AV-TEST CYBERSECURITY FOUNDATION

Product of the year

Based on the Advanced In The Wild Malware Test

Summary of security tests in 2022

February 2023

The most severe threats and attacks of the year 2022

2022 dominated by ransomware and wipers

During the entire year developers of modern endpoint security solutions update their software several times by fixing errors and adding new features. Thanks to the in-depth Advanced In-The-Wild Malware Tests it is possible to check the effectiveness of protection throughout the year.

Cyber criminals are constantly looking for new ways to outsmart the security of systems and applications designed to protect, and because the existence of malware in the wild is short but dynamic and destructive, developers must adapt protection technologies for systems preventing data theft, encryption, or destruction by so-called wipers.

Fortinet **[1]** claims that this is a trend of the evolution of threats as one of the hacker's tools, as evidenced by the spread of malicious software that removes data. Ransomware-Wiper is designed to destroy or delete important data on computers and network. It can be delivered in different ways, including email attachments, malicious websites or software installers.

If you think you may be a victim of an attacks, it is important to take an immediate action to minimize harm and prevent further spreading. This may include isolating workstation, restoring data from backup, or seeking help from cyber security specialist.

In 2022 cyber criminals sent much more messages with malicious content than in 2021. Developers of the oldest Polish antivirus mks_vir **[2]** noted a significant increase in encryption threats. Out of all detected malicious files, as many as many as 40% were ransomware, often with a payload that destroys data. There were also “old players” with a participation of 10% in the controlled Emotet botnet and related attacks: traffic redirection, spam, DDoS, credential stealing. PUAs and PUPs had clear participation in statistics as fake antivirus, applications pretending to clean the system or update drivers (16%), spyware, and adware (10%).

A large percentage of this type of applications has an advanced mechanism that make them difficult to detect and remove from the system. The most popular systems in telemetry of Polish developer are: Windows 10 (74%), Windows 7 (11%), Windows 11 (11%), Windows 8/8.1 (3%), Windows XP/Vista (1%). It is worth mentioning that despite only 1% of the market share for the old Windows XP and Vista systems, their presence is stable and does not decrease in developer’s statistics, mainly due to the use of old hardware and the need for older versions of applications (for example accounting) that prevent the exclusion of such system from use.

The mks_vir telemetry data is consistent with the Cisco report **[3]**: in the past quarter, ransomware was 40% of the observed cyber security threats and the most common target of the attacks were educational institutions, financial services, government systems, power industry, and e-commerce. Similar conclusions are being drawn from the study “Data Protection Trends Report 2022” by the Veeam company **[4]**: healthcare providers have irretrievably lost nearly 40% of data that were encrypted as a result of ransomware attack. Cyber-attacks were also the reason for most interruptions in hospitals and clinics.

[1] Fortinet: https://avlab.pl/dwukrotny-wzrost-ransomware-proby-zniszczenia-backupu
[2] mks_vir: The data was provided by a Polish vendor of an endpoint and mobile device security solution
[3] Cisco: https://avlab.pl/4-fakty-o-konsumentach-w-zakresie-ochrony-danych-dla-e-commerce
[4] Veem: https://avlab.pl/cyberataki-odpowiadaja-za-najwiecej-przerw-w-dzialalnosci-szpitali-i-klinik/

There will be more social engineering attacks in 2023!

In 2022 we saw a noticeable increase in the number of social engineering attacks. Experts predict that this will be a strengthening trend in 2023. According to an expert from Acronis **[1]** the BEC attacks will increasingly spread to other messaging services such as SMS, Slack, Teams, and other communicators in order to avoid filtering and detection by security solutions. On the other hand, ESET **[2]** predicts that in Poland in 2023 the most popular will be malicious software, website and Remote Desktop Protocol attacks.

The resources available to companies may be insufficient both in terms of software and the staff of IT specialists. This is conducive to crime, and increases the risk that the attack will succeed if the weakest link is an untrained employee. In the period from January to December 2022, a big problem for companies was the lack of awareness of cyber threats among employees, as well as the financial consequences of hacker intrusion. Image losses were reflected in customer churn where more than 70% of consumers say **[3]** they would not have made a purchase from a company that they do not trust in terms of the processing of personal data. In 2023 special attention should be paid to the BEC (Business Email Compromise) attacks, as these are scams made using social engineering techniques. Data leaks and intrusions into companies have found a wide echo in the media that has a negative impact on the image of the attacked company.

[1] Cisco: https://avlab.pl/cisco-talos-ostrzega-ransomware-powrocil-do-lask-cyberprzestepcow
[2] Acronis: https://avlab.pl/prognozy-dotyczace-zagrozen-cybernetycznych-w-2023-roku
[3] Eset: https://avlab.pl/eset-polskie-firm-najbardziej-obawiaja-sie-malware-i-atakow-na-strony-internetowej

Summary of test in 2022

The aim of this summary is to reward developers whose software were involved in tests conducted by AVLab Cybersecurity Foundation in 2022. When choosing a solution to the needs, enterprises should select important features that will comprehensively protect their resources. The special award “Product of the Year 2022” is a good opportunity to encourage people in IT management positions, technology and security leaders (CISO) whose task is to implement appropriate standards and procedures to keep the company secure using the best solutions. In addition, cybersecurity technology providers can learn how the testing industry assesses protection mechanisms. A comprehensive look at security from the perspective of tests requires supplementing the knowledge of employees on the subject of social engineering attacks.

About the Advanced In The Wild Malware Test

It is a long-term analysis that the primary purpose is to verify in real time the effectiveness of Windows security solutions in various aspects. We simulate user behavior when browsing the Internet, and may fall victim to a social engineering attack. Due to the real malware used, the test is the most beneficial for developers as it indicates the type of technology that helps to block a threat. It is also a confirmation of the usefulness of tools for early-stage alerting on threats from the Internet and mechanisms for detecting malware during its analysis in the system memory.

For the tested solutions, less than half of all samples on average used in the tests in 2022 were an unknown threat at the date of analysis which corresponds to 0-day files with unknown reputation.
This is explained by the following legend for the Post-Launch level:

PRE-LAUNCH	POST-LAUNCH	FAIL
Applies to detecting malware before it is launched in the system.	Applies to the analysis when a virus has got into the system, has been launched, and detected by tested solutions.	Malware has not been blocked and infected the system.

Advanced In The Wild Malware Test in numbers

In 2022 we conducted 6 editions of the test. Each was carried out every two months. For example, starting from January: at the beginning of February we sent feedback to developers and publish the results. In March we start another edition. Similarly, in the following months. In 2022 we used 10453 samples of unique malicious software. This means that there was no situation of testing on the same sample of malware throughout the year 2022.

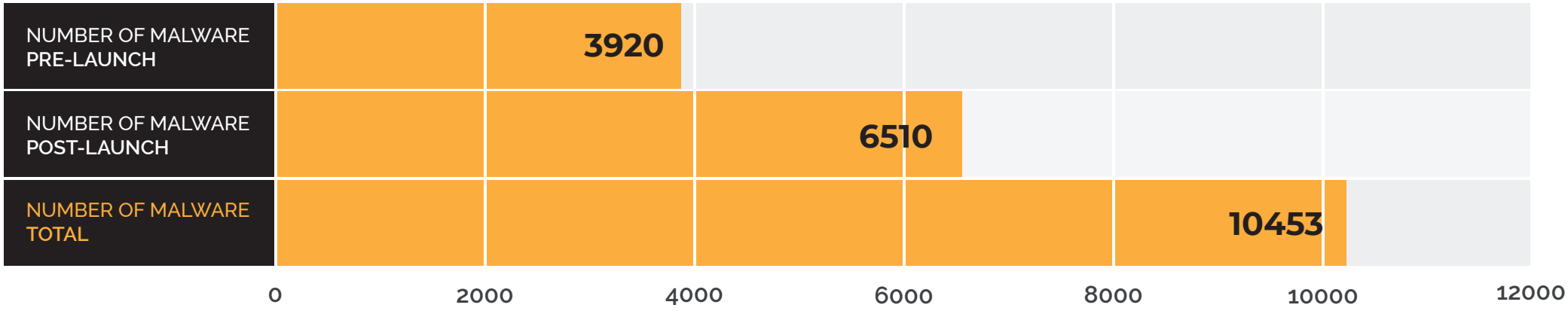
Total number of malware in 2022: **10453**

JANUARY	MARCH	MAY
1824	2044	1922

JULY	SEPTEMBER	NOVEMBER
2182	2081	400*

* In the November edition we changed the way malware gets into Windows. This resulted in a reduction of the number of the in-the-wild samples, but better reflects the test assumptions. In subsequent editions we will use this improved method.
You can learn more in the summary of the November 2022 edition:
https://avlab.pl/en/security-test-of-400-malicious-samples-in-the-wild/

Telemetry data from the test system



Malware w liczbach

MALWARE PRE-LAUNCH

3920

The total number of malware where the time of preventive blocking is 0 seconds. It is the situation when a sample in the test has been blocked in early-stage of access to the malicious website, when downloading a file in a browser, or just after saving a file to a hard drive, even before launching a malicious file.

MALWARE POST-LAUNCH

6510

The total number of malicious software after getting into the system and being detected by any technology using the available protection modules of the developer. The detection time of such samples is greater than 0 seconds. The exact detection time after launching an unknown file will be provided from the next edition of the test.

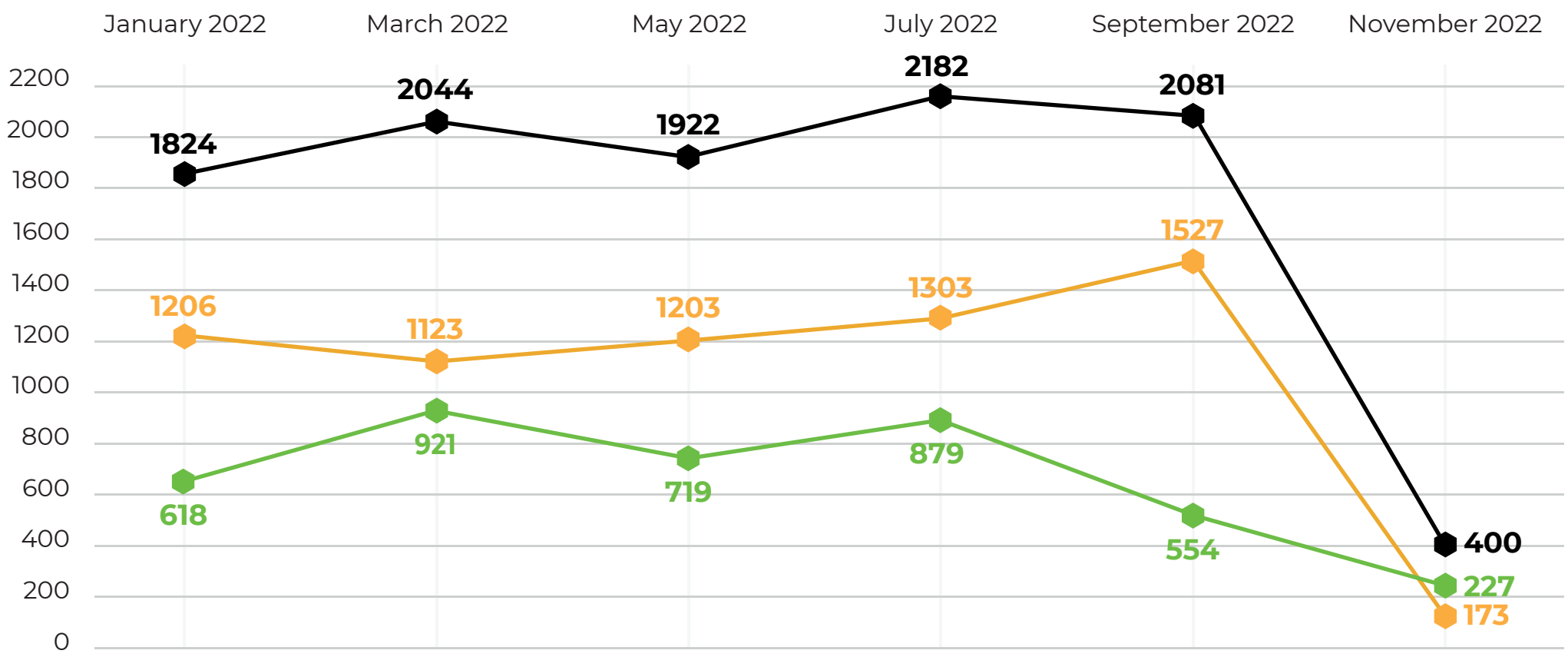
MALWARE TOTAL

10453

The total number of malware analyzed in Windows by the tested solutions in 2022.

Number of malware in the Advanced In The Wild Malware Test

Divided into individual editions of the test in a given month



10453 Total number of malware

6510 Average number of malware blocked at the Pre-Launch level

3920 Average number of malware blocked at the Post-Launch level

Product of the Year 2022

A product had to meet certain conditions in order to win the award which is a special certificate:

1. Participate in all editions of the Advance In The Wild Malware Test.

2. Block all samples in every edition of the test.

A solution could not get a unique certificate if:

- A product has failed to block at least one sample in any edition of the test.
- A product has not participated in all editions of the test. *

* Some developers declare willingness to participate in the test in order to check protection just once. Having in mind the long-term nature of the tests, we must take into account both groups by granting appropriate certificate „Product of the Year 2022" only to those security solutions that participated in all editions of the test.

Special award
„Product of the Year 2022”

AVAST
Free Antivirus

Software to protect workstations took part in all editions of the test. In total, 10453 out of 10453 malware samples were blocked throughout the year resulting in a maximum score of 100% of the in-the-wild threats stopped.

- Over 26% threats have been blocked in a browser or just after saving a file to a hard drive at the Pre-Launch level.
- Over 73% threats have been blocked after launching malicious software at the Post-Launch level.

6 x

PARTICIPATION IN TEST 6/6

	PRE	POST	FAIL	TOTAL
JANUARY	21%	79%	-	100%
MARCH	16,49%	83,51%	-	100%
MAY	7,79%	92,21%	-	100%
JULY	10,94%	89,06%	-	100%
SEPTEMBER	7.87%	92.23%	-	100%
NOVEMBER	95.75%	4.25%	-	100%
AVERAGE	26,64%	73,37%	-	100%

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.

CatchPulse®

Special award
„Product of the Year 2022”

CATCHPULSE (formalnie SecureAPlus Pro)

The software to protect workstation has participated in all editions of the test. It has blocked 10453/10453 malware samples which result in a maximum score of 100% protection against threats in the wild.

- More than 58% of threats have been blocked in a browser or after saving to a disk.
- Over 41% of threats have been blocked after launching malicious software.

6 x

PARTICIPATION IN TEST 6/6

	PRE	POST	FAIL	TOTAL
JANUARY	77%	23%	-	100%
MARCH	72,15%	27,85%	-	100%
MAY	51,79%	48,21%	-	100%
JULY	75,01%	24,99%	-	100%
SEPTEMBER	70,86%	29,14%	-	100%
NOVEMBER	1,75%	98,25%	-	100%
AVERAGE	58,09%	41,49%	-	100%

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.

EMSISOFT

Special award
„Product of the Year 2022”

Emsisoft Business Security

The software to protect workstation has participated in all editions of the test. It has blocked 10453/10453 malware samples which result in a maximum score of 100% protection against threats in the wild.

- More than 10% of threats have been blocked in a browser or after saving to a disk.
- Over 89% of threats have been blocked after launching malicious software.

	PRE	POST	FAIL	TOTAL
JANUARY	-	100%	-	100%
MARCH	-	100%	-	100%
MAY	-	100%	-	100%
JULY	2,79%	97,21%	-	100%
SEPTEMBER	0,15%	99,85%	-	100%
NOVEMBER	62,75%	37,25%	-	100%
AVERAGE	10,94%	89,06%	-	100%

6 x

PARTICIPATION IN TEST 6/6

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.

xcitium

The Power of Zero. Unleashed.

Special award
„Product of the Year 2022”

Xcitium ZeroThreat Advanced Endpoint Protection

The software to protect workstation has participated in all editions of the test. It has blocked 10453/10453 malware samples which result in a maximum score of 100% protection against threats in the wild.

- More than 7% of threats have been blocked in a browser or after saving to a disk.
- Over 92% of threats have been blocked after launching malicious software.

6 x

PARTICIPATION IN TEST 6/6

	PRE	POST	FAIL	TOTAL
JANUARY	1%	99%	-	100%
MARCH	0,34%	99,66%	-	100%
MAY	0,1%	99,9%	-	100%
JULY	19,13%	80,87%	-	100%
SEPTEMBER	21,48%	78,52%	-	100%
NOVEMBER	2%	98%	-	100%
AVERAGE	7,34%	92,66%	-	100%

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.

xcitium

The Power of Zero. Unleashed.

Special award
„Product of the Year 2022”

Xcitium Internet Security Pro

The software to protect workstation has participated in all editions of the test. It has blocked 10453/10453 malware samples which result in a maximum score of 100% protection against threats in the wild.

- More than 2% of threats have been blocked in a browser or after saving to a disk.
- Over 97% of threats have been blocked after launching malicious software.

6 x

PARTICIPATION IN TEST 6/6

	PRE	POST	FAIL	TOTAL
JANUARY	2%	98%	-	100%
MARCH	0,39%	99,61%	-	100%
MAY	0,31%	99,69%	-	100%
JULY	3,43%	96,57%	-	100%
SEPTEMBER	0,19%	99,81%	-	100%
NOVEMBER	6%	94%	-	100%
AVERAGE	2,05%	97,95%	-	100%

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.

Avira

Avira Antivirus Pro

The software to protect workstation has participated in all editions of the test. It has blocked 99,74% malware samples.

- More than 67% of threats have been blocked in a browser or after saving to a disk.
- Over 33% of threats have been blocked after launching malicious software.

	PRE	POST	FAIL	TOTAL
JANUARY	66%	33%	1%	99%
MARCH	76,49%	23,22%	0,29%	99,71%
MAY	76,49%	23,35%	0,16%	99,84%
JULY	84,58%	15,33%	0,09%	99,91%
SEPTEMBER	7,83%	92,27%	-	100%
NOVEMBER	92%	8%	-	100%
AVERAGE	67,23%	33,52%	-	99,74%

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.

6 x

PARTICIPATION IN TEST 6/6

Bitdefender®

Bitdefender Total Security

The software to protect workstation has participated in one edition of the test. It has blocked 1922/1922 malware samples which result in a maximum score of 100% protection against threats in the wild.

- Over 99% of threats have been blocked in a browser or after saving to a disk.
- About 1% of threats have been blocked after launching malicious software.

	PRE	POST	FAIL	TOTAL
JANUARY	-	-	-	-
MARCH	-	-	-	-
MAY	99,84%	0,16%	-	100%
JULY	-	-		-
SEPTEMBER	-	-	-	-
NOVEMBER	-	-	-	-
AVERAGE	99,84	0,16	-	100%

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.

1 ×

PARTICIPATION IN TEST 1/6

ESET
Smart Security Premium

The software to protect workstation has participated in two editions of the test. It has blocked 2322/2322 malware samples which result in a maximum score of 100% protection against threats in the wild.

- Over 96% of threats have been blocked in a browser or after saving to a disk.
- Over 3% of threats have been blocked after launching malicious software.

2 x

PARTICIPATION IN TEST 2/6

ADVANCED IN-THE-WILD MALWARE TEST
AVLAB CYBERSECURITY FOUNDATION
EXCELLENT
NOVEMBER 2022

	PRE	POST	FAIL	TOTAL
JANUARY	-	-	-	-
MARCH	-	-	-	-
MAY	100%	-	-	100%
JULY	-	-		-
SEPTEMBER	-	-	-	-
NOVEMBER	93%	7%	-	100%
AVERAGE	96,5%	3,5%	-	100%

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.

F-Secure

F-SECURE Total

The software to protect workstation has participated in one edition of the test. It has blocked 1824/1824 malware samples which result in a maximum score of 100% protection against threats in the wild.

- Over 97% of threats have been blocked in a browser or after saving to a disk.
- About 3% of threats have been blocked after launching malicious software.

	PRE	POST	FAIL	TOTAL
JANUARY	97%	3%	-	100%
MARCH	-	-	-	-
MAY	-	-	-	-
JULY	-	-		-
SEPTEMBER	-	-	-	-
NOVEMBER	-	-	-	-
AVERAGE	97%	3%	-	100%

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.

1 ×

PARTICIPATION IN TEST 1/6

G DATA
Total Security

The software to protect workstation has participated in one edition of the test. It has blocked 2182/2182 malware samples which result in a maximum score of 100% protection against threats in the wild.

- Over 99% of threats have been blocked in a browser or after saving to a disk.
- Almost 1% of threats have been blocked after launching malicious software.

1 ×

PARTICIPATION IN TEST 1/6

	PRE	POST	FAIL	TOTAL
JANUARY	-	-	-	-
MARCH	-	-	-	-
MAY	-	-	-	-
JULY	99,95%	0,05%		100%
SEPTEMBER	-	-	-	-
NOVEMBER	-	-	-	-
AVERAGE	99,95%	0,05%	-	100%

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.

kaspersky

KASPERSKY Total Security

The software to protect workstation has participated in one edition of the test. It has blocked 400/400 malware samples which result in a maximum score of 100% protection against threats in the wild.

- Over 94% of threats have been blocked in a browser or after saving to a disk.
- More than 5% of threats have been blocked after launching malicious software.

1 ×

PARTICIPATION IN TEST 1/6

	PRE	POST	FAIL	TOTAL
JANUARY	-	-	-	-
MARCH	-	-	-	-
MAY	-	-	-	-
JULY	-	-		-
SEPTEMBER	-	-	-	-
NOVEMBER	94,5%	5,5%	-	100%
AVERAGE	94,5%	5,5%	-	100%

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.

Malwarebytes

MALWAREBYTES Endpoint Protection

Software to protect workstations took part in three editions of the test. It has blocked 100% threats in-the-wild.

- Over 32% threats have been blocked in a browser or just after saving a file to a hard drive at the Pre-Launch level.
- Over 67% threats have been blocked after launching malicious software at the Post-Launch level.

	PRE	POST	FAIL	TOTAL
JANUARY	-	-	-	-
MARCH	-	-	-	-
MAY	-	-	-	-
JULY	8,01%	91,99%		100%
SEPTEMBER	2,06%	97,94%	-	100%
NOVEMBER	88,75%	11,25%	-	100%
AVERAGE	32,94%	67,06%	-	100%

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.

3 ×

PARTICIPATION IN TEST 3/6

Malwarebytes

MALWAREBYTES Premium

Software to protect workstations took part in all editions of the test. It has blocked 99,9% threats in-the-wild.

- Over 20% threats have been blocked in a browser or just after saving a file to a hard drive at the Pre-Launch level.
- Over 79% threats have been blocked after launching malicious software at the Post-Launch level.

	PRE	POST	FAIL	TOTAL
JANUARY	-	99,9%	0,1%	99,9%
MARCH	3,37%	96.63%	-	100%
MAY	4,39%	95,61%	-	100%
JULY	4,39%	95,61%	-	100%
SEPTEMBER	1,3%	98,7%	-	100%
NOVEMBER	90,75%	9,25%	-	100%
AVERAGE	20,84%	79,81%	0,1%	99,9%

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.

6 ×

PARTICIPATION IN TEST 6/6

Microsoft Defender

The software to protect workstation has participated in five editions of the test. It has blocked over 95% threats in the wild.

- More than 3% of threats have been blocked in a browser or after saving to a disk.
- Over 92% of threats have been blocked after launching malicious software.

	PRE	POST	FAIL	TOTAL
JANUARY	-	78%	22%	78%
MARCH	-	-	-	-
MAY	-	98,6%	1,4%	98,6%
JULY	2,79%	97,21%	-	100%
SEPTEMBER	-	100%	-	100%
NOVEMBER	13,75%	86,25%	-	100%
AVERAGE	3,30%	92,01%	-	95,32%

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.

4 ×

PARTICIPATION IN TEST 5/6

1 ×

mks_vir

MKS_VIR
Endpoint Security

The software to protect workstation has participated in three editions of the test. It has blocked 100% malware samples which result in a maximum score of protection against threats in the wild.

- More than 99% of threats have been blocked in a browser or after saving to a disk.
- Almost 1% of threats have been blocked after launching malicious software.

3 ×

PARTICIPATION IN TEST 3/6

	PRE	POST	FAIL	TOTAL
JANUARY	-	-	-	-
MARCH	-	-	-	-
MAY	100%	-	-	100%
JULY	100%	-		100%
SEPTEMBER	99,86%	0,14%	-	100%
NOVEMBER	-	-	-	-
AVERAGE	99,95%	0,5%	-	100%

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.

TREND MICRO

TREND MICRO
Maximum Security

Oprogramowanie do ochrony stacji roboczej uczestniczyło w jednej edycji testu. Zablokowało 2081 z 2081 próbek malware, co daje maksymalny wynik 100% zatrzymanych zagrożeń in-the-wild.

- Ponad 98% zagrożeń zablokowało już w przeglądarce albo tuż po zapisaniu na dysk na poziomie Pre-launch.

	PRE	POST	FAIL	TOTAL
JANUARY	-	-	-	-
MARCH	-	-	-	-
MAY	-	-	-	-
JULY	-	-	-	-
SEPTEMBER	98,85%	-	0,15%	99,85%
NOVEMBER	-	-	-	-
AVERAGE	98,85%	-	0,15%	99,85%

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.

1 ×

PARTICIPATION IN TEST 1/6

WEBROOT SecureAnywhere®

WEBROOT Antivirus

The software to protect workstation has participated in all editions of the test. It has blocked 99,96% threats in the wild.

- More than 62% of threats have been blocked in a browser or after saving to a disk.
- Over 37% of threats have been blocked after launching malicious software.

6 x

PARTICIPATION IN TEST 6/6

	PRE	POST	FAIL	TOTAL
JANUARY	73%	26,9%	0,1%	99,9%
MARCH	64,88%	35,17%	0,05	99,95%
MAY	68,93%	31,01%	0,06%	99,94%
JULY	73,63%	26,36%	0,01	99,99%
SEPTEMBER	50%	50%	-	100%
NOVEMBER	42%	58%	-	100%
AVERAGE	62,07%	37,91%	-	99,96%

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.

AVLAB
CYBERSECURITY FOUNDATION

As an independent organization we are committed to protect privacy and security on the Internet. 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 cyber security. Our strongest asset are 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 popular testing laboratories..

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