

F R E Q U E N C Y X™

STRAIGHT DOPE ON THE VULNERABILITY DU JOUR FROM **IBM Internet Security Systems**

CURRENT THREAT LEVEL

[« Strategic Security – Embedding it](#) | [Home](#)



BROWSE ARCHIVES

-- Browse by Month --

LINKS

- [About Frequency X](#)
- [Contact Us](#)
- [X-Force Web Site](#)
- [Vulnerability Disclosure Guidelines](#)
- [Subscribe to Frequency X](#)

637 million Users Vulnerable to Attack

Posted by **Gunter Ollmann** on July 01, 2008 at 8:20 AM EDT.

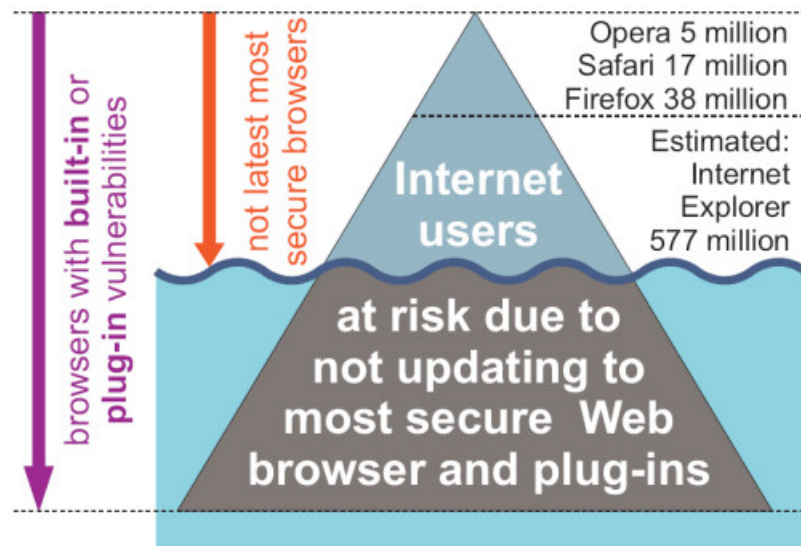
You can sum up a lot in a single number. [637 million](#). That's the approximate number of users currently surfing the Web on a daily basis with an out-of-date browser – i.e. not running a current, fully patched Web browser version – or, to put it another way, 45.2 percent of all Internet surfers have neglected to update their favorite Web browser and are potentially vulnerable to all sorts of nastiness. If you think that that's a big number, wait until you start factoring in Web browser plug-ins also missing their latest security patches.

Since the beginning of the year we've all been reading about the monthly barrage of 100,000+ or 1,000,000+ mass-defacements with injected malicious iframes (in fact I've written about a few of [them](#) on this very blog), but have you ever wondered how many hosts could be infected by the product of these defacements? – i.e. if an attacker seeded enough Web sites around the globe with Web browser exploit material, how many users would likely find their host infected with some malicious backdoor, Trojan or bot-agent?

Well, with the help of some good friends over at ETH Zurich and Google – Stefan Frei, Thomas Duebendorfer and Martin May (and the kind permission of Google management) – I was lucky enough to work with them in analyzing the daily USER-AGENT data collected by Google's Web search and application servers around the world, and managing to study how users patch and update their Web browsers. From that, we were able to work out just how many users are taking their systems integrity in their hands as they browse an increasingly dangerous Internet – 637 million in June – and that was just the tip of the iceberg.

While the full whitepaper and our analysis can be found over [here](#), I thought I'd point out a few of the more interesting security points in the meantime...

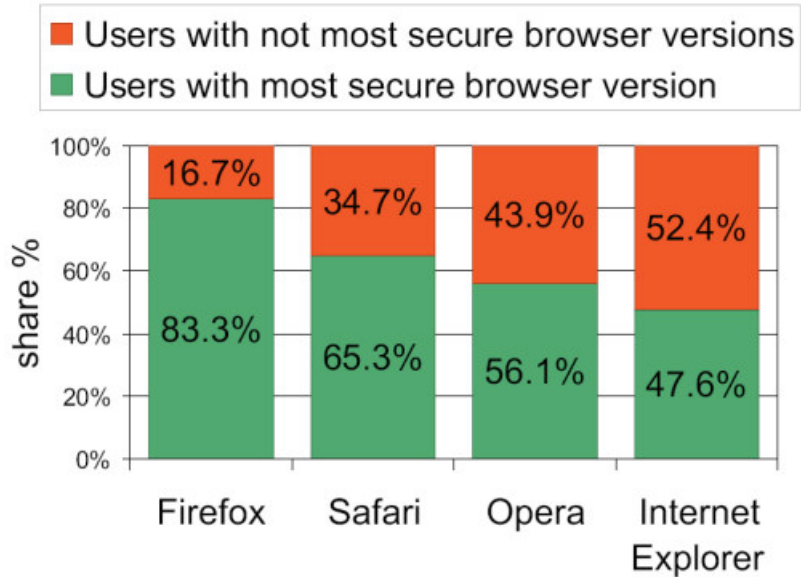
(1) I think that most people would agree that Google's visibility of the Internet is unmatched, with an estimated 75 percent or all Web searches done through their engine. That meant we had fabulous global coverage of Web browser usage. And, before you ask, no – we didn't have access to any personally identifiable information – but CO2 emissions were kept to a minimum and no small furry animals suffered any distress at our hands while writing the whitepaper. As a result, we counted some 637 million users as using out-of-date Web browsers and potentially vulnerable to popular drive-by-download attack vectors and exploits.



(2) We found that Firefox users were the most diligent in using the latest version of their favorite Web browser, with 83.3 percent of them safely surfing the Web. Meanwhile, Internet Explorer users came in last place, with less than half of them (47.6 percent)

Internet Explorer users came in last place, with less than half of them (47.6 percent) managing to surf with a fully patched IE7 installation. I think it may be a little unfair for many IE users to be grouped in the “less diligent” bucket because they’re stuck to using IE5 or IE6 for compatibility issues with their corporate applications but, quite frankly, in this climate of commercial mass-defacements, “unfair” isn’t going to keep them safe.

Share of most secure browser versions



(3) Being able to tap the USER-AGENT fields of the Web browser HTTP headers to Google’s search engines since the beginning of 2007 meant that we could also study the minor version information of popular browsers such as Firefox and Opera. There were some really interesting dynamics visible once it was all plotted out, and the most important component was the speed at which users updated their browser to the most current patched version. For example, Firefox users typically updated within three days, while Opera users managed 11 days and (cynically) Internet Explorer users are still struggling to transition to IE7 (let alone any incremental super-Tuesday patches) even after a year-and-a-half. So, with that in mind, Firefox’s auto-update system wins hands-down in my opinion.

Best Before

One of the new concepts we came up for combating the inadequacies of Web browser patching was that of applying the food industries “Best Before” date to the Web browser and its plug-ins. I know, it initially sounds a little strange, but take a gander at that section of the whitepaper and you’ll quickly see what we mean. Of all the parts to the paper, that’s the part I’m most interested in seeing how the software industry reacts.

I suspect that reactions to the concept will be quite mixed. Proponents of the concept may see dollar signs – a built-in expiry date may result in more users updating to new versions of their software for a premium price. Meanwhile, opponents could argue that it would confuse users and just become a revenue vehicle for software vendors... and the hardcore opponents may just argue that it’s the user’s fault, so why pander to them in the first place? (Obviously not my sentiment)

Personally, I think it’s a great way of helping raise the visibility of risk to users as they surf the Web – and not just for Web browsers, but for all types and classes of software.

At the moment we have a problem that a measureable 637 million users are surfing the Web daily with out-of-date and vulnerable browser technologies – and I’m pretty sure that the majority of them have no idea as to how much risk they’re exposing themselves to. A clear “Best Before” date/reminder would ram-home the fact that they’re exposed (in full Technicolor splendor).

Failing that, you could also use the “best before” date at the application Web server as a way of managing risk from your customers – e.g. a customer is using a browser that’s been “expired” for 9 months, therefore the probability that they have been infected by something in the meantime is approximately 75 percent; so it’s probably prudent to double check the account numbers that the customer is trying to transfer money to before authorizing the transfer for online banking.

Hack the Planet

Having completed this first round of research, I guess I’m a little disappointed (but not surprised) by the real number of users not taking advantage of the latest and most secure Web browsers.

As a previous naysayer to those colossally high estimates of botnet compromised hosts (public estimates of 40-200 million), I guess I’m now a little surprised that the botnets aren’t in fact much larger than the biggest reports I’ve seen. Perhaps their command and control infrastructures can’t scale to that size? </joke>

aren't in fact much larger than the biggest reports I've seen. Perhaps their command and control infrastructures can't scale to that size? </joke>

I suppose that once you factor in the 637 million users running non-current Web browser versions and mix that with the overlapping vulnerable (and unpatched) plug-in technologies, we're probably looking in the realm of 800 million to 1 billion users out there vulnerable to a "perfect storm" of current drive-by-download attacks. Talk about "hack the planet"!

I get the feeling that we can weather our way through it all though – but a little help from the browser makers probably wouldn't go amiss.



©2007 IBM Internet Security Systems. All rights reserved worldwide.

[Terms Of Use](#) | [Privacy Policy](#) | [Code Of Conduct](#) | [Trademarks](#) | [Contact Us](#)

Comments or opinions expressed on this Weblog are the opinions of the authors alone. They are not necessarily reviewed in advance by anyone but the individual authors, and neither IBM Internet Security Systems nor any other party necessarily agrees with them. The views expressed by outside contributors and links to outside websites do not represent the views of IBM Internet Security Systems, its management or employees. All content on this Weblog has been made available on an "as-is" basis, and IBM Internet Security Systems shall not be liable for any direct or indirect damages arising out of use of this Weblog.