

9 November 2006

By: Ionut Ilascu, Editor, Software Reviews



"Security Must Not Be a Privilege"

When your anti-virus is impotent, A-Squared Anti-Malware enforcement is needed

It would be nice to surf the Web at any time without being afraid that your computer may contact who knows what disease. Malware fills up the Internet and we always strive to keep our machine as clean as possible. This is not always possible even if you have your antivirus updated with the definitions or your firewall is strong enough to face all the threats and devious plans of the hackers. This is why there appeared a new trend on the computer security market. Besides your regular antivirus and firewall you should also install an anti malware software which performs a double check of the accuracy of the other two. Today I will present to you a software that may be familiar to you as the free version has already been reviewed by Codrut Nistor, my colleague and friend here at Softpedia. The application is called A-Squared (A2) Anti-Malware and it is developed by Emsi Software GmbH, a company which thinks that "everyone should be able to surf the web securely". From the first launching of the software, you can clearly see that the developer has not sacrificed the aesthetics for the utility and functionality. The interface is very nicely drawn and every option is placed in its place (that's maybe because the developing centers are located in Austria and Switzerland, and we all know how serious these peoples are). There are no eye-hurting colors and everything about the aspect is cool and relaxing. Among the features of the application you will find an anti-malware scanner, a quarantine box and the hijack free option. Scheduling the software to scan your computer at a certain time of the day or to automatically check for updates are also available and I must say that they work pretty fine. This way, you will no longer have to remember to scan your machine or to worry that the software is not updated. Before starting to actually use the software, the user has to create a user account and you will be given a username and password. The Security Wizard that makes you do this will continue configuring the main settings for the updater: the user can choose to install the program help, additional languages, the beta updates or submit names of detected malware. In the same window, there is a small setting that says "Edit alerts settings" and which allows you to make the settings for the news and alerts (news boxes, update message, restart alerts - displays a message when a computer restart is needed). Clicking OK and Next will start the software's updating process. After the updates are downloaded, you will be displayed what has been added: languages, engine components, signatures for trojans, dialers, worms and spyware. Press Clean Computer Now button to proceed to scanning your machine for the above mentioned malware. There are four types of scans available: quick scan (scans the active programs), Smart Scan (only important folders will be checked), Deep Scan (every file on your hard disk will be scanned) and Custom Scan (all the scanner options are edited manually). To know how much of this wizard is left, the software displays in the upper part of the window the total number of tasks and a thin red line will tell you exactly in what stage you are. Of course, you can close the wizard at any time you like and configure all these features later. The next section after the scan is finished is Prevent Infection. Here, you can set the background guard's way of protecting you and keeping the malware outside your machine. The user can set it to start on system startup, download and install updates automatically, schedule scans, use heuristics as alert when an unknown malware is detected, activate the paranoid mode (displays lots of suspicions), activate cookie monitoring and automatically blocking tracking cookies. That was the last step of the wizard and you can close it in order to proceed to the Security Center and make some more settings or change the ones you have already made in the wizard. The main application window of the Security Center allows the user to configure each option of the Background Guard, perform a scan or update the software (you

are displayed with the day and hour of the last update check). The Quarantine box contains all the detected malware that was detected during the scan and you did not want to delete in the first place. Here all the items will be displayed beginning with their source, type of infection, risk level and date. The two options below the quarantined items' window permit the user to restore or delete them. Configuration section permits you to change the settings for Background Guard, set some Application Rules for different applications (select the application, set the security mode and choose between the rules displayed). Cookie Rules window is a bit less complicated as all you have to do is select the cookie and select the security mode (either allow or deny them). Scheduled Scan permits you to fix a date and time for the software to perform a scan and its recurrence, or you can set an interval start and end for the scan. Updating and Auto-Update are no longer hiding secrets as I have revealed them above and the latter option works exactly like the scheduled scan. HiJackFree option may seem more complicated for most of the users as it is dedicated to more advanced customers. There are five menus in here and each of them has a set of options. The first one is called Processes and it is similar to the Task Manager in Windows, the only difference being that the A2 feature will display the full path to the executed files and their loaded files and modules. You will also be provided with an online analysis of the process (the information is updated online). The Ports section shows the user all the ports that are open and the processes listening, the process ID and the protocol type. In the information window below you will be presented with the properties of the file, process details and the online information. In Autoruns A2 Anti-Malware allows viewing and editing all autorun entries. There are more than 50 locations displayed and you can add new items, edit the existing ones or delete them. The online information window will give you a hint about what a certain process does. Services can also be started or stopped and you will get the clues about them in the information window. This section includes a Service Manager which shows the full path to the executable as an additional feature. Other section contains Explorer AddOns (view and edit plugins of Windows Explorer and Internet Explorer), LSP Protocols (shows all installed Layered Service Providers), Hosts (contains the mapping of IP addresses to host names; it is helpful in redirecting ad network server names to localhost in order to avoid ads on websites) and ActiveX components (you can check them out and uninstall the harmful ones). **The Good** The software is quite flexible regarding the options it has and you have a wide range of features you can use to protect your computer. I was very impressed by the full version and I had absolutely no problem in handling it. The Background Guard option is most useful as it alerts you of potential and real risks that are knocking at your computer's ports. **The Bad** I was particularly annoyed by the fact that when leaping from one menu to another the window closed for reopening in the desired menu. And when I wanted to return to a section in the Security Center I had to close the window, wait for the Security Center screen to appear and then make my pick. Inside the menu, things work the usual way (click on the submenu and the window opens). It seemed to me pretty annoying as I am not accustomed with this means of opening the menus. **The Truth** Considering the costs (\$39.95 and about 50MB of memory) and benefits (realtime protection, pretty large signature database, scanning and cleaning your computer of malware, scheduled scans and updates, etc.) I think that the software is worth testing at least until the trial period expires (30 days). The software is still at the beginning and I am sure that the Austrian-Swiss development team will eliminate all the nagging aspects and will continue improving the software. *Here are some snapshots of the application in action:*