Quick Test

Emsi Software a-squared Anti-Malware 4.5

Up to 3,000 new software pests per day are now appearing on computers and threatening data. The security software manufacturers must create a new signature for every new software pest in order for it to be reliably recognized. This shows the major weak point of this detection process. A software pest must already have spread to a certain number of computers before a security software manufacturer is even aware that it exists. This means that the authors of Malware are basically always one step ahead of the security software manufacturers.

To overcome this deficit, the security software manufacturers are attempting to develop new techniques for reliably detecting previously unknown Malware without using signatures. One approach is behavior recognition, where the behavior of each running program is carefully monitored. If a program exhibits suspicious behavior then it is stopped, thus preventing a possible infection. The Austrian company Emsi Software has integrated this type of technology into its a-squared Anti-Malware protection system. Emsi Software also combines two scan engines in the current version of a-squared Anti-Malware, whereby double recognition is filtered out. With this system, the manufacturer promises the highest possible recognition performance but with a very low load on the system.

The a-squared engine was originally developed for recognition of Spyware and Trojans and achieved a certain level of recognition in this area. The engine developed by Emsi Software also detects Cookies and Spyware traces in the Registry. The second engine comes from Ikarus, who are also based in Austria, and specializes in the detection of Viruses, Worms and other types of Malware. However, Emsi Software went one step further and also integrated a third line of defense in their protection system: Behavior recognition. This was reason enough for the ProtectStar test lab to subject the program to a practical test.

Security

The protection concept used by a-squared follows a different approach to the usual method: Whereas classical virus scanners examine files for damaging code when the files are read or written (on-access scan), a-squared only analyses the files when they are executed. This process is also known as an on-execution scan.

A-squared does not use a single scan engine for the classical signature scan but rather checks each file three times before it is executed.

Before it is allowed to run, the file is checked using the first scan engine. A-squared uses the Ikarus engine for this first pass. This is followed by a second check using the scan engine developed by Emsi. The third and final examination checks and monitors the behavior of the running file. If a-squared notices behavior that is typical for Malware then the program is stopped and a possible infection is prevented. Emsi calls this technique “Malware-IDS”, whereby IDS stands for “Intrusion Detection System”. The user can decide what types of suspicious behavior should be monitored.

The default settings cause the IDS to examine every executed program for potentially damaging behavior. The executed program is monitored for behavior typical of Spyware, Backdoors, Trojans, Worms and Dialers. It is also checked for Rootkit behavior, manipulation of the Hosts file or installation of hidden drivers. Processes that modify Autostart entries or manipulate (patch) other programs are also detected.

The user can set options defining how to deal with each suspicious file. Since many harmless programs also exhibit Malware-typical behavior, rules can be automatically created for each program. Emsi Software uses the experience of the a-squared user base for this using a type of “In the cloud” technology. Every user decision relating to a particular program is sent to Emsi Software in the form of a checksum, allowing a ranking to be created for every program. Once a certain number of users have classified a program as harmless or damaging then an alert is no longer raised and a rule for this program is automatically created and used by the

program. One example is the first start of the well-known Firefox browser. A-squared signals suspicious behavior of the browser and issues a query asking for the user ranking of “Firefox”. Since Firefox is ranked as trustworthy by at least 90% of the users, a-squared automatically creates a rule allowing Firefox to run. This all happens within a fraction of a second and the alert dialog is only briefly displayed. After this, no more alerts are displayed when Firefox is started. The percentage of users classifying a program as harmless or dangerous before a rule can be created is configurable. The default setting uses a threshold of 90%. This option can also be completely switched off. When using the Paranoid mode, where all suspicious behavior of all programs is signaled, the user ranking also has no relevance and is not used. The signature scan is always used, regardless of any rules that may exist. The classical on-demand signature scan is provided for regular Malware scanning of the computer. Both scan engines are used for this. If desired, all files in the computer can be checked, whereas the Background Guard only checks executable files when they are actually run. The scan time is still acceptable, despite using two scan engines. On our test system with 178 GB of data and a total of 109,886 files, a-squared takes 44 minutes and 48 seconds to scan the entire system and 4.47 GB of clean files are scanned in 3 minutes. Gdata AntiVirus 2010, which also uses 2 scan engines, requires 4 minutes and 12 seconds for the same task.

However, the system load during the a-squared scan is very low and normal work on the computer is still possible without significant limitations. The recognition performance of the program is very good. A-squared detected 99% of the 500 samples in our small test set.

The same test set was used for testing four other current virus scanners. All products performed the scan using a signature update from 03.09.09. Only Gdata, which also uses two scan engines, achieved a slightly higher recognition rate.

Scan results of selected virus scanners

A-squared 4.5	Avira 9.0	BitDefender 2010	GData 2010	Kaspersky 2010
99,0%	97,6%	97,8%	99,4%	95,2%

This good result is confirmed by the results we have seen in the test series performed at www.virustotal.com. A-squared also delivered good rates of detection in these tests. Of course, the rate of false positives should also be taken into account. Emsi Software takes this problem seriously and immediately corrects false alerts as soon as they are known. For example, at the beginning of the test series the Trojan.Banload.a Malware was detected in the “Iron” Open Source browser. This false alert was corrected after two days – without being explicitly logged at Emsi Software.

A-squared does not contain a HTTP scanner or an Email scanner. It takes a different approach to surf protection by not scanning the entire content of a website but rather attacking the problem at the source by preventing access to dangerous hosts and/or web servers. The default settings cause a-squared to issue a warning when visiting these hosts and requires the user to confirm navigation, with a default setting of “Block”. A rule is created each time such a decision is made, which soon leads to a personalized rule base allowing the user to surf without worries.

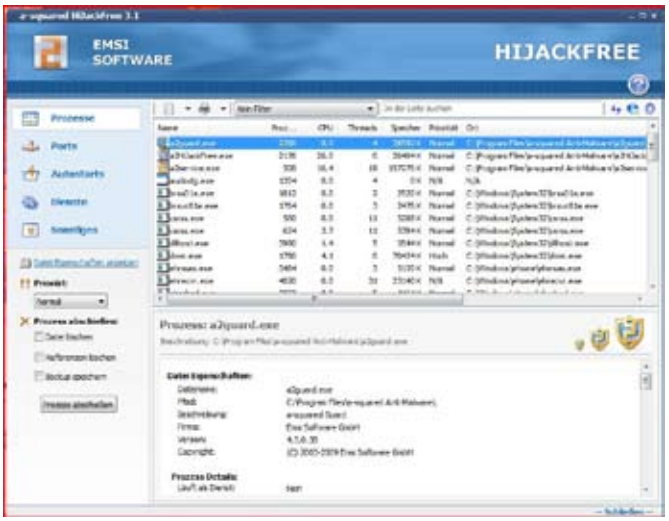
The program thus takes action before damaging software is able to reach the computer. The hit-rate achieved by Emsi Software using this method is simply amazing. Also amazing is the huge number of potentially dangerous hosts that surface when you make a simple search for “Wallpaper”. A-squared is sometimes a bit over-enthusiastic in this area. For example, access to the site “freemail.web.de” is blocked because the “Smartsurfer” program is available at this address. This program is a dial-up program provided by web.de. A-squared correctly detects this program as a Dialer and thus blocks access to the entire site.

The lack of a mail scanner is no real risk because all executable files are still scanned three times. This method cannot prevent Malware from entering the computer or being passed on via email. The a-squared concept does not directly address this issue.

User-friendliness

After easy installation of the program, which does not require the computer to be restarted, the user is greeted by a setup wizard that helps with the first steps. An update is first performed, followed by an initial system scan before the real time scanner starts working. Unfortunately there is no “Remaining Time” display for the scan and no way to automatically shut shown the computer when the scan is finished. There

is also no report history and the highly descriptive and clear reports can only be manually saved directly after each scan. We would also like to see more configuration options for the on-demand scan. The basic settings are heavily oriented toward normal daily use, offering a good compromise between security and convenience. Most user interactions usually result in the creation of a rule so that the user is only queried once for each new program. The default recommended action is always set to “Block” so that thoughtless clicking will not lead to a Malware infection.



The messages generated by the real time scanner are easy to understand and should not generally present the user with any problems, especially since the suggested actions have been very carefully chosen with a major emphasis on security. It takes a real amount of effort to actually run a program classified as dangerous by a-squared Anti-Malware. In addition to this, the previously described community-based alert reduction system is configured for the automatic creation of rules for most well-known programs.

The default settings cause the program to search for updates every hour. This update interval can be configured as desired. New signatures are indicated by a small popup in the information area and a balloon tip when the mouse is moved over the icon in the System Tray.

We regard this solution as very clear, allowing the current version of the signature database to be queried without having to start the normal program user interface. According to the manufacturer, a-squared searches for new signatures three minutes after the system is started. During the test series, new signatures were not downloaded until about 10 minutes after starting the system. This seemed too long to us. Our test series indicated that Emsi Software usually provides new signatures 4-5 times a day.

Performance

The fact that the real-time guard only springs into action when a file is executed can be seen in the outstanding performance of the program.

It is amazing to see the level of performance available, even in older systems, when you do not use the type of on-access scan provided by normal virus protection programs.

Searching large folders or multimedia collections is not slowed down, since the real-time scanner only takes action when a file is actually run. A small delay is only noticeable when programs are started. The special operating manner of the program means that it has no effect on copying, packing or unpacking files.

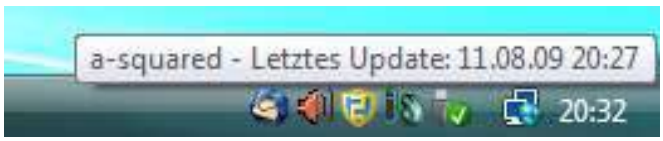
However, it allows itself a generous 180 MB of RAM to contain the complete scan engine and signatures. A well-dimensioned amount of RAM is therefore to be recommended. The surf protection has no effect on the surfing performance. The system startup time was not visibly affected by the presence of the program.

Products included

The package also includes the Hijack-Free program, which provides a comprehensive view of the programs installed and running on the computer. It offers convenient management of components loaded on system startup, way beyond the normal features offered by Windows. This component is a powerful tool in the hands of an experienced user.

The products included in the a-squared package cannot compete with a comprehensive “Security Suite”. It does not include a Firewall or Spam filter.

In this case, you must use the existing Windows components, such as the Windows Firewall, or the Spam Filter provided in your mail client. This does not necessarily make a Windows system less safe; in fact it reduces the possibility of system conflicts and saves system resources. This actually represents



an advantage in comparison to the use of a comprehensive "Security Suite".

Support:

An easy to understand and comprehensive online help system is provided to answer any questions regarding the program. A very well moderated forum, directly accessible from the program, is also available. This forum is directly moderated by the developers, resulting in fast and competent support. Comprehensive FAQs are provided at the manufacturer's web-site. General notes on computer security are also available. Interested users can find more detailed documentation on the technology used by a-squared. All documents are clearly written and provide a great deal of detail.

Summary:

A-squared Anti Malware 4.5 from EMSI Software made a very positive impression during the test series.

The recognition performance is very good and the additional behavior monitoring provides a very high level of protection. The number of user query dialogs generated by the program declines rapidly as the program is used, thus requiring less and less interaction. The user interface is clearly structured and well thought-out.

The software showed almost no negative affects on system performance and ran absolutely stable. A-squared is aimed at users wanting a high level of protection with very low loss of system performance and who are willing to forgo an HTTP or Mail scanner. The decisive elements of the program are the be-havioral analysis and the fact that files are only scanned when a signature-based scan is started.

The program is available for downloading at www.emsisoft.com at a price of €30. A Freeware version without the real-time protection and the Hijack-Free module is also available.

Anti-Malware 4.5 was awarded the ProtectStar Award 2009 for its outstanding total performance.

Oliver Rosenow
o.rosenow@protectstar.com

Suggestions, criticism and donations

ProtectStar™ Test Lab's work is strictly independent.

The test analyses carried out here, the evaluation and report of test results, the design of the test report, translations, publications, working hours, salaries, provisions, etc., were financed exclusively by ProtectStar™, Inc. The publishers named in the test report merely provided (some only partly) test versions and licenses required for the test series.

ProtectStar™ is thankful for every kind of suggestions and criticism from our readers to make it possible for us to improve the test series in the future. Please tell us what you found especially positive and of which test we could have reported in greater detail in your opinion.

If you liked the test report and if it helped you make a decision to buy a product, or if you gained new insights by reading about the opinions of experts in the area of IT security, we would thank you for **materially supporting** the charitable **ProtectStar™ Foundation** (www.protectstar-foundation.org)

Charitable aid projects will profit from your support. Especially in the areas of education, health care and IT for students your help will be gladly accepted.

Contact

Corporate Headquarter:
ProtectStar, Inc.
TestLab
444 Brickell Avenue
Suite 51103
33131 Miami, FL
USA

Phone: +1 888 218 4123
Fax : +1 888 218 8505
e-Mail: testcenter@protectstar.com
Web : www.protectstar-testlab.org

European Headquarter:
ProtectStar, Inc.
Test Lab
Daws House
33-35 Daws Lane
London NW7 4SD
UK

Phone: +44 20 8906 6651
Fax : +44 20 8906 6611
e-Mail: testcenter@protectstar.com
Web : www.protectstar-testlab.org

Copyright