BROWSER SECURITY COMPARATIVE ANALYSIS

Phishing Protection

2012 – Randy Abrams, Orlando Barrera, Jayendra Pathak

Tested Products

Apple Safari 5

Google Chrome 21

Microsoft Internet Explorer 10

Mozilla Firefox 15

Overview

During October 2012 NSS Labs performed a comprehensive test of web browser phishing protection against our live web browser security testing methodology v2.0. This report is based upon empirically validated evidence gathered by NSS Labs during 10 days of continuous testing. Testing was performed every 6 hours for a total of 37 discrete test runs, each one adding fresh new phishing URLs. Each product was updated to the most current version available at the time testing began and allowed access to the live Internet.

The most common and impactful security threats facing users today are socially engineered malware and phishing attacks. As such, they have been the primary focus of NSS Labs continued research and testing 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 a successful phishing attack and clickjacking attacks often lead to a phishing web page.

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

The average phishing URL catch rate for browsers over the entire 10 day test period ranged from 90 percent for Firefox (version 15) to 94 percent for Chrome (version 21). With a margin of error of about 2 percent, there is little difference in the average block rate of the browsers and one must consider other factors, such as socially engineered malware blocking capabilities, for qualitative differences in the security effectiveness of the browsers.

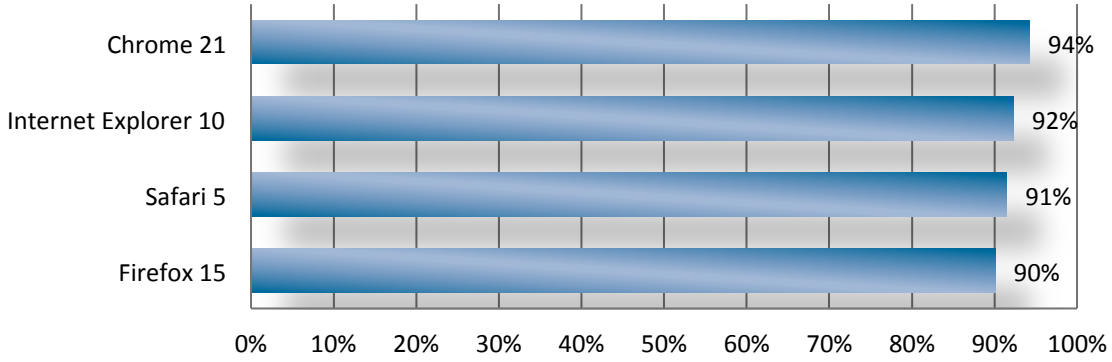


Figure 1 - Mean Block Rate for Phishing (higher is better)

Generally available software releases were used in all cases except for Internet Explorer 10, which was only available in Windows 8 and was generally only available as a beta during the test. Each product was updated to the most current version available at the time testing began.

Internet Explorer 10 was the only tested browser that does not use the Google SafeBrowsing API and had a mean block rate of 92%. For products using the SafeBrowsing API, Chrome 21 had a mean block rate of 94%, Safari 5 achieved a mean block rate of 90%, and Firefox 15 had a mean block rate of 90%.

There was a maximum difference of 4% between browsers using Google's SafeBrowsing API. In NSS Labs 2009 Web Browser Group Test, there was a 78% difference in protection levels between the most and least effective SafeBrowsing products.

Key Findings

- The mean phishing block rates among the tested browsers have improved from a group average of approximately 47 percent just 3 years ago to a group average of approximately 92 percent today.
- The time required to add protection for new phishing site is an important factor and can vary by more that 25%.
- 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.

Recommendations

- Use current versions of web browsers to increase protection against phishing attacks.
- The average time to block attacks should be a factor in browser selection.
- Augment browser protection with education to protect against the attacks that do bypass the browsers.
- Include the ability to block socially engineered malware in the browser selection decision.

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

Table of Contents

Table of Figures

Analysis

Long before the Greeks hid a group of soldiers in a wooden gift horse (Trojan horse), social engineering was a popular tool for con artists and other criminals deceiving people for their own personal gain. Phishing is the natural application of modern technology to social engineering by criminals perpetrating this proven attack strategy. In this report, NSS Labs studied the leading web browsers' ability to protect against phishing. In a companion report, NSS Labs reported the findings of the protection capabilities of web browsers against socially engineered malware (see: Browser Security Comparative Analysis: Socially Engineered Malware).

The Phishing Threat

"Phishing" attacks can be constructed in two basic ways. The first is an attempt to persuade a victim to provide personal information to the attacker. The information may be 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. The second type of phishing attack attempts to lure users into installing a malicious application or navigating to a website where malicious software will be installed through the exploitation of vulnerable software. Common to both phishing attacks is that they arrive via email, instant messages, SMS messages, and links on social networking sites.

Phishing attacks pose a significant risk to individuals and organizations alike, by threatening to compromise or acquire sensitive personal and corporate information. The number of reported phishing attacks peaked in 2009. However, they have remained high and the actual number of unique phishing sites has increased from 56,362 in August 2009 to a high of 63,253 in April of 2012. The average number of unique phishing sites detected in 2011 was well under 40,000 per month. In 2012, the average number of unique phishing sites detected has consistently been well over 50,000 per month.[1] 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. [2] The speed at which these threats are "rotated" to new locations is staggering and 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. The 2009 NSS Labs Web Browser Group Test stated:

"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."

The proof of this becomes obvious when comparing the results of the two tests. In 2009, the average block rate was 46%, whereas it currently stands at 91.75%.

[1] http://www.antiphishing.org/phishReportsArchive.html

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

Web Browser Security

Web browsers have stepped up their role in protecting clients by adding mechanisms for warning users about suspected phishing sites, and even blocking them. This report examines the abilities of four different web browsers to protect users from live phishing attacks.

The foundation is an in-the-cloud reputation-based system that scours the Internet for malicious websites and categorizes content accordingly, either by adding it to a black or white list, or assigning a score (depending on the vendor's approach.) This may be performed manually, automatically, or a combination of the two. The second functional component resides within the web browser and requests reputation information from the in-the-cloud systems about specific URLs, and then enforces warning and blocking functions.

When 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, when 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 by the browser.

Test Composition – Phishing URLs

Data in this report spans a testing period of 10 days from October 15 through October 25, 2012. All testing was performed in the NSS Labs testing facility in Austin, TX. During the course of the test, NSS Labs engineers routinely monitored connectivity to ensure 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 as new URLs were constantly being added to the test and dead sites removed. See the methodology for more details.

Total Number Of Malicious URLs In The Test

Throughout the course of this study, 158, 635 results were collected from 37 discrete tests conducted without interruption over 240 hours (every 6 hours for 10 days.) A collection of 4,306 unique URLs were available at the time of entry into the test and were successfully accessed by the browsers in at least one run. NSS Labs engineers removed samples that did not pass the validation criteria, including those tainted by exploits (not part of this test.) Ultimately 2,291 unique URLs were included in our final set of phishing sites, providing a margin of error of 2.05% with a 95% confidence interval.

Average Number Of Malicious URLs Added Per Day

On average, 208 new validated URLs were added to the test set per day; numbers varied on some days as criminal activity levels fluctuated.

Mix Of URLs

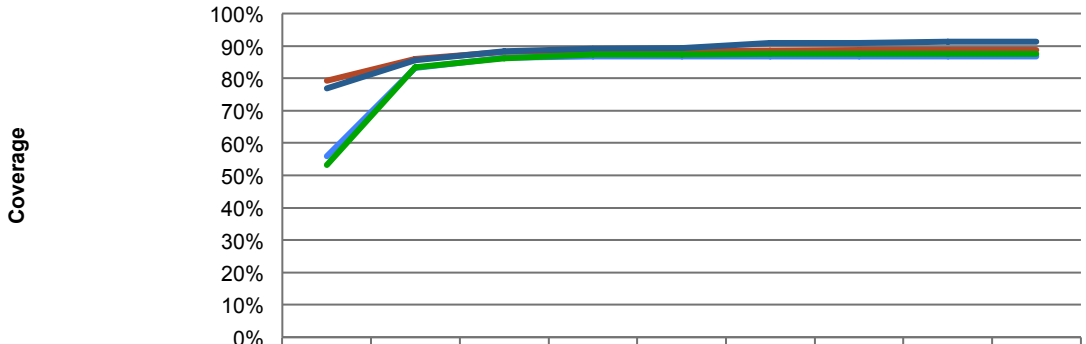
The mixture of URLs used in the test was representative of current threats on the Internet. Care was taken not to overweight any one domain to represent more than 10% of the test set; sites were pruned once this limit was reached.

Blocking Phishing URLs

NSS Labs assessed the browsers' ability to block malicious URLs as quickly as they were discovered on the Internet. Engineers continued testing them 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

The following histogram shows how long it took the 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 53.2% (Chrome 21) to 79.2% (Firefox 15.)



	0-hr	1d	2d	3d	4d	5d	6d	7d	Total
Firefox 15	79.2%	86.1%	88.2%	88.6%	88.6%	88.7%	88.7%	88.7%	88.7%
Safari 5	76.9%	85.6%	88.4%	89.2%	89.3%	90.9%	91.0%	91.3%	91.4%
Internet Explorer 10	55.9%	83.2%	86.3%	86.7%	86.8%	86.8%	86.8%	86.8%	86.8%
Chrome 21	53.2%	83.5%	86.2%	87.4%	87.4%	87.5%	87.5%	87.5%	87.5%

Figure 2 - Phishing URL Response Histogram

Firefox demonstrated the strongest protection for zero hour phishing attacks at 79.2%, adding 6.9% during the first 24 hours and only 2.6% over the rest of the test. Safari started strong at 76.9% and had caught up with Firefox by the second day. Internet Explorer and Chrome had weak starts ranging between 53.2% and 55.9%. Internet Explorer 10 reached its maximum rate in 4 days and Chrome 21 required 5 days.

Longer-term blocking of phishing sites was comparable across all of the browsers. Firefox, Safari and Chrome share the SafeBrowsing API and, in 2009, the differences in protection were significant. In this test, the SafeBrowsing

products exhibited little difference over time. However, Firefox and Safari had a distinct advantage when blocking zero hour attacks. This demonstrates that either different implementations yield different results or that Firefox and Safari are not relying on the SafeBrowsing API alone.

Average Response Time To Block Phishing

This table answers the question of how long a user must wait on average until a requested phishing URL is added to the block list. It shows the average time to block a phishing site once it was introduced into the test set, but only if it was blocked during the course of the test. Unblocked sites are not included, as there is no mathematically empirical way to score "never."

Note that phishing sites have an average life expectancy of only 23 hours.

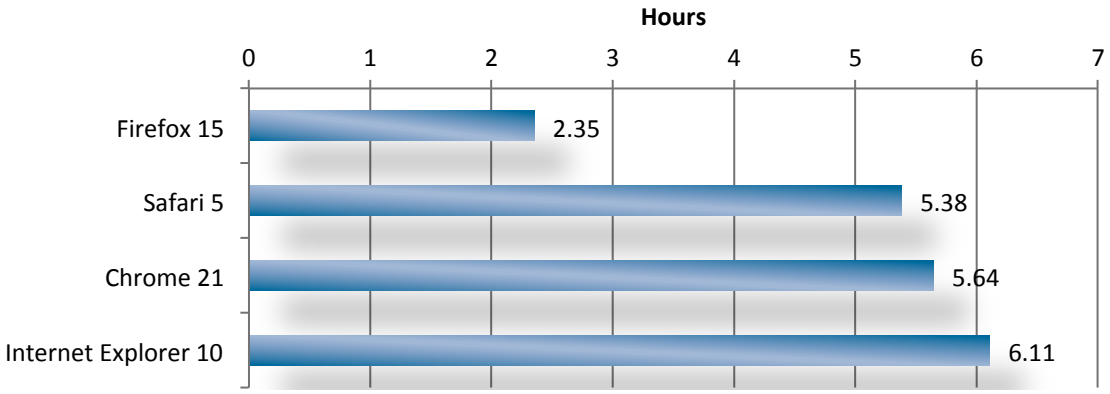


Figure 3 - Average Time to Block (shorter time is better)

The mean time to block a site (if it is blocked at all) is 4.87 hours. Firefox 15 was significantly faster at adding protection in the earliest hours of a phishing attack than any of the other browsers. Safari, Chrome and Internet Explorer 10 were fairly close to each other in response time.

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 continuing to block these sites is a key criterion for effectiveness. NSS Labs tested a set of live URLs every six hours. The graph below shows protection at each of the 37 incremental tests of over a period of 10 days and each score represents protection at a given point in time. The mean protection rate over time for all browsers was 46% in 2009, and now approaches 92%.

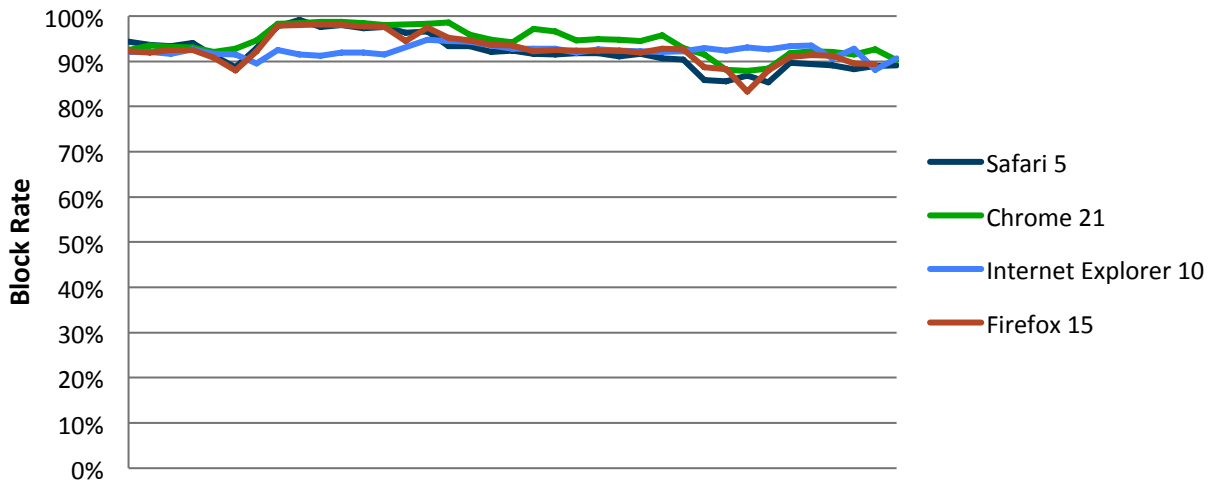


Figure 4 - Phishing Protection Over Time

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 on, it will improve the score. If it continues to be missed, however, it will detract from the score. Results of individual URL tests were compounded over time.

SafeBrowsing Analysis

Chrome 21, Firefox 15 and Safari 5 all use the Google SafeBrowsing API. In 2009, NSS Labs' testing revealed wide-ranging results in the effectiveness of phishing URL blocking. In 2009, the worst browser had a 2% block rate and the best 83%. In 2012, the gaps have been effectively closed and protection levels are extremely close.

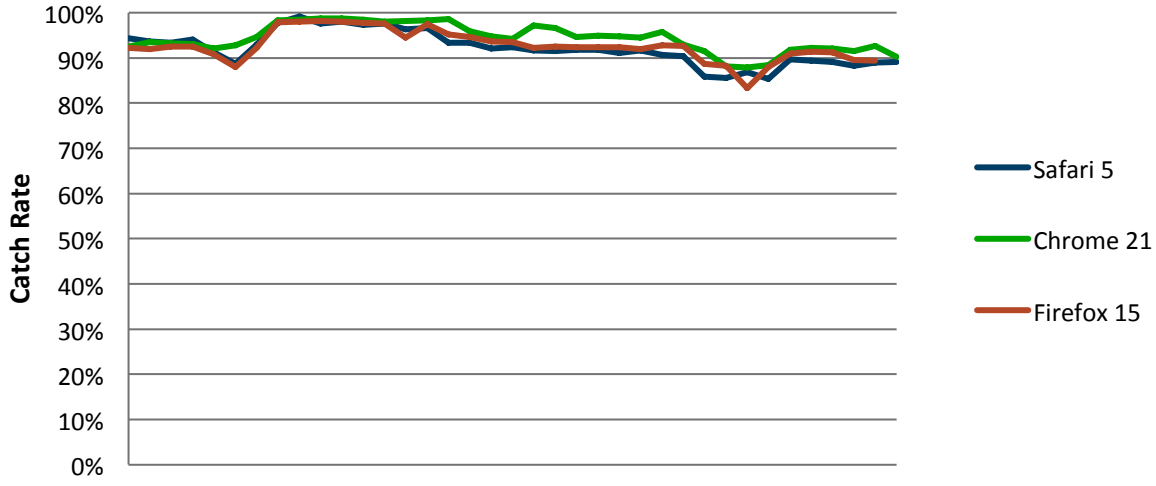


Figure 5 - Phishing Protection Over Time – SafeBrowsing Products

Conclusion

Web browsers are in a unique position to combat phishing and other criminal activities by warning potential victims that they are about to stray onto a malicious website. Since phishing sites have an average lifespan of only 23 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 now block substantially more phishing sites in the first 24 hours of detection than they did after 5 days in 2009.

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.

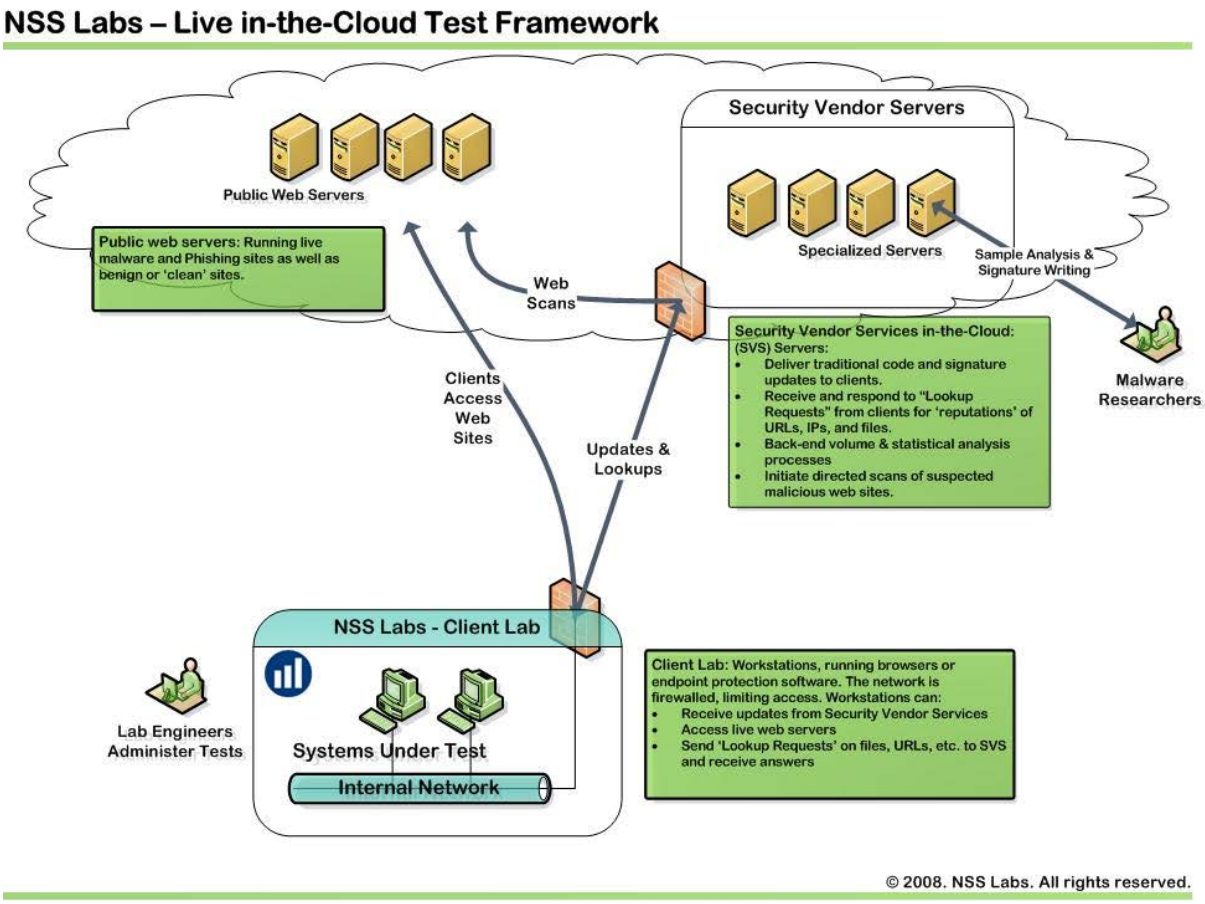
Google Chrome's overall block rate of 94% was 2.25% above the average, which, with a 2% margin of error, means that there is very little difference between the overall ability of the tested browsers to block phishing URLs.

Looking back to 2009 when the best browser blocked 83% and the worst a mere 2%, it is obvious that all of the tested vendors have made significant strides in their abilities to block phishing attacks. Going forward, the challenge will be to bring down the response time, especially for targeted brands with the largest consumer bases.

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 Labs Browser Security Comparative Analysis: Socially Engineered Malware provides essential information with respect to the ability of browsers to block socially engineered malware attacks.

Appendix A: Test Environment

NSS Labs 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 Labs created a unique "Live Testing™" harness in order to duplicate user experiences under real world conditions. 158,635 individual tests (URL lookups) were performed over a period of 10 days (37 discrete test runs).



Client Host Description

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

- Microsoft Windows 8
- 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 Labs. Generally available software releases were used in all cases, except for Internet Explorer 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
- Google Chrome 21
- Microsoft Internet Explorer 10
- Mozilla Firefox 15

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.

Network Description

The browsers were tested for their ability to protect the client in "connected" use cases. Thus, the tests consider and analyze the effectiveness of browser protection in NSS Labs' real-world, Live Testing harness.

The host system has one network interface card (NIC) and is connected to the network via a 1Gb switch port. For the purposes of this test, NSS Labs utilized up to 32 desktop systems each running a web browser – eight each per web browser (four browser types). Results were recorded into a MySQL database.

Appendix B: General Test Procedures

The purpose of the test is to determine how well the tested web browsers protect users from phishing threats on the Internet today. A key aspect is the timing. Given the rapid rate and aggressiveness with which criminals propagate and manipulate phishing URLs, a key objective is to ensure that the "freshest" sites possible are included in the test.

NSS Labs has developed a unique proprietary "Live Testing™" harness and methodology. On an ongoing basis, NSS Labs collects web-based threats from a variety of sources, including partners and its own servers. Potential threats are vetted algorithmically before being inserted into the test queue. Threats are being inserted and vetted continually 24x7. Note: unique to this procedure is that NSS Labs validates the samples before *and* after the test. Actual testing of the threats occurs every two hours and starts with validation of the site's existence and conformance to the test definition.

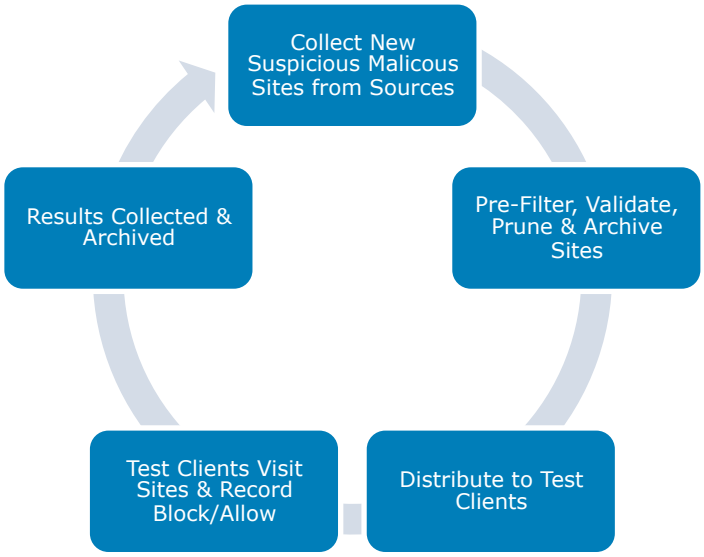
All tests are executed in a highly controlled manner, and results are meticulously recorded and archived at each interval of the test.

Test Duration

This NSS Labs' browser test is performed continuously (24x7) for 10 days. Throughout the duration of the test, new URLs are added as they are discovered.

Test Frequency

Over the course of the test, each URL is run through the test harness every six hours. Regardless of success or failure, the "victim machine" in the test harness will attempt to browse to the phishing site for the duration of the test.



Samples Sets For Phishing URLs

Freshness of phishing sites is a key attribute of this type of test. In order to utilize the freshest most representative URLs, NSS Labs receives a broad range of samples from a multiple sources.

Sources

NSS Labs operates its own network of spam traps and honeypots. These email accounts with high- volume traffic yield thousands of unique emails and URLs per day. NSS Labs maintains a growing archive of phishing and malicious URLs and other malware. This archive contains multiple gigabytes of confirmed samples. Although only phishing URLs are used in this test, some phishing URLs may also contain malware and exploits. In addition, NSS Labs maintains relationships with other independent security researchers, networks, and security companies that provide access to URLs and malicious content. Sample sets contain phishing URLs distributed via spam, social networks, and other websites. Every effort is made to consider submissions that reflect a real-world distribution of phishing, categorically, geographically, and by platform.

In addition, NSS maintains a collection of "clean URLs" that includes such sites as Yahoo, Amazon, Microsoft, Google, NSS Labs, major banks, etc. Periodically, clean URLs are run through the system to verify browsers are not over-blocking.

Catalog URLs

New sites are added to the URL *consideration set* as soon as possible following initial discovery. The date and time each sample is introduced is noted. Most sources are automatically and immediately inserted, while some methods require manual handling and can be processed in under 30 minutes. All items in the consideration set are cataloged with a unique NSS Labs ID, regardless of their validity. This enables NSS Labs engineers to track effectiveness of sample sources.

Confirm Sample Presence of URLs

Time is of the essence, since the objective is to test the effectiveness against the 'freshest' possible phishing sites. 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 the site could quickly disappear. However, each of the test items is given an initial review to verify it meets the basic criteria and is accessible on the live Internet.

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

This validation occurs within minutes of receiving the samples. Note: These classifications are further validated after the test, and URLs are reclassified and/or removed accordingly.

Archive Active URL Content

The active URL content is downloaded and saved to an archive server with a unique NSS ID number. This enables NSS Labs to preserve the URL content for control and validation purposes.

Visit Each URL

A customized client automation utility requests each of the URLs deemed "present" via each of the web browsers in the test. The test harness records whether or not the phishing site is successfully accessed, and if the attempt to visit the site triggers a warning from the browser's phishing protection.

Scoring & Recoding the Results

The resulting response is recorded as either "*allowed*" or "*blocked and warned*."

- **Success**: NSS Labs defines "success" based upon a web browser successfully preventing access to a phishing URL.
- **Failure**: NSS Labs defines a "failure" based upon a web browser failing to block and issue a warning.

Pruning

Throughout the test, lab engineers review and prune out non-conforming URLs and content from the test execution set. For example, a URL that was classified initially as phishing and that has subsequently been replaced by the web host with a generic splash page will be removed from the test.

If a URL sample becomes unavailable during the course of the test, the sample is removed from the test collection for that iteration. NSS Labs continually verifies each sample's presence (availability to access) and adds/removes each sample from the test set accordingly. Should a phishing sample be unavailable for a test iteration and then become available again for a subsequent iteration, it will be added back into the test collection. Unavailable samples are not included in calculations of success or failure by a web browser.

Post-Test Validation

Post-test validation enables NSS Labs to reclassify and even remove samples which were either not malicious or not available before the test started. NSS Labs performs both automated and manual validation of suspected phishing sites. At the end of this process, there were 2,291 URLs that were live and valid at the time of testing and are now part of this report. The targeted brands are in the table below.

ABN-AMRO	ABSA	AhliUnitedBank	Alibaba
Alipay	Allegro	AlliedDirect	Amazon
AmBankGroup	AOL	ASB	BancoAVVillas
BancoAzteca	BancoBOD	BancoDeEspana	BancoDelaNacion
BancoDeVenezuela	BancoFalabella	Bancopichincha	BankOfBrazil
BankOfchina	BankWest	Barclays	Battle.Log
Battle.net	BienvenuedansAccesD	BMO	BOA
Bradesco	BT	Cadastro	CapitalBank
CapitecBank	CartaSi	CenturyLink	Chase
ChinaBank	ChinaConstructionBank	CIBC	Cielo
CIMB	Co-Operativebank	CommonwealthBank	DBA
DiamondBank	Ebay	Email	Facebook
FirstOnline	GlobalMail	GlobalSources	Gmail

Halifax	HelpDesk	HiperCard	HomeBank
HongLeong	Hotmail	HSBC	ICBC
ING	InternalRevenueService	IRS	Itau
Kiwi	LaBanquePostale	LibertyReserve	Linkedin
Lloyds	MailBox	MasterCard	MayBank
MBNA	MicrosoftAccount	NAB	NatWest
Nets	Nordea	Outlook	PaEbay
Paypal	PNC	Popular	Posteitaliane
postepay	QNB	QuickQuid	RAKBank
RBC	Regions	ReMax	RuneScape
Santander	SFR	Sicredi	Skype
Smiles	St.george	Steam	Suntrust
TAM	TDCanadaTrust	TradeMe	TSB
TSBBank	USAA	Vadofone	Verizon
Very	VISA	Vodafone	WebMail
Wellsfargo	Westpac	WindowSecurity	WindowsSecurity
Yahoo			

Contact Information

NSS Labs, Inc.
6207 Bee Caves Road, Suite 350
Austin, TX 78746 USA
+1 (512) 961-5300
info@nsslabs.com
www.nsslabs.com