BROWSER SECURITY COMPARATIVE ANALYSIS

Phishing Protection

2013 – Randy Abrams, Orlando Barrera, Jayendra Pathak

Tested Vendors

Apple, Google, Microsoft, Mozilla, Opera

Overview

The most common and effective security threats facing users today are socially engineered malware and phishing attacks. As such, they have been the focus during continued research and testing by NSS Labs of the security effectiveness of browsers. While drive-by downloads and clickjacking are also effective attacks that have achieved notable publicity, they represent a smaller percentage of today's threats. Drive-by downloads are commonly the result of successful phishing attacks, and clickjacking attacks often lead to phishing web pages.

During March 2013, NSS performed a comprehensive test of web browser phishing protection against the NSS *"Phishing Protection Test Methodology V2.0."* This report is based upon empirically validated evidence gathered by NSS during 12 days of continuous testing. Testing was performed every 6 hours for a total of 45 discrete test runs, adding fresh new phishing URLs with each iteration. Each product was updated to the most current version available at the time that testing began and each product was given access to the live Internet.

Note: This test was performed alongside a similar test of socially engineered malware (see *"2012 Browser Security Comparative Analysis: Socially Engineered Malware" (CAR).)*

The average phishing URL catch rate for browsers over the entire 12-day test period ranged from 96 percent for Firefox (version 19) to 83 percent for Internet Explorer (IE) (version 10). Compared to the *"2012 Browser Security Comparative Analysis Phishing Protection,"* Firefox and Safari have improved by 6 percent and 4 percent respectively. Chrome's protection dropped by 2 percent and Internet Explorer's fell by 9 percent. Opera was not included in the 2012 CAR. Significant fluctuations do occur and comparisons between past tests and this test highlight why a historical analysis of tests is important in assessing the long-term quality of security products.

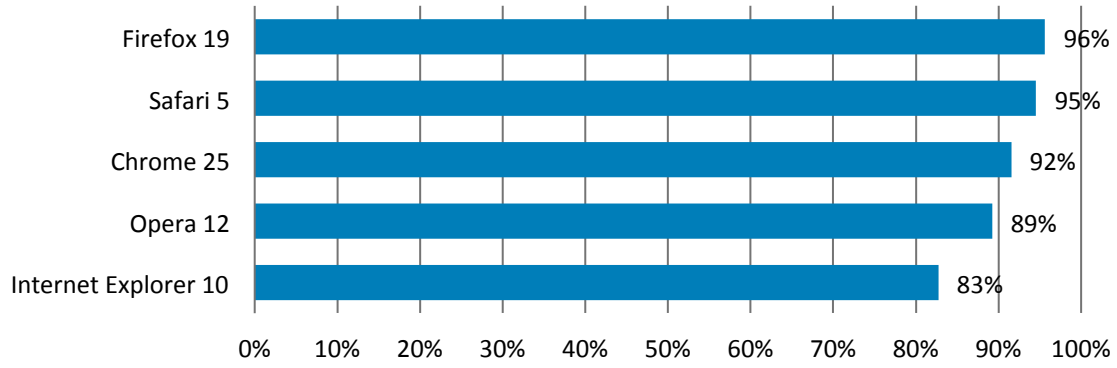


Figure 1 - Mean Block Rate

Chrome, Firefox and Safari all use Google's Safe Browsing API, and all scored within 4 percent of each other. Previously, these products also had a 4 percent spread; however, Chrome and Firefox swapped relative positions in effectiveness in this round of testing. Internet Explorer uses Microsoft's SmartScreen technology for both malware and phishing protection. Opera uses a combination of blacklists from Netcraft[1] and PhishTank,[2] as well as a malware blacklist from TRUSTe.[3] Opera's approach was competitive with Google's *Safe browsing API,* with Opera scoring just 3 percent below Chrome. The relatively poor showing by Internet Explorer was a surprise given results in previous tests. This may prove of concern should future testing demonstrate a trend in decreased protection.

The 13 percent spread in protection scores is significant considering the spread was just 4 percent across all products in the last test. With an approximate margin of error of 2 percent, Microsoft's low score is significant when compared to the top three performers in this test.

The ability to warn potential victims that they are about to stray onto a malicious website puts Web browsers in a unique position to combat phishing and other criminal activities. Since phishing sites have an average lifespan of only 26 hours, it is essential that the site is discovered, validated, classified, and added to the reputation system as quickly as possible. This explains the correlation between average-time-to-block and catch-rate. A good reputation system must be both accurate and fast in order to realize high catch rates. Browser developers clearly understand this relationship, and substantially more phishing sites are blocked in the first 24 hours of detection than have ever been blocked before. While the average uptime for phishing sites rose from 23 hours in the first half of 2012 to 26 hours in the second half of 2012, the median uptime climbed from 5 hours and 45 minutes to 10 hours and 19 minutes. The improved zero hour protection across the board is significant in protecting against these threats.

Early detection of phishing sites is very important, but should not be given undue weight. The majority of standard phishing attacks (not spearphishing) are not relevant to the recipients. For example, if an HSBC customer receives a Bank of America phish, the earliest possible detection does not afford greater protection across the board.

[1] http://www.netcraft.com/

[2] http://www.phishtank.com/

[3] http://www.truste.com/

While Firefox and Safari outperformed the browsers under test, phishing protection is only one measure of browser security. Chrome's superior protection against socially engineered malware makes a strong case for Chrome over Firefox and Safari. The superior performance of Internet Explorer over Chrome in socially engineered malware protection compensates for the lower than expected phishing protection observed in this test. The dangers associated with socially engineered malware and drive-by downloads are significant enough that the security capabilities of a browser protection against these threats should be considered a more critical component of the selection criteria. The NSS *"2013 Browser Security Comparative Analysis: Socially Engineered Malware"* provides essential information with respect to the ability of browsers to block socially engineered malware attacks.

In the previous browser phishing protection comparative it was noted that "Going forward, the challenge will be to bring down the response time" and this test shows significant improvement in that area. The browser vendors are steadily improving their products, and the onus will be on industry coalitions to keep find ways to keep the average phishing site uptime down.

NSS Labs Findings

- Overall response times have improved dramatically across the board.
- Phishing protection is only one security attribute of a browser. Socially engineered malware blocking capabilities must be factored into an assessment of overall browser security.
- The time required to add protection for new phishing sites is an important factor, and zero hour protection rates can vary by as much as 20 percent.
- The browsers using Google's Safe Browsing API averaged 94 percent, an increase from last year's 91.7 percent for the same products.
- The mean phishing block rate among the tested browsers is 90.1 percent, a decrease from last year's average of almost 2 percent.

NSS Labs Recommendations

Enterprises should:

- Use current versions of web browsers to increase protection against phishing attacks.
- Consider a browser's average time to block attacks when selecting a browser.
- Augment browser protection with education to protect against the attacks that do bypass the browsers.
- Include in the browser selection criteria the ability to block socially engineered malware.
- Increase security awareness. Good judgment remains the best defense against social engineering attacks.

This analyst brief was produced as part of NSS Labs' independent testing information services. Leading vendors were invited to participate fully at no cost, and NSS received no vendor funding to produce this report.

Table of Contents

Tested Vendors 1
Overview 1
NSS Labs Findings 3
NSS Labs Recommendations 3
Analysis 5
The Phishing Threat 5
Web Browser Security 6
Test Composition – Phishing URLs 6
Total Number Of Malicious URLs In The Test 6
Average Number Of Malicious URLs Added Per Day 6
Mix Of URLs 7
Blocking Phishing URLs 7
Average Time To Block Phishing URLs 7
Average Response Time To Block Phishing 8
Real-Time Blocking Of Phishing URLs Over Time 9
SafeBrowsing Analysis 9
Appendix A: Test Environment 10
Client Host Description *10*
The Tested Browsers *10*
Test Methodology 11
Reading List 12
Contact Information 13

Table of Figures

Figure 1 - Mean Block Rate *2*
Figure 2 - Phishing URL Response Histogram *7*
Figure 3 - Average Time To Block (Shorter Time Is Better) *8*
Figure 4 - Phishing Protection Over Time *9*
Figure 5 - Phishing Protection Over Time – SafeBrowsing Products *9*

Analysis

Social engineering has long been a popular tool for confidence tricksters and other criminals seeking to deceive people for personal gain. Phishing is the natural application of modern technology to social engineering by the criminals that perpetrate this attack strategy. In this report, NSS studied the leading web browsers' ability to protect against phishing. A companion report reveals the findings of the protection capabilities of web browsers against socially engineered malware (see *"2013 Browser Security Comparative Analysis: Socially Engineered Malware").*

The Phishing Threat

"Phishing" attacks are executed in one of two ways. Either an attacker attempts to persuade a victim to provide personal information (such as credit card details, login information for email or social media accounts, or other personal information that can be used for identity theft and other information-based attacks), or an attacker attempts to lure users into installing a malicious application or into navigating to a website where malicious software will be installed through the exploitation of vulnerable software. Both types of phishing attacks can be delivered through email, instant messages, SMS messages, and links on social networking sites.

Phishing attacks have the potential to compromise sensitive personal and corporate information and as such they pose a significant risk to individuals and organizations. In 2012, a monthly average of 26,673 unique email phishing campaigns were reported and 52,542 unique phishing websites detected.[4] The average number of unique phishing sites detected in 2011 was well under 40,000 per month. The average uptime for a phishing attack has been steadily falling from a high of 73 hours in the second half of 2010 to a record low of 23 hours and 10 minutes in the first half of 2012. [5] The second half of 2012 saw a slight increase in uptime for phishing attacks.[6] The speed at which these threats are "rotated" to new locations is staggering, and it poses a significant challenge to those attempting to defend against such attacks.

In response to this trend, security vendors have developed reputation systems that classify malicious and phishing URLs via in the cloud services. As early as 2009, NSS predicted the necessity of web reputations system in combatting these threat in a Web browser group test, stating:

"Reputation systems are literally the next "big thing" in computer security and offer an additional layer of protection to client endpoint machines, which have effectively become the mobile corporate perimeter. For home users this was always the case, and now they too can benefit from in the cloud services, usually without even knowing it."

[4] http://www.antiphishing.org/resources/apwg-reports/ (aggregated from quarterly reports)

[5] http://www.antiphishing.org/reports/APWG_GlobalPhishingSurvey_1H2012.pdf

[6] http://docs.apwg.org/reports/APWG_GlobalPhishingSurvey_2H2012.pdf

Web Browser Security

The evolution of the browser is comparable to the evolution of anti-virus software. Where anti-virus software first detected only self-replicating threats, then Trojans, and now detects a myriad of threats, browsers initially managed annoyances like pop-ups and cookies and then were required to confront more serious security issues. Phishing websites are among the top threats against which the browser must protect. This report examines the abilities of five different web browsers to protect users from live phishing attacks.

The foundation of browser phishing protection is cloud-based reputation-based systems that search the Internet for malicious websites and categorize content accordingly, either by adding the site to a blacklist or whitelist, or by assigning the site a score (depending on the vendor's approach). The classification may be performed through manual or automatic methods, or by using a combination of the two approaches. The second functional component resides within the web browser; it requests reputation information from the cloud-based systems about specific URLs and then enforces warning and blocking functions.

When results indicate that a site is "bad," the web browser redirects the user to a message warning the user that the URL is malicious. Some programs also include educational content. Conversely, when a website is determined to be "good," the web browser takes no action and the user remains unaware that the browser performed a security check.

Test Composition – Phishing URLs

Data in this report spans a testing period of 12 days from March 11 through March 22, 2013. All testing was performed at the NSS testing facility in Austin, TX. During the test, NSS engineers routinely monitored connectivity to ensure that the browsers could access the live Internet sites being tested, as well as their reputation services in the cloud.

The emphasis was on freshness, thus a larger number of sites were evaluated than were ultimately kept as part of the result set, since new URLs were constantly being added to the test and dead sites were being removed.

Total Number Of Malicious URLs In The Test

Throughout this study, 168, 462 results were collected from 45 discrete tests conducted without interruption over 360 hours (every 6 hours for 12 days). NSS engineers removed samples that did not pass the validation criteria, including those tainted by exploits (not part of this test.) Ultimately, 3008 unique URLs were included in the final set of phishing sites, providing a margin of error of 1.85 percent with a 95 percent confidence level.

Average Number Of Malicious URLs Added Per Day

On average, 251 new validated URLs were added to the test set per day; numbers varied on some days as criminal activity levels fluctuated.

Mix Of URLs

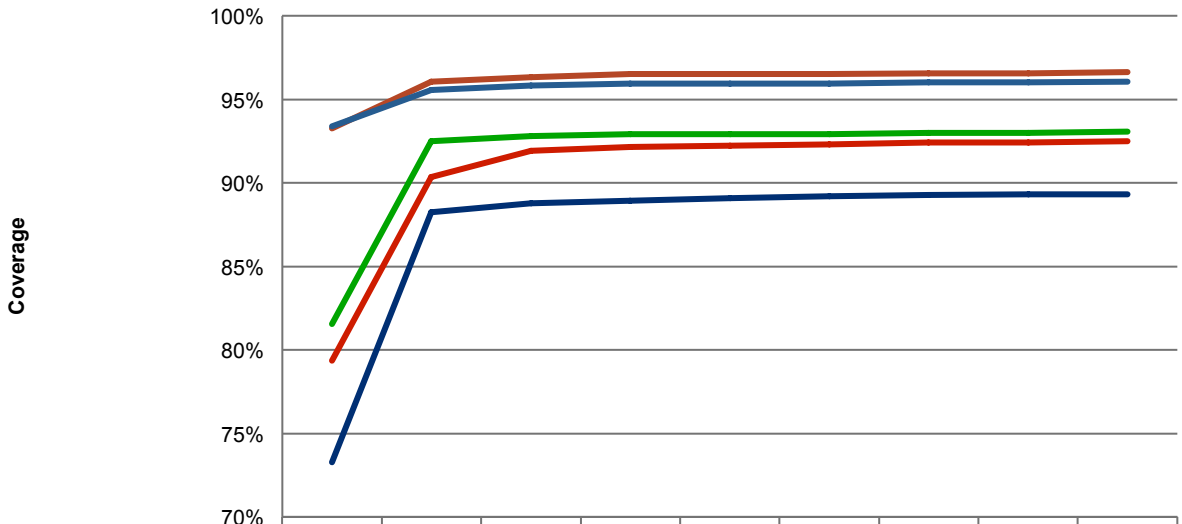
The mixture of URLs used in the test was representative of current threats on the Internet. Care was taken not to overweight any one domain to represent more than 10 percent of the test set; sites were pruned once this limit was reached.

Blocking Phishing URLs

NSS assessed the browsers' ability to block malicious URLs as quickly as they were discovered on the Internet. Engineers repeated these tests every six hours to determine how long it took a vendor to add protection, if they did at all.

Average Time To Block Phishing URLs

Figure 2 illustrates the time that was required for browsers to block a threat once it was introduced into the test cycle. Cumulative protection rates are listed at the time of introduction, the "zero hour," through the end of the test. Final protection scores for the URL test duration are summarized under the "Total" column. The initial protection from phishing sites ranged from 73.3 percent (IE 10) to 93.4 percent (Safari).



	0-hr	1d	2d	3d	4d	5d	6d	7d	Total
Firefox	93.3%	96.0%	96.3%	96.5%	96.5%	96.5%	96.6%	96.6%	96.6%
Chrome	81.5%	92.5%	92.8%	92.9%	92.9%	92.9%	93.0%	93.0%	93.1%
Opera	79.4%	90.4%	91.9%	92.2%	92.2%	92.3%	92.4%	92.4%	92.5%
Internet Explorer 10	73.3%	88.2%	88.8%	88.9%	89.1%	89.2%	89.3%	89.3%	89.3%
Safari	93.4%	95.5%	95.8%	95.9%	95.9%	95.9%	96.0%	96.0%	96.0%

Figure 2 - Phishing URL Response Histogram

The zero hour protection rates showed significant improvement since the last round of testing, with products improving this critical detection by an average of 19 percent. By the end of day one, all products in this test had

performed better than any product had done in the previous test. With the average uptime for phishing sites hovering close to 24 hours, these metrics are extremely important.

Firefox and Safari continued to lead the other browsers in phishing protection overall and in the early hours of attacks. Opera was not included in the previous test; however, Opera performed well in this test and better than any of the browsers in the previous test at zero hour and day 1 protection. IE10 was relatively weak at zero hour, competitive at day one protection, but ultimately trailed the other browsers in this test.

Average Response Time To Block Phishing

Figure 3 reveals the average length of time that a user must wait for a requested phishing URL to be added to a block list. Figure 3 depicts the browser's average time to block a phishing site once it was introduced into the test set, but only if the phishing site was blocked during the course of the test. Unblocked sites are not included since there is no mathematically empirical way to score "never."

Note that phishing sites in the second half of 2012 had an average life expectancy of only 26 hours.

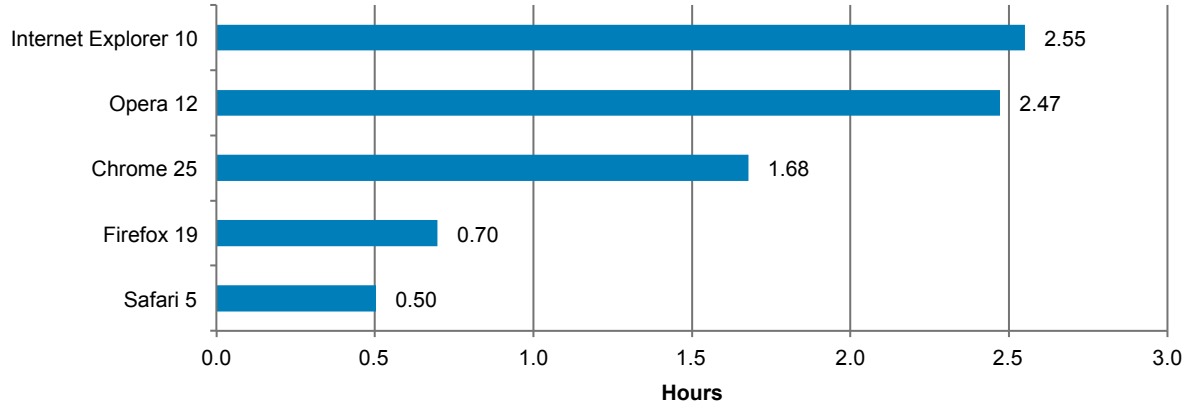


Figure 3 - Average Time To Block (Shorter Time Is Better)

The mean time to block a site (if it is blocked at all) is 1.6 hours. Firefox and Safari were significantly faster than any of the other browsers at adding protection in the earliest hours of a phishing attack. Chrome, IE10, and Opera were nearly twice as fast at blocking new phishing URLS than the average block time during the October 2012 test.

Real-Time Blocking Of Phishing URLs Over Time

The metrics for blocking individual URLs represent just one perspective. When it comes to daily usage scenarios, users are visiting a wide range of sites that may change quickly. At any given time, the available set of phishing URLs is evolving, and a continued ability to block these sites is a key criterion for effectiveness. NSS tested a set of live URLs every six hours. Figure 4 shows protection at each of the 45 incremental tests over a period of 12 days, and each score represents protection at a given point in time.

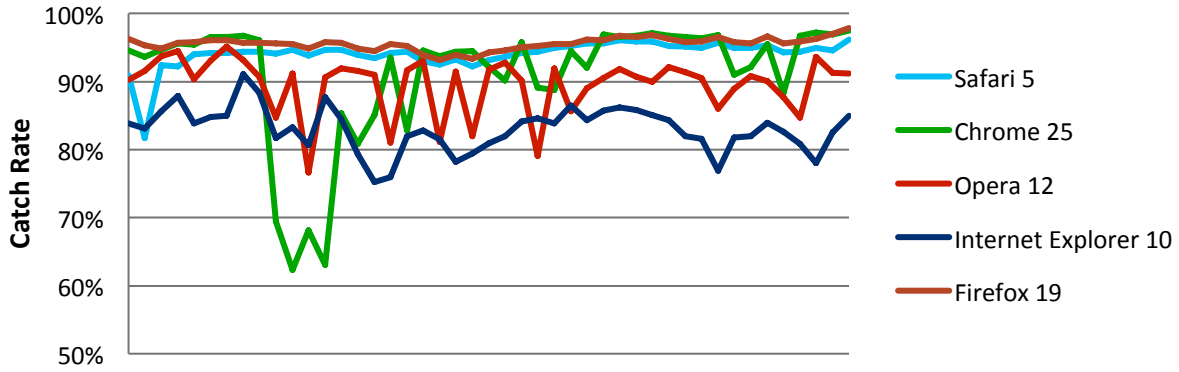


Figure 4 - Phishing Protection Over Time

Note that the protection percentage will deviate from the unique URL results for several reasons. First, this data includes multiple tests of a URL, so if it is blocked early in the testing cycle, it will improve the score. If the URL continues to be missed, however, it will detract from the score. Results of individual URL tests were compounded over time.

SafeBrowsing Analysis

Chrome 25, Firefox 19, and Safari 5 all use the Google SafeBrowsing API. The mean detection rates for these browsers are very close; however, Chrome lags behind Firefox and Opera in early protection and then exhibits significantly more erratic behavior over time, as seen in Figure 5.

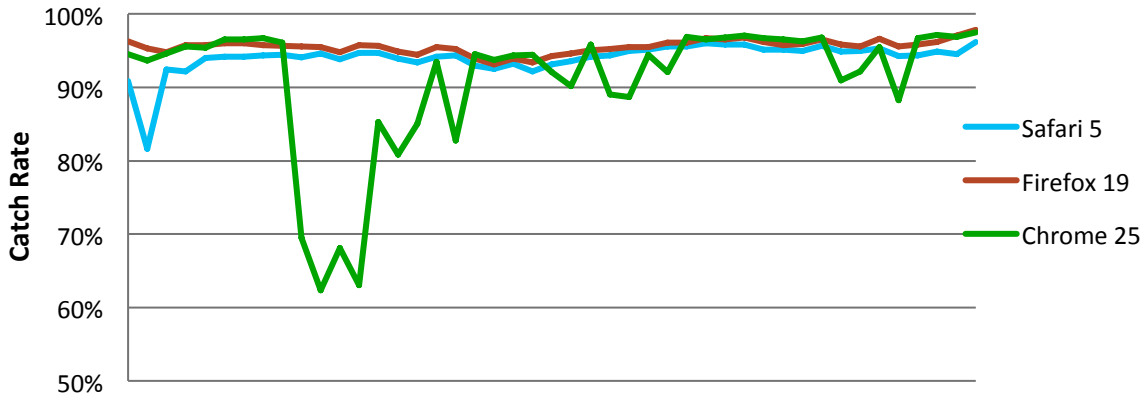


Figure 5 - Phishing Protection Over Time – SafeBrowsing Products

Appendix A: Test Environment

NSS has created a complex test environment and methodology to assess the protective capabilities of Internet browsers under the most real-world conditions possible, while also maintaining control and verification of the procedures. For this browser security test, NSS created a unique "Live Testing™" harness in order to duplicate user experiences under real world conditions. 168,462 individual tests (URL lookups) were performed over a period of 12 days (45 discrete test runs).

Client Host Description

All tested browser software was installed on identical virtual machines with the following specifications:

- Microsoft Windows 8 Enterprise
- 4GB RAM
- 60GB HD

Browser machines were tested prior to and during the test to ensure proper functioning. Browsers were given full access to the Internet so they could visit the actual live sites.

The Tested Browsers

The browsers under test were obtained independently by NSS. Generally available software releases were used in all cases, except for IE 10. Each product was updated to the most current version available at the time testing began. The following is a current list of the web browsers that were tested:

- Apple Safari 5.1.7(7534.57.2)
- Google Chrome 25.0.1364.172m
- Microsoft Internet Explorer 10.0.9200.16484
- Mozilla Firefox 19.0.2
- Opera 12.14 build 1738

Once testing began, the product version was frozen in order to preserve the integrity of the test. This test relied upon Internet access for the reputation systems and access to live content. Generally, there is a configurable separation between software updates and database or signature updates – to draw analogies from the anti-virus, IPS, and general software practices.

Test Methodology

"Phishing Protection Test Methodology V2.0" NSS Labs, December 2012 (https://www.nsslabs.com/reports/phishing-protection-test-methodology-v20)

Reading List

"2013 Browser Security Comparative Analysis: Socially Engineered Malware" NSS Labs, May 2013 (https://www.nsslabs.com/reports/2013-browser-security-comparative-analysis-socially-engineered-malware)

"2012 Browser Security Comparative Analysis Phishing Protection" NSS Labs, November 2012 (https://www.nsslabs.com/reports/2012-browser-security-comparative-analysis-phishing-protection

"2009 Q3 Web Browser Group Test: Phishing" NSS Labs, August 2009 (https://www.nsslabs.com/reports/2009-q3-web-browser-group-test-phishing)

"2012 Browser Security Comparative Analysis Socially Engineered Malware" NSS Labs, October 2012 https://www.nsslabs.com/reports/2012-browser-security-comparative-analysis-socially-engineered-malware

Contact Information

NSS Labs, Inc.
206 Wild Basin Road
Building A, Suite 200
Austin, TX 78746 USA
+1 (512) 961-5300
info@nsslabs.com
www.nsslabs.com