Published on *Tux Machines* (http://www.tuxmachines.org)

Beware How You Google

By *srlinuxx*
Created *28/04/2005 - 5:18am*
Submitted by srlinuxx on Thursday 28th of April 2005 05:18:00 AM Filed under Web [1]

A simple misspelling of Google's domain name could lead to a Web surfer's worst nightmare.

In a new twist to the old practice of "typosquatting," virus writers have registered a slight variation of Google Inc.'s popular search-engine site to take advantage of any users who botch the spelling of the google.com URL.

The malicious site, googkle.com, is infested with Trojan droppers, downloaders, backdoors and spyware, and an unsuspecting user only has to visit the page to be at risk of computer hijack attacks, according to a warning from Finnish anti-virus vendor F-Secure Corp.

When googkle.com is opened in a browser, two pop-up windows are immediately launched with redirects to third-party sites loaded with scripts. One of the sites, ntsearch.com, downloads and runs a "pop.chm" file, and the other, toolbarpartner.com, downloads and runs a "ddfs.chm" file, F-Secure said.

"Both files are downloaded using exploits and they contain exploits themselves to run embedded executable files. One of the Web pages of the 'toolbarpartner.com' website downloads a file named 'pic10.jpg' using an exploit. This JPG file is actually an executable that replaces [the] Windows Media Player application," the warning reads.

The typosquatters also launch a steady stream of pop-up Web pages with different .exe files.

One batch of exploits loads a malware package that includes two backdoors, two Trojan droppers, a proxy Trojan, a spying Trojan and a Trojan downloader.

It is not yet clear if the attack vector takes advantage of an unpatched version of Microsoft Corp.'s Internet Explorer. Redmond officials could not be reached for comment.

Full Story [2].

Web

Source URL: http://www.tuxmachines.org/node/746

Links:
[1] http://www.tuxmachines.org/taxonomy/term/103
[2] http://www.eweek.com/article2/0,1759,1790348,00.asp