April 2017

# Protection test against drive-by download attacks

THE INDEPENDENT ANTIVIRUS TESTS

# Contents

# Introduction to the test

It's difficult to detect attacks which exploit software vulnerabilities. This process is even more complicated if hackers are aiming to take control of a workstation through fully undetectable vulnerabilities known as FUD (Fully Undetectable) or 0-day vulnerabilities that are distributed among a small group of people, mostly cybercriminals, but also among hardware manufacturers or antivirus software developers. These types of situations are particularly dangerous when a victim has to deal with an ATP (Advanced Persistent Threat), an advanced, a long-lasting attack. Elements of a social engineering used almost always in conjunction with an effective watering hole tactics, put users in a losing position.

Traditional anti-exploit techniques are mainly focused on:

- developing patterns based on known threats,
- scanning newly opened websites,
- detecting API functions used by spyware or key loggers,
- a dynamic analysis of a website content, for example, to detect redirections, downloaded files, a JavaScript code,
- using traps which prevent the attacks based on software vulnerabilities, whether or not they are 0-day vulnerabilities,
- using a NIDS and HIPS systems which monitor events,
- updating applications and an operating system,
- hardening a system by installing updates,
- changing default settings and rules,
- educating users in a prevention, as well as threats and attacks identification.

The mentioned rules primarily refer to the attacks that uses commonly known vulnerabilities, and unfortunately these attacks aren't always detectable by an antivirus software. If we accept the principle that the exploit distributed as a plug-in for a web browser or office suite won't be detected by most security software, then probability of stopping a similar attack with 0-day exploit (before running  a dangerous payload) is even smaller.

Consequences of a successful security breach can last many months since the attack initiation. Specialized web portals wrote about this kind of incident when hackers attacked the Financial Supervision Commission's website which is a valuable source of information for many governmental and private institutions in Poland. As a result of using the watering hole tactics for infecting the most visited source by victims, cybercriminals managed to infiltrate systems of a thoroughly selected targets.

The document titled "Attack analysis on banks in Poland" which was prepared by engineers from Preventity company, describes each attack phase which took place at the turn of 2016/2017. According to the report, the event that initiated the attack was to use vulnerabilities in WWW server, modify one of the JavaScript files, and redirect visitors to another server – also a hacked one – where a victim recognition process was initiated:

- It was checked if IP addresses are within range defined by exploit authors.
- A operating system and its architecture have been verified.
- A browser version and type have been verified.
- A version of installed plug-ins: Flash, Java, SilverLight, Office, were verified.
- A presence of EMET software has been verified.

Based on the patterns above, the exploit was adjusted automatically.

The another report titled "Lazarus Under The Hood" developed by Kaspersky Lab suggests that the FSC attack was only part of a larger scale event. It's also confirmed by Symantec company which clearly states that the malicious software detected in "Downloader.Ratankba" nomenclature is closely related to Lazarus group which was involved in espionage military campaigns, and sabotage activities of financial institutions, media stations, and factories.

# Tested software

**Products for home users**

360 Total Security (9.0.0.11.46)
Arcabit Home Security (2017.04.07)
Avast Free Antivirus 2017 (17.03.2291)
Avast Premier 2017 (17.03.2291)
AVG Free Antivirus 2017 (17.03.3011)
AVG Internet Security 2017 (17.03.3011)
Avira Free Antivirus 2017 (15.025.172)
Avira Internet Security Suite 2017 (15.025.172)
Bitdefender Total Security 2017 (21.0.24.62)
Comodo Cloud Antivirus (1.10.413855.478)
Comodo Internet Security Pro 10 (10.0.1.6209)
Dr. Web Space Security 11 (11.0.5.04031)
ESET Smart Security 10 (10.0.390.0)
F-Secure SAFE (2.76.212.0)
FortiClient Free 5 (5.4.3.0870)
G DATA Total Protection (25.03.03)
Kaspersky Total Security 2017 (17.0.0.611)
Malwarebytes Anti-Malware Prem. (3.0.6.1469)
McAfee LiveSafe (8.0.1210.13)
Norton Security (22..9.1.12)
Panda Free Antivirus 2017 (18.01.00.0000)
Panda Internet Security 2017 (17.00.01.0000)
Quick Heal Total Security (17.00)
SecureAPlus (4.5.2)
Sophos HOME (1.1.1.3)
Trend Micro Internet Security 2017 (11.00)
Webroot SecureAnywh. Complete (9.0.15.50)
Windows Defender (4.10.14393.953)
Zemana Antimalware Premium (2.72.2.388)
ZoneAlarm Internet Sec. 2017 (15.1.501.17249)

**Products for small and medium business**

Arcabit Endpoint Security (2017.04.07)
Bitdefender GravityZone (6.2.19.894)
Comodo ONE (8.3.0.5263)
ESET Endpoint Security (6.5.2094.1)
F-Secure Protection Service for Bus. (12. 0.1)
G DATA Client Security Business (14.01.122)
Kaspersky Endpoint Security 10 (10.2.5.3201)
Kaspersky Small Office Security (17.0.0.611)
Panda Endpoint Protection (7.65.00.0000)
Seqrite Endpoint Security (7.2)
Trend Micro Worry-Free Business (19.0.3144)
Webroot SecureAnywhere Endpoint (9.0.15.50)

# Automatic drive-by download attacks

In recent months, viruses that were infecting personal computers and employee workstations through drive-by download attacks have been playing a major role in global threats. These techniques are commonly used in exploit kits, tools that make it easy to automatically search for vulnerabilities (mostly installed in browsers and plug-ins). They optimize and adapt exploits to an operating system version and an architecture, and an installed browser.

The exploit sets (also known as exploit kits or exploit packs) have become one of the most popular attack methods for cybercriminals. Their price may vary from several dozen dollars  to several thousand dollars for monthly subscription. The goals for which they were programmed focus on:

- Maximizing a risk of infection,
- Installing executable files,
- Automatically running viruses that break into a system with a minimum amount of failures.

In the following attack scheme, it's important that a victim isn't in any way encouraged to run a downloaded file – as it usually happens with harmful attachments in email messages. When a website containing an exploit kit is opened, a virus carrying a payload is downloaded and run.

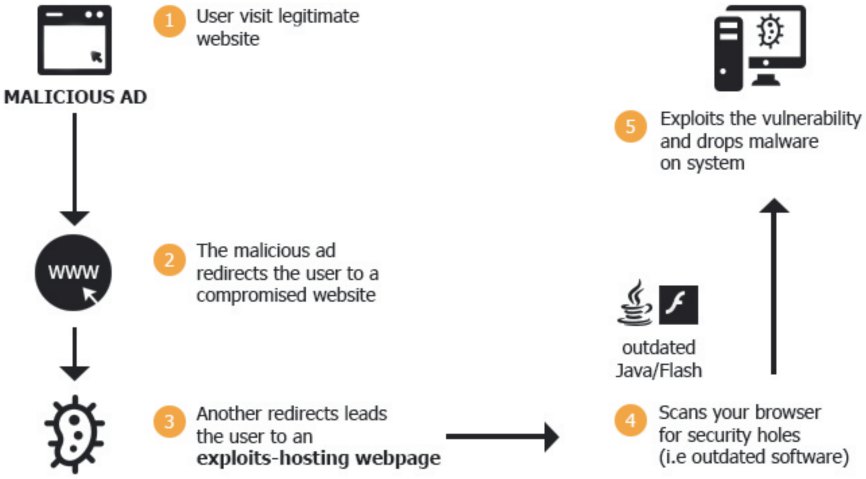

MALICIOUS AD
1 User visit legitimate website
WWW
2 The malicious ad redirects the user to a compromised website
3 Another redirects leads the user to an exploits-hosting webpage
outdated Java/Flash
4 Scans your browser for security holes (i.e outdated software)
5 Exploits the vulnerability and drops malware on system

Figure: The drive-by download attack scheme: a victim visits a website with a malicious advertisement which redirects him to an infected web page where a system infection occurs through an automatic exploit adjustment to a system and an installed browser.

Exploit kit tool is usually Internet application which has graphical user interface. This makes easier for people who don't have advanced programming and network skills, to use it. Its task is to compile several scripts so that cybercriminal can quickly and easily place a payload on a victim's device. There are several ways to achieve this operation:

- Through a scam,
- Through a phishing,
- Through hacking a friend social networking account,
- Through malvertising,
- Through a watering hole attack.

There is no need for an additional interaction to infect a victim's device (e.g., downloading and running a virus). A single visit to a malicious website automatically initiates an infection. Workstations which don't have a comprehensive protection, and an installed software isn't updated regularly, are very easy targets for these attacks which give hackers an opportunity to remote access and escalate effects of a security breach.

# Exploits

One of the key techniques, used in exploit kit tools to avoid a detection by antivirus scanning, is called obfuscation. Developers of these exploit kit tools use different code protection techniques: compressing a binary file, adding useless characters, or encrypting a virus code. In addition, almost every exploit pack contains embedded code hiding features and "Command and Control" server addresses and landing pages masking capabilities that domains can be generated with DGA (Domain Generation Algorithm). All this makes a detection of website from which an attack is carried out – as well as an infection process itself – a very difficult task, even for security teams working in antivirus companies.

The best known Exploit Kit tools include*:

**Rig Exploit Kit**

- It's still used by cybercriminals.
- It has at least two variants: RIG-E, RIG-V.
- After the fall of Angler Exploit Kit in last year, it became number "1".

**Beps, znany jako Sundown Exploit Kit**

- It reached the greatest popularity among cybercriminals in 2016.
- It used identical techniques known from other exploit packs (probably stolen and copied "1:1").
- It was temporarily disabled due to a recent code leak.

**Terror EK / Blaze EK / Nebula EK / Neptune EK / Eris EK**

- This exploit kit appeared under different names at the beginning of this year.
- At the beginning, it reaped full benefits of stolen Sundown Exploit Kit code.
- Although, it doesn't exist a long time, quickly achieved a favor of many cybercriminals.

### Neutrino Exploit Kit

- It has been around for several years now on cybercriminal forums.
- It's used very rarely in smaller scale attacks.
- It includes vulnerability sets for Adobe software.

### Magnitude Exploit Kit

- It's significant exploit pack in the cybercriminal world.
- Security teams know it from attacks that use malicious advertisements (ad networks often aren't able to verify every single ad which they place on large portals, such as java.com, youtube.com).
- Attacks involving Magnitude EK are concentrated in Asian countries.

### Kaixin Exploit Kit

- Chinese exploit kit, active since 2012.
- Primarily used for attacks on users from that part of the world.
- Its attacks are concentrated mainly on vulnerabilities of Java and Adobe Flash Player applications.

### Astrum Exploit Kit

- Highly advanced exploit pack which uses steganography.
- Its attacks are carried out by using a malicious advertising.
- It contains a very sophisticated chain of infection, it has many implemented techniques which hinder its analysis.

* Information about the exploit kit tools is provided by Check Point.

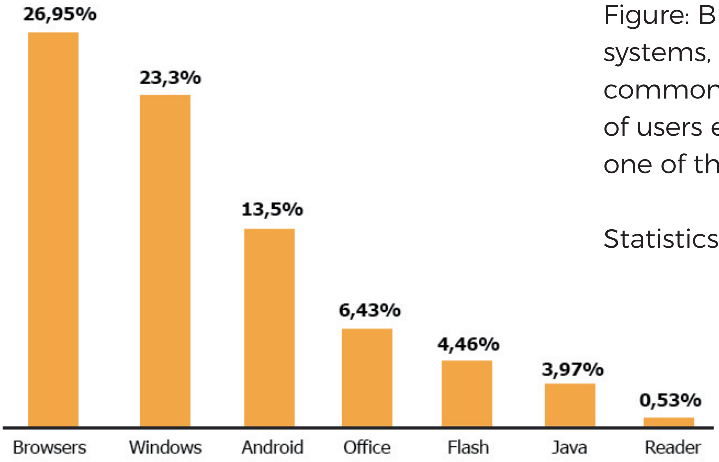


Figure: Browsers, Windows and Android systems, and Microsoft Office suite were most commonly used by exploits - in 2016, 69,8% of users encountered at least one exploit in one of the software.

Statistics are provided by Kaspersky Lab.

# Test assumptions

In this unique test, we wanted to check if comprehensive security applications protect against attacks which use software vulnerabilities. If it was necessary, we enabled protection against exploits, as well as website scanners. All other options were set to default.

One way to execute malicious code on a victim's device is to send a malware file, for example, via email. This isn't a sophisticated method, but sooner or later a well-prepared social engineering attack will convince a user to open an attachment. This operation must be preceded by a recognition of the software used by a victim or utilization of the application vulnerability used by many people in the targeted geographical region.

However, we have focused on another scenario which is more difficult to accomplish, but very effective at the same time. We have checked if as a result of exploiting a vulnerability in the Firefox browser, a hacker is able to remotely access an infected workstation and browse disks and folder contents, steal files, take screenshots, download malicious files using a PowerShell interpreter, and change, for example, the Microsoft Office security settings by modifying values of the system registry keys.

We are aware that security software which have a firewall module and IPS (Intrusive Prevention System), can scan incoming and outgoing traffic and thus find themselves in privileged position unlike products which provide only a basic antivirus protection. For this reason, we have decided to grant separate recommendations for solutions with a firewall and without this feature.

# Attack scenario

In the test carried out in middle April 2017, we used a virtual Windows 10 x64 system located in Poland. Computer which performed controlled attacks was located in France.

The essential tools needed to get remote access victim computer are as follows:

- Malicious software, undetectable for most antivirus application.
- Exploit for Firefox browser (CVE 2016-9079).
- Metasploit which was an instrument of consolidating the whole attack procedure (a system penetration, file theft, additional malicious files download, a system registry modification using a PowerShell interpreter).

*The URL address which contained an exploit, may be placed on a victim's workstation through various social engineering methods. For the test purposes, a link to malicious website was simply run by a tester in a browser*

The attack procedure has been divided into two categories:

**[F] First Attack**

Automatic placement of a payload and remote connection establishment: if the attack was stopped by a protection module against exploits, we applied the second social engineering attack (see [S] Second Attack).

However, if the attack wasn't stopped in a browser, a tester was getting a remote access to a victim's workstation. Then using a PowerShell interpreter, we checked if the software downloaded by the trusted system process powershell.exe was detected through signature scanning, heuristic techniques – or at very least, if a connection with a hacker's server was interrupted by a firewall or IDS/IPS module on default settings.

### [S] Second Attack

Opening website by a user: in this scenario, a website contains obfuscated JavaScript code that was redirecting a victim to another page where a tester downloaded a file and run a virus.

At first glance, the difference between the first [F] and the second [S] attack isn't clear. We wanted to check if antivirus applications have rules for detecting downloaded and run malicious files by a system process, such as a PowerShell interpreter which is very often used to run malicious scripts.

> *As our test showed, protection results for particular file, but coming from another source (PowerShell, browser) often give completely different outcomes.*

**Explanation of the test results on the example of Qihoo 360 Total Security:**

| | .EXE (1) | | .BAT (2) | | .EXE (3) | | .DOCX (4) | | .ODT (5) | |
|---|---|---|---|---|---|---|---|---|---|---|
| Qihoo 360 | F: 0/1/-/- | 🟠 | F: 0/0/0/0 | 🔴 | F: 0/1/-/- | 🟠 | F: 0/1/-/- | 🟠 | F: 0/0/0/0 | 🔴 |
| | S: 0/1/-/- | 🟢 | S: 0/0/0/0 | 🔴 | S: 0/1/-/- | 🟢 | S: 0/1/-/- | 🟢 | F: 0/0/0/0 | 🔴 |

(1) Protection results for the first EXE file
(2) Protection results for a BAT file
(3) Protection results for the second EXE file
(4) Protection results for the first macro virus for MS Office 2016
(5) The result of protection for the second macro virus for LO / Open Office

For [F] and [S] where n/n/n/n refer respectively:

- (e.g., F: 1/-/-/-) detection by a WWW scanning or a dedicated protection against exploits
- (e.g., F: 0/1/0/0) threat detection by signatures
- (e.g., F: 0/0/1/-) threat detection by a heuristic or proactive protection after remotely file run
- (e.g., F: 0/0/0/1) detection of a harmful connection by firewall, IPS or IDS module and stopping the attack
- (e.g., F: 0/1/-/-) the pause means that the next stage wasn't checked if a threat was detected in the previous one

🟢 The green color in the first attack [F] indicates a blocked drive-by download attempt by a protection module against exploits. In the second attack [S], it indicates a successfully blocked malicious software which as a result of getting access to a PowerShell interpreter, was downloaded from a server controlled by a hacker and run on victim's workstation.

🟠 The yellow color appears only in the first attack [F]. It indicates a blocked malicious software placed on a victim's workstation as a result of applying  an exploit in a drive-by download attack. The color also symbolizes an unblocked hacker connection with an infected workstation by a firewall module. In this case, a cybercriminal may still try other security bypass techniques.

🔴 In this case, both the attack on a browser and a download and run of malicious software by a PowerShell interpreter wasn't blocked by an antivirus application. Regardless of the [F] and the [S] attack, red color indicates an effective security breach of antivirus protection and a successful operating system infection.

# Step by step procedure

0. Antivirus software update and system restart.

1. **[F] First attack:**

Opening a URL address in Firefox browser containing an exploit for CVE 2016-9079 vulnerability: automatic use of an exploit and a payload run.

1.1. If an antivirus application managed to stop the attack (prevented a payload run and interrupted a connection with a hacker's server), we went to step 2. Otherwise:

1.2. Getting access to a PowerShell interpreter and downloading 5 malicious files from a remote server (EXE, BAT, EXE, DOCX, ODT).

1.3. A sequential run of each file and examining a reaction of antivirus software.

*As a result of malicious file run, we were establishing a second remote connection in case of interrupting a previous session. In this step, a hacker could use a downloaded file for completely different, more malicious purposes, e.g., like remotely running a ransomware or installing a banking Trojan.*

2. **[Second] Second Attack:**

Opening URL address, redirecting to a target website with a virus and downloading the same malicious files.

2.1. A sequential file run and verification of protection effectiveness for tested security software.

*For documents with macro viruses, warnings were ignored by a tester. There is an option to remotely change security settings for macros in Microsoft Office 2016 (read "Results interpretation").*

3. Saving the results and back to the beginning.

# Protection results for business solutions

| | .EXE (1) | | .BAT (2) | | .EXE (3) | | .DOCX (4) | | .ODT (5) | |
|---|---|---|---|---|---|---|---|---|---|---|
| Arcabit Endp. | F: 1/-/-/- | 🟢 | F: 1/-/-/- | 🟢 | F: 1/-/-/- | 🟢 | F: 1/-/-/- | 🟢 | F: 1/-/-/- | 🟢 |
| | S: 1/-/-/- | 🟢 | S: 0/0/0/1 | 🟢 | S: 1/-/-/- | 🟢 | S: 0/0/1/- | 🟢 | S: 0/0/0/1 | 🟢 |

| | .EXE (1) | | .BAT (2) | | .EXE (3) | | .DOCX (4) | | .ODT (5) | |
|---|---|---|---|---|---|---|---|---|---|---|
| Bitdefender GZ | F: 1/-/-/- | 🟢 | F: 1/-/-/- | 🟢 | F: 1/-/-/- | 🟢 | F: 1/-/-/- | 🟢 | F: 1/-/-/- | 🟢 |
| | S: 1/-/-/- | 🟢 | S: 1/-/-/- | 🟢 | S: 1/-/-/- | 🟢 | S: 1/-/-/- | 🟢 | S: 1/-/-/- | 🟢 |

| | .EXE (1) | | .BAT (2) | | .EXE (3) | | .DOCX (4) | | .ODT (5) | |
|---|---|---|---|---|---|---|---|---|---|---|
| Comodo ONE | F: 0/1/-/- | 🟠 | F: 0/0/0/1 | 🟠 | F: 0/0/1/- | 🟠 | F: 0/0/1/- | 🟠 | F: 0/0/1/- | 🟠 |
| | S: 0/1/-/- | 🟢 | S: 0/0/1/- | 🟢 | S: 0/0/1/- | 🟢 | S: 0/0/1/- | 🟢 | S: 0/0/1/- | 🟢 |

| | .EXE (1) | | .BAT (2) | | .EXE (3) | | .DOCX (4) | | .ODT (5) | |
|---|---|---|---|---|---|---|---|---|---|---|
| ESET Endp. | F: 1/-/-/- | 🟢 | F: 1/-/-/- | 🟢 | F: 1/-/-/- | 🟢 | F: 1/-/-/- | 🟢 | F: 1/-/-/- | 🟢 |
| | S: 1/-/-/- | 🟢 | S: 1/-/-/- | 🟢 | S: 1/-/-/- | 🟢 | S: 1/-/-/- | 🟢 | S: 0/0/0/1 | 🟢 |

| | .EXE (1) | | .BAT (2) | | .EXE (3) | | .DOCX (4) | | .ODT (5) | |
|---|---|---|---|---|---|---|---|---|---|---|
| F-Secure PSB | F: 0/0/1/- | 🟠 | F: 0/0/1/- | 🟠 | F: 0/0/1/- | 🟠 | F: 0/0/1/- | 🟠 | F: 0/0/1/- | 🟠 |
| | S: 1/-/-/- | 🟢 | S: 1/-/-/- | 🟢 | S: 1/-/-/- | 🟢 | S: 1/-/-/- | 🟢 | S: 0/0/0/1 | 🟢 |

| | .EXE (1) | | .BAT (2) | | .EXE (3) | | .DOCX (4) | | .ODT (5) | |
|---|---|---|---|---|---|---|---|---|---|---|
| G DATA Client S. | F: 1/-/-/- | 🟢 | F: 1/-/-/- | 🟢 | F: 1/-/-/- | 🟢 | F: 1/-/-/- | 🟢 | F: 1/-/-/- | 🟢 |
| | S: 1/-/-/- | 🟢 | S: 0/0/0/0 | 🔴 | S: 0/0/1/- | 🟢 | S: 0/0/0/0 | 🔴 | S: 0/0/0/0 | 🔴 |

| | .EXE (1) | | .BAT (2) | | .EXE (3) | | .DOCX (4) | | .ODT (5) | |
|---|---|---|---|---|---|---|---|---|---|---|
| Kaspersky End. | F: 1/-/-/- | 🟢 | F: 1/-/-/- | 🟢 | F: 1/-/-/- | 🟢 | F: 1/-/-/- | 🟢 | F: 1/-/-/- | 🟢 |
| | S: 1/-/-/- | 🟢 | S: 0/0/1/- | 🟢 | S: 1/-/-/- | 🟢 | S: 1/-/-/- | 🟢 | S: 0/0/0/1 | 🟢 |

| | .EXE (1) | | .BAT (2) | | .EXE (3) | | .DOCX (4) | | .ODT (5) | |
|---|---|---|---|---|---|---|---|---|---|---|
| Kaspersky SO | F: 1/-/-/- | 🟢 | F: 1/-/-/- | 🟢 | F: 1/-/-/- | 🟢 | F: 1/-/-/- | 🟢 | F: 1/-/-/- | 🟢 |
| | S: 1/-/-/- | 🟢 | S: 0/0/1/- | 🟢 | S: 1/-/-/- | 🟢 | S: 1/-/-/- | 🟢 | S: 0/0/0/1 | 🟢 |

| | .EXE (1) | | .BAT (2) | | .EXE (3) | | .DOCX (4) | | .ODT (5) | |
|---|---|---|---|---|---|---|---|---|---|---|
| Panda Endp. | F: 0/1/-/- | 🟠 | F: 0/0/0/0 | 🔴 | F: 0/0/1/- | 🟠 | F: 0/0/1/- | 🟠 | F: 0/0/0/0 | 🔴 |
| | S: 0/1/-/- | 🟢 | S: 0/0/0/0 | 🔴 | S: 0/1/-/- | 🟢 | S: 0/0/1/- | 🟢 | S: 0/0/0/0 | 🔴 |

| | .EXE (1) | | .BAT (2) | | .EXE (3) | | .DOCX (4) | | .ODT (5) | |
|---|---|---|---|---|---|---|---|---|---|---|
| SEQRITE Endp. | F: 1/-/-/- | 🟢 | F: 1/-/-/- | 🟢 | F: 1/-/-/- | 🟢 | F: 1/-/-/- | 🟢 | F: 1/-/-/- | 🟢 |
| | S: 0/1/-/- | 🟢 | S: 0/0/0/1 | 🟢 | S: 0/1/-/- | 🟢 | S: 0/0/1/- | 🟢 | S: 0/0/0/1 | 🟢 |

| | .EXE (1) | | .BAT (2) | | .EXE (3) | | .DOCX (4) | | .ODT (5) | |
|---|---|---|---|---|---|---|---|---|---|---|
| TrendMic Worry-F. | F: 0/1/-/- | 🟠 | F: 0/0/0/0 | 🔴 | F: 0/1/-/- | 🟠 | F: 0/0/1/- | 🟠 | F: 0/0/0/0 | 🔴 |
| | S: 1/-/-/- | 🟢 | S: 0/0/0/0 | 🔴 | S: 1/-/-/- | 🟢 | S: 1/-/-/- | 🟢 | S: 1/-/-/- | 🟢 |

| | .EXE (1) | | .BAT (2) | | .EXE (3) | | .DOCX (4) | | .ODT (5) | |
|---|---|---|---|---|---|---|---|---|---|---|
| Webroot Endp. | F: 0/1/-/- | 🟠 | F: 0/0/0/0 | 🔴 | F: 0/1/-/- | 🟠 | F: 0/0/1/- | 🟠 | F: 0/0/0/0 | 🔴 |
| | S: 0/1/-/- | 🟢 | S: 0/0/0/0 | 🔴 | S: 0/1/-/- | 🟢 | S: 0/0/1/- | 🟢 | S: 0/0/0/0 | 🟢 |

# Protection results for individual user solutions

| | .EXE (1) | | .BAT (2) | | .EXE (3) | | .DOCX (4) | | .ODT (5) | |
|---|---|---|---|---|---|---|---|---|---|---|
| Qihoo 360 | F: 0/1/-/- | 🟠 | F: 0/0/0/0 | 🔴 | F: 0/1/-/- | 🟠 | F: 0/1/-/- | 🟠 | F: 0/0/0/0 | 🔴 |
| | S: 0/1/-/- | 🟢 | S: 0/0/0/0 | 🔴 | S: 0/1/-/- | 🟢 | S: 0/1/-/- | 🟢 | S: 0/0/0/0 | 🔴 |

| | .EXE (1) | | .BAT (2) | | .EXE (3) | | .DOCX (4) | | .ODT (5) | |
|---|---|---|---|---|---|---|---|---|---|---|
| Arcabit Int. Sec. | F: 1/-/-/- | 🟢 | F: 1/-/-/- | 🟢 | F: 1/-/-/- | 🟢 | F: 1/-/-/- | 🟢 | F: 1/-/-/- | 🟢 |
| | S: 1/-/-/- | 🟢 | S: 0/0/0/1 | 🟢 | S: 1/-/-/- | 🟢 | S: 0/0/1/- | 🟢 | S: 0/0/0/1 | 🟢 |

| | .EXE (1) | | .BAT (2) | | .EXE (3) | | .DOCX (4) | | .ODT (5) | |
|---|---|---|---|---|---|---|---|---|---|---|
| Avast Free | F: 0/1/-/- | 🟠 | F: 0/0/0/0 | 🔴 | F: 0/1/-/- | 🟠 | F: 0/1/-/- | 🟠 | F: 0/0/0/0 | 🔴 |
| | S: 0/1/-/- | 🟢 | S: 0/0/0/0 | 🔴 | S: 0/1/-/- | 🟢 | S: 0/1/-/- | 🟢 | S: 0/0/0/0 | 🔴 |

| | .EXE (1) | | .BAT (2) | | .EXE (3) | | .DOCX (4) | | .ODT (5) | |
|---|---|---|---|---|---|---|---|---|---|---|
| Avast Premier | F: 0/1/-/- | 🟠 | F: 0/0/0/0 | 🔴 | F: 0/1/-/- | 🟠 | F: 0/1/-/- | 🟠 | F: 0/0/0/0 | 🔴 |
| | S: 0/1/-/- | 🟢 | S: 0/0/0/0 | 🔴 | S: 0/1/-/- | 🟢 | S: 0/1/-/- | 🟢 | S: 0/0/0/0 | 🔴 |

| | .EXE (1) | | .BAT (2) | | .EXE (3) | | .DOCX (4) | | .ODT (5) | |
|---|---|---|---|---|---|---|---|---|---|---|
| AVG Free | F: 0/1/-/- | 🟠 | F: 0/0/0/0 | 🔴 | F: 0/1/-/- | 🟠 | F: 0/1/-/- | 🟠 | F: 0/0/0/0 | 🔴 |
| | S: 0/1/-/- | 🟢 | S: 0/0/0/0 | 🔴 | S: 0/1/-/- | 🟢 | S: 0/1/-/- | 🟢 | S: 0/0/0/0 | 🔴 |

| | .EXE (1) | | .BAT (2) | | .EXE (3) | | .DOCX (4) | | .ODT (5) | |
|---|---|---|---|---|---|---|---|---|---|---|
| AVG Int. Sec. | F: 0/1/-/- | 🟠 | F: 0/0/0/0 | 🔴 | F: 0/1/-/- | 🟠 | F: 0/1/-/- | 🟠 | F: 0/0/0/0 | 🔴 |
| | S: 0/1/-/- | 🟢 | S: 0/0/0/0 | 🔴 | S: 1/-/-/- | 🟢 | S: 0/1/-/- | 🟢 | S: 0/0/0/0 | 🔴 |

| | .EXE (1) | | .BAT (2) | | .EXE (3) | | .DOCX (4) | | .ODT (5) | |
|---|---|---|---|---|---|---|---|---|---|---|
| Avira Free | F: 0/1/-/- | 🟠 | F: 0/0/0/0 | 🔴 | F: 0/0/1/- | 🟠 | F: 0/0/1/- | 🟠 | F: 0/0/0/0 | 🔴 |
| | S: 0/1/-/- | 🟢 | S: 0/0/0/0 | 🔴 | S: 0/0/1/- | 🟢 | S: 0/0/1/- | 🟢 | S: 0/0/0/0 | 🔴 |

| | .EXE (1) | | .BAT (2) | | .EXE (3) | | .DOCX (4) | | .ODT (5) | |
|---|---|---|---|---|---|---|---|---|---|---|
| Avira Int. Sec | F: 0/1/-/- | 🟠 | F: 0/0/0/0 | 🔴 | F: 0/0/1/- | 🟠 | F: 0/0/1/- | 🟠 | F: 0/0/0/0 | 🔴 |
| | S: 1/-/-/- | 🟢 | S: 0/0/0/0 | 🔴 | S: 0/0/1/- | 🟢 | S: 0/0/1/- | 🟢 | S: 0/0/0/0 | 🔴 |

| | .EXE (1) | | .BAT (2) | | .EXE (3) | | .DOCX (4) | | .ODT (5) | |
|---|---|---|---|---|---|---|---|---|---|---|
| Bitdefender TS. | F: 1/-/-/- | 🟢 | F: 1/-/-/- | 🟢 | F: 1/-/-/- | 🟢 | F: 1/-/-/- | 🟢 | F: 1/-/-/- | 🟢 |
| | S: 1/-/-/- | 🟢 | S: 0/0/0/1 | 🟢 | S: 1/-/-/- | 🟢 | S: 1/-/-/- | 🟢 | S: 1/-/-/- | 🟢 |

| | .EXE (1) | | .BAT (2) | | .EXE (3) | | .DOCX (4) | | .ODT (5) | |
|---|---|---|---|---|---|---|---|---|---|---|
| Comodo CAV | F: 0/0/1/- | 🟠 | F: 0/0/0/0 | 🔴 | F: 0/0/1/- | 🟠 | F: 0/0/1/- | 🟠 | F: 0/0/1/- | 🟠 |
| | S: 0/0/1/- | 🟢 | S: 0/0/1/- | 🟢 | S: 0/0/1/- | 🟢 | S: 0/0/1/- | 🟢 | S: 0/0/1/- | 🟢 |

| | .EXE (1) | | .BAT (2) | | .EXE (3) | | .DOCX (4) | | .ODT (5) | |
|---|---|---|---|---|---|---|---|---|---|---|
| Comodo Int. Sec. | F: 0/0/1/- | 🟠 | F: 0/0/0/1 | 🟠 | F: 0/1/-/- | 🟠 | F: 0/0/1/- | 🟠 | F: 0/0/1/- | 🟠 |
| | S: 0/0/1/- | 🟢 | S: 0/0/1/- | 🟢 | S: 0/1/-/- | 🟢 | S: 0/0/1/- | 🟢 | S: 0/0/1/- | 🟢 |

| | .EXE (1) | | .BAT (2) | | .EXE (3) | | .DOCX (4) | | .ODT (5) | |
|---|---|---|---|---|---|---|---|---|---|---|
| Dr. Web Sp. Sec. | F: 1/-/-/- | 🟢 | F: 1/-/-/- | 🟢 | F: 1/-/-/- | 🟢 | F: 1/-/-/- | 🟢 | F: 1/-/-/- | 🟢 |
| | S: 1/-/-/- | 🟢 | S: 0/0/0/0 | 🔴 | S: 0/0/0/1 | 🟢 | S: 0/0/1/- | 🟢 | S: 0/0/0/1 | 🟢 |

| | .EXE (1) | | .BAT (2) | | .EXE (3) | | .DOCX (4) | | .ODT (5) | |
|---|---|---|---|---|---|---|---|---|---|---|
| ESET Sm. Sec. | F: 1/-/-/- | 🟢 | F: 1/-/-/- | 🟢 | F: 1/-/-/- | 🟢 | F: 1/-/-/- | 🟢 | F: 1/-/-/- | 🟢 |
| | S: 1/-/-/- | 🟢 | S: 1/-/-/- | 🟢 | S: 1/-/-/- | 🟢 | S: 1/-/-/- | 🟢 | S: 0/0/0/1 | 🟢 |

| | .EXE (1) | | .BAT (2) | | .EXE (3) | | .DOCX (4) | | .ODT (5) | |
|---|---|---|---|---|---|---|---|---|---|---|
| F-Secure SAFE | F: 0/0/1/- | 🟠 | F: 0/0/1/- | 🟢 | F: 0/0/1/- | 🟠 | F: 0/0/1/- | 🟠 | F: 0/0/1/- | 🟠 |
| | S: 1/-/-/- | 🟢 | S: 1/-/-/- | 🟢 | S: 1/-/-/- | 🟢 | S: 1/-/-/- | 🟢 | S: 0/0/0/1 | 🟢 |

| | .EXE (1) | | .BAT (2) | | .EXE (3) | | .DOCX (4) | | .ODT (5) | |
|---|---|---|---|---|---|---|---|---|---|---|
| Fortinet Free | F: 0/1/-/- | 🟠 | F: 0/0/0/0 | 🔴 | F: 0/1/-/- | 🟠 | F: 0/1/-/- | 🟠 | F: 0/0/0/0 | 🔴 |
| | S: 1/-/-/- | 🟢 | S: 0/0/0/0 | 🔴 | S: 1/-/-/- | 🟢 | S: 0/1/-/- | 🟢 | S: 0/0/0/0 | 🔴 |

| | .EXE (1) | | .BAT (2) | | .EXE (3) | | .DOCX (4) | | .ODT (5) | |
|---|---|---|---|---|---|---|---|---|---|---|
| G DATA Total P. | F: 1/-/-/- | 🟢 | F: 1/-/-/- | 🟢 | F: 1/-/-/- | 🟢 | F: 1/-/-/- | 🟢 | F: 1/-/-/- | 🟢 |
| | S: 1/-/-/- | 🟢 | S: 0/0/0/0 | 🔴 | S: 0/0/1/- | 🟢 | S: 0/0/0/0 | 🔴 | S: 0/0/0/0 | 🔴 |

| | .EXE (1) | | .BAT (2) | | .EXE (3) | | .DOCX (4) | | .ODT (5) | |
|---|---|---|---|---|---|---|---|---|---|---|
| Kaspersky Total | F: 1/-/-/- | 🟢 | F: 1/-/-/- | 🟢 | F: 1/-/-/- | 🟢 | F: 1/-/-/- | 🟢 | F: 1/-/-/- | 🟢 |
| | S: 1/-/-/- | 🟢 | S: 0/0/1/- | 🟢 | S: 1/-/-/- | 🟢 | S: 1/-/-/- | 🟢 | S: 1/-/-/- | 🟢 |

| | .EXE (1) | | .BAT (2) | | .EXE (3) | | .DOCX (4) | | .ODT (5) | |
|---|---|---|---|---|---|---|---|---|---|---|
| MBAM Prem. | F: 1/-/-/- | 🟢 | F: 1/-/-/- | 🟢 | F: 1/-/-/- | 🟢 | F: 1/-/-/- | 🟢 | F: 1/-/-/- | 🟢 |
| | S: 0/0/1/- | 🟢 | S: 0/0/1/- | 🟢 | S: 0/0/0/0 | 🔴 | S: 0/0/1/- | 🟢 | S: 0/0/1/- | 🟢 |

| | .EXE (1) | | .BAT (2) | | .EXE (3) | | .DOCX (4) | | .ODT (5) | |
|---|---|---|---|---|---|---|---|---|---|---|
| McAfee LiveSafe | F: 0/1/-/- | 🟠 | F: 0/0/0/0 | 🔴 | F: 0/0/0/0 | 🔴 | F: 0/0/1/- | 🟠 | F: 0/0/0/0 | 🔴 |
| | S: 0/1/-/- | 🟢 | S: 0/0/0/0 | 🔴 | S: 1/-/-/- | 🟢 | S: 1/-/-/- | 🟢 | S: 1/-/-/- | 🟢 |

| | .EXE (1) | | .BAT (2) | | .EXE (3) | | .DOCX (4) | | .ODT (5) | |
|---|---|---|---|---|---|---|---|---|---|---|
| Norton Security | F: 1/-/-/- | 🟢 | F: 1/-/-/- | 🟢 | F: 1/-/-/- | 🟢 | F: 1/-/-/- | 🟢 | F: 1/-/-/- | 🟢 |
| | S: 1/-/-/- | 🟢 | S: 1/-/-/- | 🟢 | S: 0/0/1/- | 🟢 | S: 0/0/1/- | 🟢 | S: 0/0/0/1 | 🟢 |

| | .EXE (1) | | .BAT (2) | | .EXE (3) | | .DOCX (4) | | .ODT (5) | |
|---|---|---|---|---|---|---|---|---|---|---|
| Panda Free | F: 0/0/1/- | 🟠 | F: 0/0/0/0 | 🔴 | F: 0/0/1/- | 🟠 | F: 0/1/-/- | 🟠 | F: 0/0/0/0 | 🔴 |
| | S: 1/-/-/- | 🟢 | S: 0/0/0/0 | 🔴 | S: 0/0/1/- | 🟢 | S: 0/0/1/- | 🟢 | S: 0/0/0/0 | 🔴 |

| | .EXE (1) | | .BAT (2) | | .EXE (3) | | .DOCX (4) | | .ODT (5) | |
|---|---|---|---|---|---|---|---|---|---|---|
| Panda Int. Sec. | F: 0/0/1/- | 🟠 | F: 0/0/0/0 | 🔴 | F: 0/0/1/- | 🟠 | F: 0/0/1/- | 🟠 | F: 0/0/0/0 | 🔴 |
| | S: 0/1/-/- | 🟢 | S: 0/0/0/0 | 🔴 | S: 0/0/1/- | 🟢 | S: 0/0/1/- | 🟢 | S: 0/0/0/0 | 🔴 |

| | .EXE (1) | | .BAT (2) | | .EXE (3) | | .DOCX (4) | | .ODT (5) | |
|---|---|---|---|---|---|---|---|---|---|---|
| Quick Heal | F: 1/-/-/- | 🟢 | F: 1/-/-/- | 🟢 | F: 1/-/-/- | 🟢 | F: 1/-/-/- | 🟢 | F: 1/-/-/- | 🟢 |
| | S: 0/1/-/- | 🟢 | S: 0/0/0/1 | 🟢 | S: 0/1/-/- | 🟢 | S: 0/0/1/- | 🟢 | S: 0/0/0/1 | 🟢 |

| | .EXE (1) | | .BAT (2) | | .EXE (3) | | .DOCX (4) | | .ODT (5) | |
|---|---|---|---|---|---|---|---|---|---|---|
| SecureA Plus | F: 0/1/-/- | 🟠 | F: 0/1/-/- | 🟠 | F: 0/0/1/- | 🟠 | F: 0/1/-/- | 🟠 | F: 0/0/1/- | 🟠 |
| | S: 0/0/1/- | 🟢 | S: 0/0/1/- | 🟢 | S: 0/0/1/- | 🟢 | S: 0/0/1/- | 🟢 | S: 0/0/1/- | 🟢 |

| | .EXE (1) | | .BAT (2) | | .EXE (3) | | .DOCX (4) | | .ODT (5) | |
|---|---|---|---|---|---|---|---|---|---|---|
| Sophos HOME | F: 0/1/-/- | 🟠 | F: 0/0/0/0 | 🔴 | F: 0/1/-/- | 🟠 | F: 0/0/1/- | 🟠 | F: 0/0/0/0 | 🔴 |
| | S: 1/-/-/- | 🟢 | S: 0/0/0/0 | 🔴 | S: 1/-/-/- | 🟢 | S: 0/0/1/- | 🟢 | S: 0/0/0/0 | 🔴 |

| | .EXE (1) | | .BAT (2) | | .EXE (3) | | .DOCX (4) | | .ODT (5) | |
|---|---|---|---|---|---|---|---|---|---|---|
| Trend Micro IS. | F: 1/-/-/- | 🟢 | F: 1/-/-/- | 🟢 | F: 1/-/-/- | 🟠 | F: 1/-/-/- | 🟢 | F: 1/-/-/- | 🟢 |
| | S: 1/-/-/- | 🟢 | S: 0/0/0/0 | 🔴 | S: 1/-/-/- | 🟢 | S: 1/-/-/- | 🟢 | S: 1/-/-/- | 🟢 |

| | .EXE (1) | | .BAT (2) | | .EXE (3) | | .DOCX (4) | | .ODT (5) | |
|---|---|---|---|---|---|---|---|---|---|---|
| Webroot Compl. | F: 0/1/-/- | 🟠 | F: 0/0/0/0 | 🔴 | F: 0/1/-/- | 🟠 | F: 0/0/1/- | 🟢 | F: 0/0/0/0 | 🔴 |
| | S: 0/1/-/- | 🟢 | S: 0/0/0/0 | 🔴 | S: 0/1/-/- | 🟢 | S: 0/0/1/- | 🟢 | S: 0/0/0/0 | 🔴 |

| | .EXE (1) | | .BAT (2) | | .EXE (3) | | .DOCX (4) | | .ODT (5) | |
|---|---|---|---|---|---|---|---|---|---|---|
| Windows Defender | F: 0/0/0/0 | 🔴 | F: 0/0/0/0 | 🔴 | F: 0/1/-/- | 🟠 | F: 0/1/-/- | 🟠 | F: 0/0/0/0 | 🔴 |
| | S: 0/0/0/0 | 🔴 | S: 0/0/0/0 | 🔴 | S: 0/1/-/- | 🟢 | S: 0/1/-/- | 🟢 | S: 0/0/0/0 | 🔴 |

| | .EXE (1) | | .BAT (2) | | .EXE (3) | | .DOCX (4) | | .ODT (5) | |
|---|---|---|---|---|---|---|---|---|---|---|
| Zemana AM | F: 0/0/0/0 | 🔴 | F: 0/0/0/0 | 🔴 | F: 0/0/0/0 | 🔴 | F: 0/0/0/0 | 🔴 | F: 0/0/0/0 | 🔴 |
| | S: 0/0/1/- | 🟢 | S: 0/0/1/- | 🟢 | S: 0/0/1/- | 🟢 | S: 0/0/1/- | 🟢 | S: 0/0/0/0 | 🔴 |

| | .EXE (1) | | .BAT (2) | | .EXE (3) | | .DOCX (4) | | .ODT (5) | |
|---|---|---|---|---|---|---|---|---|---|---|
| Zone Alarm IS. | F: 1/-/-/- | 🟢 | F: 1/-/-/- | 🟢 | F: 1/-/-/- | 🟢 | F: 1/-/-/- | 🟢 | F: 1/-/-/- | 🟢 |
| | S: 1/-/-/- | 🟢 | S: 0/0/0/0 | 🔴 | S: 1/-/-/- | 🟢 | S: 0/0/1/- | 🟢 | S: 1/-/-/- | 🟢 |

# Results interpretation

To fully understand the intentions of AVLab experts and correctly interpret results achieved by individual antivirus applications, you should look at the test comprehensiveness from wider perspective:

Tested software was categorized into so-called “comprehensive packages” and those which due to lack of a firewall module, weren’t able to detect and stop an Internet connection established with hacker’s server.

Non-technical users may not be aware of attacks and threats, they may face every day. Freeware protection applications which don’t have a firewall module, an anti-exploit protection, a website scanner, and most importantly their own techniques of protecting computer against drive-by download attacks, won’t able to stop unauthorized intrusion into a system or a data theft. However, there are exceptions to this rule.

SecureAPlus is one of them. Defining SecureAPlus as “antivirus“ is a big understatement. SecureAPlus is powered by 12 cloud antivirus engines and one local engine (ClamAV) which is used for both a real-time protection and so-called an offline mode. In addition, SecureAPlus belongs to a security software group which bases on the application white lists, and a local data security is additionally verified on the basis of checksum information and a digital signature for every file. All this makes a difficult task for a hacker to bypass its security without triggering SecureAPlus warning alerts.

The exception of this rule is also Comodo software, which has implemented a local sandbox mechanism and uknown files scanning in the cloud, both ensuring that runnning uknown applications and scripts (.ps1, wscript.exe, .vba, .cmd, .bat, cmd.exe, .pl, .pdf, powershell.exe and others) won't access a network so they won't do any serious damage to the system.

In the context of the drive-by download attacks, 0-day exploits, and particularly the exploit kit tools, almost all of the tested security products lacked adequate CMD and PowerShell rules. As our test proved, a heuristic protection actually worked in some cases, but only after the stage of remotely run of a malicious file on victim's workstation.

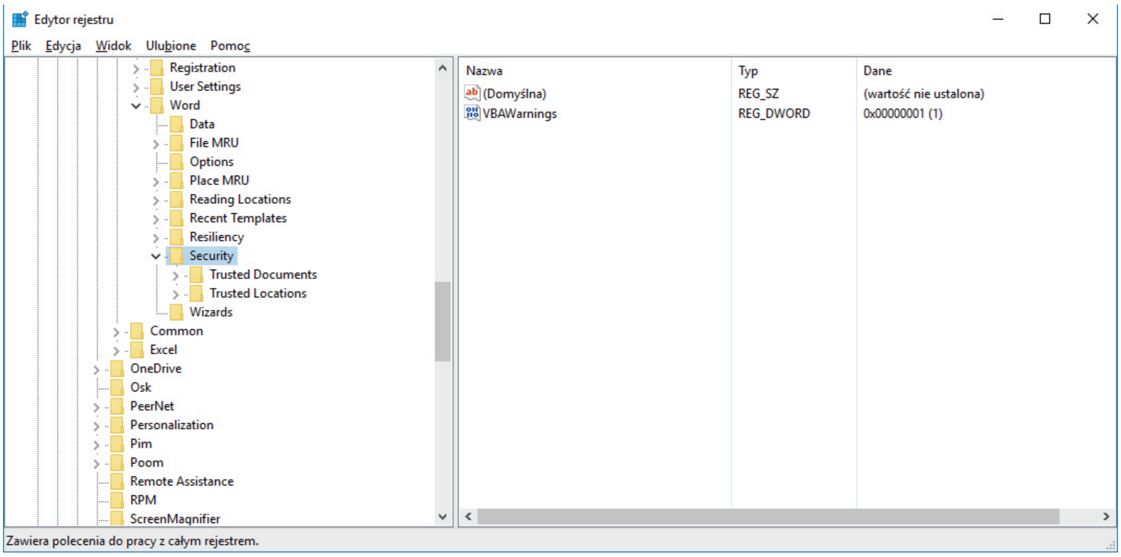
A system interpreter is a favorite tool used by hackers and malicious software developers. Scripts from an external source are a big threat. Among others, they are used for:

- Downloading payloads and performing a network recognition,
- Targeting attacks on private and governmental organizations,
- Mass attacks on regular users,
- Running malicious software directly in RAM memory (so-called fileless attacks),
- Downloading and running macro commands in MS Office,
- Running viruses written in JavaScript programming language,
- Detecting sandbox environments,
- Disabling MS Office security.

As a result of getting a remote access to attacked workstation, it's possible to bypass its security in many ways. In a situation where malicious software is detected, but Internet connection with a hacker isn't interrupted, a cybercriminal may still try other ways to bypass a security.

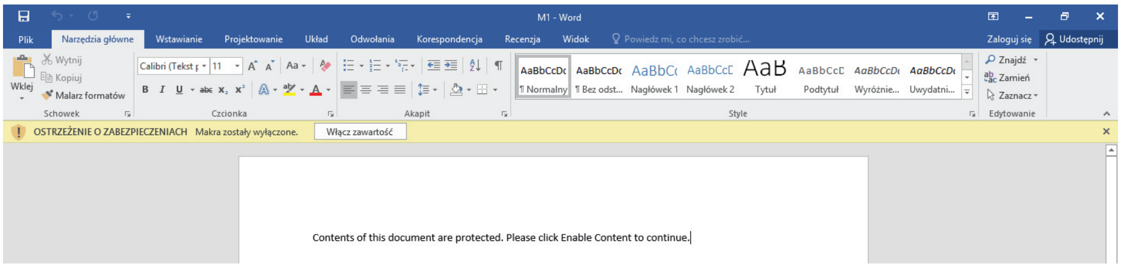
The skillful use of a PowerShell interpreter can give a hacker a significant advantage over a victim, such as disabling a security warning for documents containing macros. This is possible through adding a "VBAWarnings" key with "1" value in a registry branch:

```
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Security
```



| Nazwa | Typ | Dane |
|---|---|---|
| (Domyślna) | REG_SZ | (wartość nie ustalona) |
| VBAWarnings | REG_DWORD | 0x00000001 (1) |

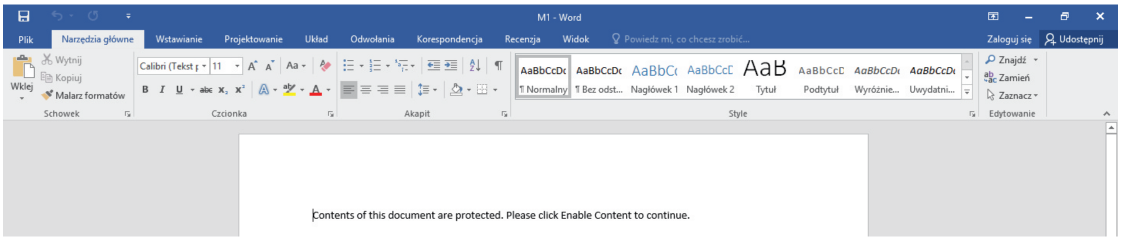
Figure. Registry modifications disable a protection in the "Trust Center" for macro settings, enabling to run a dangerous code without a warning message.



OSTRZEŻENIE O ZABEZPIECZENIACH Makra zostały wyłączone. Włącz zawartość

Contents of this document are protected. Please click Enable Content to continue.

Figure. Known by users the yellow bar is a warning about a potentially dangerous content. View before changing the key value in the registry.



Contents of this document are protected. Please click Enable Content to continue.

Figure. The same document after the modification of key value – security message isn't displayed anymore. As a result of this actions, a document downloaded from a remote server can be run by using malicious script in a PowerShell interpreter.

*Read our previous test of browsers and virtual environments for online banking in which we used a PowerShell interpreter to steal passwords directly from RAM memory.*

# Conclusions

AVLab partnership with security solution providers already brings positive results. The fruits of our work will satisfy end-users who have already gained new security rules. They were implemented by software engineers in response to our tests and provided technical details. In this case, a specific recognition is given to several developers:

SecureAge Technology, headquartered in Singapore. Their SecureAPlus software (although it doesn't have a firewall module) did a great job of detecting remotely downloaded and run files.

Software provider Comodo quickly implemented appropriate security rules for scripts and applications run by a PowerShell interpreter.

Acrabit immediately examined issues with scripts run by a PowerShell interpreter in the context of attacks and malicious software.

Several other security solutions developers in the last moment have released updates for their software before publishing this test.

Unfortunately, our sincere intentions and attempts to pass evidence of concept about security bypass have been ignored by most known developers. It's a great shame, only end-users will suffer because of this. They have spent money on a security software which doesn't protect them against the attacks shown in our test.

Out protection test against drive-by download attacks has proved that a comprehensive antivirus software isn't always sufficient enough to prevent an unauthorized intrusion into company and home workstations. To make matters worse, ignored basic security principles don't contribute to improving the situation.

Most of the tested antivirus solutions include unique protection mechanisms against attacks and malicious software. They also have weaknesses which skilled cybercriminals know very well. For this reason,  it's a good idea to take care of our own safety where network and system penetration is least likely:

* Don't run files and applications as "administrator", if it's not necessary. By creating a standard user account, you can avoid up to 99,9% of viruses.

* Keep your software and operating system up to date and uninstall unnecessary software which can be used for exploit attacks.

* Draw conclusions from someone else mistakes: by reading specialized web portals, you gain priceless knowledge about the scope of viruses, tools used by cybercriminals, and attack methods.

* Before installing a particular antivirus software, make sure that it has adequate components of protection, not only against "traditional" malware, but also against malicious scripts.

* If the security solution includes a firewall module, use its advantage, interactive mode. By creating your own rules during an attempt of getting access to the Internet by a process, you have more control over a network traffic. Doing so, you don't put yourself into a lost position in the context of the presented attacks. For the convenience of users, security application providers automatically allow outgoing and incoming traffic for trusted system processes, such as powershell.exe, cmd.exe, wscript.exe.

* Use modules to automatically update applications and system. Software for business which don't have such functionality, unless it includes unique protection mechanisms against unknown malware (such as automated sandbox, rules based on the application white lists), aren't worth your attention nowadays.

# Recommendations

### Recommendations for applications without a firewall module

🟢🟠

BEST+++, if application partially stopped the attacks
(only green and yellow indicators are allowed)

🟢🟠🔴

BEST++, if application didn't stop only one attack
(one red indicator is allowed)

🟢🟠🔴🔴

GOOD+, if application didn't stop two attacks
(up to two red indicators are allowed)

🟢🟠🔴🔴🔴

ONLY TESTED, if application didn't stop at least three attacks
(three or more red indicators)

### Recommendations for comprehensive security solutions

### Recommendations for business solutions

🟢

BEST+++, if application completely stopped all attacks
(all indicators are green)

🟢🟠

BEST++, if application partially stopped the attacks
(indicators are green and yellow)

🟢🟠🔴

GOOD+, if application didn't stop only one attack
(one red indicator is allowed)

🟢🟠🔴🔴

ONLY TESTED, if application didn't stopped more than two attacks
(only two red indicators are allowed)

## Recommendations for applications without a firewall module

| | |
|---|---|
| AVLAB AWARD BEST+++ | SecureAPlus |
| AVLAB AWARD BEST++ | Comodo Cloud Antivirus<br>Malwarebytes Anti-Malware Premium |
| AVLAB AWARD GOOD+ | --- |
| AVLAB ONLY TESTED | Avast Free Antivirus 2017<br>AVG Antivirus Free 2017<br>FortiClient 5<br>Panda Free Antivirus 2017<br>Sophos HOME<br>Windows Defender<br>Zemana Antimalware Premium<br>Qihoo 360 Total Security |

## Recommendations for business solutions

| | |
|---|---|
| AVLAB AWARD BEST+++ | Arcabit Endpoint Security<br>Bitdefender GravityZone<br>ESET Endpoint Security<br>Kaspersky Endpoint for Windows 10<br>Kaspersky Small Office Security<br>Seqrite Endpoint Security 7.2 |
| AVLAB AWARD BEST++ | Comodo ONE<br>F-Secure PSB Protection |
| AVLAB AWARD GOOD+ | --- |
| AVLAB ONLY TESTED | G Data Client Security Business<br>Panda Endpoint Protection<br>Trend Micro Worry-Free Business<br>Webroot SecureAnywhere Endpoint |

## Recommendations for comprehensive security solutions

AVLAB AWARD BEST+++

Arcabit Internet Security

Bitdefender Total Security Multi-Device 2017

Eset Smart Security 10

Kaspersky Total Security 2017

Norton Security 2017

Quick Heal Total Security 17.00

AVLAB AWARD BEST++

Comodo Internet Security 10 Pro

F-Secure SAFE

AVLAB AWARD GOOD+

Dr.Web Space Security 11

Malwarebytes Anti-malware Premium

Trend Micro Internet Security 2017

ZoneAlarm Internet Security 2017

AVLAB ONLY TESTED

Avast Premier 2017

AVG Internet Security 2017

Avira Internet Security  2017

G Data Total Protection

McAfee LiveSafe

Panda Internet Security 2017

Webroot SecureAnywhere Complete

Windows Defender

# Information about AVLab

**Our previous publications:**

Test of antivirus modules for online e-payments protection

Protection test against ransomware threats

Test of free malware scanners

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.

THE INDEPENDENT ANTIVIRUS TESTS
AVLab.pl