NSS Labs

Security. Certified.

WEB BROWSER SECURITY

SOCIALLY ENGINEERED MALWARE PROTECTION COMPARATIVE TEST RESULTS 2ND EDITION

NSS Labs

TESTED

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.

CONTACT:

P.O. Box 130573
Carlsbad, CA 92013

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

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.

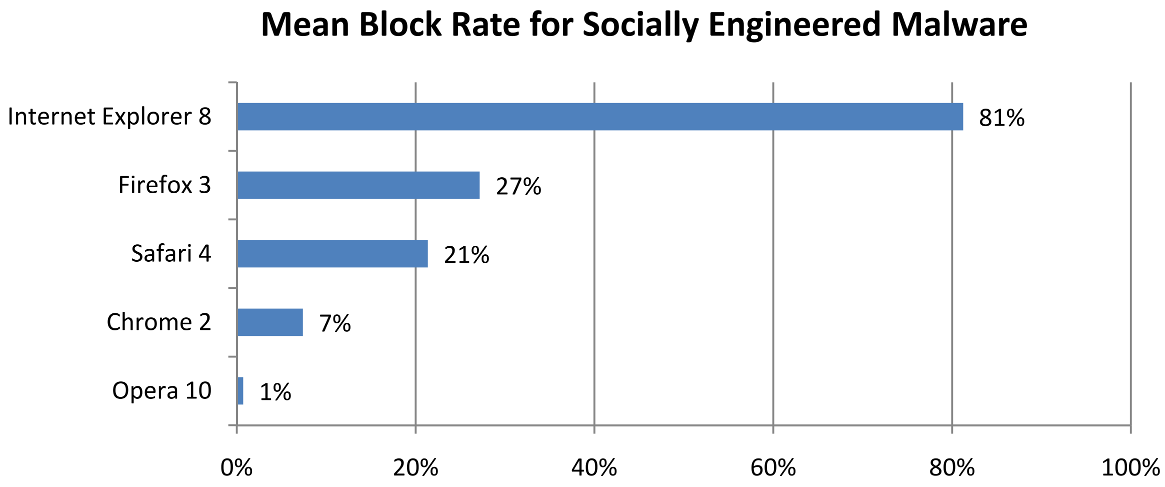
3. NO WARRANTIES, EXPRESS OR IMPLIED ARE GIVEN BY THE NSS LABS. ALL IMPLIED WARRANTIES, INCLUDING IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT ARE DISCLAIMED AND EXCLUDED BY NSS LABS. IN NO EVENT SHALL NSS LABS BE LIABLE FOR ANY CONSEQUENTIAL, INCIDENTAL 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 second test of web browser protection against socially engineered malware - the most common and impactful security threat facing Internet users today.[1] This report followed the same Live Testing methodology as the test conducted in Q1 2009, (see: www.nsslabs.com/browser-security). It is based upon empirically validated evidence gathered during 12 days of 24x7 testing, performed every 4 hours, over 69 discrete test runs, each one adding fresh new malware URLs. Each product was updated to the most current version available at the time testing began, and allowed access to the live Internet.



Internet Explorer 8 caught 81% of the live threats, an exceptional score which surpassed the next best browser (Firefox 3) by a 54% margin. Windows Internet Explorer 8 improved 12% between Q1 and Q2 tests, evidence of concerted efforts Microsoft is making in the SmartScreen technology.

Firefox 3 caught 27% of live threats, far fewer than Internet Explorer 8. It was, however, the best among products utilizing the Google SafeBrowsing API. (Note: Firefox 3.5 was not stable enough to be tested during the course of this test. A patch has subsequently become available to address the stability issue. We were able to manually verify that the protection was identical between versions 3.0.11 and 3.5).

Safari 4 caught 21% of live threats. Overall protection varied greatly, with two short periods of severe dips.

Chrome 2 caught just 7% of live threats an 8% drop from the previous test.

Opera 10 Beta caught a mere 1% of live threats, providing virtually no protection against socially engineered malware. In our test bed validation, we verified there was effectively no difference between Opera 9 and Opera 10 Beta.

[1] Note: This study does not compare browser security related to vulnerabilities in plug-ins or the browsers themselves.

CONTENTS

1 Introduction

1.1 The Socially Engineered Malware Threat

Socially engineered malware attacks pose a significant risk to individuals and organizations alike by threatening to compromise, damage or acquire sensitive personal and corporate information. 2008 and 2009 statistics show an acceleration of the trend. Detecting and preventing these threats continues to be a challenge as criminals remain aggressive. Antivirus researchers report detecting between 15,000 and 50,000 new malicious programs per day, and even as high as "millions per month," according to Kaspersky.[2]

While not all of these malicious programs are used in social engineering attacks, this technique is increasingly being applied to the web to quickly distribute malware and evade traditional security programs. 53% of malware is now delivered via internet download versus just 12% via email, while IFrame exploits and other vulnerabilities comprise 7% and 5%, respectively, of the global malware infection vectors, according to statistics from Trend Micro. [3] And as many as 0.5% of the download requests made through Internet Explorer 8 are malicious according to Microsoft.[4]

Criminals are taking advantage of the implied trust relationships inherent in social networking sites (e.g. Facebook, MySpace, LinkedIn, etc.) and user-contributed content (e.g. blogs, Twitter, etc.) which allow for rapid publishing and anonymity. Furthermore, the speed at which these threats are 'rotated' to new locations is staggering and poses a significant challenge to security vendors.

For clarity, the following definition is used for a socially engineered malware URL: a web page link that directly leads to a 'download' that delivers a malicious payload whose content type would lead to execution. These are links that appear to be safe, like a screen saver application, video codec upgrade, etc., designed to fool the user into downloading it. Security professionals also refer to these threats using different terms such as consensual or dangerous downloads.

1.2 Web Browser Security

Modern web browsers offer an additional layer of protection against these threats by leveraging in-the-cloud, reputation-based mechanisms to warn users. This report examines the ability of five different web browsers to protect users from socially engineered malware.[5] Each of the five web browsers has added

[2] Kaspersky, Eugene in http://www.examiner.com/x-11905-SF-Cybercrime-Examiner~y2009m7d17-Antimalware-expert-and-CEO-Eugene-Kaspersky-talks-about-cybercrime

[3] Cruz, Macky "Most Abused Infection Vector". *Trend Labs Malware Blog*, 7 Dec 2008. http://blog.trendmicro.com/most-abused-infection-vector/

[4] http://blogs.msdn.com/ie/archive/2009/03/25/ie8-security-part-ix-anti-malware-protection-with-ie8-s-smartscreen-filter.aspx

[5] Exploits that install malware without the user being aware (also referred to as "clickjacking" and "drive-by downloads") are not included in this particular study.

security technologies to combat web-based threats. However, not all of them have taken the same approach, nor claim to stop the same breadth of attacks.[6]

Browser protection contains two main functional components. 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.

When results are returned that a site is "bad", the web browser redirects the user to a warning message/page instructing that the URL was malicious. In the event that the URL is a download, the web browser instructs the user that the content about to be downloaded (or being downloaded) is malicious and that the download should be aborted / cancelled. 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 – Malicious URLs

Data in this report spans a testing period of 12 days, from July 7 through July 18 2009. 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. Throughout the course of this study, 69 discrete tests were performed (every 4 hours) without interruption for each of the 5 browsers.

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

From an initial list of 12,000 new suspicious sites, 2,171 potentially malicious URLs were pre-screened for inclusion in the test, and were available at the time of entry into the test. These 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 or that contained invalid samples. Of the initial 2,171 URLs, ultimately 608 URLs passed our post-validation process and are included in the final results – providing a margin of error of 3.91% with a confidence interval of 95%.

2.1.2 Average number of malicious URLs added per day

On average, 197 new validated URLs were added to the test set per day. Although certain days more or less were added as criminal activity levels fluctuated.

[6] Phishing protection was tested separately for technical reasons and is available in a companion report.

2.1.3 Mix of URLs

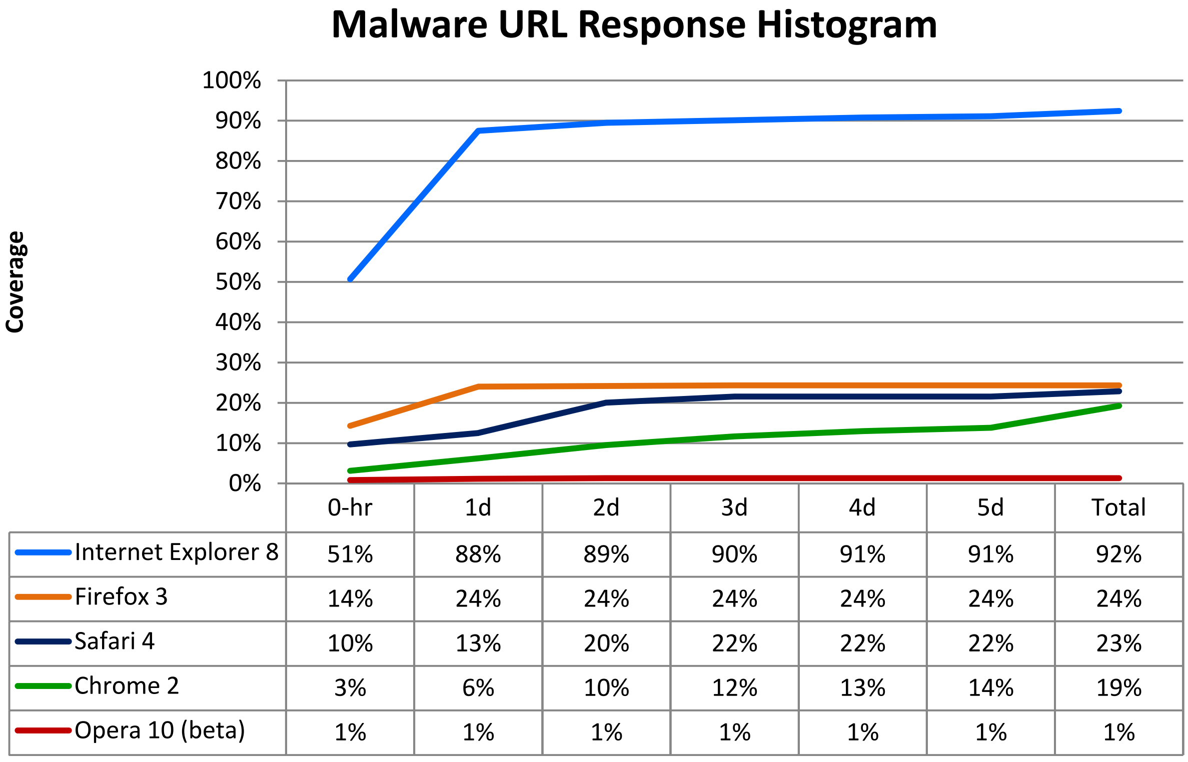
The mixture of URLs used in the test was representative of the threats on the Internet. Care was taken not to overweight any one domain to represent more than 10% of the test set. Thus a number of sites were pruned after reaching their limit.

2.2 Blocking URLs with Socially Engineered Malware

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 Malicious Sites

The following response time graph 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 for the 'zero hour', and then the first 5 days. Final protection scores for the URL test duration are summarized under the "Total" column. Generally, at least half of a browser's total protection was achieved in the zero hour. But, Internet Explorer 8 continued to add as much as 41% of additional protection over the course of the test. Other browsers added between just 0% and 16% over the course of the test.



	0-hr	1d	2d	3d	4d	5d	Total
Internet Explorer 8	51%	88%	89%	90%	91%	91%	92%
Firefox 3	14%	24%	24%	24%	24%	24%	24%
Safari 4	10%	13%	20%	22%	22%	22%	23%
Chrome 2	3%	6%	10%	12%	13%	14%	19%
Opera 10 (beta)	1%	1%	1%	1%	1%	1%	1%

Ultimately, the results reveal great variations in the abilities of the browsers to protect against socially engineered malware, with Internet Explorer 8 protecting users from 68% more unique malicious URLs than its nearest competitor, Firefox 3. Trends show Chrome 2, Safari 4, and Firefox 3 all converging at a protection rate just under 25%, indicating that while they all share the Google SafeBrowser feed, there is an operational difference in its implementation.

2.2.2 Average Response Time to Block Malware

In order to protect the most people, a browser's reputation system must be both fast and accurate. This table answers the question: how long on average must a user wait before a visited malicious site is added to the block list? It shows the average time to block a malware 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." Thus, while Opera 10 Beta recorded the fastest block time, it cannot be assumed that it therefore blocked more malware. In fact, it blocked the least of all the browsers.

The value of this table is in providing context for the *overall block rate,* so that if a browser blocked 100% of the malware, but it took 240 hours (10 days) to do so, it is actually providing less protection than a browser with a 70% overall block rate and an average response time of 10 hours.

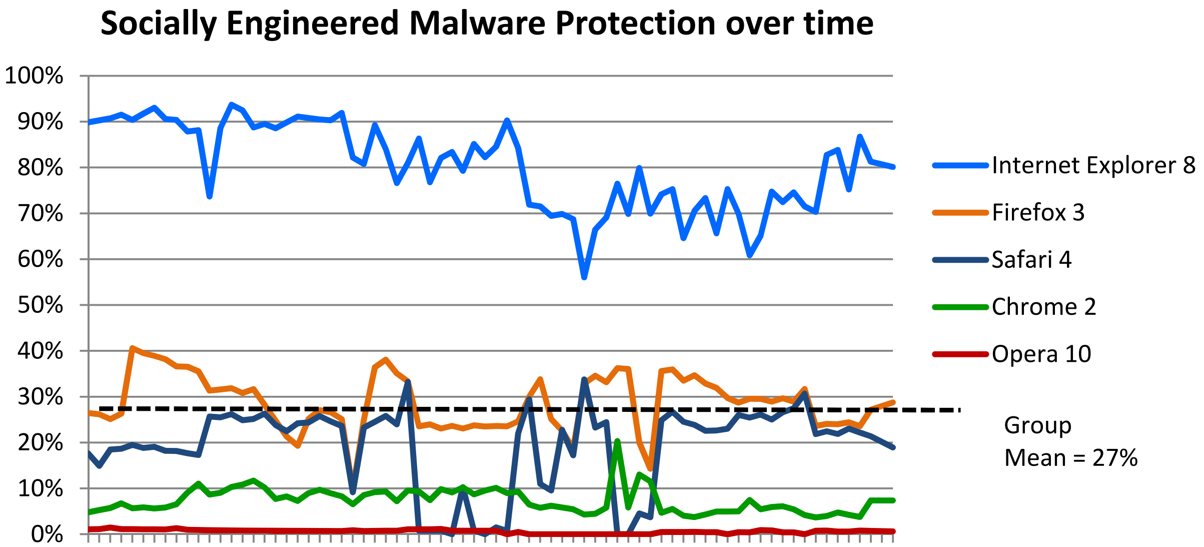
Browser	Avg. Add Time
Opera 10 Beta	5.5
Firefox 3	6.7
Internet Explorer 8	9.2
Safari 4	31.5
Chrome 2	76.8
mean	*25.9*

The mean time to block a site (if it is blocked at all) is 25.9 hours. Thus, Opera, Firefox and Internet Explorer were above average at adding new blocks.

2.3 Blocking URLs with Socially Engineered Malware 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 malicious URLs is revolving, and continuing to block these sites is a key criteria for effectiveness. Therefore, NSS Labs tested a set of live URLs every four hours. The following tables and graphs show the repeated evaluations of blocking over the course of 12 days, 69 test cycles for each of five browsers. Each score represents protection at a given point in time.

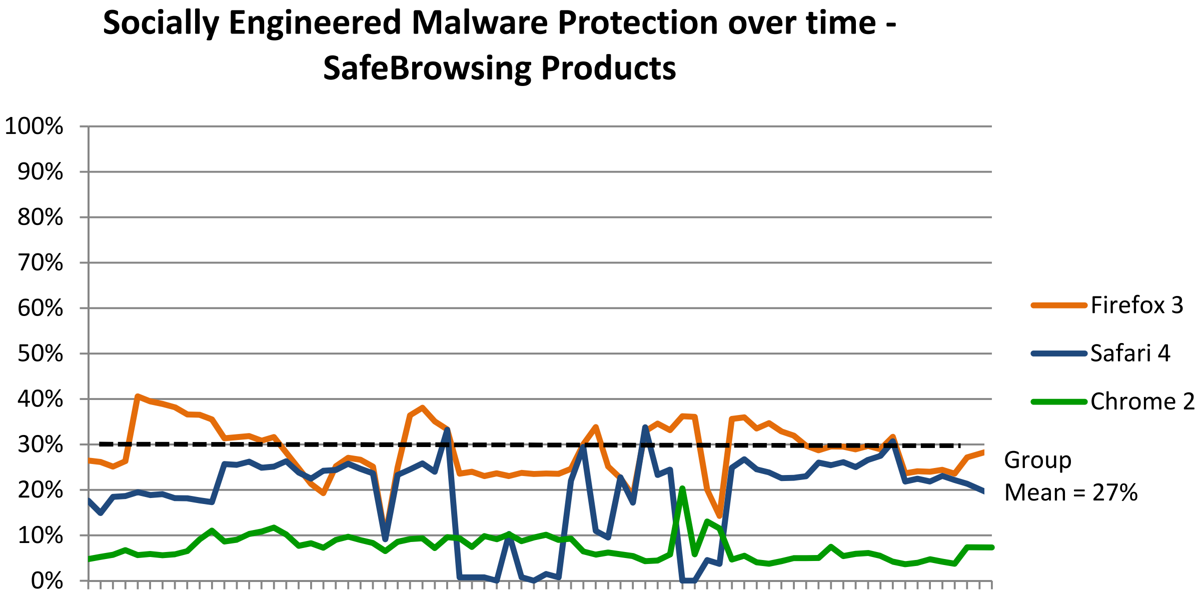
As seen on the graph, Internet Explorer 8 demonstrated a very high level of protection, but did fall off in the second half of the test and then show signs of recovery near the end. Safari was very inconsistent, with two short periods of severe dips in protection. Firefox ranged between 20% and 40%.



Note that the average 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 SafeBrowsing Products

Even though Chrome, Firefox and Safari all use the Google Safe Browsing data feed, our testing detected vastly different results in terms of effectiveness in blocking socially engineered malware 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.

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. Last, as mentioned in section 2.2.1 and indicated in the Malware URL Response Histogram, the SafeBrowsing products' protection rates were showing signs of converging just under 25%. This supports the notion that there are operational differences between the implementations of the API, but that the block lists are the same (or very similar).

2.5 Inter-Test Changes

Using the same test methodology on both the February and July 2009 tests allows for an easy apples-to-apples comparison of performance changes over time. As demonstrated by the table below, Internet Explorer 8 increased its protection by 12%, a considerable gain from an already strong 69% in the previous test.

	Feb '09	July '09	Change	Internet Explorer Compared	Firefox Compared
Internet Explorer 8	69%	81%	12%		-54%
Firefox 3	30%	27%	-3%	54%	
Safari 4	24%	21%	-3%	60%	6%
Chrome 2	16%	8%	-8%	74%	20%
Opera 10 Beta	5%	1%	-4%	80%	27%

All of the other browsers decreased protection, between 3 and 8% - within the margin in the error. The left-most columns indicate how much better (or worse) Internet Explorer 8 and Firefox 3 are compared to the other browsers' scores.

Between the previous test and this one, all of the browser versions were upgraded to the latest available code. Internet Explorer 8 was upgraded from a Release Candidate (RC) to Generally Available (GA) code. Firefox 3.07 was upgraded to 3.0.11. Safari was upgraded from v3 to v4. Chrome was upgraded from v1.0.154 to v2.0.172.39 Opera was upgraded from v9.64 to v10 beta.

3 Conclusions

The use of reputation systems to assist browsers in the fight against socially engineered malware is a strong use of cloud technologies. But, not all vendor implementations and daily operations yield the same results.

It became obvious from this test and comparisons to the earlier test that Microsoft continues to make considerable improvements in adding protection from socially engineered malware into Internet Explorer 8 (SmartScreen Filter technology). With a unique URL blocking score of 92%, and over-time protection rating of 81%, Internet Explorer 8 was by far the best at protecting against socially engineered malware. The 41% increase from zero-hour to 5 days of blocking suggests a far superior feedback mechanism.

Coming in a distant second, Firefox 3 achieved a 27% protection rating against malware – 54% less protection than Internet Explorer 8. Firefox's unique URL score was also significantly lower, at 24%.

Safari 4 caught 23% of the unique URLs, and just 21% of the malware sites available during our test over time. This represented a 3% decline compared to the previous quarter's test. Furthermore, protection varied greatly, with two short periods of severe dips.

Unlike the previous test, where operational issues were seen, Chrome 2 performed very consistently, albeit very poorly. Chrome 2 lost the most ground compared to Internet Explorer 8 over the two tests, declining 8% and blocking 74% fewer malicious sites than the leader.

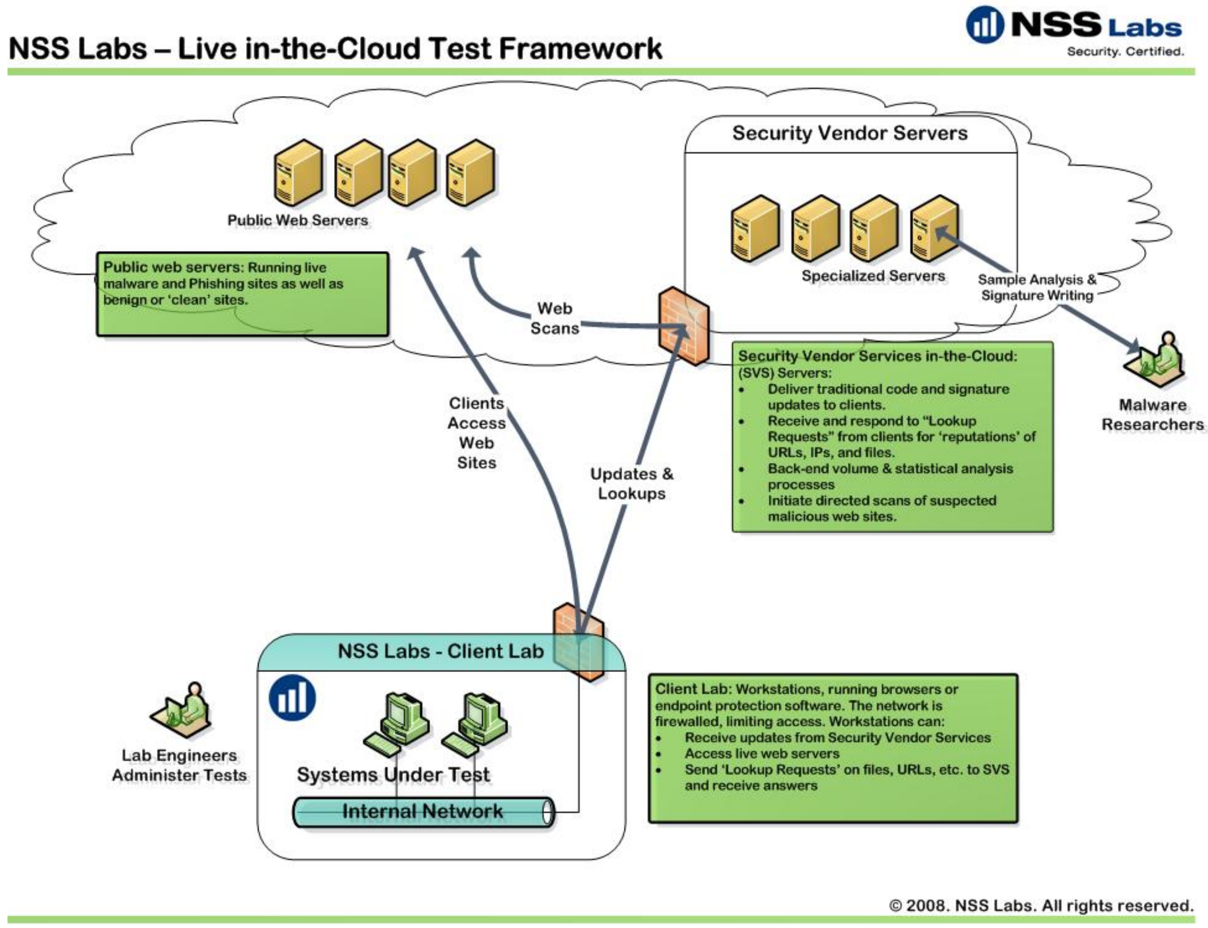
Opera 10's overall blocking rate of 1% was well under the margin of error. To be sure, we double checked the setup and manually verified a significant portion of URLs – with the same result. Users should not expect any protection against socially engineered malware from Opera 10 Beta.

Browsers give users another free layer of protection against socially engineered malware, in addition to endpoint protection products, and should not be considered a replacement for antivirus programs. Look for upcoming tests of anti-malware products from NSS Labs in Q3 2009.

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.



NSS Labs – Live in-the-Cloud Test Framework

Public web servers: Running live malware and Phishing sites as well as benign or 'clean' sites.

Security Vendor Services in-the-Cloud: (SVS) Servers:
- Deliver traditional code and signature updates to clients.
- Receive and respond to "Lookup Requests" from clients for 'reputations' of URLs, IPs, and files.
- Back-end volume & statistical analysis processes
- Initiate directed scans of suspected malicious web sites.

Client Lab: Workstations, running browsers or endpoint protection software. The network is firewalled, limiting access. Workstations can:
- Receive updates from Security Vendor Services
- Access live web servers
- Send 'Lookup Requests' on files, URLs, etc. to SVS and receive answers

© 2008. NSS Labs. All rights reserved.

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

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 84 desktop systems each running a web browser – six (14) each per web browser (6 browser types). Results were recorded into a MySQL DB.

5 Appendix B: Test Procedures

The purpose of the test was to determine how well the tested web browsers protect users from the most important malware threat on the Internet today. A key aspect was the timing. Given the rapid rate and aggressiveness with which criminals propagate and manipulate the malicious web sites, 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 four hours and starts with validation of the site's existence and conformance to the test definition.

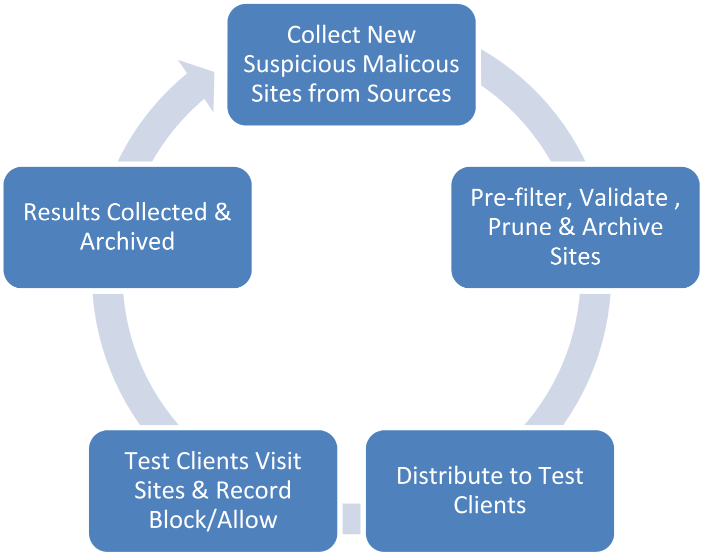
All tests were executed in a highly controlled manner, and results were meticulously recorded and archived at each interval of the test.

5.1 Test Duration

NSS Labs' Browser test was performed continuously (24x7) for 12 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 continues to attempt to download a malware sample with the Web Browser for the duration of the test.


Collect New Suspicious Malicous Sites from Sources
Pre-filter, Validate , Prune & Archive Sites
Distribute to Test Clients
Test Clients Visit Sites & Record Block/Allow
Results Collected & Archived

5.2 Sample sets for malware URLs

Freshness of malware 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 several hundred unique URLs per day. NSS Labs' continuously growing archive of Malware and Viruses that contains Gigabytes of confirmed samples. In addition, NSS Labs maintains relationships with other independent security researchers, networks, and security companies, which provide access to URLs and malicious content. Sample sets contain malicious URLs distributed via: SPAM, social networks, and malicious websites. Exploits containing malware payloads (exploits + malware) a.k.a. "clickjjacking" or "drive-by downloads" were excluded from the test. Every effort was made to consider submissions that reflect a real-world distribution of malware, 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 were added to the URL Consideration Set as soon as possible. The date and time each sample is introduced is noted. Most sources were automatically and immediately inserted, while some methods require manual handling and can be processed in under 30 minutes. All items in the consideration set were 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 malware 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 was given a cursory review to verify it was present and 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 cycle, 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 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.

5.5 Dynamically execute each URL

A client automation utility requests each of the URLs deemed 'present' based upon results of test 5.4 via each of the web browsers in the test. NSS records whether or not the malware was allowed to be downloaded, and if the download attempt triggered a warning from the browser's malware 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 malware from being downloaded, and *correctly* issuing a warning.

- Failure: NSS Labs defines a "failure" based upon a web browser *failing* to prevent the malware from being downloaded and *failing* to 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 malware 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 for download during the course of the test, the sample will be removed from the test collection for that iteration. NSS Labs continually verifies each sample's presence (availability for download) and adds/removes each sample from the test set accordingly. Should a malware 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 used two different sandboxes to prune and validate the malware (Sunbelt's CW Sandbox and Norman Analyzer), and further validated suspicious samples using multiple antivirus scanners if necessary.

6 Appendix C: Test Infrastructure

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

AutomatedQA
test, debug, deliver!

assurent
secure technologies | a TELUS Company

solidcore

Sunbelt Software
we keep the bad guys out℠

mailshell™

NORMAN

vmware