DSA-2019: Debian Security Advisory: Lovestruck Leaders

By Roy Schestowitz
Created 14/02/2022 - 11:44pm
Clients and friends have been asking a very similar question recently: what do the scandals in Debian and other free software organizations mean for me, my computers, my servers, my business?

[...]

Many people perceive social engineering as an attempt to gain access to confidential information, for example, successfully impersonating the queen to obtain medical records.

Yet social engineering attacks go much further. Sophisticated attackers encourage their targets to break rules in the hope that the shared knowledge of these crimes will give the attacker an opportunity to blackmail the target. Edward Snowden revealed an unsophisticated plot to entrap a Saudi banker in Geneva by orchestrating a drink driving violation.

Many of the attackers have a long-term view. They start by testing small rule violations and gradually lead their target deeper and deeper into the hot water.

[...]

Once again, we need to come back to the question that started this blog: what does it mean for the user? These social engineering attacks under the guise of diversity may not compromise any of the archive keys or add new backdoors into the code. On the other hand, when ordinary volunteers see these rorts they may lose motivation. Fixes for security bugs, like everything else in Debian, depend on the motivation of volunteers to fix them promptly. A volunteer who was treated rudely at DebConf may simply leave a bug open for an extra week. High-impact projects that never finish: see the example of FreedomBox, which still hasn’t made an official release after more than 12 years. Social engineering
can play a role in all of these phenomena.

[3]

Source URL: http://www.tuxmachines.org/node/161460

Links: