**Q2 2022 Google Chrome | Microsoft Edge | Mozilla Firefox**

**Overview**
During Q2, 2022, CyberRatings.org performed an independent test of malware protection offered by popular web browsers running on Windows 10 & 11. The tests ran for 24 days with 96 discrete test runs. To protect against malware, Microsoft Edge uses Microsoft Defender SmartScreen; Google Chrome and Mozilla Firefox use the Google Safe Browsing API.

Microsoft Edge offered the most protection, blocking 97.0% of malware. Google Chrome provided the second-highest protection, blocking an average of 88.4%, followed by Mozilla Firefox at 84.6%.

The ability to warn potential victims that they are about to stray onto a malicious website puts web browsers in a unique position to combat malware. Websites that trick (socially engineer) users to download malware have short lifespans, so it is essential that the site is discovered and added to the reputation system as quickly as possible. This explains the relationship between average-time-to-block and catch-rate.

**Average Time to Block on Windows 10 & 11**

We measured each browser’s ability to block malware as quickly as we found them on the Internet. This continued every six hours to determine how long it would take a vendor to add protection. The average time each browser took to block malware once the threat was introduced into the test cycle was then calculated and recorded.

**Summary of Results**

Attackers’ malware campaigns are constantly changing, with the bulk of new attacks occurring in the first few hours after an attack is launched. URL reputation systems shorten the time attackers have to achieve their goals by preventing/warning users that a URL is a known malware site. Similarly, file reputation systems alert users that a file is known to be malware.
Each browser’s individual block performance was measured continuously. A browser’s overall block rate is calculated as the number of successful blocks divided by the total number of test cases. For example, with tests conducted every 6 hours, a URL that was online for 48 hours will be tested eight (8) times. A browser blocking it on 6 (out of a maximum 8) test runs will achieve a block rate of 75%.

**Malware Protection Over Time on Windows 10**

![Graph showing malware protection over time on Windows 10]

- **Google Chrome**: 88.3%
- **Microsoft Edge**: 96.5%
- **Mozilla Firefox**: 84.6%

**Malware Protection Over Time on Windows 11**

![Graph showing malware protection over time on Windows 11]

- **Google Chrome**: 88.5%
- **Microsoft Edge**: 97.5%
- **Mozilla Firefox**: 84.5%
Malware Attacks

Social engineered malware (SEM) attacks use deceptions to trick users into downloading malware: Hijacked email and social media accounts take advantage of the implicit trust between contacts and deceive victims into believing that links to malicious files are trustworthy. Other deceptions include pop-up messages advising users that applications (such as Adobe Flash Player) need to be installed or warn that a user’s computer is infected, or that it requires an update. Once malware is installed, victims are vulnerable to credential theft, identity theft, bank account compromise, etc.

Web Browsers Protection Against Malware

To protect against malware, cloud-based reputation systems scour the Internet for malicious websites and then categorize content accordingly. Web browsers then ask the cloud-based reputation systems about specific URLs, files, or applications. If results indicate that malware is present, the web browser redirects the user to a warning message explaining that the URL, file, or application is malicious. Some reputation systems also include additional educational content.

Google Chrome and Mozilla Firefox use the Google Safe Browsing API for both URL reputation and application reputation for blocking malicious files. Microsoft Edge uses Microsoft Defender SmartScreen, which provides protection from attacks via a cloud-based reputation service for URL reputation, as well as application reputation for malicious file blocking.

Average Number of Malicious Malware Samples Added Per Day

On average, 41 new validated malware samples were added to the test set per day; numbers varied on some days as criminal activity levels fluctuated.

Test Environment

- Microsoft Windows 10 Pro, 21H1 (OS Build 19044.1766)
- Microsoft Windows 11 Pro 21H1 (OS Build 22000.739)

Total Number of Malicious Samples Tested

28,506 raw, unvalidated samples were tested multiple times with each web browser, over a total of 96 test cycles each, conducted without interruption over 576 hours (every 6 hours for 24 days). Our engineers removed samples that did not pass the validation criteria, including those tainted by exploits (not part of this test). Ultimately, 903 unique, valid malware samples were included in the final set of 120,450 discrete, valid malware tests (20,075 tests per web browser), providing a margin of error of less than 0.91 percent (0.91%) at a confidence level of 99%.

How We Tested – Malware Samples

Data in this report spans a testing period of twenty (20) days between May 28 and June 20, 2022. During the test, CyberRatings engineers routinely monitored connectivity to ensure the browsers under test could access the malware as well as the reputation services in the cloud.

The emphasis was on freshness with new samples constantly being added to the test and dead samples removed.

How We Assessed Results

We measured each browser’s ability to block malware as quickly as they were discovered on the Internet. Engineers repeated these tests every six hours to determine how long it would take a vendor to add protection if they did at all. Each browser’s performance was measured continuously, and the overall block rate of all malware samples tested with the browser was recorded. Each browser’s overall block rate was calculated as the number of successful blocks divided by the total number of test cases. For example, with tests conducted every 6 hours, a malware sample that was online for 48 hours was tested eight (8) times. A browser blocking it on 6 (out of a maximum of 8) test runs achieved a block rate of 75%.

Tested Products

- Google Chrome: Version 100.0.4951.67 - 102.0.5005.285
- Microsoft Edge: Version: 101.0.1210.47- 102.0.1245.44
- Mozilla Firefox: Version 100.0.1 - 101.0.1
WEB BROWSER COMPARATIVE TEST REPORT: MALWARE PROTECTION

Authors

Thomas Skybakmoen, Vikram Phatak

Test Methodology

CyberRatings Web Browser Security Test Methodology v1.0 is available at www.cyberratings.org

Contact Information

CyberRatings.org
2303 Ranch Road 620 South
Suite 160, #501
Austin, TX 78734
info@cyberratings.org
www.cyberratings.org

© 2022 CyberRatings.org. All rights reserved. No part of this publication may be reproduced, copied/scanned, stored on a retrieval system, emailed or otherwise disseminated or transmitted without the express written consent of CyberRatings.org. (“us” or “we”).

1. The information in this report is subject to change by us without notice, and we disclaim any obligation to update it.

2. The information in this report is believed by us to be accurate and reliable at the time of publication, but is not guaranteed. All use of and reliance on this report are at your sole risk. We are not liable or responsible for any damages, losses, or expenses of any nature whatsoever arising from any error or omission in this report.

3. NO WARRANTIES, EXPRESS OR IMPLIED ARE GIVEN BY US. ALL IMPLIED WARRANTIES, INCLUDING IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT, ARE HEREBY DISCLAIMED AND EXCLUDED BY US. IN NO EVENT SHALL WE BE LIABLE FOR ANY DIRECT, CONSEQUENTIAL, INCIDENTAL, PUNITIVE, EXEMPLARY, OR INDIRECT DAMAGES, OR FOR ANY LOSS OF PROFIT, REVENUE, DATA, COMPUTER PROGRAMS, OR OTHER ASSETS, EVEN IF ADVISED OF THE POSSIBILITY THEREOF.

4. This report does not constitute an endorsement, recommendation, or guarantee of any of the products (hardware or software) tested or the hardware and/or software used in testing the products. The testing does not guarantee that there are no errors or defects in the products or that the products will meet your expectations, requirements, needs, or specifications, or that they will operate without interruption.

5. This report does not imply any endorsement, sponsorship, affiliation, or verification by or with any organizations mentioned in this report.

6. All trademarks, service marks, and trade names used in this report are the trademarks, service marks, and trade names of their respective owners.