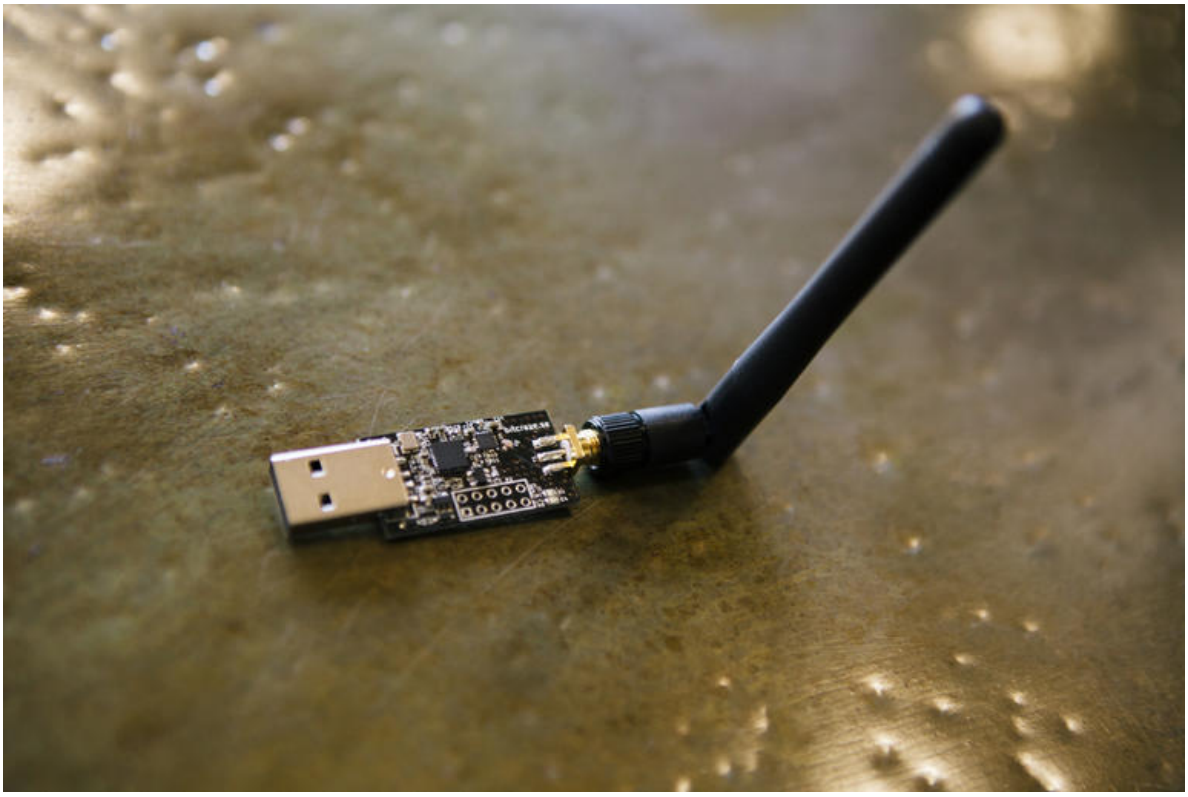
Flaws in wireless keyboards let hackers snoop on everything you type

Many popular, low-cost wireless keyboards don't encrypt keystrokes.

By Zack Whittaker for Zero Day | July 26, 2016 -- 13:30 GMT (06:30 PDT) | Topic: Security



This nondescript USB dongle can be used to spy on wireless keyboards from hundreds of feet away. (Image: Bastille)

Your wireless keyboard is giving up your secrets -- literally. With an antenna and wireless dongle worth a few bucks, and a few lines of Python code, a hacker can passively and covertly record everything you type on your wireless keyboard from hundreds of feet away. Usernames, passwords, credit card data, your manuscript or company's balance sheet -- whatever you're working on at the time.
It's an attack that can't be easily prevented, and one that almost nobody thought of -- except the security researchers who found it.

Security firm Bastille calls it "KeySniffer," a set of vulnerabilities in common, low-cost wireless keyboards that can allow a hacker to eavesdrop from a distance. Here's how it works: a number of wireless keyboards use proprietary and largely unsecured and untested radio protocols to connect to a computer -- unlike Bluetooth, a known wireless standard that's been tried and tested over the years. These keyboards are always transmitting, making it easy to find and listen in from afar with the right equipment. But because these keystrokes aren't encrypted, a hacker can read anything on a person's display, and directly type on a victim's computer.
The attack is so easy to carry out that almost anyone can do it -- from petty thieves to state-actors.
Marc Newlin, a researcher at the company who was credited with finding the flaw said it was "pretty alarming" to discover.

"A hacker can 'sniff' all of the keystrokes, as well as inject their own keystrokes on the computer," he explained on the phone this week.

The researchers found that eight out of 12 keyboards from well-known vendors -- including HP, Kensington, and Toshiba -- are at risk of eavesdropping, but the list is far from exhaustive.

The scope of the problem is so large that the researchers fully expect that "millions" of devices are vulnerable to this new attack.

Worst of all? There's no fix.

"I think a lot of consumers reasonably expect that the wireless keyboard they're using won't put them at risk, but consumers might not have a high awareness of this risk," he said.

Ivan O'Sullivan, the company's chief research officer, admitted that the ease of this attack had him unsettled.

"As a consumer, I expect that the keyboard that I buy won't transmit my keystrokes in plain-text."

"We were shocked. And consumers should be, too," he said.

This isn't the first time wireless devices have put their users at risk. Bastille was the company behind the now-infamous MouseJack flaw, which let hackers compromise a person's computer through their wireless mouse. Even as far back as 2010, it was known that some keyboards with weak encryption could be easily hacked.

Over half a decade later, Newlin said he was hopeful that his research will make more people aware, but he doesn't think this problem "will be resolved."

"Most of the vendors have not responded to our disclosure information," he said. "Many of the vendors haven't responded past an acknowledgement, or they haven't responded at all to our inquiries."

Though not all wireless keyboards are created equal and many are not vulnerable to the eavesdropping vulnerability, there is an easy fix to a simple problem. "Get a wired keyboard," the researchers said.