WEB BROWSER SECURITY

SOCIALLY-ENGINEERED MALWARE PROTECTION

COMPARATIVE TEST RESULTS

Apple® Safari® 5
Google Chrome™ 6
Windows® Internet Explorer® 8
Windows® Internet Explorer® 9
Mozilla® Firefox® 3.6
Opera™ 10

METHODOLOGY VERSION: 1.2
OCTOBER 2010

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.

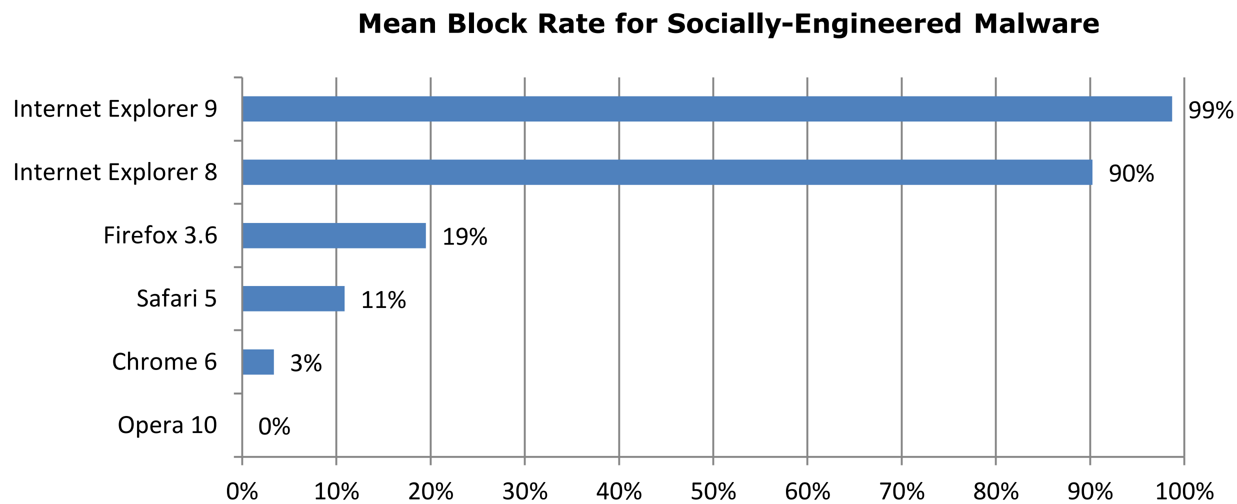
6. All trademarks, service marks, and trade names used in this report are the trademarks, service marks, and trade names of their respective owners.

CONTACT INFORMATION

NSS Labs, Inc.
P.O. Box 130573
Carlsbad, CA 92013 USA
+1 (512) 961-5300
info@nsslabs.com
www.nsslabs.com

EXECUTIVE SUMMARY

In September 2010, NSS Labs performed the fourth 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 tests conducted in Q1 2009, Q3 2009, and Q1 2010 (www.nsslabs.com/browser-security). This report contains empirically-validated evidence gathered during 11 days of 24 x 7 testing, performed every six hours, over 39 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.



Windows Internet Explorer 9 (beta) caught an exceptional 99% of the live threats, leading the non-IE pack by 80%. IE9's protection includes SmartScreen URL filtering, which is included in IE8 as well as SmartScreen application reputation, which is new to IE9.

Windows Internet Explorer 8 caught 90% of the live threats, an exceptional score which was a 5% improvement from the Q1 2010 test and built upon prior improvements from the Q3 2009 and Q1 2009 tests. IE8 showed a 71% lead over the next best browser.

Mozilla Firefox 3.6 caught 19% of the live threats, far fewer than Internet Explorer 8 or Internet Explorer 9. This is a 10% decrease in protection from the Q1 2010 test.

Apple Safari 5 caught 11% of the live threats. Overall protection declined 18% from Q1 2010.

Google Chrome 6 caught 3% of the live threats, down 14% from the Q1 2010 test.

Opera 10 caught 0% of the live threats, providing virtually no protection against socially-engineered malware.

---

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

TABLE OF CONTENTS

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 and 2009 show that this trend is increasing at a rapid rate. According to Symantec, "social engineering will be the primary attack vector" in 2010;[2] 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."[3]

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 e-mail according to statistics from Trend Micro.[4]

Criminals are taking advantage of the implied trust relationships inherent in social networking sites (Facebook®, MySpace™, LinkedIn®, 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 six different web browsers to protect users from socially-engineered malware.[5] Each of the web browsers has added 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.

---

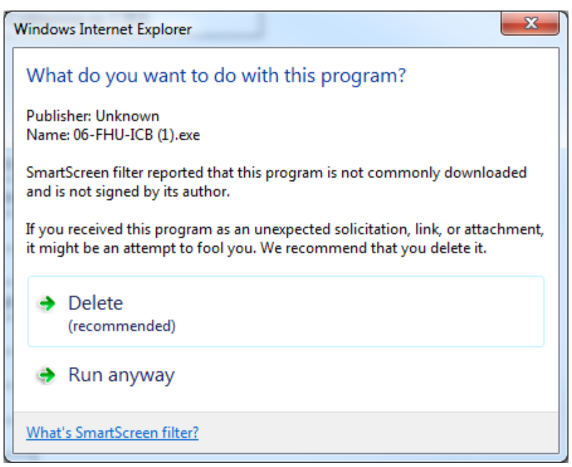
[2] Symantec *Reality Check* "Tech Briefs." http://www.symantec.com/connect/zh-hans/blogs/expect-these-security-trends-dominate-2010
[3] Kaspersky, Eugene in http://www.examiner.com/x-11905-SF-Cybercrime-Examiner~y2009m7d17-Antimalware-expert-and-CEO-Eugene-Kaspersky-talks-about-cybercrime.
[4] Cruz, Macky "Most Abused Infection Vector". *Trend Labs Malware Blog*, 7 Dec 2008. http://blog.trendmicro.com/most-abused-infection-vector/
[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.

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. 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 3.6 Warning

Internet Explorer 8 Warning



IE 9 application reputation warning

2 Effectiveness Results

2.1 Test Composition: Malicious URLs

Data in this report spans a testing period of 11 days, from September 17 through September 27, 2010. 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, 39 discrete tests were performed (every six hours) without interruption for each of the six browsers.

The emphasis was on freshness; thus, a larger number of sites (1,209) 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.

2.1.1 Total number of malicious URLs in the test

From an initial list of 8,000 new suspicious sites, 1,209 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 636 URLs passed our post-validation process and are included in the final results, providing a margin of error of 3.88% with a confidence interval of 95%.

2.1.2 Average number of malicious URLs added per day

On average, 124 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.

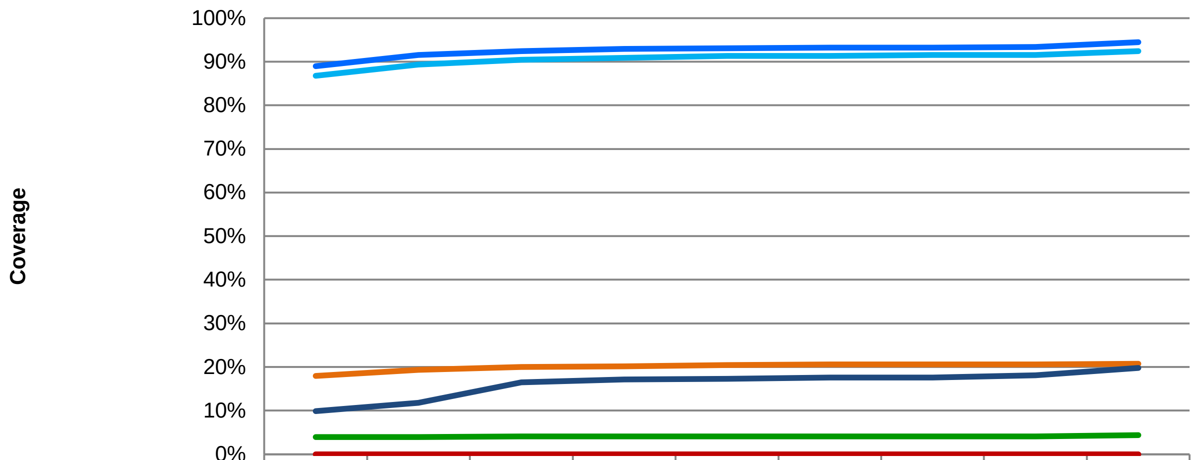
2.2 Blocking URLs with Socially-Engineered Malware

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



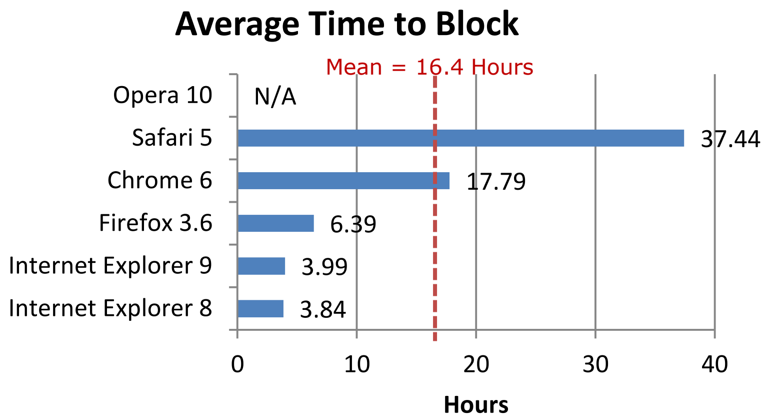
	0-hr	1d	2d	3d	4d	5d	6d	7d	Total
Internet Explorer 9	89%	92%	92%	93%	93%	93%	93%	93%	94%
Internet Explorer 8	87%	89%	90%	91%	91%	91%	92%	92%	92%
Firefox 3.6	18%	19%	20%	20%	20%	21%	21%	21%	21%
Safari 5	10%	12%	17%	17%	17%	18%	18%	18%	20%
Chrome 6	4%	4%	4%	4%	4%	4%	4%	4%	4%
Opera 10	0%	0%	0%	0%	0%	0%	0%	0%	0%

Ultimately, the results reveal great variations in the abilities of the browsers to protect against socially-engineered malware. Trends show Safari and Firefox converging at a protection rate just under 20%, indicating that while they share the Google Safe Browser feed, there is a difference in each browser's 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. 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 264 hours (11 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.

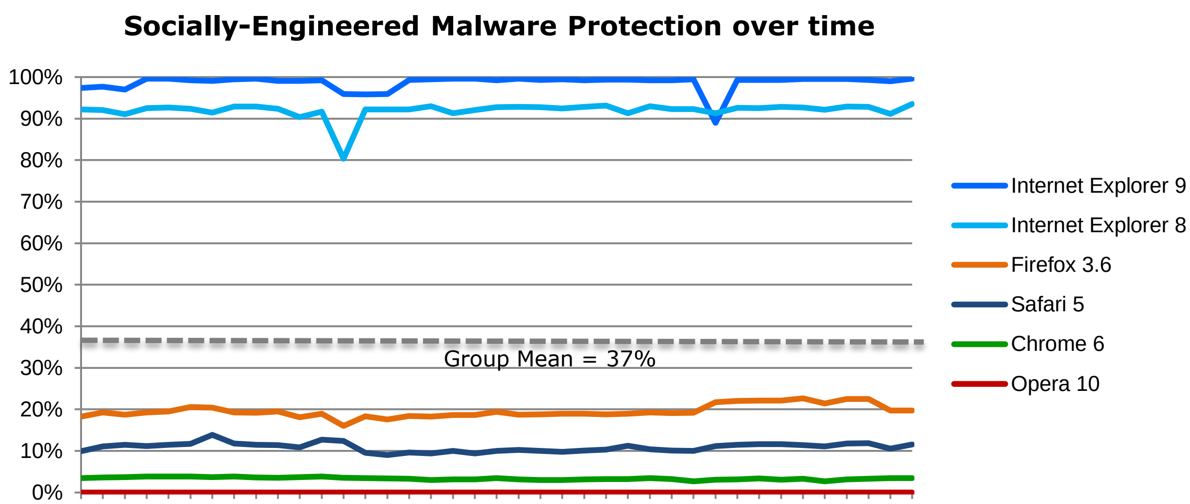


The mean time to block a site (if it is blocked at all) is 16.4 hours. Thus, Chrome and Safari were above average at adding new blocks. With the exception of Opera, which failed to block a single malware download, all browsers blocked at least one malware download.

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 evolving, and continuing to block these sites is a key criterion for effectiveness. Therefore, NSS Labs tested a set of live URLs every six hours. The following tables and graphs show the repeated evaluations of blocking over the course of 11 days, 39 test cycles for each of six browsers. Each score represents protection at a given point in time.

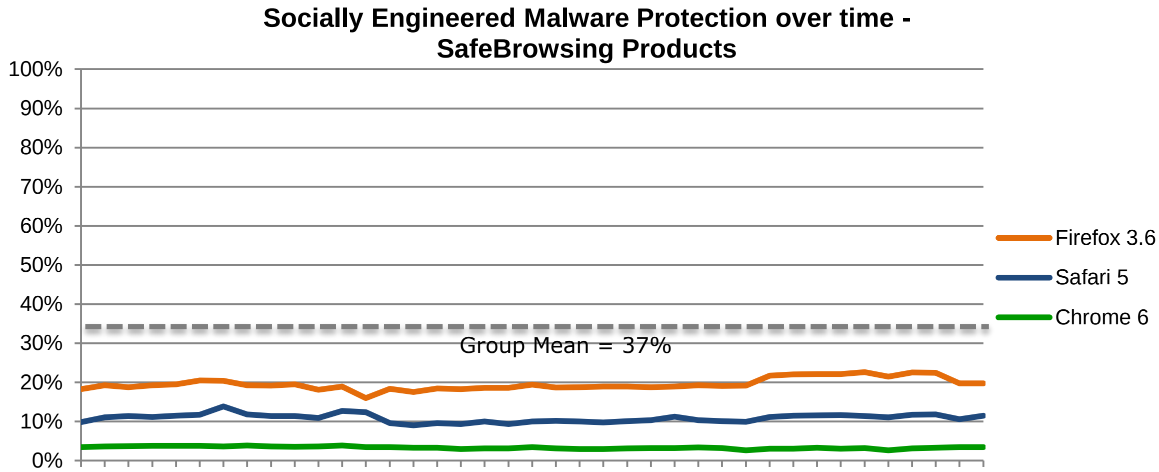
As seen on the graph, both Internet Explorer 8 and 9 demonstrated a very high level of protection. Safari, Firefox, and Chrome were consistent— albeit at a much lower level of protection.



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. So, 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.

2.4 SAFE BROWSING PRODUCTS

Even though Chrome, Firefox, and Safari all use the Google Safe Browsing data feed, our testing detected 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 browser vendors.



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.

During our smoke-test (pre-test), we discovered Safari was having trouble communicating with the Safe Browsing service, and was therefore providing inconsistent protection. The solution was to delete the Safe Browsing database and then restart Safari so the database would rebuild itself. We had to do this several times during the test. This is a known issue with prior versions that has been popping up on forums and discussion boards recently, and has not yet been resolved by Apple.[6] Separately, the overall results from browsers using the Safe Browsing API in this test declined significantly compared to the previous tests.

Product	Q1 2010	Q3 2010
Firefox 3.6	29%	19%
Safari 5	29%	11%
Chrome 6	17%	3%

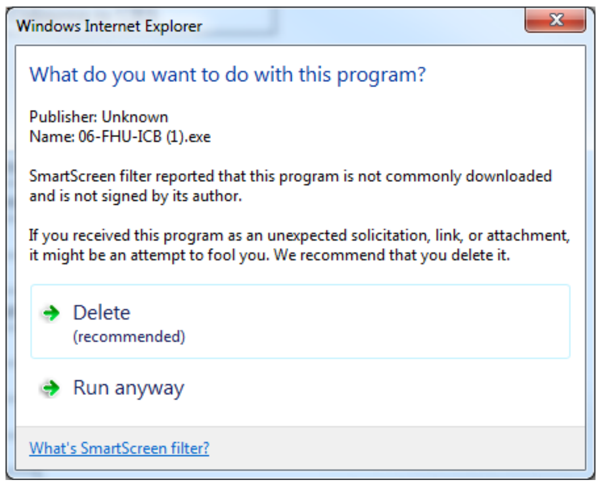
[6] "The Google Safe Browsing Service is Unavailable", http://discussions.info.apple.com/message.jspa?messageID=9725899

Upon further research, we found that in early 2010, Google made a new version of the Safe Browsing API available[7]. This new version was designed to be more efficient in terms of bandwidth usage, and help scale the Safe Browsing service.[8] Given the results, it is clear that the new implementation of the Safe Browsing service is not blocking malware URLs as successfully as before.

Lastly, as mentioned in Section 2.2.1 and indicated in the Malware URL Response Histogram, the Safe Browsing products' protection rates were showing signs of converging at just under 20%. This supports the notion that there are operational differences between the implementations of the API, but that the block lists for Firefox and Safari are the same (or very similar).

2.5 Microsoft's IE9 and Application Reputation

Internet Explorer 9 is currently in beta, and shows a 9% improvement over version 8. One notable addition to Internet Explorer 9 is the application reputation system. This new capability helps users discern malware, and potentially unsafe software from actual good software.

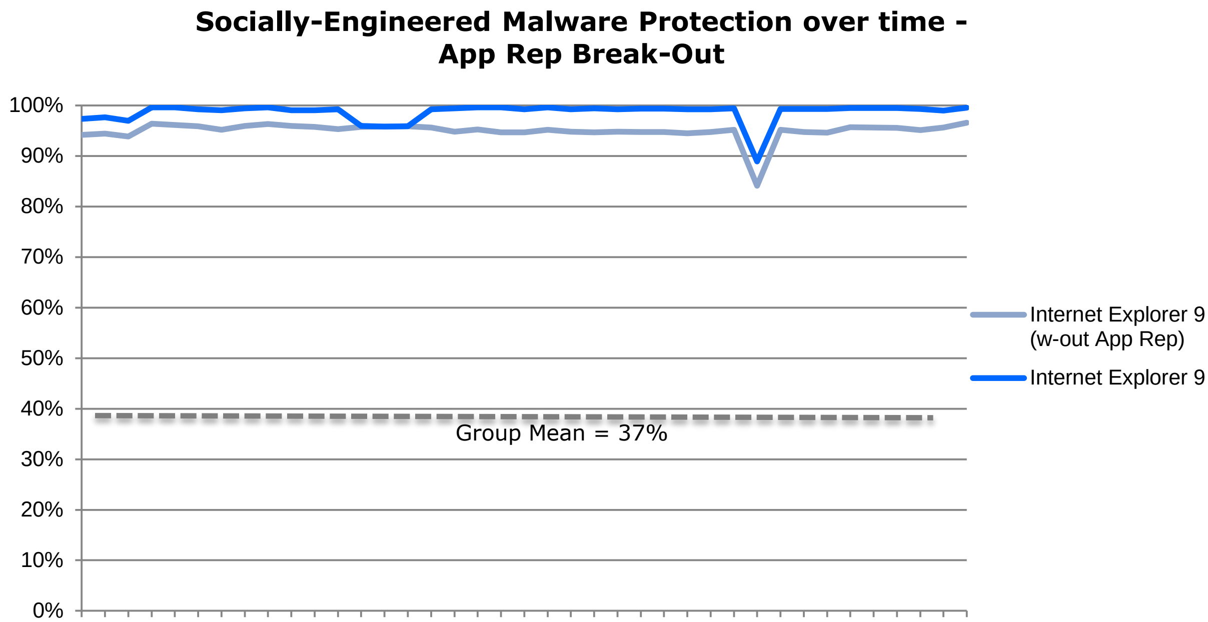


The basic value of application reputation is in its ability to add context for the user so that the user will question whether or not the source of the download is to be trusted. Users may opt-in to this feature as part of the recommended settings. In our testing, we were able to identify the additional protection of this feature based on the type of block message.

---

7 Google Safe Browsing API Developers Guide v2, http://code.google.com/apis/safebrowsing/developers_guide_v2.html#Changes

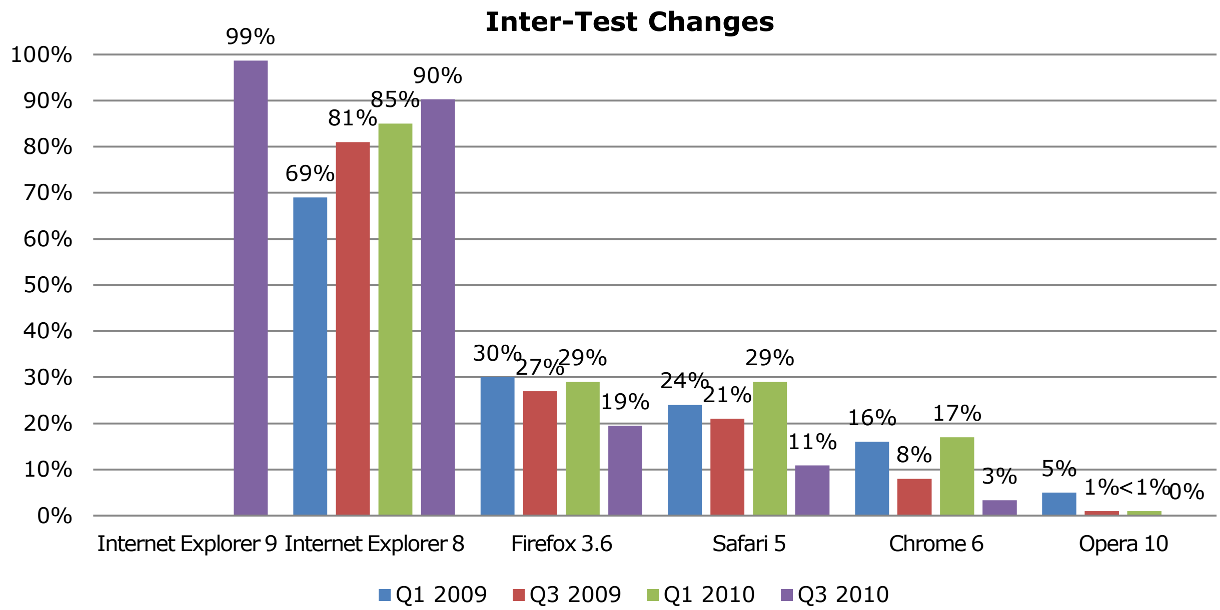
8 Google Safe Browsing API (Labs), http://code.google.com/apis/safebrowsing/



As is visible from the results, the addition of application reputation technology boosts Internet Explorer 9's protection capabilities an additional 4% to 99%.

2.6 Inter-Test Changes

Using the same test methodology for the Q1 2009, Q3 2009, Q1 2010, and Q3 2010[9] tests allows for an easy "apples-to-apples" comparison of performance changes over time. As demonstrated by the following table, Internet Explorer 8 increased its protection by 9% since Q3 2009 and 16% since the initial Q1 2009 test.



The protection offered by all browsers declined from the previous test, with the exception of Internet Explorer 8, which increased by 5%. Over the past several tests, Internet Explorer has been consistently trending upwards while protection from other products has been erratic.

All of the products that utilized Google Safe Browsing exhibited a significant decline from Q1 2010, likely due to the new v2 of Safe Browsing API.

In the current test Opera offered no protection from socially-engineered malware.

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 improve their IE malware protection in **Internet Explorer 8** (through its SmartScreen® Filter technology) and in **Internet Explorer 9** (with the addition of SmartScreen application reputation technology). With a unique URL blocking score of 94% and over-time protection rating of 99%, Internet Explorer 9 was by far the best at protecting against socially-engineered malware. The 89% zero-hour block rate suggests a far superior malware identification, collection, and classification method.

Firefox 3.6 achieved a 19% protection rating, a decline of 10% from our prior test —80% less protection than Internet Explorer 9 and 71% less than Internet Explorer 8. Firefox exhibited a considerable deterioration in protection from our last test which can be attributed to either the implementation of Safe Browsing API v2 or new tactics being used by cybercriminals which Safe Browsing has not yet adapted to. Protection was consistent during our test, a sign that the operational processes are improved. There was a slight 2.8% improvement between zero-hour protection (17.9%) and eventual protection at the 11 day mark (20.8%).

Safari 5 achieved an 10% protection rating, a decline of 18% from our prior test. Safari did appear to be converging with Firefox at just over 20% block rate after 11 days, however there is a considerable lag in protection so that zero-hour protection is just under 10%.

With a protection rating of just 3%, **Chrome 6** dropped more than 14% from our last test. And, Chrome's unique URL score of 4% was also a major decline. Chrome's overall poor protection makes it difficult to compare it to other Safe Browsing API-related products.

Opera 10's overall blocking rate of 0% was consistent with results from our last test. Once again, we double-checked the setup and manually verified a significant portion of URLs. In addition, given Opera's publicly announced partnership with AVG, we verified that Opera was not blocking malware that was caught by AVG's *Online Shield* reputation system, indicating that the technology integration is not yet complete. Users should not expect any protection against socially-engineered malware from Opera 10.

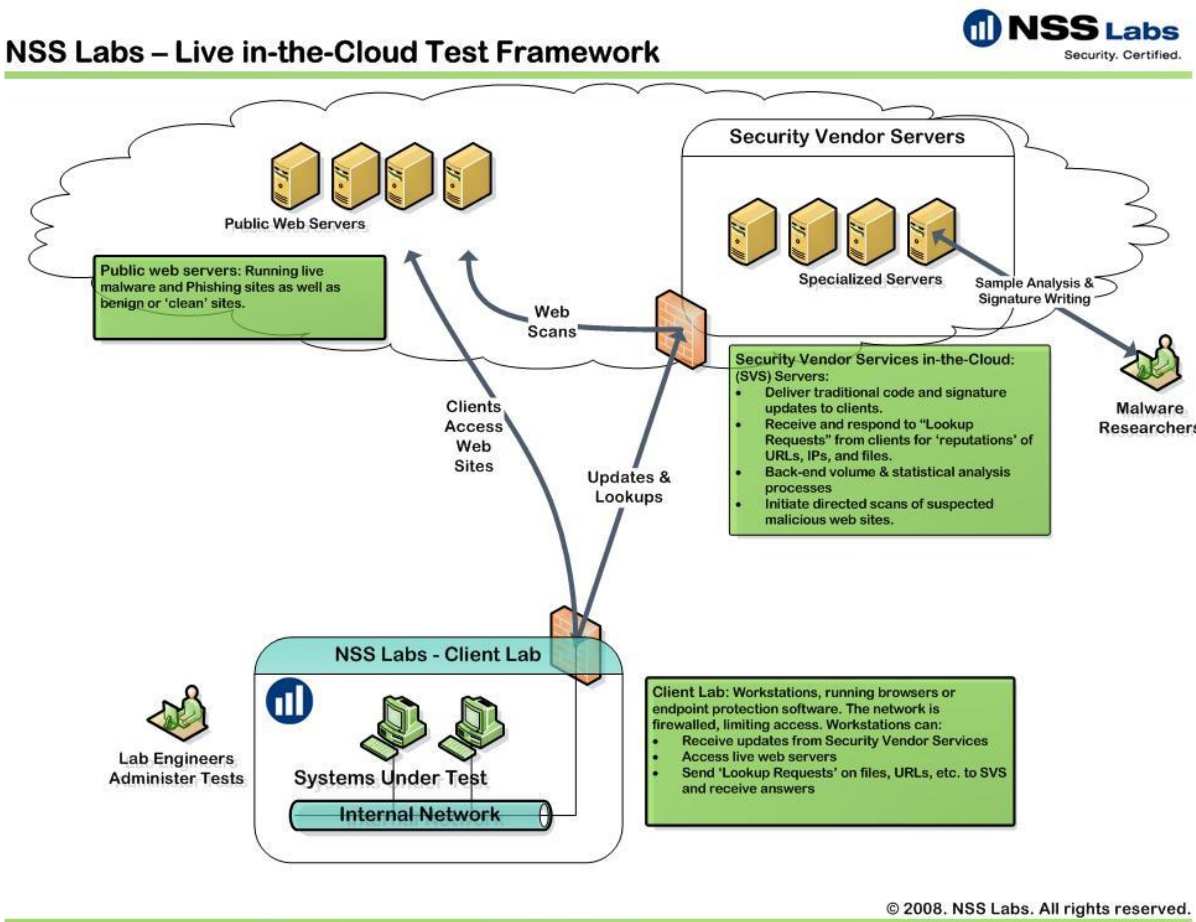
Browsers provide a layer of protection against socially-engineered malware, in addition to endpoint protection products; as this report shows, not all are created equal. Users should ensure that they are running the latest version available of their browser, with the latest browser and operating system updates at all times. However, the overall decline in protection offered by Firefox, Safari, and Chrome is concerning and users should be sure to purchase endpoint protection products that offer strong reputation-based malware protection to compensate for the lack of protection offered by those browsers. Internet Explorer users should upgrade to IE 8 and consider upgrading to Internet Explorer 9 at the earliest opportunity.

Look for upcoming tests of endpoint protection products from NSS Labs in Q4 2010 to help select the optimal endpoint protection / anti-virus product to compliment your browser selection.

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.



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 v6.0.472.63
- Windows Internet Explorer 8 (build 8.0.7600.16385)
- Windows Internet Explorer 9 pre-BETA (build 9.0.7930.16402)
- Mozilla Firefox v3.6.10
- Opera v10.62 (build 3500)
- Safari v5.0.1(7533.17.8)

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 up to 48 desktop systems each running a web browser—eight each per web browser (six browser types). Results were recorded into a MySQL database.

4.4 About this Test

This private test was contracted by Microsoft’s SmartScreen product team as an internal benchmark, leveraging our Live Testing framework. It has subsequently been approved for public release.

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 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 11 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

First, 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. NSS Labs' continuously growing archive of malware and viruses 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: e-mail, instant messaging, social networks, and malicious websites. No content was used from the tested parties.

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 which 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.

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: