

The Browser Wars Just Got Ugly

Summary

Internet Explorer, Firefox, and Chrome were the subject of a [Google-funded publication](#) by security reseller Accuvant in which Google Chrome comes out on top, seemingly at the expense of Mozilla Firefox. What should end users make of the results? At the request of several enterprise clients, NSS Labs has reviewed the Google/Accuvant publication and supporting tools and data to provide an independent opinion. NSS analysts have also examined data from ongoing NSS Labs browser research to provide additional guidance.

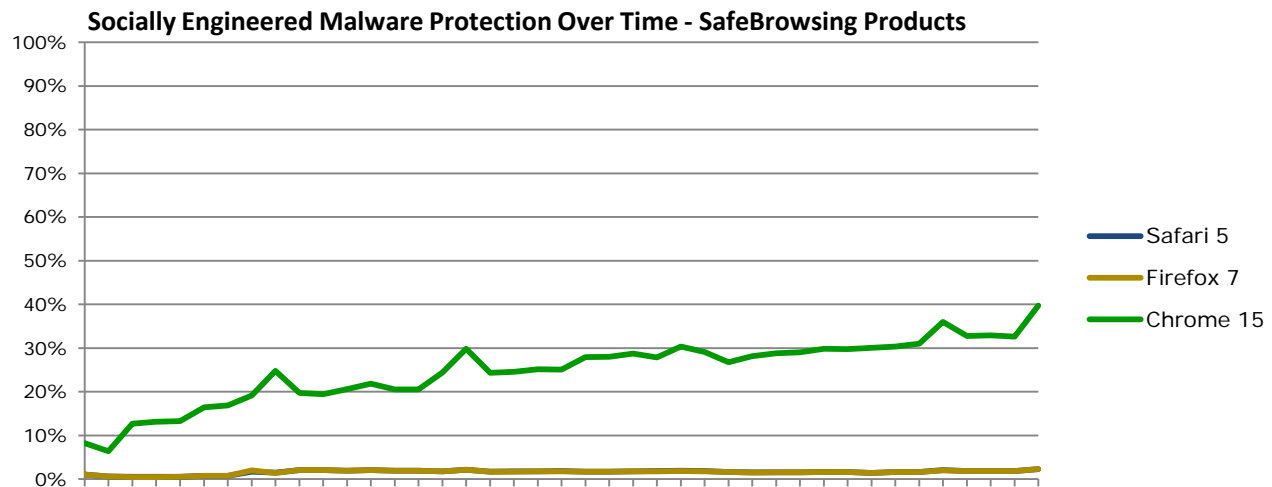
Overview

The timing of the Google/Accuvant report¹ is interesting, given that Google's search contract with Mozilla expired at the end of November. Given that this report was commissioned much earlier in the year – according to the paper, research was completed in July 2011, yet was not published until December 2011 – this would suggest a larger strategic move by Google to eliminate the competition. Examination of the test methodology indicates bias in favor of Google Chrome at the expense of Mozilla Firefox.

The Google/Accuvant report does an excellent job of explaining the various browser security technologies such as JIT hardening, sandboxing, etc., and its authors are recognized as leading vulnerability researchers. However, it is possible for vendors to game a test and gain an unfair advantage by influencing the test methodology. That appears to be what happened in this case, unsurprising given the source of funding for the project. Unfortunately, the clear bias in the test methodology does a disservice to the researchers' work, and diminishes the report to a propaganda piece for Google. Upon examination, it became evident that important security technologies incorporated within Firefox (such as frame poisoning) were not included in the test methodology.

In addition, NSS Labs' own ongoing (and completely independent) research shows that, in the 11-day period from November 22nd through December 2nd, Chrome increased its protection against traditional malware from 8% to nearly 40% (a 5x increase), while Firefox and Safari declined to less than 2% protection in the same period.

¹ Browser Security Comparison: A Quantitative Approach, Accuvant,
http://www.accuvant.com/sites/default/files/AccuvantBrowserSecCompar_FINAL.pdf
<http://www.accuvant.com/sites/default/files/Google%20Package%20v1.zip>



As the above chart illustrates, the new reputation-based protection against malware offered by Chrome does not appear to be part of the SafeBrowsing API, indicating that Google no longer believes it is in its interest to share with partners/competitors such as Firefox and Safari.

It appears Google has purposefully withheld important malware protection from its SafeBrowsing feed coinciding with its break from Firefox and release of the Google-funded report by Accuvant. This episode could indicate a more aggressive direction for Google.

NSS Labs Findings:

- Google paid product reseller Accuvant to publish a report comparing browser security. However, given the deficiencies in the methodology it would appear that the main aim of the report was to undermine confidence in Firefox. Either Accuvant has been lax in defining its methodology, or Google – as the project funder – has asserted undue influence in the production of that methodology to its own advantage. Accuvant may have been used unwittingly, of course - however that is one of the dangers in publishing vendor-funded test reports².
- Methodology matters! Unfortunately, the integrity of the methodology is often the first casualty in vendor-driven reports, as would appear to be the case in this report. Upon examination it became evident that key security technologies incorporated within Firefox (such as frame poisoning) were not included in the test methodology. And the JIT hardening analysis failed to give ample credit to the more proactive technologies employed by IE9, which happened to not be present in Chrome.
- As NSS Labs has noted on numerous occasions, design and implementation are two very different animals. Testers cannot assume a technology has been implemented properly - in fact, *that is why you test*. Yet that is exactly the mistake Accuvant made on several occasions in this report.

² NSS Labs does not publish vendor funded test reports

- Accuvant disabled highly relevant portions of non-Google browsers' protection without noting the impact on the overall results. This error in testing resulted in an erroneously negative assessment of the browsers' protection capabilities, since some browsers will **only** block malware during or after download and before execution.
- By utilizing malware sites garnered exclusively from free public lists, the malware sample set was highly skewed in Google's favor. Justifying not using high-quality, professional malware feeds because Microsoft and/or Google may or may not subscribe to them is highly suspect. Testers should source samples that most accurately reflect threats to users, regardless of the impact on vendors.
- The Historical Vulnerability Analysis section applied highly questionable logic in an apparent effort to downplay Google Chrome's very poor showing. Having to disclose over 300 vulnerabilities during a 30 month period is a problem, not a virtue.
- It appears Google has withheld important malware protection from its SafeBrowsing feed coinciding with its break from Firefox and release of the Google-funded report by Accuvant.

NSS Labs Recommends:

- If you choose to read the Google/Accuvant report, do so with the understanding that the methodology appears to be skewed in Google's favor, and does not reflect real world attack scenarios.
- For those curious about the inner workings of sandbox and JIT hardening technologies, the detail provided in this report is informative and mostly accurate.
- Do not draw conclusions on overall browser security (or lack thereof) based upon this one report.
- Keep up to date with the current version of the browser of your choice as well as third party applications; it is the best way to prevent being exploited.
- Readers should remember that there is a difference between "third party" and "independent," and that just because a document says it is independent, doesn't mean it is. The easiest way to discern the difference is to "follow the money trail".

Analysis

How vulnerable a modern web browser is to attack is certainly a high profile question. It is a well-documented phenomenon that new software contains more bugs (which may expose vulnerabilities) than software that has been around for a while. It is part of the software development lifecycle. Examining historical data on the number of vulnerabilities discovered during a period of time provides insight into the maturity of the software in question and is a good indicator of how many future vulnerabilities will be discovered.

The most frequently exploited vulnerabilities leading to system infection with malware are found in third party software such as Java software³ and the most popular exploit toolkits being used by criminal organizations (such as Black Hole) primarily target third party software (such as Java). This focus on third party applications is likely due to frequent and semi-automatic updates by browser vendors which shrinks the opportunity-time an attacker has to compromise

³ ESET Threat Blog, <http://blog.eset.com/2011/12/04/carberp-blackhole-growing-fraud-incidents>

a target, as well as the cross browser-platform nature of third party applications. In essence, if you think from an attackers standpoint, why design an exploit for Chrome 15 and a separate one Firefox 8 and a separate one for Internet Explorer 9 when they will have very short shelf life, when a single Java exploit will do the trick just fine? In addition, exploits that use interpreted languages such as Java are very difficult to defend against. Unless they have a pattern match for a known exploit, network and host intrusion prevention systems as well as anti-virus/endpoint protection products are unable to discern legitimate Java from malicious Java. So as an attacker, there is an added "stealth" benefit to exploiting third party software such as Java.

Google withholding important malware protection from its SafeBrowsing feed so that its own product has an advantage over Firefox and Safari, is an important precedent and contains echoes of accusations made against the company that it improperly provided preferential search results for its own products over third parties. While Google is entitled to improve its product, the way in which the company approached the break with Firefox should be noted.

©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:

The information in this brief is subject to change by NSS Labs without notice.

The information in this brief 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 brief 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.

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.

This brief does not imply any endorsement, sponsorship, affiliation, or verification by or with any organizations mentioned in this brief.

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