Preparation 1

If a system is suspected of being "infected" or of performing maliciously, isolate it and contact your security team/officer or the internal incident response capability who is authorised to perform forensics activities for support.

Maintenance and availability of the following:

- Keep an update list of persons who need to be contacted in case of such an incident
- Take regular snapshots of usual network performance and local activities of the system, including description of usual port activity, to have a comparison baseline with current state.
- Ensure there is a good knowledge of the impacted infrastructure, including services and installed applications. Do not hesitate to ask a Windows expert for assistance.
- Activate system logs and monitoring tools, and analyse the logs regularly.
- Take notes of important details, including dates and times, which may later help the investigator.
- Prepare a read-only media like a CD with a trusted version of all executables that you will run during the identification phase. This includes all executables listed in this paper and the command line (cmd.exe). Before starting the identification phase:
  1) start the trusted cmd.exe
  2) set your path to first point to the folder hosting all trusted executables.
- Facilitate physical access to the suspicious system for the forensic investigator to safeguard a forensic copy of the evidence right from the start.
- It is recommended to do the copy as soon as possible with a minimal number of commands run on the suspicious system to limit the loss of evidences.

  1) Win32dd or win64dd can be used to acquire the memory.

  2) dd, dc3dd or imager tool can be used to acquire the disk.
  Note that this procedure may require a power-off the machine which may erase evidences of infection. Obtain the approval before proceeding in line with your local policy.

Identification 2

General signs of malware presence on the desktop

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

- Antivirus or other security system 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 or not available at all.

- The computer reboots without reason.
- Some applications are crashing, unexpectedly.
- Error messages and Pop-up windows are appearing while browsing on the web (sometimes even without browsing).k
- 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 use default Windows tools. Authorized users can use the **Sysinternals** Troubleshooting Utilities to perform these tasks*

Unusual Accounts

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

- *C:\> lusrmgr.msc*

Unusual Files

- Look for unusually 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
HKLM\System\CurrentControlSet\Services

Identification 2

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*
- 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 owning process:
  - *C:\> netstat –nao 5*
- 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*
  - *C:\systemroot\Winnt32.log*

Identification

2

- Search for events like the following :
  - o *"Event log service was stopped"*
  - o *"Windows File Protection is not active"*
  - o *"The protected System file <name> was not restored to its original"*
  - o *"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

After having analysed the impact on the service, and after having received the approval from the incident response handler, physically disconnect the infected machine from the network by unplugging the network cable.

Eradication

4

Recover the users' data

Remove the hard disk and deliver it to the internal incident response capability who will take a forensics copy and recover important data on user's request.

Remove the binaries and the related registry entries.

It is usually sufficient to run a full antivirus scan using known good sources for the antivirus software and signatures.

- 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.

for more sophisticated types of malware, this method may not be sufficient. In such cases the safest approach is to rebuild the system from scratch.

Recovery

5

Rebuild the workstation from a standard known good configuration (reference configuration/gold build) is the safest method.

This method may however inconvenience the user considerably as usually the user-specific customisations are lost causing considerable effort on the user's part to return to a working system.

Aftermath

6

Report
An incident report should be written and relevant information distributed on the basis of the need to know principle. Sensitive information should be sanitized

The following themes should be described:

- Initial detection.
- Actions and timelines.
- What went right.
- What went wrong.
- Incident cost.
- Whether the incident led to disciplinary action or prosecution

Capitalize
Actions to improve the Windows malware detection processes should be identified to learn from this experience.

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**
- **Eradication: remove the threat**
- **Recovery: recover to a normal stage**
- **Aftermath: draw up and improve the process**

IRM provides detailed information for each step.

The original author of this incident response methodology is the Incident Response Methodology (IRM) Author:
CERT-SG / Cédric Pernet
IRM version: 1.2

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

computer emergency response team | CERT-EU for the EU institutions, bodies and agencies

Security White Paper 2011-003

Incident Response Methodology #7

Guidelines for handling common malware infections on Windows based workstations

Authorised User: CERT-EU

E-Mail: cert-eu.@ec.europa.eu
Web: http://cert.europa.eu/

Last updated : 15 May 2012

Abstract

This Incident Response Methodology is a cheat sheet dedicated to handlers investigating IT security incidents.
Who should use these sheets?
This guidelines may be used by IT professionals in coordination with security team/officer or the internal incident response capability of your organisation/Institution.

In specific cases, in particular if the malware is advanced, performing such activities may make prejudice to the analysis of the incident. Therefore, no investigation shall be performed prior approval from the team in charge of responding to incidents within the organisation

WARNING
This White Paper is being issued by CERT-EU without prejudice to any policies, procedures or standards which the effected organisation may already have in place. It is intended as an aide, to IT specialists working in coordination with security team/officer or the internal incident response capability of the Institution, for cases where the persons responsible must act immediately and/or do not have other superseding policies, procedures and standards to address the problem. Persons responsible for dealing with information security matters should primarily abide by the policies, procedures and standards of their respective organisations.