



THE INDEPENDENT ANTIVIRUS TESTS



protection test against
ransomware threats

software for home user
and SMB company

October 2016

Date of the test: October 2016

Synopsis

An objective of the test conducted by AVLab in October 2016 was to check a real protection provided by security software against threats of crypto-ransomware to home users and small and medium businesses. Results presented in this document reflect actual effectiveness of antivirus software, that by using all available protection components and correlated dynamic heuristic and behavioral methods, provide end users with comprehensive real-time protection, including a detection of unknown crypto-ransomware threats.

Although, some tested security suites allow users to create a separate folder, where files are continuously monitored against modification by antivirus software, purpose of the test was to verify, if it handles modern and unknown threats of crypto-ransomware. This kind of malicious software is highly destructive — often causes a financial loss and affects a business productivity resulting in a standstill in a company.

RANSOMWARE AND CRYPTO-RANSOMWARE

Ransomware belongs to a type of malicious software, that prevents or restricts users from accessing a operating system.

Nowadays, ransomware threats have gained a new name: crypto-ransomware. These viruses encrypt specific types of files, and then display a message requesting a ransom in exchange for decrypting data.

Among the latest variants of ransomware, we can mention one more type: disk-encryption. These malicious applications or scripts, having destructive impact to user computers, encrypt the Master Boot Record (MBR) and overwrite it with its own one, which causes a system reboot. Due to this action, malware displays a fake message about disk scanning for errors (CHKDSK). Meanwhile, crypto-ransomware encrypts the Master File Table (MFT), which contains entries for each file on a partition. Therefore, a operating system doesn't know where files are stored, making it impossible to properly boot up a computer.

User computers can be infected in many different ways. Crypto-ransomware usually spreads via e-mail, concealing under form of an invoice, debt enforcement proceedings or information about undelivered postal item.

In recent months, FortiGuards Labs experts have noticed, that currently one of the most popular variant of ransomware in Poland — Locky — is downloaded by Nemucod Trojan. On the other hand, malware analysts working for F-Secure Labs, have identified a malicious campaign, that installs Cerberus crypto-ransomware by taking advantage of vulnerabilities in Adobe Flash and using tools like Magnitude Exploit Kit.

In the category for home users, these applications received the highest award:

Arcabit Internet Security

Comodo Cloud Antivirus

Emsisoft Internet Security 11

Emsisoft Internet Security 12

Foltyn SecurityShield

F-Secure SAFE

G DATA Internet Security

Kaspersky Internet Security 2017

Qihoo 360 Total Security

SecureAPlus Premium

Trend Micro Internet Security 2017

Voodoo Shield Pro

Zemana Anti-Malware Premium

ZoneAlarm Internet Security Suite

In the category for small and medium businesses, these applications received the highest award:

Arcabit Endpoint Security

Comodo ONE Enterprise

Emsisoft Anti-Malware for endpoints

F-Secure Protection Service for Business

G DATA Client Security Business

Kaspersky Endpoint Security 10 for Windows

Seqrite Endpoint Security Enterprise Suite

Sophos Endpoint Protection



Methodology

In order to apply principles of equality for tests, we decided to test with default settings and in an identical test environment all known antivirus software for home users and small and medium businesses, as well as two independent applications: Foltyn SecurityShield and Voodoo Shield Pro, which differ in terms of operability from traditional antivirus software. By preserving this principle, every application has been verified in the same conditions and for the same collection of threats.

For testing, we used 28 malicious software files of crypto ransomware. Among others there were: Cerber, CryptXXX, DetoxCrypto, Hitler Ransomware, HolyCrypt, Locky, Numecod, Petya, Jigsaw, Vipasana, Stampado and many others. The study included the total amount of 28 samples collected in a collaboration with independent researchers.

AVLab obtains samples for tests without collaborating with any security software developer. This way, there is no suspicion, that tested application detects threats provided by its developer.

The only equitable method of comparative testing is to examine all application in the same conditions and on the same basis — on default settings. There are antivirus applications on the market, which have special mechanisms protecting files or folders against encryption, but not all developers decided to enable these components by default. This gives rise to suspicions, that these mechanisms can excessively affect the overall performance of the security suite, reducing its score in benchmark tests.

In order to check a protection effectiveness of the most popular antivirus applications for businesses and home users, we have prepared an image of Windows 10 Professional x64 with the latest updates dated the day before the test. This way, all products have been tested in the identical test environment and had access to the Internet.

Operation algorithm

1. We were restoring the image of operating system for every tested software, so we accurately reproduced the work environment for each application.
2. If necessary, we granted a permission to run malware with administrator privileges.
3. Tested software were indented to prevent the encryption of prepared collection of files located on the desktop.

WHY CRYPTO-RANSOMWARE CAUSES PROBLEM TO HOME USERS?

Bitdefender has published a report from survey conducted in November 2015 among 3009 Internet users from the US, France, Germany, Denmark, United Kingdom and Romania, in which were raised issues with threats of ransomware (Those encrypting files and demanding a ransom for data restoration):

- 50% of the respondents don't know anything about threats of ransomware.
- Up to half of respondents are willing to pay up to \$500 for files decryption.
- Personal documents, which appear at the top of the list of the most valuable data for the ordinary citizens, are the most important for the users.
- The users from United Kingdom and Romania are willing to pay the most for the file recovery.
- In 2015, users from the United States were main victims of crypto-ransomware.

Tested applications

Software for home users:

Product	Version
Ad-Aware Free Antivirus+	11.12.945.9202
Arcabit Internet Security	2016.00.248
Avast Free Antivirus 2016	12.3.2280
Avast Internet Security 2016	12.3.2280
AVG AntiVirus Free Edition	16.121.7858
AVG Internet Security	16.121.7858
Avira Free Antivirus	15.0.22.54
Avira Internet Security Suite	15.0.22.54
Bitdefender Antivirus Free Edition	1.0.3.9
Bitdefender Internet Security 2017	21.0.18.898
Comodo Cloud Antivirus	1.6.400657.347
Comodo Internet Security 8	8.4.0.5165
Comodo Internet Security Pro 10 (BETA)	10.0.0.5144
Dr Web Katana	1.01.07290
Dr. Web Space Security	11.03.09220
Emsisoft Internet Security 11	11.10
Emsisoft Internet Security 12	12.0
ESET Smart Security 9	9.0.385.1
ESET Smart Security 10 (BETA)	10.0.171.0
Foltyn SecurityShield	1.0.0

FortiClient Free	5.4.1.0840
F-Secure SAFE	16.3
G DATA Internet Security	25.2.0.3
Kaspersky Internet Security 2017	17.0.0.611
Malwarebytes Anti-Malware Premium	2.2.1.1043
Malwarebytes Anti-Ransomware (BETA)	0.9.17.661
McAfee LiveSafe	15.1.156
Norton Security	22.8.0.50
Panda Free Antivirus	17.00.01.0000
Panda Internet Security	17.00.01.0000
Qihoo 360 Total Security	8.8.0.1080
SecureAPlus Premium	4.3.3
Sophos HOME	10.5.4
Trend Micro Internet Security 2017	11.0.158
TrustPort Internet Security	2016.16.02.5698
Voodoo Shield Pro	3.45 (beta)
Webroot SecureAnywhere Complete	9.0.13.50
Zemana Antimalware Premium	2.50.133
ZoneAlarm Internet Security Suite	15.0.123.17051
Windows Defender	4.10.14393.0

WHY CYBER CRIMINALS ARE INTERESTED IN COMPANIES AND PUBLIC INSTITUTIONS?

Companies are identified with money.

Cyber criminals are aware, that some percent of the victims will pay a ransom anyway.

Encrypted data is too valuable to be written off.

Company computers are often insufficiently protected.

The weakest link in the security chain is a human (an employee).

An employee may be an easy victim of social engineering.

Some variants of crypto ransomware encrypt files not only on the local drives, but also in the cloud and on the local network.

Most companies won't report the attack in fear of a contact with law enforcement and loss of reputation.

Small businesses are unprepared for advanced attacks.

Small businesses aren't in control of users: they don't take into account a trend of BYOD and Shadow IT.

Public and government institutions manage large databases, that contain valuable information suitable for sale.

Protection level of public institutions is lower than the private sector.

Public sector employees are insufficiently trained.

Public institutions often use outdated software.

For a long time the public sector suffers from deficit of computer security experts.

Solutions for small and medium businesses:

Product	Version
Arcabit Endpoint Security	2016.00.248
AVAST for Business Endpoint Security	12.3.2515
AVAST for Business Basic Antivirus	12.3.2515
AVG AntiVirus Business Edition	2016.111.7797
Avira Antivirus for Endpoint	15.0.22.54
Bitdefender GravityZone	6.2.10.883
Comodo ONE Enterprise	8.3.0.5191
Emsisoft Anti-Malware for Endpoints	11.10
ESET Endpoint Security	6.4.2014.2
F-Secure Protection Service for Business	12.0.1
G DATA Client Security Business	14.0.0.641
Kaspersky Endpoint Security 10 for Windows	10.2.5.3201
Kaspersky Anti-Ransomware Tool for Business	1.1.24.0
Panda Adaptive Defense	7.62.0
Seqrite Endpoint Security Enterprise Suite	17.00
Sophos Endpoint Protection	11.5.1
Trend Micro Worry-Free Business Security	19.0.2166

Product

Results of solutions dedicated for home users and micro businesses.

Number of malware sample - >	<u>1</u>	<u>2</u>	<u>3</u>	<u>4</u>	<u>5</u>	<u>6</u>	<u>7</u>	<u>8</u>	<u>9</u>	<u>10</u>	<u>11</u>	<u>12</u>	<u>13</u>	<u>14</u>	<u>15</u>	<u>16</u>	<u>17</u>	<u>18</u>	<u>19</u>	<u>20</u>	<u>21</u>	<u>22</u>	<u>23</u>	<u>24</u>	<u>25</u>	<u>26</u>	<u>27</u>	<u>28</u>	
Ad-Aware Free	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0/1	1	0/0	1	1	0/0	1	1	1	0/0	1	
Arcabit Internet Security	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0/1	1	0/1	1	1	0/1	1	1	1	0/1	1	
Avast Free Antivirus	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0/0	0/0	1	1	1	1	1	
Avast Internet Security	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0/1	0/0	1	1	1	1	1	
AVG AntiVirus Free	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0/0	1	1	1	1	1	1	1	0/0	1	
AVG Internet Security	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0/0	1	1	1	1	1	1	1	0/0	1	
Avira Free Antivirus	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0/0	1	1	0/0	0/0	1	1	0/0	1	1	0/0	0/0	1	
Avira Internet Security	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0/0	0/1	1	1	0/1	1	1	1	1	1	
Bitdefender Free	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0/1	1	1	0/0	1	1	1	0/1	1	
Bitdefender IS 2017	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0/1	1	0/1	1	1	0/0	1	1	1	0/1	1	
Comodo Cloud Antivirus	0/1	1	0/1	0/1	1	1	0/1	0/1	1	1	1	1	0/1	1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	1	0/1	1	0/1	1
Comodo IS 8	1	1	0/1	0/1	1	1	0/1	0/1	1	1	1	1	0/1	1	1	0/1	0/1	0/1	0/1	0/1	0/1	0/0	0/0	0/1	1	0/1	1	0/1	1
Comodo IS Pro 10 (BETA)*	1	1	0/0	0/0	1	1	0/0	0/0	1	1	1	1	0/0	1	1	0/0	0/0	0/0	0/0	0/0	0/0	0/0	0/0	0/0	1	0/0	1	0/0	1
Dr. Web Katana	0/1	0/1	0/1	0/1	0/1	0/0	0/0	0/1	0/1	0/1	0/1	0/1	0/0	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/0	0/0	0/0	0/1	0/1	0/1	0/1	0/0	0/1
Dr. Web Space Security	1	1	1	1	1	1	0/1	1	1	1	1	1	0/0	1	1	1	1	1	1	1	0/1	1	1	1	1	1	1	1	1
Emsisoft IS 11	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0/1	1	0/1	1	1	0/1	1	1	1	0/1	1	
Emsisoft IS 12	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0/1	1	0/1	1	1	0/1	1	1	1	0/1	1	
ESET Smart Security 9	1	1	1	1	1	1	1	1	1	1	1	1	0/0	1	1	1	1	1	0/0	1	1	1	1	1	1	1	0/0	1	
ESET SS 10 (BETA)	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0/0	1	1	1	1	1	1	1	1	1	
Foltyn SecurityShield	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	
FortiClient Free	1	1	1	0/1	1	1	1	1	1	1	1	1	1	1	1	1	1	0/1	0/0	0/1	1	1	0/0	1	0/0	1	1	1	
F-Secure SAFE	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0/1	1	0/1	1	1	0/1	1	1	1	1	1	
G DATA Internet Security	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0/1	1	0/1	1	1	0/1	1	1	1	0/1	1	
Kaspersky IS 2017	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0/1	1	1	1	0/1	1	0/1	1	1	1	
MBAM Premium	1	1	1	1	1	1	0/0	0/1	1	1	1	1	1	1	1	0/0	1	0/1	0/0	0/1	0/1	0/1	1	1	0/0	0/0	1	1	
MBAM Anti-R. (BETA)	0/0	0/1	0/1	0/1	0/0	0/0	0/0	0/0	0/0	0/0	0/1	0/1	0/0	0/0	0/0	0/0	0/1	0/0	0/0	0/0	0/0	0/0	0/0	0/0	0/0	0/1	0/0	0/0	
McAfee LiveSafe	1	1	1	1	1	1	0/1	0/1	1	1	1	1	1	1	1	0/0	1	0/1	0/0	0/0	0/1	0/1	0/0	1	0/1	0/0	1	1	
Norton Security	1	1	1	1	1	1	0/1	1	1	1	1	1	1	1	1	1	1	0/1	0/0	0/1	0/1	1	0/0	1	0/0	1	1	1	
Panda Free Antivirus	1	1	1	1	1	1	0/1	0/1	1	1	1	1	1	1	0/1	0/0	1	1	0/0	0/0	0/0	0/0	0/0	0/0	1	1	0/1	1	
Panda Internet Security	1	1	1	1	1	1	0/1	0/1	1	1	1	1	1	1	0/1	0/0	1	1	0/0	0/1	0/1	0/1	0/0	1	1	1	1	1	
Qihoo 360 Total Security	1	1	0/1	1	1	1	1	0/1	1	1	1	1	1	1	1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	1	0/1	0/1	1	1	

<i>SecureAPlus Premium</i>	0/1	1	0/1	0/1	1	1	0/1	0/1	1	1	1	1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	1	0/1	0/1	0/1	0/1
<i>Sophos HOME</i>	1	1	1	1	1	1	0/1	1	1	1	1	1	1	1	1	0/0	1	0/1	0/0	1	0/1	1	0/0	1	0/1	0/1	1	1
<i>Trend Micro IS 2017</i>	1	1	1	1	1	1	1	1	1	1	1	0/1	1	1	1	0/1	1	0/1	0/1	1	1	1	0/1	1	0/1	0/1	1	1
<i>TrustPort IS</i>	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0/1	1	1	1	1	1	0/0	1	1	1	1
<i>Voodoo Shield Pro*</i>	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1
<i>Webroot SA Complete</i>	0/1	1	1	1	1	1	0/1	0/1	1	1	1	1	0/0	1	0/1	0/0	1	0/1	0/0	1	0/1	0/1	0/0	0/1	0/1	0/1	0/0	0/1
<i>Zemana AM Premium</i>	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0/1	0/1	0/1	1	1	1	1	1
<i>ZoneAlarm Internet Security Suite</i>	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0/1	1	1	1	1	0/1	1	0/1	1	1	1
<i>Windows Defender</i>	1	1	1	1	1	1	0/0	0/0	0/0	1	1	0/0	0/0	0/0	1	1	0/0	0/0	0/0	1	0/0	0/0	0/0	0/0	0/0	0/0	0/0	0/0

0/0: files were encrypted, protection was ineffective

0/1: file was run and explicitly blocked by proactive protection

1: file was run and blocked by on access scanning

* Voodoo Shield Pro was tested in two modes: the AutoPilot mode on and the ApplicationWhitelist (SMART, ALWAYS ON). Identical results in both cases.

* Comodo Internet Security Pro 10 BETA failed to respect the automatic sandbox module settings, which is the core protection against unknown malware. During testing, stable version hasn't been available yet, so don't put an equal sign between BETA and stable version results of Comodo Internet Security Pro 10.

Product

Results of solutions dedicated for small and medium businesses.

	<u>1</u>	<u>2</u>	<u>3</u>	<u>4</u>	<u>5</u>	<u>6</u>	<u>7</u>	<u>8</u>	<u>9</u>	<u>10</u>	<u>11</u>	<u>12</u>	<u>13</u>	<u>14</u>	<u>15</u>	<u>16</u>	<u>17</u>	<u>18</u>	<u>19</u>	<u>20</u>	<u>21</u>	<u>22</u>	<u>23</u>	<u>24</u>	<u>25</u>	<u>26</u>	<u>27</u>	<u>28</u>
Arcabit Endpoint Security	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0/1	1	0/1	1	1	0/1	1	1	1	0/1	1
AVAST for Business Endpoint Security	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0/0	1	1	1	1	1
AVAST for Business Basic Antivirus	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0/0	1	1	1	1	1
AVG AntiVirus Business Edition	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0/0	1	1	1	1	1	1	1	1	1
Avira Antivirus for Endpoint	1	1	1	1	1	1	0/1	0/1	1	1	1	1	1	1	1	0/1	1	1	0/0	0/1	0/1	0/1	0/0	1	1	0/1	0/1	1
Bitdefender GravityZone	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0/1	1	1	1	1	0/0	1	1	1	1	1
Comodo ONE Enterprise	1	1	0/1	0/1	1	1	0/1	0/1	1	1	1	1	0/1	1	1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	1	0/1	1	0/1	1
Emsisoft Anti-Malware for endpoints	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0/1	1	1	1	1	1
ESET Endpoint Security	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0/0	1	1	1	0/0	1	1	1	1	1
F-Secure Protection Service for Business	1	1	1	1	1	1	0/1	1	1	1	1	1	1	1	1	1	1	1	1	1	0/1	1	0/1	1	1	1	1	1
G DATA Client Security Business	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
Kaspersky Endpoint Security 10 for Windows	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0/1	1	1	1	1	1
Kaspersky Anti-Ransomware Tool for Business	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/0	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1
Panda Adaptive Defense	1	1	1	1	1	1	0/1	0/1	1	1	1	1	1	1	0/1	1	1	1	1	1	0/1	0/1	0/0	1	1	1	1	1
Seqrite Endpoint Security Enterprise Suite	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0/1	1	1	1	1	1
Sophos Endpoint Protection	0/1	1	1	1	1	1	0/1	0/1	1	1	1	1	1	1	0/1	1	1	1	1	1	0/1	0/1	1	1	1	1	1	1
Trend Micro Worry-Free Business Security	1	0/0	0/0	0/1	1	1	1	1	0/0	1	1	0/0	1	1	1	0/0	0/0	0/0	1	1	0/0	1	0/0	1	1	0/1	0/1	1

0/0: files were encrypted, protection was ineffective

0/1: file was run and explicitly blocked by proactive protection

1: file was run and blocked by on access scanning

SAFESTORAGE IN ARCABIT INTERNET SECURITY

Many times tested Arcabit software, like most security applications, uses file, email and browser monitoring. But unlike other competitive and similar security suites, implemented by the developer, unique SafeStorage mechanism, particularly drew our attention.

A very important purpose of SafeStorage mechanism is to protect data against catastrophic, from the user point of view, effects of actions taken by crypto-ransomware threats.

During an attempt of file encryption SafeStorage creates a copy of it, allowing user and administrator (SafeStorage also takes into account a shared network resources) to restore encrypted files to the state before an infection in less than a minute.

The copies are stored in internal database of Arcabit suite, in a zipped and an encrypted form and they are protected by the internal mechanisms of Arcabit suite — external applications can't access them.

Additionally, SafeStorage has its own mechanism for database, that cleans up and remove files when the application decides, that a potential threat has been subsided. This allows to efficiently use a disk space (mechanisms that clean up SafeStorage are triggered when idle, reducing an impact on the system performance).

During installation, Arcabit security suite prompts the user where he wants to keep SafeStorage database (only if there are more than one disk or partition on the system). Therefore, user can effectively control a resource consumption, e. g. when first disk is low capacity SSD and the second disk is high capacity HDD, which is only used for data storage.

SafeStorage works synchronously with events in the files system, creating copies of documents, photos and other important files in situations, that could potentially endanger their contents. Synchronicity work of SafeStorage ensures that a copy of a file will be moved intact to the internal database of Arcabit suite. However, the key SafeStorage mechanisms work in the context of driver in kernel mode, which brings a significant advantage over threats of ransomware and other applications, that can (even potentially) damage user files.

Within the context of a very effective method of restoring files after crypto-ransomware attack (without having a backup files on external storage), we strongly recommend you Arcabit Internet Security.



kwarantanna



SafeStorage



kopie
zapasowe



menadżer
procesów



audyt systemu



Arcabit
Rescue Disk



czyszczenie
systemu

WHY USERS HAVE PROBLEMS?

Safety education is insufficient, which is reflected in an awareness in the context of a manipulation by the social engineering attacks.

Home users only incidentally care about a backup of their data. Completely different than small and medium businesses.

Users insufficiently protect their files and systems.

Users don't update their software. This creates an opportunity for attacks with exploits.

User are incorrectly certain, that since they don't click on malicious links and enter suspicious websites, they've got nothing to fear.

Users aren't aware, that a transparent drive-by attacks and these exploiting vulnerabilities inside browser and installed software, don't display any alert in the system — and in addition don't require any interaction.

Computers protected by antivirus software aren't responsible for security. Decision making on this issue is still in the hands of users.

Result interpretations

At the beginning, we mentioned that the objective of this test was to indicate the best solution for the real-time protection against crypto-ransomware. To maintain equal conditions for the test, we decided to use the default settings, although some of the tested security suites have protection against ransomware, but developers decided to disable by default this specific functionality.

Moreover, for a long time we thought about whether to add an extra category of evaluation: restoring file after crypto-ransomware attack. After careful inspection, it turned out, that it would be unjust towards all tested software — for one reason: Arcabit Internet Security would receive overwhelming advantage, which doesn't reflect the true picture of mechanisms available in other suites with default settings. With SafeStorage, user can take advantage of the full capabilities of Arcabit Internet Security Suite without any additional configuration.

We didn't take into account dedicated tools available for files decryption, because their effectiveness depends on too many factors. This kind of tools allow us to restore files only in case of successful exploitation of incorrect implementation encryption functions or using private key acquired through cooperation of the police and computer security experts. Such test would be very difficult to prepare and take a very long time — disproportionately to the needs of rapidly changing threat of crypto-ransomware

Granted awards

BEST+++

100% effectiveness

GOOD+

2 infections allowed

ONLY TESTED

more than 4 infections

BEST++

1 infection allowed

AVERAGE

3 infections allowed

For software indented for protecting home users and micro businesses computers:



Arcabit Internet Security
Comodo Cloud Antivirus
Emsisoft Internet Security 11
Emsisoft Internet Security 12
Foltyn SecurityShield
F-Secure SAFE
G DATA Internet Security
Kaspersky Internet Security 2017
Qihoo 360 Total Security
SecureAPlus Premium
Trend Micro Internet Security 2017
Voodoo Shield Pro
Zemana Antimalware Premium
ZoneAlarm Internet Security Suite



Avast Internet Security 2016
Avira Internet Security Suite
Bitdefender Antivirus Free Edition
Bitdefender Internet Security 2017
Dr. Web Space Security
ESET Smart Security 10 (BETA)
TrustPort Internet Security



Avast Free Antivirus 2016
AVG AntiVirus Free Edition
AVG Internet Security
Comodo Internet Security 8



Ad-Aware Free Antivirus
ESET Smart Security 9
FortiClient Free
Norton Security
Panda Internet Security
Sophos HOME



Malwarebytes Anti-Malware Premium
McAfee LiveSafe
Webroot SecureAnywhere Complete
Avira Free Antivirus
Dr Web Katana
Panda Free Antivirus
Comodo Internet Security Pro 10 (BETA)
Windows Defender
Malwarebytes Anti-Ransomware (BETA)

For software indented for protecting small and medium businesses workstations:



Arcabit Endpoint Security
Comodo ONE Enterprise
Emsisoft Anti-Malware for endpoints
F-Secure Protection Service
for Business
G DATA Client Security Business
Kaspersky Endpoint Security 10
for Windows
Seqrite Endpoint Security
Enterprise Suite
Sophos Endpoint Protection



Avast for Business Endpoint Security
AVAST for Business Basic Antivirus
AVG AntiVirus Business Edition
Bitdefender GravityZone
Kaspersky Anti-Ransomware Tool
for Business
Panda Adaptive Defense



Avira Antivirus for Endpoint
ESET Endpoint Security





Trend Micro Worry-Free Business Security

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 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.



avlab.pl