

# Building A NO-FRILS

# **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



Canada



# 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 <u>Malware</u> 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

- Browser compromise
- Keyloggers
- RootKits
- Botnets
- Trojans

- etc...

- Worm

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 <u>prevent</u> 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 <u>unknown</u> 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:<u>http://www.symantec.com</u> ۲
- 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: <u>http://www.virustotal.com</u>
- Anubis: http://anubis.iseclab.org/index.php •
- Sunbelt: http://research.sunbelt-software.com/Submit.aspx •



Canada



#### **Virus Total**

		· Mozilla Firefox	
<u>E</u> dit <u>V</u> iew Hi <u>s</u> tory <u>B</u> oo	okmarks <u>T</u> ools <u>H</u> elp		
🍬 🝷 🙆 🏫	file:///		☆ 🗸 Google
ost Visited 👻 📔 Smart B	ookmarks 👻 🚞 CCIRC 👻	📔 Online tools 👻	Performance Analys
u ) (in unTabal unu			
:: virusiotai :::::			11000000000000000000000000000000000000
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
	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
karus	T3.1.1.8	06.19.2007	Backdoor.VB.EV
<aspersky< td=""><td>4.0.2.24</td><td>06.19.2007</td><td>no virus found</td></aspersky<>	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
ymantec	10	06.19.2007	no virus found
ГheHacker	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
Wohuncher Catouru	6.0.1	06 19 2007	Trojan Hupigon Gen



Canada

② 2 Errors □ (N) S

Done

File size: 1856512 bytes

#### Anubis

Edit View History Bookmarks Tools Help		العا
🔿 👻 🍪 🕋 🗽 file:///	☆ <b>- G -</b> Go	ogle
Most Visited 👻 📔 Smart Bookmarks 👻 📄 CCIRC 👻 📄 Online tools 👻 🌑 Perform	ance Analys	
	UX778F0000 0	X12000 I
C:\WINDOWS.0\system32\Apphelp.dll	0x77B10000 0	x22000
C:\WINDOWS.0\system32\msacm32.dll	0x77BB0000 0	x15000
C:\WINDOWS.0\system32\version.dll	0x77BD0000 0	×8000
C:\WINDOWS.0\system32\msvcrt.dll	0x77BE0000 0	x58000
C:\WINDOWS.0\system32\SHLWAPI.dll	0x77F40000 0	x76000
C:\WINDOWS.0\system32\SHELL32.dll	0x7C9D0000 0	x81E000
2.a) 200512.exe - File Activities		
Files Created:		
Files Created: C:\Program Files\NetMeeting\msmsgs		
Files Created: C:\Program Files\NetMeeting\msmsgs Files Read:		
Files Created:   C:\Program Files\NetMeeting\msmsgs   Files Read:   C:\InsideTm\200512.exe		
Files Created:   C:\Program Files\NetMeeting\msmsgs   Files Read:   C:\InsideTm\200512.exe   C:\WINDOWS.0\system32\ADVAPI32.dll		
Files Created:   C:\Program Files\NetMeeting\msmsgs   Files Read:   C:\InsideTm\200512.exe   C:\WINDOWS.0\system32\ADVAPI32.dll   C:\WINDOWS.0\system32\KERNEL32.dll		
Files Created:   C:\Program Files\NetMeeting\msmsgs   Files Read:   C:\InsideTm\200512.exe   C:\WINDOWS.0\system32\ADVAPI32.dll   C:\WINDOWS.0\system32\KERNEL32.dll   C:\WINDOWS.0\system32\USER32.dll		
Files Created:   C:\Program Files\NetMeeting\msmsgs   Files Read:   C:\InsideTm\200512.exe   C:\WINDOWS.0\system32\ADVAPI32.dll   C:\WINDOWS.0\system32\KERNEL32.dll   C:\WINDOWS.0\system32\USER32.dll   Directories Created:		





#### **Sunbelt**







# Outsourcing



**Private Sector Alliances** 

- Microsoft
- Contracted agencies

#### **Public/Government Sector Alliances**

Military 

Canada

- Law Enforcement  $\bullet$
- 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 <u>known</u> 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, <u>CHEAP</u> (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



Canada



#### **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**





 Sécurité publique Canada



#### **Analysis station using Virtualisation**







#### Windows XP Pro

VMWare Workstation

•Several Guest Host versions

•Guests OS bridge to the testing zone or Host only network



Canada









#### Windows XP Pro

•3 main images at various patching stages

•Microsoft Office installed





#### **The Network**









### The Firewall







#### <u>Ubuntu</u>

•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

27

- 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.



Canada



# 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.





- 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





- 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





- 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







- 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.



- 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

41

 Network recording with tcpdump (Always record all packets to a binary file) tcpdump –ni *if* –s 0 –w *outputfile*





- 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.





#### 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	localh	ost. root.localhost.	(
				1 ; Seri	al
			60480	0 ; Refr	esh
			8640	0 ; Retr	У
			241920	0 ; Expi	re
			8640	0 ) ; Negative Ca	ache TTL
;					
@		IN	NS	localhost.	
	1 4 4 0 0	<b>T 1 T</b>	-	100 100 101 0	
★.	⊥4400	⊥N	А	TAS.T08.T0T.S	

44



Public Safety Sécurité publique Canada



#### 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</pre>

;; QUESTION SECTION:

;test.vancouver.com.	IN	A

#### ;; ANSWER SECTION:

test.vancouver.com.		14400	IN	Α	192.168.101.2
;; AUTHORITY SECTION:		86400	IN	NS	localhost.
;; ADDITIONAL SECTION:					
localhost.	604800	IN	А	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





Canada

- 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 --todestination 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.







- 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







#### First things to do:

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







- 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.







- 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...







- 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







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





- 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







- 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







#### 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



Canada





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.



Canada





#### PROCEXP.EXE – Process Explorer

🧦 Process Explorer - Sysinternals: www.sysinternals.com [GREM-F39ED4815A\g... 🖡

Options View Process Find Users Help File ы -----2 R 44 • 121 x Description Company Name PID CPU Process System Idle Process 96.12 0 Interrupts n/a Hardware Interrupts DPCs n/a Deferred Procedure Calls System 4 smss.exe 308 Windows NT Session Mana... Microsoft Corporation Client Server Runtime Process Microsoft Corporation CSISS exe 460 🖃 🎒 winlogon.exe 484 Windows NT Logon Applica... Microsoft Corporation 652 1.94 Services and Controller app services.exe Microsoft Corporation Generic Host Process for Wi... Microsoft Corporation svchost.exe 816 svchost.exe 896 Generic Host Process for Wi... Microsoft Corporation Generic Host Process for Wi... Microsoft Corporation svchost.exe 936 wscntfy.exe 1756 Windows Security Center N., Microsoft Corporation 🍓 wuauclt.exe 348 Automatic Updates Microsoft Corporation Generic Host Process for Wi... Microsoft Corporation 996 sychost.exe 1020 svchost.exe Generic Host Process for Wi... Microsoft Corporation 1284 Spooler SubSystem App spoolsv.exe Microsoft Corporation 1733 Application Layer Gateway ... Microsoft Corporation alg e Window dows NT Save Dump Ut... Microsoft Corporation savedur Isass.ex Export Version) Microsoft Corporation exe Set Priority . explorer.exe Microsoft Corporation Explorer ervice Additions Service WVBoxService.exe Kill Process Del innotek GmbH = cv cmd.exe dows Command Processor Microsoft Corporation Kill Process Tree 🔎 procexp.exe internals Process Explorer Sysinternals Restart Suspend CPU Usage: 3.88% 21 Comr Debug **Public Safety** Sécur Canada Properties... Canad 61 Search Online... Ctrl+M

Canada



#### PROCEXP.EXE – Process Explorer

💐 Process Explorer - Sys 🖬 msmsgs:1076 Properties File Options View Process Performance Performance Graph Services Image **E** 177 H ¢ TCP/IP Strings. Security Environment Threads Process. Printable strings found in the scan: System Idle Process hEP Interrupts ^ hEP DPCs MZP 🔜 System -This program must be run under Win32 🖃 🥅 smss.exe .rsrc CSISS.exe .MaskPE 🖃 🌆 winlogon.exe idata. 🖃 💳 services.exe Themida svchost. .MaskPE svchost. C&pQ 🖃 🥅 sychost. uC#I - wsch 0eTx svchost. WkC{ sychost. JC}{g spoolsv.e ZIZ ZTG alg.exe NaZ@ 🖃 📷 msmsgs IPZ **IEXP** Sp1XV 🗂 Isass.exe (20 L--💂 explorer.exe 💿 Image Memory WVBoxService.exe Find Save 🈂 procexp.exe cmd.exe 0K Cancel CPU Usage: 87.13% Commit ( Public Safety Canada Sécurité publique Canada Canada 62



#### PROCEXP.EXE – Process Explorer

and the second s	💐 Process Explorer - Sys	🖻 msmsgs:1076 Properties 📃 🗖 🔁	
	File     Options     View     Process       Image: Imag	Image Performance Performance Graph Services Threads TCP/IP Security Environment Strings	
	Process  System Idle Process Interrupts DPCs System System System Srss.exe Srss.exe Srss.exe Srss.exe Srss.exe Srss.exe Srss.exe Srss.exe	Printable strings found in the scan: Make sure that this file is not being used by another program. NOreans.vxd WhV !This program cannot be run in DOS mode. Rich LCOD XPROTVXD XPROTVXD	
	svchost.e svchost.e svchost.e svchost.e svchost.e svchost.e spoolsv.e alg.exe	VerPP 1vsR2vsR3vsR ijh iii XPROTVXD_DDB ADVAPI32.DLL OpenSCManagerA CreateServiceA	
	EXPL EXPL Isass.exe VBoxService.exe VDoxService.exe Comprocexp.exe Comprocexp.exe Comprocexp.exe	GetNativeSystemInfo	
<b>∳</b> Р С	CPU Usage: 89.11% Commit o ublic Safety Sécurité anada Canada	OK Cancel Dublique 63	Canada

E ----



#### **FILEMON.EXE – File Monitor**



🖹 File Monitor - Sysinternals: www.sysinternals.com

File Edit Options Volumes Help 2

#### 🔒 🖻 🗌 🚧 👜 🗌 🍳 🔛 💟 🕼 📔

205       948/08 AM       svchost.ex QUERY INFORMATION       C\       SUCCESS       FileInternalInformation         205       948/08 AM       svchost.ex QUERY       C\       SUCCESS       Options: Open Access: 000         208       948/08 AM       svchost.ex QUERY       C\MAR\       SUCCESS       Options: Open Access: 000         209       948/08 AM       svchost.ex QUERY INFORMATION       C\MAR\       SUCCESS       Options: Open Access: 000         210       948/08 AM       svchost.ex QUERY INFORMATION       C\MAR\BIN\       SUCCESS       Options: Open Access: 000         211       948/08 AM       svchost.ex QUERY INFORMATION       C\MAR\BIN\       SUCCESS       Options: Open Access: 000         212       948/08 AM       svchost.ex CLOSE       C\MAR\BIN\       SUCCESS       Options: Open Access: 000         213       948/08 AM       svchost.ex QUERY INFORMATION       C\MINDOWS\SYSTEM32A       SUCCESS       Options: Open Access: 000         216       948/08 AM       svchost.ex QUERY INFORMATION       C\MINDOWS\SYSTEM32A       SUCCESS       Options: Open Access: 000         217       948/08 AM       svchost.ex QUERY INFORMATION       C\MINDOWS\SYSTEM32A       SUCCESS       Options: Open Access: 000         218       948/08 AM	#	Time	Process	Request	Path	Result	Other	~
206       94808AM       evchostex DEEN       C\       SUCCESS         208       94808AM       evchostex QUERY INFORMATION       C\MARN       SUCCESS         209       94808AM       evchostex QUERY INFORMATION       C\MARN       SUCCESS         209       94808AM       evchostex QUERY INFORMATION       C\MARN       SUCCESS       Options: Open Access: 000         211       94808AM       evchostex QUERY INFORMATION       C\MARNINN       SUCCESS       Options: Open Access: 000         213       94808AM       evchostex QUERY INFORMATION       C\MARNINN       SUCCESS       Options: Open Access: 000         214       94808AM       evchostex QUERY INFORMATION       C\MARNINN       SUCCESS       Options: Open Access: 000         213       94808AM       evchostex QUERY INFORMATION       C\MINDOWS\SYSTEM32       SUCCESS       Options: Open Access: 000         214       94808AM       evchostex CLOSE       C\MINDOWS\SYSTEM32       SUCCESS       Options: Open Access: 000         218       94808AM       evchostex QUERY INFORMATION       C\MINDOWS\SYSTEM32       SUCCESS       Options: Open Access: 000         219       94808AM       evchostex QUERY INFORMATION       C\MINDOWS\SYSTEM32       SUCCESS       Options: Open Access: 000.	205	9:48:08 AM	🔲 svchost.ex	. QUERY INFORMATION	C:\	SUCCESS	FileInternalInformation	
207       94808 AM       evchost.ex OPEN       C:MAR\       SUCCESS       Options: Open Access: 000         209       94808 AM       evchost.ex OUERY INFORMATION       C:MARN       SUCCESS       Options: Open Access: 000         209       94808 AM       evchost.ex OUERY INFORMATION       C:MARN       SUCCESS       Options: Open Access: 000         210       94808 AM       evchost.ex OUERY INFORMATION       C:MARNBINN       SUCCESS       Options: Open Access: 000         212       94808 AM       evchost.ex QUERY INFORMATION       C:WIANDWS\       SUCCESS       Options: Open Access: 000         213       94808 AM       evchost.ex QUERY INFORMATION       C:WINDOWS\       SUCCESS       Options: Open Access: 000         214       94808 AM       evchost.ex QUERY INFORMATION       C:WINDOWS\SYSTEM32\N       SUCCESS       Options: Open Access: 000         215       94808 AM       evchost.ex QUERY INFORMATION       C:WINDOWS\SYSTEM32\DRIVERS\       SUCCESS       Options: Open Access: 000         217       94808 AM       evchost.ex QUERY INFORMATION       C:WINDOWS\SYSTEM32\DRIVERS\       SUCCESS       Options: Open Access: 000         219       94808 AM       evchost.ex QUERY INFORMATION       C:WINDOWS\SYSTEM32\DRIVERS\       SUCCESS       Options: Open Access:	206	9:48:08 AM	🔲 svehostlex	CLOSE	C:V	SUCCESS		
208       948.08 AM       svchost ex QUERY INFORMATION       C:MARN       SUCCESS       Pieinternalinformation         209       948.08 AM       svchost ex QPEN       C:MARN BINN       SUCCESS       Options: Open Access: 000         211       948.08 AM       svchost ex QUERY INFORMATION       C:MARNBINN       SUCCESS       Options: Open Access: 000         212       948.08 AM       svchost ex QUERY INFORMATION       C:MARNBINN       SUCCESS       Options: Open Access: 000         213       948.08 AM       svchost ex QUERY INFORMATION       C:WINDOWS\       SUCCESS       Options: Open Access: 000         214       948.08 AM       svchost ex QUERY INFORMATION       C:WINDOWS\       SUCCESS       Options: Open Access: 000         214       948.08 AM       svchost ex QUERY INFORMATION       C:WINDOWS\SYSTEM32\       SUCCESS       Options: Open Access: 000         214       948.08 AM       svchost ex QUERY INFORMATION       C:WINDOWS\SYSTEM32\       SUCCESS       Options: Open Access: 000         219       948.08 AM       svchost ex QUERY INFORMATION       C:WINDOWS\SYSTEM32\DRIVERS\       SUCCESS       Options: Open Access: 000         219       948.08 AM       svchost ex QUERY INFORMATION       C:WINDOWS\WINSSS\       SUCCESS       Options: Open Access: 000<	207	9:48:08 AM	🔲 svehostlex	OPEN	C:\MAR\	SUCCESS	Options: Open Access: 000	
209       948.08 AM       evchost.ex DDEN       C:MAR\BIN\       SUCCESS         219       948.08 AM       evchost.ex DEN       C:MAR\BIN\       SUCCESS         219       948.08 AM       evchost.ex OUERY INFORMATION       C:MAR\BIN\       SUCCESS         219       948.08 AM       evchost.ex OUERY INFORMATION       C:MAR\BIN\       SUCCESS         219       948.08 AM       evchost.ex OUERY INFORMATION       C:WINDOWS\       SUCCESS         214       948.08 AM       evchost.ex OPEN       C:WINDOWS\       SUCCESS         215       948.08 AM       evchost.ex OPEN       C:WINDOWS\SYSTEM32\       SUCCESS         216       948.08 AM       evchost.ex OPEN       C:WINDOWS\SYSTEM32\       SUCCESS         217       948.08 AM       evchost.ex OPEN       C:WINDOWS\SYSTEM32\       SUCCESS         219       948.08 AM       evchost.ex CLOSE       C:WINDOWS\SYSTEM32\DRIVERS\       SUCCESS         219       948.08 AM       evchost.ex OUERY INFORMATION       C:WINDOWS\SYSTEM32\DRIVERS\       SUCCESS         219       948.08 AM       evchost.ex OUERY INFORMATION       C:WINDOWS\SYSTEM32\DRIVERS\       SUCCESS         219       948.08 AM       evchost.ex OUERY       C:WINDOWS\WINSXS\       SUCCESS<	208	9:48:08 AM	🔲 svehostlex	QUERY INFORMATION	C:\MAR\	SUCCESS	FileInternalInformation	
210       948.08 AM       evchost.ex	209	9:48:08 AM	🔲 svehostlex	CLOSE	C:\MAR\	SUCCESS		
211       948:08 AM       svchost.ex QUERY INFORMATION       C:WARNBIN\       SUCCESS       Fielnternalinformation         212       948:08 AM       svchost.ex QUERY INFORMATION       C:WARNBIN\       SUCCESS       Options: Open Access: 000         213       948:08 AM       svchost.ex QUERY INFORMATION       C:WINDOWS\       SUCCESS       Options: Open Access: 000         215       948:08 AM       svchost.ex QUERY INFORMATION       C:WINDOWS\SYSTEM32\       SUCCESS       Options: Open Access: 000         216       948:08 AM       svchost.ex QUERY INFORMATION       C:WINDOWS\SYSTEM32\       SUCCESS       Options: Open Access: 000         217       948:08 AM       svchost.ex QUERY INFORMATION       C:WINDOWS\SYSTEM32\DRIVERS\       SUCCESS       Options: Open Access: 000         219       948:08 AM       svchost.ex QUERY INFORMATION       C:WINDOWS\SYSTEM32\DRIVERS\       SUCCESS       Options: Open Access: 000         219       948:08 AM       svchost.ex QUERY INFORMATION       C:WINDOWS\SYSTEM32\DRIVERS\       SUCCESS       Options: Open Access: 000         229       948:08 AM       svchost.ex QUERY INFORMATION       C:WINDOWS\SYSTEM32\DRIVERS\       SUCCESS       Options: Open Access: 000         229       948:08 AM       svchost.ex QUERY INFORMATION       C:WINDOWS\WINSXS\	210	9:48:08 AM	🔲 svehostlex	OPEN	C:\MAR\BIN\	SUCCESS	Options: Open Access: 000	
212       9.48:08 AM       svchost.ex CLOSE       C:\/WINDOWS\       SUCCESS         213       9.48:08 AM       svchost.ex QUERY INFORMATION       C:\/WINDOWS\       SUCCESS         214       9.48:08 AM       svchost.ex QUERY INFORMATION       C:\/WINDOWS\       SUCCESS         215       9.48:08 AM       svchost.ex QUERY INFORMATION       C:\/WINDOWS\SYSTEM32\       SUCCESS         216       9.48:08 AM       svchost.ex QUERY INFORMATION       C:\/WINDOWS\SYSTEM32\       SUCCESS         217       9.48:08 AM       svchost.ex QUERY INFORMATION       C:\/WINDOWS\SYSTEM32\       SUCCESS         219       9.48:08 AM       svchost.ex QUERY INFORMATION       C:\/WINDOWS\SYSTEM32\DRIVERS\       SUCCESS         219       9.48:08 AM       svchost.ex QUERY INFORMATION       C:\/WINDOWS\SYSTEM32\DRIVERS\       SUCCESS         219       9.48:08 AM       svchost.ex QUERY INFORMATION       C:\/WINDOWS\SYSTEM32\DRIVERS\       SUCCESS         221       9.48:08 AM       svchost.ex QUERY       C:\/WINDOWS\SWINSXS\       SUCCESS       Options: Open Access: 000         222       9.48:08 AM       svchost.ex QUERY       C:\/WINDOWS\WINSXS\       SUCCESS       Options: Open Access: 000         224       9.48:08 AM       svchost.ex QUERY       C:\/WIND	211	9:48:08 AM	🔲 svehostlex	QUERY INFORMATION	C:\MAR\BIN\	SUCCESS	FileInternalInformation	
213       9.48:08 AM       svchostex OPEN       C:\/\/INDOWS\       SUCCESS       Options: Open Access: 000         214       9.48:08 AM       svchostex CLOSE       C:\//INDOWS\       SUCCESS       Options: Open Access: 000         215       9.48:08 AM       svchostex OPEN       C:\//INDOWS\SYSTEM32\       SUCCESS       Options: Open Access: 000         217       9.48:08 AM       svchostex OPEN       C:\//INDOWS\SYSTEM32\       SUCCESS       Options: Open Access: 000         218       9.48:08 AM       svchostex OPEN       C:\//INDOWS\SYSTEM32\DRIVERS\       SUCCESS       Options: Open Access: 000         219       9.48:08 AM       svchostex OPEN       C:\//INDOWS\SYSTEM32\DRIVERS\       SUCCESS       Options: Open Access: 000         220       9.48:08 AM       svchostex CLOSE       C:\//INDOWS\SYSTEM32\DRIVERS\       SUCCESS       Options: Open Access: 000         2219       9.48:08 AM       svchostex CLOSE       C:\//INDOWS\SYSTEM32\DRIVERS\       SUCCESS       Options: Open Access: 000         222       9.48:08 AM       svchostex CLOSE       C:\//INDOWS\V/INSXS\       SUCCESS       Options: Open Access: 000         223       9.48:08 AM       svchostex QUERY INFORMATION       C:\//INDOWS\V/INSXS\       SUCCESS       Options: Open Access: 000	212	9:48:08 AM	📰 svehostlex	CLOSE	C:\MAR\BIN\	SUCCESS		
214       9.48/08 AM       svchost ex QUERY INFORMATION       C:\WINDOWS\\       SUCCESS       FileInternalInformation         215       9.48/08 AM       svchost ex QUERY INFORMATION       C:\WINDOWS\SYSTEM32\       SUCCESS       Dptions: 0.pen Access: 000         217       9.48/08 AM       svchost ex QUERY INFORMATION       C:\WINDOWS\SYSTEM32\       SUCCESS       Dptions: 0.pen Access: 000         218       9.48/08 AM       svchost ex QUERY INFORMATION       C:\WINDOWS\SYSTEM32\DIVERSI       SUCCESS       Dptions: 0.pen Access: 000         219       9.48/08 AM       svchost ex QUERY INFORMATION       C:\WINDOWS\SYSTEM32\DIVERSI       SUCCESS       Dptions: 0.pen Access: 000         220       9.48/08 AM       svchost ex QUERY INFORMATION       C:\WINDOWS\SYSTEM32\DIVERSI       SUCCESS       Options: 0.pen Access: 000         221       9.48/08 AM       svchost ex QUERY INFORMATION       C:\WINDOWS\WINSXS\       SUCCESS       Options: 0.pen Access: 000         222       9.48/08 AM       svchost ex QUERY INFORMATION       C:\WINDOWS\WINSXS\       SUCCESS       Options: 0.pen Access: 000         223       9.48/08 AM       svchost ex QUERY INFORMATION       C:\WINDOWS\WINSXS\       SUCCESS       Options: 0.pen Access: 000         225       9.48/08 AM       svchost ex QUERY INFORMATION <td>213</td> <td>9:48:08 AM</td> <td>📰 svehostlex</td> <td> OPEN</td> <td>C:\WINDOWS\</td> <td>SUCCESS</td> <td>Options: Open Access: 000</td> <td></td>	213	9:48:08 AM	📰 svehostlex	OPEN	C:\WINDOWS\	SUCCESS	Options: Open Access: 000	
215       9.48/08 AM       svchost.ex OPEN       C:\/\/IND0WS\SYSTEM32\       SUCCESS         216       9.48/08 AM       svchost.ex OPEN       C:\/\/IND0WS\SYSTEM32\       SUCCESS         217       9.48/08 AM       svchost.ex OLOSE       C:\/\/IND0WS\SYSTEM32\       SUCCESS         218       9.48/08 AM       svchost.ex OPEN       C:\//IND0WS\SYSTEM32\DRIVERS\       SUCCESS         219       9.48/08 AM       svchost.ex OPEN       C:\//IND0WS\SYSTEM32\DRIVERS\       SUCCESS         220       9.48/08 AM       svchost.ex QUERY INFORMATION       C:\//IND0WS\SYSTEM32\DRIVERS\       SUCCESS         220       9.48/08 AM       svchost.ex QUERY INFORMATION       C:\//IND0WS\SYSTEM32\DRIVERS\       SUCCESS         221       9.48/08 AM       svchost.ex QUERY INFORMATION       C:\//IND0WS\SYSTEM32\DRIVERS\       SUCCESS         222       9.48/08 AM       svchost.ex QUERY INFORMATION       C:\//IND0WS\S/INSXS\       SUCCESS         223       9.48/08 AM       svchost.ex QUERY INFORMATION       C:\//IND0WS\S/INSXS\       SUCCESS         224       9.48/08 AM       svchost.ex QLOSE       C:\//IND0WS\S/INSXS\       SUCCESS         225       9.48/08 AM       svchost.ex QLOSE       C:\//IND0WS\S/INSXS\S86_MICRO       SUCCESS	214	9:48:08 AM	📰 svehostlex	QUERY INFORMATION	C:\WINDOWS\	SUCCESS	FileInternalInformation	
216       9:48:08 AM       svchost.ex 0PEN       C:\WINDOWS\SYSTEM32\       SUCCESS       Options: Open Access: 000         217       9:48:08 AM       svchost.ex 0LOSE       C:\WINDOWS\SYSTEM32\       SUCCESS       Options: Open Access: 000         219       9:48:08 AM       svchost.ex 0LOSE       C:\WINDOWS\SYSTEM32\       SUCCESS       Options: Open Access: 000         219       9:48:08 AM       svchost.ex 0LOSE       C:\WINDOWS\SYSTEM32\DRIVERS\       SUCCESS       Options: Open Access: 000         220       9:48:08 AM       svchost.ex 0DEN       C:\WINDOWS\SYSTEM32\DRIVERS\       SUCCESS       Options: Open Access: 000         221       9:48:08 AM       svchost.ex 0LOSE       C:\WINDOWS\SYSTEM32\DRIVERS\       SUCCESS       Options: Open Access: 000         222       9:48:08 AM       svchost.ex 0LOSE       C:\WINDOWS\WINSXS\       SUCCESS       Options: Open Access: 000         224       9:48:08 AM       svchost.ex 0LOSE       C:\WINDOWS\WINSXS\       SUCCESS       Options: Open Access: 000         225       9:48:08 AM       svchost.ex 0LOSE       C:\WINDOWS\WINSXS\       SUCCESS       Options: Open Access: 000         226       9:48:08 AM       svchost.ex 0LOSE       C:\WINDOWS\WINSXS\%86_MICRO       SUCCESS       Options: Open Access: 000 <td>215</td> <td>9:48:08 AM</td> <td>📰 svchost.ex</td> <td> CLOSE</td> <td>C:\WINDOWS\</td> <td>SUCCESS</td> <td></td> <td></td>	215	9:48:08 AM	📰 svchost.ex	CLOSE	C:\WINDOWS\	SUCCESS		
217       9.48.08 AM       svchost.ex QUERY INFORMATION       C:WINDOWS/SYSTEM32/       SUCCESS         218       9.48.08 AM       svchost.ex QUERY INFORMATION       C:WINDOWS/SYSTEM32/       SUCCESS         219       9.48.08 AM       svchost.ex QUERY INFORMATION       C:WINDOWS/SYSTEM32/DRIVERS/       SUCCESS         220       9.48.08 AM       svchost.ex QUERY INFORMATION       C:WINDOWS/SYSTEM32/DRIVERS/       SUCCESS       Options: Open Access: 000         221       9.48.08 AM       svchost.ex QUERY INFORMATION       C:WINDOWS/SYSTEM32/DRIVERS/       SUCCESS       Options: Open Access: 000         222       9.48.08 AM       svchost.ex QPEN       C:WINDOWS/WINSXS/       SUCCESS       Options: Open Access: 000         223       9.48.08 AM       svchost.ex QPEN       C:WINDOWS/WINSXS/       SUCCESS       Options: Open Access: 000         225       9.48.08 AM       svchost.ex QUERY INFORMATION       C:WINDOWS/WINSXS/W86_MICRO       SUCCESS       Options: Open Access: 000         226       9.48.08 AM       svchost.ex QUERY INFORMATION       C:WINDOWS/WINSXS/W86_MICRO       SUCCESS       Options: Open Access: 000         227       9.48.08 AM       svchost.ex CLOSE       C:WINDOWS/WINSXS/W86_MICRO       SUCCESS       Options: Open Access: 000         230 </td <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> <td></td>	216	9:48:08 AM	📰 svchost.ex	OPEN	C:\WINDOWS\SYSTEM32\	SUCCESS	Options: Open Access: 000	
218       9:48:08 AM       svchost.ex CLOSE       C:W/INDOWS/SYSTEM32/DRIVERS/       SUCCESS         219       9:48:08 AM       svchost.ex QUERY INFORMATION       C:W/INDOWS/SYSTEM32/DRIVERS/       SUCCESS       Options: Open Access: 000         211       9:48:08 AM       svchost.ex CLOSE       C:W/INDOWS/SYSTEM32/DRIVERS/       SUCCESS       Options: Open Access: 000         222       9:48:08 AM       svchost.ex CLOSE       C:W/INDOWS/SYSTEM32/DRIVERS/       SUCCESS       Options: Open Access: 000         223       9:48:08 AM       svchost.ex DPEN       C:W/INDOWS/WINSXS/       SUCCESS       Options: Open Access: 000         224       9:48:08 AM       svchost.ex QUERY INFORMATION       C:W/INDOWS/WINSXS/       SUCCESS       Options: Open Access: 000         225       9:48:08 AM       svchost.ex QUERY INFORMATION       C:W/INDOWS/WINSXS/       SUCCESS       Options: Open Access: 000         226       9:48:08 AM       svchost.ex QUERY INFORMATION       C:W/INDOWS/WINSXS/X86_MICRO       SUCCESS       Options: Open Access: 000         227       9:48:08 AM       svchost.ex CLOSE       C:W/INDOWS/WINSXS/X86_MICRO       SUCCESS       Options: Open Access: 000         228       9:48:08 AM       svchost.ex CLOSE       C:W/INDOWS/WINSXS/X86_MICRO       SUCCESS <td< td=""><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>FileInternalInformation</td><td></td></td<>	217	9:48:08 AM	📰 svchost.ex	QUERY INFORMATION	C:\WINDOWS\SYSTEM32\	SUCCESS	FileInternalInformation	
219       9:48:08 AM       svchost.ex 0PEN       C:\WIND0W\$\SYSTEM32\DRIVERS\       SUCCESS       Options: 0pen Access: 000         220       9:48:08 AM       svchost.ex 0LOSE       C:\WIND0W\$\SYSTEM32\DRIVERS\       SUCCESS       Options: 0pen Access: 000         221       9:48:08 AM       svchost.ex 0LOSE       C:\WIND0W\$\SYSTEM32\DRIVERS\       SUCCESS       Options: 0pen Access: 000         222       9:48:08 AM       winlogon.e READ       C:       SUCCESS       Options: 0pen Access: 000         223       9:48:08 AM       svchost.ex 0PEN       C:\WIND0W\$\WINSXS\       SUCCESS       Options: 0pen Access: 000         224       9:48:08 AM       svchost.ex 0PEN       C:\WIND0W\$\WINSXS\       SUCCESS       Options: 0pen Access: 000         225       9:48:08 AM       svchost.ex 0PEN       C:\WIND0W\$\WINSXS\       SUCCESS       Options: 0pen Access: 000         226       9:48:08 AM       svchost.ex 0PEN       C:\WIND0W\$\WINSXS\X86_MICR0       SUCCESS       Options: 0pen Access: 000         229       9:48:08 AM       svchost.ex CLOSE       C:\WIND0W\$\WINSXS\X86_MICR0       SUCCESS       Options: 0pen Access:         230       9:48:08 AM       winlogon.e READ       C:       SUCCESS       Options: 0pen Access:         231 </td <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></td> <td></td>	218	9:48:08 AM	📰 svchost.ex	CLOSE	C:\WINDOWS\SYSTEM32\	SUCCESS		
220       9:48:08 AM       svchost.ex       QUERY INFORMATION       C:\/WINDOWS\SYSTEM32\DRIVERS\       SUCCESS       FileInternalInformation         221       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       OPEN       C:\/WINDOWS\WINSXS\       SUCCESS       Options: Open Access: 000         225       9:48:08 AM       svchost.ex       OPEN       C:\/WINDOWS\WINSXS\       SUCCESS       Options: Open Access: 000         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       Options: Open Access: 000         228       9:48:08 AM       svchost.ex       CLOSE       C:\/WINDOWS\WINSXS\X86_MICRO       SUCCESS       Options: Overwritelf Access:         229       9:48:08 AM       svchost.ex       CREATE       C:\/WINDOWS\WINSXS\X86_MICRO       SUCCESS       Offset: 4620288 Length: 4096       0ptions: Overwritelf Access:	219	9:48:08 AM	📰 svchost.ex	OPEN	C:\WINDOWS\SYSTEM32\DRIVERS\	SUCCESS	Options: Open Access: 000	
221       9.48:08 AM       svchost.ex CLOSE       C:\WINDOWS\SYSTEM32\DRIVERS\       SUCCESS         222       9.48:08 AM       winlogon.e READ       C:\WINDOWS\WINSXS\       SUCCESS       Options: Open Access: 000         223       9.48:08 AM       svchost.ex QUERY INFORMATION       C:\WINDOWS\WINSXS\       SUCCESS       Options: Open Access: 000         224       9.48:08 AM       svchost.ex QUERY INFORMATION       C:\WINDOWS\WINSXS\       SUCCESS       Options: Open Access: 000         225       9.48:08 AM       svchost.ex QUERY INFORMATION       C:\WINDOWS\WINSXS\X86_MICRO       SUCCESS       Options: Open Access: 000         226       9.48:08 AM       svchost.ex QUERY INFORMATION       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       Options: Open Access: 000         229       9.48:08 AM       svchost.ex CREATE       C:\WINDOWS\WINSXS\X86_MICRO       SUCCESS       Options: Overwritelf Access:         230       9.48:08 AM       winlogon.e READ       C:       SUCCESS       Offset: 4630564 Length: 4096         233       9.48:08 AM       winlogon.e READ       C:       SUCCESS       Offset: 4653056 Length: 4096	220	9:48:08 AM	📰 svchost.ex	QUERY INFORMATION	C:\WINDOWS\SYSTEM32\DRIVERS\	SUCCESS	FileInternalInformation	
222       9.48:08 AM       winlogon.e READ       C:       SUCCESS       Offset: 4648960 Length: 4096         223       9.48:08 AM       svchost.ex QUERY INFORMATION       C:\/\VINDOWS\\VINSXS\       SUCCESS       Dptions: Open Access: 000         224       9.48:08 AM       svchost.ex QUERY INFORMATION       C:\/VINDOWS\\VINSXS\       SUCCESS       FileInternalInformation         225       9.48:08 AM       svchost.ex OPEN       C:\/VINDOWS\\VINSXS\\S86_MICRO       SUCCESS       Options: Open Access: 000         226       9.48:08 AM       svchost.ex OPEN       C:\/VINDOWS\\VINSXS\\X86_MICRO       SUCCESS       Options: Open Access: 000         227       9.48:08 AM       svchost.ex QUERY INFORMATION       C:\/VINDOWS\\VINSXS\X86_MICRO       SUCCESS       Options: Open Access: 000         228       9.48:08 AM       svchost.ex CLOSE       C:\/VINDOWS\\VINSXS\X86_MICRO       SUCCESS       Options: Overwritelf Access:         230       9.48:08 AM       winlogon.e READ       C:       SUCCESS       Offset: 4650288 Length: 4096         231       9.48:08 AM       winlogon.e READ       C:       SUCCESS       Offset: 308864 Length: 4096         233       9.48:08 AM       winlogon.e READ       C:       SUCCESS       Offset: 30480536 Length: 4096 <tr< td=""><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></td><td></td></tr<>	221	9:48:08 AM	🔲 svchost.ex	CLOSE	C:\WINDOWS\SYSTEM32\DRIVERS\	SUCCESS		
223       9:48:08 AM       svchost.ex 0PEN       C:\WIND0WS\WINSXS\       SUCCESS       Options: 0pen Access: 000         224       9:48:08 AM       svchost.ex QUERY INFORMATION       C:\WIND0WS\WINSXS\       SUCCESS       FileInternalInformation         225       9:48:08 AM       svchost.ex CLOSE       C:\WIND0WS\WINSXS\       SUCCESS       Options: 0pen Access: 000         226       9:48:08 AM       svchost.ex 0PEN       C:\WIND0WS\WINSXS\       SUCCESS       Options: 0pen Access: 000         227       9:48:08 AM       svchost.ex 0PEN       C:\WIND0WS\WINSXS\X86_MICRO       SUCCESS       Options: 0pen Access: 000         228       9:48:08 AM       svchost.ex 0PEN       C:\WIND0WS\WINSXS\X86_MICRO       SUCCESS       Options: 0pen Access: 000         229       9:48:08 AM       svchost.ex CLOSE       C:\WIND0WS\WINSXS\X86_MICRO       SUCCESS       Options: 0verwitelf 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: 3108864 Length: 4096         233       9:48:08 AM       winlogon.e READ       C:       SUCCESS       Offset: 34623056 Length: 4096         234       9:48:	222	9:48:08 AM	📃 winlogon.e	READ	C:	SUCCESS	Offset: 4648960 Length: 4096	
224       9:48:08 AM       svchost.ex QUERY INFORMATION       C:\WINDOWS\WINSXS\       SUCCESS       FileInternalInformation         225       9:48:08 AM       svchost.ex OLOSE       C:\WINDOWS\WINSXS\       SUCCESS       Options: Open Access: 000         227       9:48:08 AM       svchost.ex QUERY INFORMATION       C:\WINDOWS\WINSXS\X86_MICRO       SUCCESS       Options: Open Access: 000         228       9:48:08 AM       svchost.ex QUERY INFORMATION       C:\WINDOWS\WINSXS\X86_MICRO       SUCCESS       Options: Open Access: 000         229       9:48:08 AM       svchost.ex QUERY INFORMATION       C:\WINDOWS\WINSXS\X86_MICRO       SUCCESS       Options: Overwritelf Access:         230       9:48:08 AM       svchost.ex CREATE       C:\WINDOWS\Prefetch\FILEMON.EX       SUCCESS       Options: Overwritelf Access:         231       9:48:08 AM       winlogon.e READ       C:       SUCCESS       Offset: 4055040 Length: 4096         233       9:48:08 AM       winlogon.e READ       C:       SUCCESS       Offset: 3108864 Length: 4096         233       9:48:08 AM       winlogon.e READ       C:       SUCCESS       Offset: 342336 Length: 4096         234       9:48:08 AM       winlogon.e READ       C:       SUCCESS       Offset: 4653056 Length: 4096       Ch	223	9:48:08 AM	📰 svchost.ex	OPEN	C:\WINDOWS\WINSXS\	SUCCESS	Options: Open Access: 000	
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       Options: Open Access: 000         228       9:48:08 AM       svchost.ex CLOSE       C:\WINDOWS\WINSXS\X86_MICRO       SUCCESS       Options: Overwritelf Access:         230       9:48:08 AM       svchost.ex CREATE       C:\WINDOWS\Prefetch\FILEMON.EX       SUCCESS       Options: Overwritelf Access:         231       9:48:08 AM       winlogon.e READ       C:       SUCCESS       Offset: 4620288 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         234       9:48:08 AM       winlogon.e READ       C:       SUCCESS       Offset: 4653056 Length: 4096         235       9:48:08 AM       winlogon.e READ	224	9:48:08 AM	📰 svchost.ex	QUERY INFORMATION	C:\WINDOWS\WINSXS\	SUCCESS	FileInternalInformation	
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       Options: Overwritelf Access:         230       9:48:08 AM       svchost.ex CREATE       C:\WINDOWS\Prefetch\FILEMON.EX SUCCESS       Options: Overwritelf Access:         231       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: 3423366 Length: 4096         234       9:48:08 AM       winlogon.e READ       C:       SUCCESS       Offset: 4655056 Length: 4096         235       9:48:08 AM       winlogon.e READ       C:       SUCCESS       Offset: 4655056 Length: 4096         234       9:48:08 AM       winlogon.e DIRECTORY       C:\WINDOWS\system32	225	9:48:08 AM	📰 svchost.ex	CLOSE	C:\WINDOWS\WINSXS\	SUCCESS		
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       Options: Overwritelf 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: 4620288 Length: 4096         232       9:48:08 AM       winlogon.e       READ       C:       SUCCESS       Offset: 4055040 Length: 4096         233       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       Public Safety       Sécurité publique       C:\WINDOWS\system32       Change Notify       Public Safety       Sécurité publique       C:\WINDOWS\System32       Change Notify       Public Safety       Sécurité publique       C:\WINDOWS\System44       C:\WINDOWS\System44 <t< td=""><td>226</td><td>9:48:08 AM</td><td>🔲 svchost.ex</td><td> OPEN</td><td>C:\WINDOWS\WINSXS\X86_MICRO</td><td>SUCCESS</td><td>Options: Open Access: 000</td><td></td></t<>	226	9:48:08 AM	🔲 svchost.ex	OPEN	C:\WINDOWS\WINSXS\X86_MICRO	SUCCESS	Options: Open Access: 000	
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: Overwritelf 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         236       9:49:08 AM       Winlogon.e DIRECTORY       C:\WINDOWS\System32       Change Notify         237       9:49:08 AM       Winlogon.e DIRECTORY       C:\WINDOWS\system32       Change Notify         238       9:49:08 AM       Winlogon.e DIRECTORY       C:\WINDOWS\System32       Change Notify         239       9:49:08 AM       Winlogon.e DIRECTORY	227	9:48:08 AM	🔲 svchost.ex	QUERY INFORMATION	C:\WINDOWS\WINSXS\X86_MICRO	SUCCESS	FileInternalInformation	
229       9:48:08 AM       svchost.ex CREATE       C:\WINDOWS\Prefetch\FILEMON.EX SUCCESS       Options: Overwritelf 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         236       9:40:00 AW       Winlogon.e DIRECTORY       C:\WINDOWS\System32       Change Notify         237       9:40:00 AW       Winlogon.e DIRECTORY       C:\WINDOWS\System32       Change Notify         238       9:40:00 AW       Winlogon.e DIRECTORY       C:\WINDOWS\System32       Change Notify         239       9:40:00 AW       Winlogon.e DIRECTORY       C:\WINDOWS\System42       CHORECTORY       C:WINDOWS\System32       Change Notify         W	228	9:48:08 AM	🔲 🛄 svchost.ex	CLOSE	C:\WINDOWS\WINSXS\X86_MICRO	SUCCESS		
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         236       9:40:00 AM       Winlogon.e DIRECTORY       C:\/WINDOWS\system32       Change Notify         236       9:40:00 AM       Winlogon.e DIRECTORY       C:\/WINDOWS\system32       Change Notify         237       9:40:00 AM       Winlogon.e DIRECTORY       C:\/WINDOWS\System32       Change Notify         238       9:40:00 AM       Winlogon.e DIRECTORY       C:\/WINDOWS\System32       Change Notify         239       9:40:00 AM       Winlogon.e DIRECTORY       C:\/WINDOWS\System32       Change Notify         239       9:40:00 AM       Winlogon.e AF       CAN	229	9:48:08 AM	🔲 🛄 svchost.ex	CREATE	C:\WINDOWS\Prefetch\FILEMON.EX	SUCCESS	Options: Overwritelf Access:	
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:       SUCCESS       Offset: 4653056 Length: 4096         236       9:40:00 AM       winlogon.e DIRECTORY       C:\WINDOWS\system32       Change Notify         237       9:40:00 AM       Securité publique       C:\WINDOWS\system32       Change Notify         237       9:40:00 AM       Securité publique       C:\WINDOWS\system32       Change Notify         238       9:40:00 AM       Securité publique       C:\WINDOWS\System32       Change Notify         239       9:40:00 AM       Securité publique       C:WINDOWS\System32       Change Notify         239       9:40:00 AM       Securité public       Securité public       Securité public	230	9:48:08 AM	winlogon.e	READ	C:	SUCCESS	Offset: 4620288 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: 3342336 Length: 4096         235       9:48:08 AM       winlogon.e DIRECTORY       C:       SUCCESS       Offset: 4653056 Length: 4096         236       9:48:08 AM       winlogon.e DIRECTORY       C:\WINDOWS\system32       Change Notify         236       9:40:00 AM       Securité publique       C:\WINDOWS\System32       Change Notify         237       9:40:00 AM       Securité publique       C:WINDOWS\System32       Change Notify         237       9:40:00 AM       Securité publique       C:WINDOWS\System32       Change Notify         238       9:40:00 AM       Securité publique       C:WINDOWS\System32       Change Notify         239       9:40:00 AM       Securité publique       C:WINDOWS\System32       Change Notify	231	9:48:08 AM	winlogon.e	READ	C:	SUCCESS	Offset: 4055040 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         236       9:40:09 AM       Securité publique       C:\WINDOWS\System32       Change Notify         237       9:40:09 AM       Securité publique       C:\WINDOWS\System32       Change Notify         237       9:40:09 AM       Securité publique       C:\WINDOWS\System32       Change Notify         238       0:40:09 AM       Securité publique       C:WINDOWS\System32       Change Notify	232	9:48:08 AM	winlogon.e	READ	C:	SUCCESS	Offset: 3108864 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         236       9:40:00 AW       Securité publique       C:\WINDOWS\System32       Change Notify         Public Safety       Sécurité publique       C:\WINDOWS\Ductory       C:\WINDOWS\Ductory       C:\WINDOWS\Ductory         Canada       Canada       CA       C:\WINDOWS\Ductory       C:\WINDOWS\Ductory       C:\WINDOWS\Ductory	233	9:48:08 AM	winlogon.e.	READ	C:	SUCCESS	Offset: 3342336 Length: 4096	
235     9:48:08 AM     → winlogon.e DIRECTORY     C:\WINDOWS\system32     Change Notify       235     9:40:09 AM     → Winlogon.e DIRECTORY     C:\WINDOWS\System32     Change Notify       236     9:40:09 AM     → Winlogon.e DIRECTORY     C:\WINDOWS\System32     Change Notify       237     9:40:09 AM     → Winlogon.e DIRECTORY     C:\WINDOWS\System32     Change Notify       238     Public Safety     Sécurité publique     CA     Change Notify       Canada     64     Change Notify     Canada	234	9:48:08 AM	winlogon.e.	READ	C:	SUCCESS	Offset: 4653056 Length: 4096	-
Public Safety Sécurité publique 64 Canada	235	9:48:08 AM	winlogon.e.	DIRECTORY	C:\WINDOWS\system32		Change Notify	
Canada Canada 64 Canada			Cofoty Of		P.()) ///////////////////////////////////	PHPPPP	Disatan A-	104
		Canada	a Ca	anada	64		C	anada



#### **REGMON.EXE – Registry Monitor**

🗱 Registry Monitor - Sysinternals: www.sysinternals.com

File Edit Options Help

#### 🖬 🚘 | 🍳 🕮 😰 🥙 | 😽 🚆 | 🚧 🏄

#	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	🔲 Isass	OpenKey	HKLM\SECURITY\Policy	SUCCE	Access: 0x	
840	1.04729426	🔲 Isass	OpenKey	HKLM\SECURITY\Policy\SecDesc	SUCCE	Access: 0x	
841	1.04730260	🔲 Isass	QueryValue	HKLM\SECURITY\Policy\SecDesc\(D	. BUFFE		
842	1.04731524	🔲 Isass	CloseKey	HKLM\SECURITY\Policy\SecDesc	SUCCE		
843	1.04732919	🔲 Isass	OpenKey	HKLM\SECURITY\Policy\SecDesc	SUCCE	Access: 0x	
844	1.04733670	🔲 Isass	QueryValue	HKLM\SECURITY\Policy\SecDesc\(D	. SUCCE	NONE	
845	1.04734600	🔲 Isass	CloseKey	HKLM\SECURITY\Policy\SecDesc	SUCCE		
846	1.04768908	🛄 Isass	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	
	7 7777/179	Custo	CloseKou	HKLMS Susters' CurrentControlS of Control	CHICCE		

65



Public Safety Sécurité publique Canada



\_ 7 🛛

^



#### TCPVIEW.EXE – TCP connections



\_ 7

#### 📩 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
🗂 Isass.exe:668	UDP	0.0.0.0:500	×.×	
🗂 Isass.exe:668	UDP	0.0.0.0:4500	×.×	
🗂 svohostlexe:1096	UDP	10.0.2.15:1900	×.×	
🗂 svehostlexe:1096	UDP	127.0.0.1:1900	×.×	
🗂 svohostlexe:892	TCP	0.0.0.0:135	0.0.0.0:0	LISTENING
🗂 svehost.exe:928	UDP	10.0.2.15:123	×.×	
🗂 svohostlexe:928	UDP	127.0.0.1:123	×.×	
🗂 svchost.exe:928	UDP	127.0.0.1:1043	×.×	
🗂 svohostlexe:980	UDP	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	×.× ·	





SPER	RegShot -	
R	egshot 1.8.2	
Cor	Plain TXT C HTML document	
Г С:	Scan dir1[;dir2;;dir nn]: WINDOWS Clear	
Ou	🖡 - res - Notepad	×
C	File Edit Format View Help	
Ad	Keys added:1	^
Γ	HKU\S-1-5-21-527237240-436374069-839522115-1003\Software\Sysinternals\A	
	values added:3	
	Values modified:6	Mill
	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 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	



0

Public Safety Canada Sécurité publique Canada







## 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.











🖎 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]		
<pre>[HKEY_LOCAL_MACHINE\HARDWARE\ACPI\DSDT\UBOX\UBOXBIOS\00000002] "00000000"=hex:44,53,44,54,3f,10,00,00,01,aa,56,42,4f,58,20,20,56,42,4f,58,4 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 45,21,46,5b,81,0b,44,42,47,30,01,44,48,45,31,08,5b,81,0b,44,42,47,30,02,44,48</pre>	2.\	







## **AUTORUNS.EXE**

📨 Autoruns [JAMIE-13F427558\jamie] - Sysinternals: www.sysinternals.com 🛛 📮 🗖 🔀						
File Entry Options User Help						
🔚 Boot Execute 🛛 🔚 Image Hijacks 🛛 🕥 AppInit 👘 🕥 KnownDLLs 👘	🏨 Winlogon 📄					
🥂 🛸 Winsock Providers 👘 🍓 Print Monitors 👘 😻 LSA Providers 👘 👰 Netwo	ork Providers					
📨 Everything 🛛 🆽 Logon 🛛 🚼 Explorer 🛛 🥭 Internet Explorer 🛛 🙆 Scheduled Tasks 🛛 🎇 Service	es 📕 Drivers					
Autorun Entry Description Publisher Image Path						
#KLM\System\CurrentControlSet\Control\Terminal Server\Wds\rdpwd\StartupPrograms	_					
🔽 🔄 rdpclip RDP Clip Monitor Microsoft Corporation c:\windows\syste	m32\rdpcl					
HKLM\S0FTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Userinit						
🔽 🔄 C:\WINDOWS Userinit Logon Application 🛛 Microsoft Corporation 👘 c:\windows\syste	m32\useri					
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell						
🔽 😼 Explorer.exe Windows Explorer Microsoft Corporation c:\windows\explo	prer.exe					
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run						
Microsoft Corporation c:\windows\ime\i IME	.mjp8_1\im					
MSPY2002 c:\windows\syste	m32\ime\					
🔽 😼 PHIME2002A 🛛 ??????? 2002a 🦳 Microsoft Corporation c:\windows\syste	:m32\ime\					
🔽 🛃 PHIME2002AS ??????? 2002a 🛛 Microsoft Corporation c:\windows\syste	:m32\ime\ 🔽					
Ready.						
Public Safety Sécurité publique	0					







# 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	Ø	212 K
smss.exe	548	Console	Ø	372 K
csrss.exe	596	Console	Ø	4,128 K
winlogon.exe	620	Console	Ø	4,064 K
services.exe	664	Console	Ø	3,896 K
lsass.exe	676	Console	Ø	1,320 K
svchost.exe	824	Console	Ø	4.532 K
svchost.exe	904	Console	Ø	3,980 K
svchost.exe	940	Console	Ø	16,964 K
svchost.exe	984	Console	Ø	2,776 K
svchost.exe	1044	Console	Ø	4.316 K
spoolsv.exe	1296	Console	Ø	4.356 K
alg.exe	1740	Console	Ø	3,316 K
explorer.exe	1860	Console	Ø	14,980 K
VBoxService.exe	1916	Console	Ø	2,248 K
wscntfy.exe	2004	Console	Ø	2,124 K
cmd.exe	444	Console	Ø	2.464 K
tasklist.exe	380	Console	Ø	4,152 K
wmiprvse.exe	1960	Console	Ø	5,436 K





- 0


### SC.EXE – Service Control command line utility





Canada





#### 🛋 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	Ø	Ø	1	Ø	Ø	16	Ø
System	4	8	54	149	1876	212	Ø
ัรพรร	548	11	3	21	3800	372	164
CSPSS	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
alq	1740	8	5	98	32424	3316	1120
lsass	676	9	19	336	40944	1376	3668
explorer	1860	8	9	316	63960	16944	8636
ćmd	1516	8	1	31	30180	2484	2004
pslist	1820	13	2	74	30108	2344	1032
VBoxService	1916	8	4	30	31068	2248	768
C-\\\							



- 🗆 X



#### 🔤 Command Prompt

Microsoft Windows XP [Version 5.1.2600] <c> Copyright 1985-2001 Microsoft Corp.</c>
C:\>psservice 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 i s stopped, programs that use administrative alerts will not receive them. If thi s service is disabled, any services that explicitly depend on it will fail to st
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 WIN32_OWN_PROCESS START_TYPE : 3 DEMAND_START ERROR_CONTROL : 1 NORMAL BINARY_PATH_NAME : C:\WINDOWS\System32\alg.exe LOAD_ORDER_GROUP : TAG : 0





- 🗆 🗙





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







Canada

Canada

### 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

ev Comm	and Prompt			- 🗆 🗙
licrosof (C) Copy	t Windows XP [Versio right 1985-2001 Mice	on 5.1.2600] rosoft Corp.		
C:∖>nets	tat -an			
Active C	Connections			
Proto TCP TCP TCP UDP UDP UDP UDP UDP UDP	Local Address 0.0.0.0:135 0.0.0.0:445 127.0.0.1:1025 0.0.0.0:445 0.0.0.0:500 0.0.0.0:4500 127.0.0.1:123 127.0.0.1:1900	Foreign Address 0.0.0.0:0 0.0.0.0:0 0.0.0.0:0 *:* *:* *:* *:* *:*	State LISTENING LISTENING LISTENING	
::∖>_				
				-









Cor	nmand Prompt					- 🗆	×
Copyri http:/	ight 2000 by Fou //www.foundston	undst e.cor	tone, ] m	lnc.			
Pid 648 .exe	Process servterm	->	Port 23	Proto TCP	Path Z:\software\windows-based\servt-10\servt	erm	
892 4 4 1828	System System	-> -> ->	135 139 445 1025	TCP TCP TCP TCP			
0 0 0 6 48	System System System servterm	-> -> -> ->	123 137 138 445	UDP UDP UDP UDP UDP	Z:\software\windows-based\servt-10\servt	erm	
.exe 892 4 4 0 0 1828	System System System System	-> -> -> -> ->	500 1036 1042 1043 1900 4500	UDP UDP UDP UDP UDP UDP UDP			
C:\>_							-







#### 🔤 Command Prompt

~					▲	I
C: A A A A A A A A A A	∖>attrib SH SHR SHR SHR SHR SHR SHR SH	C:\AUTO C:\boot C:\CONF C:\IO.S C:\MSDO C:\MSDO C:\NTDE C:\ntld C:\page	EXEC.BAT ini IG.SYS YS S.SYS IECT.COM File.sys			
C:: U, U, D	∖>dir olume in olume Sen irectory	drive C rial Num] of C:\	has no label. ber is 2CE9-030	7		
05. 05. 05. 05. 05.	/12/2008 /12/2008 /12/2008 /12/2008 /15/2008 /12/2008 /15/2008	11:16 11:16 11:45 01:56 12:57 02:53 2 F 4 D	AM AM AM (DIR) PM (DIR) PM (DIR) PM (DIR) ile(s) ir(s) 84,053,6	0 AUTOEXEC.BAT 0 CONFIG.SYS Documents and S MAR Program Files WINDOWS 0 bytes 43,264 bytes free	ettings	
C:	<>_				-	
	+ Put Car	olic Safety nada	Sécurité publique Canada	80	Canadä	1







🐼 Command Prompt		- 🗆 🗙
Microsoft Windows XP [Version 5.1.2600] (C) Copyright 1985-2001 Microsoft Corp.		<b>^</b>
C:∖>md5sums .		
MD5sums 1.2 freeware for Win9x/ME/NT/2000/XP+ Copyright (C) 2001-2005 Jem Berkes - http://w Type md5sums -h for help	ww.pc-tools.net/	
[Path] / filename	MD5 sum	
[C:\] AUTOEXEC.BAT boot.ini CONFIG.SYS hklm.txt IO.SYS MSDOS.SYS NTDETECT.COM ntldr pagefile.sys	d41d8cd98f00b204e9800998ecf84 fa579938b0733b87066546afe9510 d41d8cd98f00b204e9800998ecf84 593d59056d827779fc05ac7d25a56 d41d8cd98f00b204e9800998ecf84 d41d8cd98f00b204e9800998ecf84 d41d8cd98f00b204e9800998ecf84 b2de3452de03674c6cec68b8c8ce7 9ec920f4179d45af3a6638a083d39 Unable to open!	127e 982c 127e 50bb 127e 427e 427e 7c78 7c85
C:\>		<b>_</b>









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







📼 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

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

<u>\\$\$\\$\$-20080623-072351.71></u>

- 🗆 🗙



#### Command Prompt

\*

T:\SS\SS-20080623-072351.71>fc /L /N ATTRIB.txt\SS-20080623-070953.82\ATTRIB.		
	-1	
Comparing files ATTRIB.txt and\SS-20080623-070953.82\ATTRIB.TXT		
$\frac{2}{2}$ Ado $\frac{1}{2}$		
848: H C:\Program Files\NetHeeting\N323CC.dll		
947: SHK C:\Frogram Files\NetHeating\Nsmsgs		
0.00 H $0.170$ $0.170$ $0.110$ $0.110$ $0.110$ $0.1120$ $0.1120$		
848: A C:\Program Files\NetMeeting\h323cc dll		
849: A C:\Program Files\NetMeeting\NS120.DLL		
XXXXX		
***** ATTRIB.txt		
4814: A C:\WINDOWS\PeerNet\sqlse20.dll		
4815: A C:\WINDOWS\Prefetch\200512.EXE-17CE5174.pf		
4816: AC:\WINDOWS\Prefetch\AGENTSVR.EXE-002E45AB.pf		
*****\\$\$-20080623-070953.82\ATTRIB.TXT		
4813: A C:\WINDOWS\PeerNet\sqlse20.dll	- 11	
4814: H C:\WINDOWS\Prefetch\HGENISVR.EXE=002E45HB.pf		
*****	- 11	
XXXXX ATTRIR tyt		
$4841:$ 0 C:\UINDOUS\Prefetch\MSIFXEC FXF-2F868C6F rf		
4842: A C:\VINDOVS\Prefetch\MSMSGS=013FAF85_nf		
4843: A C:\VINDOWS\Prefetch\MSOOBE_EXE=30411B02.nf		
*****\\$\$-20080623-070953.82\ATTRIB.TXT		
4839: A C:\WINDOWS\Prefetch\MSIEXEC.EXE-2F8A8CAE.pf		
4840: A C:\WINDOWS\Prefetch\MSOOBE.EXE-30411B02.pf		
****		
ACCOUNT AND A A A A A A A A A A A A A A A A A A		
4880: H C:WINDOWS\Prefetch\IHSKLISI.EXE-I0D94B23.pt		
4881: H G: WINDOWS \FFEFETCA\IHSKMGK.EKE=20256.55.pf 4992: 6 G: UINDOUS Profetch: TINTETE FETE VE_20PE0722f		
1002- H G-NHINDUWS NEETELCHNIINISEIF.EAE-37DF0/32.pr		
$\frac{1}{4979} = 0$		
4878: A C:\VINDOWS\Prefetch\TINTSFTP_FXF-39BF0732 nf		
***** ATTRIB.txt		nadä
10908: C:\WINDOWS\Debug		laua
10909: A C:\WINDOWS\Delete.bat	-1	
10910: A C:\WINDOWS\desktop.ini	•	

- 🗆 🗙





INTERNATIONAL - KDiff3							
File Edit Directory Movement Diffview Merge Window Settings Help							
🚰 ⊨ 🛋 ▼ ▲ ▼ ★ ▼ ★ ¥ A B C 🖤 🗆 123 💠 📑 🖬 ==							
A: SS/SS-20080623-070953.82/ATTRIB.txt Top line 835 B:	: T:/SS/SS-20080623-072351.71/ATTRIB.txt Top line 835						
A C:\Program Files\NetMeeti	A C:\Program Files\NetMeeting\cb32.exe						
A C:\Program Files\NetMeeti	A C:\Program Files\NetMeeting\conf.exe						
A C:\Program Files\NetMeeti	A C:\Program Files\NetMeeting\confmrsl.dll						
A C:\Program Files\NetMeeti	A C:\Program Files\NetMeeting\dcap32.dll						
A C:\Program Files\NetMeeti	A C:\Program Files\NetMeeting\h323cc.dll						
	SHR C:\Program Files\NetMeeting\msmsgs						
A C:\Program Files\NetMeeti	A C:\Program Files\NetMeeting\MST120.DLL						
A C:\Program Files\NetMeeti	A C:\Program Files\NetMeeting\MST123.DLL						
A C:\Program Files\NetMeeti	A C:\Program Files\NetMeeting\nac.dll						
A C:\Program Files\NetMeeti	A C:\Program Files\NetMeeting\netmeet.htm						
A C:\Program Files\NetMeeti	A C:\Program Files\NetMeeting\nmas.dll						
A C:\Program Files\NetMeeti	A C:\Program Files\NetMeeting\nmasnt.dll						
A C:\Program Files\NetMeeti	A C:\Program Files\NetMeeting\nmchat.dll						
A C:\Program Files\NetMeeti	A C:\Program Files\NetMeeting\nmcom.dll						
A C:\Program Files\NetMeeti	A C:\Program Files\NetMeeting\nmft.dll						
A C:\Program Files\NetMeeti	A C:\Program Files\NetMeeting\nmoldwb.dll						
A C:\Program Files\NetMeeti	A C:\Program Files\NetMeeting\nmwb.dll						
A C:\Program Files\NetMeeti	A C:\Program Files\NetMeeting\rrcm.dll						







	/A	TTRIB.txt	- KDiff3				×	
Fi	File Edit Directory Movement Diffview Merge Window Settings Help							
8	🖻 🗏	<i></i> 🖂 🔺	× ▲ ▼ 숲 ¥ 숲 ¥ A B (			🔲 123 💠 🔜 🗮 💻 🚥		
A:	SS/SS	-20080623-07	/0953.82/ATTRIB.txt Top line 10798	B: T:7S	s/ss-	20080623-072351.71/ATTRIB.txt Top line 10802	^	
	A		C:\WINDOWS\cmsetacl.log	1	L	C:\WINDOWS\cmsetacl.log	- 1	
	A		C:\WINDOWS\Coffee Bean.bm	1	L	C:\WINDOWS\Coffee Bean.bmp		
	A		C:\WINDOWS\comsetup.log	1	L	C:\WINDOWS\comsetup.log		
			C:\WINDOWS\Config			C:\WINDOWS\Config		
			C:\WINDOWS\Connection Wiz			C:\WINDOWS\Connection Wizard		
	A		C:\WINDOWS\control.ini	1	L	C:\WINDOWS\control.ini		
			C:\WINDOWS\Cursors			C:\WINDOWS\Cursors		
			C:\WINDOWS\Debug			C:\WINDOWS\Debug		
				P	L .	C:\WINDOWS\Delete.bat		
	A		C:\WINDOWS\desktop.ini	1	L	C:\WINDOWS\desktop.ini		
		S	C:\WINDOWS\Downloaded Pro		S	C:\WINDOWS\Downloaded Program Files 🧮	- 1	
			C:\WINDOWS\Driver Cache			C:\WINDOWS\Driver Cache		
	A		C:\WINDOWS\DtcInstall.log	1	L	C:\WINDOWS\DtcInstall.log		
			C:\WINDOWS\ehome			C:\WINDOWS\ehome		
	A		C:\WINDOWS\explorer.exe	1	L	C:\WINDOWS\explorer.exe		
	A		C:\WINDOWS\explorer.scf	1	L	C:\WINDOWS\explorer.scf		
	A		C:\WINDOWS\FaxSetup.log	1	L	C:\WINDOWS\FaxSetup.log		
	A		C:\WINDOWS\FeatherTexture	1	L	C:\WINDOWS\FeatherTexture.bmp		
		SR	C:\WINDOWS\Fonts		S	R C:\WINDOWS\Fonts		
	A		C:\WINDOWS\Gone Fishing.b:	1	L	C:\WINDOWS\Gone Fishing.bmp		





### **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.









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









- 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









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\$







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

<u>http://www.partimage.org/Main\_Page</u>

SysAnalyzer

<u>http://labs.idefense.com/software/malcode.php</u>

FPort

<u>http://www.foundstone.com/us/resources/proddesc/fport.htm</u>

RegShot

<u>https://sourceforge.net/projects/regshot</u>

MD5SUMS PC-Tools

<u>http://www.pc-tools.net/win32/md5sums/</u>

SysInternals Tools

<u>http://technet.microsoft.com/en-us/sysinternals/default.aspx</u>

Kdiff3

<u>http://kdiff3.sourceforge.net/</u>

Netcat

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

MBRutil

<u>ftp://ftp.symantec.com/public/english\_us\_canada/tools/pq/utilities/head.zip</u>





lanac





# DEMO



