BROWSER SECURITY COMPARATIVE ANALYSIS

Socially Engineered Malware Blocking

2013 - Randy Abrams, Jayendra Pathak, Orlando Barrera

Tested Vendors

Apple, Google, Microsoft, Mozilla, Opera

Overview

The web browser is the primary vector by which malware is introduced to computers. Links in phishing emails, compromised web sites, and trojanized "free" software downloads all deliver malware via web browser downloads.

The web browser is also the first line of defense against malware infection. Browsers must provide a strong layer of defense from malware, especially in mobile operations, rather than relying upon third-party anti-malware solutions and operating system protections. This test examines the effectiveness of five leading web browsers in blocking socially engineered malware.

Five leading browsers were tested against 754 samples of real-world malicious software. Major differences in the ability to block malware were observed. Data represented in this report was captured over 28 days through NSS Labs' unique live testing harness. The data provides insight into the built-in protection capabilities of modern browsers, including Chrome, Firefox, Internet Explorer, Opera, and Safari.

Beyond how much malware is blocked, the definition of "blocked" and the technologies that are used to achieve protections make a significant difference in the usefulness of that protection and in its reliability. If "blocked" includes a situation where a user is issued a warning as opposed to being given no choice, the effectiveness of blocking is affected.

If a 100% false positive acceptance rate is acceptable, it is trivial to protect users from all malicious downloads. With just a few lines of code, Firefox, Safari, and Opera could displace Internet Explorer and Chrome as the leaders of protection against socially engineered malware. However, describing every download as "malicious" would break the Internet. Finding a balance between accuracy and safety is the challenge for browsers at the front of protection technology.

Both Figure 1 and Figure 2 illustrate this challenge.

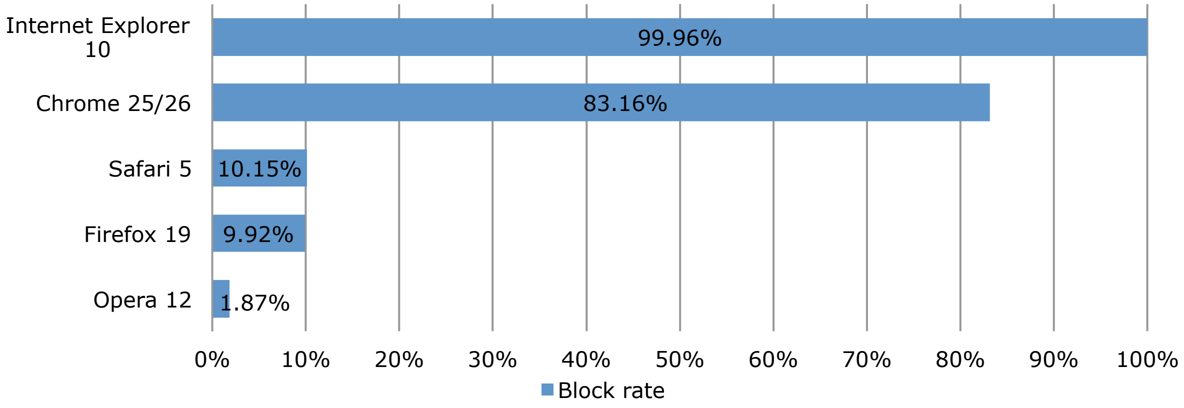


Figure 1 - Overall Malware Block Rate By Browser (Higher Values Are Better).

Figure 1 shows that Microsoft and Google are ahead of Apple, Mozilla, and Opera in terms of built-in download security protection; however, further analysis is necessary to explain adequately the difference in 99.96% and 83.16% protection rates between Internet Explorer and Chrome. These differences in protection are far from linear.

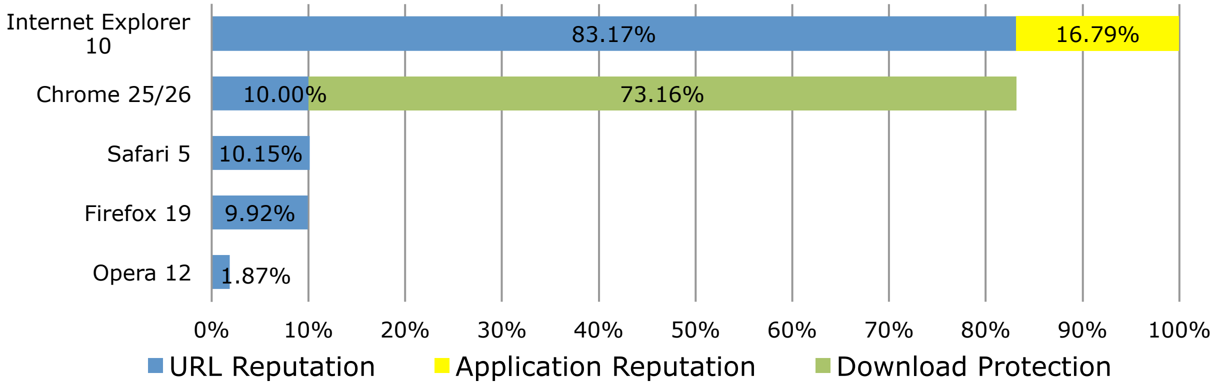


Figure 2 - Blocking Technologies Used By Browsers (Higher Is Better).

Microsoft's "*Application Reputation*" and Google's "*Download Protection*" are fundamentally both content agnostic malware protection (CAMP) schemes, however the extent to which this technology is relied on is an important differentiator, as the technology is flawed.

CAMP technology is by definition content agnostic and therefore more susceptible to false positives and user error. In order to offset the higher false positive rate of CAMP technologies the user is given a choice to block or allow content that is flagged as potentially untrustworthy, based upon reputational schemes. Good software that is not well known will be blocked. Malicious software that has been engineered to have excellent reputational aspects may evade protection. Depending on an untrained user to make the correct choice is unwise.

Figure 2 shows that without CAMP technology, Chrome demonstrates similar effectiveness to Safari and Firefox. The use of CAMP technology allows Chrome to approach the protection rates offered by Internet Explorer *prior* to the incorporation of Microsoft's own CAMP (Application Reputation) technology.During the testing period, Internet Explorer 10 had a mean malware block rate of 99.96% and Chrome had a mean malware block rate of 83.16%. Safari and Firefox, with mean malware block rates of 10.15% and 9.92% respectively, provided negligible protection but were still more than five times more effective than Opera, which blocked only 1.87% of the malware in this test.

To put the numbers in perspective, for every ten web encounters with socially engineered malware, Firefox and Safari users will be protected from approximately one attack. This implies that nine out of ten browser malware encounters will test the defenses of installed anti-virus or other operating system defenses. Chrome users will be protected from just over eight out of ten attacks and Internet Explorer 10 users will generally be afforded protection from all but about 4 out of 1,000 socially engineered malware attacks. It should be noted that some of the download protection mechanisms require a user choice and this can decrease the effectiveness of the protections. Opera users are afforded virtually no protection against socially engineered malware.

Tested Products

- Apple Safari 5
- Google Chrome 25/26
- Microsoft Internet Explorer 10
- Mozilla Firefox 19
- Opera 12

In a test running from March 13, 2013 through April 9, 2013, over 96,000 test cases were used in the data sampling captured via NSS' unique "Live Testing" harness. An initial sample set of 11,296 unique and suspicious URLs entered the system; 754 URLs were found active and malicious, and met the criteria for entry into the test. In total, 550 test runs were performed by the five browsers against these unique 754 URLs – resulting in over 18,000 test cases per browser.

Testing was repeated every 6 hours until the target URL was no longer active. Samples that did not pass the validation criteria were removed, including false positives and adware. Ultimately, 913 URL test cases passed the post-validation process and are included in the results. Each sample payload was validated internally.

NSS Labs Findings

- Malware downloads (via web browser) are the most common infection vector for criminals attempting to monetize malware via account/password theft, bank/financial fraud, gaming fraud, click fraud, and bot installation.
- The leading browsers show a significant variance in their ability to block malware. Internet Explorer 10 had the highest malware block rate at 99.96%, followed by Chrome 25/26 at 83.16%. Safari 5 and Firefox 19 were a distant third and fourth, with 10.15% and 9.92% respectively. Opera offered virtually no malicious download protection, with a 1.87% score
- Browsers with low malware block rates place consumers at significant risk.

- The download protection offered by Chrome has continued to increase. Both Chrome and Internet Explorer benefit significantly from file reputation systems combined with URL reputation and site blocking technologies.

NSS Labs Recommendations

- Users should consider browser security to be a critical part of their security.
- Users should select browsers with higher malware block rates in order to minimize risk.
- Users of less secure browsers should consider antivirus suites with robust web reputation technologies.
- Users should not rely upon browser technologies to eliminate the need for basic user security education.

Table of Contents

Table of Figures

Analysis

This report examines the ability of five different web browsers to protect users from malware downloads, also known as *socially engineered malware* (SEM).[1] Modern web browsers offer an added layer of protection against these threats by leveraging in-the-cloud, reputation-based mechanisms to warn users of potential infection. However, not all vendors have taken the same approach.

As the most widely used and ubiquitous means of accessing the Internet, web browsers are uniquely positioned to prevent malware from being downloaded or installed. When the browser fails to block a threat, it becomes the burden of the antivirus and operating systems to protect against infection. Antivirus software can be likened to a goalkeeper; if the defense allows too many shots on goal, something will eventually get through. These second line defenses have proved to be inadequate by themselves in protecting against attacks. The NSS analyst brief, *"Cybercrime Kill Chain vs. Defense Effectiveness,"* demonstrates that holes in one layer of defense are often not closed by secondary and tertiary technologies.

To complement traditional defenses and to address the highly dynamic nature of current attacks and attack distribution methods, modern web browsers employ technologies that block access to malicious URLs, before loading the content. Blocking access to malicious URLs is a formidable first line of defense, since it provides complete protection against malware entering the system. Chrome, Firefox, and Safari all demonstrate that the Google Safe Browsing API alone is not up to the task of blocking malicious downloads. Google augments its Safe Browsing API with additional download protection that is seven times more effective than the Safe Browsing API. The combination of the Safe Browsing API and Google's download protection puts Chrome on a par with Internet Explorer's URL reputation and comparable download protection schemes, but Microsoft's application reputation technology bolsters the protection IE offers against malicious downloads by an additional 16.8% above Chrome.

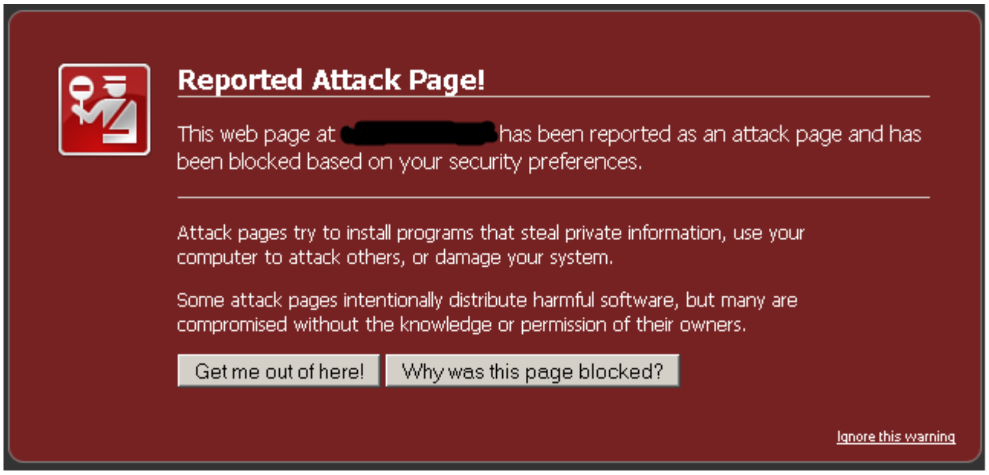
Browser protection contains two main functional components. The foundation is an in-the-cloud reputation-based system that scours the Internet for malicious web sites and categorizes files accordingly, either by adding them to a black or white list, or by assigning them a score (depending on the vendor's approach). This categorization may be performed manually, automatically, or by 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 of applications and files downloaded from the Internet. The second functional component resides within the web browser itself, requesting reputation information from the in-the-cloud systems about specific URLs and then enforcing warning and blocking functions.

When results indicate that a site is "bad," the web browser redirects the user to a warning message or page, which states 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 likely to be 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.

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

Safe Browsing vs. Application Reputation

The core functionality of URL blacklisting is to protect against drive-by downloads, as opposed to socially engineered malware delivery. NSS determined that Google's Safe Browsing API v2 includes additional download protection that has been integrated into Chrome, but not into Firefox or Safari. This functionality provides reputation services for executable files or, as Google describes them, "malicious downloads." Internet Explorer uses a different technology, known as Application Reputation (App Rep), to block malicious downloads. App Rep technologies use a variety of sources to set a threshold of how trustworthy an application appears to be. This is not the same as saying that an application is good or bad. Opera uses several partners, including the Russian Internet company, Yandex, to increase browsing safety, but the sum of its efforts has been inconsequential.



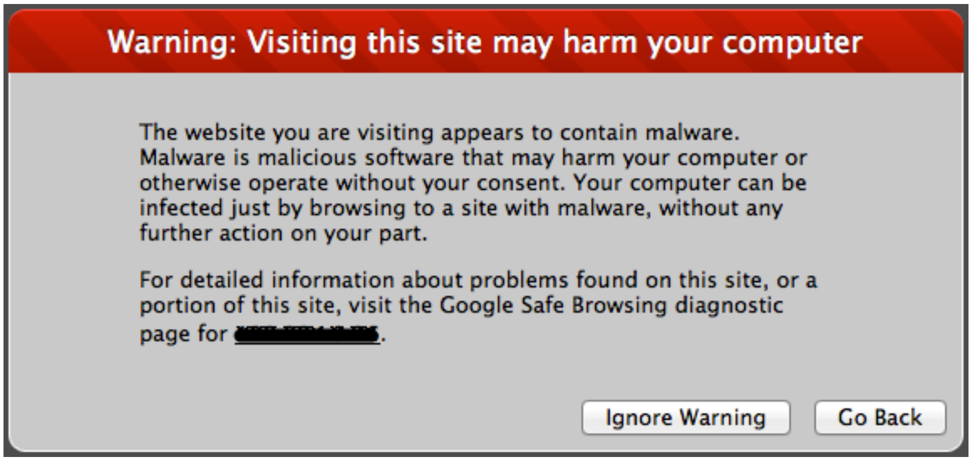
Reported Attack Page!

This web page at [redacted] has been reported as an attack page and has been blocked based on your security preferences.

Attack pages try to install programs that steal private information, use your computer to attack others, or damage your system.

Some attack pages intentionally distribute harmful software, but many are compromised without the knowledge or permission of their owners.

Figure 3 - Firefox Safe Browsing Warning.



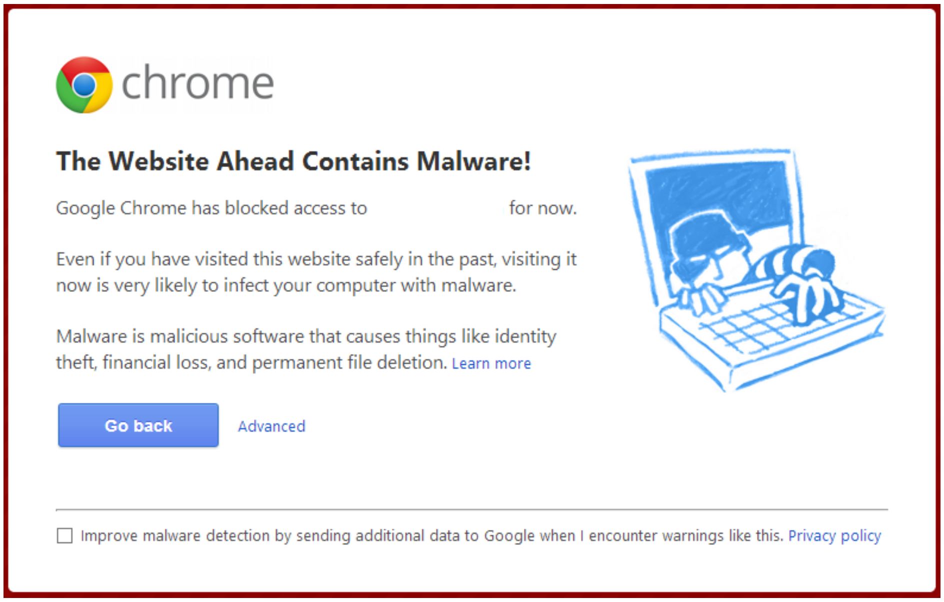
Warning: Visiting this site may harm your computer

The website you are visiting appears to contain malware. Malware is malicious software that may harm your computer or otherwise operate without your consent. Your computer can be infected just by browsing to a site with malware, without any further action on your part.

For detailed information about problems found on this site, or a portion of this site, visit the Google Safe Browsing diagnostic page for [redacted].

Figure 4 - Safari Safe Browsing Warning.

Both Firefox and Safari use Google's Safe Browsing API, and their blocking rates are, predictably, comparable. In 2012, NSS testing found these products to be within one percentage point of each other. Google's Chrome browser was no more effective in its use of the Safe Browsing API than Apple's. However, Chrome does not rely upon the Safe Browsing API alone; Google has added its download protection technology to increase the protection offered by Chrome against socially engineered malware.



chrome

The Website Ahead Contains Malware!

Google Chrome has blocked access to for now.

Even if you have visited this website safely in the past, visiting it now is very likely to infect your computer with malware.

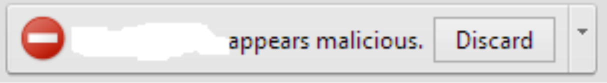
Malware is malicious software that causes things like identity theft, financial loss, and permanent file deletion. Learn more

Go back Advanced

□ Improve malware detection by sending additional data to Google when I encounter warnings like this. Privacy policy

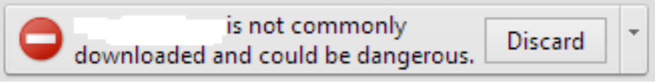
Figure 5 - Chrome Safe Browsing Warning.

Figure 5 depicts a safe browsing alert in Chrome. There are two additional file-based blocks that result in Chrome providing significantly superior protection over Firefox and Safari.



appears malicious. Discard

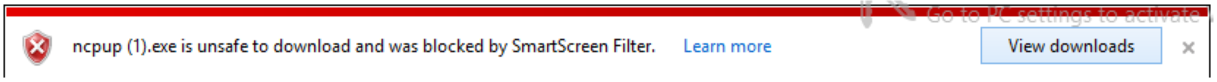
Figure 6 - Chrome Malicious File Blocking.



is not commonly downloaded and could be dangerous. Discard

Figure 7 - Chrome Application Reputation Blocking.

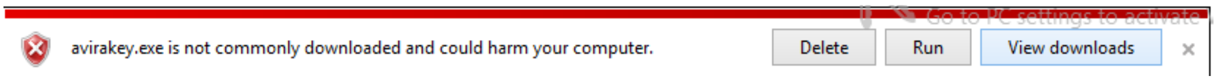
In certain situations, a web site may not be blocked; however, a malicious file may be present. In other cases, a reputation system such as Microsoft's App Rep is used to determine whether a file is not well enough known to establish trust. In these cases, the dialog boxes in Figure 6 and Figure 7 will appear.



ncpup (1).exe is unsafe to download and was blocked by SmartScreen Filter. Learn more View downloads ×

Figure 8 - Internet Explorer SmartScreen Warning.

Internet Explorer's answer to Google's Safe Browsing API includes Microsoft's SmartScreen as well as URL reputation. Just these components alone in Internet Explorer match the protection of Chrome.



avirakey.exe is not commonly downloaded and could harm your computer.

Figure 9 - Internet Explorer App Rep Warning.

Figure 9 shows the App Rep technology that Microsoft has built into Windows 8 and into Internet Explorer 10. When App Rep is combined with Microsoft's other technologies, Internet Explorer provides almost 100% protection against malicious downloads. Microsoft's App Rep is also available in Internet Explorer 9 running on Windows 7. Theoretically, the underlying OS should be irrelevant if the protections are wholly contained in IE 10; however, NSS has not tested IE 10 on Windows 7, and therefore it cannot be assumed that the same level of protection is offered by that combination.

Malware Block Performance

Each browser's individual block performance was tracked, and an overall block rate of all malware collected by browser was developed. A browser's overall block rate is defined as the percentage of successful blocks divided by the total number of test cases. With tests conducted every 6 hours, a URL that was online for 48 hours will be tested 8 times. A browser blocking it on 6 (out of a maximum 8) test runs will achieve a block rate of 75%. Figure 10 shows the overall block performance of the four browsers tested. As expected, since Firefox and Safari are using the same technology, they are achieving similar block rates. However, the large difference of the average block rate between browsers is noteworthy, with results ranging from 2% to almost 100%.

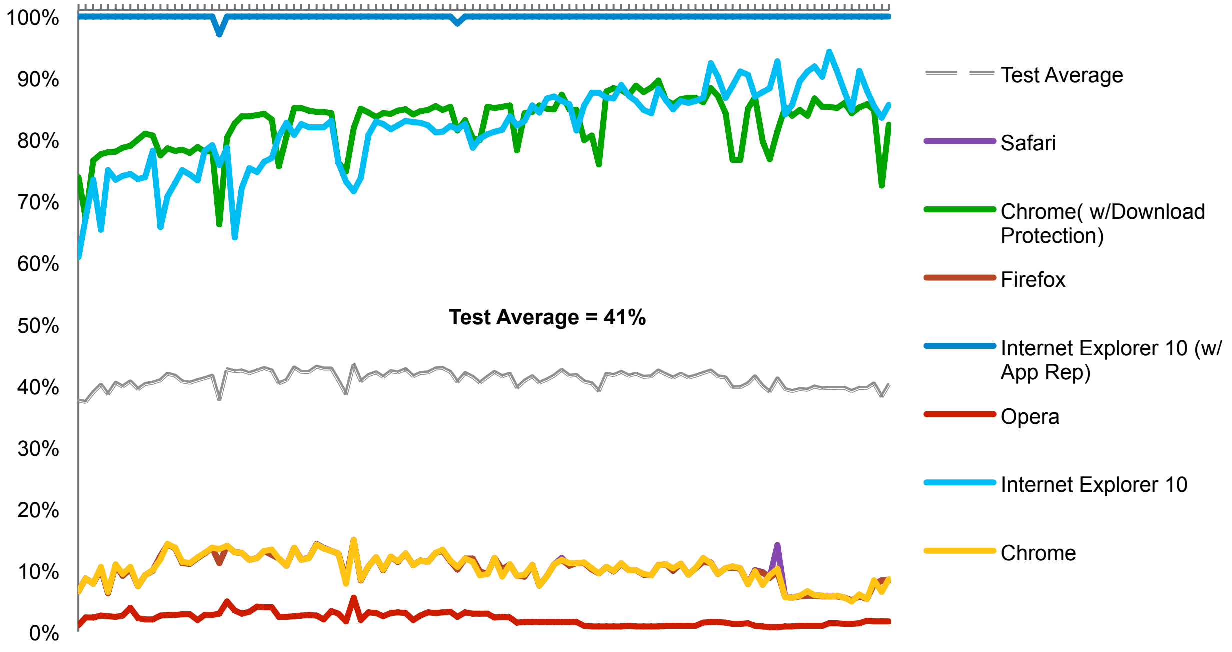


Figure 10 - Malware Block Rate Over Time.

To assess the effectiveness of different blocking technologies, the NSS test harness also records the mechanism that blocked access to a URL.

Of the three browsers using Google's Safe Browsing API, Chrome is the only one to also utilize Google's malicious download technology; this technology attempts to block malicious downloads from sites that are not blocked by URL reputation. Figure 10 shows the block performance of the URL blocking component and the additional download block component used by Google's Chrome and Internet Explorer. The URL blocking performance of the three Safe Browsing technology browsers was consistent at about 10%. Google's malicious download protection proved to be approximately seven times more effective than URL blocking alone, increasing overall blocking performance by 73.2% when compared to URL blocking alone. The malicious download technology accounts for the majority of the blocking performance of Google Chrome.

The core protection technology within Internet Explorer is SmartScreen, which provides URL-based protection from attacks via an integrated, cloud-based URL-reputation service, as well as known malicious file blocking. Microsoft also uses App Rep to great advantage to boost protection levels. On the face of it, Chrome has virtually identical protection to Internet Explorer 10, at approximately 83%. However, Chrome relies on the arguably less reliable CAMP technologies to achieve that. For Internet Explorer, App Rep picks up the bulk of the remaining 17% of the malicious files that were encountered in the test, resulting in a protection level approaching 100%.

The Reality Of Application Reputation

Both Google's and Microsoft's application reputation blocking technologies are likely to yield less effective real-world results than in an automated test environment.

Application reputation technologies allow untrained users to override the protection mechanisms used to protect against malicious application downloads. Although there are times that this is appropriate, there is also the danger that social engineering attacks can deceive users into bypassing the file blocking and installing malicious software. In NSS testing, a successful block was always assumed if a URL was presented as a threat.

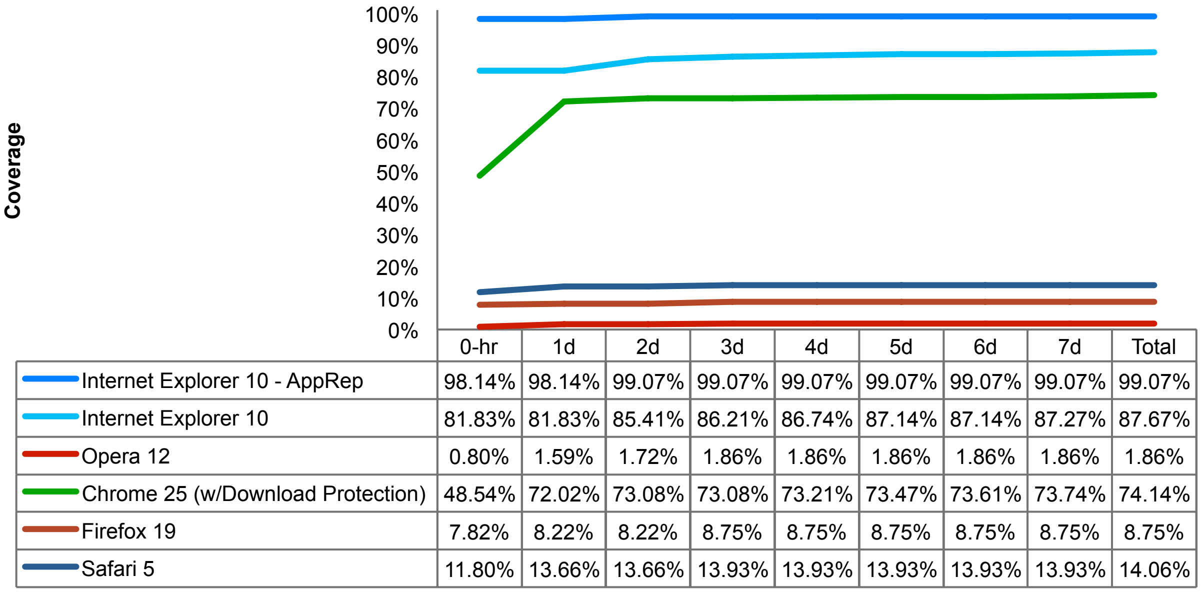
If it were arbitrarily assumed that users would override Internet Explorer's application reputation component about 10% of the time, then Internet Explorer would be assumed to have a 90% block rate, more than 10% higher than Google's unmodified score. Without empirical testing of user behavior outside the lab, it is not known how often application reputation warnings are ignored. It cannot be assumed that the usage rates would be identical for Chrome and Internet Explorer users, since the exact wording of the warning message, as well as the difficulty in overriding the block, will affect absolute rates.

Regardless of the shortcomings of systems that rely upon untrained users to make correct choices, application reputation is a highly significant and effective protection technology.

Google marketing recently collaborated on a research paper about Google's Content-Agnostic Malware Protection (CAMP) technology. Several news organizations reported that Google was claiming a 99% malware detection rate for CAMP. However, closer examination of the paper in question reveals the actual claim was that CAMP "exhibits accuracy close to 99% relative to proprietary VM-based dynamic analysis". Comparison to a "proprietary virtual machine" is one way for a marketing department to avoid having to publish disappointing results, while attempting to make technology look nearly perfect. In real world testing, the combination of the Safe Browsing API and Google's CAMP is 83% effective at blocking malware. This is significantly lower than the 99% that is claimed by Google; the difference is explained by the fact that NSS compares empirically validated block rates to what actually evades detection by the technology under test.

Time To Block Malicious Sites

When new online attacks are created and deployed, it is vital that they are detected as quickly as possible. The following response time graph displays how long each of the browsers took to block a threat, once the threat was introduced into the test cycle. Cumulative protection rates are calculated each day until blocked.



	0-hr	1d	2d	3d	4d	5d	6d	7d	Total
Internet Explorer 10 - AppRep	98.14%	98.14%	99.07%	99.07%	99.07%	99.07%	99.07%	99.07%	99.07%
Internet Explorer 10	81.83%	81.83%	85.41%	86.21%	86.74%	87.14%	87.14%	87.27%	87.67%
Opera 12	0.80%	1.59%	1.72%	1.86%	1.86%	1.86%	1.86%	1.86%	1.86%
Chrome 25 (w/Download Protection)	48.54%	72.02%	73.08%	73.08%	73.21%	73.47%	73.61%	73.74%	74.14%
Firefox 19	7.82%	8.22%	8.22%	8.75%	8.75%	8.75%	8.75%	8.75%	8.75%
Safari 5	11.80%	13.66%	13.66%	13.93%	13.93%	13.93%	13.93%	13.93%	14.06%

Figure 11 - Time To Block Malicious Sites.

When Google announced the acquisition of Virus Total, there was speculation that it would be used to enhance Google's download protection. Chrome's performance has improved by 13% since its analysis in the 2012 NSS report, *"Browser Security Comparative Analysis: Socially Engineered Malware."* The use of Virus Total information may also play a role in the sharp increase in protection between zero-hour and day 1; however, Internet Explorer's implementation of App Rep demonstrates that reputation is a more effective browser security technology than actual malware detection. There are add-ons for Firefox and Safari that help to improve security but, in general, these protective technologies are neither used, nor understood by the non-technical users. For the average user, Internet Explorer 10 or Chrome is recommended. Users choosing Safari, Firefox, or Opera will want to use add-ons and other technologies to augment their protection where possible.

Appendix A – Methodology

Client Host Description

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

Microsoft® Windows 8 Enterprise®
4GB RAM
60GB hard drive

Figure 12 - Virtual Machine Specifications.

Browser machines were tested prior to the test and during the test, to ensure proper functionality. Browsers were given full access to the Internet to enable them to visit live sites.

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 that testing began. The following is a current list of the web browsers that were tested:

- Apple Safari® v5.1.7 (7534.57.2)
- Google ChromeTM v25 and v26
- Microsoft® Internet Explorer® 10
- Mozilla® Firefox® v19.0.2
- OperaTM v12.14 Build 1738

Once testing began, the product version was monitored, and new updates were applied in a realistic patching methodology. As a new version of a browser was made publicly available during the testing window, NSS would update the test harness machines and run both versions in parallel over the course of a two-week phase-out of the prior version of the browser. This maintained the integrity of the virtual instances that were under test, while still allowing for fresh instances to start with the new browser version. 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.

Network Description

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

The host system had one network interface card (NIC) and was connected to the network via a 1Gb switch port. For the purposes of this test, NSS Labs utilized 120 desktop systems, with each system running a web browser. Results were recorded into a MySQL database.

Test Duration

NSS' browser test was performed continuously for 28 days. Throughout the test, new URLs were added as they were discovered.

Test Frequency

Over the course of the test, each URL was run through the test harness every six hours. Regardless of success or failure, NSS continued to attempt to download a malware sample with the web browser for the duration of the test.

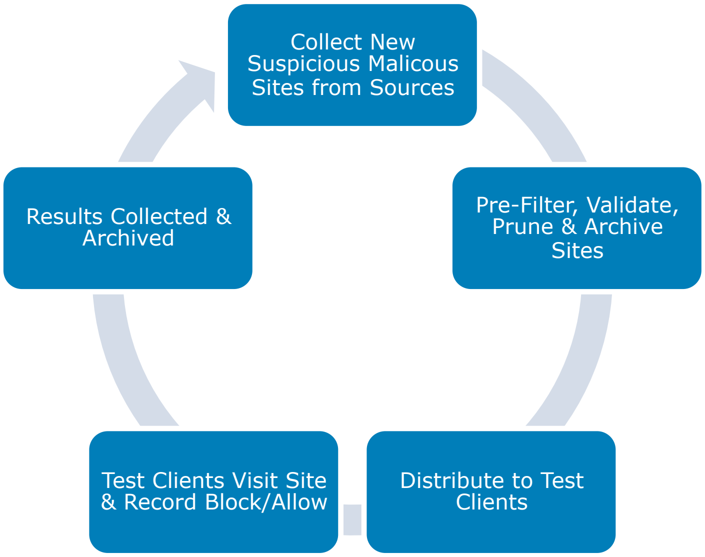

Collect New Suspicious Malicous Sites from Sources
Pre-Filter, Validate, Prune & Archive Sites
Distribute to Test Clients
Test Clients Visit Site & Record Block/Allow
Results Collected & Archived

Figure 13 - NSS Labs Browser Test Harness.

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 received a broad range of samples from a number of different sources.

Sources

NSS operates its own network of spam traps and honeypots. These e-mail accounts with high-volume traffic yield thousands of unique e-mails and URLs per day. In addition, NSS maintains relationships with other independent security researchers, networks, and security companies that 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 is used from the tested parties.

Malicious URLs targeting users throughout the globe are identified and selected for inclusion in this test. Users are defined as individuals residing within the North American, 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. This report is comprised only of data from the United States of America samples; future papers will include additional data gathered.

The ultimate determinant of whether or not a malicious URL is included in this test is its participation in a malware campaign targeting users. The use of a malicious URL in a campaign targeting an Asia-Pacific or a North American user does not necessarily preclude its use in other campaigns targeting users from other regions.

Exploits containing malware payloads (exploits plus malware), also known as "clickjacking" or "drive-by downloads," are excluded from the test. Every effort is 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," including sites from Yahoo, Amazon, Microsoft, Google, NSS, major banks, and others. Periodically, clean URLs are run through the system to verify that the browsers are not over-blocking.

Catalog URLs

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

Confirm Sample Presence of URLs

Timing is critical since the 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 is given a brief review to verify that it is 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 occurs within minutes of receiving the samples from NSS sources. **Note:** These classifications are further validated after the test, and URLs are reclassified and/or removed accordingly.

Archival Of Active URL Content

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

Dynamic Execution Of 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 records whether or not the malware is downloaded and if the download attempt triggers a warning from the browser's malware protection.

Scoring And Recording The Results

The resulting response is recorded as either "Allowed" or "Blocked and Warned."

Success: NSS Labs defines success as a web browser *successfully* preventing malware from being downloaded and *correctly* issuing a warning.

Failure: NSS Labs defines failure as a web browser *failing* to prevent the malware from being downloaded and/or *failing* to issue a warning.

Pruning

Throughout the test, lab engineers review and remove non-conforming URLs and content from the test execution set. For example, a URL that was initially classified as malware, but that has since been replaced 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 is 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 that is unavailable for one test iteration become available for a subsequent iteration, it will be added back into the test collection. Unavailable samples are not included in calculations of success or failure by a web browser.

Post-Test Validation

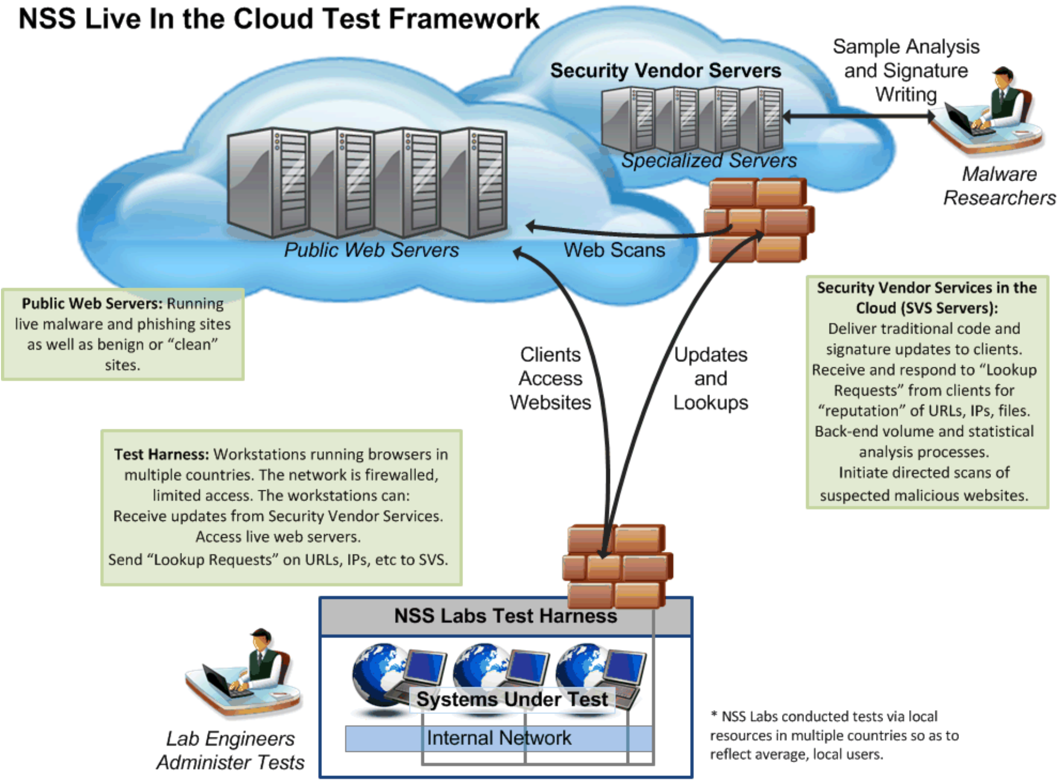
Post-test validation enables NSS to reclassify and even remove samples that were either not malicious or not available before the test started. NSS uses the Norman® Analyzer sandbox to prune and validate the malware. Further validation is performed using proprietary tools, system instrumentation, and code analysis as needed.

NSS Labs Test Environment and Methodology

NSS has created a complex "Live Testing" 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.

The purpose of the study was to determine how well current web browsers protect users from the most prevalent malware threats on the Internet today. An important aspect in any test of this nature is the timing. Given the aggressive manner in which criminals propagate and manipulate malicious websites, a key objective is to ensure that the "freshest" sites possible are included in the test.

As part of the live test methodology, web-based threats are continually collected from multiple sources, including partners' and NSS' own servers and high-interaction honeynets. Potential threats are screened algorithmically before being inserted into the test queue; threats are continually inserted and screened throughout the test. Unique in this procedure is that NSS validates the samples before and after the test. Actual testing of the threats is repeated every six hours and starts with validation of the site's existence and conformance to the test definition. All tests are executed in a highly controlled manner, and results are recorded and archived at each interval.



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 "reputation" of URLs, IPs, files. Back-end volume and statistical analysis processes. Initiate directed scans of suspected malicious websites.

Test Harness: Workstations running browsers in multiple countries. The network is firewalled, limited access. The workstations can:
Receive updates from Security Vendor Services.
Access live web servers.
Send "Lookup Requests" on URLs, IPs, etc to SVS.

* NSS Labs conducted tests via local resources in multiple countries so as to reflect average, local users.

Figure 14 - NSS Labs Live In-The-Cloud Test Framework.

Contact Information

NSS Labs, Inc.
206 Wild Basin Rd.
Building A, Suite 200
Austin, TX 78746 USA
+1 (512) 961-5300
info@nsslabs.com
www.nsslabs.com

V. 130513c

This report was produced as part of NSS Labs' independent testing information services. Leading products were tested at no cost to the vendor, and NSS Labs received no vendor funding to produce this report.

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 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.