

Security Leftovers

By *Roy Schestowitz*

Created 21/09/2019 - 9:17am

Submitted by Roy Schestowitz on Saturday 21st of September 2019 09:17:34 AM Filed under [Security](#) [1]

- [Security updates for Friday](#) [2]

Security updates have been issued by Debian (bird, opendmarc, php7.3, and qemu), Fedora (bird, dino, nbdkit, and openconnect), Oracle (nginx:1.14, patch, and thunderbird), Red Hat (dovecot, kernel, kernel-alt, and kernel-rt), Scientific Linux (thunderbird), and SUSE (kernel, openssl, openssl-1_1, python-SQLAlchemy, and python-Werkzeug).

- [Skidmap malware drops LKMs on Linux machines to enable cryptojacking, backdoor access](#) [3] [Ed: This is not a "Linux" issue any more than Adobe Photoshop malicious files are a "Windows" issue]

Researchers have discovered a sophisticated cryptomining program that uses loadable kernel modules (LKMs) to help infiltrate Linux machines, and hides its malicious activity by displaying fake network traffic stats.

Dubbed Skidmap, the malware can also grant attackers backdoor access to affected systems by setting up a secret master password that offers access to any user account in the system, according to Trend Micro threat analysts Augusto Remillano II and Jakub Urbanec in a company blog post.

- [Linux for ethical hackers 101](#) [4]

In order to familiarize yourself with the full range of ethical hacking tools, it is important to be conversant with the Linux OS. As the systems engineer Yasser Ibrahim said in a post on

Quora: ?In Linux you need to understand from the basics to the advanced, learn the console commands and how to navigate and do everything from your console, also shell programming (not a must, but always preferable), know what a kernel is and how it works, understand the Linux file systems, how to network on Linux.?

[Security](#)

Source URL: <http://www.tuxmachines.org/node/128350>

Links:

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

[2] <https://lwn.net/Articles/800149/rss>

[3] <https://www.scmagazineuk.com/skidmap-malware-drops-lkms-linux-machines-enable-cryptojacking-backdoor-access/article/1604840>

[4] <https://resources.infosecinstitute.com/category/certifications-training/ethical-hacking/linux-for-ethical-hackers-101/>