TEST METHODOLOGY

Web Browser Security

August 28, 2018

v4.0

Table of Contents

1 Introduction

Most web interactions occur via browsers, both at work and at home. Since the web browser is strategically located to defend against web-based threats, choosing one that provides an effective layer of defense against attacks reduces the burden on other deployed security controls. since browsers often have visibility into threats before other security technologies that are deployed both on the network or as local clients, their selection and configuring can dramatically impact an organization's security posture.

Significant changes have occurred since the inception of web browsers. As content has grown richer, so too has the number of plug-ins and software extensions that are required to access this content. However, these additional browser plug-ins increase the likelihood of new vulnerabilities. Additionally, threat actors have grown more competent at deceiving users into clicking on malicious links.

The scope of this test methodology is limited to assessing the efficacy of browser protection against malware that utilizes social engineering and phishing attack capabilities. These more insidious attacks can be difficult to identify even for the seasoned security practitioner, and this is why browser protection can make a difference.

1.1 Browser Protection against Socially Engineered Attacks

Even when a system is fully patched, a user can be deceived by an effective socially engineered attack that leverages natural human curiosity or exploits familiarity in order to get the user to click on a link. This simple action can lead to a malware download or redirection to a phishing site.

Browsers often provide protection against socially engineered attack techniques through cloud-based reputation-based systems. These systems traverse the Internet and categorize content according to whether they consider it malicious or non-malicious. After URLs are categorized, they are added to a black or white list, or if a verdict is not binary, they may be assigned a rating (depending on the vendor's approach). These ratings are assigned manually, automatically, or some combination of the two.

If reputation results are returned 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, if 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.

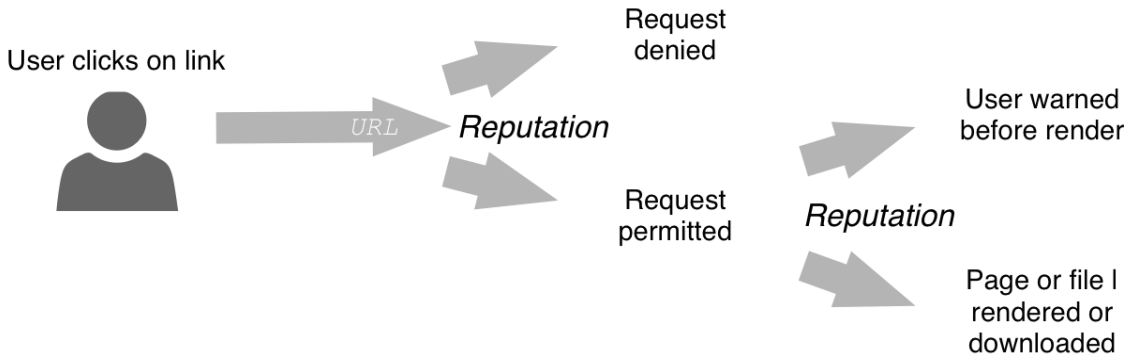


Figure 1 – Attack Workflow for Socially Engineered Malware and Phishing Attacks

2 NSS Labs Test Environment

NSS Labs has created a test environment in order to assess the reputation protection capabilities of web browsers under the most real-world conditions possible. NSS uses a proprietary live testing harness that is massively scalable and capable of running thousands of concurrent instances of each of the browsers under test.

NSS Labs test methodologies are continually evolving in response to feedback. If you would like to provide input, please contact advisors@nsslabs.com. For a list of changes, please reference the Change Log in the Appendix.

2.1 Overview and Scope

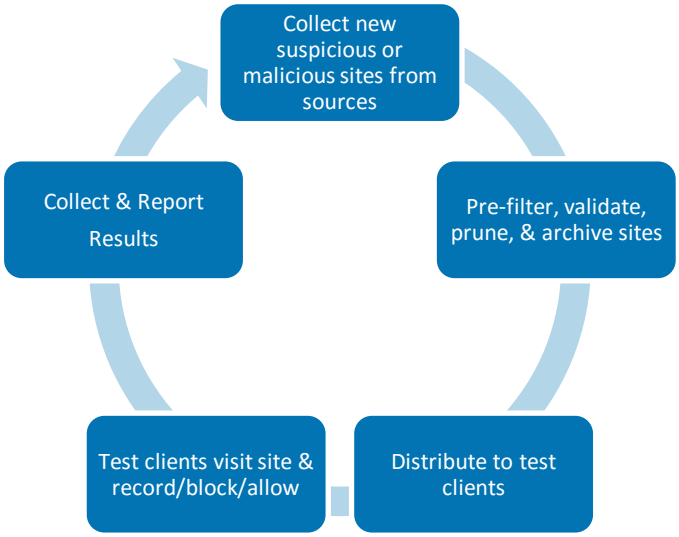
This test is designed to determine the efficacy of the reputation protection capabilities of web browsers against social attacks (phishing and malware delivered via social engineering.)

2.2 Browser Configuration

Browsers are installed using their default configurations. If a user must select an option in order to continue the installation, then the options providing the most security are selected. Before testing begins, the product is monitored, and any new updates are applied. The browsers are provided with Internet access in order to have access to reputation systems and live content. For each test, all browsers are installed on identical platforms (e.g., workstations, mobile devices, etc.).

2.3 Threat Categorization

In this test, NSS utilizes the following workflow while gathering and categorizing malicious URLs.



2.3.1 Sample Sets for URLs (Phishing and Malware)

In order to utilize the most current, wide-reaching, and representative URLs, NSS receives a broad range of samples from diverse sources, including email, instant messaging, social networks, and malicious websites. These URLs are grouped into what NSS calls “sample sets.” NSS also maintains relationships with other security companies and independent researchers that provide malicious URLs.

Exploits containing malware payloads, also known as “drive-by downloads,” are not included in this test, and therefore are not found in the NSS URL sample sets.

2.3.2 URL Cataloging

All URLs under consideration are cataloged with a unique NSS Labs ID. Prompt and accurate URL cataloging enables NSS engineers to monitor the quality of sample sources and simplify investigation and analysis.

New sites are added to the URL test set following initial discovery. The date and time that each URL is introduced is recorded. Most sources are automatically and immediately inserted, while some methods require manual handling and can be processed in under 30 minutes.

2.3.3 URL Status Confirmation

Each URL in the test set receives an initial review to verify that it meets basic test criteria and is accessible on the Internet at the time of testing. However, given the nature of the feeds and the rate of change, it is not possible to validate each site in depth before the test, since many sites quickly disappear.

In order to be included in the test set, URLs must be live during each iteration of the test. At the beginning of each iteration, the availability of the URL is confirmed by ensuring that the site can be reached and is active (for example, a non-404 web page is returned).

Validation occurs within minutes of receiving the samples. The active URL content is downloaded and saved to an archive server with a unique NSS ID number. This enables NSS to preserve the URL content for control and validation purposes. While it is not feasible to validate samples in depth before testing, every sample is validated after the test, and URLs are reclassified and/or removed accordingly.

3 Security Effectiveness

3.1 False Positive Testing

The ability of the browser to identify and allow legitimate traffic while maintaining protection against threats is just as important as its abilility to protect against malicious content. This test will include a varied sample of legitimate traffic, popular websites, and legitimate applications, which should be identified and allowed. Any inappropriate blocks or warnings will be reported.

3.2 Protection against Phishing Attacks

Browsers are expected to accurately identify both good and malicious sites and handle them appropriately. Responses are recorded as either “Allowed,” or “Blocked.”

- **Success**: Web browser successfully identifies phishing URL and consequently prevents access to URL
- **Failure**: Web browser fails to correctly identify and block phishing URL

3.3 Protection against Malware

Browsers are expected to accurately identify both good and malicious sites hosting the linked content and handle them appropriately. Responses are recorded as either “Allowed,” or “Blocked.”

- **Success:** Web browser successfully prevents malware from being downloaded and/or correctly issues user warning
- **Failure:** Web browser fails to prevent malware from being downloaded and/or fails to issue warning

4 Impaired Performance

4.1 Low Bandwidth

This test focuses on the browser's ability to protect users that have not connected their devices to Wi-Fi hotspots but has connected them to 3G/4G/LTE connections and vice versa. The browser's protection efficacy is expected to remain consistent throughout the test.

4.2 Power Management Scenario

In order to preserve battery power, some applications will proactively reduce network and/or CPU usage to preserve battery life. Security efficacy should not decline when clients are on battery power without the users being notified that this is occurring . The browser's protection efficacy is expected to remain consistent throughout the test.

Appendix: Change Log

Version 4.0 – August 28, 2018

- Collapsed Web Browser Security: Socially Engineered Malware (SEM) Protection Test Methodology and Web Browser Security: Phishing Protection Test Methodology into Web Browser Security Test Methodology

Contact Information

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

This and other related documents available at: **www.nsslabs.com**. To receive a licensed copy or report misuse, please contact NSS Labs.