Security: Updates, Devices With Default Credentials and Open Ports, Regulatory Compliance and Red Hat Security and More

By *Roy Schestowitz*
Created *27/06/2019 - 5:19am*
Submitted by Roy Schestowitz on Thursday 27th of June 2019 05:19:34 AM Filed under Security [1]

- **Security updates for Wednesday [2]**

- **This Malware Created By A 14-Yr-Old Is Bricking Thousands Of Devices [3] [Ed: "It's targeting any Unix-like system with default login credentials," the original source says.]**

  > A new malware called Silex is on its way to brick thousands of IoT devices. The malware has been developed by a 14-year old teenager known by the pseudonym Light Leafon. The malware strain is inspired by the infamous malware called BrickerBot, which is notorious for bricking millions of IoT devices way back in 2017.

- **New Silex malware is bricking IoT devices, has scary plans [4]**

- **Regulatory Compliance and Red Hat Security [5]**

  > In today?s interconnected world, data security has never been more important. Virtually every industry, from healthcare to banking and everything in between, has rules for how businesses handle data. Failure to meet regulatory compliance spells serious trouble for your business.

Depending on the severity of the infraction, you could end up with fines, loss of reputation/revenue, or jail time.

Fortunately, these consequences are avoidable with a few proactive steps. By training your IT staff to keep your systems secure, you can prevent harmful or costly data breaches.

- **Using Quay.io to find vulnerabilities in your container images [6]**

  You?ve created a container image that has all the packages that you and your team need to do something useful, or maybe you?ve built a public image that anybody can use. But, what if that image contains packages with known security vulnerabilities? Regardless of the severity of those vulnerabilities, you?ll want to learn more and take steps to mitigate them as soon as possible.

  Fortunately, your team uses Quay.io* as your registry. When you push an image to Quay.io, it automatically runs a security scan against that image.

Security

Source URL: http://www.tuxmachines.org/node/125277

Links:
[1] http://www.tuxmachines.org/taxonomy/term/59
[2] https://lwn.net/Articles/792111/rss
[3] https://fossbytes.com/malware-creator-bricking-thousands-iot-devices/
[4] https://www.zdnet.com/article/new-silex-malware-is-bricking-iot-devices-has-scary-plans/
[5] https://wpengine.linuxacademy.com/security/regulatory-compliance-and-red-hat-security/
[6] https://developers.redhat.com/blog/2019/06/26/using-quay-io-to-find-vulnerabilities-in-your-container-images/