WEB BROWSER SECURITY COMPARATIVE REPORT

Phishing Protection

NOVEMBER 1, 2016

Authors – Jayendra Pathak, Thomas Skybakmoen, Morgan Dhanraj

Tested Products[1]

Google Chrome: Version 53.0.2785

Microsoft Edge 38.14393.0.0

Mozilla Firefox: Version 48.0.2

Environment

Windows 10 Enterprise – Version 1607

Phishing Protection Test Methodology v3.0

[1] Each product was updated to the most current version available at the time testing began, and the product versions were frozen to maintain the integrity of the test. However, for the duration of the test, protection against SEM and phishing remained the same across all available browser versions.

Overview

The results presented in this report were obtained from continuous, live testing between October 1st, 2016 and October 12th, 2016 at the NSS facility in Austin, Texas. This test was conducted free of charge, and NSS did not receive any compensation in return for vendor participation.

This Comparative Report is based on empirically validated evidence gathered by NSS during 12 days of continuous testing. Testing was performed every six hours for a total of 44 discrete test runs, with each test cycle adding new phishing URLs.

Among the most prominent and impactful security threats facing users today are socially engineered malware (SEM) and phishing attacks. As such, they have been the primary focus of NSS' continued research and testing of the security effectiveness of browsers. While drive-by downloads and clickjacking are also effective attacks that have achieved much publicity, they still represent a smaller percentage of today's threats.[2] [3]

Figure 1 depicts the average block rate for phishing.

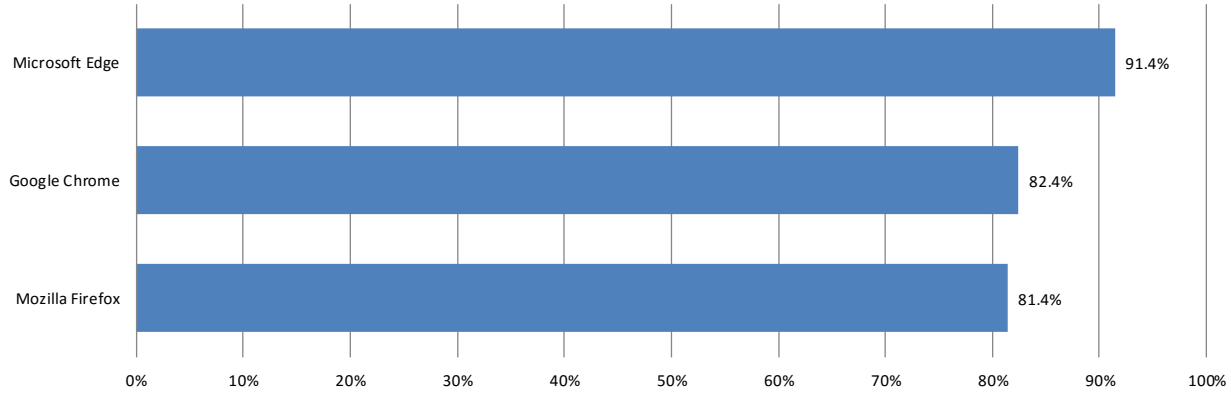


Figure 1 – Average Block Rate

The average phishing URL catch rate for browsers over the entire 12-day test period ranged from 91.4% for Microsoft Edge to 81.4% for Mozilla Firefox.

[2] https://securelist.com/analysis/kaspersky-security-bulletin/73038/kaspersky-security-bulletin-2015-overall-statistics-for-2015/

[3] https://securelist.com/analysis/quarterly-malware-reports/75640/it-threat-evolution-in-q2-2016-statistics/

NSS Labs Findings

- Zero-hour protection rates can vary by as much as 9.4%: thefore, the time required to add protection for a new phishing site is an important factor in browser selection
- The average time to block phishing attacks varied by as much as one hour between the tested browsers.
- Phishing protection is only one security attribute of a browser. SEM-blocking capabilities must also be factored into any overall assessment of browser security.

NSS Labs Recommendations

- When considering browser security, users should minimize risk by selecting browsers with higher phishing block rates, consistency of protection, and early protection against new threats.
- Augment browser protection with education to protect against the attacks that do bypass the browsers.
- Include the ability to block socially engineered malware during browser selection.

Table of Contents

Table of Figures

Analysis

Long before the Greeks hid a group of soldiers in a wooden gift horse (Trojan horse), social engineering was a popular tool for con artists and other criminals deceiving people for their own personal gain. Phishing is the natural application of modern technology to social engineering by criminals perpetrating this proven attack strategy. Web browsers are in a unique position to combat phishing and other criminal activities by warning potential victims that they are about to stray onto a malicious website. 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.

In this report, NSS studied the leading web browsers' ability to protect against phishing. In a companion report, NSS reports the findings of the protection capabilities of web browsers against socially engineered malware (see: the Web Browser Security Comparative Report: Socially Engineered Malware Protection).

The Phishing Threat

"Phishing" attacks can be constructed in two basic ways. The first is an attempt to persuade a victim to provide personal information to the attacker. The information may be credit card details, login information for email or social media accounts, or other personal information that can be used for identity theft and other information-based attacks. The second type of phishing attack attempts to lure users into installing a malicious application or navigating to a website where malicious software will be installed through the exploitation of vulnerable software. Common to both phishing attacks is that they arrive via email, instant messages, SMS messages, and links on social networking sites.

Phishing attacks pose a significant risk to individuals and organizations alike, by threatening to compromise or acquire sensitive personal and corporate information. In 2016, an average of 145,581 unique email phishing campaigns were reported each month, and 125,906 unique phishing websites were detected each month—which is the highest ever recorded.[4] Phishing attacks are becoming increasingly complex and sophisticated, making these attacks harder to detect and more difficult to prevent.

[4] http://docs.apwg.org/reports/apwg_trends_report_q2_2016.pdf

Web Browser Security

The evolution of the browser can be compared to the evolution of antivirus software. Where antivirus software once only detected self-replicating threats, then Trojans, and eventually a myriad of types of threats, browsers initially dealt with annoyances such as pop-ups and cookies and then were required to tackle more serious security issues. Phishing websites are among the top threats that the browser must protect against. This report examines the abilities of three different web browsers to protect users from live phishing attacks.

The foundation of browser phishing protection is the cloud-based, reputation-based system that scours the Internet for malicious websites and then categorizes content accordingly, either by adding to a black or white list, or by assigning a score (depending on the vendor's approach.) These techniques may be performed manually, automatically, or by using a combination of the two approaches. The second functional component resides within the web browser and requests reputation information from the cloud-based systems about specific URLs, then enforces warning and blocking functions.

When results are returned which indicate that a site is "bad," the web browser redirects the user to a warning message explaining that the URL is malicious. Some programs include additional educational content as well. Conversely, when a website is determined to be "good," the web browser takes no action and the user is unaware that a security check was just performed by the browser.

Test Composition – Phishing URLs

Data in this report spans a testing period of 12 days from October 1st, 2016 through October 12th, 2016. All testing was performed at the NSS testing facility in Austin, TX. During the test, NSS engineers routinely monitored connectivity to ensure the browsers could access the Internet sites being tested, as well as their reputation services in the cloud.

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

Total Number of Malicious URLs in The Test

Throughout this test, 78,921 results were collected from 44 discrete tests conducted without interruption over 360 hours (every 6 hours for 12 days). NSS engineers removed samples that did not pass the validation criteria, including those tainted by exploits (which were not part of this test.) Ultimately, 991 unique URLs were included in NSS' final set of phishing sites.

Average Number of Malicious URLs Added Per Day

On average, 90 new validated URLs were added to the test set per day; numbers varied on some days as criminal activity levels fluctuated.

Mixture of URLs

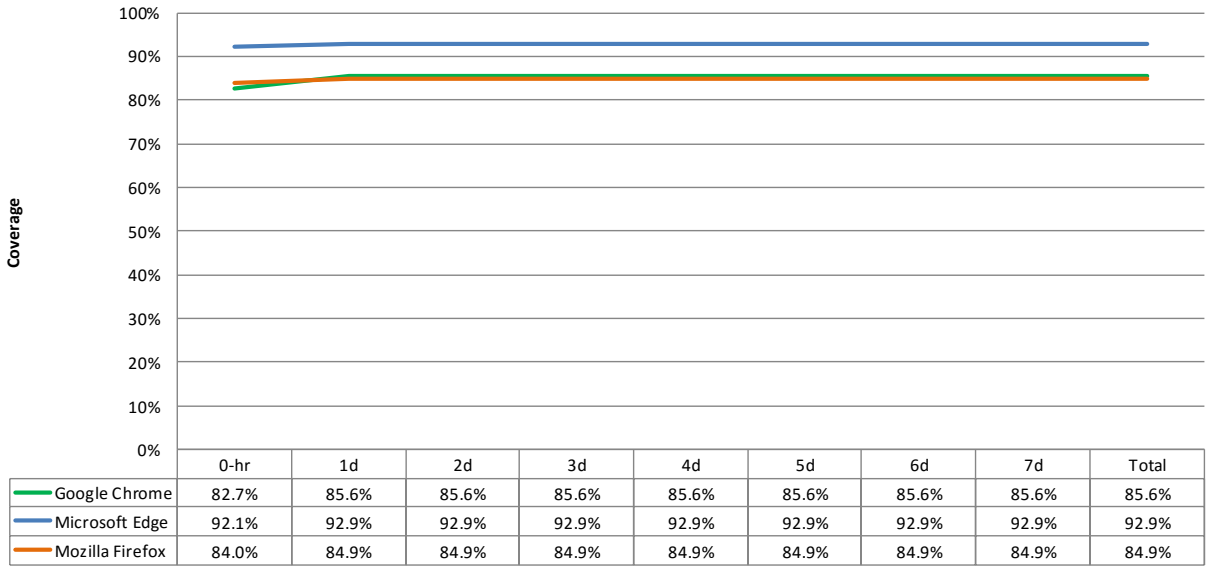
The mixture of URLs used in the test was representative of current threats on the Internet.

Blocking Phishing URLs

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

Average Time to Block Phishing URLs

Figure 2 depicts how long it took the browsers to block a threat once it was introduced into the test cycle. Cumulative protection rates are listed at the time of introduction, i.e., the "zero hour," through the end of the test. Final protection scores for the duration of the URL test are summarized under the "Total" column.



	0-hr	1d	2d	3d	4d	5d	6d	7d	Total
Google Chrome	82.7%	85.6%	85.6%	85.6%	85.6%	85.6%	85.6%	85.6%	85.6%
Microsoft Edge	92.1%	92.9%	92.9%	92.9%	92.9%	92.9%	92.9%	92.9%	92.9%
Mozilla Firefox	84.0%	84.9%	84.9%	84.9%	84.9%	84.9%	84.9%	84.9%	84.9%

Figure 2 – Phishing URL Response Histogram

Initial protection from phishing sites ranged from 82.7% for Google Chrome to 92.1% for Microsoft Edge. Since both Google Chrome and Mozilla Firefox rely on the Google Safe Browsing API, their protection is almost identical.

Average Response Time to Block Phishing

Figure 3 answers the question of how long a user must wait on average until a requested phishing URL is added to a block list. It shows the average time to block a phishing site once it was introduced into the test set, but only if it was blocked during the the test. Unblocked sites are not included, as there is no mathematically empirical way to score "never."

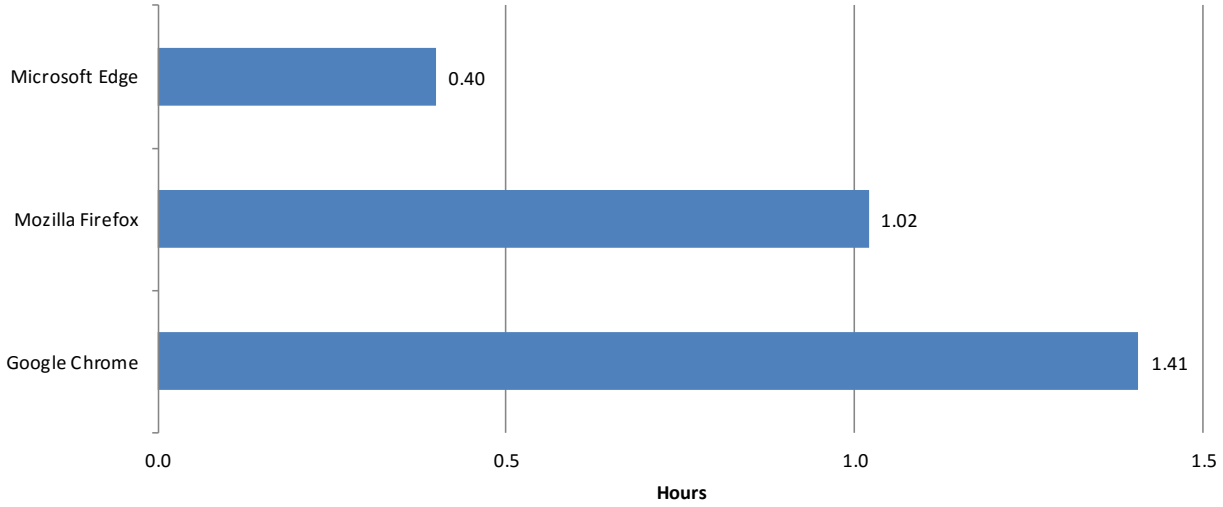


Figure 3 – Average Time to Block (shorter time is better)

The average time to block a site (if it is blocked at all) is 56.4 minutes. Microsoft Edge was significantly faster at adding protection in the earliest hours of a phishing attack than any of the other browsers. Google Chrome and Mozilla Firefox took more than one hour on average to block new phishing websites.

Real-time Blocking of Phishing URLs Over Time

The metrics for blocking individual URLs represent just one perspective. For daily usage scenarios, users are visiting a wide range of sites that may change quickly. At any given time, the available set of phishing URLs is evolving, and continuing to block these sites is a key criterion for effectiveness. NSS tested a set of live URLs every six hours.

Note that the protection percentage will deviate from the unique URL results for several reasons. First, this data includes multiple tests of a URL, so if it is blocked early on, it will improve the score. If it continues to be missed, however, it will detract from the score. Results of individual URL tests were compounded over time.

Figure 4 shows protection at each of the 44 incremental tests of over a period of 12 days, and each score represents protection at a given point in time.

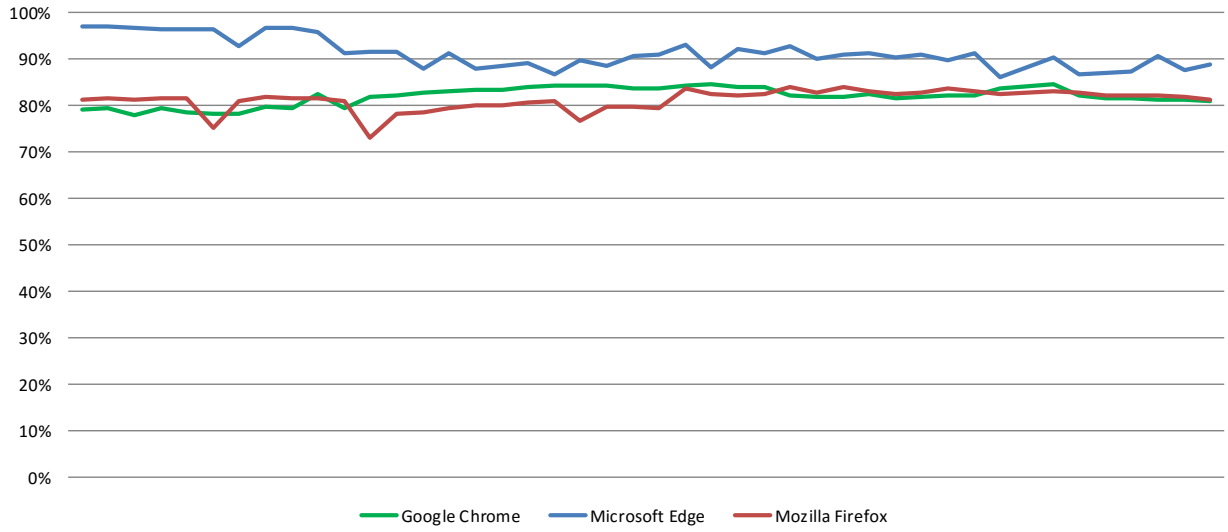


Figure 4 – Phishing Protection Over Time

Google Chrome and Mozilla Firefox use the Google Safe Browsing API. The mean detection rates for these browsers is very close; however, Chrome lags behind Firefox in early protection.

Test Methodology

Web Browser Security: Phishing Protection Test Methodology v3.0

A copy of the test methodology is available on the NSS Labs website at www.nsslabs.com.

Contact Information

NSS Labs, Inc.
206 Wild Basin Road
Building A, Suite 200
Austin, TX 78746
info@nsslabs.com
www.nsslabs.com