Real World Protection Test in Detail

AV-Comparatives' Real-World Protection Test is currently the cutting edge when it comes to the analysis of antivirus products. Automation of the test process makes it possible to test security suites under real-world conditions. Analysis of the results from this test enables the most precise and realistic assessment of the products ever.

Test Environment

In order to produce the most realistic possible test conditions, AV-Comparatives avoid any use of virtualisation technology. Every antivirus program tested is installed on its own physical PC, using the standard installation procedure that an ordinary computer user would employ. The manufacturer's default settings are left unchanged.

Each test PC has its own individual Internet connection with an external IP address. Our Internet service providers ensure a stable connection, without failover clustering or traffic blocking. Our own security measures, such as a specially configured firewall, ensure there can be no interference between test PCs or any chance of a virus spreading from one to another.

While the tests are being run, the experts responsible for the tests are on-site, so that they can intervene if there is any sort of problem. However, the actual analysis of the test results is run automatically without the need for any manual intervention.

Test Set

To test the effectiveness of the security suites, AV-Comparatives pit them against thousands of live infected Internet sites. The investigations concentrate on the ability of the security products to stop current malware. The analysis checks whether the Internet malware has been effectively blocked.

AV-Comparatives use an extensive list of malware-infected websites for the Real-World Test. This list is continually checked, updated and expanded by AV-Comparatives' own staff. In the event that more compromised websites are required for a test, third-party providers are used, who allow exclusive use of their databases. A sufficiently large test set is essential if significant results are to be produced.

The majority of the URLs used in the test lead to exploits or drive-by downloads. Some lead directly to malware. This is identical to a real-life situation in which a link on a social network site leads to e.g. a falsified video file, which is in fact a Trojan.

Test procedure

The security suites participating in the test are checked every morning for updates (signatures and software) and brought fully up to date. The installation on each test PC is then "frozen", i.e. an image is made. This can be used to return the PC to its starting state, either to be used for the next test run, or in the event of any problems occurring.

The security products are automatically updated before each test run (visit to a particular infected URL). The URL is then opened in exactly the same way that a user would surf to a particular page or file, and the work of the anti-malware software begins. Any and all technologies that are active in a default installation of the product can be used to protect the test PC from infection.

The recognition algorithms make a permanent record of each malware find, and every change to the PC brought about by malware. When a test run has been completed, the test PCs are returned to their starting configurations and the products updated again. This is necessary because many manufacturers provide multiple signature updates each day.

Test Criteria

The test scenario and criteria are oriented towards the behaviour of the average PC user, who simply installs the software and expects it to provide complete protection without any further input. The question is thus not how, but if the security suite protects against malware.

The test PC is regarded as having been protected if the system has not been compromised by malware. That means no malicious software is active (having been deleted or blocked), and no significant changes to the system have been made.

The test PC is regarded as NOT having been protected if:

- the user is able to infect the PC by ignoring warnings from the security suite;
- a malicious program has been executed and there has been no attempt by the security suite to block it within a predefined time period.

In the event that a malware sample is not recognised, analysis will indicate whether this could have resulted from the user failing to heed a warning message from the security suite. If this is the case, the product concerned will be awarded a half point for the test run (as opposed to a full point for blocking without user intervention being required, or no points for infection without warning).

Test Results

The test results are available to publishers and readers free of charge. The manufacturers can use the feedback from the tests to identify and rectify any weaknesses in their products, while users can see at a glance which products provide the best protection.