AV-LAB

THE INDEPENDENT ANTIVIRUS TESTS

Emsisoft Internet Security 12 prepare for even better protection

November 2016

Cyber security sector has its own laws. There is no time to relax, and certainly antivirus developers can't afford this privilege.

Threat landscape can change from week to week. End users suffer from it mostly, so antivirus software providers must quickly respond to the events arising from popularization of "crimeware as a service", which imply multiplication of the cyber attacks. Do you remember the first ransomware viruses? Although, this specific type of malicious software has greatly evolved, some security applications developers still can't come up with effective blocking and avoiding user file encryption.

> *In this regard, behavioral protection against unknown threats and malicious software of crypto-ransomware, implemented in Emsisoft Anti-Malware 12 and Emsisoft Internet Security 12, is doing very well. Here you can read more about this test.*

Emsisoft in Poland

Emsisoft security applications are very popular in Poland — not only because of the good real-time protection, but because of the free anti-malware scanner, Emsisoft Emergency Kit. For brand fans and prospective new customers, who haven't decided yet or still hesitate as regards the choice of antivirus software, we have prepared some interesting facts:

— users from Poland are 6th most numerous group of customers of Emsisoft applications from around the world — there are over 100 000 Poles. We were outrun by users from the USA, Germany, Russian and France. TOP 10 belongs to (sorted by the highest number of users): USA, Germany, Russia, France, Italy, Poland, United Kingdom, Canada, Ukraine, Netherlands.

Developer declares it has got about 4 million active licenses, including free scanner, Emsisoft emergency Kit, and trial and paid versions of Emsisoft applications.

— most of the detected by Emsisoft threats, which concern our country, are primarily potentially unwanted programs (PUP). This isn't surprising, considering the fact, that Emsisoft puts a strong emphasis on detection of "junk" applications and cleaning obtrusive elements after installation of free software. So it double solves the problem — with good detection of PUP, less experienced users aren't harassed by ads coming out from freeware, and their browsers are free of unnecessary add-ons and toolbars.

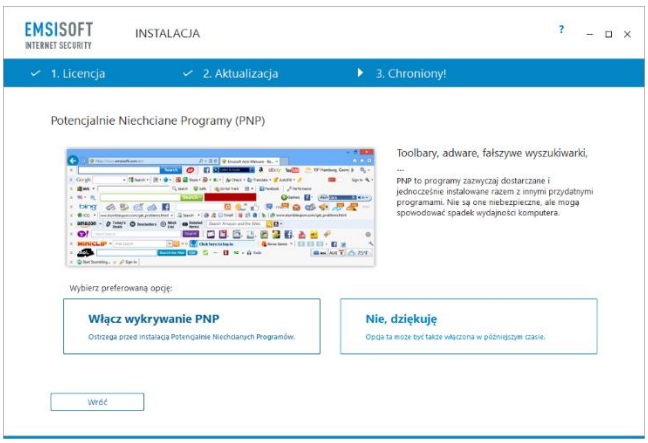

Figure 1. Before installation, we strongly recommend to enable PUP detection feature.

— when it comes to malicious software, definitely the highest detection rates applies to ransomware and crypto-ransomware. In this regard, we strongly recommend tools developed by Fabian Wosar — decrypters, which you can download for free to decrypt files. At least you can try: https://decrypter.emsisoft.com

— developer has shared, that he is working on mechanism, which on the basis of event logging functions in the system, allows a event analysis after a cyber attack and investigate what happened in the computer in the past. This feature may be of especially interesting for network administrators, who must analyze activities related to the safety of their customers. It remains unclear, whether the module will appear in the software for individual users or only for businesses (although, these are the same applications).

Innovations in “12” version. No, not this time

The information we were able to obtain from the developer indicates, that the new series of products for individual users and small businesses, namely: Emsisoft Internet Security 12 and Emsisoft Anti-Malware 12 doesn’t include any new features. But…

The producer has improved already developed protection modules, which now gain an even better quality of collateral:

In the new software has been improved, among others, detection algorithm of ransomware viruses (which can be observed in our tests) and detection of potentially unwanted applications mechanism. Moreover, developer refined the mechanisms of antivirus self-protection, which before booting the operating system and while working, constantly monitor potentially dangerous consequences of access antivirus files through processes, which due to the injection of malicious code by malware to another process, could crash and cause permanent damage to the integrity of the antivirus files. Such a situation doesn’t happen often, but could be a real problem for the user — malware, which manages to stop antivirus monitor or add its files to safe list, could execute unauthorized malicious code under privileges of the process, which malicious software was initiated to run from.

But that’s not all. Emsisoft team also arranged:

- minimizing the problem of false positives (although, we believe this problem is no longer present),
- functioning of the white list has been changed, which now allows creating protecting exclusion for applications, and even files located inside indicated folders on user hard drive,
- integration with the notification system has been modernized — in this regard “12” version brings enhanced integration with the action center in Windows 10,
- the user interface has undergone cosmetic changes.

In addition to the changes above, developer also introduced hundreds of minor improvements on the basis of collaboration with the community and independent testers.

What about protection?

We confirmed effectiveness of behavioral protection in our newest test, which is very popular among antivirus software developers — although, we have to admit, that not all of them are happy about this outcome. Of course, we mean low results achieved by some applications. One thing is certain — antivirus market is changing dynamically, so software, which were shining in all tests in the past, not necessarily must keep the same situation till the end of the world and one day more.

Going back to our protection, in Emsisoft Internet Security 12 settings, we can find some interesting features, namely: Behavior Blocker, which is an invaluable advantage of this product.

Figure 2 Behavior Blocker is one of the advanced modules, responsible for protection against unknown threats.

The idea behind this is that the user is protected against unknown threat — if producer hasn't developed any signature yet — can block behavior similar to backdoors, spywares, hijack type of programs and defend indicated applications against attempting to inject code by other processes (in case of this kind of malicious file, behavior blocker detects potentially dangerous behavior, which differs from the conventional system modifications while running and installing secure applications).

Additionally, the user can create application rules for network traffic (firewall), suspicious crack type applications, blocking system applications, e.g. Cortana, blocking a host list (Emsisoft is able to recognize IP addresses from TXT file and block them), and what's interesting — blocking ads host (this functions is disabled by default), so all files and scripts, which are downloaded when loading website resources from "strangers" servers whose IP addresses don't belong to a record A defined in a DNS configuration of a TLD domain.

In this review, we turn in traditional antivirus tests confirming the effectiveness of real-time protection, because good protection quality was verified by our protection test against ransomware threats. On the other hand, we cannot skip a performance test:

We checked the performance of Emsisoft Internet Security 12 for processes created exclusively by antivirus applications on workstation equipped with a modern 6-core CPU and 2GB of allocated RAM. This method makes it possible to separate the use of CPU and RAM by installed applications from antivirus software.

During a 10 minutes test when idle, we were gathering results for CPU time and RAM usage of all antivirus processes. The results were averaged.

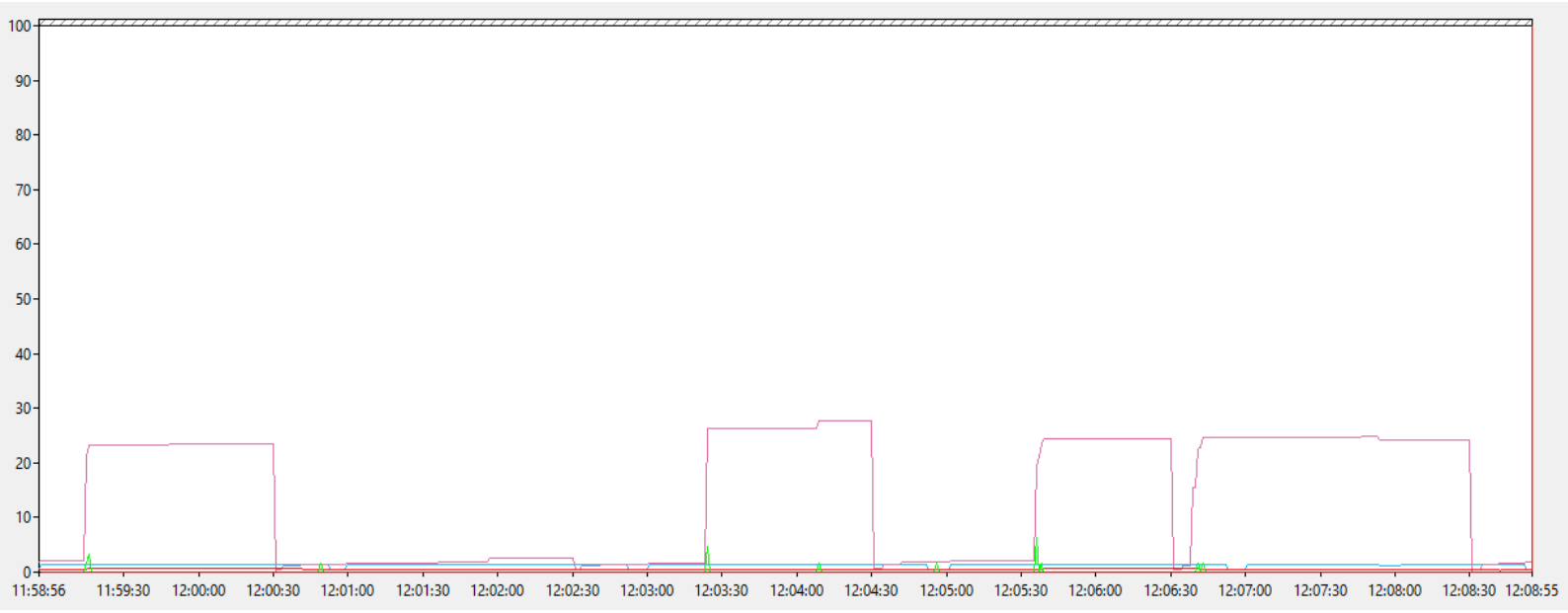

Figure 3 On average, the application to operate needed 0,042% of single core processor time and ~14,69MB of RAM.

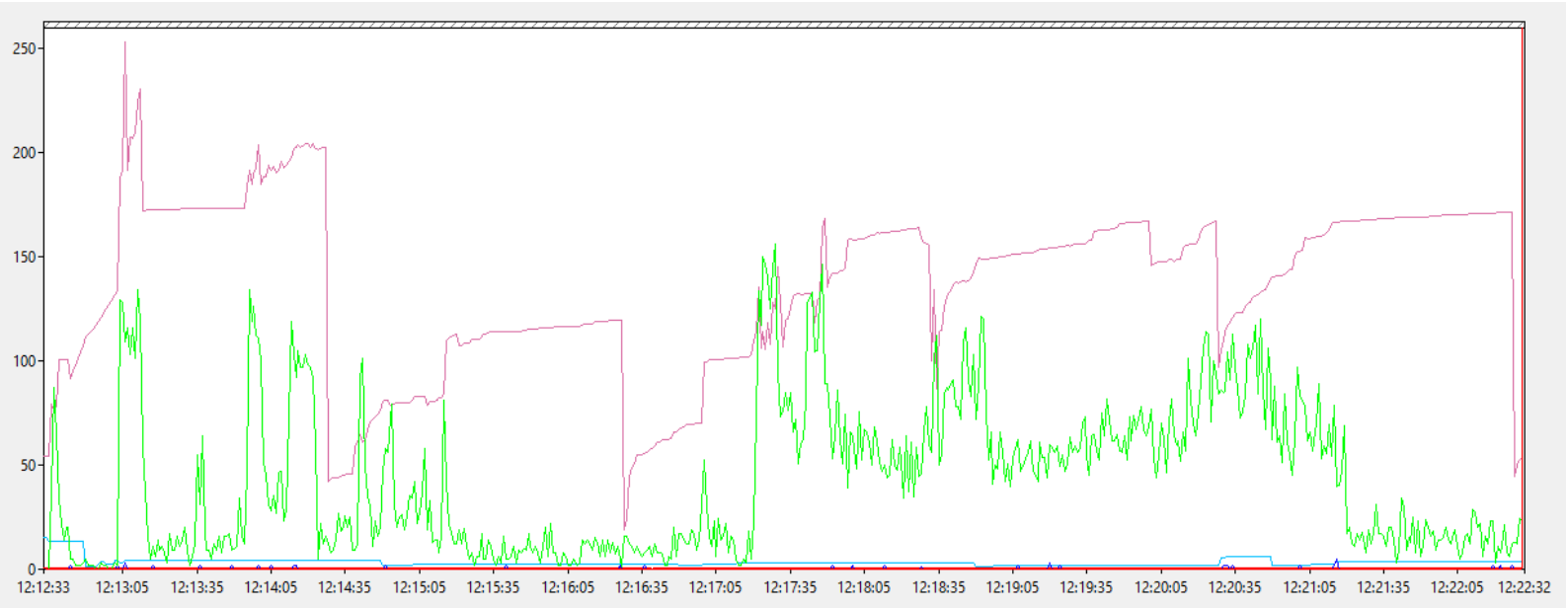

Figure 4 During the 10 minutes full system scan (Custom Scan on default settings), Emsisoft processes consumed an average of 42,978% of single core processor time and ~141MB of RAM.

The green line on the graph represents CPU. Other closer to “zero” is hard to see. A value where, the green line exceeded the scale of “100” means 100% of processor single core usage. At the peak load of CPU by antivirus processes, the value reached 156%, which means, that in a given second one core went into 100% load, while the second 56%. Over a period of 10 minutes of scanning, the average CPU usage of only one core was 42,978%.

Conclusion

When it comes to Emsisoft antivirus software, for the umpteenth time we are positively surprised with the quality of behavioral protection and simple and understandable messages of mechanism detecting suspicious virus activities in the operating system. We are puzzled how such a small company makes every effort to prepare application for protection against the whole spectrum of malicious and potentially unwanted software. Although, Emsisoft doesn’t belong to group of corporations, which have millions of users (in our opinion, applications developed by this producer are addressed to specialized users and less technical ones), the only gripe seems to be disproportionate popularity compared to other developers, such as: Kaspersky Lab, Avast, ESET, G Data, or even F-Secure and Comodo. Therefore, here is our request — if you know people, who are looking for good and “silent” antivirus software — without any contraindications, you can recommend installing or at least trying Emsisoft Anti-Malware 12 or Emsisoft Internet Security 12.

AV LAB
THE INDEPENDENT ANTIVIRUS TESTS

https://avlab.pl

For press (big size resolution certificate): https://avlab.pl/dla-prasy

About AVLab

AVLab brings together enthusiasts of antivirus software and web safety. Our activities include program testing and sharing results of our analyzes with all Internet users. We are not controlled and/or linked with any software developer.

AVLab tests are independent and take place in conditions close to reality. Don’t be guided by our results when making a final decision in choosing antivirus program. In order to make a final choice we suggest to read tests from other independent laboratories that use different methods and techniques for testing antivirus software. In addition, decisions depends on personal preferences, specified features, efficiency, detection rate, impact on system performance, user interface, price, usability, compatibility, language, technical support quality and many other factors.