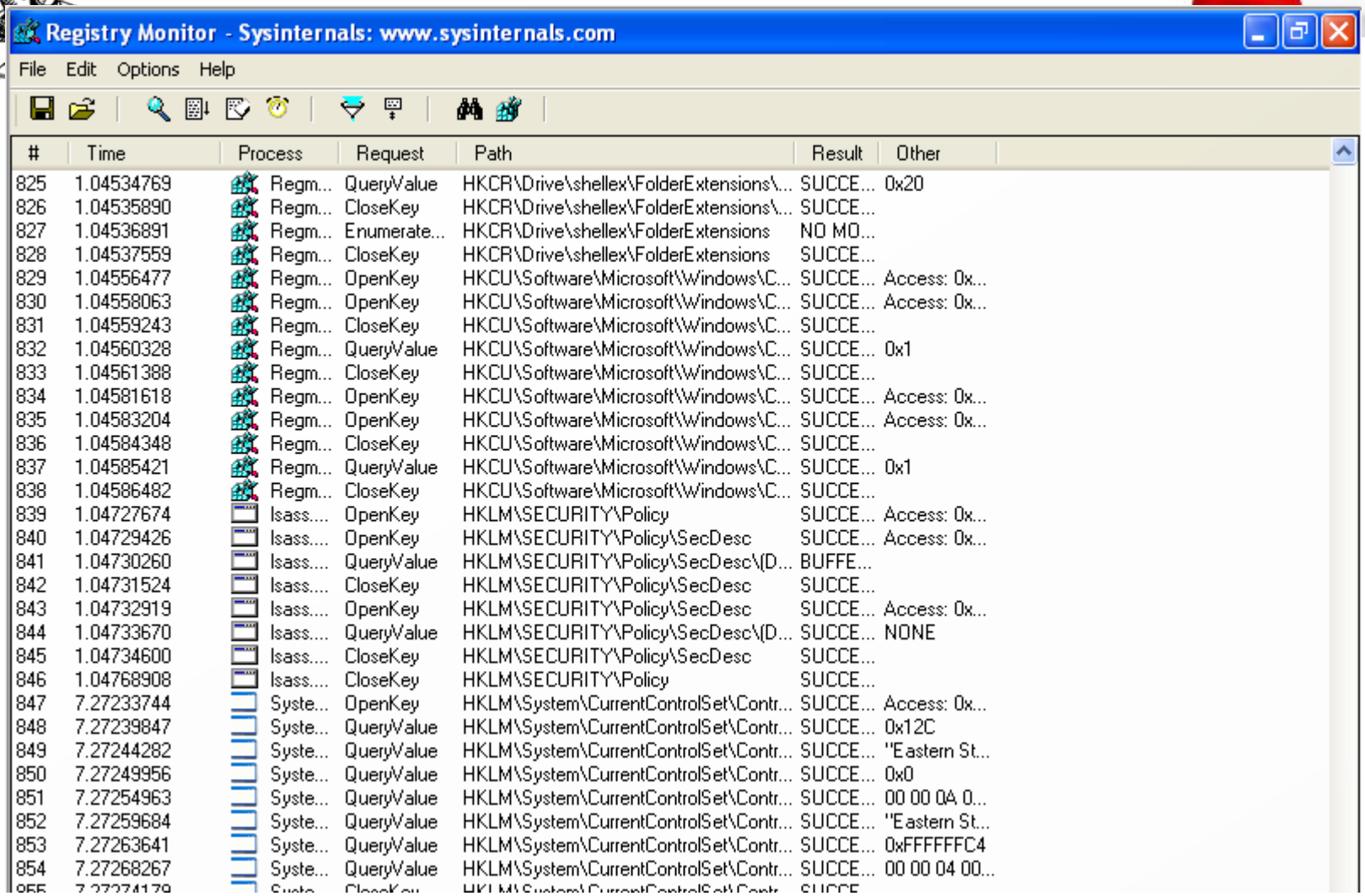


FILEMON.EXE – File Monitor



#	Time	Process	Request	Path	Result	Other
205	9:48:08 AM	svchost.ex...	QUERY INFORMATION	C:\	SUCCESS	FileInternalInformation
206	9:48:08 AM	svchost.ex...	CLOSE	C:\	SUCCESS	
207	9:48:08 AM	svchost.ex...	OPEN	C:\MAR\	SUCCESS	Options: Open Access: 000...
208	9:48:08 AM	svchost.ex...	QUERY INFORMATION	C:\MAR\	SUCCESS	FileInternalInformation
209	9:48:08 AM	svchost.ex...	CLOSE	C:\MAR\	SUCCESS	
210	9:48:08 AM	svchost.ex...	OPEN	C:\MAR\BIN\	SUCCESS	Options: Open Access: 000...
211	9:48:08 AM	svchost.ex...	QUERY INFORMATION	C:\MAR\BIN\	SUCCESS	FileInternalInformation
212	9:48:08 AM	svchost.ex...	CLOSE	C:\MAR\BIN\	SUCCESS	
213	9:48:08 AM	svchost.ex...	OPEN	C:\WINDOWS\	SUCCESS	Options: Open Access: 000...
214	9:48:08 AM	svchost.ex...	QUERY INFORMATION	C:\WINDOWS\	SUCCESS	FileInternalInformation
215	9:48:08 AM	svchost.ex...	CLOSE	C:\WINDOWS\	SUCCESS	
216	9:48:08 AM	svchost.ex...	OPEN	C:\WINDOWS\SYSTEM32\	SUCCESS	Options: Open Access: 000...
217	9:48:08 AM	svchost.ex...	QUERY INFORMATION	C:\WINDOWS\SYSTEM32\	SUCCESS	FileInternalInformation
218	9:48:08 AM	svchost.ex...	CLOSE	C:\WINDOWS\SYSTEM32\	SUCCESS	
219	9:48:08 AM	svchost.ex...	OPEN	C:\WINDOWS\SYSTEM32\DRIVERS\	SUCCESS	Options: Open Access: 000...
220	9:48:08 AM	svchost.ex...	QUERY INFORMATION	C:\WINDOWS\SYSTEM32\DRIVERS\	SUCCESS	FileInternalInformation
221	9:48:08 AM	svchost.ex...	CLOSE	C:\WINDOWS\SYSTEM32\DRIVERS\	SUCCESS	
222	9:48:08 AM	winlogon.e...	READ	C:	SUCCESS	Offset: 4648960 Length: 4096
223	9:48:08 AM	svchost.ex...	OPEN	C:\WINDOWS\WINSXS\	SUCCESS	Options: Open Access: 000...
224	9:48:08 AM	svchost.ex...	QUERY INFORMATION	C:\WINDOWS\WINSXS\	SUCCESS	FileInternalInformation
225	9:48:08 AM	svchost.ex...	CLOSE	C:\WINDOWS\WINSXS\	SUCCESS	
226	9:48:08 AM	svchost.ex...	OPEN	C:\WINDOWS\WINSXS\X86_MICRO...	SUCCESS	Options: Open Access: 000...
227	9:48:08 AM	svchost.ex...	QUERY INFORMATION	C:\WINDOWS\WINSXS\X86_MICRO...	SUCCESS	FileInternalInformation
228	9:48:08 AM	svchost.ex...	CLOSE	C:\WINDOWS\WINSXS\X86_MICRO...	SUCCESS	
229	9:48:08 AM	svchost.ex...	CREATE	C:\WINDOWS\Prefetch\FILEMON.EX...	SUCCESS	Options: OverwriteIf Access:...
230	9:48:08 AM	winlogon.e...	READ	C:	SUCCESS	Offset: 4620288 Length: 4096
231	9:48:08 AM	winlogon.e...	READ	C:	SUCCESS	Offset: 4055040 Length: 4096
232	9:48:08 AM	winlogon.e...	READ	C:	SUCCESS	Offset: 3108864 Length: 4096
233	9:48:08 AM	winlogon.e...	READ	C:	SUCCESS	Offset: 3342336 Length: 4096
234	9:48:08 AM	winlogon.e...	READ	C:	SUCCESS	Offset: 4653056 Length: 4096
235	9:48:08 AM	winlogon.e...	DIRECTORY	C:\WINDOWS\system32		Change Notify

REGMON.EXE – Registry Monitor



#	Time	Process	Request	Path	Result	Other
825	1.04534769	Regm...	QueryValue	HKCR\Drive\shellex\FolderExtensions\...	SUCCE...	0x20
826	1.04535890	Regm...	CloseKey	HKCR\Drive\shellex\FolderExtensions\...	SUCCE...	
827	1.04536891	Regm...	Enumerate...	HKCR\Drive\shellex\FolderExtensions	NO MO...	
828	1.04537559	Regm...	CloseKey	HKCR\Drive\shellex\FolderExtensions	SUCCE...	
829	1.04556477	Regm...	OpenKey	HKCU\Software\Microsoft\Windows\C...	SUCCE...	Access: 0x...
830	1.04558063	Regm...	OpenKey	HKCU\Software\Microsoft\Windows\C...	SUCCE...	Access: 0x...
831	1.04559243	Regm...	CloseKey	HKCU\Software\Microsoft\Windows\C...	SUCCE...	
832	1.04560328	Regm...	QueryValue	HKCU\Software\Microsoft\Windows\C...	SUCCE...	0x1
833	1.04561388	Regm...	CloseKey	HKCU\Software\Microsoft\Windows\C...	SUCCE...	
834	1.04581618	Regm...	OpenKey	HKCU\Software\Microsoft\Windows\C...	SUCCE...	Access: 0x...
835	1.04583204	Regm...	OpenKey	HKCU\Software\Microsoft\Windows\C...	SUCCE...	Access: 0x...
836	1.04584348	Regm...	CloseKey	HKCU\Software\Microsoft\Windows\C...	SUCCE...	
837	1.04585421	Regm...	QueryValue	HKCU\Software\Microsoft\Windows\C...	SUCCE...	0x1
838	1.04586482	Regm...	CloseKey	HKCU\Software\Microsoft\Windows\C...	SUCCE...	
839	1.04727674	lsass....	OpenKey	HKLM\SECURITY\Policy	SUCCE...	Access: 0x...
840	1.04729426	lsass....	OpenKey	HKLM\SECURITY\Policy\SecDesc	SUCCE...	Access: 0x...
841	1.04730260	lsass....	QueryValue	HKLM\SECURITY\Policy\SecDesc\(D...	BUFFE...	
842	1.04731524	lsass....	CloseKey	HKLM\SECURITY\Policy\SecDesc	SUCCE...	
843	1.04732919	lsass....	OpenKey	HKLM\SECURITY\Policy\SecDesc	SUCCE...	Access: 0x...
844	1.04733670	lsass....	QueryValue	HKLM\SECURITY\Policy\SecDesc\(D...	SUCCE...	NONE
845	1.04734600	lsass....	CloseKey	HKLM\SECURITY\Policy\SecDesc	SUCCE...	
846	1.04768908	lsass....	CloseKey	HKLM\SECURITY\Policy	SUCCE...	
847	7.27233744	Syste...	OpenKey	HKLM\System\CurrentControlSet\Contr...	SUCCE...	Access: 0x...
848	7.27239847	Syste...	QueryValue	HKLM\System\CurrentControlSet\Contr...	SUCCE...	0x12C
849	7.27244282	Syste...	QueryValue	HKLM\System\CurrentControlSet\Contr...	SUCCE...	"Eastern St...
850	7.27249956	Syste...	QueryValue	HKLM\System\CurrentControlSet\Contr...	SUCCE...	0x0
851	7.27254963	Syste...	QueryValue	HKLM\System\CurrentControlSet\Contr...	SUCCE...	00 00 0A 0...
852	7.27259684	Syste...	QueryValue	HKLM\System\CurrentControlSet\Contr...	SUCCE...	"Eastern St...
853	7.27263641	Syste...	QueryValue	HKLM\System\CurrentControlSet\Contr...	SUCCE...	0xFFFFFFC4
854	7.27268267	Syste...	QueryValue	HKLM\System\CurrentControlSet\Contr...	SUCCE...	00 00 04 00...

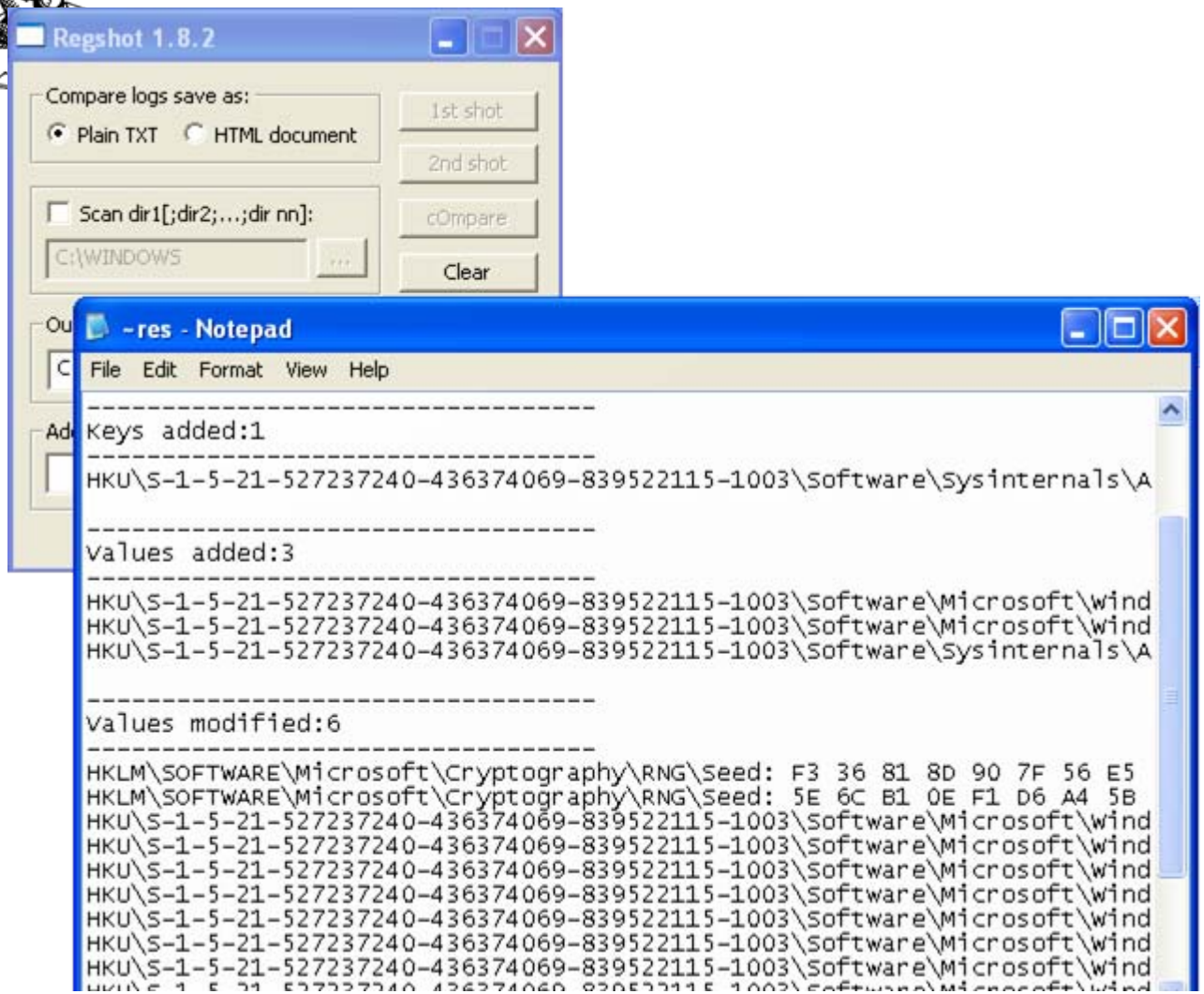
TCPVIEW.EXE – TCP connections

TCPView - Sysinternals: www.sysinternals.com

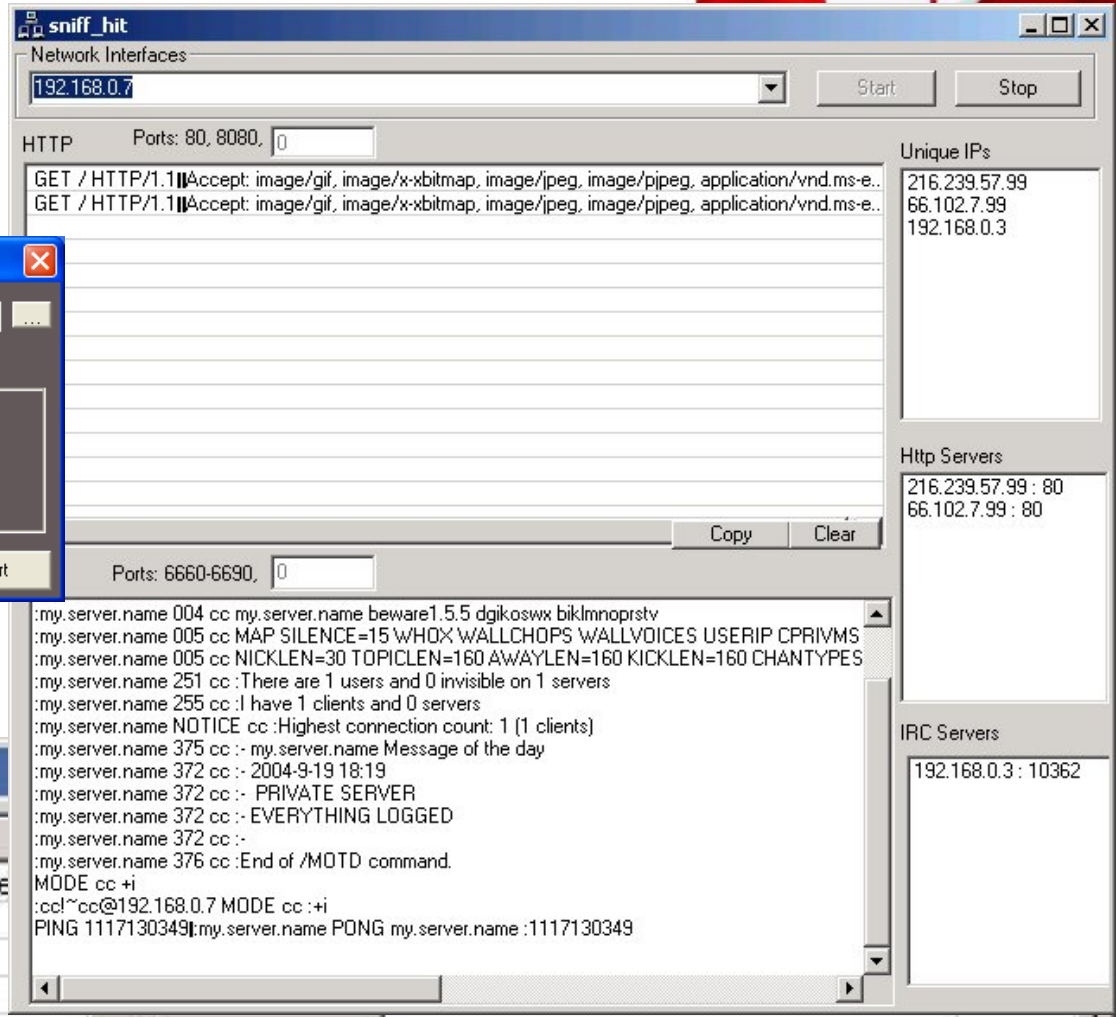
File Options Process View Help

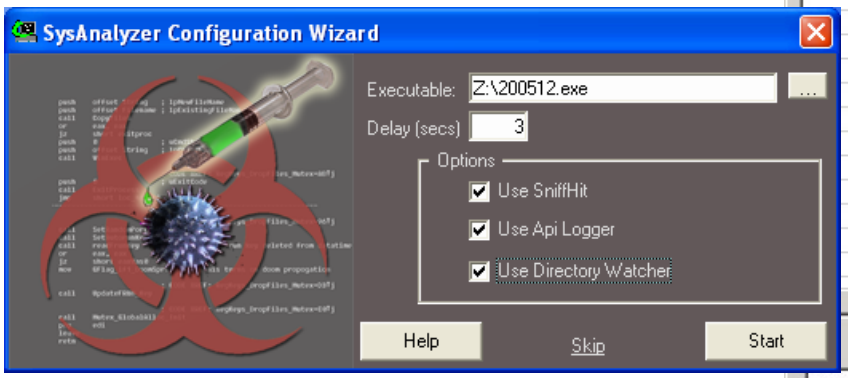
Process	Protocol	Local Address	Remote Address	State
alg.exe:1828	TCP	127.0.0.1:1025	0.0.0.0:0	LISTENING
lsass.exe:668	UDP	0.0.0.0:500	*:*	
lsass.exe:668	UDP	0.0.0.0:4500	*:*	
svchost.exe:1096	UDP	10.0.2.15:1900	*:*	
svchost.exe:1096	UDP	127.0.0.1:1900	*:*	
svchost.exe:892	TCP	0.0.0.0:135	0.0.0.0:0	LISTENING
svchost.exe:928	UDP	10.0.2.15:123	*:*	
svchost.exe:928	UDP	127.0.0.1:123	*:*	
svchost.exe:928	UDP	127.0.0.1:1043	*:*	
svchost.exe:980	UDP	0.0.0.0:1036	*:*	
svchost.exe:980	UDP	0.0.0.0:1042	*:*	
System:4	TCP	0.0.0.0:445	0.0.0.0:0	LISTENING
System:4	TCP	10.0.2.15:139	0.0.0.0:0	LISTENING
System:4	UDP	0.0.0.0:445	*:*	
System:4	UDP	10.0.2.15:138	*:*	
System:4	UDP	10.0.2.15:137	*:*	

RegShot -


Regshot 1.8.2
Compare logs save as:
Plain TXT
HTML document
1st shot
2nd shot
cOmpare
Clear
Scan dir1[;dir2;...;dir nn]:
C:\WINDOWS
-res - Notepad
File Edit Format View Help
Keys added:1
HKU\S-1-5-21-527237240-436374069-839522115-1003\Software\Sysinternals\A
Values added:3
HKU\S-1-5-21-527237240-436374069-839522115-1003\Software\Microsoft\Wind
HKU\S-1-5-21-527237240-436374069-839522115-1003\Software\Microsoft\Wind
HKU\S-1-5-21-527237240-436374069-839522115-1003\Software\Sysinternals\A
Values modified:6
HKLM\SOFTWARE\Microsoft\Cryptography\RNG\Seed: F3 36 81 8D 90 7F 56 E5
HKLM\SOFTWARE\Microsoft\Cryptography\RNG\Seed: 5E 6C B1 0E F1 D6 A4 5B
HKU\S-1-5-21-527237240-436374069-839522115-1003\Software\Microsoft\Wind
HKU\S-1-5-21-527237240-436374069-839522115-1003\Software\Microsoft\Wind
HKU\S-1-5-21-527237240-436374069-839522115-1003\Software\Microsoft\Wind
HKU\S-1-5-21-527237240-436374069-839522115-1003\Software\Microsoft\Wind
HKU\S-1-5-21-527237240-436374069-839522115-1003\Software\Microsoft\Wind
HKU\S-1-5-21-527237240-436374069-839522115-1003\Software\Microsoft\Wind
HKU\S-1-5-21-527237240-436374069-839522115-1003\Software\Microsoft\Wind

SysAnalyzer - iDEFENSE





Low footprint monitoring

Registry tools
- REG.EXE
- AUTORUNS.EXE

Network
- NETSTAT.EXE
- FPORT.EXE

Processes and services
- TASKLIST.EXE
- SC.EXE
- PSLIST.EXE
- PSSERVICE.EXE
- WMIC

FILE system
- ATTRIB.EXE
- MD5DEEP.EXE

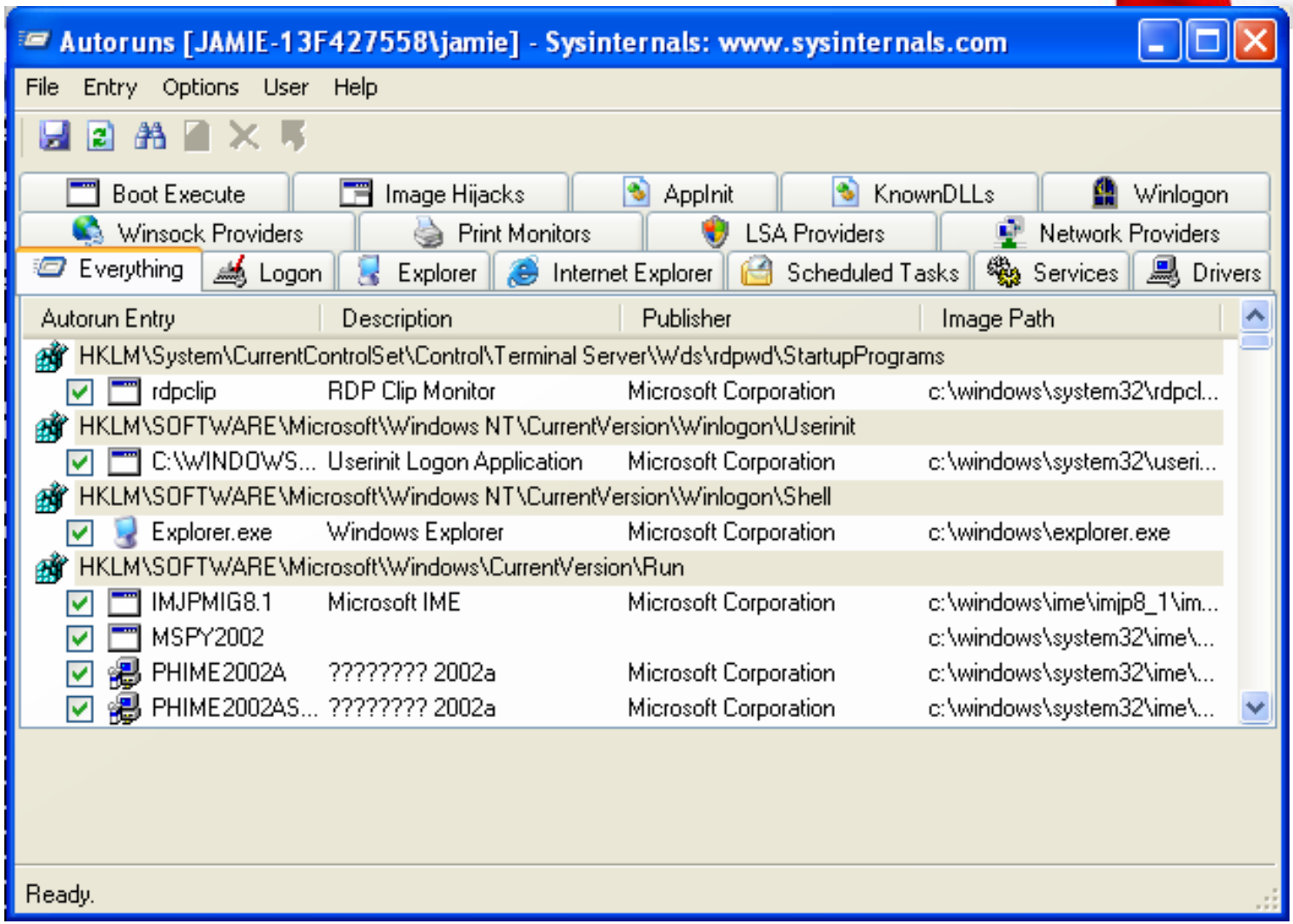
Using these tools we can take a snapshot of the system state before and after having run the malware. These snapshots can be saved to files and compared to identify changes made by the malware.

REG.EXE – Console Registry Tool for Windows

Command Prompt

```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\>reg export hklm hklm.txt

The operation completed successfully

C:\>type hklm.txt | more
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE]

[HKEY_LOCAL_MACHINE\HARDWARE]

[HKEY_LOCAL_MACHINE\HARDWARE\ACPI]

[HKEY_LOCAL_MACHINE\HARDWARE\ACPI\DSDT]

[HKEY_LOCAL_MACHINE\HARDWARE\ACPI\DSDT\VBOX__]

[HKEY_LOCAL_MACHINE\HARDWARE\ACPI\DSDT\VBOX__\VBOXBIOS]

[HKEY_LOCAL_MACHINE\HARDWARE\ACPI\DSDT\VBOX__\VBOXBIOS\00000002]
"00000000"=hex:44,53,44,54,3f,10,00,00,01,aa,56,42,4f,58,20,20,56,42,4f,58,42,\
  49,4f,53,02,00,00,00,49,4e,54,4c,09,03,05,20,5b,80,44,42,47,30,01,0b,00,30,\
  0a,04,5b,81,0b,44,42,47,30,01,44,48,45,31,08,5b,81,0b,44,42,47,30,02,44,48,\
  45,32,10,5b,81,0b,44,42,47,30,03,44,48,45,34,20,5b,81,0d,44,42,47,30,01,00,\
```

AUTORUNS.EXE



TASKLIST.EXE – Windows Processes and services

Command Prompt

```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\>tasklist

Image Name                     PID Session Name     Session#    Mem Usage
========================= ====== ================ ======== ============
System Idle Process              0 Console                0         16 K
System                           4 Console                0        212 K
smss.exe                       548 Console                0        372 K
csrss.exe                      596 Console                0      4,128 K
winlogon.exe                   620 Console                0      4,064 K
services.exe                   664 Console                0      3,896 K
lsass.exe                      676 Console                0      1,320 K
svchost.exe                    824 Console                0      4,532 K
svchost.exe                    904 Console                0      3,980 K
svchost.exe                    940 Console                0     16,964 K
svchost.exe                    984 Console                0      2,776 K
svchost.exe                   1044 Console                0      4,316 K
spoolsv.exe                   1296 Console                0      4,356 K
alg.exe                       1740 Console                0      3,316 K
explorer.exe                  1860 Console                0     14,980 K
VBoxService.exe               1916 Console                0      2,248 K
wscntfy.exe                   2004 Console                0      2,124 K
cmd.exe                        444 Console                0      2,464 K
tasklist.exe                   380 Console                0      4,152 K
wmiprvse.exe                  1960 Console                0      5,436 K

C:\>_
```

SC.EXE – Service Control command line utility

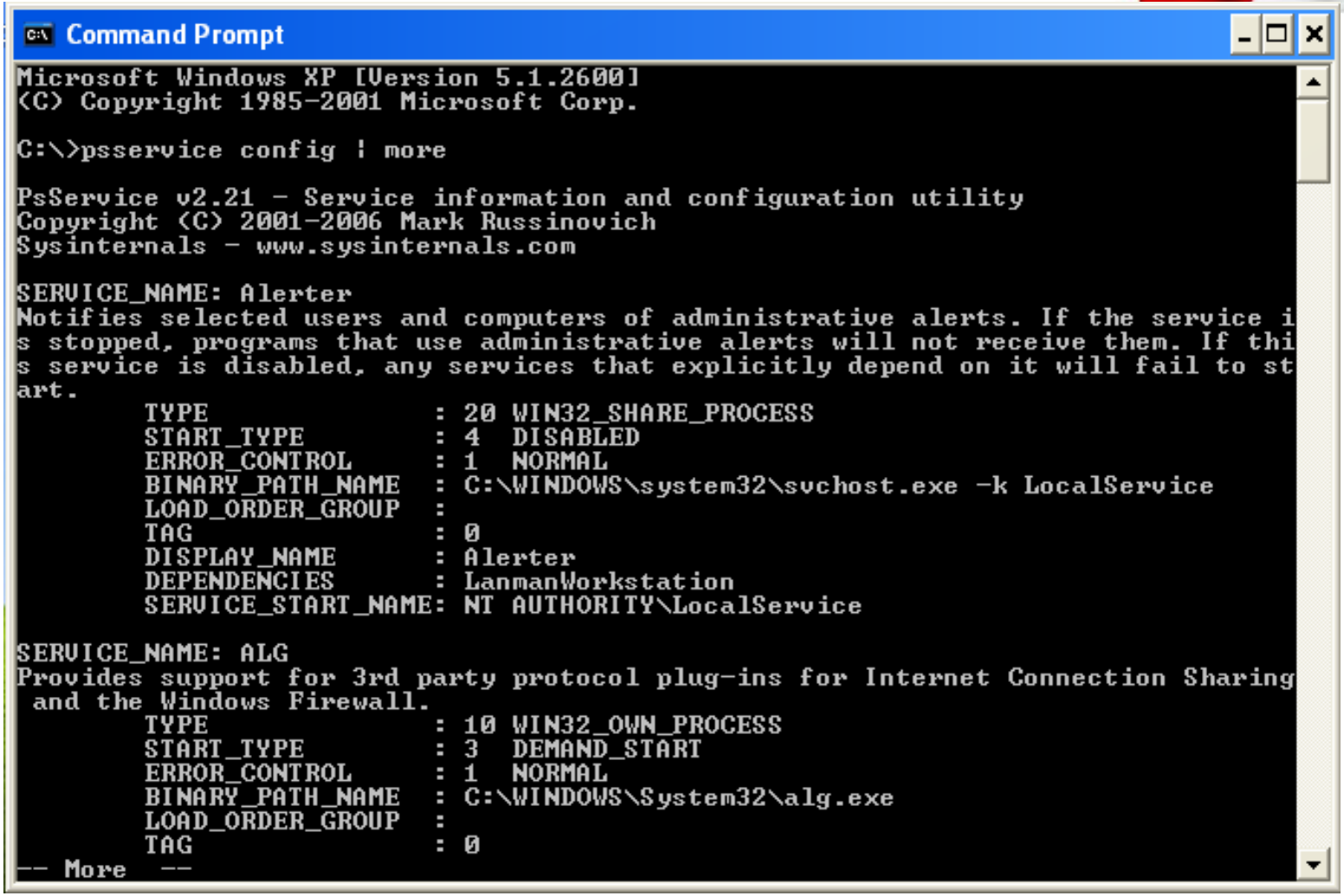
```
Command Prompt
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\>sc queryex RemoteRegistry

SERVICE_NAME: RemoteRegistry
        TYPE               : 20  WIN32_SHARE_PROCESS
        STATE              : 4  RUNNING
                                (STOPPABLE,NOT_PAUSABLE,IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x0
        PID                : 1044
        FLAGS              :

C:\>_
```

PSLIST.EXE – SysInternals

Command Prompt

```
C:\>pslist -t

pslist v1.28 - Sysinternals PsList
Copyright © 2000-2004 Mark Russinovich
Sysinternals

Process information for JAMIE-13F427558:

Name                                Pid Pri Thd  Hnd      VM      WS    Priv
Idle                                  0   0   1    0       0      16       0
  System                              4   8  54  149    1876     212       0
    smss                            548  11   3   21    3800     372     164
      csrss                         596  13  12  304   26392    4120    1968
      winlogon                      620  13  17  549   54948    4064    7536
        services                    664   9  15  250   33424    3908    1912
          svchost                   824   8  17  194   61836    4548    3032
            wmiprvse               1092   8   7  145   40572    5516    2436
          svchost                   904   8   9  230   35580    3980    1708
          svchost                   940   8  51 1061  108588   16740   11172
            wscntfy                2004   8   1   30   27644    2124     600
          svchost                   984   8   4   55   28640    2776    1168
          svchost                  1044   8  13  196   38376    4316    1768
          spoolsv                  1296   8  10  119   41236    4356    3036
          alg                      1740   8   5   98   32424    3316    1120
        lsass                       676   9  19  336   40944    1376    3668
explorer                           1860   8   9  316   63960   16944    8636
  cmd                              1516   8   1   31   30180    2484    2004
    pslist                         1820  13   2   74   30108    2344    1032
  VBoxService                      1916   8   4   30   31068    2248     768

C:\>
```

PSERVICE.EXE - SysInternals



WMIC - Windows Management Instrumentation Command

This is the Swiss Army knife on steroids…

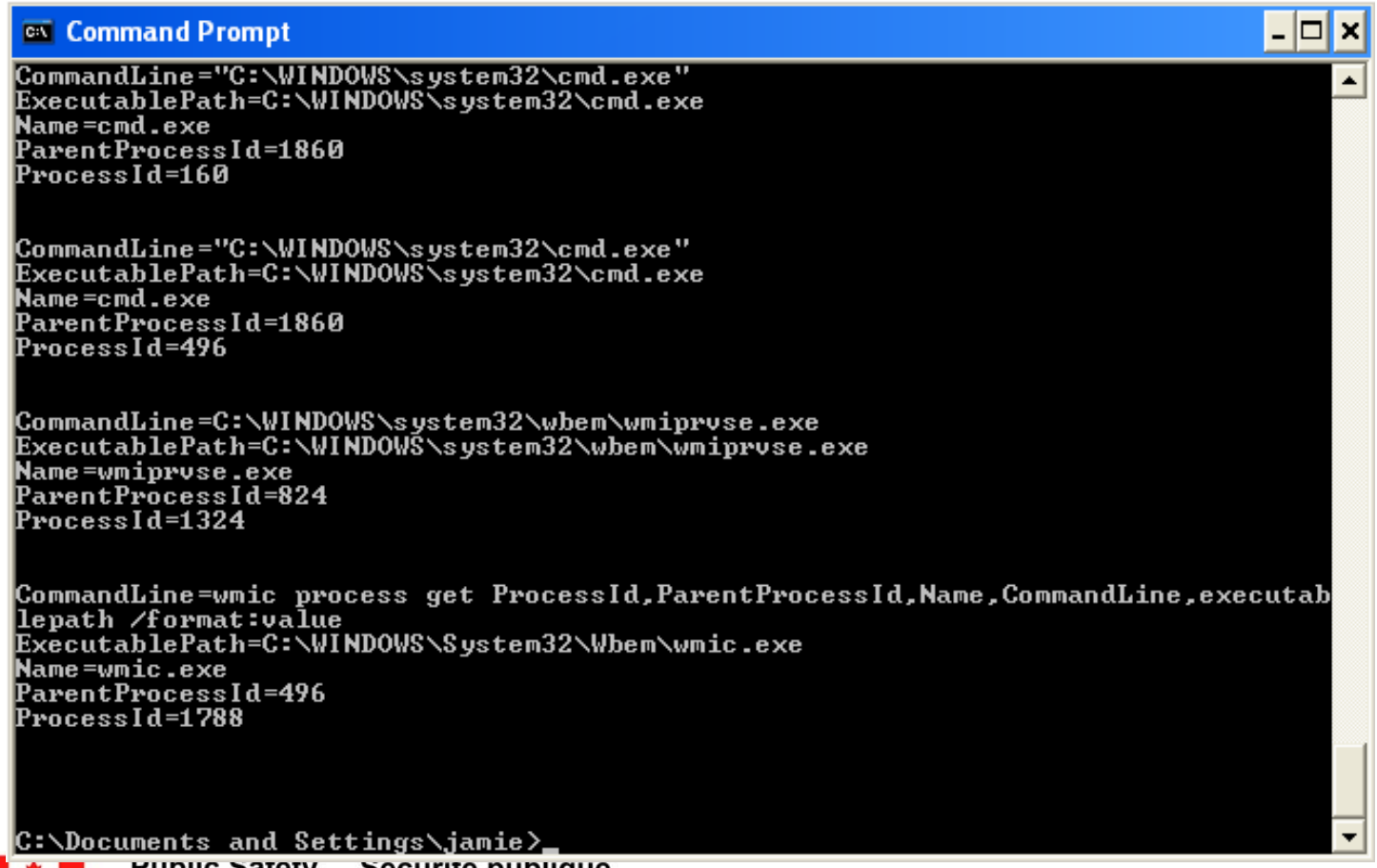
It can:

- Query or change almost any system setting locally or remotely
- Output the results in various format: CSV, XML, TABLE and HTML
- Display all properties or only those specified
- Output can be easily piped to another command or redirected to a file
- Easily scriptable

WMIC - Windows Management Instrumentation Command

List processes with command line switches, executable path, Name, Process ID and Parent PID:

```
wmic process get ProcessId,ParentProcessId,Name,ExecutablePath,CommandLine /format:value
```



NETSTAT.EXE – TCP/IP network connections and statistics

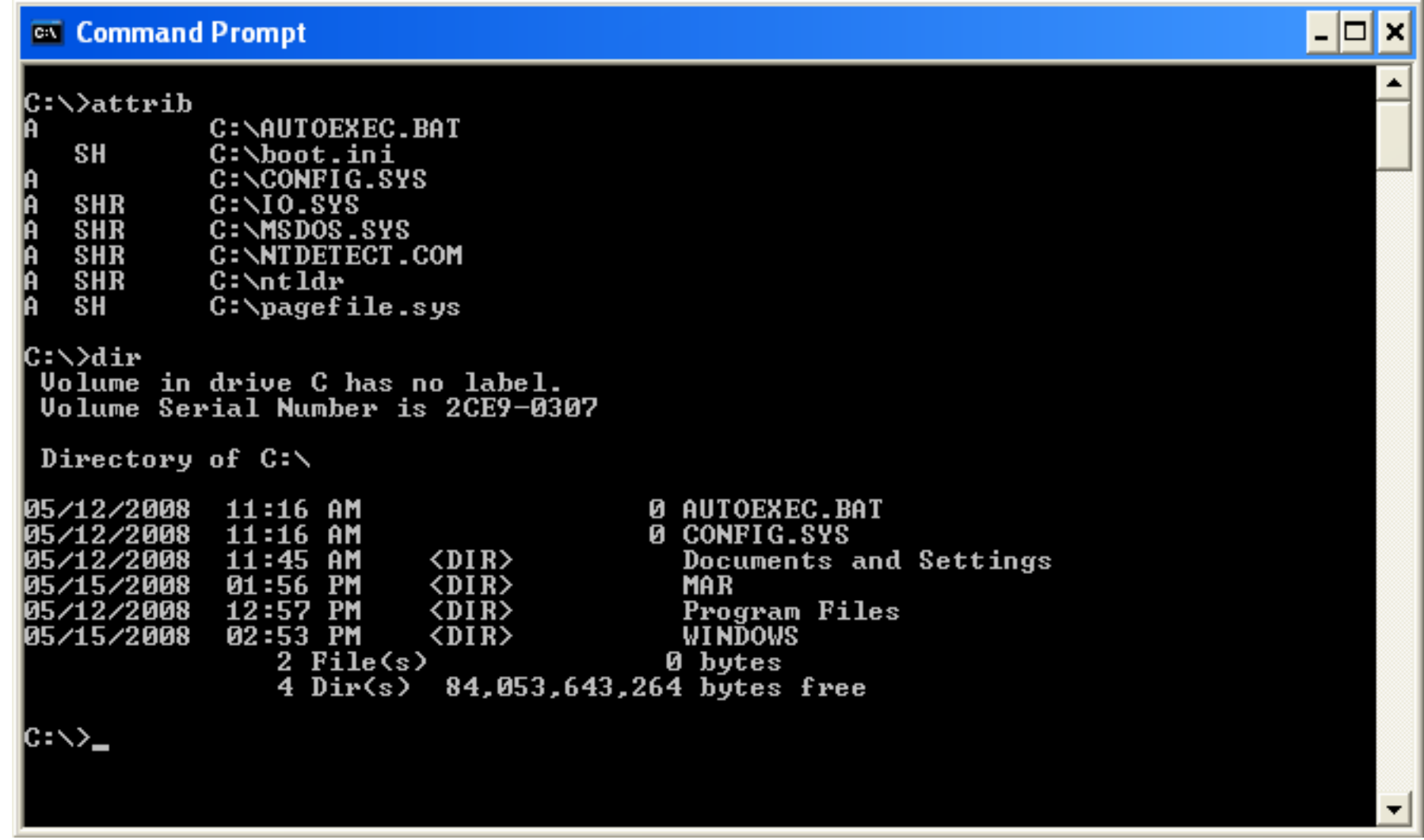
Command Prompt

```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\>netstat -an

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    127.0.0.1:1025         0.0.0.0:0              LISTENING
  UDP    0.0.0.0:445            *:*
  UDP    0.0.0.0:500            *:*
  UDP    0.0.0.0:4500           *:*
  UDP    127.0.0.1:123          *:*
  UDP    127.0.0.1:1900         *:*

C:\>_
```

FPORT.EXE – from Foundstone

```
Command Prompt
Copyright 2000 by Foundstone, Inc.
http://www.foundstone.com

Pid   Process            Port  Proto Path
648   servterm       ->  23    TCP   Z:\software\windows-based\servt-10\servterm
.exe
892                  ->  135   TCP
4     System         ->  139   TCP
4     System         ->  445   TCP
1828                 ->  1025  TCP

0     System         ->  123   UDP
0     System         ->  137   UDP
0     System         ->  138   UDP
648   servterm       ->  445   UDP   Z:\software\windows-based\servt-10\servterm
.exe
892                  ->  500   UDP
4     System         ->  1036  UDP
4     System         ->  1042  UDP
0     System         ->  1043  UDP
0     System         ->  1900  UDP
1828                 ->  4500  UDP


C:\>_
```

ATTRIB.EXE – File Attributes



MD5DEEP.EXE – Integrity checker

Command Prompt

```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\>md5sums .

MD5sums 1.2 freeware for Win9x/ME/NT/2000/XP+
Copyright (C) 2001-2005 Jem Berkes - http://www.pc-tools.net/
Type md5sums -h for help

[Path] / filename                                    MD5 sum
-----------------------------------------------------------------------------
[C:\]
AUTOEXEC.BAT                                         d41d8cd98f00b204e9800998ecf8427e
boot.ini                                             fa579938b0733b87066546afe951082c
CONFIG.SYS                                           d41d8cd98f00b204e9800998ecf8427e
hklm.txt                                             593d59056d827779fc05ac7d25a560bb
IO.SYS                                               d41d8cd98f00b204e9800998ecf8427e
MSDOS.SYS                                            d41d8cd98f00b204e9800998ecf8427e
NTDETECT.COM                                         b2de3452de03674c6cec68b8c8ce7c78
ntldr                                                9ec920f4179d45af3a6638a083d39c85
pagefile.sys                                        Unable to open!

C:\>
```

Snapshot utility

- Take a snapshot of several parts on the host
  - Registry
  - File System
  - Networking
  - Processes
- Stores the snapshots in several text files for easy comparison

Snapshot utility

Command Prompt

```
T:\>cd ss

T:\SS>dir
 Volume in drive T is VBOX_files
 Volume Serial Number is 0000-0807

 Directory of T:\SS

06/23/2008  07:30 AM    <DIR>          SS-20080623-072351.71
06/23/2008  07:15 AM    <DIR>          SS-20080623-070953.82
               0 File(s)              8,192 bytes
               2 Dir(s)   6,246,199,296 bytes free

T:\SS>cd SS-20080623-072351.71

T:\SS\SS-20080623-072351.71>dir
 Volume in drive T is VBOX_files
 Volume Serial Number is 0000-0807

 Directory of T:\SS\SS-20080623-072351.71

06/23/2008  07:30 AM                12 PSSERVICE.txt
06/23/2008  07:29 AM            30,450 TASKLIST.txt
06/23/2008  07:30 AM            33,935 SC.txt
06/23/2008  07:30 AM           599,926 ATTRIB.txt
06/23/2008  07:30 AM                12 FPORT.txt
06/23/2008  07:29 AM               765 ROUTE.txt
06/23/2008  07:29 AM               583 NETSTAT.txt
06/23/2008  07:30 AM                17 MD5DEEP.txt
06/23/2008  07:30 AM                12 PSLIST.txt
06/23/2008  07:29 AM        14,145,662 REG.txt
              10 File(s)     14,811,374 bytes
               0 Dir(s)   6,243,045,376 bytes free

T:\SS\SS-20080623-072351.71>
```

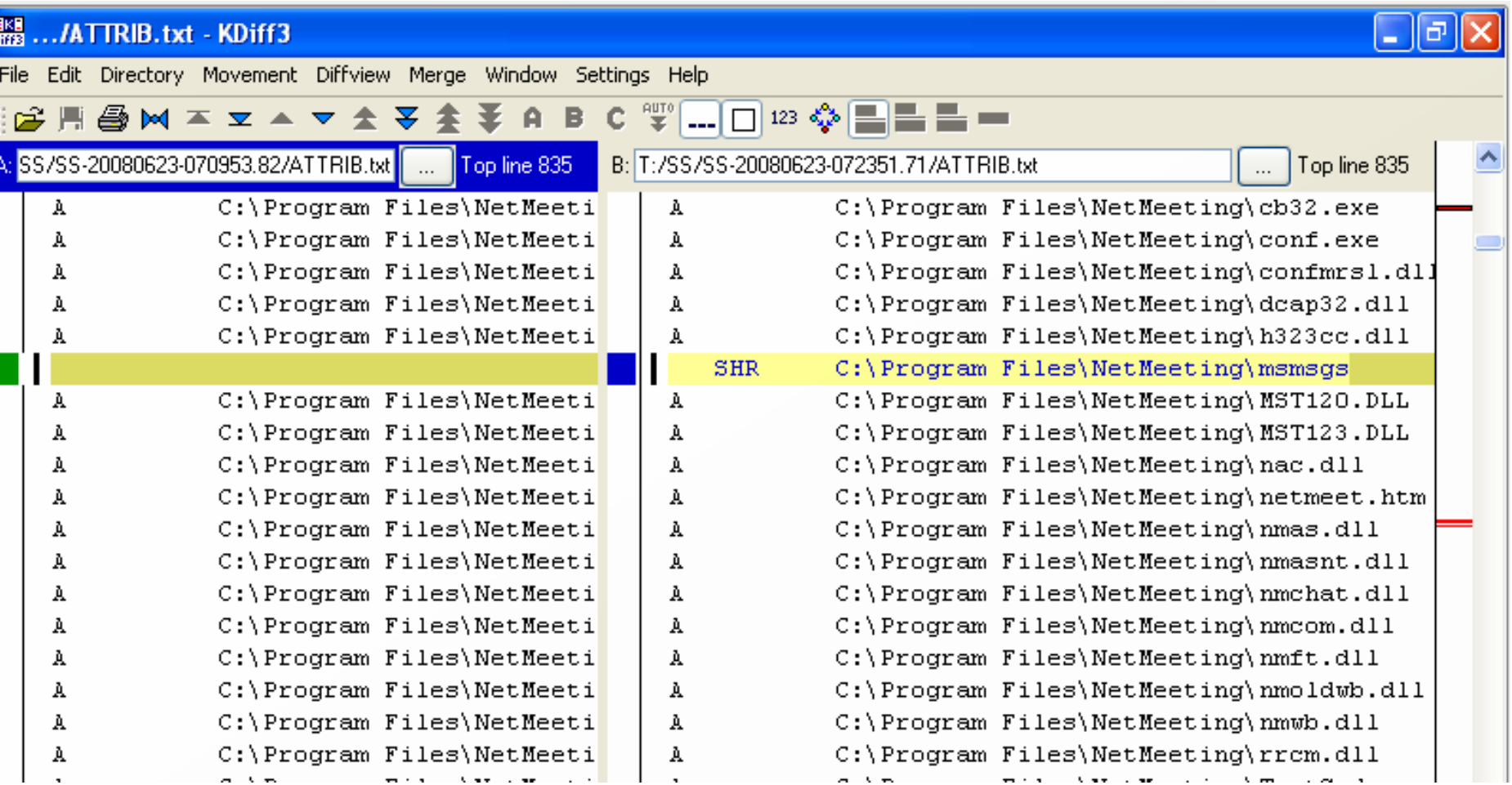
FC – File Comparison Tool

Command Prompt

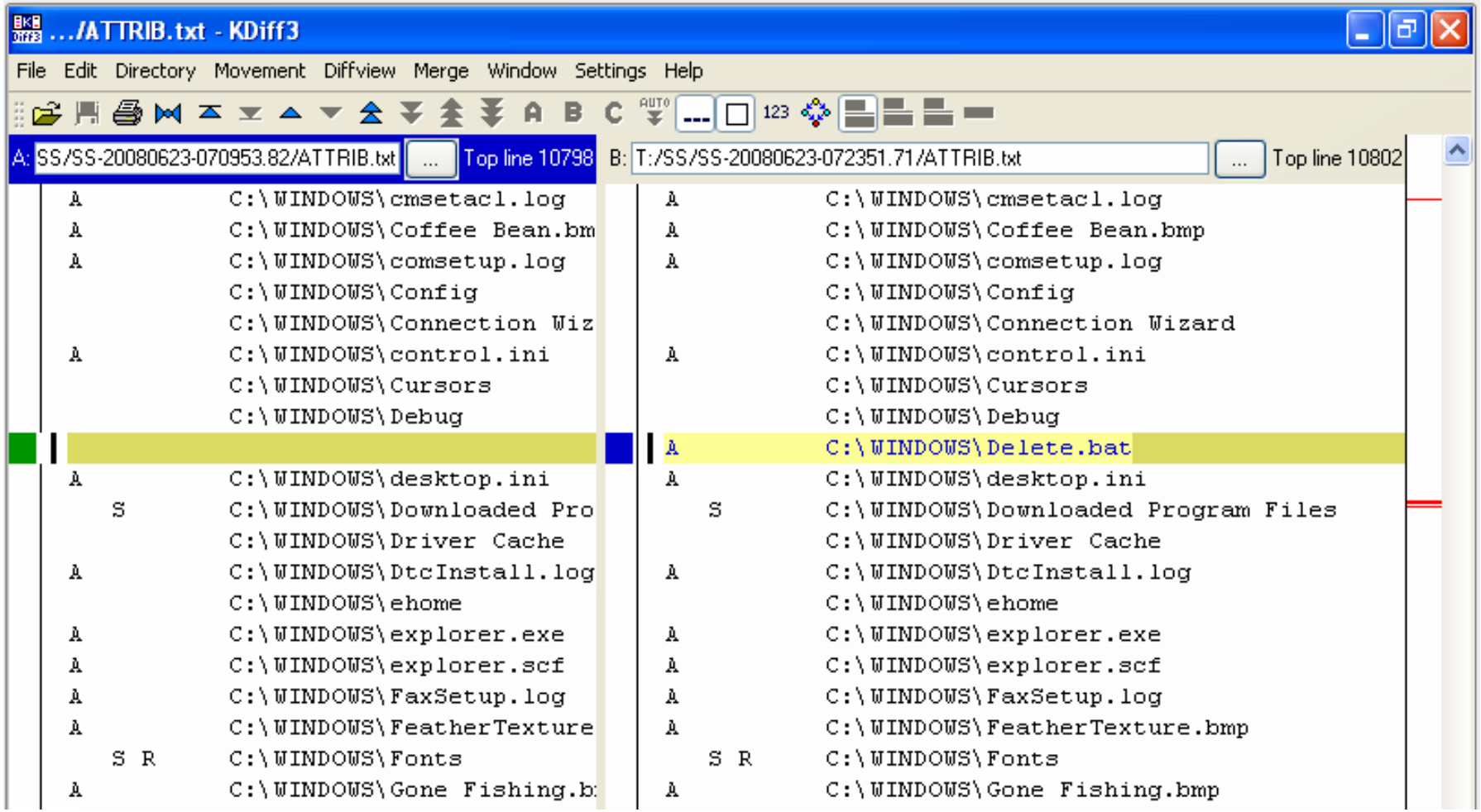
```
T:\SS\SS-20080623-072351.71>fc /L /N ATTRIB.txt ..\SS-20080623-070953.82\ATTRIB.
txt
Comparing files ATTRIB.txt and ..\SS-20080623-070953.82\ATTRIB.TXT
***** ATTRIB.txt
  848:  A           C:\Program Files\NetMeeting\h323cc.dll
  849:      SHR     C:\Program Files\NetMeeting\msmsgs
  850:  A           C:\Program Files\NetMeeting\MST120.DLL
***** ..\SS-20080623-070953.82\ATTRIB.TXT
  848:  A           C:\Program Files\NetMeeting\h323cc.dll
  849:  A           C:\Program Files\NetMeeting\MST120.DLL
*****

***** ATTRIB.txt
 4814:  A           C:\WINDOWS\PeerNet\sqlse20.dll
 4815:  A           C:\WINDOWS\Prefetch\200512.EXE-17CE5174.pf
 4816:  A           C:\WINDOWS\Prefetch\AGENTSVR.EXE-002E45AB.pf
***** ..\SS-20080623-070953.82\ATTRIB.TXT
 4813:  A           C:\WINDOWS\PeerNet\sqlse20.dll
 4814:  A           C:\WINDOWS\Prefetch\AGENTSVR.EXE-002E45AB.pf
*****

***** ATTRIB.txt
 4841:  A           C:\WINDOWS\Prefetch\MSIEXEC.EXE-2F8A8CAE.pf
 4842:  A           C:\WINDOWS\Prefetch\MSMSGS-013FAF85.pf
 4843:  A           C:\WINDOWS\Prefetch\MSOOBE.EXE-30411B02.pf
***** ..\SS-20080623-070953.82\ATTRIB.TXT
 4839:  A           C:\WINDOWS\Prefetch\MSIEXEC.EXE-2F8A8CAE.pf
 4840:  A           C:\WINDOWS\Prefetch\MSOOBE.EXE-30411B02.pf
*****

***** ATTRIB.txt
 4880:  A           C:\WINDOWS\Prefetch\TASKLIST.EXE-10D94B23.pf
 4881:  A           C:\WINDOWS\Prefetch\TASKMGR.EXE-20256C55.pf
 4882:  A           C:\WINDOWS\Prefetch\TINTSETP.EXE-39BF0732.pf
***** ..\SS-20080623-070953.82\ATTRIB.TXT
 4877:  A           C:\WINDOWS\Prefetch\TASKLIST.EXE-10D94B23.pf
 4878:  A           C:\WINDOWS\Prefetch\TINTSETP.EXE-39BF0732.pf
*****

***** ATTRIB.txt
10908:             C:\WINDOWS\Debug
10909:  A          C:\WINDOWS\Delete.bat
10910:  A          C:\WINDOWS\desktop.ini
```

nada

KDiff3 – File comparison tool



KDiff3 – File comparison tool



Boot Sector malware

- Some malware may hide in boot sectors
- In order to detect such malware you need to save your Master Boot Record (MBR)
- MBRutil from PowerQuest is a free tool that will do just that.
  - `MBRutil /S=MBRBACKP.BIN`
  - `Run malware`
  - `MBRutil /S=MBR.BIN`
- You should only have to do this once.
- You can use the following command to compare:
  - `COMP MBRBACKP.BIN MBR.BIN`

Beyond-layer-7 Parts

- Training….
  - Training is key to do effective malware analysis
- Books
  - Reference Books are handy to understand some registry keys. And good information can be found on the net.

Costs

- Most of the cost will come from the training and personnel salary
- Hardware and software will probably be the cheapest part of your lab.

Costs

- Hardware needed
  - High end PC for Analysis station (Virtualization Host)
  - 4 PCs (minimum 2)
    - 1 Firewall providing Network services
    - 3 Test PCs
  - Ethernet Switch with port forwarding (or a Hub)
    - You can probably find an old switch in you organization

Hardware Costs

Analysis Workstation (VM)	2000.00$
1 Firewall	0$
3 Test PCs	0$
Analysis Tools	0$
KVM switch with cables	Under 400.00$
Ethernet Switch	0$ - 2000.00$

Software and misc. Costs

MSDN Subscription	2000.00$ per individual (Yearly renewal)
Virtualization Software	0 – 190.00$
Software (Other than Microsoft)	Depends on licensing
Personnel	Depends on salary and time dedicated to malware analysis
Training	6000.00$ - 8000.00$ (including hotel and travel)

Wrapping-up

- CIRT teams will find benefits of having their own behavioural malware analysis
- This behavioural analysis setup should provide enough information to start mitigation of unknown malware in a short time. It is not meant to replace assembly level analysis which is more thorough.
- Key to behavioural malware analysis is knowing your OS and your tools. So, training is important

Wrapping-up

- Setting up the lab is not neither difficult nor expensive
- Most of the tools needed for behavioural analysis are pre-installed in Windows or free
- MSDN subscription is HIGHLY recommended for National/Governmental CIRTs

- You should be able to setup your own lab for under 10,000$

URLS

Partimage
- http://www.partimage.org/Main_Page

SysAnalyzer
- http://labs.idefense.com/software/malcode.php

FPort
- http://www.foundstone.com/us/resources/proddesc/fport.htm

RegShot
- https://sourceforge.net/projects/regshot

MD5SUMS PC-Tools
- http://www.pc-tools.net/win32/md5sums/

SysInternals Tools
- http://technet.microsoft.com/en-us/sysinternals/default.aspx

Kdiff3
- http://kdiff3.sourceforge.net/

Netcat
- http://www.hackosis.com/wp-content/uploads/2007/12/nc111nt.zip
- http://joncraton.org/files/nc111nt.zip

MBRutil
- ftp://ftp.symantec.com/public/english_us_canada/tools/pq/utilities/head.zip

DEMO