Recent Results in November 2025

LATEST DATA FROM THE ADVANCED IN-THE-WILD MALWARE TEST

Summary of **November 2025**

14
TESTED
SOLUTIONS

244
UNIQUE
SAMPLES

214
MALWARE HOSTED OVER HTTP

30
MALWARE HOSTED OVER HTTPS

153

AVERAGE MALICIOUS CHANGES [1]

PRE-LAUNCH LEVEL PREVENTION **89%**

POST-LAUNCH LEVEL PROTECTION **10%**

AVERAGE BLOCKED MALWARE [2] **99%**

POTENTIAL DATA BREACHES **2**

14s

AVERAGE INDUSTRY
REMEDIATION TIME

* based on data telemetry

0s

THE QUICKEST AVERAGE REMEDIATION TIME

Bitdefender

ESET

[1] The number of harmful changes made to Windows during dynamic analysis of the malware sample.
[2] Average blocking of malware by all tested solutions, regardless of level of prevention or protection.

Remember! HTTPS protocol can be used to host malware! SSL certificate and the so-called padlock at the web address does not certify safety of the website.

TOP 3

HIJACKED SERVERS LOCATION

63

58

23

TOP 3

TLD COMPROMISED DOMAINS

.com

22

.dev

6

.sbs

4

Examples illustrating the blocking of malware in the test

LOLBins in statistical terms

Legitimate and trusted software and built-in components in Windows are often used by cybercriminals to hide malicious activity. The so-called “Living off the Land Binaries” (LOLBin) are necessary for the proper functioning of the operating system. During a cyberattack, it can be difficult or impossible to block them, making them a very attractive method for malware developers. Below we present the most commonly used LOLBin in this edition of the test.

DOWNLOAD LOLBINS OVERVIEW

svchost.exe
5443

msedge.exe
4443

certutil.exe
3044

explorer.exe
1908

sh.exe
1878

taskhostw.exe
1143

Malware Comparison Table in **November 2025**

The following summary shows a comparison of tested solutions to protect workstations against malware. We encourage you to become familiar with a detailed description and read our testing methodology in order to understand the results.

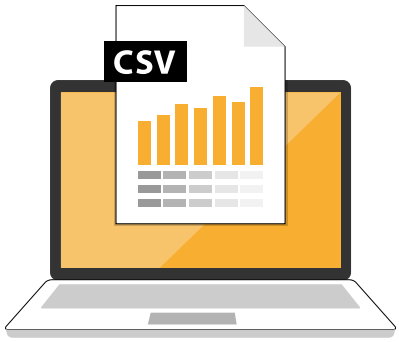
PRE-LAUNCH: The classification concerns detecting malware samples before they are launched in the system.
POST-LAUNCH: The analysis level, i.e. a virus has been run and blocked by a tested product.
FAIL: The failure, i.e. a virus hasn't been blocked and it has infected a system.
Sandbox Column: Number of indicators, i.e. malicious changes made to the system without the anti-virus installed.

Automatic Average Remediation Time (RT): The time expressed in seconds counted from the introduction of malware into the system by the browser, through the launch to the detecting and resolving a security incident.

Certificates are granted to solutions that are characterized by a high level of security, with a

rating of at least 99% of blocked threats in the Advanced In-The-Wild Malware Test.

Our tests comply with the guidelines of the Anti-Malware Testing Standards Organization. Details about the test are available at this website as well as in our methodology.



DOWNLOAD COMPARISON TABLE

Recent Results in **November 2025**

ENTERPRISE PRODUCTS

EXCELLENT

Emsisoft Enterprise Security + EDR

PRE-LAUNCH:

85.25%

POST-LAUNCH:

14.75%

Blocked: **244/244**
Total: **100%**
RT: **1.752 seconds**

EXCELLENT

mks_vir

mks_vir Endpoint Security + EDR

PRE-LAUNCH:

97.95%

POST-LAUNCH:

2.05%

Blocked: **244/244**
Total: **100%**
RT: **9.3 seconds**

EXCELLENT

ThreatDown Powered by Malwarebytes

ThreatDown Endpoint Protection + EDR

PRE-LAUNCH:

98.77%

POST-LAUNCH:

1.23%

Blocked: **244/244**
Total: **100%**
RT: **8.013 seconds**

EXCELLENT

WatchGuard

WatchGuard Endpoint Security

PRE-LAUNCH:

94.26%

POST-LAUNCH:

4.92%

FAIL:

0.82%

Blocked: **222/224**
Total: **99.18%**
RT: **32.6 seconds**
FAIL: 2

HOME PRODUCTS

EXCELLENT

Avast

Avast Free Antivirus

PRE-LAUNCH:

98.36%

POST-LAUNCH:

1.64%

Blocked: **244/244**
Total: **100%**
RT: **8.094 seconds**

EXCELLENT

Bitdefender

Bitdefender Total Security

PRE-LAUNCH:

100%

POST-LAUNCH:

0%

Blocked: **244/244**
Total: **100%**
RT: **0 seconds**

EXCELLENT

Eset Smart Security

PRE-LAUNCH:

95.71%

POST-LAUNCH:

4.29%

Blocked: **244/244**
Total: **100%**
RT: **0 seconds**

EXCELLENT

F-Secure Total

PRE-LAUNCH:

13.52%

POST-LAUNCH:

86.48%

Blocked:**244/244**
Total: **100%**
RT: **106 seconds**

EXCELLENT

G Data Internet Security

PRE-LAUNCH:

99.59%

POST-LAUNCH:

0.41%

Blocked: **244/244**
Total: **100%**
RT: **0.11 seconds**

EXCELLENT

Malwarebytes

Malwarebytes Premium

PRE-LAUNCH:

99.59%

POST-LAUNCH:

0.41%

Blocked: **244/244**
Total: **100%**
RT: **2.18 seconds**

EXCELLENT

Microsoft Defender

PRE-LAUNCH:

97.95%

POST-LAUNCH:

2.05%

Blocked: **244/244**
Total: **100%**
RT: **1.342 seconds**

EXCELLENT

NortonLifeLock

Norton Antivirus Plus

PRE-LAUNCH:

98.36%

POST-LAUNCH:

1.64%

Blocked: **244/244**
Total: **100%**
RT: **1.657 seconds**

EXCELLENT

Trend Micro Internet Security

PRE-LAUNCH:

98.36%

POST-LAUNCH:

1.64%

Blocked: **244/244**
Total: **100%**
RT: **0.192 seconds**

EXCELLENT

Webroot Antivirus

PRE-LAUNCH:

85.25%

POST-LAUNCH:

14.75%

Blocked: **244/244**
Total: **100%**
RT: **33 seconds**

Related Publication in Details

Dive into our latest publication, dedicated to security test against malware. Uncover analyses, methodology, and results that provide invaluable insights into the latest edition of the Advanced In-The-Wild Malware Test.

READ MORE

Additional Files

- Summary table in a graphical form.
- Download all materials related to the test in the form of convenient ZIP file.

See the previous results

You can always go back in time and check how each individual security product performed during previous editions of the test. We make the results from all previous tests available to you to verify if your favorite developer has improved protection against latest malware in his security software.

The AVLab Cybersecurity Foundation is an independent organization dedicated to protecting privacy and security on the Internet. We are a member of the Anti-Malware Testing Standards Organization and a member of the Microsoft Virus Initiative.

Shortcuts

Our Special Test

Detailed EDR-XDR Solutions Overview 2025, Edition 3rd

Simulate offensive cyberattacks with telemetry event visibility

Award „Product of The Year 2025”

Additional TOP Remediation Time 2025 Certification and Advanced In-The-Wild Malware Test Summary

Newsletter

SIGN UP

FOLLOW US: