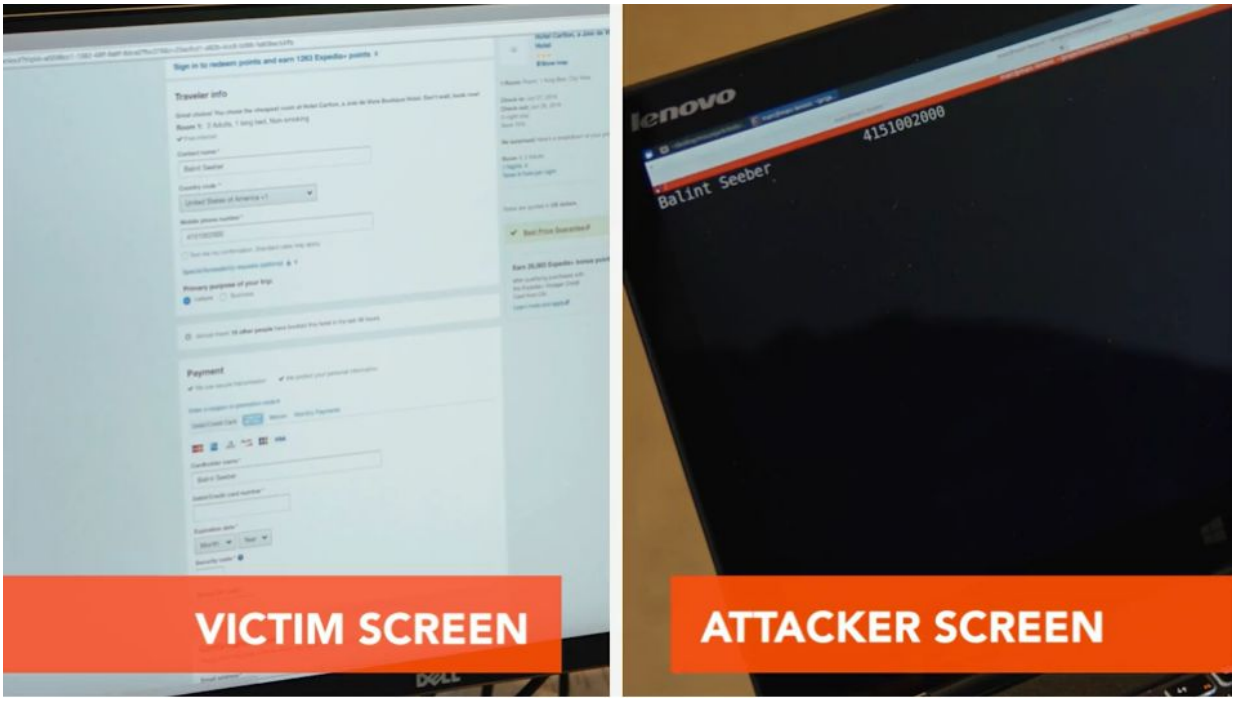
Some wireless keyboards may let snoopers have your numbers

July 28 2016, by Nancy Owano



(Tech Xplore)—Security research alert: There is something around called KeySniffer. Hang around with the wrong kind of keyboard, and you may find it has sniffed up personal identification and access numbers you really do not want to even think about being stolen.

Marc Newlin, the Bastille Research Team member responsible for the

KeySniffer discovery explained how KeySniffer works in a video. He is a security researcher for the company, Bastille Networks.

He talked about one vulnerability where attackers sniff all keystrokes being sent from your wireless keyboard to your computer—thus the name. He and a colleague did a demo, with a laptop, USB dongle from third-party vendor and antenna.

His colleague is Balint Seeber, director of vulnerability research, Bastille Networks. For the sake of the demo, he is using a vulnerable wireless keyboard.

The room is scanned with a USB dongle plugged into Newlin's computer and identifying the keyboard in use. That allows someone to sniff all the keystrokes that Seeber is typing, said Newlin. "We can see his credit card number, his email address, his card validation code, his billing address."

Advice? Switch to a wired keyboard or Bluetooth keyboard, which has a higher level of security.

What is really going on here, how would the mischief makers do it? The company described the vulnerability as affecting non-Bluetooth wireless keyboards from a number of vendors, not all wireless keyboard vendors. "The wireless keyboards susceptible to KeySniffer use unencrypted radio communication protocols."

What gets seen? Let's suppose the victim is ordering something online.

It would be possible for an attacker to eavesdrop on all the keystrokes typed by the victim from several hundred feet away using less than $100 of equipment, said the company.

Chris Brook of *Threatpost* reported on how the discovery was made. "After purchasing wireless keyboards from a big box store, Newlin's plan was to reverse engineer the devices, figure out their protocols and start looking for problems with their encryption. It turned out that eight of the 12 they tested – two thirds – didn't have encryption to begin with."

The company, listing the products that they tested, also noted that this should not be considered an exhaustive list of all vulnerable keyboards. "There may be other brands/models that are vulnerable to this, or other attacks."

Dave Lee, North America technology reporter, BBC, similarly reported on how this came about. "We went into a bunch of big box stores and purchased wireless keyboards," said Ivan O'Sullivan, Bastille's chief research officer, according to the BBC report. "We were shocked to find that two-thirds transmitted all of their data in clear text, no encryption. "We did not expect to see this. We didn't think it would be in clear text."

The BBC further reported that the company has praised Logitech, Dell and Lenovo for using higher-end chips in their wireless keyboards with stronger security.

An official release from the company stated that "Bluetooth keyboards and higher-end wireless keyboards from manufacturers including Logitech, Dell, and Lenovo are not susceptible to KeySniffer."

More information: www.keysniffer.net/ , www.keysniffer.net/affected-devices/

Citation: Some wireless keyboards may let snoopers have your numbers (2016, July 28) retrieved