



WEB BROWSER SECURITY
SOCIALLY-ENGINEERED MALWARE PROTECTION
COMPARATIVE TEST RESULTS
GLOBAL

Apple® Safari® 5
Google Chrome™ 12
Windows® Internet Explorer® 9
Mozilla® Firefox® 4
Opera™ 11



METHODOLOGY VERSION: 1.2
AUGUST 2011



© 2011 NSS Labs, Inc. 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 at the time of publication, but is not guaranteed. All use of and reliance on this report are at the reader's 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 the reader's expectations, requirements, needs, or specifications, or that they will operate without interruption.
5. This report does not imply any endorsement, sponsorship, affiliation, or verification by or with any organizations mentioned in this report.
6. All trademarks, service marks, and trade names used in this report are the trademarks, service marks, and trade names of their respective owners.

CONTACT INFORMATION

NSS Labs, Inc.

P.O. Box 130573

Carlsbad, CA 92013 USA

+1 (760) 270-9852

info@nsslabs.com

www.nsslabs.com

EXECUTIVE SUMMARY

Worldwide Test of Malware Protection

In Q2 of 2011, NSS Labs performed a test of web browser protection against socially-engineered malware targeting users around the globe.¹ This test was in addition to our recent European and Asia-Pacific browser tests. Socially engineered malware (SEM) remains the most common security threat facing Internet users today. Recent studies show that users are four times more likely to be tricked into downloading malware than be compromised by an exploit.²



The web remains the biggest opportunity for malware infection. Emails carry malicious links and attachments, while web sites play host to exploits and drive-by downloads targeting browsers and other software.

European and American users have found themselves particular targets of malware authors over the last 12 months. North America has consistently been the primary host of malicious URLs, while users in Asia have been victims of the greatest number of malicious URLs³.

In 2010, threat researchers discovered new ZBOT variants specifically targeting banking systems in four European countries. Companies targeted have high-profile clientele, and included the major UniCredit Group Subsidiary Bank of Rome; U.K.-based Abbey National; Hong Kong's HSBC; Germany's leading IT service provider in the cooperative financial system, the FIDUCIA Group; and one of France's largest retail banks, Crédit Mutuel.

According to the EU's statistics office, Eurostat, almost one third of internet users in the European Union were victims of malware infections in 2010 despite the majority having security software installed. Of the 27 EU countries surveyed (totaling over 200,000 users), those with the highest malware infections include Bulgaria (58%), Slovakia (47%), Hungary (46%), Italy (45%) and Estonia (43%.) The PandaLabs Quarterly Report for Q1 2011 concurs, showing several European countries - including France, Spain and Ireland - hovering around the 40% infection level.

PandaLabs Quarterly Report for Q1 2011⁴ also notes that the APAC region continues to demonstrate the highest levels of infected users per country. Infection levels of end-user

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

² Hughes, Bruce "Social Engineering Trumps a Zero-Day Every Time". *VB2010 Conference*, 30 September 2010. <http://www.virusbtn.com/conference/vb2010/abstracts/Hughes.xml>

³ TrendLabs Global Threat Trends 1H 2010.

http://us.trendmicro.com/imperia/md/content/us/trendwatch/researchandanalysis/tm101hthreat_report.pdf

⁴ Panda Security, "Quarterly Report PandaLabs (January-March 2011)". *PandaLabs*, 4 April 2011.

systems in China are almost 70%, while Thailand and Japan are not far behind at approximately 65% and 59% respectively. In comparison, incidents from the Asia-Pacific (APAC) region such as the one concerning the infection of users by drive-by download hosted by the Punjab National Bank (PNB) web site in 2010 are rare.

A worrying trend is that APAC countries in the middle of the list still show infection levels of 50 percent or higher, all the way up to 60-70% in the top three countries of China, Thailand and Japan.

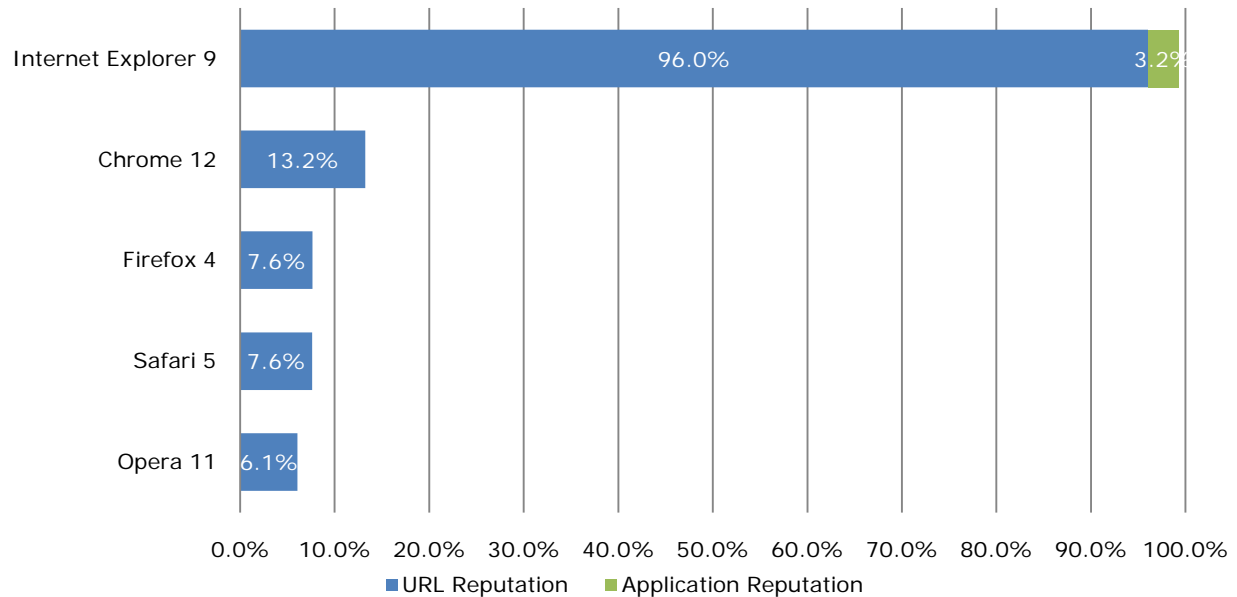
Interestingly, the first quarter of 2011 saw the U.S. disappear from the Top 20 list of countries most affected by malware infections, whereas countries like France, Spain and Ireland have re-entered it.

Latin America is also showing an increase, with countries like Peru and Ecuador showing infection levels between 30 and 40 percent. In all cases, the predominant type of malware found is the Trojan, with adware and worms being the next most prevalent.

This NSS Labs report focused on URLs chosen to be of significant threat and followed the same Live Testing methodology as the global tests conducted in Q1 2009, Q3 2009, Q1 2010, and Q3 2010 (www.nsslabs.com/browser-security). This report contains empirically-validated evidence gathered during 14 days of 24 x 7 testing, performed every six hours, over 55 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. For region specific reports, please see our Q2 2011 European and Q3 2011 Asia-Pacific tests, as these two tests used unique infrastructure and data sets specifically concentrating on malware targeting users in these regions.

This report 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.

Mean Block Rate for Socially Engineered Malware / Worldwide



Windows Internet Explorer 9 (IE9) caught an exceptional 99.2% of live threats: 96% with the SmartScreen URL reputation and an additional 3.2% with Application Reputation. URL Reputation, which is included in IE8, and Application Reputation, which is new to IE9, are the two components that make up IE9's SmartScreen Filter. IE9 with SmartScreen offers the best protection of any browser against socially engineered malware. Protection against malware matched our previous findings from the Q2 2011 European test and Q3 2010 global test as well as the Q3 2011 Asia-Pacific test.

Google Chrome 12 caught 13.2%⁵ of the live threats, considerably more than the 3% observed during the Q3 2010 global test. This improvement tracks to an enhancement in SafeBrowsing so that, according to Google, "Chrome now warns you before downloading some types of malicious files"⁶.

Apple Safari 5 caught 7.6% of the live threats. Protection offered was near identical to that of Firefox.

Mozilla Firefox 4 caught 7.6% of the live threats, far fewer than Internet Explorer 9. Results were 11.4% less than the 19% protection rate observed in our Q3 2010 global test, indicating an overall drop in protection for Firefox.

Opera 11 caught 6.1% of the live threats, providing considerably less protection against socially-engineered malware than the other browsers tested.

⁵ NSS Labs validated that Google Chrome v12.0.742.30 beta-m and Google Chrome v12.0.742.91 (*stable version released on June 7, 2011*) provided identical protection when presented with malicious downloads

⁶ Walker, Adrienne "A new stable release of Chrome: safer and snazzier" *Google Chrome Blog*, 7 June 2011. <http://chrome.blogspot.com/2011/06/chrome-12-safer-and-snazzier.html>

TABLE OF CONTENTS

1	<i>Introduction</i>	1
1.1	The Socially-Engineered Malware Threat	1
1.2	Web Browser Security.....	1
2	<i>Effectiveness Results</i>	3
2.1	Test Composition: Malicious URLs	3
2.2	Blocking URLs with Socially-Engineered Malware	3
2.3	Blocking URLs with Socially-Engineered Malware Over Time	5
2.4	Safe Browsing Products	6
2.5	Microsoft's IE9 and Application Reputation.....	6
3	<i>Conclusions</i>	8
4	<i>Test Environment</i>	10
4.1	Client Host Description	10
4.2	The Tested Browsers.....	11
4.3	Network Description	11
4.4	About this Test.....	11
5	<i>Appendix A: Test Procedures</i>	12
5.1	Test Duration	12
5.2	Sample Sets for Malware URLs.....	12
5.3	Catalog URLs.....	13
5.4	Confirm Sample Presence of URLs	13
5.5	Dynamically Execute Each URL	13
5.6	Pruning	14
5.7	Post-Test Validation.....	14
	<i>Appendix B: Test Infrastructure</i>	15

1 INTRODUCTION

1.1 THE SOCIALLY-ENGINEERED MALWARE THREAT

Socially-engineered malware attacks pose a significant risk to individuals and organizations by threatening to compromise, damage, or acquire sensitive personal and corporate information; statistics from 2008 - 2010 show that this trend is increasing at a rapid rate. According to a recent study by AVG, users are four times more likely to be tricked into downloading malware than be compromised by an exploit;⁷ detecting and preventing these threats continues to be a challenge as criminals continue to increase their use of malware as a cybercrime attack vector. Anti-virus researchers report detecting between 15,000 and 50,000 new malicious programs per day, Kaspersky Lab has even reported detecting up to “millions per month.”⁸

While not all of these malicious programs are social engineering attacks, the 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 e-mail according to statistics from Trend Micro.⁹

From a cybercriminal’s perspective, tricking users into downloading and installing malware is a preferred means of attack since the weakness they are exploiting is the naiveté of their victim; this enables criminals to cast a wide net since there are no technology dependencies. In contrast, drive-by attacks require the user’s computer to be vulnerable to the exploit being attempted.

Criminals are taking advantage of the implied trust relationships inherent in social networking sites (Facebook®, MySpace™, Badoo, StudiVZ, Skyrock, LinkedIn®, renren, Kaixin001 (a.k.a. Happy Net), 51, Multiply, Cyworld, Orkut, Mixi, etc.) and user-contributed content (blogs, Twitter™, etc.) which allow for rapid publishing and anonymity. Furthermore, the speed at which these threats are “rotated” to new locations 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, or more generally a website known to host malware links.** These downloads appear to be safe, like those for a screen saver application, video codec upgrade, etc., and are designed to fool the user into taking action. Security professionals also refer to these threats as “consensual” or “dangerous” downloads.

1.2 WEB BROWSER SECURITY

Modern web browsers offer an **added 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.¹⁰ Each of the web browsers has added security technologies to combat web-based threats. However, not all of them have taken the same approach.

⁷ Hughes, Bruce “Social Engineering Trumps a Zero-Day Every Time”. *VB2010 Conference*, 30 September 2010. <http://www.virusbtn.com/conference/vb2010/abstracts/Hughes.xml>

⁸ Kaspersky, Eugene “Anti-malware expert and CEO, Eugene Kaspersky, offers theory for stopping cybercrime”. *SF Cybercrime Examiner*, 17 July 2009. <http://www.examiner.com/x-11905-SF-Cybercrime-Examiner-y2009m7d17-Antimalware-expert-and-CEO-Eugene-Kaspersky-talks-about-cybercrime>.

⁹ Cruz, Macky “Most Abused Infection Vector”. *Trend Labs Malware Blog*, 7 Dec 2008. <http://blog.trendmicro.com/most-abused-infection-vector/>

¹⁰ 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.

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 categorization may be performed manually, automatically, or using both methods. Some vendors will utilize feedback from user agents on their customers’ endpoints to report back to the reputation system automatically, providing information relevant to the trustworthiness, or otherwise, of applications and files downloaded from the internet. 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.

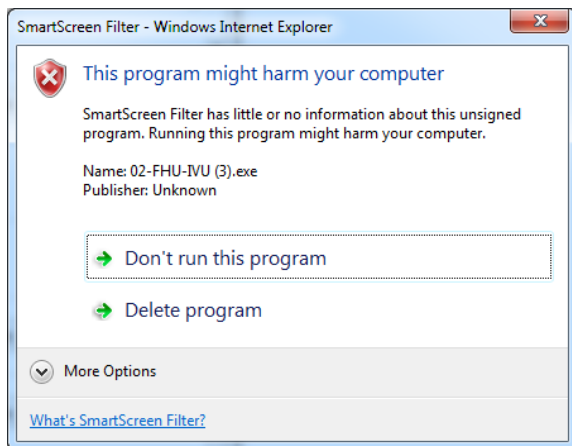
When results are returned that a site is “bad,” the web browser redirects the user to a warning message or page instructing that the URL is malicious. In the event that the URL links to a download, the web browser instructs the user that the content is malicious and that the download should be cancelled. 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 performed.



Firefox 4 Warning



Internet Explorer 9 Warning



IE 9 application reputation warning

2 EFFECTIVENESS RESULTS

2.1 TEST COMPOSITION: MALICIOUS URLS

Data in this report spans a testing period of 14 days, from May 27 through June 10, 2011. 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, 55 discrete tests were performed (every six hours) without interruption for each of the five browsers.

The emphasis was on freshness; thus, a larger number of sites were evaluated than were ultimately kept as part of the result set. The NSS Labs Socially-Engineered Malware Protection Comparative Test Methodology provides additional details on the URLs evaluated and used in the result set.

Malicious URLs contained within this test were deemed a threat to users worldwide. The ultimate determinant of whether or not a malicious URL was included in this test was its participation in a malware campaign targeting users.

2.1.1 TOTAL NUMBER OF MALICIOUS URLS IN THE TEST

From an initial list of over 5,000 new suspicious sites, 3,296 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 containing adware or that were not valid malware. Ultimately, 1,188 URLs passed our post-validation process and are included in the results, providing a margin of error of 2.76% with a confidence interval of 95%.

2.1.2 AVERAGE NUMBER OF MALICIOUS URLS ADDED PER DAY

On average, 86 new URLs were added to the test set per day. On certain days, however, more or fewer URLs were added to the test set 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.

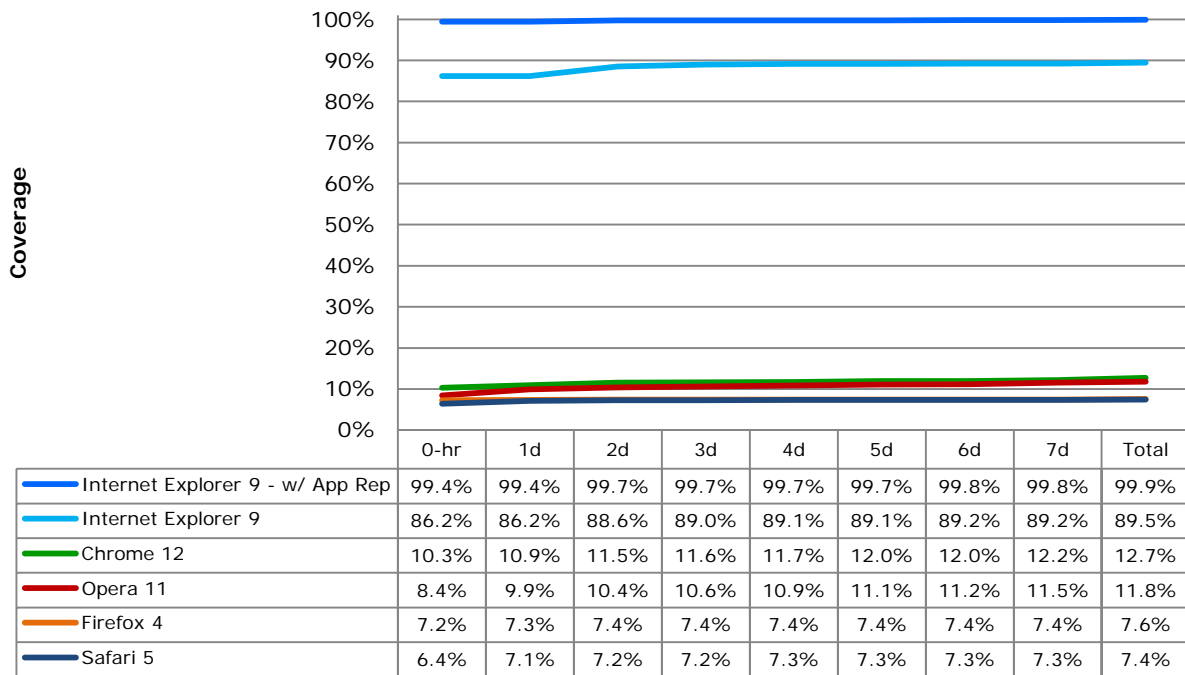
2.2 BLOCKING URLS WITH SOCIALLY-ENGINEERED MALWARE

NSS Labs assessed the browsers' ability to block malicious URLs as quickly as we found them on the Internet. We continued testing them every six hours to determine how long it took a vendor to add protection.

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 each day until blocked. Final protection scores for the URL test duration are summarized under the "Total" column.

Malware URL Response Histogram / Worldwide



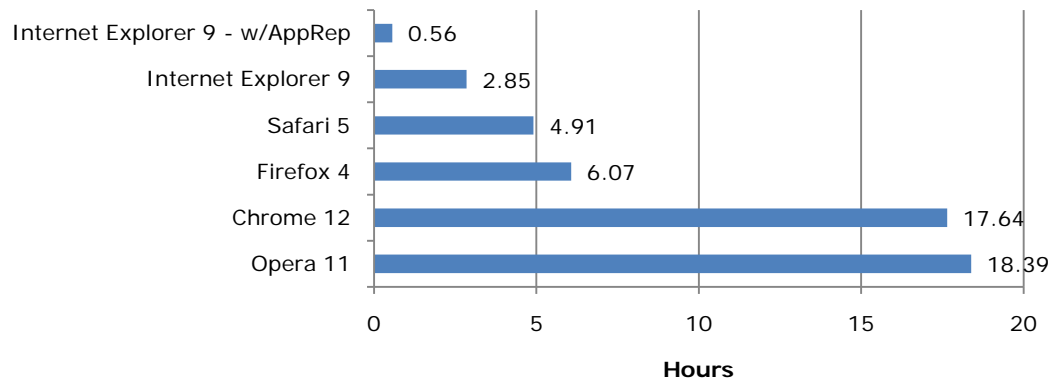
Ultimately, the results reveal great variations in the abilities of the browsers to protect against socially-engineered malware. Chrome provided more protection than the other browsers using the Safe Browsing feed, apparently due to the “enhancements” added to Chrome 12. Trends show minor differences between Firefox and Safari. Opera fared better when viewed through the lens of unique URLs (11.8%), however it displayed inconsistent behavior throughout the test, first blocking and then not blocking malicious URLs (See section 2.3). This appears to be due to a race condition where the warning message sometimes appears after the malware has completed downloading/executing.

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. The table below answers the question of how long on average a user must 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 mathematical way to score “never.”

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 216 hours (9 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 24 hours.

Average Time to Block / Worldwide

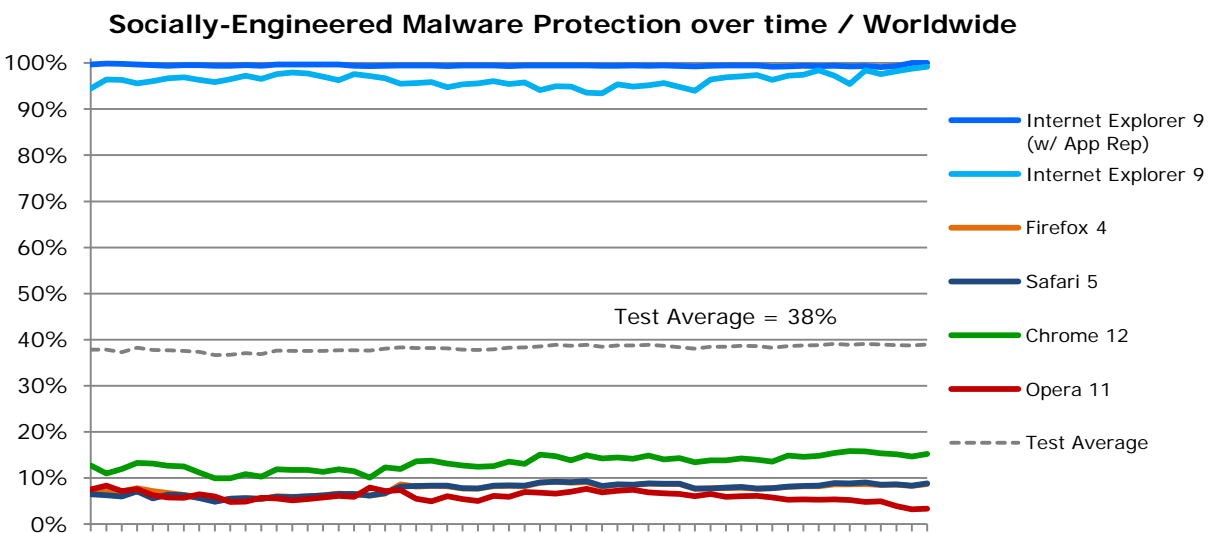


The mean time to block a site (if it is blocked at all) is 9.97 hours. Thus, IE9 (w/App Rep), IE9 (without App Rep), Safari, and Firefox were above average at adding new blocks. All browsers blocked at least one malware download during the test.

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 that may change quickly. Thus, at any given time, the available set of malicious URLs is evolving, and continuing to block these sites is a key criterion for effectiveness. Therefore, NSS Labs tested all of the live URLs every six hours. The following tables and graphs show the repeated evaluations of blocking over the course of 20 days, 78 test cycles for each of five browsers. Each score represents protection at a given point in time.

As seen on the graph, Internet Explorer 9 demonstrated a very high level of protection. Safari, Firefox, and Chrome were reliable—albeit at a much lower level of protection.

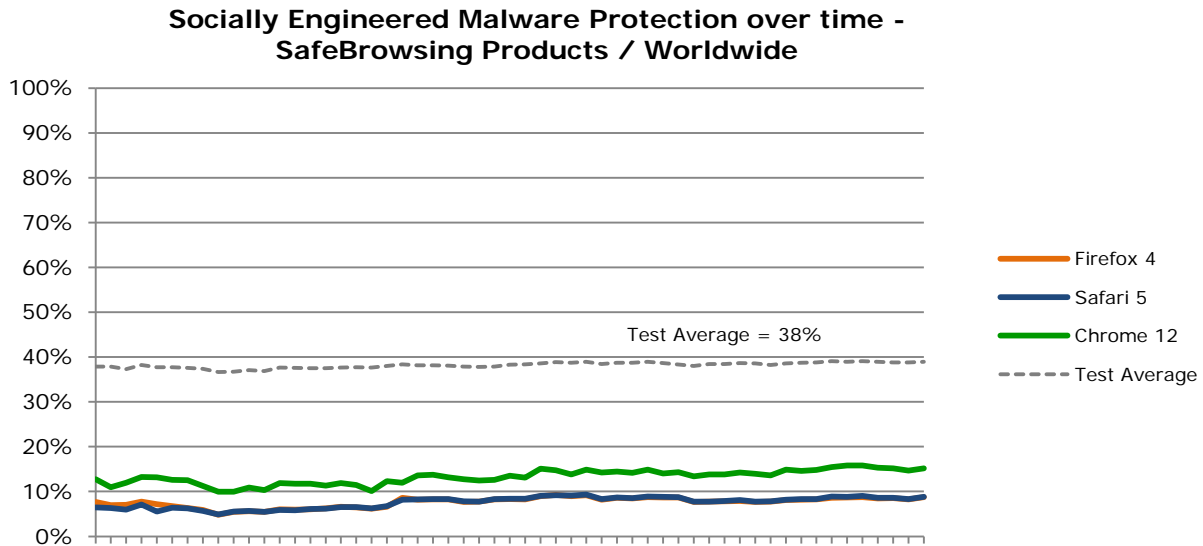


Note that the average protection percentage will deviate from the unique URL results for several reasons. First, this data includes multiple tests of a URL. Therefore, if a URL is blocked early on, it will improve the score. If it continues to be missed, it will detract from the score. Thus, results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

Opera displayed increasingly poor results over the course of this test, first blocking and then not blocking malicious URLs. This appears to be due to a race condition where the warning message oftentimes appears after the malware has completed downloading/executing.

2.4 SAFE BROWSING PRODUCTS

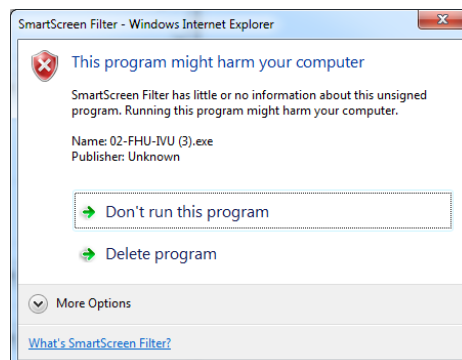
Chrome, Firefox, and Safari all use the Google Safe Browsing data feed. However, our testing found that Chrome provided slightly better protection than that of Firefox or Safari against socially-engineered malware URLs.



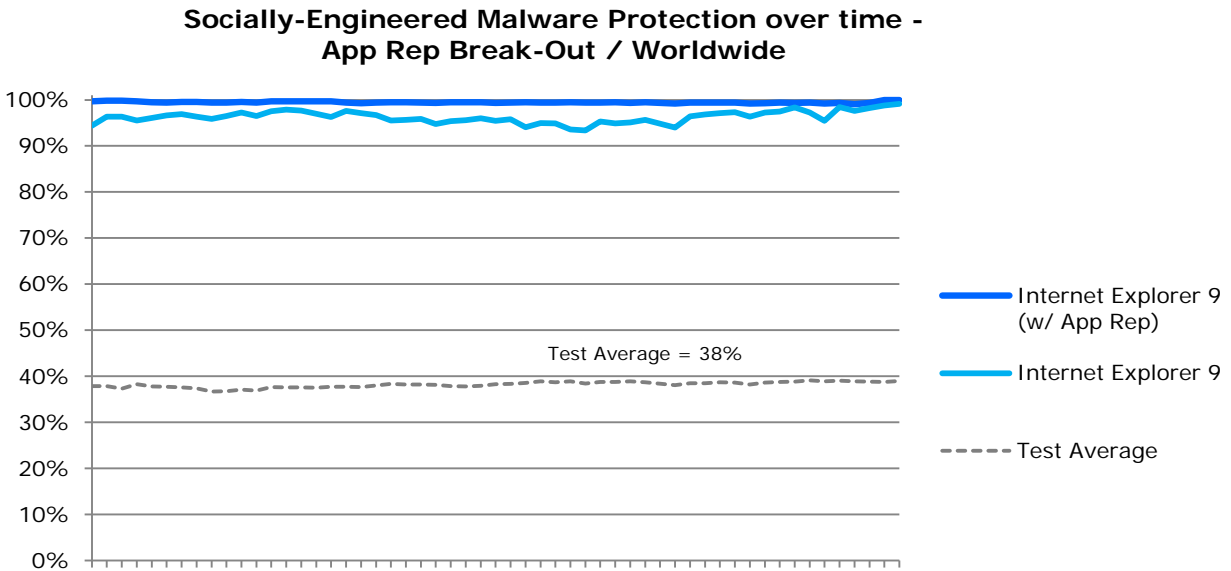
As mentioned in Section 2.2.1 and indicated in the Malware URL Response Histogram, Firefox and Safari's protection rates were nearly identical, showing signs of converging at roughly 7.6%. In fact, while Chrome provides roughly 5.6% more protection than Firefox and Safari, the protection across the three browsers was in lock step with each other, rising and falling in unison. This supports the notion that the block lists for Chrome, Firefox, and Safari are the same (or very similar), and that Chrome provides protection above and beyond what is available in the Safe Browsing feed.

2.5 MICROSOFT'S IE9 AND APPLICATION REPUTATION

Internet Explorer 9 with application reputation shows a 3.2% improvement over Internet Explorer 9 without the application reputation system. This new capability helps users discern malware, and potentially unsafe software from actual good software.



The basic value of application reputation is in its ability to add context for the user so that the user will question whether the source of the download is to be trusted.



As is visible from the results, the addition of application reputation technology boosts Internet Explorer 9's protection capabilities an additional 3.2% to 99.2%.

3 CONCLUSIONS

Socially-engineered malware is a widespread problem, claiming one third of internet users as victims. The use of free browser-based reputation systems to assist in the fight against socially-engineered malware is a strong use of cloud technologies. However, in this global test of socially-engineered malware, we found that not all vendor implementations and daily operations yield the same results.

Q3 2010 Global Test	Blocked	Q3 2011 Global Test	Blocked	Change
Internet Explorer 9 (w/ App Rep)	99%	Internet Explorer 9 (w/ App Rep)	99.2%	0.2%
Chrome 6	3%	Chrome 12	13.2%	10.2%
Safari 5	11%	Safari 5	7.6%	-3.4%
Firefox 3.6.15	19%	Firefox 4	7.6%	-11.4%
Opera 10	0%	Opera 11	6.1%	6.1%

The table below shows the mean block rate and malicious URL sample size across our 2011 European, Asia-Pacific, and global tests. This illustrates, despite varying URL samples and sizes, that the mean block rate was largely consistent across multiple geographic regions and timeframes for IE, Chrome, and Opera. But inconsistent for Safari and Firefox. As already stated in this report, the inconsistency with Safari and Firefox may not be due to the region or the timing of the test, but may be indicative of these two browsers not implementing the new socially engineered malware protection that was introduced in Chrome 12.

	Q2 2011 Europe Test	Q3 2011 APAC Test	Q3 2011 Global Test
<i>Malicious URL Sample Size</i>	650	977	1,188
<i>Test Duration</i>	19 days	20 days	14 days
Browser	Blocked		
Internet Explorer	100%	99.8%	99.2%
Chrome	13%	15.4%	13.2%
Safari	13%	9.0%	7.6%
Firefox	13%	8.9%	7.6%
Opera	5%	5.4%	6.1%

It became obvious from this worldwide test and our recent European and Asia-Pacific tests, in comparison to our earlier global tests, that Microsoft continues to improve their IE malware protection in **Internet Explorer 9** through its SmartScreen® Filter technology and with the addition of SmartScreen Application Reputation technology. With SmartScreen enabled and Application Reputation disabled, IE9 achieved a unique URL blocking score of 89.5% and over-time protection rating of 96%. Enabling Application Reputation on top of SmartScreen increased the unique URL block rate of Internet Explorer 9 by 10.4% (to 99.9%) as well as the over-time protection by 3.2% (to 99.2%). Internet Explorer 9 was by far the best at protecting against socially-engineered malware, even before App Rep's protection is layered on top of SmartScreen.

The significance of Microsoft's new application reputation technology cannot be overstated. Application reputation is the first attempt by any vendor to create a definitive list of every application on the Internet. This new capability helps users discern malware, and potentially unsafe software from actual good software. The list is dynamically created and maintained, much the same way Google, (or Bing) is continuously building and maintaining a library of content for search purposes.

With a protection rating of 13.2%¹¹, **Chrome 12** offered inferior protection to IE9, yet superior protection to Opera, Safari and Firefox. The improvement vs. Safari and Firefox appears to be the result of “enhancements” to Chrome. According to Google, “Chrome now warns you before downloading some types of malicious files”¹². NSS Labs commends Google for adding some protection against socially engineered malware to Chrome. Further, we view the addition of this protection as evidence that even as Google’s PR engine downplayed the findings of prior NSS Labs test reports, the Chrome engineering team was working hard to address this known deficiency.

Firefox 4 achieved a 7.6% protection rating, slightly better than the protection offered by Safari. However, Firefox provided less protection when compared with our Q3 2010 global test. The deterioration in protection may be attributed to a more standardized implementation of the new Safe Browsing API v2 or evasion tactics being used by cybercriminals to which Firefox has not yet adapted. There was a slight 0.6% improvement between zero-hour protection (7.2%) and eventual protection at the 14 day mark (7.6%).

On par with Firefox 4, **Safari 5** achieved an overall protection rating of 7.6%. Safari’s unique URL block rate was roughly 7.4% after 14 days, however Safari lagged behind Firefox with zero-hour protection of 6.4% (vs. Firefox’s 7.2%).

Opera 10’s overall blocking rate of 6.1% was consistently the lowest in the group. However, this was an improvement over the 0% scores in our previous global tests, and is likely attributable to the company’s partnership with antivirus firm AVG. Opera displayed increasingly poor results over the course of this test, first blocking and then not blocking malicious URLs. This appears to be due to a race condition where the warning message oftentimes appears after the malware has completed downloading/executing.

¹¹ NSS Labs validated that Google Chrome v12.0.742.30 beta-m and Google Chrome v12.0.742.91 (stable version released on June 7, 2011) provided identical protection when presented with malicious downloads --

<http://googlechromereleases.blogspot.com/2011/06/chrome-stable-release.html>

¹² Walker, Adrienne “A new stable release of Chrome: safer and snazzier” *Google Chrome Blog*, 7 June 2011.

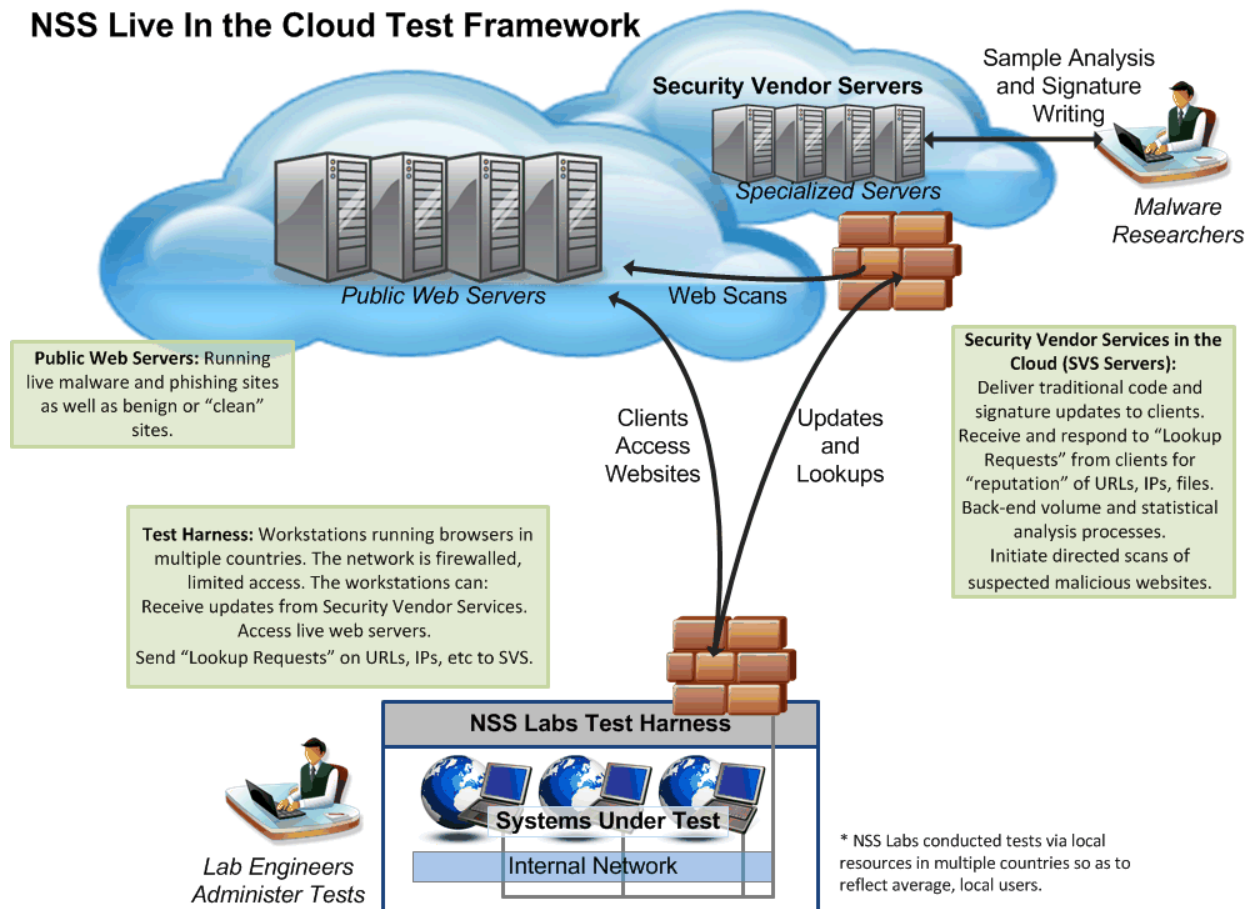
<http://chrome.blogspot.com/2011/06/chrome-12-safer-and-snazzier.html>

4 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 “live” test lab environment in order to duplicate user experiences under real-world conditions.

NSS Live In the Cloud Test Framework



4.1 CLIENT HOST DESCRIPTION

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

- Microsoft Windows 7
- 1GB RAM
- 20GB hard drive

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. 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:

- Google Chrome v12.0.742.30
- Google Chrome v12.0.742.91
- Windows Internet Explorer 9 (build 9.0.8112.16421)
- Mozilla Firefox v4.0.1
- Opera v11.10 Build 2092
- Safari v5.0.5(7533.21.1)

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 anti-virus, intrusion prevention, 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 192 desktop systems each running a web browser. Results were recorded into a MySQL database.

4.4 ABOUT THIS TEST

This report 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.

5 APPENDIX A: 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 websites, 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. Unique in this procedure is that NSS Labs validates the samples before and after the test. Actual testing of the threats proceeded every six hours and starts with validation of the site’s existence and conformance to the test definition.

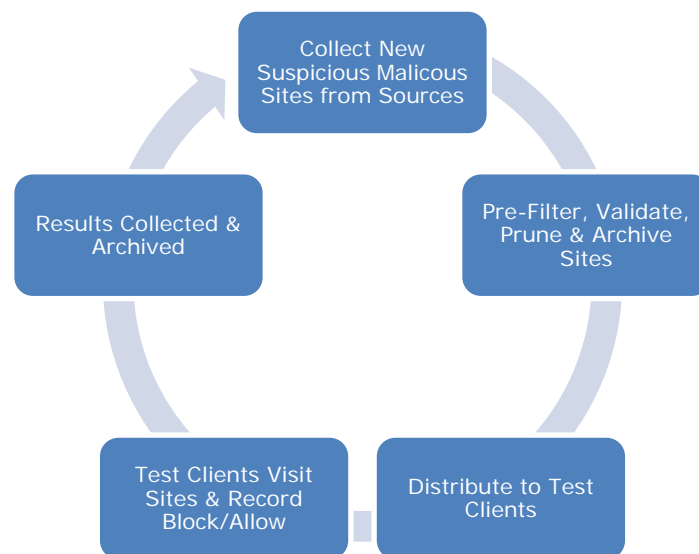
All tests were executed in a highly controlled manner, and results were meticulously recorded and archived at each interval of the test.

5.1 TEST DURATION

NSS Labs’ browser test was performed continuously (24 x 7) 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 six 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.



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

NSS Labs operates its own network of spam traps and honeypots. These e-mail accounts with high-volume traffic yield thousands of unique e-mails, and several hundred unique URLs per day. 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: e-mail, instant messaging, social networks, and malicious websites. No content was used from the tested parties.

Malicious URLs targeting users throughout the globe were identified and selected for inclusion in this test. Users are defined as individuals residing within the North America, South American, European, and Asia-Pacific regions, including: Argentina, Australia, Austria, Brazil, Canada, China, France, Germany, India, Italy, Japan, Indonesia, Mexico, New Zealand, Singapore, Spain, South Korea, Sweden, Thailand, the United Kingdom, the United States of America, and Vietnam. The ultimate determinant of whether or not a malicious URL was included in this test was its participation in a malware campaign targeting users. Lastly, just because a malicious URL was included in a campaign targeting an Asia-Pacific or a North American user does not mean that the URL was not used in other campaigns targeting users from other regions.

Exploits containing malware payloads (exploits plus malware), also known as “clickjacking” 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 Labs maintains a collection of “clean URLs” which includes sites from Yahoo, Amazon, Microsoft, Google, NSS Labs, major banks, and others. Periodically, clean URLs were run through the system to verify that the 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, such that 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 the test described in Section 5.4 via each of the web browsers in the test. NSS Labs 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 AND 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. For example, 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 that were either not malicious or not available before the test started. NSS Labs used two different commercial sandboxes to prune and validate the malware (Sunbelt’s CWSandbox and Norman[®] Analyzer). Further validation was done using proprietary tools, system instrumentation, and code analysis as needed.

APPENDIX B: TEST INFRASTRUCTURE

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

