WEB BROWSER SECURITY COMPARATIVE REPORT

Socially Engineered Malware Protection

NOVEMBER 1, 2016

Authors – Jayendra Pathak, Thomas Skybakmoen

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

Socially Engineered Malware 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 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 a browser that provides a strong layer of defense from malware, rather than relying upon third-party anti-malware solutions. 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].

The results presented in this report were obtained from continuous live testing between September 26th, 2016 and October 9th, 2016 at the NSS Labs facility in Austin, Texas. During testing, all browsers were subjected to the same set of social malware. This test comprised 220,918 test cases that included 5,224 unique suspicious samples. Ultimately, 304 samples met NSS validation criteria and were included as part of the test. This test was conducted free of charge, and NSS did not receive any compensation in return for vendor participation.

Figure 1 depicts the percentage of SEM samples blocked throughout the test.

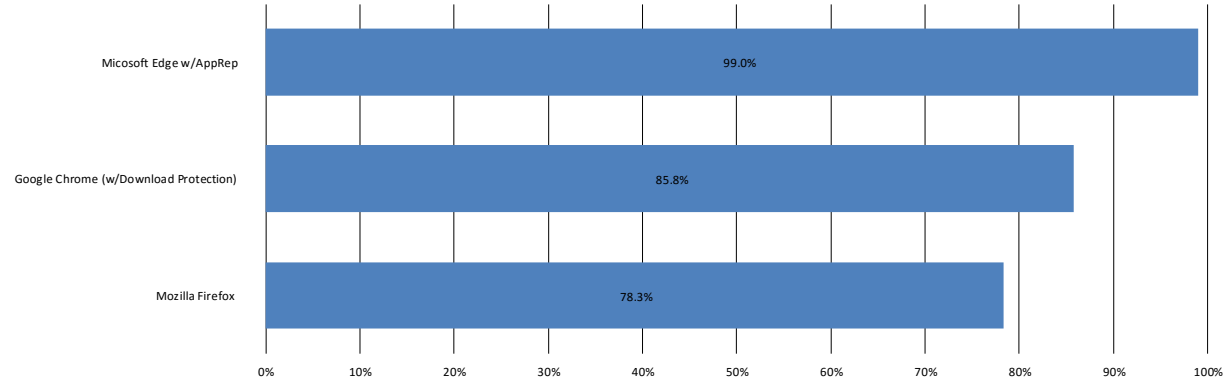


Figure 1 – Average Block Rate for SEM

The Microsoft Edge browser blocked 99.0% of the SEM samples. Microsoft Edge provides malware protection by using a combination of SmartScreen URL filtering and Application Reputation (App Rep), a technology that requires no knowledge of whether an application is harmful or benign. Google Chrome blocked 85.8% of the SEM samples; Google Chrome uses URL filtering and an application reputation system called Download Protection. Mozilla Firefox blocked 78.3% of the SEM samples; Mozilla Firefox also uses URL filtering and Download Protection.

[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

- Microsoft Edge provided the highest SEM protection in the test, blocking as much as 99.0% of SEM and matching several endpoint protection (EPP) products that have been tested by NSS for SEM protection[4].
- Both Microsoft's App Rep and Google's Download Protection are content-agnostic malware protection (CAMP) technologies.[5]
- Mozilla Firefox has begun incorporating download protection into the web browser, which is why its block rate has improved compared to its performance in previous NSS browser tests.

NSS Labs Recommendations

- Learn to identify social engineering attacks in order to maximize protection against SEM and other socially engineered attacks.
- Enterprises should review current NSS reports when selecting browsers. Do not assume the browser market is static.
- When considering browser security, users should minimize risk by selecting browsers with higher malware block rates, consistency of protection, and early protection against new threats.

[4] Enterprise EPP Comparative Report: Security Stack – Socially Engineered Malware. NSS Labs

[5] Microsoft Takes Scammers to CAMP. NSS Labs

Table of Contents

Environment **1**

Overview **2**

NSS Labs Findings **3**

NSS Labs Recommendations **3**

Analysis **5**

Test Composition *5*

Protection Metrics *5*

Zero-Hour Protection 6

Average Time to Block 7

Google Safe Browsing API vs Microsoft Smart Screen for SEM Protection 7

Consistency of Protection over Time 8

Education Is a Component of SEM Protection 8

Test Methodology **9**

Contact Information **9**

Table of Figures

Figure 1 – Average Block Rate for SEM 2

Figure 2 – SEM URL Response Histogram 6

Figure 3 – Average Time to Block 7

Figure 4 – Google Safe Browsing API vs Microsoft Smart Screen 7

Figure 5 – SEM Protection over Time 8

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 factors such as social media, hijacked email accounts, false notification of computer problems, and other deceptions to encourage users to download the 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.

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 attackse (see: the Web Browser Security Comparative Report: Phishing Protection).

Test Composition

The test was run between September 26th, 2016 and October 9th, 2016. More than 220,900 test cases were used in the data sampling captured via NSS' unique live testing harness. Of an initial sample set of 5,224 unique and suspicious URLs entered into the system, 304 URLs were found active and malicious and met the criteria for inclusion in this test. In total, 53 individual test runs were performed by the browsers against these unique 5,224 URLs, which resulted in more than 16,000 test cases per browser.

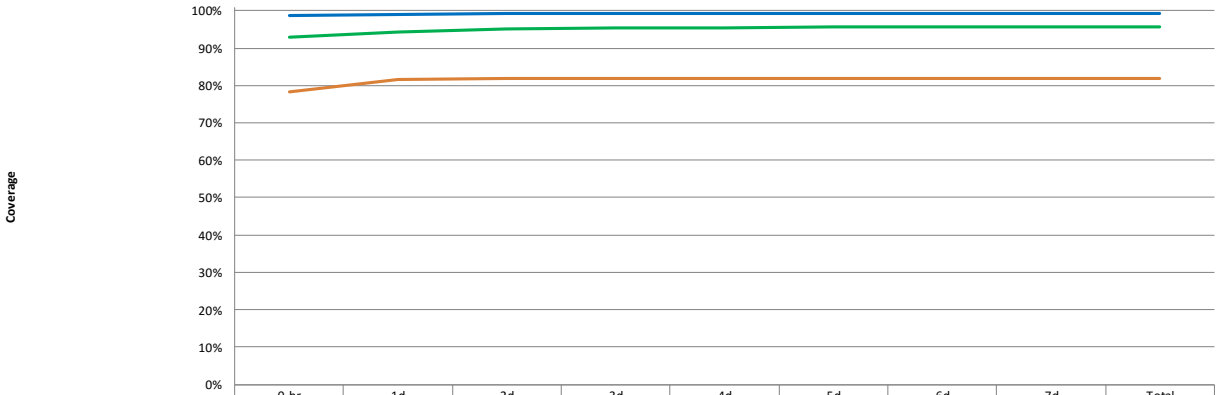
Testing was repeated every six hours until the target URL was no longer active. Samples that did not pass the validation criteria were removed, including false positives and adware.

Protection Metrics

The average SEM block rate 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 they 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, often within a relatively short amount of time. Products that fail to add protection in a timely manner may be too late to counter the threat. Figure 2 shows how long each browser took to block a threat once the threat was introduced into the test cycle. Cumulative protection rates are calculated each day until threats are blocked.



	0-hr	1d	2d	3d	4d	5d	6d	7d	Total
Firefox	78.3%	81.6%	81.9%	81.9%	81.9%	81.9%	81.9%	81.9%	81.9%
Microsoft Edge	98.7%	99.0%	99.3%	99.3%	99.3%	99.3%	99.3%	99.3%	99.3%
Chrome (w/Download Protection)	92.8%	94.4%	95.1%	95.4%	95.4%	95.7%	95.7%	95.7%	95.7%

Figure 2 – SEM URL Response Histogram

During the test, Microsoft Edge demonstrated a 98.7% zero-hour protection rate for malware. Microsoft Edge blocked 5.9% more malware than Google Chrome and 20.4% more malware than Mozilla Firefox. By the end of the seventh day of testing, Microsoft Edge was maintaining a 3.6% lead over Google Chrome and a 17.4% lead over Mozilla Firefox.

Average Time to Block

Figure 3 depicts the average time to block SEM samples for each browser.

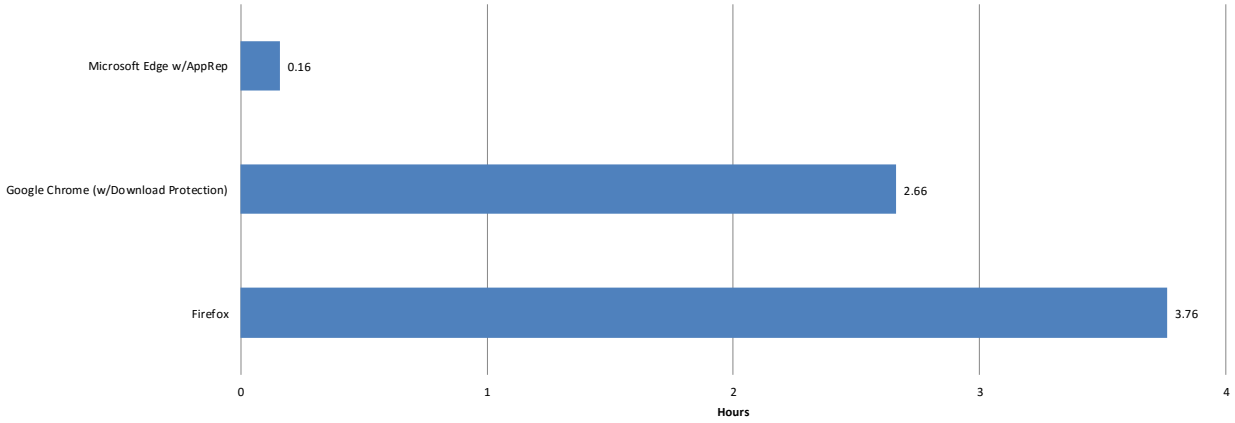


Figure 3 – Average Time to Block

Microsoft Edge required an average of less than ten minutes to block new SEM. At more than two hours and 39 minutes, Google Chrome had the next best average time to block. Mozilla Firefox took longer than three hours and 45 minutes to block malware.

Google Safe Browsing API vs Microsoft Smart Screen for SEM Protection

Figure 4 compares the use of Google Safe Browsing API vs Microsoft SmartScreen.

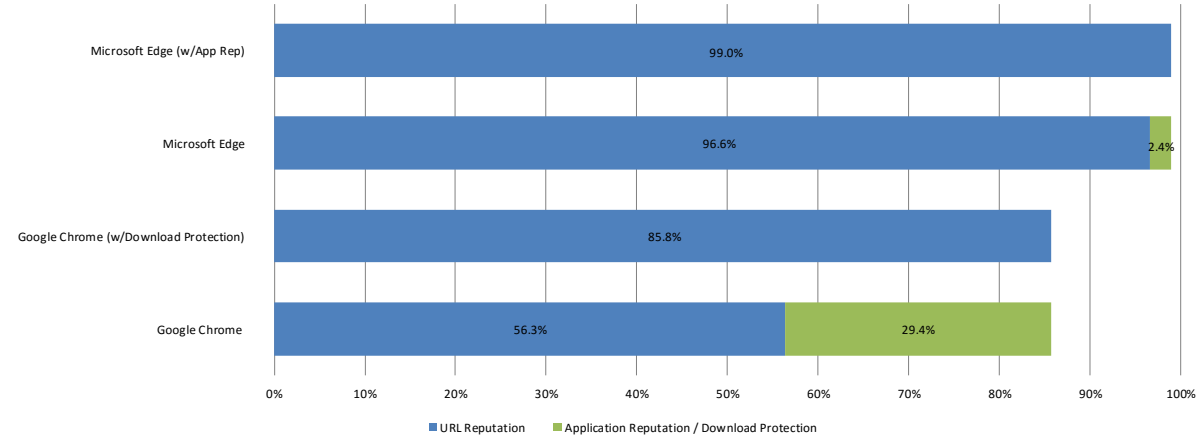


Figure 4 – Google Safe Browsing API vs Microsoft Smart Screen

Microsoft has invested significantly in its SmartScreen technology, which has constantly provided superior protection for its users over time. When Google Safe Browsing API was first rolled out, it only offered protection

against drive-by downloads and phishing sites. In response to the increase in socially engineered malware, Google added protection against SEM, which improved its block rate over previous NSS browser tests.[6]

Consistency of Protection over Time

Throughout the test, new URLs hosting SEM were added, and URLs that were either no longer reachable or no longer delivering SEM, were removed. Figure 5 shows the consistency of protection of the tested browsers throughout the testing period.

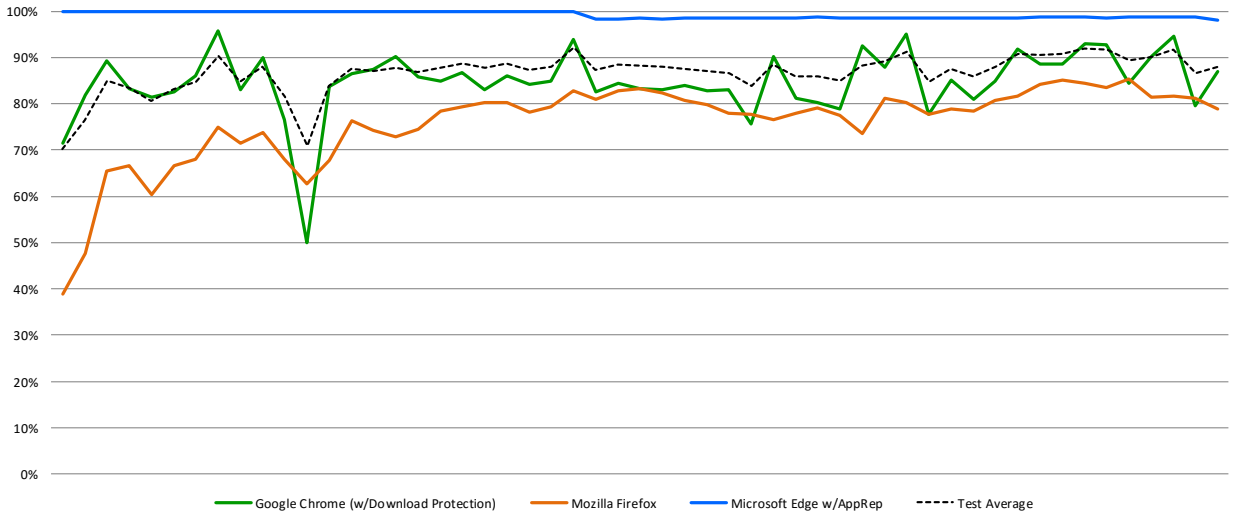


Figure 5 – SEM Protection over Time

Microsoft Edge had an average block rate of 99.0%; with its lowest recorded at 98.0%. Google Chrome had an average block rate of 85.8%; its lowest recorded at 50.0%. Mozilla Firefox had an average block rate of 78.3%, which was noticeably different than the 38.9% block rate it demonstrated at the beginning of the test.

Education Is a Component of SEM Protection

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.

[6] Evolutions in Browser Security. NSS Labs.

Test Methodology

Web Browser Security: Socially Engineered Malware 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