VESZPROG ANTI-MALWARE TEST BATTERY

2012

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).

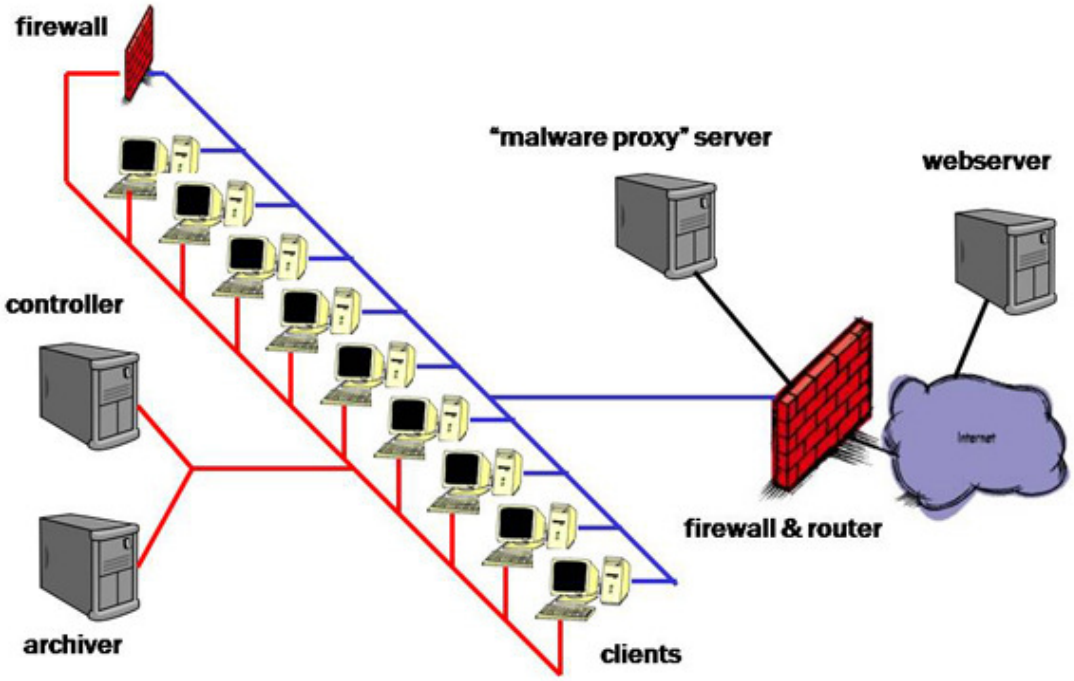

Figure 1. Technical background

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.

3.1a. On demand testing

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 2 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 two 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.

3.1b. On access testing

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 2 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 two 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.

3.2. Dynamic execution testing

This testing method tests the threat detection and blocking capabilities of the protection during the execution procedure of a 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 2 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 samples by the *1b – on access testing*. In one round of the testing only ONE sample is used.

3.3. 0hour testing

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 2 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 every 5 minutes.

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.

3.4. Remediation testing

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 two months. In one round of the testing only ONE sample is used.

3.5. Rootkit testing

This testing method tests the threat detection and restoring capabilities of the protection against an installed rootkit 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 and update the protection
5. Turn off the machine
6. Switch off the protection
7. Turn on the machine
8. Install the malware
9. Turn off the machine
10. Check and save the changes in the system (e.g. files, registries)

11. Switch on the protection
12. Turn on the machine
13. Check the internet connection, save screenshot
14. Update the protection
15. Execute full system scan, perform required steps
16. Save screenshots (if necessary), report files and create a log about this procedure
17. Turn off the machine
18. 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 rootkit files are randomly selected from the set of malware received by Veszprog Ltd. in the last two months. In one round of the testing only ONE sample is used.

3.6. Exploit testing

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 2 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.

3.7. Dynamic URL testing

This testing method tests the threat detection and blocking capabilities of the protection during the opening of a malicious URL site.

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 2 minutes for the necessary updates and protection starting
8. Open the 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 every 5 minutes.

Information for analysis

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

Used malicious samples

Malicious URLs from public black list source are used for this test. In one round of the testing only ONE sample is used.

3.8. Phishing testing

This testing method tests the threat detection and blocking capabilities of the protection during the opening of a phishing URL site.

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 2 minutes for the necessary updates and protection starting
8. Open the phishing URL
9. Check, if the URL opening was blocked
10. Save screenshots (if necessary), report files and create a log about this procedure
11. Turn off the machine

During the test the content of the malicious URL is stored in every 5 minutes.

Information for analysis

- report files,
- testing log,

Used malicious samples

Phishing URLs from public black list source are used for this test. In one round of the testing only ONE sample is used.