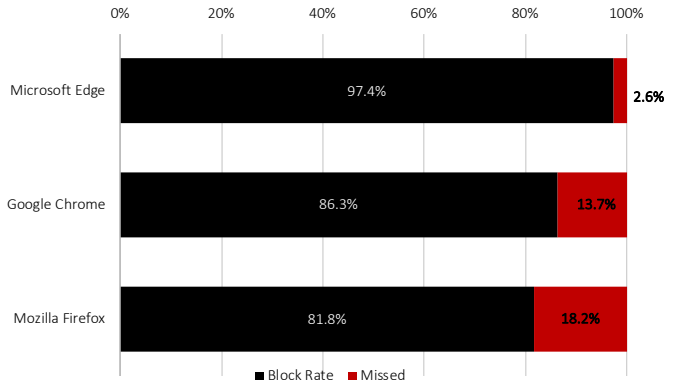
Q2 2021 Web Browsers vs. Malware

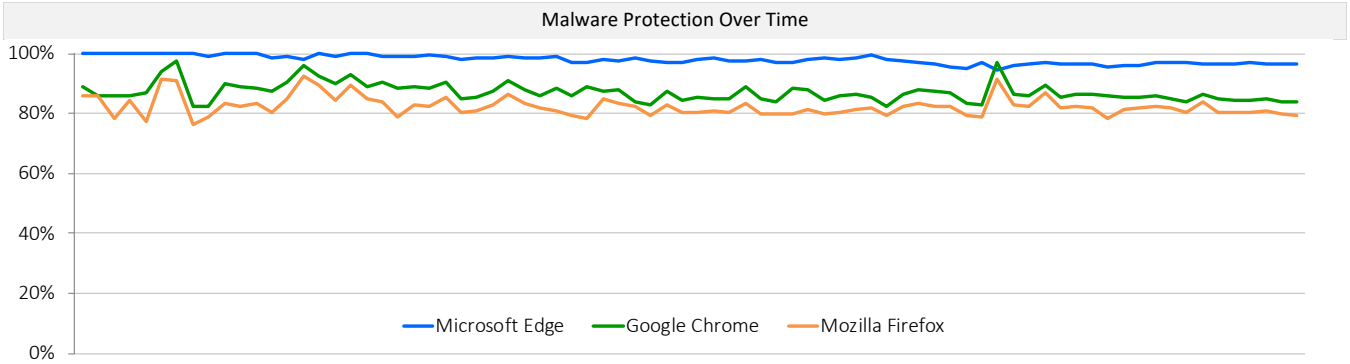
Overview

During Q2, 2021, CyberRatings.org performed an independent test of malware protection offered by web browsers. The tests ran for 20 days with 80 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 97.4% of malware while providing the highest zero-hour protection rate (97.7%). Google Chrome provided the second-highest protection, blocking an average of 86.3%, followed by Mozilla Firefox at 81.8%.

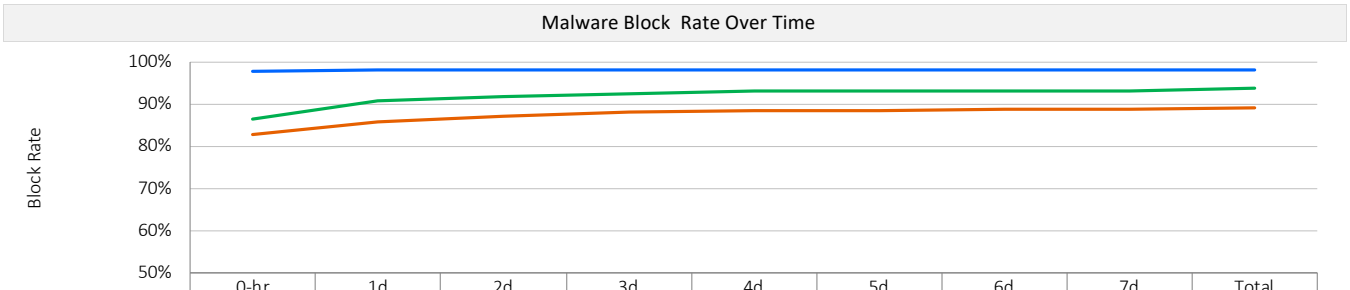


Summary of Results

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. As such, a good reputation system must be both accurate and fast to realize high catch rates.



Throughout the test, new malware was constantly added. URLs that were either no longer reachable or hosting malware were removed. Each data point is calculated from measurements recorded at a specific point in time. If the malware was blocked early on, the browser's score protection over time improved. Alternatively, if the browser did not block the malware, the score decreased.



	0-hr	1d	2d	3d	4d	5d	6d	7d	Total
Microsoft Edge	97.7%	97.9%	97.9%	97.9%	97.9%	97.9%	97.9%	97.9%	97.9%
Google Chrome	86.4%	90.6%	91.7%	92.5%	92.9%	93.1%	93.1%	93.1%	93.6%
Mozilla Firefox	82.8%	85.9%	87.1%	88.0%	88.3%	88.4%	88.6%	88.7%	89.1%

The figure above shows how long each browser took to block malware once the sample was introduced into the test cycle. The core protection technology within Microsoft Edge is SmartScreen, which provides URL-based protection from attacks via an integrated, cloud-based URL-reputation service, as well as application reputation for malicious file blocking. Google Chrome and Mozilla Firefox use the Google Safe Browsing API for both URL reputation and to block or warn users about downloading certain types of files.

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, 49 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

Total Number of Malicious Samples Tested

18,621 raw, unvalidated samples were tested multiple times with each web browser, over a total of 78 test cycles each, conducted without interruption over 468 hours (every 6 hours for 20 days). Our engineers removed samples that did not pass the validation criteria, including those tainted by exploits (not part of this test). Ultimately, 950 unique, valid malware samples were included in the final set of 48,672 discrete, valid malware tests (16,224 tests per web browser), providing a margin of error of less than 3.2 percent (<3.2%) at a confidence level of 95%.

How We Tested – Malware Samples

Data in this report spans a testing period of twenty (20) days between May 11 and May 31, 2021. 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 90.0.4430.212 - 91.0.4472.19
- Microsoft Edge: Version: 91.0.864.19 - 91.0.864.37
- Mozilla Firefox: Version 88.0.1 - 88.0.1

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