AV-TEST CYBERSECURITY FOUNDATION

Product of the Year 2024

Recommended solutions for securing Windows

Based on the Advanced In-The-Wild Malware Test from the year 2023

MARCH 2024

amtso
The cybersecurity industry's testing standard community

MEMBER

Table of contents

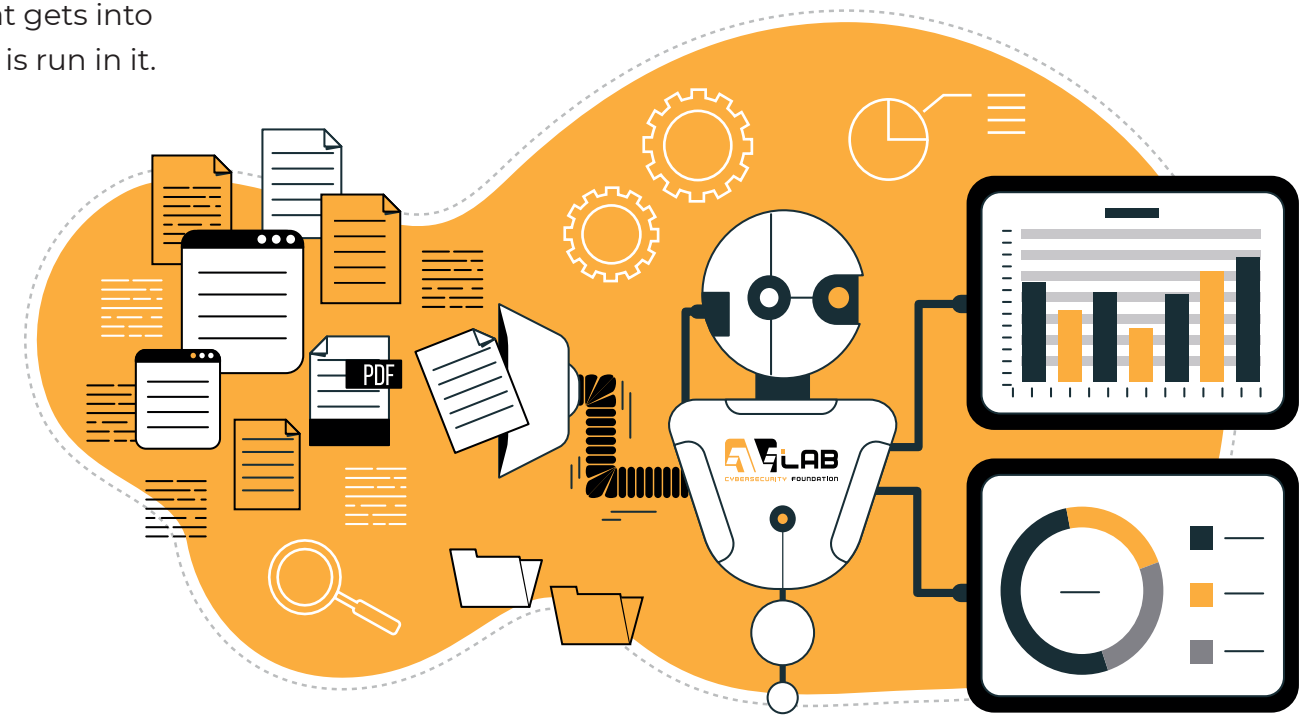
I	We award prizes.
II	Developers tested.
III	How we analyze in 3 steps.
IV	Statistics from the tests.
V	Individual Developer Cards.

Advanced In-The-Wild Malware Test Summary

The purpose of this summary is to reward those developers whose software in 2023 participated in tests initiated by the AVLab Foundation for Cybersecurity. The special Product of the Year 2024 award is a good opportunity to encourage people in IT managerial positions, heads of technology and security, whose role is to implement appropriate standards and procedures to ensure digital security using the best solutions.

When preparing the annual summary, we want to award developers in two categories. In the first one, we award the Product of the Year 2024 certificate which confirms the extremely good protection of the Windows operating system in a comprehensive perspective. Namely, we verify solutions in this series of tests on malware originating from the Internet on the default settings or with additional security features enabled, if in our opinion they should be activated.

Another distinction is the TOP Remediation Time certificate awarded for the quick response to malware that gets into the operating system in a simulated way and it is run in it. With this aspect in mind, the Advanced In-The-Wild Malware Test is very rigorous as it shows the true characteristics of the tested protection product against real threats that break into computers through spam, messengers or websites.
The TOP Remediation Time award reflects the fast response time to malware by completely neutralizing the entire "lifecycle" of malware from the moment when the sample enters the operating system to the removal of malicious activity.



Award criteria

Product of the Year 2024 and TOP Remediation Time

In order to obtain the certificate confirming the comprehensive effectiveness of protection, as well as quick and complete neutralization of the malware lifecycle , the tested solution had to meet certain requirements:

1. Participate in at least 3 editions of the Advanced In-The-Wild Malware Test.

2. Get at least 3 Excellent certificates (blocking 99% of in-the-wild malware).

3. Additionally, in order to receive the TOP Remediation Time certificate, the software had to neutralize all threats in the editions of the test which it participated in. If the solution has participated more than three times, we considered three best results of the Remediation Time indicator.

Developers tested in the year 2023

Acronis

avast

Avira

Bitdefender

COMODO
Creating Trust Online®

EMSISOFT

eset

F-Secure

G DATA

Immunet

kaspersky

Malwarebytes

norton

Quick Heal
Security Simplified

SOPHOS

ThreatDown
Powered by Malwarebytes

TREND MICRO

WEBROOT
SecureAnywhere

xcitium
The Power of Zero. Unleashed.

ZONEALARM
By Check Point

This is not a complete list, as some developers participate in tests anonymously to improve security technologies. Companies that are interested in testing their solutions, and would like to know what they can improve in their software, please contact us.

How we test – in a nutshell

Advanced In-The-Wild Malware Test is a long-term analysis that the primary purpose is to verify the protection effectiveness of the tested solutions against malware in real time. In the test, we consider business versions of security products which often have advanced EDR-XDR modules designed to automatically block threats, along with removing the effects of an attack.
We are also testing versions for individual users. In a nutshell, when we install security software on Windows, we replicate human behavior of using the Internet in a browser. This is the most common scenario where anyone can fall victim to social engineering, and unintentionally download malware into the system.

The test is based on real samples of in-the-wild malware originating from real URLs so it is the most beneficial for all users and the developers that participate in the test. A range of technical data on methods for detecting and blocking threats is revealed.
Thanks to Windows systems running in normal graphical mode, the test evaluates the adequate protection of the product, taking into account the recovery from each incident.

How we analyze in 3 steps – methodology at a glance

The results of the Advanced In-The-Wild Malware Test consist of 3 comprehensive procedures that follow each other:

1. Selecting malware for the test and analyzing logs

We collect malware in the form of real URLs from the Internet on an ongoing basis. We use a wide spectrum of samples from various sources, and these are public feeds and honeypots. The test covers the most up-to-date and diverse set of threats.

Each sample goes through a series of checks before it is tested. One of them is to compare a SHA256 sum with the existing ones in the database. As a result, the same malware is never checked twice in our tests.

The analyzed samples of potential malware undergo verification in Windows based on hundreds of rules – the most common techniques used by malware creators (the so-called LOLBin). We monitor system processes, network connections, the Windows registry, and other changes made to the operating system to find out what really indicated the harmfulness of a given sample during its analysis.

Algorithm for dealing with Malware

We check each potentially malicious file based on the following algorithm:

A SERIES OF CHECKS

A POTENTIALLY MALICIOUS FILE

1 **Is the file online?**
The threat must be available for download.

2 **Is the sample unique?**
We compare the SHA256 with the existing ones in the database.

3 **Can a file be run in Windows?**

4 **Static scanning:**
We use Yara's rules and mks_vir antivirus engine to make sure if a file is a real threat.

5 **Dynamic Scan:**
The file is run on Windows to check for malicious activity using the Sysmon utility.

MALWARE QUALIFIED FOR THE TEST

NO MALICIOUS ACTIVITY, FILE REJECTED

* Many of the threats qualified for the test are distributed over the seemingly secure HTTPS protocol. It is not difficult for the creators of malicious websites to quickly and free of charge implement a SSL certificate in order to increase the trust of the domain. Additionally, some of the files are hosted on legitimate web servers. Hackers thrive on the reputation of a given domain to fool basic security mechanisms.

2. Simulate a real-world system protection scenario

In this step, each confirmed malware sample is at the same time downloaded by a browser from the actual URL to the Windows systems where security solutions are installed. This is a very important stage of testing, because every security software should face the same threat at exactly the same time.

In the test, we simulate a real-world scenario of a threat getting into the system as a result of downloading a file from an URL. It can be a website prepared by a scammer or a link sent to the victim via messenger, e-mail, or document. After that, the link is opened in Mozilla Firefox.

SOURCE OF ATTACK **EXTRACTING URL** **DOWNLOADING MALWARE**

The result on malware sample can be classified into one of the following levels:

PRE-LAUNCH

The classification concerns detecting malware samples before they are launched in the system.

POST-LAUNCH

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

FAIL

The failure, i.e. a virus hasn't been blocked and it has infected a system.

a.

If a link to a file is quickly identified and blocked in a browser or just after saving to a hard drive by the tested product, we assign to a sample the result of the so-called PRE-LAUNCH level, where a threat is stopped at an early stage, even before it is launched.

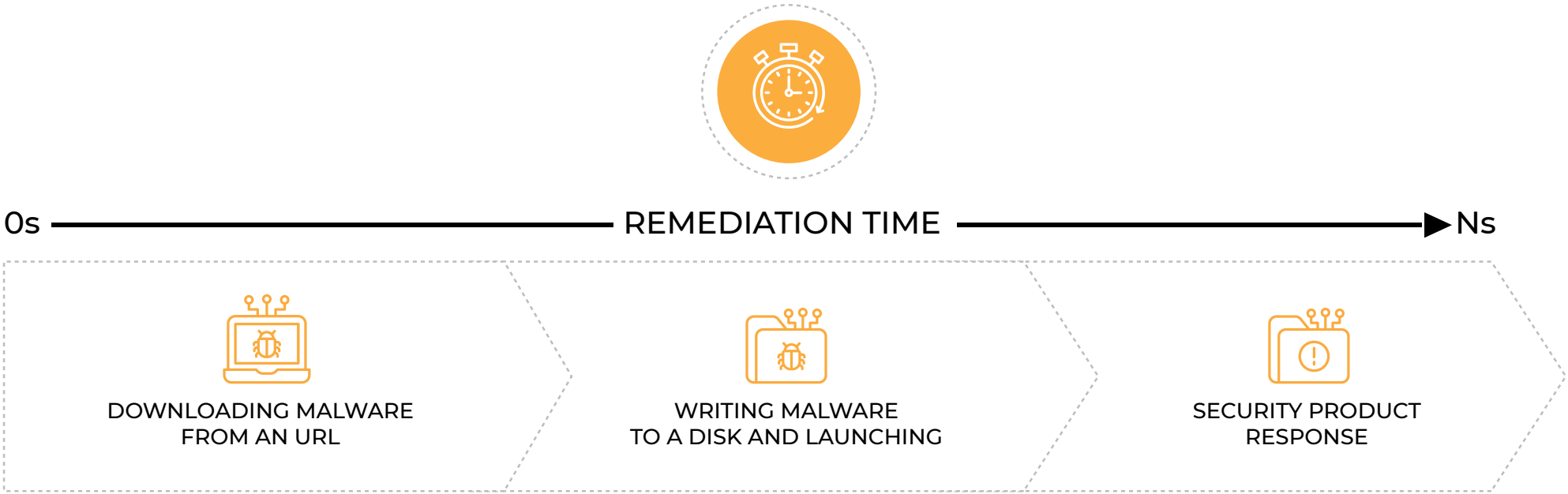
b.

If malware is downloaded, allowed to run, but successfully stopped, we assign the POST-LAUNCH level, assessing the real effectiveness of the product against known threats and 0-day files.

While the Pre-Launch level indicates the stopping of malware that was quickly detected and blocked before it activated its malicious payload, the Post-Launch level usually refers to a threat caught by any developer technology (on-premise or in the cloud) after the file has been executed in the system. It should be emphasized that the best solutions at this level are those that have differentiated protection in the form of multiple layers of security.

3. Assessment of Incident Remediation Time

Then, based on the obtained logs, in addition to detecting and blocking 0-day threats, we calculate the time of automatic remedying effects of the incident for a given malware sample. We call this the "Automatic Average Remediation Time". We configure the tested products in such a way that the effects removal of the attack along with the system repair is performed automatically, without asking a user for a decision, because this is not the purpose of the test.



To estimate the "Automatic Average Remediation Time", we assume that the incident starts with downloading a file from an URL and continues until the dynamic analysis is complete which takes 7 to 9 minutes. After that time, if we do not register any response of the security product to malware activity, this analysis ends with a negative result (Fail). Finally, for each malware sample we measure the time needed to detect indicators of compromise from the moment it is run to the automatic remediation of the incident.

Test statistics*

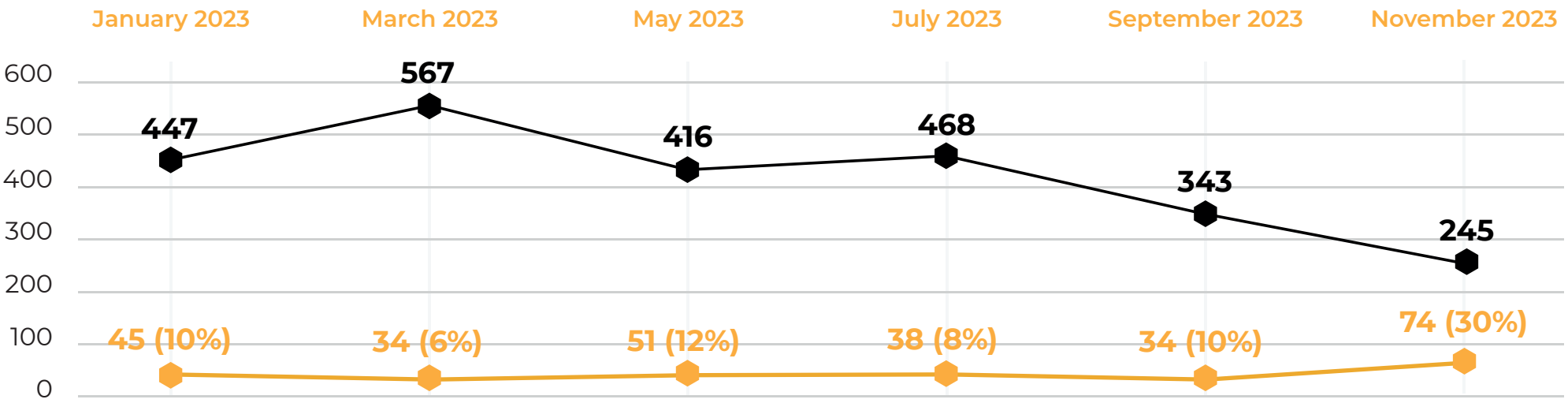
* Prepared on the basis of feedback from scanned files using the engine of our technology partner, mks_vir Sp. z o.o.

Basic information about malicious software

Taking into account telemetry data from the tested solutions, it turned out that in 2023 we used a total of 2468 samples of unique malware.

Malware in numbers

On average, 12.6% of all samples in each edition were unknown on the day of analysis which corresponds to zero-reputation files (0-day). We have noticed that malware most often were sent in the form of fake invoice files or other types of documents that impersonate well-known companies and institutions. A Trojan from the RedLine family used by cybercriminals to steal data and control user computers is very high in the statistics. In the telemetry data from the test, we find Trojan downloaders such as Zus and Zard which are most often spread by spammy email campaigns. In 2023, Trojans dominated the TOP10 list of the most common malware.

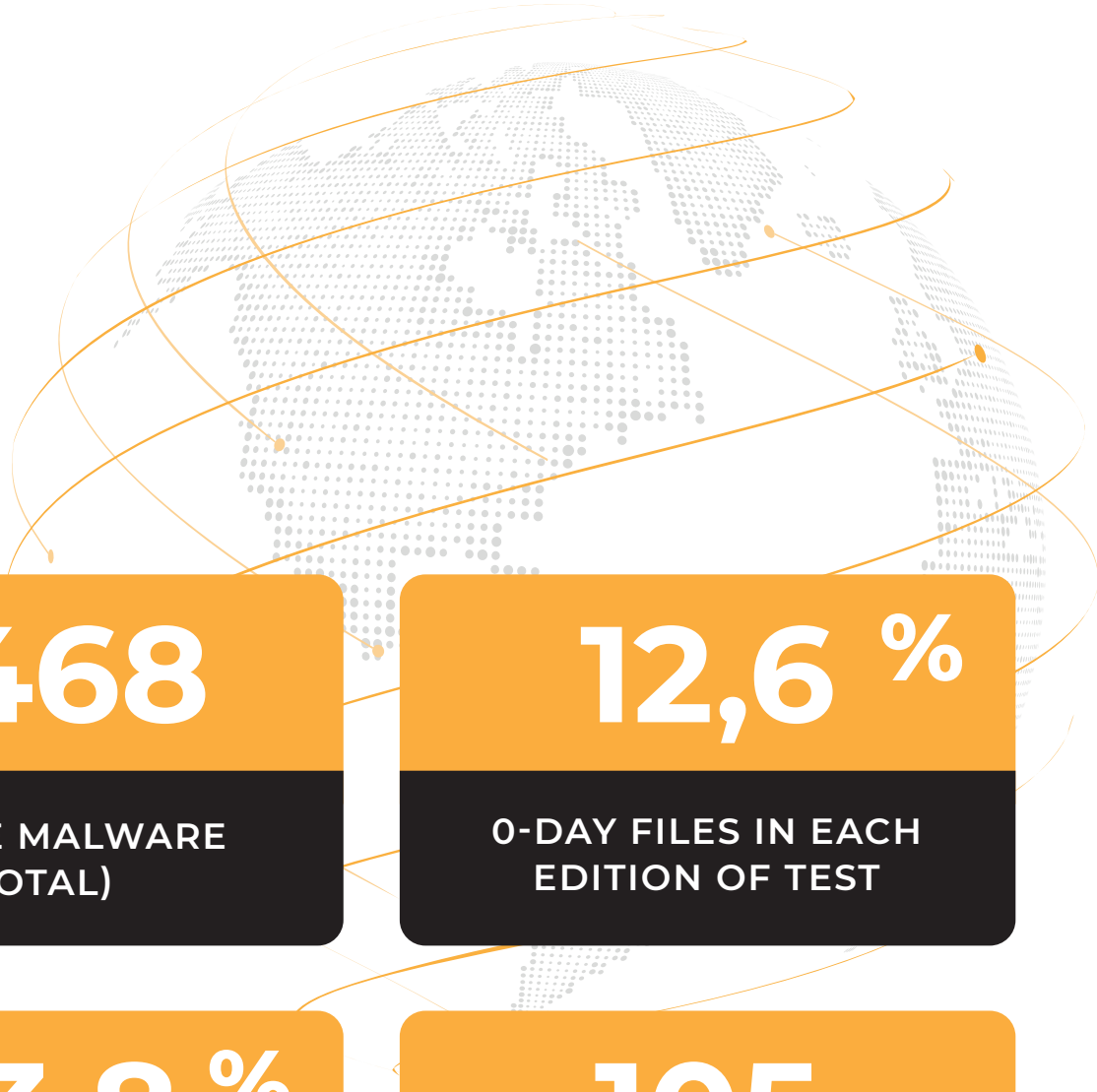


2468 Total number of confirmed malware samples in each edition of the test

276 Number of 0-day files used for the test

Other information

FROM TESTS IN 2023



6	2468	12,6 %
EDITION OF TEST	UNIQUE MALWARE (TOTAL)	0-DAY FILES IN EACH EDITION OF TEST
72,6 %	23,8 %	105 s
AVERAGE LEVEL OF MALWARE DETECTION (PRE-LANUCH)	AVERAGE LEVEL OF BLOCKING MALWARE (POST-LANUCH)	AVERAGE REMEDIATION TIME

avast

Free Antivirus

Software to protect workstations took part in all editions of the test. In total, 2468 malware samples were blocked throughout the year.
This gives a maximum score of 100% of all neutralized in-the-wild threats.

- Over 87% threats have been blocked in a browser or just after saving a file to a hard drive without running malicious software.
- Over 12% samples of malicious software have been blocked after its launch.
- Taking into account best three results, Avast needed an average of 13 seconds to automatically and flawlessly recovery from security incidents.

Based on the obtained telemetry data, we can confirm that AVAST Free Antivirus has not once exposed the operating system or data on a hard drive to potential leaks due to running malware on the test system.

	PRE	POST	FAIL	COMBINED PROTECTION	AVERAGE RT
JANUARY	94,85%	5,15%	-	100%	22s
MARCH	92,12%	6,88%	-	100%	4s
MAY	81,79%	18,21%	-	100%	43s
JULY	81,41%	18,59%	-	100%	43s
SEPTEMBER	81,79%	18,21%	-	100%	57s
NOVEMBER	90,61%	9,39%	-	100%	13s
AVERAGE	87,10%	12,74%	-	100%	13s

PRE-LAUNCH: the level concerns detecting malware samples before they are launched in the system.

POST-LAUNCH: the level refers to the analysis of when a virus broke in into the system, was launched, and detected by the tested solutions.

FAIL: the malware was not blocked, and it infected the system.

RT [REMEDIATION TIME]: average time based on the top 3 results

COMODO
Creating Trust Online®

Internet Security Pro

Software to protect workstations took part in all editions of the test. In total, 2468 malware samples were blocked throughout the year. This gives a maximum score of 100% of all neutralized in-the-wild threats.

- Over 42% threats have been blocked in a browser or just after saving a file to a hard drive without running malicious software.
- Over 57% samples of malicious software have been blocked after its launch.
- Taking into account the best three results, Comodo needed an average of 13 seconds to automatically and flawlessly recovery from security incidents.

Based on the obtained telemetry data, we can confirm that COMODO Internet Security Pro has not once exposed the operating system or data on a hard drive to potential leaks due to running malware on the test system.

	PRE	POST	FAIL	COMBINED PROTECTION	AVERAGE RT
JANUARY	21,48%	78,52%	-	100%	175s
MARCH	33,33%	66,67%	-	100%	158s
MAY	45,67%	54,33%	-	100%	170s
JULY	65,38%	34,62%	-	100%	75s
SEPTEMBER	45,95%	54,05%	-	100%	135s
NOVEMBER	43,27%	56,73%	-	100%	269s
AVERAGE	42,51%	57,49%	-	100%	123s

PRE-LAUNCH: the level concerns detecting malware samples before they are launched in the system.

POST-LAUNCH: the level refers to the analysis of when a virus broke in into the system, was launched, and detected by the tested solutions.

FAIL: the malware was not blocked, and it infected the system.

RT [REMEDIATION TIME]: average time based on the top 3 results

EMSISOFT

Enterprise Security + EDR

Software to protect workstations took part in all editions of the test. In total, 2467 out of 2468 malware samples were blocked throughout the year.
This gives almost maximum score of all neutralized in-the-wild threats.

- Almost 59% threats have been blocked in a browser or just after saving a file to a hard drive without running malicious software.
- Over 41% samples of malicious software have been blocked after its launch.
- Taking into account the best three results, Emsisoft needed an average of 106 seconds to automatically and flawlessly recovery from security incidents.

Based on the obtained telemetry data, we can confirm that EMSISOFT has not exposed the operating system or data to a potential leak in a severe manner due to running malware on the test system. One reported incident has been immediately analyzed by specialized team of analysts, and quickly eliminated.

	PRE	POST	FAIL	COMBINED PROTECTION	AVERAGE RT
JANUARY	62,75%	37,25%	-	100%	254s
MARCH	59,08%	40,92%	-	100%	242s
MAY	54,81%	45,19%	-	100%	181s
JULY	57,69%	42,31%	-	100%	167s
SEPTEMBER	57,51%	42,49%	-	100%	139s
NOVEMBER	59,59%	40,00%	0,41% (1 sample)	99,59%	13s
AVERAGE	58,57%	41,36%	0,07%	99,93%	106s

PRE-LAUNCH: the level concerns detecting malware samples before they are launched in the system.

POST-LAUNCH: the level refers to the analysis of when a virus broke in into the system, was launched, and detected by the tested solutions.

FAIL: the malware was not blocked, and it infected the system.

RT [REMEDIATION TIME]: average time based on the top 3 results

Smart Security Premium

Software to protect workstations took part 3 out of 6 editions of the test. In total, 1056 malware samples have been blocked. This gives a maximum score of 100% of all neutralized in-the-wild threats.

- Almost 86% threats have been blocked in a browser or just after saving a file to a hard drive without running malicious software.
- Over 14% samples of malicious software have been blocked after its launch.
- Taking into account the best three results, Eset needed an average of 31 seconds to automatically and flawlessly recovery from security incidents.

Based on the obtained telemetry data, we can confirm that ESET Smart Security has not once exposed the operating system or data on a hard drive to potential leaks due to running malware on the test system.

	PRE	POST	FAIL	COMBINED PROTECTION	AVERAGE RT
JANUARY	not tested	-	-	-	-
MARCH	not tested	-	-	-	-
MAY	not tested	-	-	-	-
JULY	82,26%	17,74%	-	100%	50s
SEPTEMBER	81,79%	18,21%	-	100%	34s
NOVEMBER	93,88%	6,12%	-	100%	8s
AVERAGE	85,98%	14,02%	-	100%	31s

PRE-LAUNCH: the level concerns detecting malware samples before they are launched in the system.

POST-LAUNCH: the level refers to the analysis of when a virus broke in into the system, was launched, and detected by the tested solutions.

FAIL: the malware was not blocked, and it infected the system.

RT [REMEDIATION TIME]: average time based on the top 3 results

F-Secure | Total

Software to protect workstations took part in 4 out of 6 editions of the test. In total, 1628 out of 1632 malware samples have been blocked. This gives almost maximum score of all neutralized in-the-wild threats.

- Over 82% threats have been blocked in a browser or just after saving a file to a hard drive without running malicious software.
- Over 17% samples of malicious software have been blocked after its launch.
- Taking into account the best three results, F-Secure needed an average of 13 seconds to automatically and flawlessly recovery from security incidents.

Based on the obtained telemetry data, we can confirm that F-SECURE has not exposed the operating system or data to a potential leak in a severe manner due to running malware on the test system.

	PRE	POST	FAIL	COMBINED PROTECTION	AVERAGE RT
JANUARY	not tested	-	-	-	-
MARCH	83,25%	16,05%	0,71% (1 sample)	99,29%	27s
MAY	not tested	-	-	-	-
JULY	79,49%	20,51%	-	100%	13s
SEPTEMBER	83,53%	16,47%	-	100%	21s
NOVEMBER	84,08%	15,92%	-	100%	6s
AVERAGE	82,59%	17,24%	0,18%	99,82%	13s

PRE-LAUNCH: the level concerns detecting malware samples before they are launched in the system.

POST-LAUNCH: the level refers to the analysis of when a virus broke in into the system, was launched, and detected by the tested solutions.

FAIL: the malware was not blocked, and it infected the system.

RT [REMEDIATION TIME]: average time based on the top 3 results

Total Security

Software to protect workstations took part in 4 out of 6 editions of the test. In total, 1472 malware samples have been blocked. This gives a maximum score of 100% of all neutralized in-the-wild threats.

- Over 94% threats have been blocked in a browser or just after saving a file to a hard drive without running malicious software.
- Almost 6% samples of malicious software have been blocked after its launch.
- Taking into account the best three results, G Data needed an average of 16 seconds to automatically and flawlessly recovery from security incidents.

Based on the obtained telemetry data, we can confirm that G DATA Total Security has not once exposed the operating system or data on a hard drive to potential leaks due to running malware on the test system.

	PRE	POST	FAIL	COMBINED PROTECTION	AVERAGE RT
JANUARY	not tested	-	-	-	-
MARCH	not tested	-	-	-	-
MAY	93,99%	6,01%	-	100%	81s
JULY	88,03%	11,97%	-	100%	14s
SEPTEMBER	100%	0%	-	100%	0s
NOVEMBER	95,1%	4,9%	-	100%	33s
AVERAGE	94,28%	5,72%	-	100%	16s

PRE-LAUNCH: the level concerns detecting malware samples before they are launched in the system.

POST-LAUNCH: the level refers to the analysis of when a virus broke in into the system, was launched, and detected by the tested solutions.

FAIL: the malware was not blocked, and it infected the system.

RT [REMEDIATION TIME]: average time based on the top 3 results

kaspersky | Plus

Software to protect workstations took part in 4 out of 6 editions of the test. In total, 1472 malware samples have been blocked. This gives a maximum score of 100% of all neutralized in-the-wild threats.

- Over 96% threats have been blocked in a browser or just after saving a file to a hard drive without running malicious software.
- Over 3% samples of malicious software have been blocked after its launch.
- Taking into account the best three results, Kaspersky needed an average of 16 seconds to automatically and flawlessly recovery from security incidents.

Based on the obtained telemetry data, we can confirm that KASPERSKY Plus has not once exposed the operating system or data on a hard drive to potential leaks due to running malware on the test system.

	PRE	POST	FAIL	COMBINED PROTECTION	AVERAGE RT
JANUARY	not tested	-	-	-	-
MARCH	not tested	-	-	-	-
MAY	97,84%	2,16%	-	100%	164s
JULY	97,65%	2,35%	-	100%	82s
SEPTEMBER	97,11%	2,89%	-	100%	287s
NOVEMBER	94,69%	5,31%	-	100%	122s
AVERAGE	96,82%	3,18%	-	100%	123s

PRE-LAUNCH: the level concerns detecting malware samples before they are launched in the system.

POST-LAUNCH: the level refers to the analysis of when a virus broke in into the system, was launched, and detected by the tested solutions.

FAIL: the malware was not blocked, and it infected the system.

RT [REMEDIATION TIME]: average time based on the top 3 results

Malwarebytes | Premium

Software to protect workstations took part in all editions of the test. In total, 2468 malware samples have been blocked. This gives a maximum score of 100% of all neutralized in-the-wild threats.

- Almost 85% threats have been blocked in a browser or just after saving a file to a hard drive without running malicious software.
- Over 15% samples of malicious software have been blocked after its launch.
- Taking into account best three results, Malwarebytes needed an average of 183 seconds to automatically and flawlessly recovery from security incidents.

Based on the obtained telemetry data, we can confirm that MALWAREBYTES Premium has not once exposed the operating system or data on a hard drive to potential leaks due to running malware on the test system.

	PRE	POST	FAIL	COMBINED PROTECTION	AVERAGE RT
JANUARY	95,79%	4,21%	-	100%	294s
MARCH	89,59%	10,41%	-	100%	219s
MAY	89,42%	10,58%	-	100%	209s
JULY	83,96%	16,03%	-	100%	138s
SEPTEMBER	78,03%	21,97%	-	100%	286s
NOVEMBER	70,61%	29,39%	-	100%	202s
AVERAGE	84,57%	15,43%	-	100%	183s

PRE-LAUNCH: the level concerns detecting malware samples before they are launched in the system.

POST-LAUNCH: the level refers to the analysis of when a virus broke in into the system, was launched, and detected by the tested solutions.

FAIL: the malware was not blocked, and it infected the system.

RT [REMEDIATION TIME]: average time based on the top 3 results

MICROSOFT Defender

Software to protect workstations took part in 3 out of 6 editions of the test. In total, 1420 out of 1430 malware samples have been blocked. This gives a score of 99% neutralized in-the-wild threats.

- Over 18% threats have been blocked in a browser or just after saving a file to a hard drive without running malicious software.
- Over 81% samples of malicious software have been blocked after its launch.
- Taking into account the best three results, Microsoft solution needed an average of 119 seconds to automatically and flawlessly recovery from security incidents.

Based on the obtained telemetry data, we conclude that MICROSOFT Defender may have exposed the operating system and data on a hard drive to a potential leak due to running malware on the test system.

	PRE	POST	FAIL	COMBINED PROTECTION	AVERAGE RT
JANUARY	18,79%	80,76%	0,45% (2 samples)	99,55%	115s
MARCH	15,7%	83,6%	0,7% (4 samples)	99,29%	122s
MAY	19,95%	79,09%	0,96% (4 samples)	99,04%	121s
JULY	not tested	-	-	-	-
SEPTEMBER	not tested	-	-	-	-
NOVEMBER	not tested	-	-	-	-
AVERAGE	18,15%	81,15%	0,7%	99,29%	119s

PRE-LAUNCH: the level concerns detecting malware samples before they are launched in the system.

POST-LAUNCH: the level refers to the analysis of when a virus broke in into the system, was launched, and detected by the tested solutions.

FAIL: the malware was not blocked, and it infected the system.

RT [REMEDIATION TIME]: average time based on the top 3 results

ThreatDown
Powered by Malwarebytes

Endpoint Protection + EDR

Software to protect workstations took part in all editions of the test. In total, 2468 malware samples have been blocked. This gives a maximum score of 100% of all neutralized in-the-wild threats.

- Almost 86% threats have been blocked in a browser or just after saving a file to a hard drive without running malicious software.
- Over 14% samples of malicious software have been blocked after its launch.
- Taking into account best three results, ThreatDown needed an average of 167 seconds to automatically and flawlessly recovery from security incidents.

Based on the obtained telemetry data, we can confirm that THREATDOWN Endpoint Protection has not once exposed the operating system or data on a hard drive to potential leaks due to running malware on the test system.

	PRE	POST	FAIL	COMBINED PROTECTION	AVERAGE RT
JANUARY	97,09%	2,91%	-	100%	289s
MARCH	89,42%	10,58%	-	100%	221s
MAY	89,66%	10,34%	-	100%	180s
JULY	81,84%	18,16%	-	100%	157s
SEPTEMBER	80,35%	19,65%	-	100%	189s
NOVEMBER	77,55%	22,45%	-	100%	163s
AVERAGE	85,99%	14,01%	-	100%	167s

PRE-LAUNCH: the level concerns detecting malware samples before they are launched in the system.

POST-LAUNCH: the level refers to the analysis of when a virus broke in into the system, was launched, and detected by the tested solutions.

FAIL: the malware was not blocked, and it infected the system.

RT [REMEDIATION TIME]: average time based on the top 3 results

Quick Heal
Security Simplified

Total Security

Software to protect workstations took part in 4 out of 6 editions of the test. In total, 1472 malware samples have been blocked. This gives a maximum score of 100% of all neutralized in-the-wild threats.

- Over 82% threats have been blocked in a browser or just after saving a file to a hard drive without running malicious software.
- Almost 18% samples of malicious software have been blocked after its launch.
- Taking into account the best three results, Quick Heal needed an average of 38 seconds to automatically and flawlessly recovery from security incidents.

Based on the obtained telemetry data, we can confirm that QUICK HEAL Total Security has not once exposed the operating system or data on a hard drive to potential leaks due to running malware on the test system.

	PRE	POST	FAIL	COMBINED PROTECTION	AVERAGE RT
JANUARY	not tested	-	-	-	-
MARCH	not tested	-	-	-	-
MAY	91,59%	8,41%	-	100%	36s
JULY	78,85%	21,15%	-	100%	24s
SEPTEMBER	76,59%	23,41%	-	100%	55s
NOVEMBER	81,22%	18,78%	-	100%	59s
AVERAGE	82,06%	17,94%	-	100%	38s

PRE-LAUNCH: the level concerns detecting malware samples before they are launched in the system.

POST-LAUNCH: the level refers to the analysis of when a virus broke in into the system, was launched, and detected by the tested solutions.

FAIL: the malware was not blocked, and it infected the system.

RT [REMEDIATION TIME]: average time based on the top 3 results

WEBROOT by opentext™

Antivirus

Software to protect workstations took part in all editions of the test. In total, 1471 out of 1472 malware samples have been blocked. This gives almost maximum score of 100% of all neutralized in-the-wild threats.

- Over 48% threats have been blocked in a browser or just after saving a file to a hard drive without running malicious software.
- Almost 52% samples of malicious software have been blocked after its launch.
- Taking into account the best three results, Webroot needed an average of 36 seconds to automatically and flawlessly recovery from security incidents.

Based on the obtained telemetry data, we can confirm that Webroot Antivirus has not exposed the operating system or data to a potential leak in a severe manner due to running malware on the test system.

	PRE	POST	FAIL	COMBINED PROTECTION	AVERAGE RT
JANUARY	44,3%	55,7%	-	100%	125s
MARCH	43,03%	56,97%	-	100%	25s
MAY	51,92%	47,84%	0,24% (1 sample)	99,76%	100s
JULY	63,68%	36,32%	-	100%	54s
SEPTEMBER	41,04%	58,96%	-	100%	30s
NOVEMBER	44,9%	55,1%	-	100%	180s
AVERAGE	48,15%	51,82%	0,24%	99,96%	36s

PRE-LAUNCH: the level concerns detecting malware samples before they are launched in the system.

POST-LAUNCH: the level refers to the analysis of when a virus broke in into the system, was launched, and detected by the tested solutions.

FAIL: the malware was not blocked, and it infected the system.

RT [REMEDIATION TIME]: average time based on the top 3 results

xcitium

The Power of Zero. Unleashed.

ZeroThreat Advanced + EDR

Software to protect workstations took part in all editions of the test. In total, 2468 malware samples have been blocked. This gives a maximum score of 100% of all neutralized in-the-wild threats.

- Almost 86% threats have been blocked in a browser or just after saving a file to a hard drive without running malicious software.
- Over 14% samples of malicious software have been blocked after its launch.
- Taking into account best three results, Xcitium needed an average of 79 seconds to automatically and flawlessly recovery from security incidents.

Based on the obtained telemetry data, we can confirm that XCITIUM has not once exposed the operating system or data on a hard drive to potential leaks due to running malware on the test system.

	PRE	POST	FAIL	COMBINED PROTECTION	AVERAGE RT
JANUARY	2,24%	97,76%	-	100%	136s
MARCH	7,94%	92,06%	-	100%	110s
MAY	15,14%	84,86%	-	100%	107s
JULY	5,13%	94,87%	-	100%	21s
SEPTEMBER	3,18%	96,82%	-	100%	119s
NOVEMBER	23,67%	76,33%	-	100%	179s
AVERAGE	9,55%	90,45%	-	100%	79s

PRE-LAUNCH: the level concerns detecting malware samples before they are launched in the system.

POST-LAUNCH: the level refers to the analysis of when a virus broke in into the system, was launched, and detected by the tested solutions.

FAIL: the malware was not blocked, and it infected the system.

RT [REMEDIATION TIME]: average time based on the top 3 results

The AVLab Cybersecurity Foundation is an independent organization dedicated to protecting privacy and security on the Internet. We are part of the CTF (Cyber Transparency Forum) and provide independent assessments of cybersecurity vendors' systems. We are a member of AMTSO (Anti-Malware Testing Standards Organization), which works to improve the transparency, objectivity and quality of testing.

We build awareness of users in the field of digital protection. We issue opinions, technical analyzes and tests of IT solutions in the field of cybersecurity. Our strongest assets include thorough and detailed reviews, preparation of reports related to privacy and endpoint protection, and in particular, security tests that make us recognizable all over the world as one of the most trusted and popular testing laboratories.

To learn more about other opportunities for cooperation,
please refer to our full offer and contact us: kontakt@avlab.pl

amtso
The cybersecurity industry's testing standard community
MEMBER

www.avlab.pl