Hackers can record everything you type on certain wireless keyboards

Some low-end wireless keyboards send keystrokes to your computer completely unencrypted, say researchers

CBC News Posted: Jul 27, 2016 7:53 PM ET

Researchers have developed a tool that can intercept and record keystrokes made by some wireless keyboards, allowing hackers to read everything an unsuspecting user types, from up to 75 metres away. (Kacper Pempel/Reuters)

A computer security research team has identified a weakness in several brands of low-cost wireless keyboards that could allow hackers to view and record every word, number and password typed by a user from up to about 75 metres away.

According to Bastille, an Atlanta-based research team, eight wireless keyboards made by companies such as Hewlett-Packard, Radio Shack and Toshiba send keystroke data from the board to the USB dongle that connects to your computer without the encryption needed to mask what someone is typing.

Wireless keyboards that connect to your computer with small USB dongles transmit keystrokes over a radio frequency, which Bastille was able to intercept using a radio transponder used for controlling drones that costs about $50 on Amazon, and an antenna that boosts the range to about 75 metres.

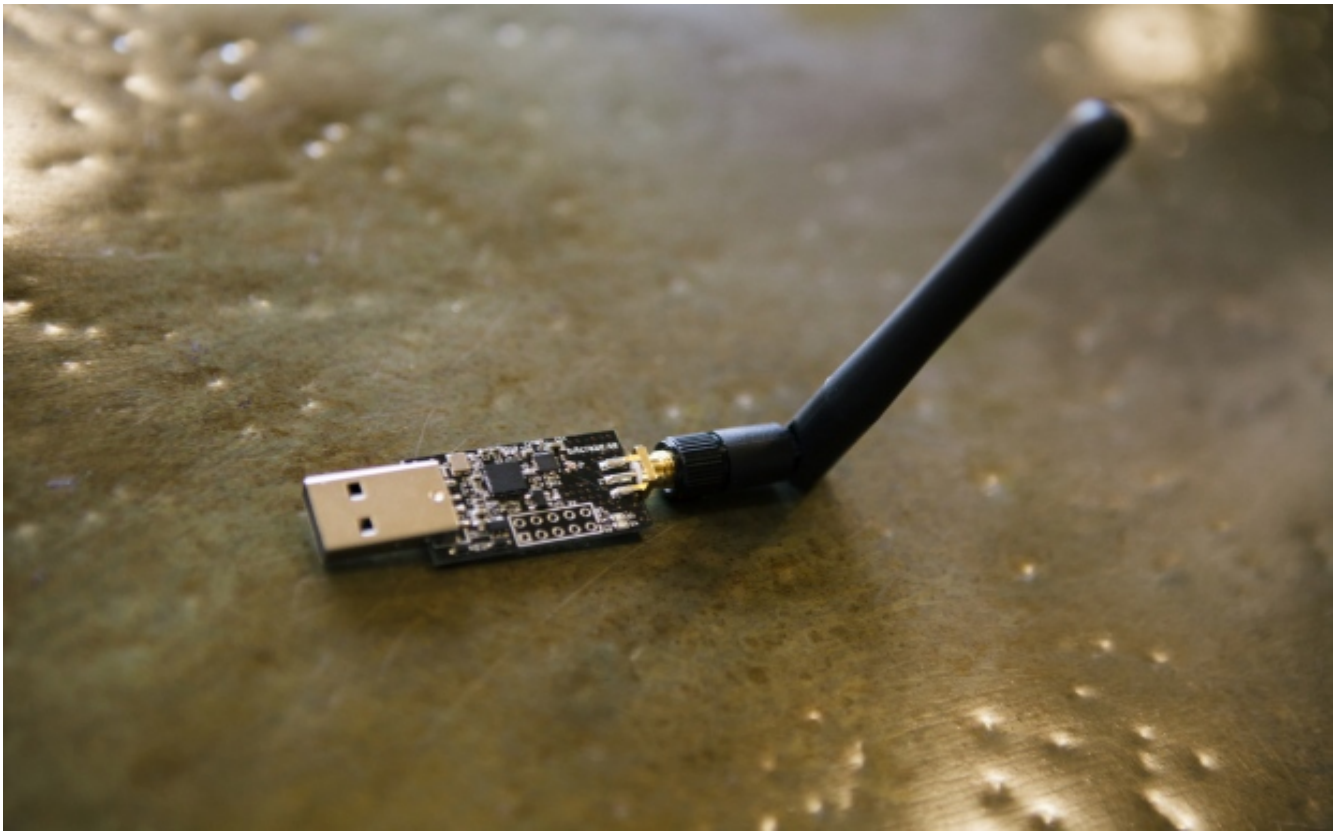
https://www.youtube.com/watch?v=6WSAh74Uxh8

In a demonstration video, Bastille security researcher Marc Newlin eavesdropped on his co-worker's keyboard using a program they developed **called Keysniffer**.

The video shows Newlin's computer screen recording the co-worker making a hotel reservation online. As the co-worker enters information including his name, credit card number and billing address, they also show up on Newlin's screen.

"We did not expect to see this. We didn't think it would be in clear text. Hackers can intercept all the keystrokes from your keyboard up to 250 feet away. Through glass, walls, floors," Bastille's chief research officer Ivan O'Sullivan **told BBC News**.

Bastille notes that Bluetooth keyboards and higher-end USB keyboards from manufacturers like Logitech, Dell and Lenovo were not susceptible to the Keysniffer method of recording keystrokes.



Bastille used a USB radio receiver and antenna to intercept and record keystrokes from unsecured wireless keyboards. The receiver sells for about $50. (Bastille)

The vulnerability that allows Keysniffer to work can't be fixed with a software or firmware update, so Bastille recommends that if you have an affected keyboard, you should replace it with a secure wireless board or a wired one instead.

Bastille received responses from Kensington and General Electric, and posted them on their website. Both said they are working to address the concerns, but didn't post specifics about return or refund policies, instead asking affected customers to contact them directly.

This isn't the first time security vulnerabilities have been identified in wireless keyboards. In 2010, cybersecurity researchers discovered that the encryption used in certain Microsoft boards was easily broken.

O'Sullivan **told The Atlantic** that Bastille isn't planning to release the Keysniffer code, but added it's plausible that someone else could have come up with it independently.