WEB BROWSER SECURITY COMPARATIVE REPORT

Protection Against Socially Engineered Malware

NOVEMBER 16, 2018

Author – Morgan Dhanraj

Tested Products[1]

Google Chrome: Version 69.0.3497

Microsoft Edge: Version 42.17134.1.0

Mozilla Firefox: Version 61

Environment

Windows 10 Enterprise Version 1803

NSS Labs Web Browser Security Test Methodology v4.0

[1] At the start of testing, each product was updated to the most current version available and given access to the Internet for the duration of the test. The product version reflects the most up-to-date version that was available at the end of the test.

Overview

The web browser is the primary vector by which malware is introduced to computers. Links in phishing emails, compromised web sites, and Trojanized "free" software downloads all deliver malware via web browser downloads. The web browser is also the first line of defense against malware infection, which emphasizes the importance of choosing a browser that provides a strong layer of defense against malware, rather than relying on third-party anti-malware solutions. With the October 2017 Windows 10 update, Windows Defender SmartScreen Application Reputation (App Rep) technology (which previously was available with the Microsoft Edge browser) became available exclusively as an OS-wide feature, providing malware protection to all browsers.

The technologies are key in protecting all Windows 10 users against malware that is delivered via social engineering. A browser in combination with Windows Defender SmartScreen Application Reputation technology constitutes a protection stack. Both SmartScreen and Application Reputation protection are available for third-party browsers as well as email clients as part of the protection stack against malware that relies on social engineering to compromise targets.

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 continue to represent a smaller percentage of today's threats.[2] [3]

The results presented in this report were obtained from continuous live testing between September 6, 2018 and September 19, 2018 at the NSS Labs facility in Austin, Texas. During testing, all browsers were subjected to the same set of SEM. This test was conducted free of charge, and NSS did not receive any compensation in return for vendor participation. Figure 1 depicts the effectiveness of the security stack against SEM throughout the test.

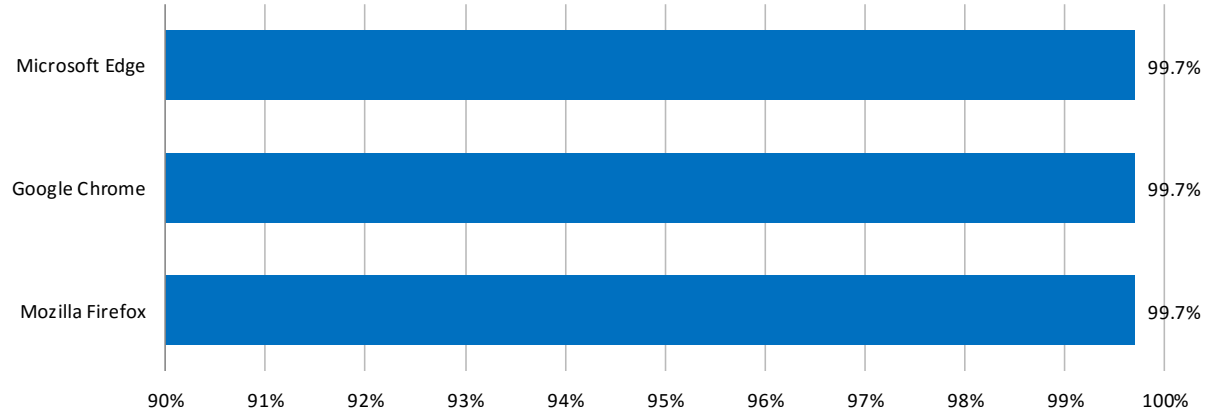


Figure 1 –Effectiveness of Security Stack against SEM (%)

During the test, Microsoft Edge, Google Chrome, and Mozilla Firefox blocked an average of 99.7% of the SEM samples they were tested against.

[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

- Windows Defender SmartScreen provided an extra layer of security for non-Microsoft browsers in the event that the attack was missed natively by non-Microsoft browsers.
- Windows Defender SmartScreen contributed between 9.6% – 19.5% to the security efficacy score of the non-Microsoft browsers.
- With the standard protection offered on Windows 10, all tested browsers exhibited similar zero-hour protection rates for malware.

NSS Labs Recommendations

- Learn to identify social engineering attacks in order to maximize your protection against SEM and other socially engineered attacks.
- When considering browser security, users should minimize risk by selecting the right combination of OS and browser.
- Enterprises must ensure that Windows Defender SmartScreen is not disabled by their existing endpoint solutions.

Table of Contents

Table of Figures

Analysis

For several years, the use of social engineering has accounted for the bulk of cyberattacks against consumers and enterprises. 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 optimizing or updates to Windows. Once malware is installed, victims are vulnerable to identity theft, bank account compromise, and other potentially devastating consequences.

To protect against SEM, browsers utilize cloud-based reputation systems that scour the Internet for malicious websites and then categorize content accordingly, either by adding it to blacklists or whitelists, or by assigning it a score (depending on the vendor's approach). These categorization techniques may be performed manually and/or automatically. The second functional component of protection against SEM involves the web browser requesting reputation information from the cloud-based reputation systems about specific URLs, and then warning against or blocking specific URLs.

If results indicate that a website 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, 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.

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

Test Composition

The test was run between September 6, 2018 and September 19, 2018 and comprised 81,729 test cases that included 1,196 unique suspicious samples. Ultimately, 708 samples met NSS' validation criteria and were included as part of the test.

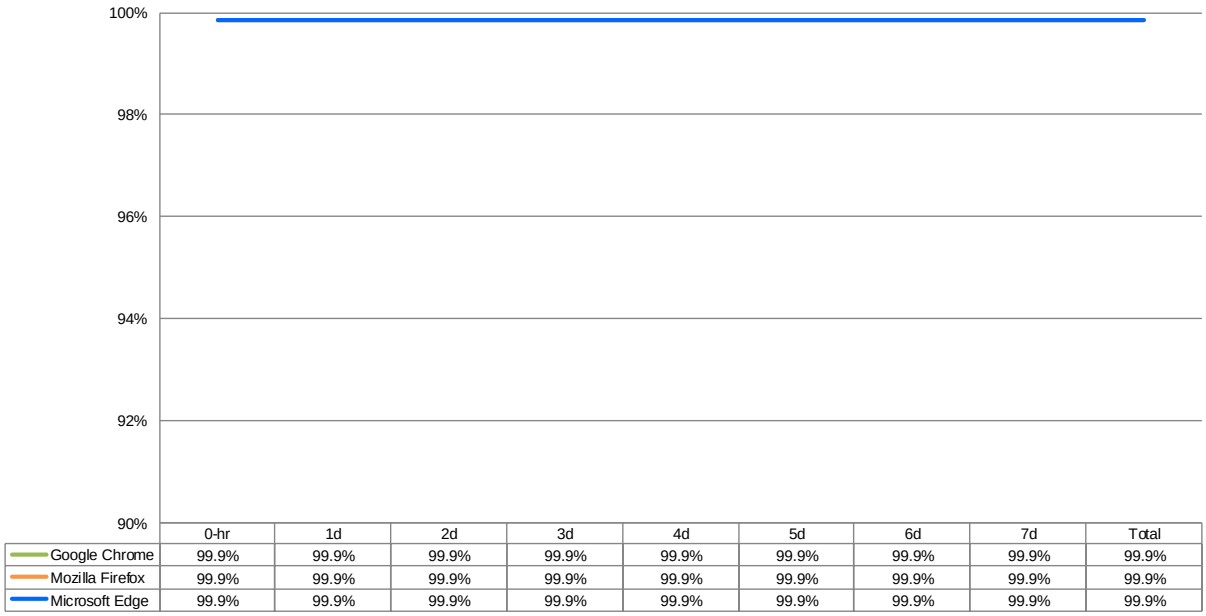
Testing was repeated every six hours on each target URL until the URL was no longer active. Samples that did not pass the validation criteria were removed, including false positives and adware.

Protection Metrics

The average block rate for SEM is a key metric against which browsers are tested. Consistency of protection, the amount of time required to add protection for new threats, and zero-day protection are also important metrics, and thus are included in this report.

Zero-Hour Protection

Immediate protection against new threats is critical. As sites that host SEM 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. Figure 2 shows how long each browser took to block a threat once the threat was introduced into the test cycle. Within the seven-day window, cumulative protection rates are calculated daily until threats are blocked.



	0-hr	1d	2d	3d	4d	5d	6d	7d	Total
Google Chrome	99.9%	99.9%	99.9%	99.9%	99.9%	99.9%	99.9%	99.9%	99.9%
Mozilla Firefox	99.9%	99.9%	99.9%	99.9%	99.9%	99.9%	99.9%	99.9%	99.9%
Microsoft Edge	99.9%	99.9%	99.9%	99.9%	99.9%	99.9%	99.9%	99.9%	99.9%

Figure 2 – Zero-Hour Stack Protection

During the test, all browsers exhibited the same zero-hour protection due to the standard protection provided by the Windows 10 operating system.

Weighted Protection Score

Once the time to add protection is known, NSS can better represent a web browser's protection against SEM by assigning a greater value (or weighting) to those browsers adding protection more quickly than those browsers adding protection more slowly. By applying this weighting to the protection score over the seven-day period, the zero-hour protection of a browser can be more accurately depicted. Figure 3 depicts the weighted protection score for each browser.

Time to Protect	Microsoft Edge	Google Chrome	Mozilla Firefox
0-hour	99.9%	99.9%	99.9%
1 day	99.9%	99.9%	99.9%
2 days	99.9%	99.9%	99.9%
3 days	99.9%	99.9%	99.9%
4 days	99.9%	99.9%	99.9%
5 days	99.9%	99.9%	99.9%
6 days	99.9%	99.9%	99.9%
7 days	99.9%	99.9%	99.9%
Protection Score	**99.9%**	**99.9%**	**99.9%**

Figure 3 – Weighted Stack Protection Score

Consistency of Protection Over Time

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

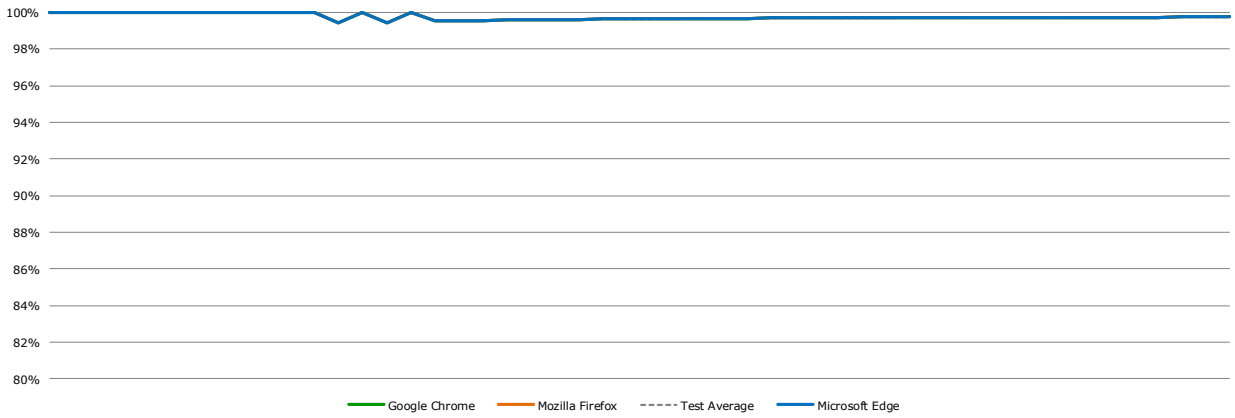


Figure 4 – Consistency of Protection Over Time

Observation and Analysis

Both Microsoft and Google have invested significantly in cloud-based reputation technology. With the October 2017 Windows 10 update, Windows Defender SmartScreen Application Reputation technology (which previously was available with the Microsoft Edge browser) became available exclusively as an OS-wide feature, providing malware protection to all browsers. The technology is a key component in protecting all Windows 10 users against malware that is delivered via social engineering.

As Figure 5 shows, Windows Defender SmartScreen technology increases browser security efficacy scores by 9.7% – 19.5%. Windows Defender SmartScreen can be accessed using the "Run" or "Open" Button available on different browsers as well as if the file is executed from the file system via Windows Explorer.

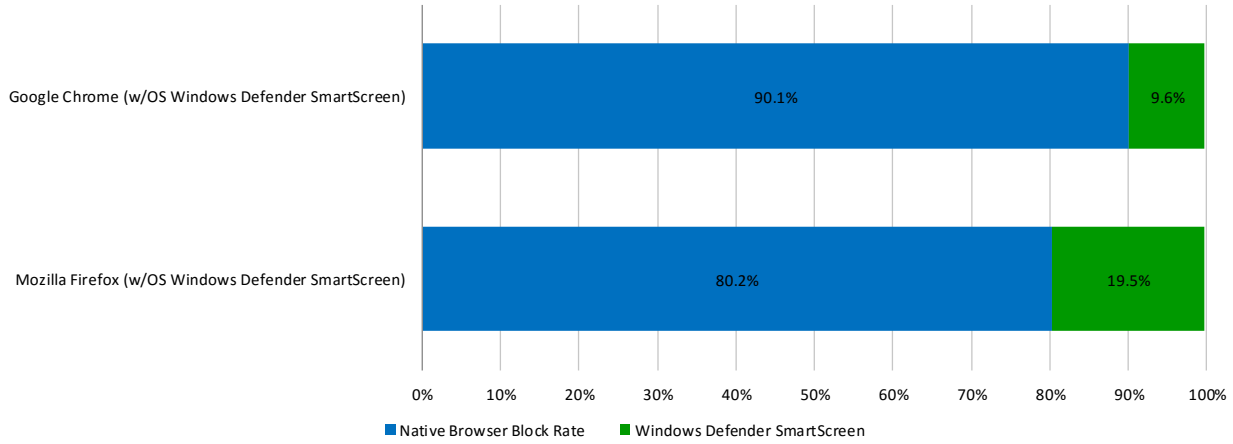


Figure 5 – Native Browser and Windows Defender SmartScreen Block Rate

Initially, the Google Safe Browsing API[4] only protected against drive-by downloads and phishing sites, but the increase in socially engineered malware prompted Google to add protection against SEM, which improved Google Chrome's block rate compared to previous NSS browser tests. Mozilla Firefox also relies upon Google's Safe Browsing API; however, the difference in protection scores indicates that the two browsers implement the technology differently.

Education Is a Component of Protection Against SEM

Users who are able to identify social engineering attacks rely less on technology for protection against such attacks. Technology will sometimes fail, but those users who can identify social engineering attacks will remain protected, regardless of the method used to attempt social engineering.

[4] Google Chrome and Mozilla Firefox use the same Google Safe Browsing API.

Test Methodology

Web Browser Security Test Methodology v4.0

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

Contact Information

NSS Labs, Inc.
3711 South MoPac Expressway
Building 1, Suite 400
Austin, TX 78746-8022
USA
info@nsslabs.com
www.nsslabs.com