VESZPROG

VESZPROG ANTI-MALWARE TEST BATTERY

2013

The number of threats increased in large measure in the last few years. A set of unique anti-malware testing procedures have been developed under the aegis of CheckVir Lab. In this document testing methods of threat protections are discussed. These testing procedures can provide actual comparative test results of anti-malware solutions automatically for the IT user community on the web and in addition other manually or semi-automatically executed tests can provide more details about the knowledge of the tested products as well. These methods can provide results soon after the new version of a particular version of an anti-malware solution is released.

1. Introduction

The number of threats increased in large measure in the last few years. In this paper testing methods of web threat protections are discussed. The main purpose of CheckVir real-time anti-malware testing is to help anti-malware developers in their work against malware and to provide correct and exact, continuously traceable information for computer users about the performance of anti-malware products. According to the test results it is possible to provide the following information:

- Comparative test results of anti-malware solutions are available automatically for the IT user community on the web. These are ready some minutes after the new version of the particular solution is released. So the results are actual.

- Summary reports can be provided to computer magazines and to other part of media. These summary could be restricted to the tested versions, testing times and as well as to the tested features.

- Test reports, execution log files as well as missed and problematic samples are provided to related anti-malware vendors.

- Anti-malware vendors can use this system for testing other features and sample sets than in the comparative tests for the public. In this case all information about this test is provided only for the related vendor.

2. Technical background

Testing procedures are executed automatically, semi-automatically or manually using a special frame system. This automatic system provides a database accessible on the Internet including the scanning results related to each version. This system includes the following parts and they works as follows in the case of testing under Windows (Figure 1).

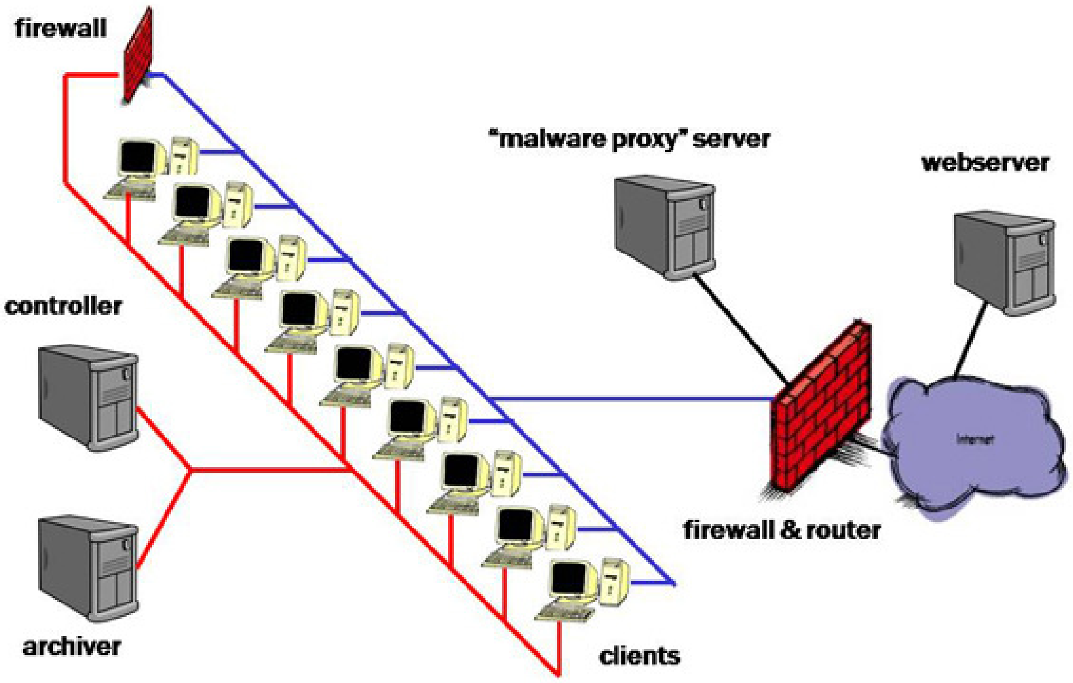

Figure 1. Technical background

Clients: These computers are able to execute different tasks related to different testing methods of the particular protection. Client computers have exactly the same hardware and software. (Even the cards are inserted into same slots.) Clients can execute testing procedures in virtual and in native environment as well. A debian Linux system and perl scripts are dealing with changing the image of the Windows operating system (including the protection) and execute them periodically. The Windows system includes installed scripts thus they can execute the steps of the corresponding testing procedure. For security reasons computer executing testing tasks are connected to the internet via a special firewall. Once the testing procedure executed all of information from the used image are saved and after the analysis of information the results ar transferred directly to the Webserver computer.

Webserver: It collects test results in its database and provides it accessible via its web page.

Archiver: All of information about executed tests is archived by this computer. It includes test results, log files and images as well as data required for testing.

Controller: This computer manages the whole process on different parts of the system.

Firewall: There is a firewall between the inner (red) and outer (blue) networks. It is used for managing the system only, it is not required by the automatic working mechanism of the system.

Firewall & router: There is a special firewall and router among the client computers, the "malware proxy" server and the internet. The main task of this computer is to distinguish between the network traffic of the virus protection and the malware. The traffic of the malware is forwarded to the "malware proxy" server however the network traffic of the virus protection is forwarded to the internet. Thus solutions may use internet connection, so the usage of "cloud technology" is not limited.

"Malware proxy" server: This server can store the content of malicious sites related to the certain time. So it can simulate the tested part of the internet for clients. It is used in the case of dynamic testing (when the malware code is executed, or a malicious site is opened).

3. Testing procedures

This chapter describes the anti-malware testing methodologies of Veszprog Ltd. It includes the testing steps (preparation, test execution and results saving) for each testing methods as well as the information used for the analysis of the results.

3.1 Efficacy tests against malicious objects

These tests are related to the detection and restoring the malicious object already stored in the attacked computer.

3.1.1 On demand scanning started by the user (V11)

This testing method tests the threat detection and removing capabilities of the protection against malicious codes stored in local files.

Testing steps

1. Prepare a physical or virtual machine with internet connection
2. Turn on the machine
3. Install and update the operating system
4. Install and update the protection
5. Turn off the machine
6. Attach an external drive with the malicious files
7. Turn on the machine
8. Wait 5 minutes for the necessary updates
9. Start the protection UI
10. Start Custom Scan with default settings on the attached drive
11. Save screenshots and report files
12. Turn off the machine
13. Save the files remained on the external drive

Information for analysis

- report files,
- remained files on the external drive,
- screenshots.

Used malicious samples

Malicious files are randomly selected from the set of malware received by Veszprog Ltd. in the last three months. The same sample set is used in the *1a – on demand testing* and *1b – on access testing*. In one round of the testing a big number of samples are used.

3.1.2 File copy from a folder to an other folder (V12)

This testing method tests the threat detection and removing capabilities of the protection during the copying procedure of malicious files.

Testing steps

1. Prepare a physical or virtual machine with internet connection
2. Turn on the machine
3. Install and update the operating system
4. Install and update the protection
5. Turn off the machine
6. Attach an external drive with the malicious files in the ***source*** directory
7. Turn on the machine
8. Wait 5 minutes for the necessary updates and protection starting
9. Start a copy procedure that copies all files from the ***source*** directory to the ***target*** directory (both on the external drive)
10. Save screenshots (if necessary) and report files
11. Turn off the machine
12. Save the files remained on the external drive

Information for analysis

- report files,
- remained files on the external drive (both ***source*** and ***target***),
- screenshots.

Used malicious samples

Malicious files are randomly selected from the set of malware received by Veszprog Ltd. in the last three months. The same sample set is used in the *1a – on demand testing* and *1b – on access testing*. In one round of the testing a big number of samples are used.

3.1.3 Executing/opening malicious files (V13)

This testing method tests the threat detection and blocking capabilities of the protection during the execution procedure of an executable malicious file.

Testing steps

1. Prepare a physical or virtual machine with internet connection
2. Turn on the machine
3. Install and update the operating system
4. Install and update the protection
5. Turn off the machine
6. Attach an external drive with a malicious file
7. Turn on the machine
8. Wait 5 minutes for the necessary updates and protection starting
9. Execute the malicious file several times
10. Save screenshots (if necessary) and report files
11. Turn off the machine
12. Check and save the changes in the system (e.g. files, registries)

Information for analysis

- report files,
- screenshots,
- system changes.

Used malicious samples

Malicious files are randomly selected from the set of missed executable samples by the *1b – on access testing*. In one round of the testing only ONE sample is used.

3.1.4. Restoring the clean environment (V14)

This testing method tests the threat detection and restoring capabilities of the protection against an installed malware on a machine.

Testing steps

1. Prepare a physical or virtual machine with internet connection
2. Turn on the machine
3. Install and update the operating system
4. Install the malware
5. Check and save the changes in the system (e.g. files, registries)
6. Turn off the machine
7. Turn on the machine
8. Check the internet connection, save screenshot
9. Install the protection
10. Update the protection
11. Execute full system scan, perform required steps
12. Save screenshots (if necessary), report files and create a log about this procedure
13. Turn off the machine
14. Check and save the changes in the system (e.g. files, registries)

Information for analysis

- report files,
- testing log,
- screenshots,
- system changes.

Used malicious samples

Malicious files are randomly selected from the set of malware received by Veszprog Ltd. in the last three months. In one round of the testing only ONE sample is used. Used samples are grouped in the following categories:

- general samples (V14g),
- rootkit samples (V14r),
- ransomware samples (V14n – from 2013Q2),
- fake antivirus samples (V14f – from 2013Q2).

3.2. Efficacy tests against malicious links

These tests are related to the detection and blocking of the malicious link and the content behind it.

3.2.1. Url testing (V21)

This testing method tests the threat detection and blocking capabilities of the protection during the opening of the recently received malicious URL site. This test is repeated several times to check protection changes.

Testing steps

1. Prepare a physical or virtual machine with internet connection
2. Turn on the machine
3. Install and update the operating system
4. Install and update the protection
5. Turn off the machine
6. Turn on the machine
7. Wait 5 minutes for the necessary updates and protection starting
8. Open the recently received malicious URL
9. If the URL is blocked GO TO 13
10. If a download window is opened then save the file
11. If the download procedure was not completed, the file saving was blocked then GO TO 13
12. Try to execute to downloaded file
13. Save screenshots (if necessary), report files and create a log about this procedure
14. Turn off the machine
15. Check and save the changes in the system (e.g. files, registries)

During the test the content of the malicious URL is stored in the malware proxy server at the first query. At later queries this content is provided.

Information for analysis

- report files,
- testing log,
- screenshots,
- system changes.

Used malicious samples

Recently received malicious URL from public black list source is used. In one round of the testing only ONE sample is used. Used samples are grouped in the following categories:

- general samples (V21g),
- phishing samples (V21p).

In the case of GATEWAY products

In the case of testing gateway protections, the protection is installed between the internet connection and the client used for this test. The protection can be hardware, software or Saas as well. During the test the sample urls are opend thru the protection. The downloaded content, the log of the downloading function and the report file of the protection are analyzed.

3.2.2 Exploit testing (V22)

This testing method tests the threat detection and blocking capabilities of the protection against an exploit attack from another computer. A special Linux server with the ***metasploit*** software is built to provide exploit attacks to clients.

Testing steps

CLIENT	SERVER
1. Prepare a physical or virtual machine with internet connection	
2. Turn on the machine	
3. Install and update the operating system	
4. Install and update the protection	
5. Turn off the machine	
6. Turn on the machine	
7. Wait 5 minutes for the necessary updates and protection starting	
	8. Start the exploit for the client's IP, create the web access for it
	9. Start the exploit procedure, with a special payload which can drop a file onto the client's desktop
10. Open the URL of the exploit, refresh it several times	
11. Save screenshots (if necessary), report files and create a log about this procedure	
12. Turn off the machine	

Information for analysis

- report files,
- testing log,
- screenshots.

Used malicious samples

For generating exploit attacks the ***metasploit*** software is used with its in-build exploit procedures.

3.3. Efficacy tests against malicious traffic

These tests are related to the detection and blocking of the network traffic produced by a malware.

3.3.1 Exfiltration testing (V31)

TBA

3.4. Performance – utilization tests

These tests are related to measure the utilization of the protection.

3.4.1 Memory (idle) testing (V51)

In this test the client memory footprint is measured in the idle state, including kernel and user memory utilization. The idle state is defined as the state where the CPU utilization is almost 0%, meaning no other activity is being done on the client. The testing is executed in the following settings:

- in the case of default settings,
- in the case of only the Antivirus is enabled,
- in the case of only the AntiSpyware is enabled,
- in the case of only the Firewall is enabled,
- in the case of all features are enabled.

Testing steps

1. Prepare a physical or virtual machine with internet connection
2. Turn on the machine
3. Install and update the operating system
4. Install and update the protection
5. Wait 5 minutes for the necessary updates and protection starting
6. Start the Task Manager
7. Save screenshots about the memory utilization in the idle state and create a log about this procedure
8. Turn off the machine

Information for analysis

- testing log,
- screenshots.

3.4.2 Memory (busy) testing (V52)

In this test the client memory footprint is measured in the busy state, including kernel and user memory utilization. The busy state is defined as the state where the system is doing an on-demand scan (i.e. a manual scan). The testing is executed in the following settings:

- in the case of default settings,
- in the case of only the Antivirus is enabled,
- in the case of only the AntiSpyware is enabled,
- in the case of only the Firewall is enabled,
- in the case of all features are enabled.

Testing steps

1. Prepare a physical or virtual machine with internet connection
2. Turn on the machine
3. Install and update the operating system
4. Install and update the protection
5. Wait 5 minutes for the necessary updates and protection starting
6. Start the protection and start an on-demand scanning procedure
7. Start the Task Manager
8. Save screenshots about the memory utilization in the idle state and create a log about this procedure
9. Turn off the machine

Information for analysis

- testing log,
- screenshots.

3.4.3 Disk testing (V53)

In this test the disk utilization of the protection on the client is measured

Testing steps

1. Prepare a physical or virtual machine with internet connection
2. Turn on the machine
3. Install and update the operating system
4. Start My computer
5. Save screenshots about the disk utilization and create a log about this procedure
6. Close My computer
7. Install and update the protection
8. Wait 5 minutes for the necessary updates and protection starting
9. Start My computer
10. Save screenshots about the disk utilization and create a log about this procedure
11. Turn off the machine

Information for analysis

- testing log,
- screenshots.

3.4.4 Network traffic testing (V54)

TBA

3.5. Performance – time tests

These tests are related to measure the working times of the protection.

3.5.1 Installation, uninstallation testing (V61)

In this test the times required for installation and uninstallation are measured.

Testing steps

1. Prepare a physical or virtual machine with internet connection
2. Turn on the machine
3. Install and update the operating system
4. Install and update the protection and continuously save screenshots while the installation is on way including the current time on the screenshots
5. Uninstall the protection and continuously save screenshots while the installation is on way including the current time on the screenshots
6. Save screenshots and create a log about this procedure
7. Turn off the machine

Information for analysis

- testing log,
- screenshots.

3.5.2 Boot time testing (V62)

In this test the times required for booting the computer is measured.

Testing steps

1. Prepare a physical or virtual machine with internet connection
2. Turn on the machine
3. Install and update the operating system
4. Install and update the protection
5. Save the current time and immediately reboot the computer
6. After booting using the STARTUP.BAT save continuously the CPU utilization for 10 minutes
7. Save recorded times and create a log about this procedure
8. Turn off the machine

Information for analysis

- testing log,
- recorded times.

3.5.3 On-demand full scan testing (V63)

In this test the times required for on-demand scan are measured.

Testing steps

1. Prepare a physical or virtual machine with internet connection
2. Turn on the machine
3. Install and update the operating system
4. Install and update the protection
5. Turn off the machine
6. Attach an external drive with the clean sample files
7. Turn on the machine
8. Wait 5 minutes for the necessary updates
9. Start the protection UI
10. Start the timer
11. Start Custom Scan with default settings on the attached drive
12. Stop the timer, record the required time for on-demand scan
13. Save screenshots, times and report files
14. Turn off the machine

Information for analysis

- report files,
- times
- screenshots.

Used samples

For this test clean files are used generally used in Windows environments.

3.5.4 On-access file copy (local) testing (V64)

In this test the times required for on-access scan are measured while clean files are copied locally from a directory to another directory.

Testing steps

1. Prepare a physical or virtual machine with internet connection
2. Turn on the machine
3. Install and update the operating system
4. Install and update the protection
5. Turn off the machine
6. Attach an external drive with clean files in the ***source*** directory
7. Turn on the machine
8. Wait 5 minutes for the necessary updates and protection starting
9. Start the timer
10. Start a copy procedure that copies all files from the ***source*** directory to the ***target*** directory (both on the external drive)
11. Stop the timer, record the required time of the copy procedure
12. Save screenshots, times and report files
13. Turn off the machine

Information for analysis

- report files,
- times
- screenshots.

Used samples

For this test clean files are used generally used in Windows environments.

3.5.5 On-access file copy (to network) testing (V65)

In this test the times required for on-access scan are measured while clean files are copied from a local directory to a network directory.

Testing steps

1. Prepare a physical or virtual machine with internet connection
2. Turn on the machine
3. Install and update the operating system
4. Install and update the protection
5. Turn off the machine
6. Attach an external drive with clean files in the ***source*** directory
7. Turn on the machine
8. Wait 5 minutes for the necessary updates and protection starting
9. Start the timer
10. Start a copy procedure that copies all files from the ***source*** directory to the ***target*** network directory
11. Stop the timer, record the required time of the copy procedure
12. Save screenshots, times and report files
13. Turn off the machine

Information for analysis

- report files,
- times
- screenshots.

Used samples

For this test clean files are used generally used in Windows environments.

3.5.6 On-access file copy (from network) testing (V66)

In this test the times required for on-access scan are measured while clean files are copied from a network directory to a local directory.

Testing steps

1. Prepare a physical or virtual machine with internet connection
2. Turn on the machine
3. Install and update the operating system
4. Install and update the protection
5. Turn off the machine
6. Attach an empty external drive with only a ***target*** directory
7. Turn on the machine
8. Wait 5 minutes for the necessary updates and protection starting
9. Start the timer
10. Start a copy procedure that copies all files from the ***source*** network directory to the ***target*** local directory
11. Stop the timer, record the required time of the copy procedure
12. Save screenshots, times and report files
13. Turn off the machine

Information for analysis

- report files,
- times
- screenshots.

Used samples

For this test clean files are used generally used in Windows environments.

3.5.7 MSI file installation testing (V67)

In this test the time required for an MSI file installation is measured.

Testing steps

1. Prepare a physical or virtual machine with internet connection
2. Turn on the machine
3. Install and update the operating system
4. Install and update the protection
5. Turn off the machine
6. Turn on the machine
7. Wait 5 minutes for the necessary updates
8. Start the timer
9. Start an MSI file installation and go thru on the installation procedure
10. Stop the timer, record the required time for the installation procedure
11. Save screenshots, times and report files
12. Turn off the machine

Information for analysis

- report files,
- times
- screenshots.

3.5.8 Opening URL pages in browser testing (V68)

In this test the time required for opening a list of URLs is measured.

Testing steps

1. Prepare a physical or virtual machine with internet connection
2. Turn on the machine
3. Install and update the operating system
4. Install and update the protection
5. Turn off the machine
6. Turn on the machine
7. Wait 5 minutes for the necessary updates
8. Start the timer
9. Start the opening procedure of a list of (clean) URLs
10. Stop the timer, record the required time for the procedure
11. Save screenshots, times and report files
12. Turn off the machine

Information for analysis

- report files,
- times
- screenshots.

3.6. Performance – 3rd party benchmark tests

These tests are related to measure the performance using third party applications.

3.6.1 Velocity (or equivalent) testing (V71)

In this test the Velocity benchmark software is used for measuring the computer capability/utilization.

Testing steps

1. Prepare a physical or virtual machine with internet connection
2. Turn on the machine
3. Install and update the operating system
4. Install and update the protection
5. Turn off the machine
6. Turn on the machine
7. Wait 5 minutes for the necessary updates
8. Start the Velocity benchmark software
9. Save screenshots, report files
10. Turn off the machine

Information for analysis

- report files,
- screenshots.

3.6.2 PCMark (or equivalent) testing (V72)

In this test the PCMark benchmark software is used for measuring the computer capability/utilization.

Testing steps

1. Prepare a physical or virtual machine with internet connection
2. Turn on the machine
3. Install and update the operating system
4. Install and update the protection
5. Turn off the machine
6. Turn on the machine
7. Wait 5 minutes for the necessary updates
8. Start the PCMark benchmark software
9. Save screenshots, report files
10. Turn off the machine

Information for analysis

- report files,
- screenshots.