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

Security: EvilGnome Scaremongering, Intel Defects, New Patches and the "Desktop Security Nightmare"

By *Roy Schestowitz*
Created *19/07/2019 - 4:24pm*
Submitted by Roy Schestowitz on Friday 19th of July 2019 04:24:28 PM Filed under Security [1]

- **EvilGnome Is A Linux Spyware That Records Audio And Steals Your Files [2] [Ed: FOSSBytes has moved on from pushing non-FOSS misinformation to actually doing anti-FOSS FUD. Painting malware one needs to actually install as a real threat.]**

- **CPU vulnerability mitigations keeping Linux devs busy: SUSE's Pavlík[3] [Ed: Intel defects now waste software developers' time. They should just replace/recall those billions of defective chips]**

  > A veteran Linux kernel developer at Germany-based SUSE says the one thing that keeps him and his team busy these days is CPU vulnerability mitigations...

- **Security updates for Friday [4]**

  > Security updates have been issued by Debian (bzip2), Fedora (freetds, kernel, kernel-headers, and knot-resolver), openSUSE (bubblewrap, fence-agents, kernel, libqb, libu2f-host, pam_u2f, and tomcat), Oracle (vim), SUSE (kernel, LibreOffice, libxml2, and tomcat), and Ubuntu (libmspack and squid, squid3).

- **The Desktop Security Nightmare [5]**

  > Many of us have extremely sensitive data on our systems. Emails to family, medical or bank

records, Bitcoin wallets, browsing history, the list goes on. Although we have isolation between our user account and root, we have no isolation between applications that run as our user account. We still, in effect, have to be careful about what attachments we open in email.

Only now it?s worse. You might ?npm install hello-world?, and audit hello-world itself, but get some totally malicious code as well. How many times do we see instructions to gem install this, pip install that, go get the other, and even curl | sh? Nowadays our risky click isn?t an email attachment. It?s hosted on Github with a README.md.

Not only that, but my /usr/bin has over 4000 binaries. Have every one been carefully audited? Certainly not, and this is from a distro with some of the highest quality control around. What about the PPAs that people add? The debs or rpms that are installed from the Internet? Are you sure that the postinst scripts ? which run as root ? aren?t doing anything malicious when you install Oracle Virtualbox?

[...]

One thing a person could do would be to keep the sensitive data on a separate, ideally encrypted, filesystem. (Maybe even a fuse one such as gocryptfs.) Then, at least, it could be unavailable for most of the time the system is on.

Of course, the downside here is that it?s still going to be available to everything when it is mounted, and there?s the hassle of mounting, remembering to unmount, password typing, etc. Not exactly transparent.

I wondered if mount namespaces might be an answer here. A filesystem could be mounted but left pretty much unavailable to processes unless a proper mount namespace is joined. Indeed that might be a solution. It is somewhat complicated, though, since nsenter requires root to work. Enter sudo, and dropping privileges back to a particular user ? a not particularly ideal situation, and complex as well.

Still, it might well have some promise for some of these things.

Security

Source URL: http://www.tuxmachines.org/node/126071

Links:
[1] http://www.tuxmachines.org/taxonomy/term/59
[2] https://fossbytes.com/evilgnome-linux-spyware-records-audio-steals-your-files/
[3] https://www.itwire.com/open-source/cpu-vulnerability-mitigations-keeping-linux-devs-busy-suse-s-pavlík.html
[4] https://lwn.net/Articles/794190/rss
[5] https://changelog.complete.org/archives/10006-the-desktop-security-nightmare