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
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
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 | 2.007.6.15.0 | 06.19.2007 | no virus found
AntiVir | 7.4.0.34 | 06.19.2007 | no virus found
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
Cyat-Quick Heal | 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-Pro | 4.3.2.9e | 06.19.2007 | no virus found
F-Secure | 6.70.1.030.0 | 06.19.2007 | no virus found
Ikarus | T3.1.1.8 | 06.19.2007 | no virus found
Kaspersky | 4.0.2.24 | 06.19.2007 | no virus found
McAfee | 5055 | 06.10.2007 | 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 | no virus found
Panda | 0.0.0.4 | 06.12.2007 | no virus found
Sophos | 4.18.0 | 06.12.2007 | no virus found
Sunbelt | 2.2.507.0 | 06.10.2007 | no virus found
Symantec | 10 | 06.19.2007 | no virus found
TheHacker | 6.1.6.134 | 06.19.2007 | no virus found
VBA32 | 3.12.0.2 | 06.19.2007 | no virus found
VirusBuster | 4.3.29.9 | 06.18.2007 | no virus found
Webwasher-Gateway | 6.3.1 | 06.19.2007 | no virus found

**Additional Information**

File size: 1856512 bytes
Anubis

Anubis: Analyzing Unknown Binaries - Mozilla Firefox

PEID Output
thamida 1.0.0.5 -> Oreans Technologies

2.a) 200512.exe - File Activities

Files Created:
C:\Program Files\NetMeeting\msmsgs

Files Read:
C:\1nsd\Tml\200512.exe
C:\WINDOWS\system32\ADVAPI32.dll
C:\WINDOWS\system32\KERNEL32.dll
C:\WINDOWS\system32\USER32.dll

Directories Created:
### Sandbox Result

**Sandbox Submit a File Report**

<table>
<thead>
<tr>
<th>ID</th>
<th>746392</th>
</tr>
</thead>
<tbody>
<tr>
<td>Comment</td>
<td>None</td>
</tr>
<tr>
<td>Flag</td>
<td>1</td>
</tr>
</tbody>
</table>

**Analysis Summary:**

- **Analysis Date:** 6/18/2007 3:25:22 AM
- **Sandbox Version:** 2.0.5
- **Filename:** e:\temp\eabf5ca0f133dd1e59001cfeca.exe

**Technical Details:**

<table>
<thead>
<tr>
<th>Analysis Number</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parent ID</td>
<td>0</td>
</tr>
<tr>
<td>Process ID</td>
<td>544</td>
</tr>
<tr>
<td>Filename</td>
<td>e:\temp\eabf5ca0f133dd1e59001cfeca.exe</td>
</tr>
<tr>
<td>Filesize</td>
<td>231,20 bytes</td>
</tr>
</tbody>
</table>
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.
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 CClRC’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

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

Ubuntu
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";
};
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
```
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)
;; 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
    - `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 CORPORATE 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

Open files monitor

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

```plaintext
openfiles /Local ON
```

Note: You will have to reboot your system for this command to take effect.
Analysis Tools

Live Monitoring tools
- SySAnalyzer
- RegShot

Low footprint monitoring
- REG
- TASKLIST
- SC
- ATTRIB
- NETSTAT
- WMIC

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

<table>
<thead>
<tr>
<th>Process</th>
<th>PID</th>
<th>CPU</th>
<th>Description</th>
<th>Company Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Idle Process</td>
<td>0</td>
<td>96.12</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Inte...</td>
<td>n/a</td>
<td>Hardware Interrupts</td>
<td>Microsoft Corporation</td>
<td></td>
</tr>
<tr>
<td>DPCs</td>
<td>n/a</td>
<td>Deferred Procedure Calls</td>
<td></td>
<td></td>
</tr>
<tr>
<td>System</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>smss.exe</td>
<td>308</td>
<td>Windows NT Session Manager</td>
<td>Microsoft Corporation</td>
<td></td>
</tr>
<tr>
<td>csrss.exe</td>
<td>460</td>
<td>Client Server Runtime Process</td>
<td>Microsoft Corporation</td>
<td></td>
</tr>
<tr>
<td>winlogon.exe</td>
<td>484</td>
<td>Windows NT Logon Application</td>
<td>Microsoft Corporation</td>
<td></td>
</tr>
<tr>
<td>services.exe</td>
<td>652</td>
<td>1.94</td>
<td>Services and Controller app</td>
<td>Microsoft Corporation</td>
</tr>
<tr>
<td>svchost.exe</td>
<td>816</td>
<td></td>
<td>Generic Host Process for Wi-Fi</td>
<td>Microsoft Corporation</td>
</tr>
<tr>
<td>svchost.exe</td>
<td>896</td>
<td></td>
<td>Generic Host Process for Wi-Fi</td>
<td>Microsoft Corporation</td>
</tr>
<tr>
<td>svchost.exe</td>
<td>936</td>
<td></td>
<td>Generic Host Process for Wi-Fi</td>
<td>Microsoft Corporation</td>
</tr>
<tr>
<td>wscntfy.exe</td>
<td>1756</td>
<td></td>
<td>Windows Security Center N.</td>
<td>Microsoft Corporation</td>
</tr>
<tr>
<td>wuausvl.exe</td>
<td>348</td>
<td></td>
<td>Automatic Updates</td>
<td>Microsoft Corporation</td>
</tr>
<tr>
<td>svchost.exe</td>
<td>996</td>
<td></td>
<td>Generic Host Process for Wi-Fi</td>
<td>Microsoft Corporation</td>
</tr>
<tr>
<td>svchost.exe</td>
<td>1020</td>
<td></td>
<td>Generic Host Process for Wi-Fi</td>
<td>Microsoft Corporation</td>
</tr>
<tr>
<td>spoolsv.exe</td>
<td>1284</td>
<td></td>
<td>Spooler SubSystem App</td>
<td>Microsoft Corporation</td>
</tr>
<tr>
<td>alg.exe</td>
<td>1722</td>
<td></td>
<td>Application Layer Gateway</td>
<td>Microsoft Corporation</td>
</tr>
<tr>
<td>explorer.exe</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>VBoxService.exe</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>cmd.exe</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>proceexp.exe</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CPU Usage: 3.88%</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Additional Menu Options
- Window
- Set Priority
- Kill Process
- Kill Process Tree
- Restart
- Suspend
- Debug
- Properties
- Search Online... Ctrl+M
PROCEXP.EXE – Process Explorer
PROCEXP.EXE – Process Explorer

Printable strings found in the scan:

- Make sure that this file is not being used by another program.
- VDrums.vxd
- WHV
- !This program cannot be run in DOS mode.
- Rich
- LCOD
- XPRTVxD
- XPRTvxD
- verPP
- 1vsR2vsR3vsR
- jk
- ih
- XPRTvxD_DDB
- ADVAPI32.DLL
- OpenSCManagerA
- CreateServiceA
- StartServiceA
- GetNativeSystemInfo
- GetServiceA
<table>
<thead>
<tr>
<th>#</th>
<th>Time</th>
<th>Process</th>
<th>Request</th>
<th>Path</th>
<th>Result</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>205</td>
<td>9:48:08 AM</td>
<td>svchost.ex_</td>
<td>QUERY INFORMATION</td>
<td>C:\</td>
<td>SUCCESS</td>
<td>FileInternalInformation</td>
</tr>
<tr>
<td>206</td>
<td>9:48:08 AM</td>
<td>svchost.ex_</td>
<td>CLOSE</td>
<td>C:\</td>
<td>SUCCESS</td>
<td>Options: Open Access: 000...</td>
</tr>
<tr>
<td>207</td>
<td>9:48:08 AM</td>
<td>svchost.ex_</td>
<td>OPEN</td>
<td>C:\MAR\</td>
<td>SUCCESS</td>
<td>FileInternalInformation</td>
</tr>
<tr>
<td>208</td>
<td>9:48:08 AM</td>
<td>svchost.ex_</td>
<td>QUERY INFORMATION</td>
<td>C:\MAR\</td>
<td>SUCCESS</td>
<td>Options: Open Access: 000...</td>
</tr>
<tr>
<td>209</td>
<td>9:48:08 AM</td>
<td>svchost.ex_</td>
<td>CLOSE</td>
<td>C:\MAR\</td>
<td>SUCCESS</td>
<td>Options: Open Access: 000...</td>
</tr>
<tr>
<td>210</td>
<td>9:48:08 AM</td>
<td>svchost.ex_</td>
<td>OPEN</td>
<td>C:\MAR\BIN\</td>
<td>SUCCESS</td>
<td>Options: Open Access: 000...</td>
</tr>
<tr>
<td>211</td>
<td>9:48:08 AM</td>
<td>svchost.ex_</td>
<td>QUERY INFORMATION</td>
<td>C:\MAR\BIN\</td>
<td>SUCCESS</td>
<td>Options: Open Access: 000...</td>
</tr>
<tr>
<td>212</td>
<td>9:48:08 AM</td>
<td>svchost.ex_</td>
<td>CLOSE</td>
<td>C:\MAR\BIN\</td>
<td>SUCCESS</td>
<td>Options: Open Access: 000...</td>
</tr>
<tr>
<td>213</td>
<td>9:48:08 AM</td>
<td>svchost.ex_</td>
<td>OPEN</td>
<td>C:\WINDOWS\</td>
<td>SUCCESS</td>
<td>Options: Open Access: 000...</td>
</tr>
<tr>
<td>214</td>
<td>9:48:08 AM</td>
<td>svchost.ex_</td>
<td>QUERY INFORMATION</td>
<td>C:\WINDOWS\</td>
<td>SUCCESS</td>
<td>Options: Open Access: 000...</td>
</tr>
<tr>
<td>215</td>
<td>9:48:08 AM</td>
<td>svchost.ex_</td>
<td>CLOSE</td>
<td>C:\WINDOWS\</td>
<td>SUCCESS</td>
<td>Options: Open Access: 000...</td>
</tr>
<tr>
<td>216</td>
<td>9:48:08 AM</td>
<td>svchost.ex_</td>
<td>OPEN</td>
<td>C:\WINDOWS\SYSTEM32\</td>
<td>SUCCESS</td>
<td>Options: Open Access: 000...</td>
</tr>
<tr>
<td>217</td>
<td>9:48:08 AM</td>
<td>svchost.ex_</td>
<td>QUERY INFORMATION</td>
<td>C:\WINDOWS\SYSTEM32\</td>
<td>SUCCESS</td>
<td>Options: Open Access: 000...</td>
</tr>
<tr>
<td>218</td>
<td>9:48:08 AM</td>
<td>svchost.ex_</td>
<td>CLOSE</td>
<td>C:\WINDOWS\SYSTEM32\</td>
<td>SUCCESS</td>
<td>Options: Open Access: 000...</td>
</tr>
<tr>
<td>219</td>
<td>9:48:08 AM</td>
<td>svchost.ex_</td>
<td>OPEN</td>
<td>C:\WINDOWS\SYSTEM32\DRIVERS\</td>
<td>SUCCESS</td>
<td>Options: Open Access: 000...</td>
</tr>
<tr>
<td>220</td>
<td>9:48:08 AM</td>
<td>svchost.ex_</td>
<td>QUERY INFORMATION</td>
<td>C:\WINDOWS\SYSTEM32\DRIVERS\</td>
<td>SUCCESS</td>
<td>Options: Open Access: 000...</td>
</tr>
<tr>
<td>221</td>
<td>9:48:08 AM</td>
<td>svchost.ex_</td>
<td>CLOSE</td>
<td>C:\WINDOWS\SYSTEM32\DRIVERS\</td>
<td>SUCCESS</td>
<td>Options: Open Access: 000...</td>
</tr>
<tr>
<td>222</td>
<td>9:48:08 AM</td>
<td>winlogon.e_</td>
<td>READ</td>
<td>C:\</td>
<td>SUCCESS</td>
<td>Offset: 4648960 Length: 4096</td>
</tr>
<tr>
<td>223</td>
<td>9:48:08 AM</td>
<td>evchost.ex_</td>
<td>OPEN</td>
<td>C:\WINDOWS\WIN\XS\</td>
<td>SUCCESS</td>
<td>Options: Open Access: 000...</td>
</tr>
<tr>
<td>224</td>
<td>9:48:08 AM</td>
<td>svchost.ex_</td>
<td>QUERY INFORMATION</td>
<td>C:\WINDOWS\WIN\XS\</td>
<td>SUCCESS</td>
<td>Options: Open Access: 000...</td>
</tr>
<tr>
<td>225</td>
<td>9:48:08 AM</td>
<td>svchost.ex_</td>
<td>CLOSE</td>
<td>C:\WINDOWS\WIN\XS\</td>
<td>SUCCESS</td>
<td>Options: Open Access: 000...</td>
</tr>
<tr>
<td>226</td>
<td>9:48:08 AM</td>
<td>svchost.ex_</td>
<td>OPEN</td>
<td>C:\WINDOWS\WIN\XS\V86\MICRO\</td>
<td>SUCCESS</td>
<td>Options: Open Access: 000...</td>
</tr>
<tr>
<td>227</td>
<td>9:48:08 AM</td>
<td>svchost.ex_</td>
<td>QUERY INFORMATION</td>
<td>C:\WINDOWS\WIN\XS\V86\MICRO\</td>
<td>SUCCESS</td>
<td>Options: Open Access: 000...</td>
</tr>
<tr>
<td>228</td>
<td>9:48:08 AM</td>
<td>svchost.ex_</td>
<td>CLOSE</td>
<td>C:\WINDOWS\WIN\XS\V86\MICRO\</td>
<td>SUCCESS</td>
<td>Options: Open Access: 000...</td>
</tr>
<tr>
<td>229</td>
<td>9:48:08 AM</td>
<td>svchost.ex_</td>
<td>CREATE</td>
<td>C:\WINDOWS\Prefetch\FILEMON.EXE\</td>
<td>SUCCESS</td>
<td>Options: Overwrite Access:...</td>
</tr>
<tr>
<td>230</td>
<td>9:48:08 AM</td>
<td>winlogon.e_</td>
<td>READ</td>
<td>C:\</td>
<td>SUCCESS</td>
<td>Offset: 4620288 Length: 4096</td>
</tr>
<tr>
<td>231</td>
<td>9:48:08 AM</td>
<td>winlogon.e_</td>
<td>READ</td>
<td>C:\</td>
<td>SUCCESS</td>
<td>Offset: 4055040 Length: 4096</td>
</tr>
<tr>
<td>232</td>
<td>9:48:08 AM</td>
<td>winlogon.e_</td>
<td>READ</td>
<td>C:\</td>
<td>SUCCESS</td>
<td>Offset: 3108864 Length: 4096</td>
</tr>
<tr>
<td>233</td>
<td>9:48:08 AM</td>
<td>winlogon.e_</td>
<td>READ</td>
<td>C:\</td>
<td>SUCCESS</td>
<td>Offset: 3342336 Length: 4096</td>
</tr>
<tr>
<td>234</td>
<td>9:48:08 AM</td>
<td>winlogon.e_</td>
<td>READ</td>
<td>C:\</td>
<td>SUCCESS</td>
<td>Offset: 4653056 Length: 4096</td>
</tr>
<tr>
<td>235</td>
<td>9:48:08 AM</td>
<td>winlogon.e_</td>
<td>DIRECTORY</td>
<td>C:\WINDOWS\system32\</td>
<td>SUCCESS</td>
<td>Change Notify</td>
</tr>
</tbody>
</table>
**REGMON.EXE – Registry Monitor**

Here is a table of registry operations monitored by REGMON:

<table>
<thead>
<tr>
<th>#</th>
<th>Time</th>
<th>Process</th>
<th>Request</th>
<th>Path</th>
<th>Result</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>025</td>
<td>1.04534769</td>
<td>Regm...</td>
<td>QueryValue</td>
<td>HKCF\Drive\shell\FolderExtensions...</td>
<td>SUCCE</td>
<td>0x20</td>
</tr>
<tr>
<td>026</td>
<td>1.04535890</td>
<td>Regm...</td>
<td>CloseKey</td>
<td>HKCF\Drive\shell\FolderExtensions...</td>
<td>SUCCE</td>
<td></td>
</tr>
<tr>
<td>027</td>
<td>1.04536891</td>
<td>Regm...</td>
<td>Enumerate</td>
<td>HKCF\Drive\shell\FolderExtensions...</td>
<td>NO MO</td>
<td></td>
</tr>
<tr>
<td>028</td>
<td>1.04537559</td>
<td>Regm...</td>
<td>CloseKey</td>
<td>HKCF\Drive\shell\FolderExtensions...</td>
<td>SUCCE</td>
<td></td>
</tr>
<tr>
<td>029</td>
<td>1.04556477</td>
<td>Regm...</td>
<td>OpenKey</td>
<td>HKCU\Software\Microsoft\Windows...</td>
<td>SUCCE</td>
<td>Access: 0x...</td>
</tr>
<tr>
<td>030</td>
<td>1.04559063</td>
<td>Regm...</td>
<td>OpenKey</td>
<td>HKCU\Software\Microsoft\Windows...</td>
<td>SUCCE</td>
<td>Access: 0x...</td>
</tr>
<tr>
<td>031</td>
<td>1.04559243</td>
<td>Regm...</td>
<td>CloseKey</td>
<td>HKCU\Software\Microsoft\Windows...</td>
<td>SUCCE</td>
<td></td>
</tr>
<tr>
<td>032</td>
<td>1.04559063</td>
<td>Regm...</td>
<td>QueryValue</td>
<td>HKCU\Software\Microsoft\Windows...</td>
<td>SUCCE</td>
<td>0x1</td>
</tr>
<tr>
<td>033</td>
<td>1.04556368</td>
<td>Regm...</td>
<td>CloseKey</td>
<td>HKCU\Software\Microsoft\Windows...</td>
<td>SUCCE</td>
<td></td>
</tr>
<tr>
<td>034</td>
<td>1.04551618</td>
<td>Regm...</td>
<td>OpenKey</td>
<td>HKCU\Software\Microsoft\Windows...</td>
<td>SUCCE</td>
<td>Access: 0x...</td>
</tr>
<tr>
<td>035</td>
<td>1.04553204</td>
<td>Regm...</td>
<td>OpenKey</td>
<td>HKCU\Software\Microsoft\Windows...</td>
<td>SUCCE</td>
<td>Access: 0x...</td>
</tr>
<tr>
<td>036</td>
<td>1.04554348</td>
<td>Regm...</td>
<td>CloseKey</td>
<td>HKCU\Software\Microsoft\Windows...</td>
<td>SUCCE</td>
<td></td>
</tr>
<tr>
<td>037</td>
<td>1.04555421</td>
<td>Regm...</td>
<td>QueryValue</td>
<td>HKCU\Software\Microsoft\Windows...</td>
<td>SUCCE</td>
<td>0x1</td>
</tr>
<tr>
<td>038</td>
<td>1.04556482</td>
<td>Regm...</td>
<td>CloseKey</td>
<td>HKCU\Software\Microsoft\Windows...</td>
<td>SUCCE</td>
<td></td>
</tr>
<tr>
<td>039</td>
<td>1.04727674</td>
<td>Isass...</td>
<td>OpenKey</td>
<td>HKLM\SECURITY\Policy</td>
<td>SUCCE</td>
<td>Access: 0x...</td>
</tr>
<tr>
<td>040</td>
<td>1.04729426</td>
<td>Isass...</td>
<td>OpenKey</td>
<td>HKLM\SECURITY\Policy\SecDesc</td>
<td>SUCCE</td>
<td>Access: 0x...</td>
</tr>
<tr>
<td>041</td>
<td>1.04730260</td>
<td>Isass...</td>
<td>QueryValue</td>
<td>HKLM\SECURITY\Policy\SecDesc...</td>
<td>BUFFER</td>
<td></td>
</tr>
<tr>
<td>042</td>
<td>1.04731524</td>
<td>Isass...</td>
<td>CloseKey</td>
<td>HKLM\SECURITY\Policy\SecDesc</td>
<td>SUCCE</td>
<td></td>
</tr>
<tr>
<td>043</td>
<td>1.04732319</td>
<td>Isass...</td>
<td>OpenKey</td>
<td>HKLM\SECURITY\Policy\SecDesc</td>
<td>SUCCE</td>
<td>Access: 0x...</td>
</tr>
<tr>
<td>044</td>
<td>1.04733670</td>
<td>Isass...</td>
<td>QueryValue</td>
<td>HKLM\SECURITY\Policy\SecDesc...</td>
<td>BUFFER</td>
<td></td>
</tr>
<tr>
<td>045</td>
<td>1.04734600</td>
<td>Isass...</td>
<td>CloseKey</td>
<td>HKLM\SECURITY\Policy\SecDesc</td>
<td>SUCCE</td>
<td>NONE</td>
</tr>
<tr>
<td>046</td>
<td>1.04758908</td>
<td>Isass...</td>
<td>CloseKey</td>
<td>HKLM\SECURITY\Policy</td>
<td>SUCCE</td>
<td></td>
</tr>
<tr>
<td>047</td>
<td>7.27233144</td>
<td>Sys...</td>
<td>OpenKey</td>
<td>HKLM\System\CurrentControlSet\Cont...</td>
<td>SUCCE</td>
<td>Access: 0x...</td>
</tr>
<tr>
<td>048</td>
<td>7.27239847</td>
<td>Sys...</td>
<td>QueryValue</td>
<td>HKLM\System\CurrentControlSet\Cont...</td>
<td>SUCCE</td>
<td>0x12C</td>
</tr>
<tr>
<td>049</td>
<td>7.27242422</td>
<td>Sys...</td>
<td>QueryValue</td>
<td>HKLM\System\CurrentControlSet\Cont...</td>
<td>SUCCE</td>
<td>&quot;Eastern Standard Time&quot;</td>
</tr>
<tr>
<td>050</td>
<td>7.27243956</td>
<td>Sys...</td>
<td>QueryValue</td>
<td>HKLM\System\CurrentControlSet\Cont...</td>
<td>SUCCE</td>
<td>0x0</td>
</tr>
<tr>
<td>051</td>
<td>7.27254963</td>
<td>Sys...</td>
<td>QueryValue</td>
<td>HKLM\System\CurrentControlSet\Cont...</td>
<td>SUCCE</td>
<td>00 00 00 04 00 00 00...</td>
</tr>
<tr>
<td>052</td>
<td>7.27259684</td>
<td>Sys...</td>
<td>QueryValue</td>
<td>HKLM\System\CurrentControlSet\Cont...</td>
<td>SUCCE</td>
<td>&quot;Eastern Standard Time&quot;</td>
</tr>
<tr>
<td>053</td>
<td>7.27263841</td>
<td>Sys...</td>
<td>QueryValue</td>
<td>HKLM\System\CurrentControlSet\Cont...</td>
<td>SUCCE</td>
<td>0xFFFC4</td>
</tr>
<tr>
<td>054</td>
<td>7.27268267</td>
<td>Sys...</td>
<td>QueryValue</td>
<td>HKLM\System\CurrentControlSet\Cont...</td>
<td>SUCCE</td>
<td>00 00 04 00 00 00...</td>
</tr>
<tr>
<td>055</td>
<td>7.27274109</td>
<td>Sys...</td>
<td>CheckKey</td>
<td>HKLM\System\CurrentControlSet\Cont...</td>
<td>SUCCE</td>
<td></td>
</tr>
<tr>
<td>Process</td>
<td>Protocol</td>
<td>Local Address</td>
<td>Remote Address</td>
<td>State</td>
<td></td>
<td></td>
</tr>
<tr>
<td>-------------</td>
<td>----------</td>
<td>------------------</td>
<td>-----------------</td>
<td>-------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>alg.exe:1828</td>
<td>TCP</td>
<td>127.0.0.1:1025</td>
<td>0.0.0.0:0</td>
<td>LISTENING</td>
<td></td>
<td></td>
</tr>
<tr>
<td>lsass.exe:668</td>
<td>UDP</td>
<td>0.0.0.0:500</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>lsass.exe:668</td>
<td>UDP</td>
<td>0.0.0.0:4500</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>svchost.exe:1096</td>
<td>UDP</td>
<td>10.0.2.15:1900</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>svchost.exe:1096</td>
<td>TCP</td>
<td>127.0.0.1:1900</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>svchost.exe:892</td>
<td>TCP</td>
<td>0.0.0.0:135</td>
<td>0.0.0.0:0</td>
<td>LISTENING</td>
<td></td>
<td></td>
</tr>
<tr>
<td>svchost.exe:928</td>
<td>UDP</td>
<td>10.0.2.15:123</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>svchost.exe:928</td>
<td>UDP</td>
<td>127.0.0.1:123</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>svchost.exe:928</td>
<td>UDP</td>
<td>127.0.0.1:1043</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>svchost.exe:980</td>
<td>UDP</td>
<td>0.0.0.0:1036</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>svchost.exe:980</td>
<td>UDP</td>
<td>0.0.0.0:1042</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>System:4</td>
<td>TCP</td>
<td>0.0.0.0:445</td>
<td>0.0.0.0:0</td>
<td>LISTENING</td>
<td></td>
<td></td>
</tr>
<tr>
<td>System:4</td>
<td>TCP</td>
<td>10.0.2.15:139</td>
<td>0.0.0.0:0</td>
<td>LISTENING</td>
<td></td>
<td></td>
</tr>
<tr>
<td>System:4</td>
<td>UDP</td>
<td>0.0.0.0:445</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>System:4</td>
<td>UDP</td>
<td>10.0.2.15:138</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>System:4</td>
<td>UDP</td>
<td>10.0.2.15:137</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
SysAnalyzer - iDEFENSE
Low footprint monitoring

Registry tools
- REG.EXE
- AUTORUNS.EXE

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

Network
- NETSTAT.EXE
- FPORT.EXE

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

```
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]
```

Canada

Public Safety
Canada

Sécurité publique
Canada
The image shows the Autoruns utility interface with several entries listed. The entries include:

- HKLM\System\CurrentControlSet\Control\Terminal Server\Wds\rdpwd\Startup Programs:
  - rdpclip: RDP Clip Monitor by Microsoft Corporation, path: c:\windows\system32\rdpclip...

- HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Userinit:
  - C:\WINDOWS... Userinit Logon Application by Microsoft Corporation, path: c:\windows\system32\useri...

- HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell:
  - Explorer.exe: Windows Explorer by Microsoft Corporation, path: c:\windows\explorer.exe

- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run:
  - IMJPMIG81: Microsoft IME by Microsoft Corporation, path: c:\windows\ime\imjp8_1\imj...
  - MSYP2002
  - PHIME2002A: ????????? 2002a by Microsoft Corporation, path: c:\windows\system32\ime\...
  - PHIME2002AS: ????????? 2002a by Microsoft Corporation, path: c:\windows\system32\ime\...
### TASKLIST.EXE – Windows Processes and services

```plaintext
C:\>tasklist

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

C:\>
SC.EXE – Service Control command line utility

```
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

```
C:\>pslist -t

c:}\pslist -t

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

Process information for JAMIE-13F427558:

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

```
Command Prompt

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

C:\>pservice config more

PsService v2.21 - Service information and configuration utility
Copyright (C) 2001-2006 Mark Russinovich
Sysinternals - www.sysinternals.com

SERVICE_NAME: Alerter
Notifies selected users and computers of administrative alerts. If the service is stopped, programs that use administrative alerts will not receive them. If this service is disabled, any services that explicitly depend on it will fail to start.

- TYPE: 20 WIN32_SHARE_PROCESS
- START_TYPE: 4 DISABLED
- ERROR_CONTROL: 1 NORMAL
- BINARY_PATH_NAME: C:\WINDOWS\system32\svchost.exe -k LocalService
- LOAD_ORDER_GROUP: 
- TAG: 0
- DISPLAY_NAME: Alerter
- DEPENDENCIES: LanmanWorkstation
- SERVICE_START_NAME: NT AUTHORITY\LocalService

SERVICE_NAME: ALG
Provides support for 3rd party protocol plug-ins for Internet Connection Sharing and the Windows Firewall.

- TYPE: 10 WIN32Own_PROCESS
- START_TYPE: 3 DEMAND_START
- ERROR_CONTROL: 1 NORMAL
- BINARY_PATH_NAME: C:\WINDOWS\System32\alg.exe
- LOAD_ORDER_GROUP: 
- TAG: 0
```

---

Public Safety
Canada

Sécurité publique
Canada

75
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

```
C:\>netstat -an

Active Connections

<table>
<thead>
<tr>
<th>Proto</th>
<th>Local Address</th>
<th>Foreign Address</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP</td>
<td>0.0.0.0:135</td>
<td>0.0.0.0:0</td>
<td>LISTENING</td>
</tr>
<tr>
<td>TCP</td>
<td>0.0.0.0:445</td>
<td>0.0.0.0:0</td>
<td>LISTENING</td>
</tr>
<tr>
<td>TCP</td>
<td>127.0.0.1:1025</td>
<td>0.0.0.0:0</td>
<td>LISTENING</td>
</tr>
<tr>
<td>UDP</td>
<td>0.0.0.0:445</td>
<td><em>:</em></td>
<td></td>
</tr>
<tr>
<td>UDP</td>
<td>0.0.0.0:500</td>
<td><em>:</em></td>
<td></td>
</tr>
<tr>
<td>UDP</td>
<td>0.0.0.0:4500</td>
<td><em>:</em></td>
<td></td>
</tr>
<tr>
<td>UDP</td>
<td>127.0.0.1:123</td>
<td><em>:</em></td>
<td></td>
</tr>
<tr>
<td>UDP</td>
<td>127.0.0.1:1900</td>
<td><em>:</em></td>
<td></td>
</tr>
</tbody>
</table>
```
<table>
<thead>
<tr>
<th>Pid</th>
<th>Process</th>
<th>Port</th>
<th>Proto</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>648</td>
<td>servterm</td>
<td>23</td>
<td>TCP</td>
<td>Z:\software\windows-based\serv-t-0\servterm.exe</td>
</tr>
<tr>
<td>892</td>
<td>System</td>
<td>135</td>
<td>TCP</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>System</td>
<td>139</td>
<td>TCP</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>System</td>
<td>445</td>
<td>TCP</td>
<td></td>
</tr>
<tr>
<td>1828</td>
<td></td>
<td>1025</td>
<td>TCP</td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>System</td>
<td>123</td>
<td>UDP</td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>System</td>
<td>137</td>
<td>UDP</td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>System</td>
<td>138</td>
<td>UDP</td>
<td></td>
</tr>
<tr>
<td>648</td>
<td>servterm</td>
<td>445</td>
<td>UDP</td>
<td>Z:\software\windows-based\serv-t-0\servterm.exe</td>
</tr>
<tr>
<td>892</td>
<td>System</td>
<td>500</td>
<td>UDP</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>System</td>
<td>1036</td>
<td>UDP</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>System</td>
<td>1042</td>
<td>UDP</td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>System</td>
<td>1043</td>
<td>UDP</td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>System</td>
<td>1900</td>
<td>UDP</td>
<td></td>
</tr>
<tr>
<td>1828</td>
<td></td>
<td>4500</td>
<td>UDP</td>
<td></td>
</tr>
</tbody>
</table>
ATTRIB.EXE – File Attributes

C:\>attrib
A   C:\AUTOEXEC.BAT
A   C:\boot.ini
A   C:\CONFIG.SYS
A   C:\IO.SYS
A   C:\MSDOS.SYS
A   C:\NTDETECT.COM
A   C:\ntldr
A   C:\pagefile.sys

C:\>dir
Volume in drive C has no label.
Volume Serial Number is 2CE9-0307

Directory of C:\
05/12/2008 11:16 AM    0 AUTOEXEC.BAT
05/12/2008 11:16 AM    0 CONFIG.SYS
05/12/2008 11:45 AM    <DIR> Documents and Settings
05/15/2008 01:56 PM    <DIR> MAR
05/12/2008 12:57 PM    <DIR> Program Files
05/15/2008 02:53 PM    <DIR> WINDOWS
          2 File(s)   0 bytes
          4 Dir(s) 84,053,643,264 bytes free
C:\>
MD5DEEP.EXE – Integrity checker
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) 14,811,376 bytes
0 Dir(s)  6,243,045,376 bytes free
FC - File Comparison Tool

```cmd
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\AGENTSUR.EXE-002E45AB.pf |
****** ..\SS-20080623-070953.82\ATTRIB.TXT
| 4813 | A | C:\WINDOWS\PeerNet\sqlse20.dll |
| 4814 | A | C:\WINDOWS\Prefetch\AGENTSUR.EXE-002E45AB.pf |

****** ATTRIB.txt
| 4841 | A | C:\WINDOWS\Prefetch\MSIEXEC.EXE-2F8A8CAE.pf |
| 4842 | A | C:\WINDOWS\Prefetch\MSMSG-913F9B5.pf |
| 4843 | A | C:\WINDOWS\Prefetch\MSSOBE.EXE-30411B02.pf |
****** ..\SS-20080623-070953.82\ATTRIB.TXT
| 4839 | A | C:\WINDOWS\Prefetch\MSIEXEC.EXE-2F8A8CAE.pf |
| 4840 | A | C:\WINDOWS\Prefetch\MSSOBE.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\TINTSETIP.EXE-39BF0732.pf |
****** ..\SS-20080623-070953.82\ATTRIB.TXT
| 4877 | A | C:\WINDOWS\Prefetch\TASKLIST.EXE-10D94B23.pf |
| 4878 | A | C:\WINDOWS\Prefetch\TINTSETIP.EXE-39BF0732.pf |

****** ATTRIB.txt
| 10908 | A | C:\WINDOWS\Debug |
| 10909 | A | C:\WINDOWS\Delete.bat |
| 10910 | A | C:\WINDOWS\desktop.ini |
```
KDiff3 – File comparison tool
<table>
<thead>
<tr>
<th>Column A</th>
<th>Column B</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>C:WINDOWS\cmsetacl.log</td>
</tr>
<tr>
<td>A</td>
<td>C:WINDOWS\Coffee Bean.bmp</td>
</tr>
<tr>
<td>A</td>
<td>C:WINDOWS\comsetup.log</td>
</tr>
<tr>
<td>A</td>
<td>C:WINDOWS\Config</td>
</tr>
<tr>
<td>A</td>
<td>C:WINDOWS\Connection Wizard</td>
</tr>
<tr>
<td>A</td>
<td>C:WINDOWS\control.ini</td>
</tr>
<tr>
<td>A</td>
<td>C:WINDOWS\ Cursors</td>
</tr>
<tr>
<td>A</td>
<td>C:WINDOWS\Debug</td>
</tr>
<tr>
<td>S</td>
<td>C:WINDOWS\desktop.ini</td>
</tr>
<tr>
<td>A</td>
<td>C:WINDOWS\DtcInstall.log</td>
</tr>
<tr>
<td>A</td>
<td>C:WINDOWS\DtcInstall.log</td>
</tr>
<tr>
<td>A</td>
<td>C:WINDOWS\ehome</td>
</tr>
<tr>
<td>A</td>
<td>C:WINDOWS\ explorer.exe</td>
</tr>
<tr>
<td>A</td>
<td>C:WINDOWS\ explorer.exe</td>
</tr>
<tr>
<td>A</td>
<td>C:WINDOWS\ explorer.scf</td>
</tr>
<tr>
<td>A</td>
<td>C:WINDOWS\ FaxSetup.log</td>
</tr>
<tr>
<td>A</td>
<td>C:WINDOWS\ FeatherTexture.bmp</td>
</tr>
<tr>
<td>S R</td>
<td>C:WINDOWS\ Fonts</td>
</tr>
<tr>
<td>A</td>
<td>C:WINDOWS\ Gone Fishing.bmp</td>
</tr>
</tbody>
</table>
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 your organization
## Hardware Costs

<table>
<thead>
<tr>
<th>Item</th>
<th>Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>Analysis Workstation (VM)</td>
<td>2000.00$</td>
</tr>
<tr>
<td>1 Firewall</td>
<td>0$</td>
</tr>
<tr>
<td>3 Test PCs</td>
<td>0$</td>
</tr>
<tr>
<td>Analysis Tools</td>
<td>0$</td>
</tr>
<tr>
<td>KVM switch with cables</td>
<td>Under 400.00$</td>
</tr>
<tr>
<td>Ethernet Switch</td>
<td>0$ - 2000.00$</td>
</tr>
</tbody>
</table>
## Software and misc. Costs

<table>
<thead>
<tr>
<th>Item</th>
<th>Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>MSDN Subscription</td>
<td>2000.00$ per individual (Yearly renewal)</td>
</tr>
<tr>
<td>Virtualization Software</td>
<td>0 – 190.00$</td>
</tr>
<tr>
<td>Software (Other than Microsoft)</td>
<td>Depends on licensing</td>
</tr>
<tr>
<td>Personnel</td>
<td>Depends on salary and time dedicated to malware analysis</td>
</tr>
<tr>
<td>Training</td>
<td>6000.00$ - 8000.00$ (including hotel and travel)</td>
</tr>
</tbody>
</table>
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

FPort

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

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

SysInternals Tools

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

Netcat
- http://joncraton.org/files/nc111nt.zip

MBRutil
DEMO