



WEB BROWSER SECURITY
PHISHING PROTECTION
COMPARATIVE TEST RESULTS



APPLE SAFARI 4
GOOGLE CHROME 2
MICROSOFT WINDOWS INTERNET EXPLORER 8
MOZILLA FIREFOX 3
OPERA 10 BETA

METHODOLOGY VERSION: 1.2
JULY 20, 2009

Published by NSS Labs.

© 2009 NSS Labs

CONTACT:

NSS Labs
P.O. Box 130573
Carlsbad, CA 92013

Tel: +1.512.961.5300
E-mail: info@nsslabs.com
Internet: <http://www.nsslabs.com>

All rights reserved. No part of this publication may be reproduced, photocopied, stored on a retrieval system, or transmitted without the express written consent of the authors.

Please note that access to or use of this Report is conditioned on the following:

1. The information in this Report is subject to change by NSS Labs without notice.
2. The information in this Report is believed by NSS Labs to be accurate and reliable, but is not guaranteed. All use of and reliance on this Report are at your sole risk. NSS Labs is not liable or responsible for any damages, losses or expenses arising from any error or omission in this Report.
3. NO WARRANTIES, EXPRESS OR IMPLIED ARE GIVEN BY THE NSS LABS. ALL IMPLIED WARRANTIES, INCLUDING IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT ARE DISCLAIMED AND EXCLUDED BY NSS LABS. IN NO EVENT SHALL NSS LABS BE LIABLE FOR ANY CONSEQUENTIAL, INCIDENTAL OR INDIRECT DAMAGES, OR FOR ANY LOSS OF PROFIT, REVENUE, DATA, COMPUTER PROGRAMS, OR OTHER ASSETS, EVEN IF ADVISED OF THE POSSIBILITY THEREOF.
4. This Report does not constitute an endorsement, recommendation or guarantee of any of the products (hardware or software) tested or the hardware and software used in testing the products. The testing does not guarantee that there are no errors or defects in the products, or that the products will meet your expectations, requirements, needs or specifications, or that they will operate without interruption.
6. All trademarks, service marks, and trade names used in this Report are the trademarks, service marks, and trade names of their respective owners, and no endorsement of, sponsorship of, affiliation with, or involvement in, any of the testing, this Report or NSS Labs is implied, nor should it be inferred.

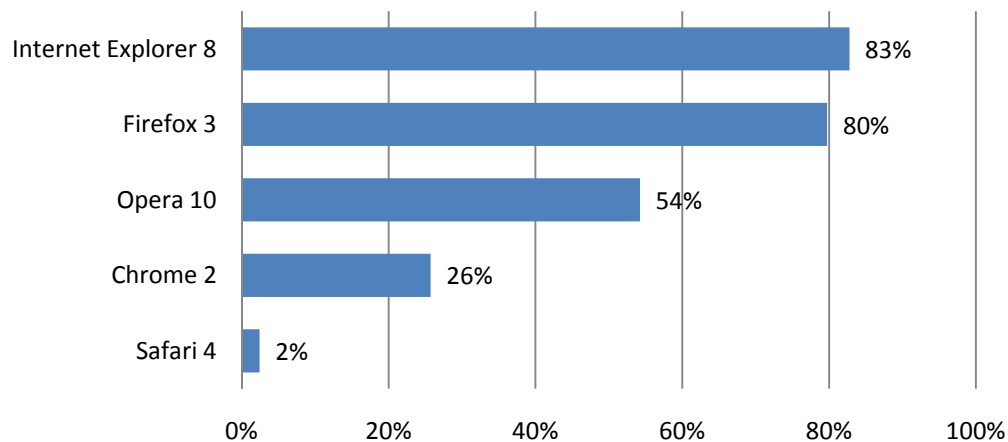
EXECUTIVE SUMMARY

During July, 2009 NSS Labs performed the industry's first comprehensive test of web browser phishing protection against our live web browser security testing methodology v1.2. This report is based upon empirically validated evidence gathered by NSS Labs during 14 days of 24x7 testing, performed every 4 hours, over 80 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.

Note: This test was performed alongside a similar test of socially engineered malware (see: www.nsslabs.com/browser-security). 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 our initial research. While drive-by downloads and click-jacking are also effective attacks and have achieved notable publicity, they represent a smaller percentage of today's threats,

The average phishing URL catch rate for browsers over the entire 14 day test period ranged from 2% for Safari 4 to 83% for Windows Internet Explorer 8. Internet Explorer 8 and Firefox 3 were the most consistent in the high level of protection they offered. Statistically, Internet Explorer 8 and Firefox 3 had a two-way tie for first, given the margin of error of 3.96%. Opera 10 beta came in third due to inconsistent protection during the test. Chrome 2 was consistent, albeit at a much lower rate of protection, and Safari offered minimal overall protection.

Mean Block Rate for Phishing



Generally available software releases were used in all cases except for Opera 10 which was in late beta and deemed to be sufficiently stable for testing. Each product was updated to the most current version available at the time testing began, with the exception of Mozilla Firefox. We would have liked to have been able to test Firefox 3.5 which was released June 30, 2009, and attempted to test it alongside the other browsers. However, serious instability where the browser repeatedly crashed (a widely reported issue) along with poor results prevented its inclusion for the sake of fairness.

Internet Explorer 8 achieved an overall block rate of 83% during our extended testing,

Firefox 3 achieved an overall block rate of 80% during our extended testing.

Opera 10 Beta achieved an overall block rate of 54% during our extended testing. NOTE: It appeared that Opera experienced operational issues during the latter part of testing which dragged down Opera 10's effectiveness. Prior to those issues, Opera 10 was comparable with Internet Explorer 8 and Firefox 3.

Chrome 2 achieved an overall block rate of 26% during our extended testing.

Safari 4 achieved an overall block rate of 2% during our extended testing.

Given that Safari 4, Chrome 2, and Firefox 3.0.11 share a feed from Google's SafeBrowsing API, these results indicate that utilizing the API itself is not an indicator of protection capabilities.

CONTENTS

1	<i>Introduction</i>	1
1.1	The Phishing Threat	1
1.2	Web Browser Security	1
2	<i>Effectiveness Results</i>	2
2.1	Test Composition – Phishing URLs	2
2.2	Blocking Phishing URLs	2
2.3	Real-Time Blocking of Phishing URLs Over Time	4
2.4	SafeBrowsing Analysis	5
2.5	Safari 4 on Mac vs. Windows	5
3	<i>Conclusion</i>	7
4	<i>Appendix A: Test Environment</i>	8
4.1	Client Host Description	8
4.2	The Tested Browsers	9
4.3	Network Description	9
5	<i>Appendix B: General Test Procedures</i>	10
5.1	Test Duration	10
5.2	Sample sets for Phishing URLs	10
5.3	Catalog URLs	11
5.4	Confirm Sample Presence of URLs	11
5.5	Visit each URL	11
5.6	Pruning	12
5.7	Post-test validation	12
6	<i>Appendix C: Safari Mac vs. Windows Test Procedures</i>	12
6.1	Test Composition – Phishing URLs	12
7	<i>Appendix D: Test Infrastructure</i>	15

1 INTRODUCTION

Without a doubt, there have always been con artists and other criminals who utilize *social engineering* techniques to commit fraud. In this report, we studied several web browsers' ability to protect against phishing. In a parallel report, we studied the protection capabilities of web browsers against socially engineered malware. (see: www.nsslabs.com/browser-security)

1.1 THE PHISHING THREAT

"Phishing" is an Internet-based fraud where victims are persuaded to part with valuable personal information such as credit card or social security numbers, and other confidential information via a website that appears to be legitimate. The explosion of alluring web 2.0 applications and other social media has provided a fertile environment for spreading phishing attacks. For the purposes of this test the following definition is used for a phishing URL: *the URL both falsely impersonates another entity and attempts to trick the user into disclosing personal information via a web form.*

Phishing attacks pose a significant risk to individuals and organizations alike by threatening to compromise or acquire sensitive personal and corporate information. In 2008 and early 2009 statistics show no abatement of the trend. And indeed, detecting and preventing these threats continues to be a challenge as criminals remain aggressive. The Anti-phishing Working Group (APWG) estimated more than 47,000 unique attacks in the second half of 2008 with an average lifespan of 52 hours.¹ Increasingly, web 2.0, instant messaging, and other social engineering techniques are being used to quickly distribute phishing attacks and evade traditional security programs. The speed at which these threats are 'rotated' to new locations is staggering and poses a significant challenge.

In response to this trend, security vendors have developed reputation systems which classify malicious and phishing URLs via in-the-cloud services. 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.

1.2 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 five different web browsers to protect users from live phishing attacks.

The foundation is an in-the-cloud reputation-based system which 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 some combination thereof. 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.

¹ Anti-Phishing Working Group, http://www.antiphishing.org/reports/apwg_report_H2_2008.pdf, pg. 11

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. Most programs include some 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.

2 EFFECTIVENESS RESULTS

2.1 TEST COMPOSITION – PHISHING URLS

Data in this report spans a testing period of just over 14 days, from July 7 through July 20. All testing was performed in our lab in Austin, TX. During the course of the test, we 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. See the methodology for more details.

2.1.1 TOTAL NUMBER OF MALICIOUS URLS IN THE TEST

Throughout the course of this study, 55,922 unique results were collected from 80 discrete tests conducted without interruption over 320 hours (every 4 hours for 14 days). From a collection of over 3,219 URLs, 856 were available at the time of entry into the test and were successfully accessed by the browsers in at least one run. We removed samples that did not pass our validation criteria, including those tainted by exploits (not part of this test). Thus, ultimately 593 unique URLs were included in our final set of phishing sites – providing a margin of error of 3.96% with a 95% confidence interval.

2.1.2 AVERAGE NUMBER OF MALICIOUS URLS ADDED PER DAY

On average, 61 new validated URLs were added to the test set per day. Although certain days more or less were added as criminal activity levels fluctuated.

2.1.3 MIX OF URLS

The mixture of URLs used in the test was representative of the threats on the Internet. Care was taken not to overweight any one domain to represent more than 10% of the test set. Thus a number of sites were pruned after reaching their limit.

2.2 BLOCKING PHISHING URLS

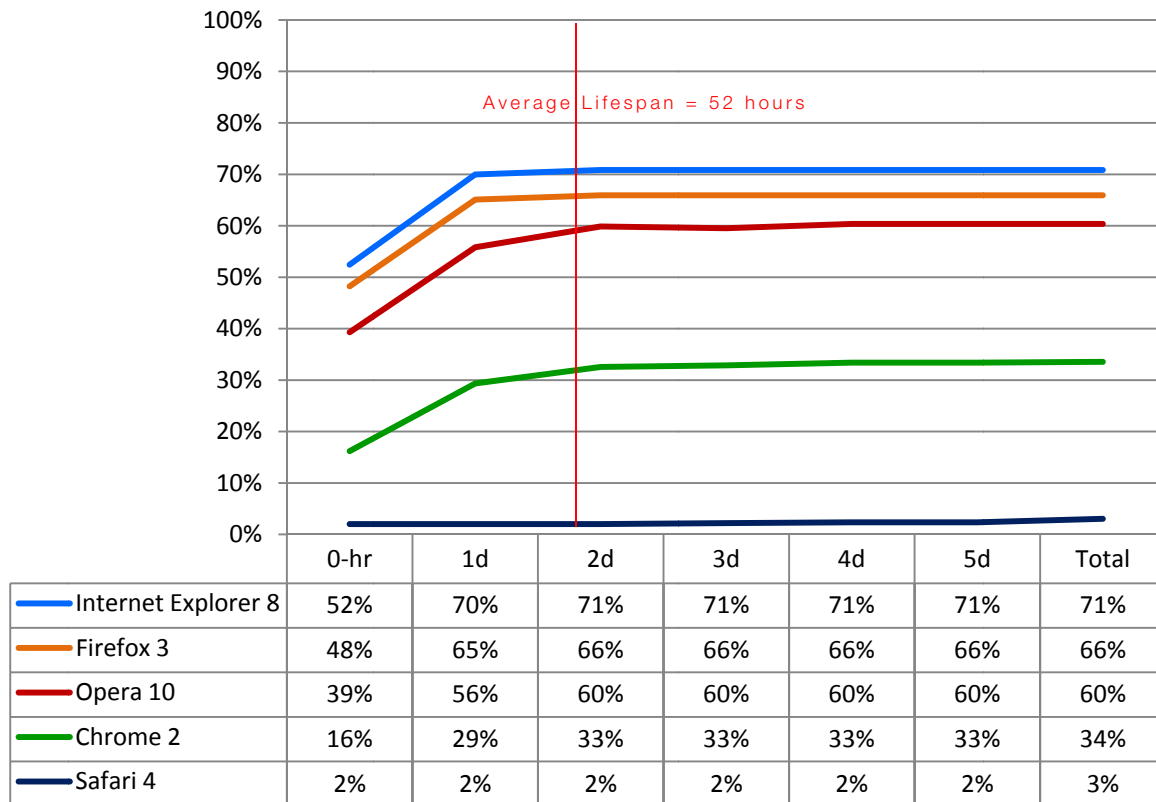
NSS Labs assessed the browsers’ ability to block malicious URLs as quickly as we found them on the Internet. We continued testing them every four hours to determine how long it took a vendor to add protection, if they did at all.

2.2.1 AVERAGE TIME TO BLOCK PHISHING URLS

The following histogram shows how long it took the browsers under test to block the 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 greatly between 2% (Safari 4) and 83% (Internet Explorer 8). Internet Explorer 8 demonstrated the strongest protection for zero-hour phishing attacks at 52%, adding 18% during the first 24 hours and only 1% over the rest of the test. Although Firefox 3 and Opera 10 started lower at 48% and 39% respectively, they caught up quickly, achieving their maximum protection rates within 2 days.

Phishing URL Response Histogram



Longer-term blocking of phishing sites was comparable across Internet Explorer 8 (71%), Firefox 3 (66%), and Opera 10 Beta (60%). However, Safari 4 and Chrome 2 exhibited considerably lower protection rates, 3% and 34% respectively. Although Firefox, Safari and Chrome share the SafeBrowsing API, their results are very different. This speaks to the impact of different implementations.

2.2.2 AVERAGE RESPONSE TIME TO BLOCK PHISHING

This table answers the question: how long on average must a user wait 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.”

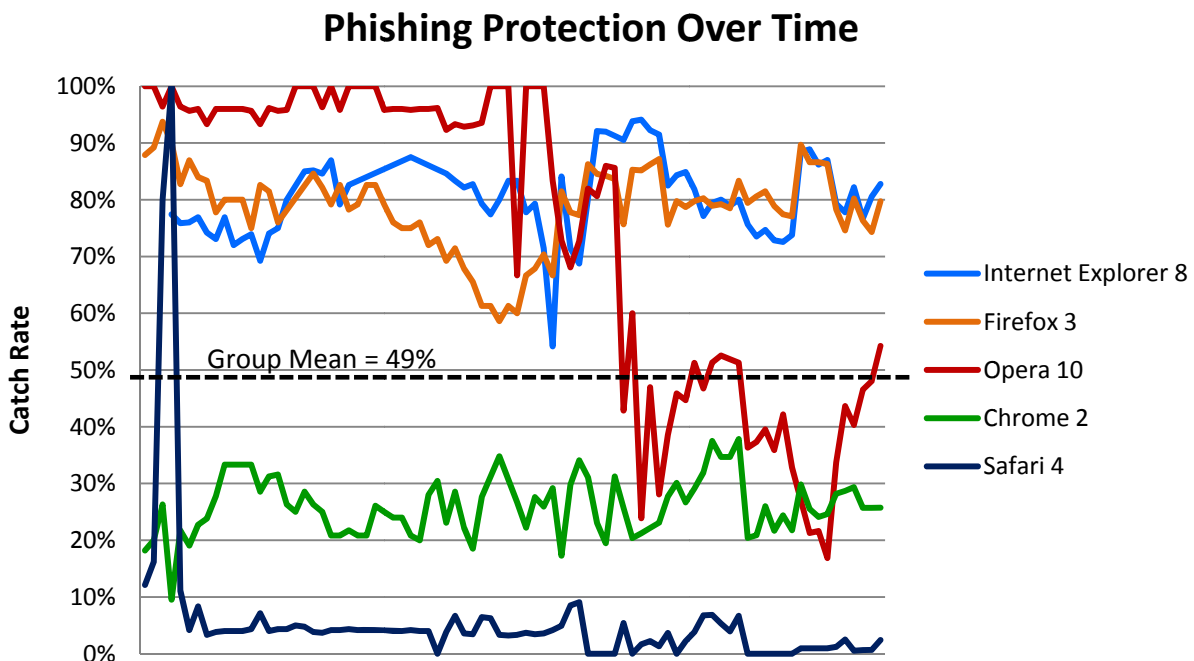
Note that phishing sites have an average life expectancy of only 52 hours.

Browser	Avg. Add Time (hrs)
Internet Explorer 8	4.96
Firefox 3	5.24
Opera 10 Beta	6.19
Chrome 2	11.08
Safari 4	54.67
<i>mean</i>	<i>16.43</i>

The mean time to block a site (if it is blocked at all) is 16.43 hours. Thus, only Safari was below average at adding new blocks.

2.3 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 which may change quickly. Thus, at any given time, the available set of phishing URLs is revolving, and continuing to block these sites is a key criteria for effectiveness. NSS Labs tested a set of live URLs every four hours. The graph below shows protection at each of the 80 incremental tests of over a period of 14 days. Each score represents protection at a given point in time. The mean protection rate over time for all browsers was 46%.

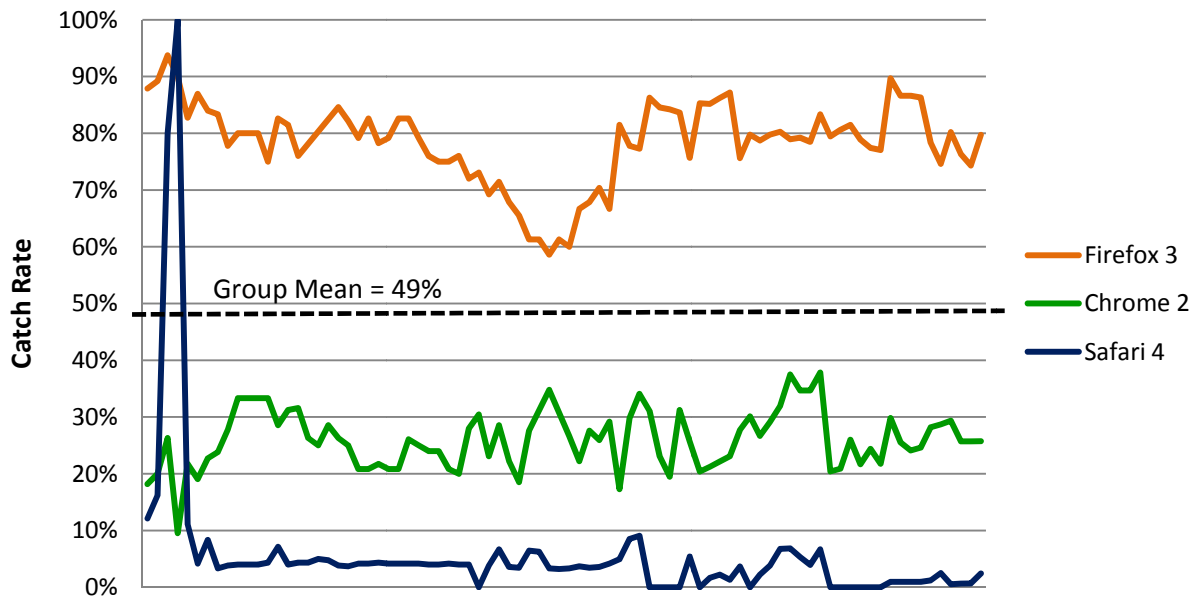


Note that the protection percentage will deviate from the unique URL results for several reasons. First, this data includes multiple tests of a URL. So if it is blocked early on, it will improve the score. If it continues to be missed, it will detract from the score. Thus, results of individual URL tests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

2.4 SAFE BROWSING ANALYSIS

Even though Chrome 2, Firefox 3 and Safari 4 all use the Google SafeBrowsing data feed, our testing detected vastly different results in terms of effectiveness in blocking phishing URLs. There could be any number of explanations for this variance, though no explanations were provided by the developers. However, we do know that each browser contacts the respective developer's site directly, and this is one point in the communication channel where additional decisions could be made.

Phishing Protection Over Time - SafeBrowsing Products



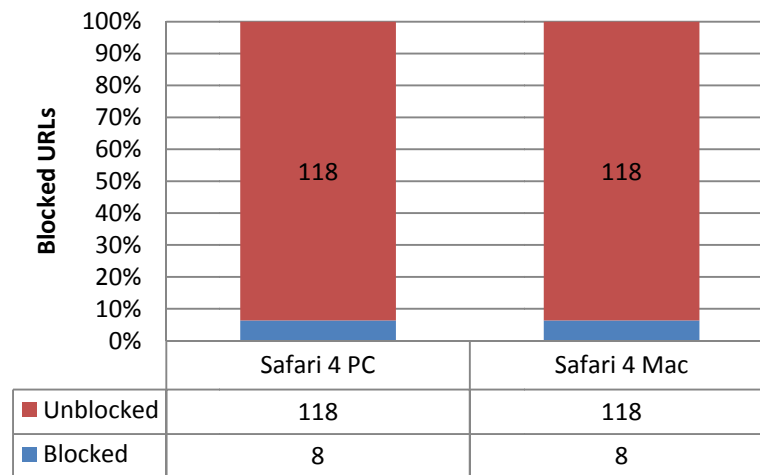
Fundamentally, each browser or intermediary server may implement the API differently; calling it at different times with different parameters, and determining blocks differently. Further, as an open source project, Mozilla's implementation uses a different database structure and access method from the other two proprietary browsers.

2.5 SAFARI 4 ON MAC VS. WINDOWS

NSS Labs evaluated the anti-phishing effectiveness of Apple's Safari 4 browser on both Microsoft Windows 7 and Macintosh OSX platforms. Our testing determined that Apple's anti-phishing service is common across all platforms, and protection on one platform is indicative of protection on another. The Windows version and Mac version of Safari 4 performed identically to each other – offering the same protection for each of the tested URLs.

The blocking of phishing sites was exactly identical across both systems. URL's that were blocked by System A were also blocked by System B. Conversely URL's that were not blocked by System A were also not blocked by System B.

Safari Phishing Block Rate - Mac vs. Windows



2.5.1 BLOCK PERCENTAGE

Out of a total of 126 valid phishing URL's, each system blocked 8 URL's, exhibiting an identical protection rate of 6.3%. This 6.3% should not be confused with Safari's overall block rate of 2% and is an artifact of testing a smaller sample set towards the end of the overall test. Furthermore, this block score was in line with the results of long term testing conducted previously.

In order to quickly achieve a high number of sites to test, NSS Labs 'reached back' 2 days to pull up older phishing sites, which we tested all on the same day over a 4 hour window of time. However, due to the short lifespan of phishing sites, very few older sites were included in this test. And thus, a high percentage of the sites were less than 1 day old.

3 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 52 hours (just over 2 days) 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.

The developers at both Microsoft and Mozilla clearly understand this relationship and respond quickly to block new phishing sites. Thus, with an overall catch rate of 83% and 80% respectively, and a margin of error of 3.96%, Internet Explorer 8 and Firefox 3 were statistically tied.

Opera was third in our tallies with an overall block rate of 54%. However data indicates that it was a solid third, and results were dragged down by a period when protection dropped off significantly during the second half of testing.

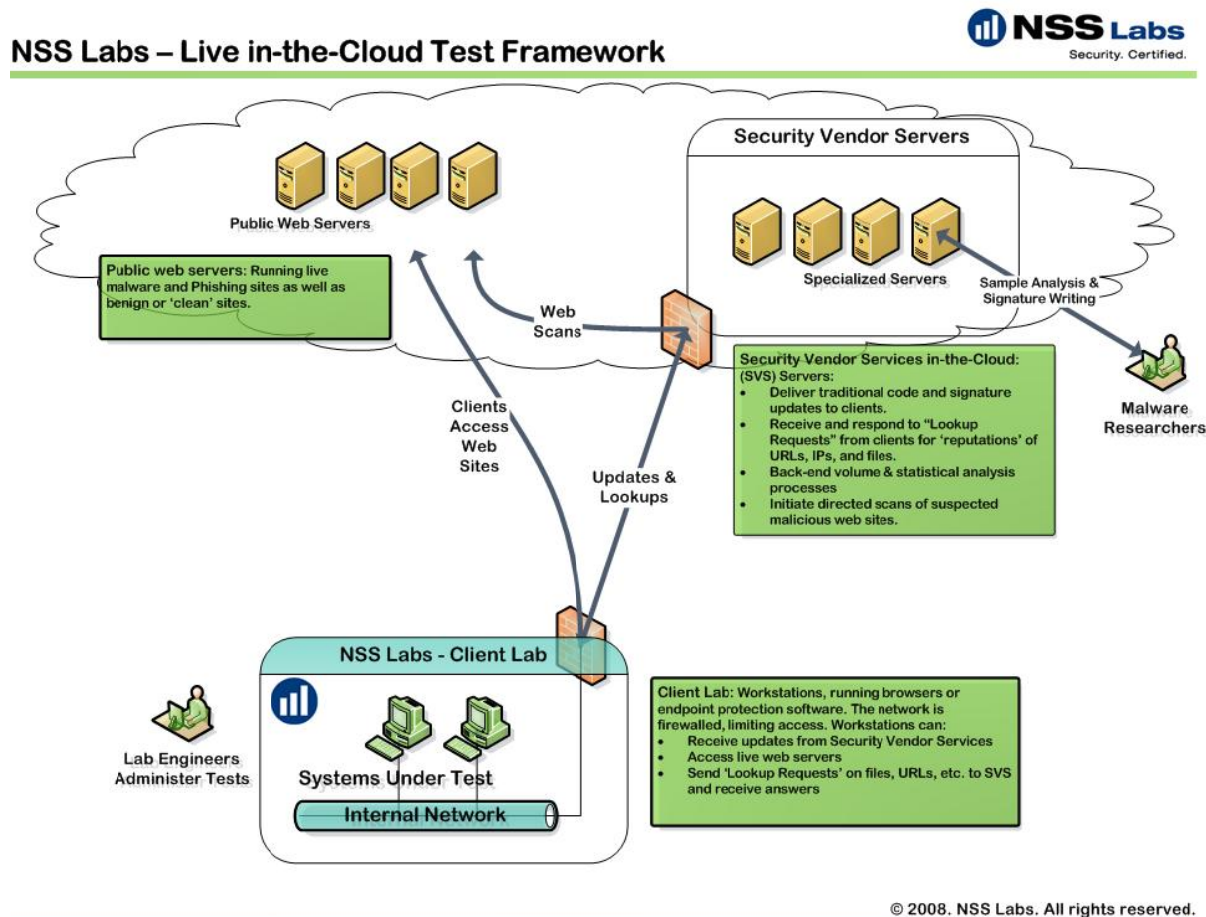
Google Chrome's overall catch rate of 26% was below average. We expected better results given the fanfare about Google's SafeBrowsing initiative. Additionally, a third-party (Firefox) was able to utilize Google's API to achieve significantly better protection than Google's own browser.

Safari 4 achieved an overall block rate of a mere 2%. Test results further indicate that Safari 4's phishing protection is identical on Mac and Windows operating systems.

4 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, whilst also maintaining control and verification of the procedures.

For this browser security test, NSS Labs created a “Live” test lab environment in order to duplicate user experiences under real world conditions. 40,891 individual tests (URL lookups) were performed over a period of 14 days (80 discrete test runs).



4.1 CLIENT HOST DESCRIPTION

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

Microsoft Windows 7 RC (Build 7100)

- 1GB RAM
- 8GB HD

Mac Mini – OSX 10.5.6

- 1GB RAM
- 8GB 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.

4.2 THE TESTED BROWSERS

The browsers, or products under test, were obtained independently by NSS Labs. Generally available software releases were used in all cases, except for Opera 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:

- Microsoft Windows Internet Explorer 8 (build 8.0.7100.0)
- Google Chrome v2.0.172.33
- Apple Safari v4.0.2 (530.19.1)
- Mozilla Firefox v3.0.11
- Opera 10 Beta – v10.00b1 (build 1551)

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 antivirus, IPS and general software practices.

4.3 NETWORK DESCRIPTION

The browsers were tested for their ability to protect the client in “connected” use cases. Thus, our tests consider and analyze the effectiveness Browser Protection in NSS Labs’ real-world, live Internet testing harness.

The host system has one network interface card (NIC) and is connected to the network via a 1Gb switch port. The NSS Labs test network is a multi-Gigabit infrastructure based around Cisco Catalyst 6500-series switches (with both fiber and copper Gigabit interfaces).

For the purposes of this test, NSS Labs utilized up to 20 desktop systems each running a web browser – four (4) each per web browser (5 browser types). Results were recorded into a MySQL DB.

5 APPENDIX B: GENERAL TEST PROCEDURES

The purpose of the test was to determine how well the tested web browsers protect users from phishing threats on the Internet today. A key aspect was the timing. Given the rapid rate and aggressiveness with which criminals propagate and manipulate phishing URLs, a key objective was to ensure that the “freshest” sites possible were 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 our own servers. Potential threats are vetted algorithmically before being inserted into our test queue. Threats are being inserted and vetted continually 24x7. Note: unique in this procedure is that NSS Labs validates the samples before and after the test. Actual testing of the threats proceeded every two hours and starts with validation of the site’s existence and conformance to the test definition.

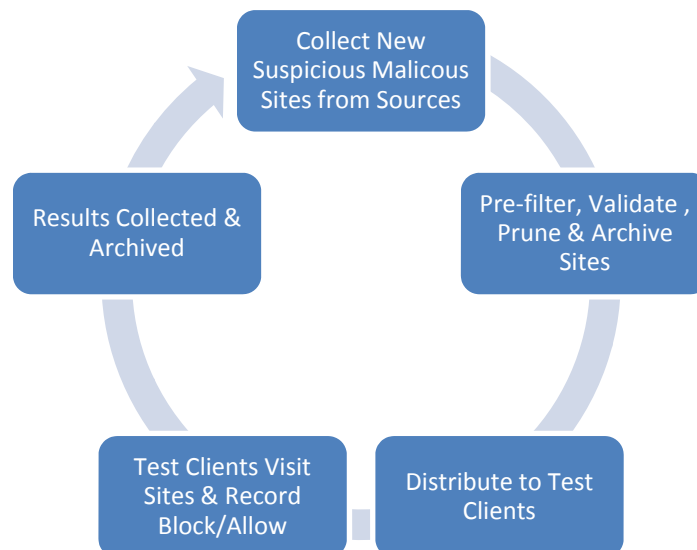
All tests are executed in a highly controlled manner, and results are meticulously recorded and archived at each interval of the test.

5.1 TEST DURATION

This NSS Labs’ browser test was performed continuously (24x7) for 14 days. Throughout the duration of the test, new URLs were added as they were discovered.

5.1.1 TEST FREQUENCY

Over the course of the test, each URL is run through the test harness every four hours, regardless of success or failure, NSS Labs attempted to visit the phishing site with the web browser for the duration of the test.



5.2 SAMPLE 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 number of different sources.

5.2.1 SOURCES

First, 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 that contains Gigabytes of confirmed samples. Although only phishing URLs were 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, which provide access to URLs and malicious content. Relevant to this test, these include: Sunbelt's Threat Track, Mailshell, Telus Security Labs, and a variety of other Enterprises who wish to remain anonymous. Sample sets contain phishing URLs distributed via: SPAM, Social networks, and other websites. Every effort was 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' which includes such sites as Yahoo, Amazon, Microsoft, Google, NSS Labs, major banks, etc. Periodically clean URLs were run through the system to verify browsers were not over-blocking.

5.3 CATALOG URLs

New sites are added to the URL Consideration Set as soon as possible. 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 enabled us to track effectiveness of sample sources.

5.4 CONFIRM SAMPLE PRESENCE OF URLs

Time is of the essence since the test objective is to test the effectiveness against the 'freshest' possible phishing sites. Given the nature of the feeds and the velocity of change, it is not possible to validate each site in depth before the test, since the sites could quickly disappear. Thus, each of the test items is given an initial review to verify it meets the basic criteria, and was 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 occurred within minutes of receiving the samples from our sources. Note: These classifications are further validated after the test and URLs were reclassified and/or removed accordingly.

5.4.1 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.

5.5 VISIT EACH URL

A customized client automation utility (*AutomatedQA's*, *TestComplete*, and *TestExecute*) requests each of the URLs deemed 'present' via each of the web browsers in the test. NSS records whether or not the phishing Site was allowed to be navigated to, and if the attempt to visit the site triggered a warning from the browser's phishing protection.

5.5.1 SCORING & RECORDING 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.

5.6 PRUNING

Throughout the test, lab engineers review and prune out non-conforming URLs and content from the test execution set. e.g. a URL that was classified as phishing that has 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 navigate to) 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.

5.7 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 performed both automated and manual validation of suspected phishing sites.

6 APPENDIX C: SAFARI MAC VS. WINDOWS TEST PROCEDURES

6.1 TEST COMPOSITION – PHISHING URLS

Data in this report spans a period of 14 days, from July 7th to July 20th although the actual testing was completed in just 2 days, from July 18th to July 19th. All testing was performed in our lab in Austin, TX.

6.1.1 MIX OF URLS

Over the period from July 18th to July 19th a total of 218 phishing URLs were tested from 3 distinct sources. Care was taken to validate the URLs were live phishing sites and that the sample set did not overweight any one domain to represent more than 10% of the test set. Thus a number of sites were pruned after reaching their limit. The resulting set was thus reduced to 126 URL’s.

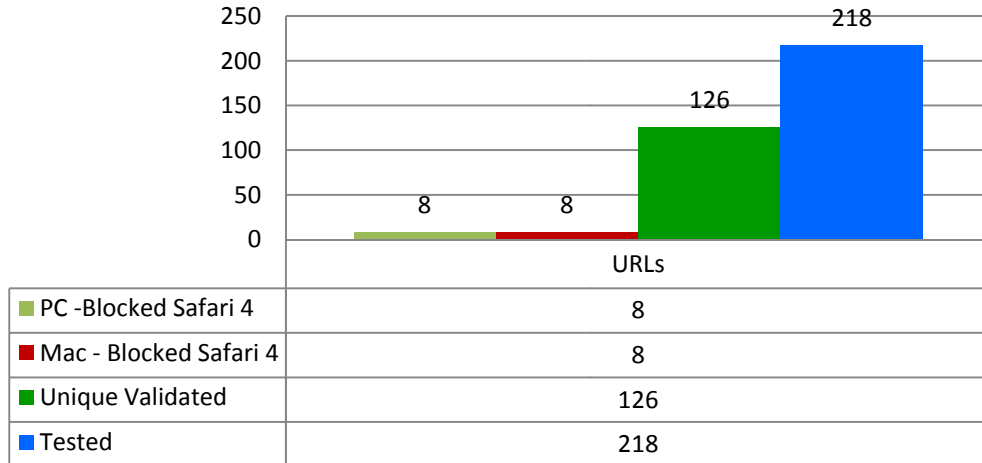
6.1.2 PRUNING PROCESS

Lab engineers reviewed and pruned out non-conforming URLs and content from the test execution set e.g. a URL classified as phishing, was replaced by the web host with a generic splash page, was removed from the test set.

We also ran an automated process to filter out URLs that did not meet certain other criteria; one of those being the site’s availability. Only those URLs that were live on the 19th of July were selected for further testing.

The pruning process narrowed our results to 126 live (validated) URLs.

Site List Overview



6.1.3 TESTING PROCESS

Each URL was tested manually by lab engineers over two time periods. The batches consisted of 95 and 91 URLs respectively. Thus a total of 186 URLs were tested, 126 of which were unique and 60 of which were duplicates – reflecting the relatively high turnover of phishing URLs.

Each set of URLs was tested simultaneously on System A and System B, by two lab engineers, each working independently. The test was broken into smaller chunks in order to ensure that each URL was tested across both systems at approximately the same time. This would avoid certain time-related issues such as sites going offline.

6.1.4 SCORING & RECORDING THE RESULT

Depending upon the test outcome each URL was assigned one of the following statuses

- a. B - URL was blocked by the browser
- b. U - URL was not blocked by the browser

In addition each URL was validated visually and was marked appropriately with the following:

- c. NF - Page not found, timeouts and other such errors
- d. V - If the phishing site appeared valid
- e. I - If the phishing Site appeared invalid

At the end of this process we had 126 URLs that were live and valid at the time of testing and are now part of this report.

Please refer to *Appendix D: Sample List of URLs* for the list of URL's that were tested.

6.1.5 ARCHIVE ACTIVE URL CONTENT

The active URL content was 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.

7 APPENDIX D: TEST INFRASTRUCTURE

Special thanks go to our test infrastructure partners who provide much of the equipment, software, and support that make this testing possible:

