AV-LAB

THE INDEPENDENT ANTIVIRUS TESTS

Test of free malware scanners

Checking the effectiveness of so-called on-demand malware scanners for threat detection is a very specific test.

Nowadays, both individual user and enterprise often use applications presented in this report. Their role remains unchanged – provides us certainty, that a device is secure.

September 2016

Synopsis

Checking the effectiveness of so-called on-demand malware scanners for threat detection is a very specific test. Nowadays, both individual user and enterprise often use applications presented in this report. Their role remains unchanged – provides us certainty, that a device is secure.

A key task of on-demand scanners is to detect and completely remove a threat, or remnants – and in some cases cure infected system, that can improve computer security and comfort.

All tested scanners let us specify the location, which should be checked for infected files based on implemented by given developer scanning technology. In this test we didn't included scanners, that offers only so-called quick scan, without taking into account user preferences on verifying security of specific location or partition.

In the detection of several thousand infected files, the best level of effectiveness has applications: Arcabit Skaner Online, Emsisoft Emergency Kit, ESET Online Scanner and Trend Micro HouseCall. Although other software received certificate confirming their effectiveness, they don't provide such a high level of detection as scanners, which have been granted the highest award "Best+++" detecting over 99% of 7089 samples.

Following scanners achieved detection ranging from 98 to 99 percent of 7089 various viruses used in this test: Dr.Web CureIt!, Kaspersky Virus Removal Tool, Panda Cloud Cleaner and Sophos Clean.

The time to scan all files by particular applications was very diverse and ranged from several to several dozen minutes, which wasn't reflected in higher detection rate. Following applications have

the longest scan time: Panda Cloud Cleaner, Comod Cleaning Essentials (in some cases this application requires system reboot to continue scanning) and Windows Defender.

Emsisoft Emergency Kit, Dr. Web Cureit!, Malwarebytes Anti-Malware and ClamWin Free Antivirus quickly managed to check sample package. Although, it should be acknowledge, with different results.

Following applications received the highest award BEST+++:

Emsisoft Emergency Kit, Trend Micro HouseCall, Arcabit Skaner Online, ESET Online Scanner

Methodology

On-demand scanner is specific software, so used by AVLab methodology transcend typical scanning of sample package. In addition to testing actual detection effectiveness of thousands malware samples, our test took into account the removal of harmful files and registry keys when the operating system has been infected.

In order to check detection of the most popular malware scanners offered as free tools by several manufacturers, we prepared a virtual image of Windows 10 Professional x64 with the latest updates. On each test day, the system was restored to its original state. This allows us to test every product in the identical environment.

A research material for the first part of the test with total of 7089 samples was obtained in collaboration with independent suppliers. Similarly – in second part of the test – we selected 6 specific threats, which wasn't included in the research material for the first part of the test.

AVLab obtains samples for tests by not collaborating with any security software developer. This way, there is no suspicion, that tested application detects threats provided by its developer.

During the test, all applications were installed with defaults settings, had Internet access and in case of two applications: Dr. Web Cureit and Kaspersky Removal Tool, their new version was downloaded every day (automatic update isn't available).

1 (scanning virus package)

1. We were restoring image of operating system for every tested software, so we accurately reproduced work environment for each application.
2. Each day, we were downloading unique threat samples.
3. Before indicating to scan folder with infected files, we were updating signatures to the latest version or downloading new version of application (if necessary) with integrated signatures.

2 (curing infected system)

1. For this part of the test, we chose different kinds of threats and manually analyzed them to determine what areas of the system are infected.
2. On restored image of the system from first part of the test, each sample was sequentially run, then we performed system reboot. If it was required, we granted permission to run malware with administrator privileges.
3. Tested applications were indented to detect infected file (dropper) or changes in system as a result of infection.
4. If it was required, we allowed system reboot while on-demand malware scanner was working.

Tested software

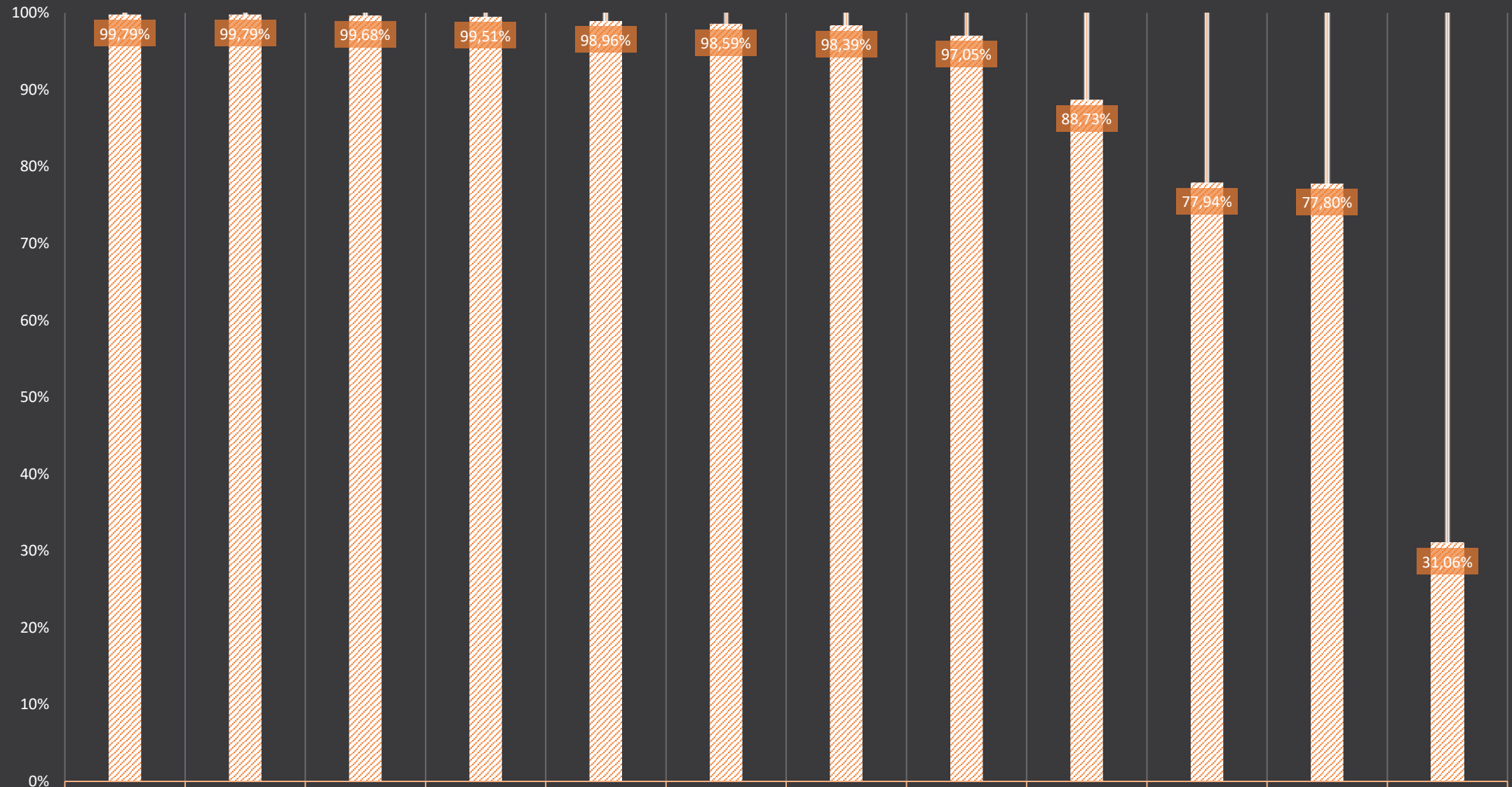
We stored versions of following applications on last day of the test.

Arcabit Skaner Online	*1.0.4*
*ClamWin Free Antivirus **	*0.99.1*
Comodo with Cleaning Essentials	*2.5.242177.201*
Dr.Web CureIt!	*11.1.2*
Emsisoft Emergency Kit	*11.9.0.6508*
ESET Online Scanner	*2.0.12.0*
Kaspersky Virus Removal Tool	*15.0.19.0*
Malwarebytes Antimalware Free	*2.2.1.1043*
Panda Cloud Cleaner	*1.1.9*
Sophos Clean (dawniej HitmanPro)	*3.7.13.262*
Trend Micro HouseCall	*(1.62)*
*Windows Defender **	*4.10.14393.0*

* CLAMWIN FREE ANTIVIRUS I WINDOWS DEFENDER PROVIDES REAL-TIME PROTECTION, BUT WE DIDN'T TAKE IT INTO ACCOUNT. DURING SCAN, PROTECTION HAS BEEN DISABLED.

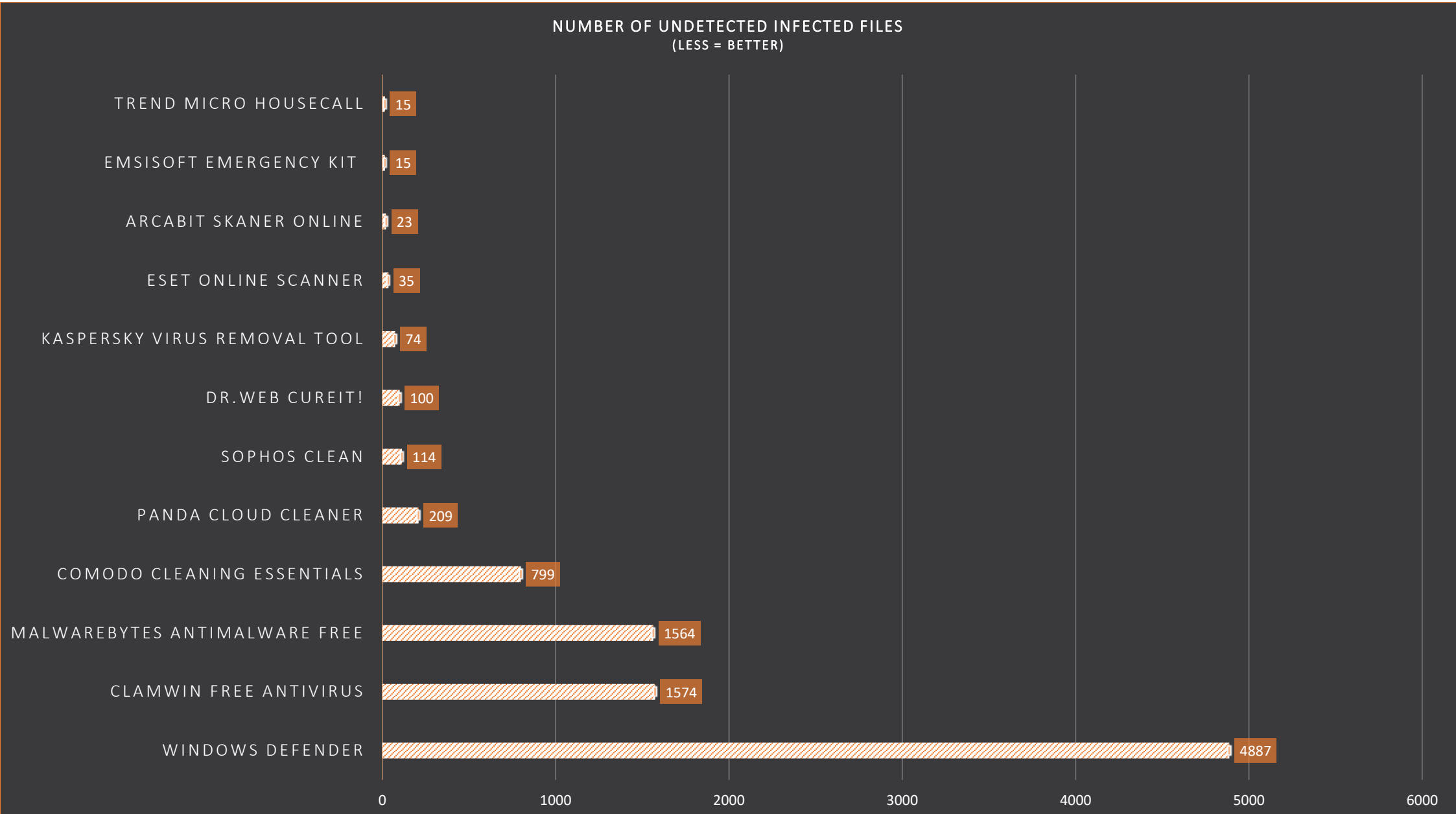
AV-LAB
THE INDEPENDENT ANTIVIRUS TESTS

NUMBER OF DETECTED THREATS OUT OF 7089 SCANNED FILES
(MORE= BETTER)



	Emsisoft Emergency Kit	Trend Micro HouseCall	Arcabit Skaner Online	ESET Online Scanner	Kaspersky Virus Removal Tool	Dr.Web CureIt!	Sophos Clean	Panda Cloud Cleaner	Comodo Cleaning Essentials	Malwarebytes Anti-Malware	ClamWin Free Antivirus	Windows Defender
Wynik	99,79%	99,79%	99,68%	99,51%	98,96%	98,59%	98,39%	97,05%	88,73%	77,94%	77,80%	31,06%

		Day 1	Day 2	Day 3	Day 4	Day 5	Day 6	Day 7	Total
	Number of malware	1039	883	1044	1006	917	915	1285	7089
	number of detected malware								
Arcabit Skaner Online		1035	882	1039	1000	914	913	1283	7066
ClamWin Free Antivirus		895	717	831	760	748	618	946	5515
Comodo Cleaning Essentials		958	713	862	953	803	859	1142	6290
Dr.Web CureIt!		1023	873	1026	981	904	915	1267	6989
Emsisoft Emergency Kit		1035	882	1039	1004	916	914	1284	7074
ESET Online Scanner		1030	880	1036	1001	914	913	1280	7054
Kaspersky Virus Removal Tool		995	881	1040	1002	912	910	1275	7015
Malwarebytes Antimalware Free		832	630	755	783	693	772	1060	5525
Panda Cloud Cleaner		1016	740	1016	1000	914	912	1282	6880
Sophos Clean		1034	844	1019	988	899	914	1277	6975
Trend Micro HouseCall		1037	879	1043	1004	915	913	1283	7074
Windows Defender		247	314	421	348	265	218	389	2202



	Windows Defender	ClamWin Free Antivirus	Malwarebytes Antimalware Free	Comodo Cleaning Essentials	Panda Cloud Cleaner	Sophos Clean	Dr.Web CureIt!	Kaspersky Virus Removal Tool	ESET Online Scanner	Arcabit Skaner Online	Emsisoft Emergency Kit	Trend Micro HouseCall
Wynik	4887	1574	1564	799	209	114	100	74	35	23	15	15

	sample A	sample B	sample C	sample D	sample E	sample F
Arcabit Skaner Online	+	+	+	+	+	+
ClamWin Free Antivirus	-	+	+	+	+	+
Comodo Cleaning Essentials	+	+	+	+	+	+
Dr.Web CureIt!	+	+	+	+	+	+
Emsisoft Emergency Kit	+	+	+	+	+	+
ESET Online Scanner	+	+	+	+	+	+
Kaspersky Virus Removal Tool	+	+	+	+	+	+
Malwarebytes Antimalware Free	+	+	+	+	+	+
Panda Cloud Cleaner	+ *	+	+	+	+	+
Sophos Clean	+ *	+	+	+	+	+
Trend Micro HouseCall	+	+	+	+	+	+
Windows Defender	-	+	-	-	+	-

+ a sample was detected or operating system was cured

- a sample was undetectable for tested solution

* SOMETIMES THE SCANNER REQUIRED OPERATING SYSTEM REBOOT IN ORDER TO REMOVE THREAT. IN THOSE TWO CASES, INFECTION WAS REMOVED ONLY IN RESCUE MODE.

sample A:

backdoor Kelihos — causes the infected workstation to send spam, steal sensitive information, download and run other infected files including trojans. Infected bot uses P2P connection to communicate with other zombie computers. I decentralized network, infected machine can operate as client or server C2 receiving and sending commands from control and management system.

sample B:

backdoor Careto — includes highly sophisticated malicious software consisting of a rootkit and bootkit. Observed by researches variations shows, that all version of this malware are indented for 32- and 64-bit Mac OS X, Linux, Windows and (probably) Android and iOS (also BlackBerry OS – unconfirmed information) systems. Because of its capabilities, Backdoor Careto (sometimes called The Mask) is believed to be the work of a nation state.

Backdoor Careto can capture network traffic, keystrokes, Skype conversation, PGP keys. It's able to analyze WiFi traffic, monitor all file operations, collect a list of documents from infected system, including encryption keys, VPN configuration, SSH keys and RDP files. In terms of sophistication, Backdoor Careto is one of the most advanced APT threats.

sample C:

keylogger Ardamax — commercial spyware, which was used in one of the social engineering campaign "the bailiff" aimed toward Polish citizens. With this tool it is possible to automatically send collected logs and data to any e-mail address or FTP account.

Keylogger Ardamax can: record keystrokes, save web browser history, capture video and sound from web camera, intercept text from clipboard, monitor AIM, Windows Live Messenger, ICQ, Skype, Yahoo Messenger, Google Talk, Miranda and QiP communicators. Stored information can be send to indicated e-mail address or FTP account.

sample D:

trojan Emotet — stores its files in system registry to hide from antivirus software. Trojan Emotet with modular design contains: its own installer, a banking module, an anti-spam bot, a module for stealing contacts from popular email clients (is able to spread, can steal addresses from email clients and send the same spam messages to victims from a contact list), module for DDoS attacks (Nitol DDoS bot).

Trojan Emotet contains a list of popular banks. If infected user visits one of the defined URLs, Emotet records all data send between user and website – even if website is encrypted with HTTPS protocol.

sample E:

trojan downloader — as the name suggests, trojan downloader contains malicious and potentially unwanted software, which is downloaded and installed on infected system. Downloaded in this way dropper file installs a appropriate virus, which can then be used for different purposes.

Dropper files are often used to carry known trojans, because it is much easier to create dropper file than completely new trojan, which antivirus software won't be able to detect.

In the test, we used Trojan, which creates few files on disk. One of them downloads additional malicious software.

sample F:

trojan Poweliks — uses a vulnerability in Microsoft Word and with a maliciously crafted Word document, which is distributed via e-mail, installs additional code, that is a PowerShell script encoded in Base64 triggering and executing a low-level program (shellcode) written in assembler. In the final stage, shellcode executes binary program, which tries to communicate with encoded IP addresses to receive futher commands from C&C servers.

Trojan Powerliks can be used to download and execute files. Its actions are stored in the registry – it doesn't create any file on the hard disk, so to detect this threat, it's required to recognize infected Word document or protect / scan registry.

99% >	BEST+++
97-98%	BEST++
95-96%	GOOD+
94-80%	AVERAGE
79%	NOT RECOMMENDED

Emsisoft Emergency Kit
Trend Micro HouseCall
Arcabit Skaner Online
ESET Online Scanner

Kaspersky Virus Removal Tool
Dr.Web CureIt!
Sophos Clean
Panda Cloud Cleaner

Comodo Cleaning Essentials
Malwarebytes Anti-Malware Free
ClamWin Free Antivirus

Windows Defender

Contact on the tests for developers: kontakt@avlab.pl

Download granted certificates in high resolution: 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 software producer in any way.

AVLab tests are independent and take place in conditions close to reality. Don't be guided by our results when making final decision in choosing antivirus program. In order to make final choice we suggest 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 things..

avlab.pl