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 their assistance, when applicable.

Identification 2

General signs of malware presence on the desktop

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

- Antivirus software raising an alert, unable to update its signatures, shutting down or unable to run manual scans.
- Unusual hard-disk activity: the hard drive makes huge operations at unexpected times.
- Unusually slow computer: sudden, unexplained slowdowns not related to system usage.
- Unusual network activity: Slow internet connection / poor network share performance at irregular intervals.
- The computer reboots without reason.
- Applications crashing unexpectedly.
- Pop-up windows appearing while browsing 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

IMPORTANT

Volatile data

Before carrying out any other actions, make sure to make a volatile memory capture by downloading and run the DumpIt utility from a USB key or disk as described in https://tools.cert.societegenerale.com/

Volatile data provides valuable forensic information and is straightforward to acquire.

IMPORTANT

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 *%SystemRoot%\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
You can use Microsoft Sysinternals *Autoruns* to view them all.

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 common Windows services is needed.

Identification 2

Unusual Network Activity

- Check for file shares *: C:\> net view \\127.0.0.1*
- List opened sessions on the machine:
C:\> net session
- Check for opened shares on other systems:
C:\> net use
- Check for suspicious Netbios connexions:
C:\> nbtstat –S
- Look for any suspicious network connections
C:\> netstat –na 5
(the **-a 5** flag sets the refresh interval to 5 seconds)
Add the **-o** flag for Windows XP/2003 to dislpay the owner of each process
- Use a sniffer (Wireshark, tcpdump etc.) and see if there are unusual attempts of connections to or from remote systems. try browsing sensitive websites (banking website for example) and check if unusual network activity is triggered.

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

- Check 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"

Identification 2

Check firewall 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.

If nothing suspicious has been found, it doesn't necessarily mean that the system is not infected (a rootkit could have been installed). The system may be investigated further by making a bit-by-bit copy of the incriminated hard-drive and analysing the copy with tools such as X-Ways, FTK or Encase.

Containment 3

Pull the network plug off physically, to prevent more infection on the network and to stop any actions being done from your computer (e.g. the malware could be sending spam, taking part in a DDoS attack or storing illegal files on the system).

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

Remediation 4

Reboot from a live CD and backup all important data on an external storage support. If unsure, bring your hard-drive to your IT 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 clean, trusted backups. If deemed necessary, you may ask your local IT helpdesk to reimage the disk.

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 suspicious files have been removed, and confirm that the workstation is not exhibiting any unusual behaviour. A full, up-to-date AV scan of the hard-drive and memory are recommended.

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 malware detection and eradication processes should be defined to capitalize on this experience.

SOCIETE GENERALE | CERT SOCIETE GENERALE

Incident Response Methodology

IRM #7

Windows Malware Detection

Live Analysis on a suspicious computer

IRM Author: CERT SG Team
IRM version: 1.3

E-Mail: cert.sg@socgen.com
Web: https://cert.societegenerale.com/
Twitter: @CertSG

Abstract

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

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

Remember: If you face an incident, follow the IRM, take notes and do not panic. Contact your 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 state**
- **Aftermath: draw conclusions; improve the process**

IRMs provide detailed information for each step.