Security: ?Medjacking?, Exploding e-Cigarettes, and Linux FUD

By *Roy Schestowitz*
Created *28/02/2018 - 5:17pm*
Submitted by Roy Schestowitz on Wednesday 28th of February 2018 05:17:12 PM Filed under Security [1]

- **?Medjacked?: Could Hackers Take Control of Pacemakers and Defibrillators?or Their Data?** [2]

  > Are high-tech medical devices vulnerable to hacks? Hackers have targeted them for years, according to a new article in the Journal of the American College of Cardiology. But Dr. Dhanunjaya Lakkireddy, senior author of the paper, says hackers have harmed no one so far.

- **Exploding e-Cigarettes Are a Growing Danger to Public Health** [3]

  > Whatever their physiological effects, the most immediate threat of these nicotine-delivery devices comes from a battery problem called thermal runaway
  >
  > [...]
  >
  > Exploding cigarettes sound like a party joke, but today?s version isn?t funny at all. In fact, they are a growing danger to public health. Aside from mobile phones, no other electrical device is so commonly carried close to the body. And, like cellphones, e-cigarettes pack substantial battery power. So far, most of the safety concerns regarding this device have centered on the physiological effects of nicotine and of the other heated, aerosolized constituents of the vapor that carries nicotine into the lungs. That focus now needs to be widened to include the threat of thermal runaway in the batteries, especially the lithium-ion variety.

- **Uh, oh! Linux confuses Bleeping Computer again** [4]

The tech website Bleeping Computer, which carries news about security and malware, has once again demonstrated that when it comes to Linux, its understanding of security is somewhat lacking.

What makes the current case surprising is the fact that the so-called security issue which the website chose to write about had already been ripped to pieces by senior tech writer Stephen Vaughan-Nicholls four days earlier.

Called Chaos, the vulnerability was touted by a firm known as GoSecure as one that would allow a backdoor into Linux servers through SSH.

- **Are Mac and Linux users safe from ransomware? [5]**

  Ransomware is currently not much of a problem for Linux systems. A pest discovered by security researchers is a Linux variant of the Windows malware ?KillDisk?. However, this malware has been noted as being very specific; attacking high profile financial institutions and also critical infrastructure in Ukraine. Another problem here is that the decryption key that is generated by the program to unlock the data is not stored anywhere, which means that any encrypted data cannot be unlocked, whether the ransom is paid or not. Data can still sometimes be recovered by experts like Ontrack, however timescales, difficulty and success rates depend on the exact situation and strain of ransomware.

Security

Links:
[1] http://www.tuxmachines.org/taxonomy/term/59
[2] https://www.theknowledgegroup.org/blogs/medjacked-hackers-take-control-pacemakers-defibrillators-data
[3] https://spectrum.ieee.org/consumer-electronics/portable-devices/exploding-ecigarettes-are-a-growing-danger-to-public-health
[4] https://www.itwire.com/open-sauce/81915-uh,-oh-linux-confuses-bleeping-computer-again.html
[5] https://www.krollontrack.co.uk/blog/the-world-of-data/are-mac-and-linux-users-safe-from-ransomware/