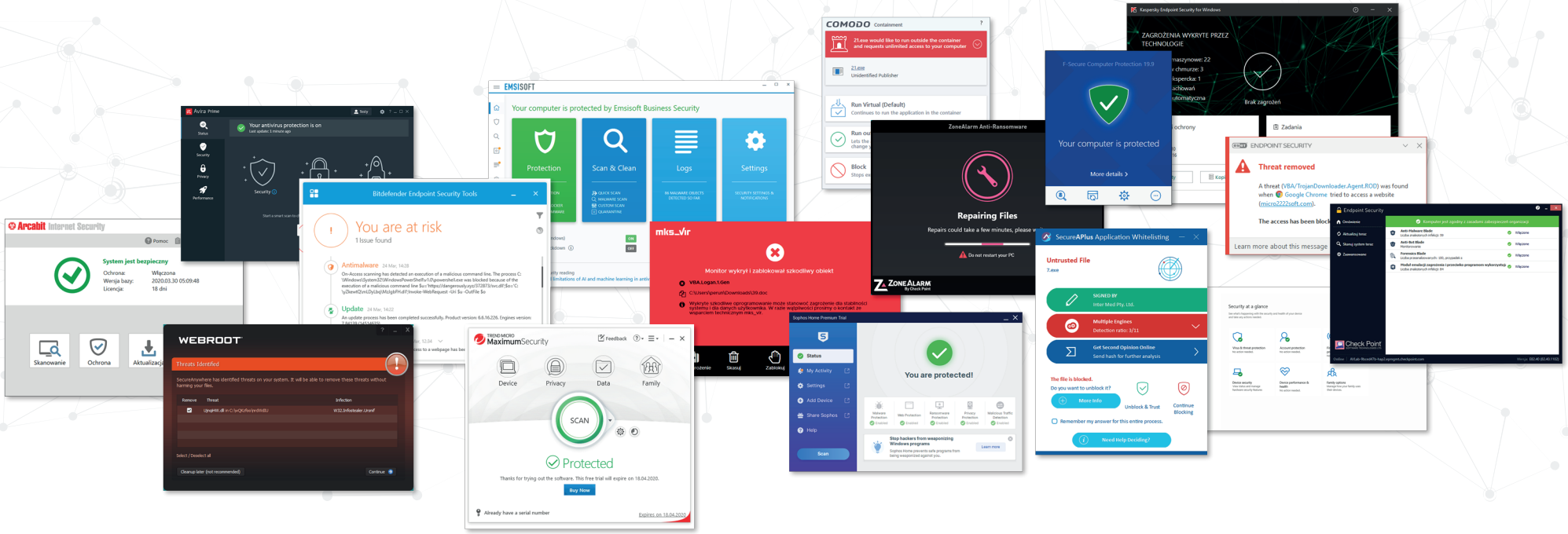
AV-TEST LAB

THE INDEPENDENT ANTIVIRUS TESTS



Date of the test: April 2020

The best antiviruses based on test of protection against fileless attacks, ransomware, and macro viruses

Main objectives of the test

The verification of security effectiveness of popular applications to protect personal computers and workstations against most common threats and cyberattacks since the beginning of 2020.

In the last quarter, cybercriminals understood that in order to avoid detection by traditional security tools, they need to combine popular types of malicious software with modern techniques of attacking. According to the reports of global IT companies, fileless attacks will be very a common phenomenon in the coming quarters. Using this type of security deception has increased by several hundred percent as Trend Micro observed in late December 2019. Tools to automatic search vulnerabilities in applications programmed by hackers are now more technically capable than before. They are also harder to observe because require no user interaction in order to execute malicious code.

Destroying the work of universities, public hospitals, and private clinics that try together to isolate diseases, is an acute problem. It is difficult to understand what primitive motives are driven by criminals, and why they turn against science and healthcare. The actions of online criminals have negative consequences in the economy as we could observe in recent weeks. Major news services wrote about incidents of forcing ransom healthcare and education institutions in exchange for encrypting data lost as a result of a cyberattack.

Trends in cyberthreats in 2020 underline the need for invest in solutions that will allow users to provide detailed reporting of significant changes to systems and networks. Developers and providers of IT solutions should take responsibility for solutions that are provided to companies and end users. On the other hand, enterprises must understand the risk, and start to protect themselves proactively against attack, and also mitigate the effects of potential attacks. Most organizations cannot afford to keep basic security to protect network, not to mention maintaining 24-hour units of monitoring infrastructure security. Companies should consider collaborating with an experience provider of security services who will help them protect IT systems against modern cyberattacks.



Malicious Office documents

Macros can be easily connected to sociotechnical techniques in phishing campaigns. Document circulation in enterprises is a normal thing, and the Office suit installed by default forces us to protect IT systems against the attempt of infecting systems.



Ransomware attacks

An organization that will lose an access to the data can have not only a serious P.R. problem, but also financial due to penalties imposed by the so called RODO. Attacks involving ransomware samples are still popular. Hackers focus mainly on medium and large organizations without excluding public institutions. And now they are not trying to extort ransom in exchange for data decryption. Criminal activities become more menacing because of increasing trade of stolen files content on forums in Tor network.



Techniques of fileless infecting of IT systems

Modern operating systems already have built-in tools used by criminals, and so they do not need to install malicious software. A script in PowerShell is easy to obfuscate, and therefore cannot be detected using older security tools. Administrators commonly use PowerShell to automate certain activities, and functioning of system processes, such as PowerShell or Windows Management Instrumentation is not unusual a corporate environment.

Hackers have a great scope of activity in targeted campaigns because they prepare to attack carefully. Typically, “a cyberattack lifecycle” is as follows: first, a target is recognized, then tools are adapted to victim’s IT system. The last step is to attack and break the chain. Targeted attacks of ATP (Advanced Threat Persistence) are more difficult to detect and stop. Unconventional techniques of bypassing security, if used in a controlled environment, they can tell a lot about protection effectiveness of a given product. Criminals care most about the money, this is why the majority of campaigns are directed to the masses. IT systems which are protected with recommended solutions, are in the advantageous position to an attacker.

Macro viruses - technical details

NO.	MACRO VIRUSES	FILE NAME
1	c141a187c5b2c7a8d91a923a0f79a8ba4c1484e7295f922c5fac3d7c0d6792b9	1.doc
2	276e5e230766222ed208b1d4d1bd994acc2e763ca71c6d28f41a17988375d099	2.doc
3	23a4d7782a91e2a297f8b082500a6036048940afbee12a951dc02da2a0004ec2	3.doc
4	6bed7ef049d8d9728a09a94488ac8670c9c20c0e6c294f80fd2153c37a2bead7	4.doc
5	dc0699e81874193e461b6a2ca9bf7164c2fe4d214381d1b5b875203541efcab7	5.doc
6	174e0317f0e0f1d0b7aa5f9fd9bff476b8a910d067effeadfa2ea9ebfcd03a46	6.doc
7	db29ff54d37ebd7694c5190fc3ddb0ceffd896c7ed43b3f4abb8ab28658ff955	7.doc
8	b98a210cb0682233e9b26bf11137456f9c93b2ed49bd15a903a88171fe754f87	8.doc
9	620b091c4d2e1da67922cba308d9d88c2e7d9de10bda08384f597f3cb1e2e3cd	9.doc
10	8e76efb8ca44047f31a9933cb281a119905ec7e390b774ac2493d5c29bbdcbe5	10.doc
	...	
65	6a864e0fc61af9a2a824654ebd6165c9ced5e9ccb2a4e6d0bd8bec7d2a83766e	65.xls



LEVEL 1

The browser level, i.e. a virus has been stopped before or after it has been downloaded onto a hard drive.



LEVEL 2

The system level, i.e. a virus has been downloaded, but it has not been allowed to run.

LEVEL 3

The analysis level, i.e. a virus has been run and blocked by a tested product.



FAIL

The failure, i.e. a virus has not been blocked and it has infected a system.

Macro viruses

	Number ordered of tested malware sample												
PRODUCT NAME	1	2	3	4	5	6	7	8	9	10	...	65	THREATS BLOCKED	CERTIFICATE GRANTED
ARCABIT Internet Security	L1	L1	L1	L1	L1	L1	L1	L1	L1	L1		L3	65/65	AWARD BEST+++
AVIRA Antivirus Pro	L1	L1	L1	L1	L1	L1	L1	L1	L1	L1		L3	65/65	AWARD BEST+++
AVIRA Prime	L1	L1	L1	L1	L1	L1	L1	L1	L1	L1		L3	65/65	AWARD BEST+++
BITDEFENDER GravityZone Elite	L1	L1	L1	L1	L1	L1	L1	L1	L1	L1		L1	65/65	AWARD BEST+++
CHECK POINT Endpoint Security	L1	L1	L1	L1	L1	L1	L1	L1	L1	L1		L3	65/65	AWARD BEST+++
COMODO Advanced Endpoint Protection	L3	L3	L3	L3	L2	L3	L3	L2	L2	L2		L3	65/65	AWARD BEST+++
COMODO Internet Security	L3	L3	L3	L3	L2	L3	L3	L2	L2	L2		L3	65/65	AWARD BEST+++
EMSISOFT Anti-Malware	L3	L3	L3	L3	L3	L3	L3	L3	L3	L3		L3	65/65	AWARD BEST+++
EMSISOFT Business Security	L3	L3	L3	L3	L3	L3	L3	L3	L3	L3		L3	65/65	AWARD BEST+++
ESET Endpoint Protection Advanced Cloud	L1	L1	L1	L1	L1	L1	L1	L1	L1	L1		L1	65/65	AWARD BEST+++

Number ordered of tested malware sample

PRODUCT NAME	1	2	3	4	5	6	7	8	9	10	...	65	THREATS BLOCKED	CERTIFICATE GRANTED
F-SECURE Protection Service for Business	L1	L1	L1	L1	L1	L1	L1	L1	L1	L1		L3	65/65	AWARD BEST+++
G DATA Endpoint Protection Business	L1	L1	L1	L1	L1	L1	L1	L1	L1	L1		L1	65/65	AWARD BEST+++
KASPERSKY Endpoint Security Cloud	L1	L1	L1	L1	L1	L1	L1	L1	L1	L1		L3	65/65	AWARD BEST+++
MKS_VIR Internet Security	L1	L1	L1	L1	L1	L1	L1	L1	L1	L1		L3	65/65	AWARD BEST+++
SECUREAPLUS Pro	L3	L3	L3	L3	L3	L3	L3	L3	L3	L3		L3	65/65	AWARD BEST+++
SOPHOS Home Premium	L1	L1	L1	L1	L1	L1	L1	L1	L1	L1		L3	65/65	AWARD BEST+++
TREND MICRO Maximum Security	L2	L3	L1	L1	L1	L1	L1	L1	L1	L1		L3	62/65	ONLY TESTED
WEBROOT SecureAnywhere Antivirus	L3	L3	L3	L3	L3	L3	L3	L3	L3	L3		L3	65/65	AWARD BEST+++
WEBROOT Endpoint Protection	L3	L3	L3	L3	L3	L3	L3	L3	L3	L3		L3	65/65	AWARD BEST+++
WINDOWS Defender Antivirus	L3	L3	L3	L3	L3	L3	L3	L3	L3	L3		L3	60/65	ONLY TESTED
ZONEALARM Extreme Security	L1	L1	L1	L1	L1	L1	L1	L1	L1	L1		L1	65/65	AWARD BEST+++

Ransomware - technical details

NO	RANSOMWARE	FILE NAME
1	3320f11728458d01eef62e10e48897ec1c2277c1fe1aa2d471a16b4dccfc1207	1.exe
2	3299f07bc0711b3587fe8a1c6bf3ee6bcbc14cb775f64b28a61d72ebcb8968d3	2.exe
3	86456ebf6b807e8253faf1262e7a2b673131c80174f6133b253b2e5f0da442a9	3.exe
4	9a4e4211f7e690ee4a520c491ef7766dcf1cc9859afa991e15538e92b435f3a1	4.exe
5	4e6c191325b37da546e72f4a7334d820995d744bf7bb1a03605adb3ad30ce9ca	5.exe
6	b933cb32689517aac6e459d33e9d8c7c8f31f0710008bfa09d9e91c2526826ef	6.exe
7	d4492a9eb36f87a9b3156b59052ebaf10e264d5d1ce4c015a6b0d205614e58e3	7.exe
8	3759f8774aee2d6185b02489612382797b110ed7b5fc39edda9665c3152cbddc	8.exe
9	9ca0776e3c226e4ebb4c8c08ea750e6dbc22e447dea68e1e8795b5d5691472c0	9.exe
10	8639825230d5504fd8126ed55b2d7aeb72944ffe17e762801aab8d4f8f880160	10.exe
	...	
24	29e5da1f13de425e105f065be573793c41e5bf693cf874cdaac69bd85c499dfd	24.exe

L1

LEVEL 1

The browser level, i.e. a virus has been stopped before or after it has been downloaded onto a hard drive.

L2

LEVEL 2

The system level, i.e. a virus has been downloaded, but it has not been allowed to run.

L3

LEVEL 3

The analysis level, i.e. a virus has been run and blocked by a tested product.

F

FAIL

The failure, i.e. a virus has not been blocked and it has infected a system.

Ransomware

	Number ordered of tested malware sample													
PRODUCT NAME	1	2	3	4	5	6	7	8	9	10	...	24	THREATS BLOCKED	CERTIFICATE GRANTED
ARCABIT Internet Security	L1	L1	L1	L1	L1	L1	L1	L1	L1	L1		L1	24/24	AWARD BEST+++
AVIRA Antivirus Pro	L1	L1	L1	L1	L1	L1	L1	L1	L1	L1		L1	24/24	AWARD BEST+++
AVIRA Prime	L1	L1	L1	L1	L1	L1	L1	L1	L1	L1		L1	24/24	AWARD BEST+++
BITDEFENDER GravityZone Elite	L1	L1	L1	L1	L1	L1	L1	L1	L1	L1		L1	24/24	AWARD BEST+++
CHECK POINT Endpoint Security	L2	L1	L1	L1	L1	L1	L1	L1	L1	L1		L1	24/24	AWARD BEST+++
COMODO Advanced Endpoint Protection	L1	L1	L1	L1	L3	L1	L3	L1	L3	L3		L3	24/24	AWARD BEST+++
COMODO Internet Security	L1	L1	L1	L1	L3	L1	L3	L1	L3	L3		L3	24/24	AWARD BEST+++
EMSISOFT Anti-Malware	L3	L3	L3	L3	L3	L3	L3	L3	L3	L3		L3	24/24	AWARD BEST+++
EMSISOFT Business Security	L3	L3	L3	L3	L3	L3	L3	L3	L3	L3		L3	24/24	AWARD BEST+++
ESET Endpoint Protection Advanced Cloud	L1	L1	L1	L1	L1	L1	L1	L1	L1	L1		L1	24/24	AWARD BEST+++

Number ordered of tested malware sample

PRODUCT NAME	1	2	3	4	5	6	7	8	9	10	...	24	THREATS BLOCKED	CERTIFICATE GRANTED
F-SECURE Protection Service for Business	L1	L1	L1	L1	L1	L1	L1	L1	L1	L1		L1	24/24	AWARD BEST+++
G DATA Endpoint Protection Business	L1	L1	L1	L1	L1	L1	L1	L1	L1	L1		L1	24/24	AWARD BEST+++
KASPERSKY Endpoint Security Cloud	L1	L1	L1	L1	L1	L1	L1	L1	L1	L1		L1	24/24	AWARD BEST+++
MKS_VIR Internet Security	L1	L1	L1	L1	L1	L1	L1	L1	L1	L1		L1	24/24	AWARD BEST+++
SECUREAPLUS Pro	L3	L3	L3	L3	L3	L3	L3	L3	L3	L3		L3	24/24	AWARD BEST+++
SOPHOS Home Premium	L1	L1	L1	L1	L1	L1	L1	L1	L1	L1		L1	24/24	AWARD BEST+++
TREND MICRO Maximum Security	L1	L1	L1	L1	L1	L1	L1	L1	L1	L1		L1	24/24	AWARD BEST+++
WEBROOT SecureAnywhere Antivirus	L1	L1	L1	L1	L1	L1	F	L1	F	L3		L1	18/24	ONLY TESTED
WEBROOT Endpoint Protection	L1	L1	L1	L1	L1	L1	F	L1	F	L1		L1	18/24	ONLY TESTED
WINDOWS Defender Antivirus	L3	L2	F	F	L1	L1	F	L1	L3	L1		L3	20/24	ONLY TESTED
ZONEALARM Extreme Security	L1	L1	L1	L1	L1	L1	L1	L1	L1	L1		L1	24/24	AWARD BEST+++

Fileless attacks - technical details

NO	FILELESS ATTACKS	FILE NAME
1	c1525592fdf22f2ea068b5e2428d5e36fd9629ef8f5dd648ee792b4cb936fe53	1.bat
2	e43ac1a50122d5f8584d21d768ea171d1f5f78075bbb73ae178506b6f8d071cb	2.hta



LEVEL 1

The browser level, i.e. a virus has been stopped before or after it has been downloaded onto a hard drive.



LEVEL 2

The system level, i.e. a virus has been downloaded, but it has not been allowed to run.

LEVEL 3

The analysis level, i.e. a virus has been run and blocked by a tested product.



FAIL

The failure, i.e. a virus has not been blocked and it has infected a system.

Fileless attacks

PRODUCT NAME	POWERSHELL ATTACK	MSHTA ATTACK	ATTACKS BLOCKED	CERTIFICATE GRANTED
ARCABIT Internet Security	Malicious commandhas been executed, but the Arcabit firewall has blocked the attack	Attack has been blocked in a browser	2/2	AWARD BEST+++
AVIRA Antivirus Pro	Threat has been blocked when accessing file	Attack has not been blocked at any of the stages *	1/2	AWARD GOOD+
AVIRA Prime	Threat has been blocked when accessing file	Attack has not been blocked at any of the stages *	1/2	AWARD GOOD+
BITDEFENDER GravityZone Elite	Threat has been blocked when accessing file	Attack has been blocked in a browser	2/2	AWARD BEST+++
CHECK POINT Endpoint Security	Threat has been blocked when accessing file	Threat has been launched, but raised the alarmof Check Point	2/2	AWARD BEST+++
COMODO Advanced Endpoint Protection	Threat has been blocked when accessing file	Threat has been blocked when accessing file	2/2	AWARD BEST+++
COMODO Internet Security	Threat has been blocked when accessing file	Attack has not been blocked at any of the stages *	1/2	AWARD GOOD+
EMSISOFT Anti-Malware	Threat has been blocked when accessing file	Threat has been blocked when accessing file	2/2	AWARD BEST+++
EMSISOFT Business Security	Threat has been blocked when accessing file	Threat has been blocked when accessing file	2/2	AWARD BEST+++
ESET Endpoint Protection Advanced Cloud	Threat has been blocked when accessing file	Threat has been blocked when accessing file	2/2	AWARD BEST+++

PRODUCT NAME	POWERSHELL ATTACK	MSHTA ATTACK	ATTACKS BLOCKED	CERTIFICATE GRANTED
F-SECURE Protection Service for Business	Threat has been blocked when accessing file	Threat has been blocked by the DeepGuard module	2/2	
G DATA Endpoint Protection Business	Threat has been blocked when accessing file	Threat has been blocked when accessing file	2/2	
KASPERSKY Endpoint Security Cloud	Threat has been blocked when accessing file	Attack has been blocked in a browser	2/2	
MKS_VIR Internet Security	Threat has been run, but the mks_vir firewall has blocked a connection with hacker's server	Attack has been blocked in a browser	2/2	
SECUREAPLUS Pro	Threat has been launched, but raised the alarmof SecureAPlus	Threat has been launched, but raised the alarmof SecureAPlus	2/2	
SOPHOS Home Premium	Attack has not been blocked at any of the stages	Attack has been blocked in a browser	1/2	
TREND MICRO Maximum Security	Threat has been blocked when accessing file	Threat has been launched, but raised the alarmof Trend Micro	2/2	
WEBROOT SecureAnywhere Antivirus	Attack has not been blocked at any of the stages	Attack has not been blocked at any of the stages *	0/2	
WEBROOT Endpoint Protection	Attack has not been blocked at any of the stages	Attack has not been blocked at any of the stages *	0/2	
WINDOWS Defender Antivirus	Threat has been run, but the firewallhas blocked a connectionwith hacker's server	Threat has been launched, but raised the alarmof antivirus	2/2	
ZONEALARM Extreme Security	Threat has been blocked when accessing file	Threat has been launched, but raised the alarmof ZoneAlarm	2/2	

AVIRA Antivirus Pro	Developer has reacted quickly on our notification. On the date of publication of this report, software already protects against this kind of attacks.
AVIRA Prime	Developer has reacted quickly on our notification. On the date of publication of this report, software already protects against this kind of attacks.
COMODO Internet Security	Threat used in the attack was launched in an isolated area – the Comodo sandbox. The bad news is that it was possible to browse the content of victim's hard drive and steal files.
WEBROOT SecureAnywhere Antivirus	Developer has reacted quickly on our notification. On the date of publication of this report, software already protects against this kind of attacks.
WEBROOT Endpoint Protection	Developer has reacted quickly on our notification. On the date of publication of this report, software already protects against this kind of attacks.

To learn more about technical details,
please contact us: kontakt@avlab.pl



AVLab is an independent organization as guardian of Internet security that provides information from the industry through articles, reportage from training and conferences. Our distinctive feature are reviews and security tests. In our tests we use malicious software, tools, and techniques of bypassing security that are used in real attacks.

Developers may send their enquiries for more technical details at: kontakt@avlab.pl