Cyber Ratings .org

TEST METHODOLOGY

Web Browser Protection - Phishing & Malware Download

January 11, 2021
v1.0

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.

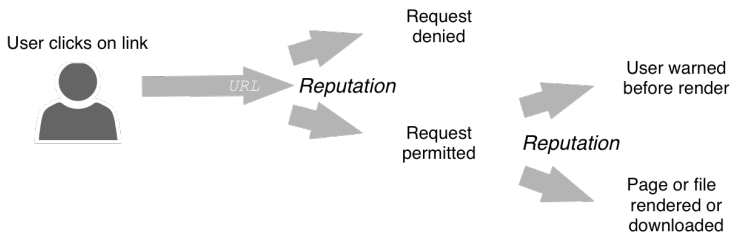
Significant changes have occurred since the inception of web browsers. As content has grown richer, so too has the number of plug-ins and software extensions that are required to access this content. However, these additional browser plug-ins and extensions increase the likelihood of new and unpatched 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 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, file or application is malicious. Some reputation systems 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.

1.2 Browser Configuration

Browsers are installed on identical platforms (e.g., workstations, mobile devices, etc.) using their default configurations. If a user must select an option 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. Auto update is enabled throughout the test. The browsers are then provided with Internet access to reputation systems and live content.

2 Test Overview

CyberRatings.org has created a test environment to assess the reputation protection capabilities of web browsers under the most real-world conditions possible. CyberRatings 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.

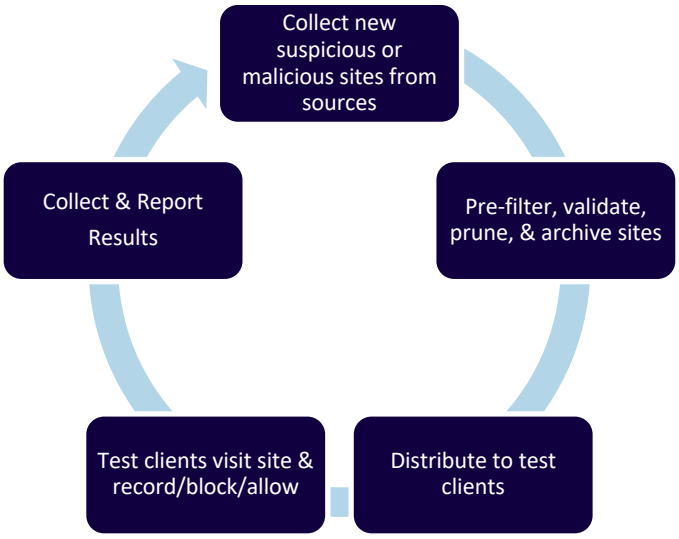


Figure 1- Test Workflow

2.1 Sample Sets for URLs (Phishing and Malware)

CyberRatings operates a network of spam traps and honeypots yielding thousands of unique samples per day. In addition, CyberRatings maintains relationships with other independent security researchers, professional networks, and security companies from which we harvest live phishing and malware URLs. Throughout the test, new URLs are added as they are discovered. Sample sets contain phishing and malware URLs distributed via spam, instant messaging, social networks, and websites.

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

2.2 URL Cataloging

All URLs under consideration are cataloged with a unique CyberRatings ID, regardless of their validity. Prompt and accurate URL cataloging enables CyberRatings engineers to monitor the quality of sample sources and simplifies investigation and analysis.

New sites are added to the URL test set as soon as possible 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. URLs that are either no longer reachable or hosting malware are removed from the test (but are maintained in the URL catalog).

2.3 URL Status Confirmation

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. However, each URL receives an initial review to verify that it meets basic test criteria and is accessible on the Internet at the time of testing.

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 CyberRatings ID number. This enables CyberRatings to preserve the URL content for control and validation purposes. Note: every sample is validated after the test, and URLs are reclassified and/or removed accordingly.

2.4 Pruning and Validation

Throughout the test, CyberRatings engineers review and remove non-conforming URLs and content from the test set. For example, a URL that initially was classified as phishing but that has since been replaced with a generic splash page will be removed and will not be included in future calculations.

CyberRatings continually verifies that each phishing and malware site is accessible and serving malicious content. Sites that are not available are not included in calculations of success or failure; however, if they become available during the test, those iterations will be included in calculations. Post-test validation enables CyberRatings to reclassify and even remove phishing / malware sites that are not malicious or that were not available during the test.

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: Browser successfully identifies phishing URL and consequently prevents access to URL
- Failure: 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: Browser successfully prevents malware from being downloaded and/or correctly issues a warning
- Failure: Browser fails to prevent malware from being downloaded and/or fails to issue warning

4 Contact Information

CyberRatings.org

2303 Ranch Road 620 South
Suite 160, #501
Austin, TX 78734

info@cyberratings.org
www.cyberratings.org