



 Biting the hand that feeds IT

[The Register](#) » [Security](#) » [Enterprise Security](#) »

Original URL:

http://www.theregister.co.uk/2008/07/03/browser_insecurity_survey/

Built-in browser expiry proposed to fight botnet menace

By [John Leyden](#)

Published Thursday 3rd July 2008 10:53 GMT

Nearly half (45.2 per cent) of all internet surfers neglect to regularly update their browser software. Slackness in applying updates in a timely fashion leaves an estimated 637 million surfers vulnerable to drive-by download attacks, according to a new survey.

Figures in the survey come from a study of user-agent data collected by Google's web search and application servers and analyzed by security researchers from IBM's ISS security division, Google and ETH Zurich University.

The study found that Firefox users were the most diligent in applying security updates, with 83.3 per cent using the latest version. Less than half (47.6 per cent) of IE users used a fully patched version. Part of the problem with IE users could be down to compatibility with older enterprise applications, notes IBM security researcher Gunter Ollmann.

"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," Ollmann [writes](http://blogs.iss.net/archive/TheWebBrowserThreat.html) (<http://blogs.iss.net/archive/TheWebBrowserThreat.html>).

Unsurprisingly the study concluded that update features within different browsers played a key role in determining how quickly users update their software. Firefox users "typically updated" within three days of the availability of a new security update. Opera users averaged around 11 days before patching their browser while some IE users are still stuck on IE6 a year and a half after the release of IE7.

The security researchers reckon browser makers could improve internet security by

taking a leaf from the book of food manufactures and applying a "best before" date to browser and plug-in software. The theory is that a built-in expiry date would ensure that more users update in a timely fashion. Ollmann concedes that opponents may argue that the concept would simply confuse less web-savvy users without having the desired effect.

A white paper on the study, *Understanding the Web browser threat*, can be found [here](http://www.techzoom.net/publications/papers.en) (<http://www.techzoom.net/publications/papers.en>). ®

Related stories

[Web browsers face crisis of security confidence](http://www.theregister.co.uk/2008/06/23/marginal_browser_security_protections/) (23 June 2008)

http://www.theregister.co.uk/2008/06/23/marginal_browser_security_protections/

[Threat remains despite Safari carpet bombing fix](http://www.channelregister.co.uk/2008/06/23/safari_security/) (23 June 2008)

http://www.channelregister.co.uk/2008/06/23/safari_security/

[Bugs casts shadow over Firefox 3](http://www.theregister.co.uk/2008/06/19/firefox3_bugs/) (19 June 2008)

http://www.theregister.co.uk/2008/06/19/firefox3_bugs/

[Opera unleashes Kestrel](http://www.theregister.co.uk/2008/06/12/opera_95_release_preview/) (12 June 2008)

http://www.theregister.co.uk/2008/06/12/opera_95_release_preview/

[Google adds Firefox 3 support to Gears](http://www.theregister.co.uk/2008/06/11/google_gears_firefox_3/) (11 June 2008)

http://www.theregister.co.uk/2008/06/11/google_gears_firefox_3/

[Doomwatchers sound Windows and IE vuln alarm](http://www.theregister.co.uk/2007/09/19/new_vulnerability_reports/) (19 September 2007)

http://www.theregister.co.uk/2007/09/19/new_vulnerability_reports/

© Copyright 2008