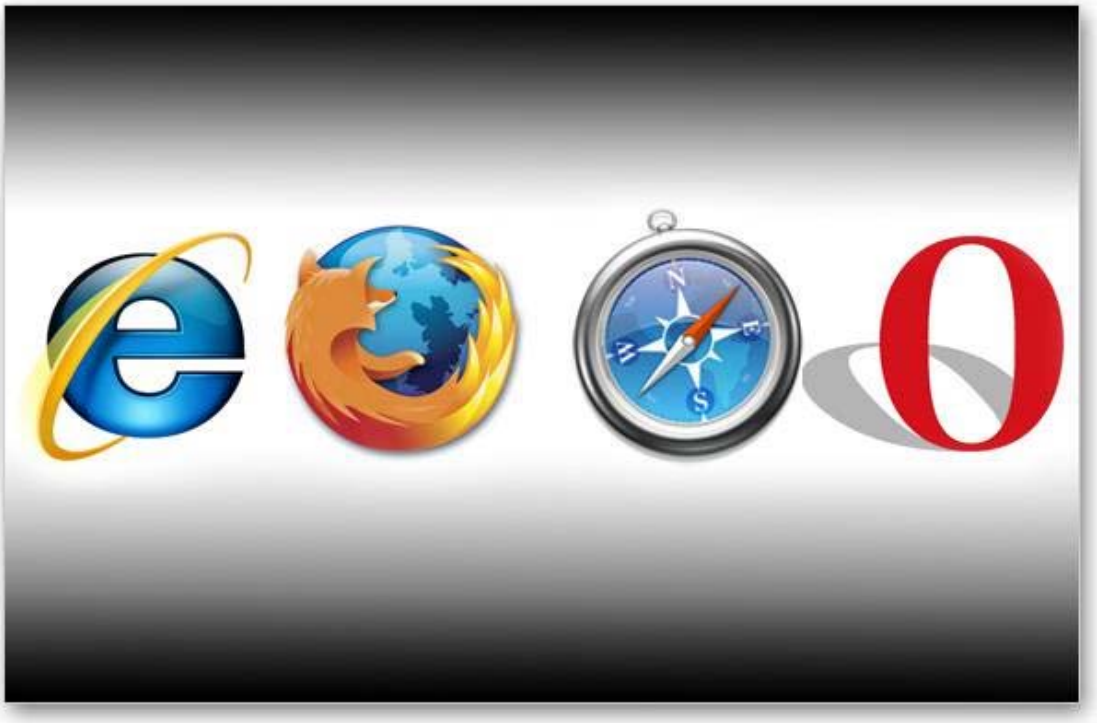
Security

More than 600M users are surfing at risk study says

by Steve Ragan - Jul 1 2008, 14:59



New data shows that 600M Web surfers are out of sync with security. (IMG:J.Andderson)

A study released this morning shows that 600 million users, or roughly forty percent of all web surfers, are surfing at risk. The study, titled in part "Understanding the Web Browser Threat" was conducted by researchers at Google, IBM and Communication Systems Group, ETH Zurich, Switzerland, and used data archived by Google's global search and Web application servers between January 2007 and June 2008 to examine the proliferation and update dynamics of Web browsers around the world.

Despite all the hype, the negative press, and often the FUD about browser layer attacks, forty percent of the planet's Internet users are surfing with old versions of their favorite browser. The insecure users are placing their networks, their selves, and others at risk. How hard is it to download a new release of your favorite browser? Most offer security updates automatically, all you do is allow them. Auto-updates work, as the study shows, browsers that implement an internal auto-update patching did much better in terms of faster update adoption rates than those without.

The threats, ones you hear about all the time, are nothing new. The study says that trend reports indicate remotely exploitable vulnerabilities are on the rise and have been increasing since the year 2000 and reached 89.4% of vulnerabilities reported in 2007. Criminals are creating new methods and expanding on classic methods to install Malware, taking advantage of under patched systems to do this. Whole methods of attack, such as drive-by-downloading, only exist because of exploitable browser installations.

"As popularity of this attack vector has blossomed, there have been frequent reports of hundreds of thousands of Web sites succumbing to mass-defacement - where the defacement often consists of an embedded Iframe. These Iframes typically include content from servers hosting malicious JavaScript code designed to exploit vulnerabilities accessible through the user's Web browser and subsequently to initiate a drive-by malware download. These mass-defacements cause once-benign sites to turn against their visitors. Even pages owned by institutions like the United Nations (un.org), the UK government (.gov.uk) and many others have succumbed to such attacks. In 2007, Google uncovered more than three million malicious Web addresses (URLs) that initiate drive-by downloads," the research points out.

Again, according to the data, as of June 2008, only 59.1% percent of Internet users worldwide are using the latest version of their favorite browser. Often times the reasoning, as is the case with Firefox, is that the new version is buggy and some of the add-ons will not work. For the bulk of self contained add-ons this is true, however most of the larger and widely used add-ons in Firefox were compatible with the 3.0 release.

Often you hear the advice, wait until the bugs are worked out before you upgrade, or wait until the end of life before switching. This is decent advice in some cases but when dealing with security it is dangerous. This may come off as alarmist, but it is true. When you consider that new attacks that target browsers seem to appear all the time, the only way to prevent them is to stay intune with the update cycle. Even Firefox 3.0 was targeted, not

more than a few hours after official release a vulnerability was discovered. The only saving grace was that the discovery was made by a professional researcher and not a malicious criminal.

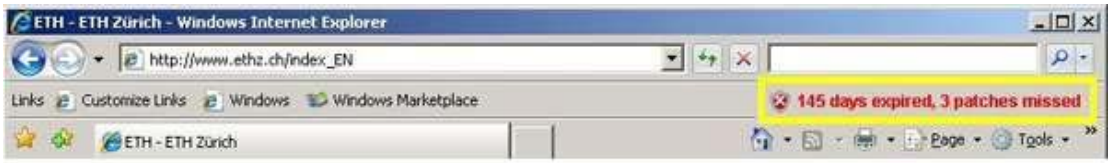
With that said, Firefox users are the most attentive to browser updates; 92.2% of them surfed with Firefox 2.x, before the recently released 3.0, whereas, only 52.5% of Microsoft Internet Explorer users are using the latest, most secure, Internet Explorer 7 to surf the net. The other side to the coin here is that, over the past eighteen months, the study said only 83.3% of Firefox users were using the latest major version (2.x) with all current patches installed. Only 56.1% and 47.6% of Opera and Internet Explorer hosts, respectively, were similarly utilizing fully-patched browsers. Apple users are no better: since the public release of Safari 3, only 65.3% of users operate the latest Safari version.

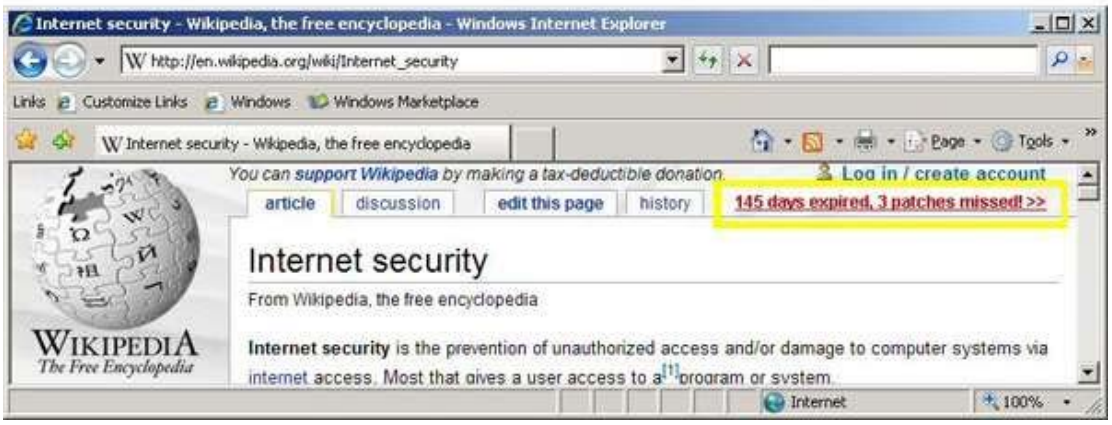
The researchers proposed an interesting solution to the lack of updating and patching for the browsers. The solution uses “best before” date, like you see with food, and corrects a fundamental problem that users are often unaware that they are out of date with the latest security offerings. “A public mindset change is required to counter evolving Internet threats, and a "best before" dating system would make visible the risks of using out-dated and insecure software. Instead of assuming software to be secure, a "best before" dating system would enable the notification of upcoming expiration and risk associated with out of date or unpatched software so that the user is aware of the need to keep installed software ‘fresh’,” the research said.

Adding that, “In order to achieve a viable "best before" dating system, software vendors need to follow stricter practices in the allocation of version number information and make those version numbers more accessible. For example Firefox, Safari, and Opera send detailed version information in the USER-AGENT header field, while Internet Explorer only provides major version information (excluding patch information).”

While some would argue that detailed USER-AGENT information can be harmful, the researchers disagree saying that, “…this is irrelevant given current attack methodologies that simply iterate through ten’s or hundred’s of exploits hoping that one will work. Access to such version information by the attacker would not increase the probability of exploitation, but merely reduce the volume of data sent to the browser by the attacker’s malicious server.”

In the examples below, the researchers listed two ways a user can be alerted to security problems in their browser. One would come from the browser itself, the other from a website.





Another problem and proposed solution is the auto-update functions. Again using Firefox as an example, while the update features work, and they do help in most cases, there is a problem with add-ons. Firefox's auto-update feature alerts users to compatible updates for plug-ins installed through, and registered by, the browser, but the researchers point out that this typically only encompasses a handful of plug-in applications commonly accessible through browser technologies.

"Any examination of the last few years of vulnerability disclosures will reveal a plethora of critical, remotely exploitable, vulnerabilities in practically all plug-in technologies (e.g., Microsoft ActiveX, Adobe Flash, Apple QuickTime, etc.). These browser plug-ins must be similarly patched and updated, just like the Web browser itself," the researchers said.

They propose that plug-in versioning be recorded and compared to a master source to determine if the user has the more recent version, and is properly maintaining their updates. This too would be displayed in the "best before" information.

"However, it is inefficient for the different engineering teams of Web browsers and plug-ins to each develop independent solutions for the same problem. We propose that information of the most recent secure version of browsers and popular plug-ins should be systematically collected by trusted organizations and made accessible using a standardized querying process that also ensures a degree of confidence and authenticity in the version information," the researchers added

The study calls the research and the amounts of data collected only the tip of the iceberg. "While none of the mechanisms proposed within this paper can guarantee to fully protect against exploitation, we are confident that widespread adoption and improvements of these technologies would dramatically reduce the dimensions of the insecurity iceberg and shrink the attack surface."

- Email
- RSS
- Talkback

- Delicious

- Digg
- FARK
- Slashdot
- StumbleUpon

View blog reactions

Talkback

There are currently no comments for this article. Be the first to comment! (no registration required)

Security
Index
News

Features
Reviews

Latest

More than 600M users are surfing at risk study says
Rhapsody launches DRM-free “Music Without Limits”
Sony details PS3 system update v2.40
Lenovo graces consumer desktop market with the IdeaCentre
eBay facing $60 million penalty for selling counterfeit goods

---

In The Tech Herald

Home
Hardware
Software
Security
Internet
Networking
Gadgets
Entertainment
Science
Current Affairs

Site

About Us
Contact Us
The Team
RSS Feeds
Privacy

The Fine Print

Servers supplied by Servint