MOZILLA PHISHING PROTECTION

TESTING METHODOLOGY ANALYSIS
NOVEMBER 9TH, 2006

iSEC Partners (iSEC) was engaged by the Mozilla Foundation (Mozilla) to perform an analysis on Firefox's testing methodology for its Phishing Protection feature, which will attempt to warn users of fraudulent websites impersonating legitimate ones. The primary purpose of the assessment was to ensure that Mozilla's methodology for testing the effectiveness of anti-phishing features in both Firefox 2 and Internet Explorer 7 was fair and unbiased.

This document describes the results of iSEC's analysis over a sixteen hour period, which was performed between October 30th and November 9, 2006.

BACKGROUND: FIREFOX'S PHISHING PROTECTION FEATURE

Mozilla aims to provide a safe and productive browsing experience for its end users. Security is a top priority for Mozilla, and providing a safe browsing experience for end users while maintaining end user privacy is a key requirement. In Firefox 2, Mozilla added a new Phishing Protection feature that provides end users with options to protect themselves against phishing sites on the Internet.

Firefox's Phishing Protection feature provides two modes of operation, local mode and third party mode. By default, Firefox 2 checks the websites visited by users against a local list of URLs that are known phishing websites. Under the local mode option, URLs of known phishing sites are downloaded locally to the browser and automatically updated approximately every 30 minutes. If a visited URL matches a URL on the local list of known phishing sites, Firefox 2 will block the website and will display a warning dialog to the user.

Firefox's local mode protects user security by ensuring each URL visited by an end user is not a known phishing site. Additionally, local mode provides a high level of end user privacy by not requiring any URL information to be sent to an online phishing service. Local mode will ensure the integrity of a user's browsing experience and the privacy of their browsing activity.

Firefox's third party mode also protects end users from phishing attacks, but in a more immediate fashion. In this mode, each URL visited by the end user will be checked using an online third party service (the default third party service used by the browser is Google). If the URL is not on the known list of phishing sites maintained by the third party, the end user will continue to browse the web in a typical fashion. If the URL is on known list of phishing websites, Firefox 2 will block the request on behalf of the end

user. The third party method allows the end user to have an immediate check of a URL in real-time. It also allows the end user to leverage a large database of known phishing URLs from a third party, which is constantly updated to ensure end user integrity.

Analysis: Mozilla's Anti-Phishing Testing Methodology

Mozilla engaged SmartWare to measure the effectiveness of anti-phishing features available in Firefox 2 and Internet Explorer 7[1]. A total of 1040 phishing URLs were used for the testing process. The following steps describe the testing process:

1. Phishing URLs were received from PhishTank every hour via a XML feed.

2. SmartWare tested a fresh list of phishing URLs against Firefox 2 and Internet Explorer 7. Testing was completed in teams of two, where testers rotated browsers during the testing process.

3. URL testing was performed in groups, with up to seven URLs in each group. The order on which browser was tested first was rotated, in order to reduce the possibility of one browser gaining a benefit due to the time lag between tests.

4. Each phishing URL was tested against the two modes provided by each browser, including:

    a. Firefox 2 local mode – A local list of known phishing URLs that is updated approximately every 30 minutes

    b. Firefox 2 third party mode – Each URL is checked by a third party database (e.g. Google) and verified against a list of known phishing URLs

    c. IE 7 Automatic Website Checking Off – A local list of approved URLs.

    d. IE 7 Automatic Website Checking On - Each URL is checked by Microsoft's database and verified against a list of known phishing URLs

5. The results of each test are recorded and time-stamped. Additionally, only URLs with active phishing sites are included in the testing process. Any URL showing 404 messages, server not found, or messages from the ISP stating the site has been removed or offline are not included in the results.

---

[1] The details on Firefox's anti-phishing feature can be found at http://www.mozilla.com/en-US/Firefox/phishing-protection/. Additionally, the details on Internet Explorer's anti-phishing feature can be found at http://www.microsoft.com/mscorp/safety/technologies/antiphishing/default.mspx.

iSEC's analysis of the testing procedure included both strengths and weaknesses. The strengths of the testing methodology include the following items:

- Independence: URLs were provided by an independent, community driven effort (PhishTank). PhishTank receives phishing URLs from its user community on a daily basis, which includes several hundred community based users. Once a URL is valided as a phishing site, PhishTank reports this information on its website and any subscribers to its XML feed; hence the amount of information sent to Mozilla for the testing process is above average. For example, PhishTank has listed over 3,500 validated phishing URLs for the month of October.

- Third party testing: While the testing process was administered by Mozilla, each test was performed by SmartWare, a third party. The independence in testing process reduces the possibility of tampering or adjustment of testing results.

- Testing groups: Testing is performed in groups of two for added verification. Furthermore, each tester rotated browsers, ensuring a browser was not tested by a single individual. The rotation of browsers ensures that testers are fully aware of the browsers being tested and their results.

- Scoring system: The scoring system gives equal balance to all anti-phishing features despite certain reporting differences. For example, each browser will receive a single point for a warn message or block on a phishing URL. For each URL that is not blocked or with no warning, the URL receives zero points. The scoring method does not penalize anti-phishing features that may warn users instead of blocking URLs.

- URL testing period: All URLs used for the testing process fell within a reasonable testing window, specifically, 15 minutes or less. The short time interval reduces the possibility of one browser having more time to update its phishing database over another.

The following section describes some of the weaknesses of the testing process:

- False positives: Mozilla did not perform any false positive testing. For example, legitimate and popular URLs, such as www.mozilla.com, less popular URLs, such as www.isecpartners.com, and/or obscure, but legitimate URLs, were not tested. There is no false positive ratio to see if the filters are blocking legitimate sites that are not phishing URLs.

- Point system: As mentioned previously, the scoring system did not differentiate between a warn and a block for a phishing URL. Hence, browsers that support warn and block were given the same points. This system may become an issue if there is a high false positive rate in a browser. For example, if a browser had a high false positive rate, a warn would actually be better than a block, enabling the user to make their own decision on the URL.

- Browser Testing Order: Browser testing order was rotated and randomized; however, it was not balanced. Firefox 2 was tested first more than half the time when compared to Internet Explorer 7, giving a slight advantage to Internet Explorer 7. Browser rotation is important as the last browser tested against a given phishing URL has more time to update its phishing database, allowing it to potentially show a positive result. The testing process should be more evenly distributed between browsers; however, since the testing window between browsers was 15 minutes of less, the lack even distribution probably did not have a significant affect on the results.

CONCLUSION

The methodology completed by Mozilla follows a fair testing process for functionality/feature testing. Key items to accurately measure the effectiveness of anti-phishing features were appropriate, such as sample size ($n > 1000$), independence (testing conducted by a third party), content independence (URLs were provided by a community based effort), scoring system (different reporting methods were not penalized), and URL testing periods (each URL was tested within a 15 minute window). iSEC has determined that methodology used for the testing process can be considered a fair and unbiased approach.

APPENDIX A

The following link is the results from Mozilla's testing process[2]:

http://www.mozilla.org/security/phishing-test-results

[2] The results of the testing process should not be considered part of the iSEC report. iSEC evaluated the testing methodology only and was not involved in its execution.