Original URL: http://www.theregister.co.uk/2009/01/27/firefox_browser_patching_study/

Easy updates best for browser patching
Google and Swiss researchers prod insecure surfers

By **John Leyden**

Posted in Enterprise Security, 27th January 2009 15:03 GMT

Free Download - Comparing Data Center Batteries, Flywheels and Ultracapacitors

Easy update mechanisms have a far greater effect on browser patching than perceived threats or other factors, according to a new study by Google and Swiss academics.

The in-depth comparative study into how browser security packages are updated discovered that Firefox's update mechanism is the most successful at getting users onto the latest version. Despite this, a steady percentage of insecure surfers - never lower than 20 per cent throughout 2007 - is always using an insecure version of Firefox.

By comparison, 54 cent of Opera users are relying on older versions of the web browser software.

The study - *Firefox (In)Security Update Dynamics Exposed* by Stefan Frei, Thomas Duebendorfer and Martin May of the Swiss Federal Institute of Technology and Google Switzerland - is a follow-up to a paper published last year entitled *Understanding the Web Browser Threat*. The research is described as the first global scale measurement of the patch dynamics of a popular browser.

The latest study looked in more detail at how the update mechanisms of browsers compared and analysed how many users failed to apply the latest browser security patches, based upon analysis of Google USER-AGENT data. The researchers paid particularly close attention to Firefox but also looked at Opera, IE and Safari. Duebendorfer and May discovered that ease of use issues played a far more important role in updates which perceived threats or other factors.

Users in large part do not actually patch their Web browsers based on recommendations, perceived threats, or any security warnings.

We found that the patch level achieved is mainly determined by the ergonomics and default settings of built-in auto-update mechanisms. Firefox' auto-update is very effective: most users installed a new version within three days. However, the maximum share of the latest, most secure version never exceeded 80% for Firefox users and 46% for Opera users at any day in 2007. This makes about 50 million Firefox users with outdated browsers an easy target for attacks.

Looking at anonymous data from Google, the researchers discovered that weekend fluctuations in the usage pattern of IE 6 and IE 7. IE7 consistently grows in popularity over the weekends. The same pattern is seen with later and earlier versions of Firefox.

"What this most likely means is that the newer version of IE is probably in greater use by home users," Gunter Ollmann, a security researcher at IBM's ISS security tools division, explains. "Meanwhile corporates, with greater restrictions on patch/update rollouts have stuck with IE6 for longer periods. Therefore you see IE6 getting greater use during the working week, and IE7 over the weekends."

This might imply that home users are protected against drive-by download attacks (which often rely on exploiting holes in older browser packages to serve up malware), were it not for the fact that other factors are in play.

"Unfortunately the big unknowns are the plug-ins - which I suspect are a bigger problem for home users," Ollmann cautions.

The *Firefox (In)Security Update Dynamics Exposed* paper was published in the January 2009 edition of the ACM SIGCOMM Computer Communication Review. An online copy can be found here (pdf) (http://www.techzoom.net/papers/sigcomm_ccr_firefox_(in) security_update_dynamics_exposed.pdf). ®

Related stories

Microsoft disables automatic IE 8 downloads (7 January 2009)
http://www.theregister.co.uk/2009/01/07/internet_explorer_8_blocker/
Mozilla security chief: Apple should open up (15 September 2008)
http://www.theregister.co.uk/2008/09/15/snyder_calls_on_apple/
Drive-by download attacks menace UK.gov (23 July 2008)
http://www.theregister.co.uk/2008/07/23/drive_by_download_asprox_menace/
Built-in browser expiry proposed to fight botnet menace (3 July 2008)
http://www.theregister.co.uk/2008/07/03/browser_insecurity_survey/
Web browsers face crisis of security confidence (23 June 2008)
http://www.theregister.co.uk/2008/06/23/marginal_browser_security_protections/
Browser makers throw up drive-by download barriers (9 June 2008)
http://www.theregister.co.uk/2008/06/09/drive_by_download_defences/
Firefox and Safari updates tackle alternative browser bugs (17 April 2008)
http://www.theregister.co.uk/2008/04/17/alt_browser_updates/
Hackers attack Mozilla site to spread spam (15 July 2005)
http://www.theregister.co.uk/2005/07/15/firefox_spam_hack/