

Preparation

1

- A physical access to the suspicious system should be offered to the forensic investigator.
- A good knowledge of the usual network and local activities of the computer is appreciated. You should have a file describing the usual port activity, to have a comparison base with current state.
- A good knowledge of the common used services and installed applications is needed. Don't hesitate to ask a Windows Expert for his assistance, when applicable.

Identification

2

General signs of malware presence on the desktop

Several leads might hint that the system could be compromised by a malware:

- Antivirus raising an alert or unable to update its signatures or stopping to run or unable to run even manually
- Unusual hard-disk activity: the hard drive makes huge operations at unexpected time.
- Unusually slow computer: while it was usually delivering good speed, it got slower recently
- Unusual network activity: Internet connection is very slow most of the browsing time.
- The computer reboots without reason.
- Some applications are crashing, unexpectedly.
- Pop-up windows are appearing while browsing on the web. (sometimes even without browsing)
- Your IP address (if static) is blacklisted on one or more Internet Black Lists.
- People are complaining about you e-mailing them/reaching them by IM etc. while you did not.

Actions below uses default Windows tools. Authorized users can use the **Sysinternals** Troubleshooting Utilities to perform these tasks.

Identification

2

Unusual Accounts

Look for unusual and unknown accounts created, especially in the Administrators group :

```
C:\> lusrmgr.msc
```

Unusual Files

- Look for unusual big files on the storage support, bigger than 10MB seems to be reasonable.
- Look for unusual files added recently in system folders, especially C:\WINDOWS\system32.
- Look for files using the "hidden" attribute:
C:\> dir /S /A:H

Unusual Registry Entries

Look for unusual programs launched at boot time in the Windows registry, especially:

```
HKLM\Software\Microsoft\Windows\CurrentVersion\Run
HKLM\Software\Microsoft\Windows\CurrentVersion\Runonce
HKLM\Software\Microsoft\Windows\CurrentVersion\RunonceEx
HKLM\Software\Microsoft\Windows NT\CurrentVersion
Winlogon
```

Check for the same entries in HKCU

Unusual Processes and Services

- Check all running processes for unusual/unknown entries, especially processes with username "SYSTEM" and "ADMINISTRATOR" :
C:\> taskmgr.exe
(or *tlisk, tasklist depending on Windows release*)
- Look for unusual/unexpected network services installed and started:
C:\> services.msc
C:\> net start

Note : a good knowledge of the usual services is needed.

Unusual Network Activity

- Check for file shares and verify each one is linked to a normal activity:
C:\> net view \\127.0.0.1
- Look at the opened sessions on the machine:
C:\> net session
- Have a look at the shares the machine has opened with other systems:
C:\> net use
- Check for any suspicious Netbios connexion:
C:\> nbtstat -S

Identification

2

- Look for any suspicious activity on the system's TCP/IP ports:

```
C:\> netstat -na 5
```

(-na 5 means sets the refresh interval to 5 seconds)

Use -o flag for Windows XP/2003 to see the owner of each process:

```
C:\> netstat -nao 5
```

- Use a sniffer (Wireshark, tcpdump etc.) and see if there are unusual attempts of connections to or from remote systems. If no suspicious activity is witnessed, do use the sniffer while browsing some sensitive websites (banking website for example) and see if there is a particular network activity.

Note: A good knowledge of the legitimate network activity is needed.

Unusual Automated Tasks

- Look at the list of scheduled tasks for any unusual entry:
C:\> at
On Windows 2003/XP : C:\> schtasks

- Also check user's autostart directories:
C:\Documents and Settings\user\Start Menu\Programs\Startup
C:\WinNT\Profiles\user\Start Menu\Programs\Startup

Unusual Log Entries

- Watch your log files for unusual entries:
C:\> eventvwr.msc
- Search for events like the following :
"Event log service was stopped"
"Windows File Protection is not active"
"The protected System file <name> was not restored to its original"
"Telnet Service has started successfully"
- Watch your firewall (if any) log files for suspect activity. You can also use an up-to-date antivirus to identify malware on the system, but be aware that it could destroy evidence.

In case nothing suspicious has been found, it doesn't mean that the system is not infected. A rootkit could be active for example, distracting all your tools from giving good results. Further forensic investigation can be done on the system while it is off, if the system is still suspicious. The ideal case is to make a bit-by-bit copy of the hard disk containing the system, and to analyse the copy using forensic tools like EnCase or X-Ways.

Containment

3

Pull the network plug off physically, to prevent more infection on the network and to stop probable illegal action being done from your computer (the malware could send spam massively, take part to DDoS attack or store illegal files on the system for example).

Send the suspect binaries to your CERT, or request CERT's help if you are unsure about the malware. The CERT should be able to isolate the malicious content and can send it to all AV companies, especially with contractors of your company. (The best way is to create a zipped file of the suspicious binary, encrypted using a password).

Remediation

4

Reboot from a live CD and backup all important data on an external storage support. If unsure, bring your harddisk to the helpdesk and ask them to make a copy of the important content.

Remove the binaries and the related registry entries.

- Find the best practices to remove the malware. They can usually be found on AntiVirus companies websites.
- Run an online antivirus scan.
- Launch a Bart PE- based live CD containing disinfection tools (can be downloaded from AV websites), or a dedicated anti-virus live CD.

Recovery

5

If possible reinstall the OS and applications and restore user's data from a trusted backups.

In case the computer has not been reinstalled completely:

Restore files which could have been corrupted by the malware, especially system files.

Reboot the machine after all the cleaning has been done, and check the system for its health, doing a virus scan of the whole system, hard disks and memory.

Aftermath

6

Report

An incident report should be written and made available to all of the stakeholders.

The following themes should be described:

- Initial detection.
- Actions and timelines.
- What went right.
- What went wrong.
- Incident cost.

Capitalize

Actions to improve the Windows malware detection processes should be defined to capitalize on this experience.

Incident Response Methodology

IRM #7

Windows Malware Detection

Live Analysis on a suspicious computer

IRM Author: CERT / Cédric Pernet
IRM version: 1.2

E-Mail: cert.sg@socgen.com
Web: <http://cert.societegenerale.com>
Twitter: @CertSG

Abstract

This Incident Response Methodology is a cheat sheet dedicated to handlers investigating on a precise security issue. Who should use IRM sheets?

- Administrators
- Security Operation Center
- CISOs and deputies
- CERTs (Computer Emergency Response Team)

Remember: If you face an incident, follow IRM, take notes and do not panic. Contact CERT immediately if needed

Incident handling steps

6 steps are defined to handle security Incidents

- Preparation: get ready to handle the incident
- Identification: detect the incident
- Containment: limit the impact of the incident
- Remediation: remove the threat
- Recovery: recover to a normal stage
- Aftermath: draw up and improve the process

IRM provides detailed information for each step.