computer emergency response team CERT-EU

Security White Paper 2011-001

Additional Malware Protection with MSS

Introduction

Malware, short for malicious software, is a piece of code designed to run on a system in an unauthorised manner. They lead to different types of risk like service disruption, password theft, data leakage, etc. Nowadays, malware can be more sophisticated and make your computer part of a group of compromised computers, known as botnet. Botnets are used in a large scaled attack like distributed denial of service attack against governmental web sites. Your computer can be part of it without you knowing it.

This white paper offers you a guideline for integrating Microsoft Safety Scanner (MSS)[1] in you defence in depth strategy against malware.

Malware Landscape Today

The diversity of malware grows continuously. McAfee reported[2] over 6 million of new unique malware samples in the first quarter of 2011, and they forecast to reach a total of 75 million cumulative malware by year end.

On the other hand, there are more and more sophisticated techniques used to get the malware installed on computers. Many of them come from emails that are, at first glance, trustable but that contain a malicious attachment or link that triggers the malware at open. Nowadays we see new techniques like cloaking the file extension[3] or getting the malware installed by just visiting a web-site (e.g., exploiting browser vulnerability).

Anti-virus software program (AV) is the best known application to protect against malware. It scans and monitors your system in real-time. Once a malware is detected, the anti-virus triggers an alert, puts the concerned file in quarantine or eventually removes it.

However, these programs may fail in detecting the latest malware or their variants, as explained in the next section. Therefore, MSS can help you in protecting your systems in the current malware landscape.

What More Does MSS Bring Comparing to an Anti-Virus Software?

MSS is a free security tool offered by Microsoft. It allows an on-demand scan of a full Microsoft operating system, detecting and removing all kinds of malware: viruses, spyware, and other malicious software.

MSS does not replace a standard anti-virus tool that scans your system in real-time. Instead, MSS can be coupled with such anti-virus and bring the following added values:

[1] Also known as MSERT
[2] http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q1-2011.pdf
[3] http://www.avast.com/pr-hackers-flip-filenames-to-create-safe-file-extensions

- An anti-virus tries to detect malicious software based on a list of specific patterns called signature. Each anti-virus vendor tries to update their signature list as quickly as possible after being informed of a new malware. This can take time. Microsoft MSS signature list might be updated sooner than others.
- On the other hand, the malware – once installed on a system – might become invisible to the anti-virus application. Again running a different anti-virus program like MSS might detect the infection.
- Each anti-virus program has its strengths and weaknesses in identifying a malware and its variants. The change of some bytes might make a malware invisible to some anti-virus product. Therefore, it might be worth to provide a backup diagnosis with a different tool like MSS.
- MSS is free, so if you are looking for a quick scan, MSS can be useful. It can also be used to verify that a computer is clean of viruses prior to downloading and installing security software on it.

How to Use MSS

System requirements

Operating System: Windows 7; Windows Server 2003; Windows Vista; Windows XP[4].

Step 1 – Download the Latest Version of MSS

It is important to download the latest version as often as possible. This will ensure you have the most complete list of signatures with the latest updates.
Direct link: http://www.microsoft.com/security/scanner/en-us/default.aspx[5]

Make sure that you download the file from Microsoft website. Do not use any other source!

Note that MSS expires 10 days after being downloaded.

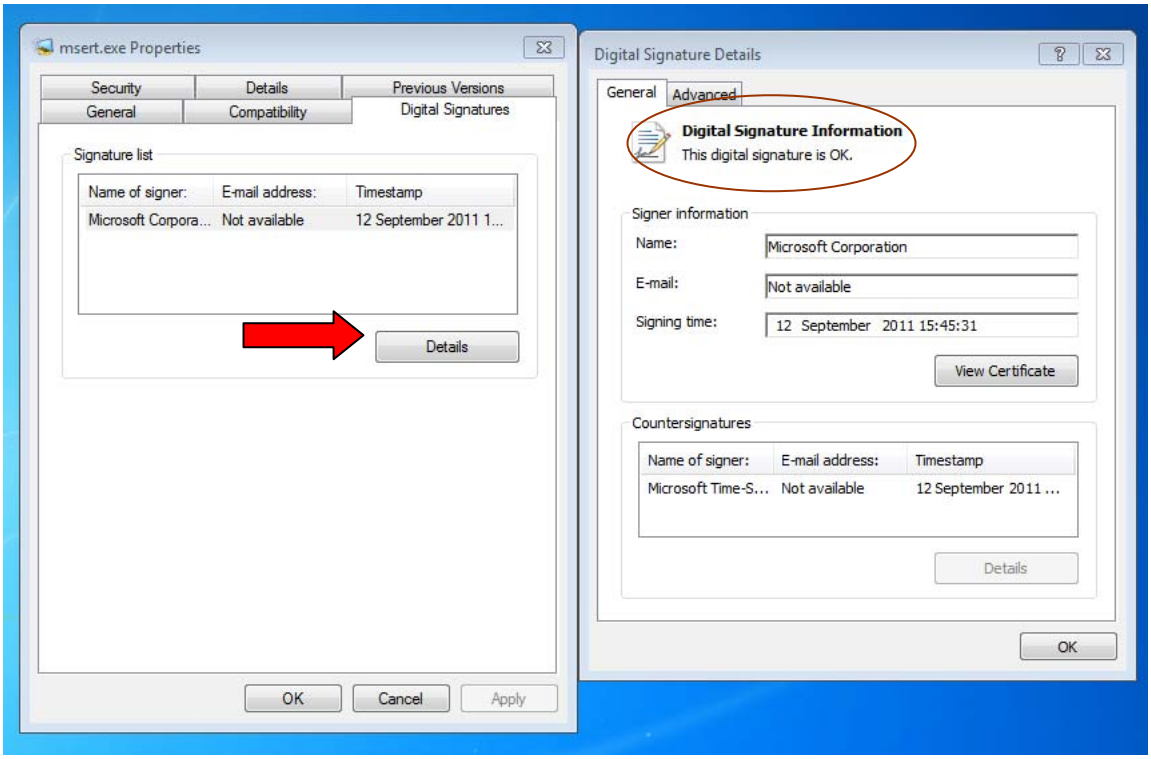
Step 2 – Verify the Authenticity of the MSS File

- Using the GUI: Right click on msert.exe file > Properties > Digital Signatures > Details
  Check for "This digital signature is ok"

- Using command line: sigcheck[6] –r msert.exe
  Check the output for “Verified= Signed” and “Publisher= Microsoft Corporate”.

If one of the above checks fails then do not run the executable!
Re-download the file from Microsoft site and try it again.

[4] Find the latest list here: http://www.microsoft.com/security/scanner/en-us/SysReq.aspx
[5] 32bit/64bit versions: https://consumersecuritysupport.microsoft.com/default.aspx?productkey=pcsafetymalware&faq=1&task=diagnostics&st=1&wfxredirect=1
[6] You can download sigcheck at http://technet.microsoft.com/en-us/sysinternals/bb897441. Verify the signature as step 2;



Step 3 – Run MSS on the Target Machine

It is recommended to run the tool in detective, silent and quick mode first. This setting can only be run from the command line[7].

- Using command line (with administrator rights): msert /n /q

MSS will delete automatically any infected file when run with the default settings.

A full scan may take hours and a lot of resources.
MSS will log the result of the scanning in \Windows\debug\msert.txt
It is as well recommended to run the scan having the Windows system in "safe-mode". However, this might not be always possible because it requires a reboot of the system.

Step 4 – Review Logs and Optionally Remove Infected Files

Check the "Return code[8]" in the MSS log file[9]:

- Return code: 0 (0x0) → no findings;
- Return code: 6 to 13 (0x6 – 0xD) → there is one or several infected files;
- Anything other Return code → there were errors while running MSS, it is recommended to review these logs as well.

[7] To launch the prompt: Type *cmd* in Start menu > Run
[8] Additional error codes: http://support.microsoft.com/kb/891716
[9] \Windows\debug\msert.txt

If there are infected files during the scan in detective mode then we recommend running again MSS to remove the malware:

- Using command line (with administrator rights): msert /q

  Check the msert log file to make sure the file has been removed.

Example of MSS log file:

```
Threat detected: Virus:DOS/EICAR_Test_File
    file://C:\Users\User1\Desktop\virusTestFile.txt
    SigSeq: 0x00000555DC2DDDB0
    SHA1:   3395856CE81F2B7382DEE72602F798B642F14140

Results Summary:
Found Virus:DOS/EICAR_Test_File, not removed.
Microsoft Safety Scanner Finished On Mon Sep 12 23:18:26 2011

Return code: 7 (0x7)
```

Hints

- MSS does not need to be installed. You can run it from a memory stick.
- You can automate the scanning via your system management solution like LANDesk. In this case, the MSS log file can be centralised for review.
- MSS sits in Microsoft's portfolio alongside with Microsoft Security Essentials, its conventional anti-malware tool (free until certain extend), and the Malicious Software Removal Tool. This latter looks similar to MSS, the differences are that it does not contain the full list of signature but only the main ones and this list is published only once a month through Windows Update.
- Keep all your applications up-to-date, malware usually exploits known vulnerabilities on your system.

MSS Privacy Statement

Note that some information might be sent to Microsoft while running MSS. You can as well disable the MSS reporting component by setting the registry setting:

```
Subkey: HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\MSERT
Entry name: \DontReportInfectionInformation
Type: REG_DWORD
Value data: 1
```

See MSS privacy statement for further information:
http://www.microsoft.com/security/scanner/en-us/Privacy.aspx

Troubleshooting

Check this link for the list of error messages and solutions:
http://support.microsoft.com/kb/2520970