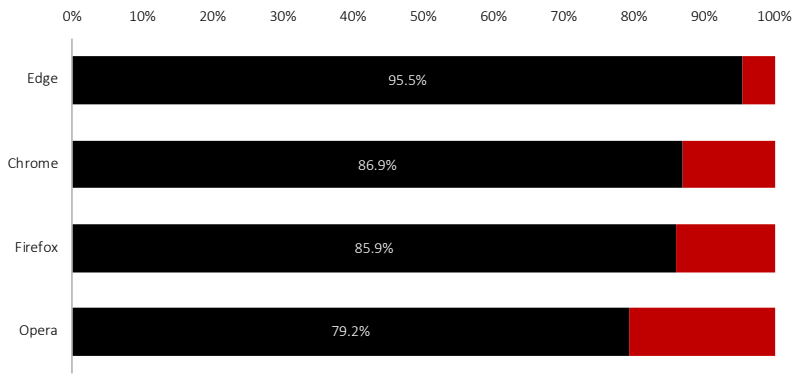
Q2 2020 COMPARATIVE TEST REPORT

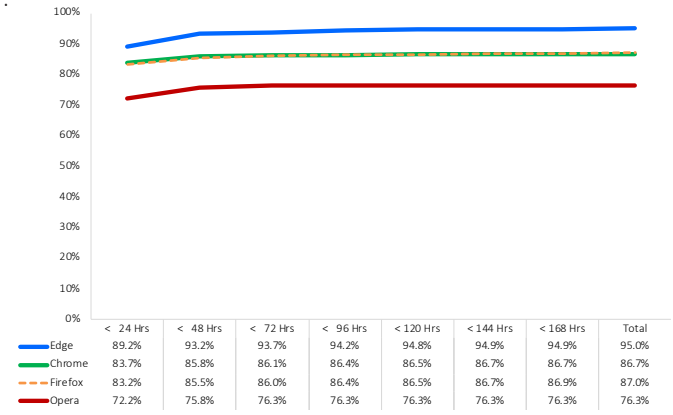
Overview

During Q2, 2020, NSS Labs performed an independent test of phishing protection offered by web browsers: 47,274 discrete tests (per web browser) using 2,443 unique phishing URLs over 18 days. To protect against phishing Microsoft Edge uses Microsoft Defender SmartScreen; Google Chrome and Mozilla Firefox utilize the Google Safe Browsing API; Opera uses a combination of third-party blocklists.

Microsoft Edge offered the most protection, blocking 95.5% of phishing URLs, while providing the highest zero-hour protection rate (89.2%). Google Chrome provided the second highest protection, blocking an average of 86.9%, followed by Mozilla Firefox at 85.9%. Opera blocked 79.2%.



Summary of Results

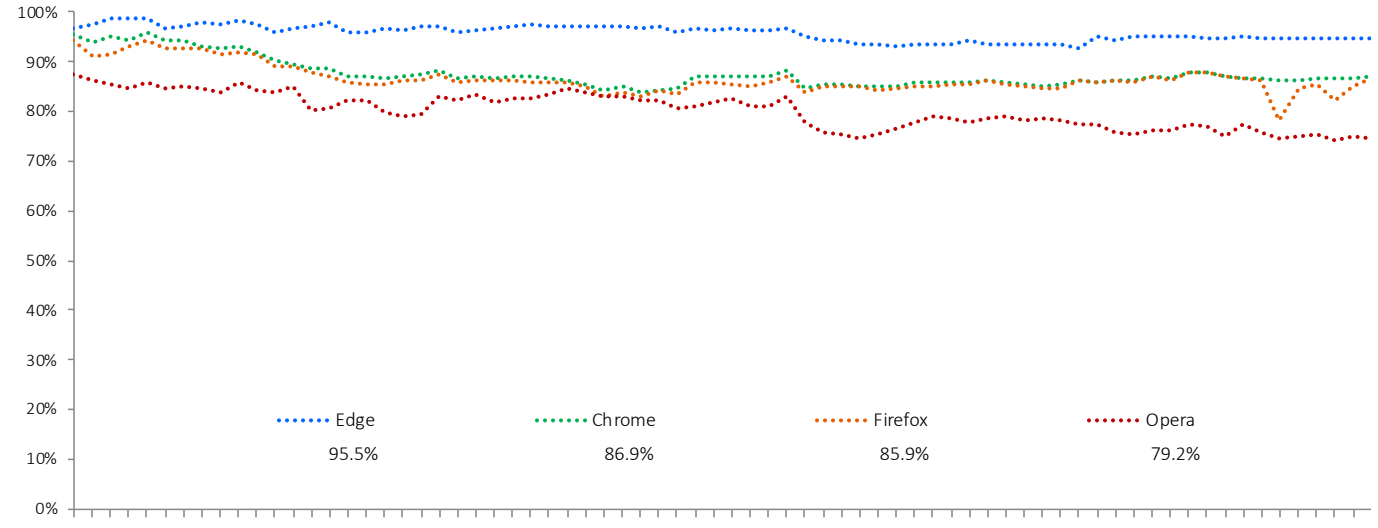


	< 24 Hrs	< 48 Hrs	< 72 Hrs	< 96 Hrs	< 120 Hrs	< 144 Hrs	< 168 Hrs	Total
Edge	89.2%	93.2%	93.7%	94.2%	94.8%	94.9%	94.9%	95.0%
Chrome	83.7%	85.8%	86.1%	86.4%	86.5%	86.7%	86.7%	86.7%
Firefox	83.2%	85.5%	86.0%	86.4%	86.5%	86.7%	86.9%	87.0%
Opera	72.2%	75.8%	76.3%	76.3%	76.3%	76.3%	76.3%	76.3%

URL reputation systems shorten the time attackers have to achieve their goals by preventing/warning users that a URL is a known phishing site. However, since users visit a wide range of web sites, many of which are new, URL reputation systems cannot simply block all new URLs. Knowing this, attackers' phishing campaigns are constantly changing, with the bulk of new attacks occurring in the first few hours after an attack is launched.

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

Phishing Protection Over Time



Throughout the test, new phishing URLs were added daily, and URLs that were either no longer reachable or no longer delivering phishing attacks were removed. Each data point represents protection at a specific point in time. If a URL was blocked early on, the browser's score for consistency of protection over time improved. Alternatively, if the browser did not block the URL, the score decreased.

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

Background

Phishing is a type of social engineering attack that attempts to persuade a victim to provide sensitive personal information to the attacker. Some examples of sensitive information are credit card numbers, social security numbers, and login information and passwords for bank accounts. Email, instant messages, SMS messages, and links on social networking sites are all vectors for phishing attacks. Often, the landing page for a phishing website also attempts to silently exploit a visitor's computer and install a malicious software (aka drive-by exploit).

Phishing attacks pose significant risk to individuals and organizations alike by threatening to compromise or acquire sensitive personal and corporate information. The Anti-Phishing Working Group (APWG) reported a total of 165,772 unique email phishing campaigns in the first quarter of 2020.[1] Phishing attacks are becoming increasingly complex and sophisticated, making them harder to detect and more difficult to prevent.

Web Browsers Protection Against Phishing

Phishing protection is provided by an application within the web browser that requests a URL's reputation from a reputation server in the cloud. The reputation server scours the Internet to find phishing websites, and then assigns each URL a score and adds it to a blocklist. That way, when a web browser is instructed to visit a URL, the browser's phishing protection (i.e. Safe Browsing, SmartScreen, etc.) requests the reputation of the URL from the cloud-based reputation server and if results say that a website is "bad," the web browser redirects the user to a warning message that explains that the URL is malicious. Some reputation systems also include additional educational content. Conversely, if a website 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.

Test Composition – Phishing URLs

Data in this report spans a testing period of 18 days between April 21, 2020 and May 8, 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 phishing URLs as well as browser reputation services in the cloud.

The emphasis was on freshness, thus a larger number of sites were evaluated than were ultimately retained as part of the resulting test set, since new URLs were constantly being added to the test and dead sites were being removed.

Total Number of Malicious URLs In the Test

A total of 4,020 raw, unvalidated URLs were tested multiple times with each web browser, for a total of 222,527 discrete tests conducted without interruption over 430 hours (every 6 hours for 18 days). NSS engineers removed samples that did not pass the validation criteria, including those tainted by exploits (not part of this test). Ultimately, 2,443 unique, valid phishing URLs were included in 189,096 discrete, valid phishing tests (47,274 per web browser), providing a margin of error of less than 2 percent (<2%) with a confidence level of 95%.

Average Number of Malicious URLs Added Per Day

On average, 136 new validated URLs were added to the test set per day; numbers varied on some days as criminal activity levels fluctuated.

Blocking Phishing URLs

NSS assessed browser abilities to block malicious URLs as quickly as they were discovered on the Internet. Engineers repeated these tests every six hours to determine how long it took a vendor to add protection, if they did at all.

The new Microsoft Edge is based on Chromium and was released on January 15, 2020. It is compatible with all supported versions of Windows and macOS. Downloading the browser will replace the legacy version of Microsoft Edge on Windows 10 PCs.

https://support.microsoft.com/en-us/help/4501095/download-the-new-microsoft-edge-based-on-chromium

[1] APWG Phishing Activity Trends Report

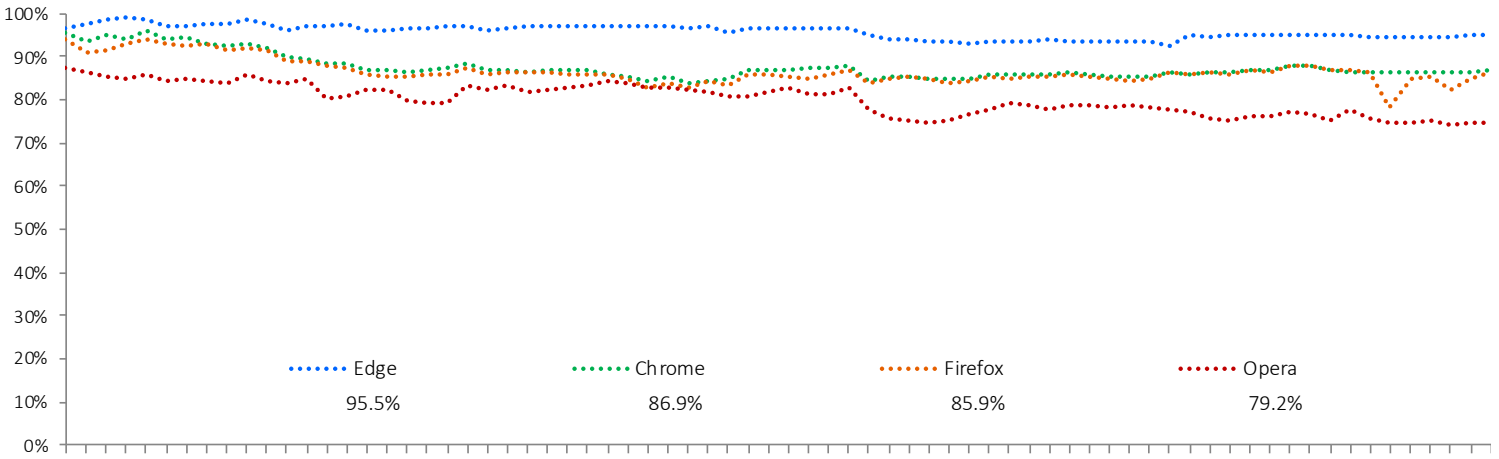
Phishing Block Rate

Google Chrome and Mozilla Firefox use Google's Safe Browsing API. Microsoft Edge uses Microsoft Defender SmartScreen, including the application reputation service, to provide protection against phishing and malware threats. Opera uses a combination of blocklist from Netcraft,[2] PhishTank,[3] and Metamask[4] as well as a malware blocklist from Yandex.[5]

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 phishing and other criminal activities. Since phishing sites have a short lifespan, it is essential that the site is discovered, validated, classified, and added to the reputation system as quickly as possible. This explains the correlation between average-time-to-block and catch-rate. 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 phishing sites are blocked in the first 24 hours of detection than thereafter.

Each browser's individual block performance was measured continuously, and the overall block rate of all URLs tested by browser was recorded. 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 8 times. A browser blocking it on 6 (out of a maximum 8) test runs will achieve a block rate of 75%.

Consistency of Protection Over Time



Throughout the test, new phishing URLs were added daily, and URLs that were either no longer reachable or no longer delivering phishing URLs were removed. Each data point represents protection at a specific point in time. If a URL was blocked early on, the browser's score for consistency of protection over time improved. Alternatively, if the browser did not block the URL, the score decreased.

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

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

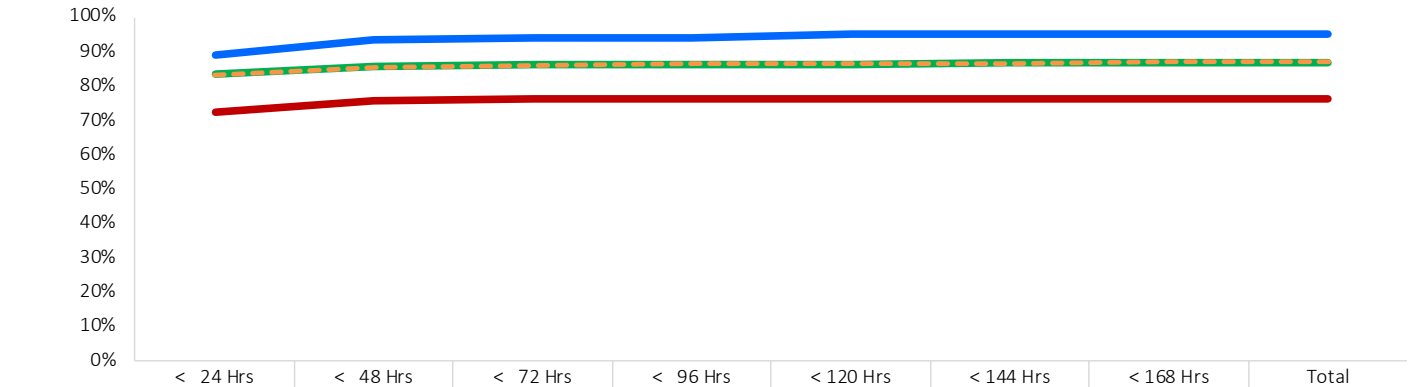
[4] https://github.com/metamask/eth-phishing-detect

[5] https://yandex.com

Phishing Protection Histogram

Immediate protection against new phishing URLs is critical. As phishing sites are discovered, they are taken down, and 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 below shows how long each browser took to block a phishing site once the threat was introduced into the test cycle. Within the seven-day window, cumulative protection rates are calculated each day until threats are blocked.

During the test, Microsoft Edge demonstrated an initial protection rate of 89.2% against phishing attacks. Google Chrome and Mozilla Firefox achieved an initial protection rate of 83.7% and 83.2% respectively. Opera's initial protection rate was 72.2%. By the end of the seventh day of testing, all web browsers saw an increase in protection. Microsoft Edge increased by 5.7% to 94.9%. Mozilla Firefox increased by 3.7% to 86.9%; Google Chrome increased by 3% to 86.7%. Opera increased by 4.1% to 76.3%



	< 24 Hrs	< 48 Hrs	< 72 Hrs	< 96 Hrs	< 120 Hrs	< 144 Hrs	< 168 Hrs	Total
Edge	89.2%	93.2%	93.7%	94.2%	94.8%	94.9%	94.9%	95.0%
Chrome	83.7%	85.8%	86.1%	86.4%	86.5%	86.7%	86.7%	86.7%
Firefox	83.2%	85.5%	86.0%	86.4%	86.5%	86.7%	86.9%	87.0%
Opera	72.2%	75.8%	76.3%	76.3%	76.3%	76.3%	76.3%	76.3%

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 – 84.0.502.0
- 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