

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

[Home](#) > [content](#) > Linux users targeted by mystery drive-by rootkit

Linux users targeted by mystery drive-by rootkit

By *srlinuxx*

Created 20/11/2012 - 6:11pm

Submitted by srlinuxx on Tuesday 20th of November 2012 06:11:05 PM Filed under [Linux](#) [1] [Security](#) [2]

Security researchers have discovered what appears to be an experimental Linux rootkit designed to infect its highly select victims during a classic drive-by website attack.

Posted anonymously to Full Disclosure on 13 November by an annoyed website owner, the rootkit has since been confirmed by CrowdStrike and Kaspersky Lab as being distributed to would-be victims via an unusual form of iFrame injection attack.

Aimed specifically at users of the latest 64-bit Debian Squeezy kernel (2.6.32-5), the rootkit has been dubbed ?Rootkit.Linux.Snakso.a? by Kaspersky Lab.

[rest here](#) [3]

[Linux Security](#)

Source URL: <http://www.tuxmachines.org/node/58967>

Links:

[1] <http://www.tuxmachines.org/taxonomy/term/63>

[2] <http://www.tuxmachines.org/taxonomy/term/59>

[3] <http://news.techworld.com/security/3412075/linux-users-targeted-by-mystery-drive-by-rootkit/>