WEB BROWSER SECURITY

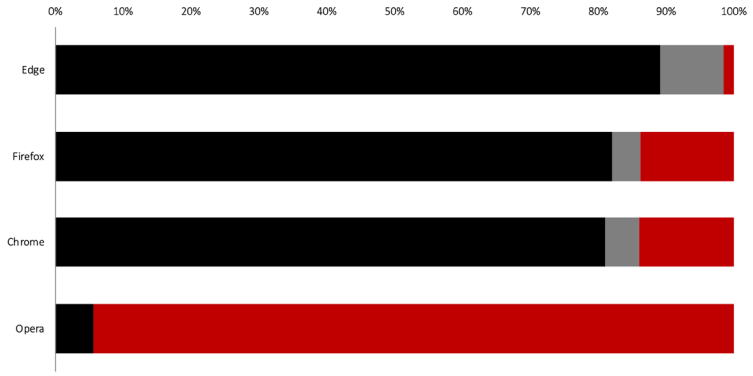
MALWARE PROTECTION 2020

Q2 2020 COMPARATIVE TEST REPORT

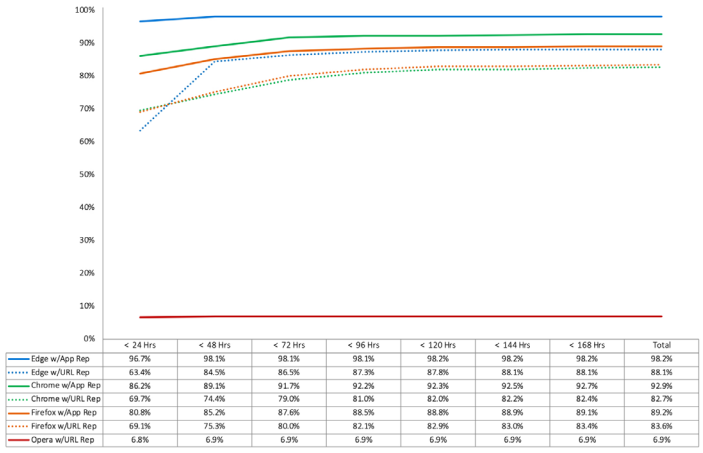
Overview

During Q2, 2020, NSS Labs performed an independent test of malware protection offered by web browsers:. 32,267 discrete tests (per web browser) using 1,065 unique samples over 34 days. To protect against malware, Microsoft Edge uses Microsoft Defender SmartScreen; Google Chrome and Mozilla Firefox use the Google Safe Browsing API; and Opera uses Yandex.

Microsoft Edge offered the most protection, blocking 98.5% of malware, while providing the highest zero-hour protection rate (96.7%). Firefox provided the second highest protection, blocking an average of 86.1%, followed by Google Chrome at 86.0%. Opera blocked 5.6%.



Summary of Results

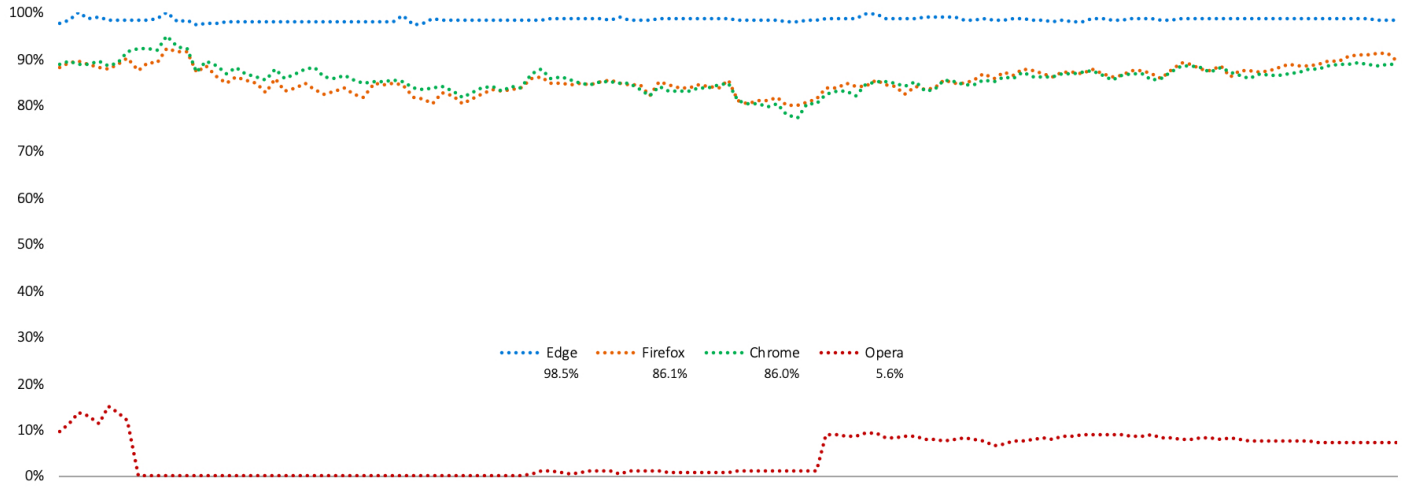


	< 24 Hrs	< 48 Hrs	< 72 Hrs	< 96 Hrs	< 120 Hrs	< 144 Hrs	< 168 Hrs	Total
Edge w/App Rep	96.7%	98.1%	98.1%	98.1%	98.2%	98.2%	98.2%	98.2%
Edge w/URL Rep	63.4%	84.5%	86.5%	87.3%	87.8%	88.1%	88.1%	88.1%
Chrome w/App Rep	86.2%	89.1%	91.7%	92.2%	92.3%	92.5%	92.7%	92.9%
Chrome w/URL Rep	69.7%	74.4%	79.0%	81.0%	82.0%	82.2%	82.4%	82.7%
Firefox w/App Rep	80.8%	85.2%	87.6%	88.5%	88.8%	88.9%	89.1%	89.2%
Firefox w/URL Rep	69.1%	75.3%	80.0%	82.1%	82.9%	83.0%	83.4%	83.6%
Opera w/URL Rep	6.8%	6.9%	6.9%	6.9%	6.9%	6.9%	6.9%	6.9%

Reputation systems shorten the time attackers have to achieve their goals by preventing or warning users that a URL, file, or application is dangerous. However, users are constantly visiting new web sites and downloading files and installing applications. Reputation systems cannot simply block everything that is new. Knowing this, attackers' malware campaigns are constantly changing, and the majority of all attacks occur in the first few hours after a campaign is launched. Therefore, accurately classifying content quickly is key to successful protection.

NSS Labs assessed the browsers' ability to block malware as quickly as we found it on the Internet. We continued testing the malicious URLs, files, and applications every six hours to determine how long it took a vendor to add protection, if they did at all.

Malware Protection Over Time



Throughout the test, new malware was constantly added. URLs, files, and applications 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 for consistency of protection over time improved. Alternatively, if the browser did not block the malware, the score decreased.

Testing was based on the Web Browser Test Methodology v4.0 (available at www.nsslabs.com).

Background

Social engineered malware (SEM) attacks use a dynamic combination of social media, hijacked email accounts, false notification of computer problems, and other deceptions to encourage users to download malware. Cybercriminals use hijacked email accounts to take advantage of the implicit trust between contacts and deceive victims into believing that links to malicious files are trustworthy. Hijacked social media accounts are used in the same way as hijacked email accounts. In the case of social networks, however, the circle becomes wider: friends and even friends of friends risk being deceived.

Social engineering tactics may use pop-up messages; for example, advising users that applications such as Adobe Flash Player need to be installed or that their computers are either infected or require updates. Once malware is installed, victims are vulnerable to identity theft, bank account compromise, and other potentially devastating consequences.

Web Browsers Protection Against Malware

To protect against malware, browsers use cloud-based reputation systems that scour the Internet for malicious websites and then categorize content accordingly, either by adding it to blocklists or whitelists, or by assigning it a score (depending on the vendor's approach).

These categorization techniques can be performed manually or automatically. The second functional component of protection against malware involves the web browser requesting reputation information from the cloud-based reputation systems about specific URLs, files, or applications, and then warning against or blocking the malware.

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. Conversely, if the content is determined to be "good," the web browser takes no action, and the user remains unaware that a security check was just performed by the browser.

Google and Firefox use the Google Safe Browsing API for both URL reputation and to block or warn users about downloading certain types of files. Microsoft Edge uses Microsoft Defender SmartScreen, including the application reputation service to provide protection against phishing and malware threats. Opera uses a combination of blocklists from Netcraft,[1] PhishTank,[2] and Metamask[3] as well as a malware blocklist from Yandex.[4]

In addition, Microsoft Defender SmartScreen was incorporated as an OS-wide feature with the October 2017 Windows 10 update. The operating system version of SmartScreen protection is a backstop for all browsers, email clients, USB, and other applications as part of the OS protection against malware. Therefore, users benefit from the browser URL protection, browser application/file protection, as well as the operating system protection.

Test Composition – Malware Samples

Data in this report spans a testing period of 34 days between April 21, 2020 and May 25, 2020. All testing was performed at the NSS testing facility in Austin, TX. During the test, NSS 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, thus a larger number of samples were evaluated than were ultimately retained as part of the resulting test set, since new samples were constantly being added to the test and dead samples were removed.

Total Number of Malicious Samples Tested

A total of 1,844 raw, unvalidated samples were tested multiple times with each web browser, for a total of 182,676 discrete tests conducted without interruption over 822 hours (every 6 hours for 34 days). NSS engineers removed samples that did not pass the validation criteria, including those tainted by exploits (not part of this test). Ultimately, 1,065 unique, valid malware samples were included in 129,068 discrete, valid malware tests (32,267 per web browser), providing a margin of error of less than 2 percent (<2%) with a confidence level of 95%.

[1] http://www.netcraft.com/

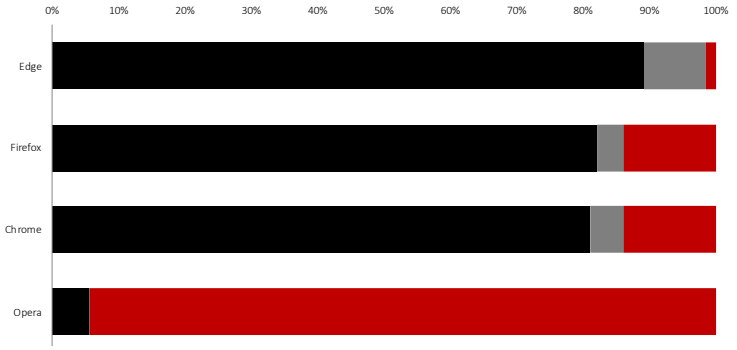
[2] http://www.phishtank.com/

[3] https://github.com/metamask/eth-phishing-detect

[4] https://yandex.com

Malware Block Rate

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 socially engineered malware. Since malware sites have short lifespans, it is essential that the site is discovered, validated, classified, and added to the reputation system as quickly as possible. As such, a good reputation system must be both accurate and fast in order to realize high catch rates. Browser developers clearly understand this relationship, and substantially more malware are blocked in the first 24 hours of detection than thereafter.



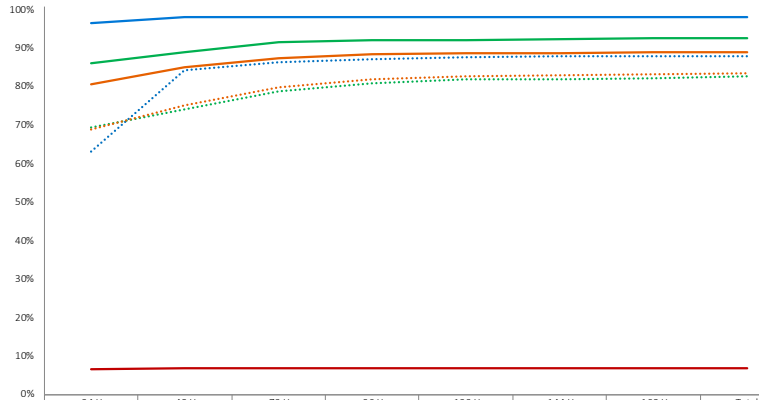
	Opera	Chrome	Firefox	Edge
URL Rep	5.6%	80.9%	82.1%	89.2%
URL + App Rep	0.0%	5.0%	4.0%	9.3%
URL + App + OS Rep	93.1%	13.1%	13.0%	0.7%
Missed	1.4%	0.9%	0.9%	0.8%

The core protection technology within 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. SmartScreen with application reputation blocked 98.5% for Edge. Mozilla Firefox and Google Chrome use the Safe Browsing API. Firefox blocked 86.1%. Google Chrome blocked 86.0%. Opera which uses a combination of blocklists from several sources blocked 5.6%.

In addition, Microsoft Defender SmartScreen blocked an additional 93.1% for Opera; 13.1% for Chrome; 13.0% for Firefox; and 0.7% malicious files for Edge when we attempted to execute them.

Malware Protection Histogram

Immediate protection against new malware is critical. As sites that host malware are discovered they are taken down, often within a relatively short amount of time. Products that fail to add protection in a timely manner may be too late to counter a threat. The histogram shows how long each browser took to block malware once the sample was introduced into the test cycle. Within the seven-day window, cumulative protection rates are calculated each day until threats are blocked.



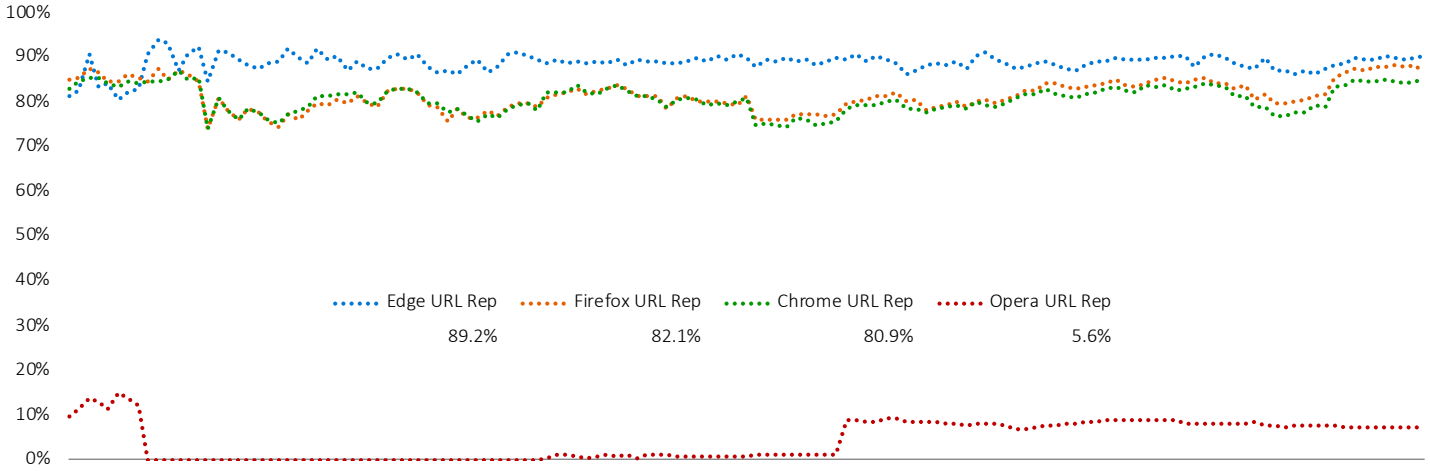
	< 24 Hrs	< 48 Hrs	< 72 Hrs	< 96 Hrs	< 120 Hrs	< 144 Hrs	< 168 Hrs	Total
Edge w/App Rep	96.7%	98.1%	98.1%	98.1%	98.2%	98.2%	98.2%	98.2%
Edge w/URL Rep	63.4%	84.5%	86.5%	87.3%	87.8%	88.1%	88.1%	88.1%
Chrome w/App Rep	86.2%	89.1%	91.7%	92.2%	92.3%	92.5%	92.7%	92.9%
Chrome w/URL Rep	69.7%	74.4%	79.0%	81.0%	82.0%	82.2%	82.4%	82.7%
Firefox w/App Rep	80.8%	85.2%	87.6%	88.5%	88.8%	88.9%	89.1%	89.2%
Firefox w/URL Rep	69.1%	75.3%	80.0%	82.1%	82.9%	83.0%	83.4%	83.6%
Opera w/URL Rep	6.8%	6.9%	6.9%	6.9%	6.9%	6.9%	6.9%	6.9%

During the test, Microsoft Edge demonstrated an initial protection rate of 96.7% against malware. Google Chrome and Mozilla Firefox achieved an initial protection rate of 86.2% and 80.8% respectively. Opera's initial protection rate was 6.8%. By the end of the seventh day of testing, all web browsers saw an increase in protection. Microsoft Edge increased by 4.5% to 98.2%. Google Chrome increased by 6.7% to 92.9%; Mozilla Firefox increased by 8.4% to 89.2%; Opera increased by 0.1% to 6.9%

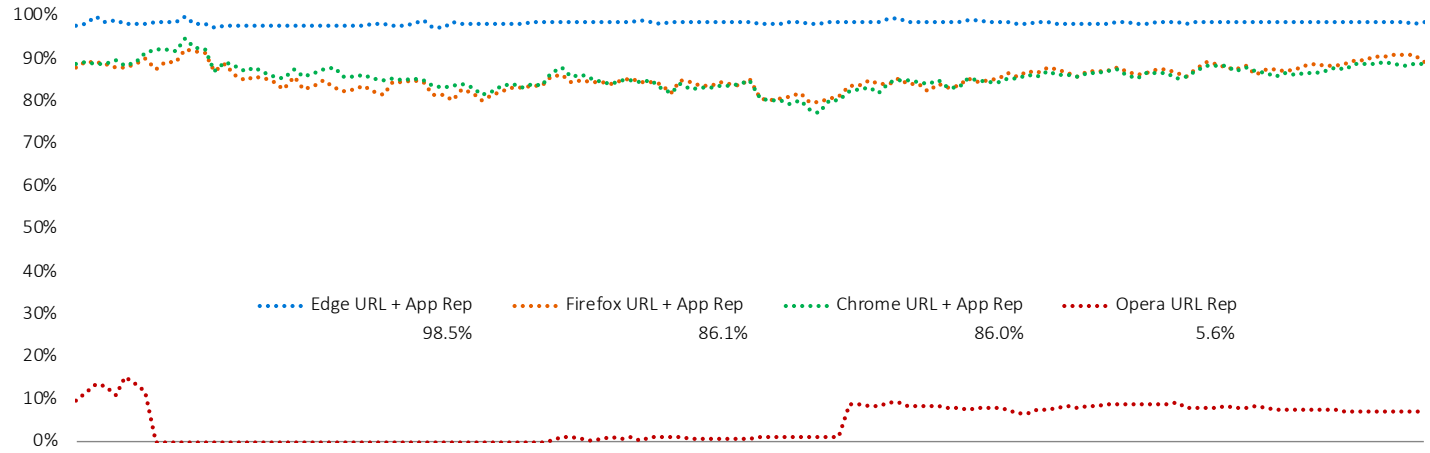
Consistency of Protection Over Time

Throughout the test, new malware was constantly added. URLs, files, and applications 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 for consistency of protection over time improved. Alternatively, if the browser did not block the malware, the score decreased.

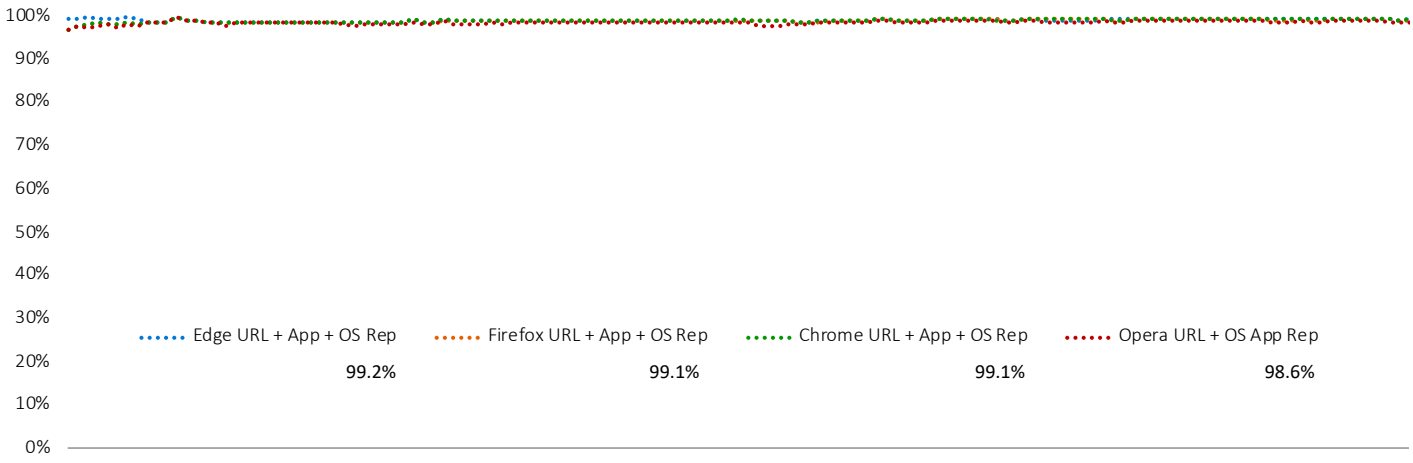
Testing revealed three layers of protection: URL reputation, application reputation in the browser, and OS application reputation. URL reputation offered reasonably good protection.



Layering on application reputation increased protection.



Operating system reputation offered yet additional protection. Ideally the web browser will block malware so that it never reaches the operating system. However, testing indicated that operating system reputation was highly effective.



Test Environment

- BaitNET™ (NSS Labs Proprietary)
- 64-bit Microsoft Windows 10 Pro (version 1909 (Build: 18363.592)
- Ubuntu 18.04.3 LTS
- Kali (Kernel release 4.19.0-kali5-amd64)
- VMware vCenter (Version 6.7u2 Build 6.7.0.30000)
- VMware vSphere (Version 6.7.0.20000)
- VMware ESXi (Version 6.7u3 Build 14320388)
- VMware Tools 10.3.5
- Wireshark version 2.6.3
- WinPcap 4.1.3
- Filezilla Server 0.9.6
- SSH Secure Shell 3.2.9 (Build 283)
- GNU Wget 1.19.4
- Curl 7.58.0

Tested Products

- Google Chrome: Version 81.0.4044.113 – 81.0.4044.138
- Microsoft Edge: Version 83.0.478.10 – 84.0.516.1
- Mozilla Firefox: Version 75.0 – 76.0.1
- Opera: Version: 67.0.3575.137 – 68.0.3618.125

Authors

Dipti Ghimire, Thomas Skybakmoen, Vikram Phatak

Test Methodology

NSS Labs Web Browser Security (WBS) Test Methodology v4.0 is available at www.nsslabs.com.

Contact Information

NSS Labs, Inc.

3711 South Mopac Expressway
Building 1, Suite 400
Austin, TX 78746

info@nsslabs.com

www.nsslabs.com