Malware Detection Rate Results

Last updated:
Sunday October 13th, 2019 CEST
CEI Security, IT Applications
Carl Forsen

Comments or feedback:
Please send questions or ideas about this test to Carl Forsen (comments or suggestions that fall in line based and using the contact form on the website.)

Notes, comments, remarks, FAQ and everything else.

About the applications (cracked from torrent sites):
The applications are all cracked versions of commercial software, and are downloaded from torrent sites. The reason for using cracked versions of commercial software is that it is not legal to download, install, and use commercial software without a valid license. In order to install and use commercial software in a legal way, one must also install the vendor's client software, which in many cases installs several processes and services that will be running in the background. Many commercial applications that may fall into a category of potentially unwanted software, also ship and install 3rd party bundleware/adware/toolbars during the installation process, unless the user opts-out from the installation of the bundled software during the installation process.

Test environment:
The test environment is a fully patched Windows 7 Ultimate SP1 x64 with Office 2010 Pro Plus x64 installed. Java, Adobe Reader, Adobe Flash, and Microsoft Silverlight are installed and updated to their latest versions. Internet Explorer is set to allow all ActiveX controls to run, and to download and install ActiveX controls without prompting.

Malware samples:
The malware samples used during this test are collected by the Malware Research Group of the Swedish IT and Telecom Agency, using their own malware collection system. The samples are all recent samples, collected during the last few weeks before the start of each test. The samples are sorted and verified automatically, to make sure that they are valid Windows executables, and that they are infecting the system they are executed on. Only samples that are successfully infecting a system during the initial execution are included in the test. This ensures that all anti-malware products are given the same "chance" to detect the malware samples when they are executed for the first time.

About VirusTotal:
VirusTotal is a service that uses more than 40 anti-virus and other security scanners to scan files and URLs for viruses, worms, trojans and other kinds of malicious software. The service also checks URLs against a number of URL reputation services. VirusTotal's goal is to make the world safer by making it easier for anti-virus companies to get samples of malicious software, and for users to check files they download or receive via email for viruses. VirusTotal does not perform any "real-time" protection against malicious software, but it does provide a very good "second opinion" service, and it also makes it possible for anti-virus companies to quickly get samples of new malicious software "in the wild" for analysis and detection. VirusTotal also makes it possible for users to check files they download or receive via email against many different anti-virus products before they open the file, to see if any of the anti-virus products recognize the file as malicious.

About this test:
This is a test of how well anti-virus products detect malware that they do not "see" on their own computers. The purpose of this test is to see how well the anti-virus products in our test protect their customers against malware that they have not been exposed to or been able to update their virus databases for. The samples used during this test are not "ancient" samples that most anti-virus products should be able to detect, but they are also not samples that are so new that they should not be expected to be detected by the anti-virus products included in this test. The samples used during this test are samples that have been "in the wild" for a few days/weeks, and samples that we can be reasonably sure that we have not been the first to discover and report to the anti-virus vendors. We do not upload any samples to VirusTotal during the time we are testing anti-virus products in this test, and we block access to the URLs we use for downloading the samples from VirusTotal while we are testing anti-virus products in this test.

Time:
The time we use for this test is based on the UTC (+2) time zone, and we use the following format for the time: Date – YYYY-MM-DD
Time – HH-MM-SS (24-hour format)
Time zone – UTC+02-00 (CEST) (Central Europe Summer Time) or UTC+01-00 (CET) (Central Europe Time)

Detection Rate:
The Detection Rate (DR) is the sum of detections (including special detections listed during scanner history), PUA (if detected), and suspicious (if not already included in the detection rate) divided by the number of samples in the test group. Detections during the execution phase are not included in the DR, unless the product has quarantined the file, or in some other way prevented the file from being executed. Detections during the execution phase are however listed in the test results, and they are included in the "Detections during execution" section of the test results.

Functionality/Usability Penalty (Detection Rate Penalty):
The Detection Rate Penalty (DRP) is the sum of false positives in the test, multiplied by the number of false positives detected in the test group. The Detection Rate Penalty is then added to the Detection Rate, to give the product a penalty for false positives. The Detection Rate Penalty (DRP) is a way to reward products that have few false positives, and to give products that have many false positives a lower total detection rate than products that have few false positives. The Detection Rate Penalty (DRP) is also a way to reward products that have been tested against a large number of samples, since a false positive that is found when testing a large number of samples will result in a lower total detection rate than a false positive that is found when testing a small number of samples.

Why do we use Detection Rate Results?
There are many different ways of testing anti-virus products. Some anti-virus vendors prefer that their customers use their own anti-virus product to download new samples to their own computer, and then see how well their own anti-virus product protects their own computer against the samples that their own anti-virus product has downloaded. This is a good way for an anti-virus vendor to test how well their own anti-virus product protects their own computer against malware that they have not been able to detect and block on their own network, but it is not a good way to test how well an anti-virus product protects its customers against malware that it has not been able to detect, since the anti-virus product in question will not be able to download any samples that it does not detect on its own network. We do not upload any samples to VirusTotal during the time we are testing anti-virus products in this test, and we block access to the URLs we use for downloading the samples from VirusTotal while we are testing anti-virus products in this test. This makes it impossible for anti-virus vendors to see what samples we are using in our test, and it makes it impossible for them to protect their customers against the samples we use in our test by using VirusTotal. We think that this is a good way to test how well anti-virus products protect their customers against malware that they have not been able to detect on their own networks, and we think that most anti-virus vendors would agree that this is a good way to test how well their customers are protected against malware that their own anti-virus product has not been able to detect.

Why do we only test anti-virus products against malware that they have not been able to detect?
There are two reasons. The first reason is that most anti-virus vendors do not want their customers to use their anti-virus products to download new samples to their own computers, and then see how well their own anti-virus product protects their own computer against the samples that their own anti-virus product has downloaded. We think that most anti-virus vendors would agree that this is a good way to test how well their customers are protected against malware that their own anti-virus product has not been able to detect on their own networks, and we think that most anti-virus vendors would agree that this is a good way to test how well their own anti-virus product protects their own computer against malware that it has not been able to detect. The second reason is that we do not upload any samples to VirusTotal during the time we are testing anti-virus products in this test, and we block access to the URLs we use for downloading the samples from VirusTotal while we are testing anti-virus products in this test. This makes it impossible for anti-virus vendors to see what samples we are using in our test, and it makes it impossible for them to protect their customers against the samples we use in our test by using VirusTotal. We think that this is a good way to test how well anti-virus products protect their customers against malware that they have not been able to detect on their own networks.

Always have the most up to date version of the DAT:
Most anti-virus products can update their virus definition files many times per hour, while most test platforms only update their anti-virus products once per week. Anti-virus vendors who release their virus definition files more often than once per week will therefore have an advantage over those who release their virus definition files less often than once per week, when they are tested in a test where the anti-virus products are updated to their latest versions before the start of the test. Most anti-virus products can be configured to download and install virus definition file updates automatically when they are connected to the Internet, and we think that most anti-virus products should be configured to download and install virus definition file updates automatically when they are connected to the Internet, in order to be able to protect their customers against the latest malware samples that are being released "in the wild" every day. We think that most anti-virus products should be able to download and install virus definition file updates at least once every hour, when they are connected to the Internet, in order to be able to provide their customers with the latest protection against malware that is being released "in the wild" every day. We think that most anti-virus products should be able to download and install virus definition file updates at least once every hour, when they are connected to the Internet, in order to be able to provide their customers with the latest protection against malware that is being released "in the wild" every day. We think that most anti-virus products should be able to download and install virus definition file updates at least once every hour, when they are connected to the Internet, in order to be able to provide their customers with the latest protection against malware that is being released "in the wild" every day.