Whole Product Dynamic Test (WPDT)

General Notes

General Notes 2011

Language: English
March 2011
Last revision: 24th April 2011

www.av-comparatives.org

Test Procedure

Testing hundreds of URL's a day with dozens of antivirus programs makes a total of thousands URL tests and only a high degree of automation makes this possible. This automation has been developed jointly with the Institute of Computer Science of the University of Innsbruck and AV-Comparatives.

Preparation for Test Series

Every antivirus program to be tested is installed on its own test computer (please note that the term "antivirus program" as used here may also mean a full Internet Security Suite). All computers are connected to the Internet, each with its own external IP address. The system is frozen, with the operating system and antivirus program installed.

Lab-Setup

The entire test is performed on real workstations. We do not use any kind of virtualization. Each workstation has its own internet connection with its own external IP. We have special agreements with several providers (failover clustering and not blocking any traffic) to ensure a stable internet connection. The tests are performed using a live internet connection. We took the necessary precautions (with special configured firewalls, etc.) not to harm others (i.e. not to cause outbreaks).

Settings

We use every security suite with its default (out-of-the-box) settings. If user interactions are required, we will choose the default option. Our whole-product dynamic test aims to simulate real-world conditions as experienced every day by users. Therefore, if there is no predefined action, we will always use the same action where we consider the warning/message to be very clear and definitive. If the message leaves it up to the user, we will mark it as such and if the message is very vague, misleading or even suggesting trusting e.g. the malicious file/URL/behavior, we will consider it as a miss, as the ordinary user would. We consider a protection if the system is not compromised. This means that the malware is not running (or is removed/terminated) and there are no significant/malicious system changes. An outbound-firewall alert about a running malware process, which asks whether to block traffic form the users' workstation to the internet is too little, too late and not considered as protection by us.

Preparation for every Testing Day

Every morning, any available antivirus software updates are downloaded and installed, and a new base image is made for that day. This ensures that even in the case the antivirus would not finish a bigger update during the day, it would at least use the updates of the morning, like it would happen to the user in the real-world.

Testing Cycle for each malicious URL

With our own crawler we are searching the web constantly for malicious sites. We are not focusing on zero-day malware/exploits (although it is possible that they are also present in the URL pool); we are looking for malicious websites that are currently out there and being a threat to the ordinary users. Be-

fore browsing to each new malicious URL/test-case we update the programs/signatures. New major product versions are installed once a month, that's why in each monthly report we only give the product main version number. Our test-software starts monitoring the PC, so that any changes made by the malware will be recorded. Furthermore, detection algorithms check whether the antivirus program detects the malware. After each test case the machine is reverted to its clean state.

Protection

Security products should protect the user's PC. It is not very important at which stage the protection takes place. This can either be while browsing to the website (e.g. protection through URL Blocker), while an exploit tries to run or while the file is being downloaded/created or while the malware is executed (either by the exploit or by the user). After the malware is executed (if not blocked before), we wait several minutes for malicious actions and also to give e.g. behavior-blockers time to react and remedy actions performed by the malware. If the malware is not detected and the system is indeed infected/compromised, the process goes to "Malware Not Detected". If a user interaction is required and it is up to the user to decide if something is malicious, and in the case of the worst user decision the system gets compromised, we rate this as "user-dependent". Due that, the yellow bars in the results graph can be interpreted either as protected or not protected (it's up to the user).

Source of test cases

We use our own crawling system to search continuously for malicious sites and extract malicious URLs (including spammed malicious links). We also research manually for malicious URLs. If our in-house crawler does not find enough valid malicious URLs on one day, we have contracted some external researchers to provide additional malicious URLs exclusively to AV-Comparatives. Although we have access to URLs shared between vendors and other public sources, we refrain from using these for the tests.

Test Set

We are not focusing on zero day exploits/malware, but on current and relevant malware that is currently out there and problematic to users. We are trying to include about 30-50% URLs pointing directly to malware. For example, if the user is tricked by social-engineering to follow links in spam mails or websites or if the user is tricked into installing some Trojan or other rogue software. The rest/bigger part were exploits / drive by downloads. Those seem to be usually well covered by security products.

Tested products

The tested products can be found on our website http://www.av-comparatives.org

Test results

The results can be found on our website http://www.av-comparatives.org

A complete overview will be released in July and December.

Copyright and Disclaimer

For more information about AV-Comparatives and the testing methodologies please visit our website.

AV-Comparatives e.V. (2011)