Security Leftovers/FUD

By *Roy Schestowitz*
Created *27/06/2019 - 8:51am*
Submitted by Roy Schestowitz on Thursday 27th of June 2019 08:51:41 AM Filed under Security [1]

- **New Linux Worm Attacks IoT Devices [2] [Ed: How to blame "Linux" for default passwords in devices (and some now also blame "Iran", citing a CIA 'proxy' Recorded Future in relation to this because they want war)]**

  > Silex has 'bricked' more than 2000 Linux-based IoT devices so far.

- **Your server remote login isn't root:password, right? Cool. You can keep your data. Oh sh... your IoT gear, though? [3] [Ed: All this "Silex" 'news' tries to blame Iran for cracking by guessing default passwords; but this is attempted every day by dozens of nations, every minute in a lot of cases. Any political motivation behind this Iran angle?]**

  > Earlier this week, infosec outfit Recorded Future claimed a Tehran-backed group known as Elfin, or APT33, has been increasingly active in recent months, largely targeting industrial facilities and companies within Saudi Arabia that do business with the US and other Western countries.

- **'Silex' Malware Renders Internet-of-Things Devices Useless. Here's How to Prevent It [4] [Ed: War lovers' media, e.g. Fortune (see parent) and CBS (through ZDNet) push this whole "Iran" angle, manufactured in part by Recorded Future, which works with the CIA [5]. This is the source of all these "Iran is cracking your gear" stories (every large nation does it all the time, so why the focus on Iran all of a sudden?)]**

- **Silex malware targeting IoT devices spotted by security researchers [6]**

-

Daily News Roundup: Hackers Broke into Ten Telecom Networks [7] [Ed: Definitely sounds like they used Windows, which executes malware without obstructing the users (who might just open an E-mail or click on a link)]

> Security researchers have revealed hackers spent years burrowing into ten different telecoms. Using a common method of an email with a link leading to malware, the hackers then used sophisticated techniques to target specific individuals.
>
> Security researchers at Cybereason revealed details of years-long attempts to break into telecom services (cell phone carriers). Starting in 2017, and possibly before, hackers sent emails to unsuspecting telecom employees with malicious links. The initial payload gave the hackers access to the telecom networks.
>
> Once in, the hackers ultimately compromised the network, gaining administrative privileges, and even creating a VPN on the system that let hackers access large amounts of data and empowered them even to shut down the telecom network entirely. The hackers had so much power that Amit Serper, Principal Security Researcher at Cybereason, described them as essentially a ?de facto shadow IT department of the company.?

Security

Links:
[1] http://www.tuxmachines.org/taxonomy/term/59
[2] https://www.darkreading.com/iot/new-linux-worm-attacks-iot-devices/d/d-id/1335065
[3] https://www.theregister.co.uk/2019/06/27/new_iran_apt_uncovered/
[4] http://fortune.com/2019/06/26/silex-malware-hack-iot-internet-of-things-smart-device-fix-how-to-prevent/
[5] https://www.bizjournals.com/boston/news/2019/05/30/somerville-cybersecurity-firm-recorded-future-to.html
[6] https://www.computing.co.uk/ctg/news/3077942/silex-malware-iot-devices
[7] https://www.howtogeek.com/fyi/daily-news-roundup-hackers-broke-into-ten-telecom-networks/