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

Home > content > Security: Updates, Mirai and Singapore's Massive Breach

Security: Updates, Mirai and Singapore's Massive Breach

By *Roy Schestowitz*
Created *21/09/2018 - 8:58pm*
Submitted by Roy Schestowitz on Friday 21st of September 2018 08:58:08 PM Filed under Security [1]

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

- **Mirai botnet hackers [sic] avoid jail time by helping FBI [3]**

  > The three men, Josiah White, 21, Dalton Norman, 22, and Paras Jha, 22, all from the US, managed to avoid the clink by providing "substantial assistance in other complex cybercrime investigations", according to the US Department of Justice. Who'd have thought young hacker [sic] types would roll over and show their bellies when faced with prison time....

- **A healthcare IT foundation built on gooey clay [4]**

  > Today, there was a report from the Solicitor General of Singapore about the data breach of the SingHealth systems that happened in July.
  >
  > These systems have been in place for many years. They are almost exclusively running Microsoft Windows along with a mix of other proprietary software including Citrix and Allscript. The article referred to above failed to highlight that the compromised ?end-user workstation? was a Windows machine. That is the very crucial information that always gets left out in all of these reports of breaches.
  >
  > I have had the privilege of being part of an IT advisory committee for a local hospital since about 2004 (that committee has disbanded a couple of years ago, btw).

> [...]
>
> Part of the reason is because decision makers (then and now) only have experience in dealing with proprietary vendor solutions. Some of it might be the only ones available and the open source world has not created equivalent or better offerings. But where there are possibly good enough or even superior open source offerings, they would never be considered ? ?Rather go with the devil I know, than the devil I don?t know. After all, this is only a job. When I leave, it is someone else?s problem.? (Yeah, I am paraphrasing many conversations and not only from the healthcare sector).
>
> I recall a project that I was involved with ? before being a Red Hatter ? to create a solution to create a ?computer on wheels? solution to help with blood collection. As part of that solution, there was a need to check the particulars of the patient who the nurse was taking samples from. That patient info was stored on some admission system that did not provide a means for remote, API-based query. The vendor of that system wanted tens of thousands of dollars to just allow the query to happen. Daylight robbery. I worked around it ? did screen scrapping to extract the relevant information.
>
> Healthcare IT providers look at healthcare systems as a cashcow and want to milk it to the fullest extent possible (the end consumer bears the cost in the end).
>
> Add that to the dearth of technical IT skills supporting the healthcare providers, you quickly fall into that vendor lock-in scenario where the healthcare systems are at the total mercy of the proprietary vendors.

Security

Source URL: http://www.tuxmachines.org/node/115789

Links:
[1] http://www.tuxmachines.org/taxonomy/term/59
[2] https://lwn.net/Articles/766112/rss
[3] https://www.theinquirer.net/inquirer/news/3063137/mirai-botnet-hackers-avoid-prison-by-helping-fbi
[4] https://harishpillay.wordpress.com/2018/09/21/a-healthcare-it-foundation-built-on-gooey-clay/