AVLAB

THE INDEPENDENT ANTIVIRUS TESTS

# TEST OF FREE MALWARE SCANNERS

October 2017

# Outline

In the modern world, both individual and corporate users reach from time to time for software presented in the report. Due to the growing number of easy to detect generic threats and reviving samples of malware which uses malicious scripts, the role of traditional scanners is no longer as important as it was before. All applications tested by AVLab enable users to select scanning destination, which is verified against infected files. In the test, we haven't included scanners which offer only so called quick check for the most important system areas because it doesn't include user personal folders so verification of virus collection is impossible.

Malicious code developers who have access to advanced tools, ready-made guides, and even cybercriminal services, don't make task easier for experts seconded to hard analytical work. On the other hand, scanner designers find it very difficult to reconcile performance of these solutions and constantly increasing number of virus signatures. Traditional scanning techniques are being phased out in favour of more advanced, automated techniques with ability to learn threats patterns. In addition, some developers completely abandon on-demand scanners, and others make use of cloud model, leaving the functionality to scan only the most important system areas (drivers, registry, and running processes).

The cost of maintaining infrastructure and access to high-speed internet connections which are necessary for proper and rapid operation of such applications, can represent financial burden for small developers. For this reason, we can observe fading interest in traditional antivirus scanners which can very precisely check every part of the operating system while maintaining acceptable performance. With this in mind, AVLab experts have decided that this is the last edition of similar test. Next year, the methodology will evolve towards detecting threats in already infected systems, including detection of malicious processes and registry keys as well as running system services.

In detection of several thousand malicious applications which were collected 24 hours before each test day, the best results were achieved by: Emsisoft Emergeny Kit, Trend Micro HouseCall, Dr.Web CureIt, Kaspersky Removal Tool, ESET Online Scanner, and Comodo Cleaning Essentials. None of the tested products exceeded detection threshold of 95%, but taking into account the freshness of infected files (using local signatures or developer cloud) the static detection rate of about 90% can be considered satisfactory.

The disadvantage of on-demand scanning tests is their duration. In theory, scanning a few thousand infected files shouldn't take too long. Experience shows that it can take even the whole working day: scanning time of all files by individual applications was varied and ranged from several minutes (Emsisoft Emergency Kit, ClamAV Free Antivirus, Dr.Web CureIt) to tens of minutes (ESET Online Scanner). During the first two days of testing, record-breaking delay of several hours belonged to Arcabit Skaner Online. Unfortunately, on the third day, developer implemented an automatic update that prevented the test from being resumed — scanner was updated to a new version which allows to scan only system areas. Change in the ways that Arcabit Skaner Online operates during the test excluded the application from the test.

# Methodology

To check detection of the most popular antivirus scanners, we have prepared a virtual image of Windows 10 Professional x64 with the latest updates. The test material for the first part of the test in total of 18562 samples was obtained in cooperation with independent researchers. When selecting sample for testing, AVLab doesn't cooperate with any security software developer. This way, there is no suspicion that a sample of the tested application detects threats provided by its developer.

During testing, each application was installed on default settings. For Dr. Web Cureit and Kaspersky Removal Tool, automatic signature update wasn't available,  so tester were downloading new version of scanner every day.

Virus collection scanning:

1. Operating system image were restored for each tested application.

2. Threat samples were selected one day before each test.

3. Before choosing folder with infected files for scanning, signatures were updated to the latest version or new versions of scanners were downloaded (if it was necessary).

# Wyniki

| **Malware samples →** | **Day 1**<br>**3281** | **Day 2**<br>**3181** | **Day 3**<br>**1395** | **Day 4**<br>**2581** | **Day 5**<br>**3294** | **Day 6**<br>**4920** | **Total**<br>**Detected** | **Result**<br>**[ % ]** |
|---|---|---|---|---|---|---|---|---|
| *Emsisoft Emergeny Kit* | 3087 | 3036 | 1315 | 2516 | 2760 | 4769 | 17483 | 93,73 |
| *Trend Micro HouseCall* | 2969 | 2982 | 1295 | 2485 | 2680 | 4724 | 17135 | 91,86 |
| *Dr.Web CureIt* | 2977 | 2985 | 1265 | 2462 | 2606 | 4677 | 16972 | 90,99 |
| *Kaspersky Removal Tool* | 2833 | 2974 | 1254 | 2465 | 2632 | 4681 | 16839 | 90,27 |
| *ESET Online Scanner* | 2977 | 2984 | 1280 | 2054 | 2692 | 4744 | 16731 | 89,70 |
| *Comodo Cleaning Essentials* | 2714 | 2873 | 1205 | 2411 | 2487 | 4552 | 16242 | 87,07 |
| *ClamAV Free Antivirus* | 2116 | 2442 | 953 | 2132 | 1727 | 3939 | 13309 | 71,35 |
| *MBAM Free* | 1958 | 2059 | 860 | 1787 | 1670 | 3291 | 11625 | 62,32 |
| *Windows Defender* | 874 | 851 | 388 | 1041 | 762 | 2009 | 5925 | 31,76 |
| *Arcabit Skaner Online [1]* | 1286 | 2920 | — | — | — | — | — | — |

[1] Due to the significant and continuous increase in number of Arcabit Skaner Online users, developer has decided to optimize scanning mechanisms which allow you to detect and remove all infections as quickly as possible, regardless of the number of files. The newest version of Arcabit Skaner Online offers single, optimized mode for scanning system resources, so it takes just few minutes to check active processes, services, drivers, and libraries for infections. Custom folders scanning feature is no longer available, so it was impossible to continue the test.

# Awards

Certificates confirming the effectiveness of on-demand scanning were granted based on the following percentage threshold:

100% — 90%: BEST+++<br>
89% — 80%: BEST++<br>
79% — 70%: GOOD+<br>
69% — 0%: ONLY TESTED

Emsisoft Emergency Kit
Trend Micro HouseCall
Dr.Web CureIt
Kaspersky Removal Tool

ESET Online Scanner
Comodo Cleaning Essentials

ClamAV Free Antivirus

Malwarebytes Anti-Malware Free
Windows Defender

Our previous publications:

☞ Protection test against drive-by download attacks

☞ Test of antivirus modules for online e-payments protection

☞ Protection test against ransomware threats

Contact us for further details about the tests:
✉ kontakt@avlab.pl

Download granted certificates in high resolution:
↗ https://avlab.pl/dla-prasy

AVLab brings together security enthusiasts and professionals in one place. Our actions include testing and sharing results from analyzes with all Internet users. We aren’t controlled and/or related in any way to any security software developer or distributor. Our tests are independent and conducted in conditions similar to reality. We use a malicious software, tools, and bypassing security techniques that are used in real attacks.

If your company provides software or equipment for monitoring and security of corporate networks and individual user devices, we can prepare for you a dedicated reviews and tests which will be published in several languages on our website. Don’t hesitate – contact us.