Bastille

Bastille Discovers "KeySniffer" Vulnerability in Wireless Keyboards Which Reveals Private Data to Hackers in Clear Text

Company Finds Millions of Low-Cost Wireless Keyboards Are Susceptible to KeySniffer Attack

ATLANTA, GA – July 26, 2016 – Bastille, the first cybersecurity company to detect and mitigate threats from the Internet of Things (IoT), today unveiled a massive vulnerability affecting the vast majority of low-cost wireless keyboards. Using a new attack that the Bastille Research Team has named "KeySniffer," hackers can remotely "sniff" ALL the keystrokes of wireless keyboards from eight manufacturers from distances up to 250 feet away. When conducting a KeySniffer attack, hackers can eavesdrop and capture every keystroke a victim types in 100 percent clear text and then search for:

- Card numbers, expiration date, CVV code
- Bank account usernames and passwords
- Answers to security questions: name of your first pet, mother's maiden name, etc.
- Network access passwords
- Any secrets: business or personal typed into a document or email

"When we purchase a wireless keyboard we reasonably expect that the manufacturer has designed and built security into the core of the product," said Bastille Research Team member Marc Newlin, responsible for the KeySniffer discovery. "Unfortunately, we tested keyboards from 12 manufacturers and were disappointed to find that eight manufacturers (two-thirds) were susceptible to the KeySniffer hack."

The keyboard manufacturers affected by KeySniffer include: Hewlett-Packard, Toshiba, Kensington, Insignia, Radio Shack, Anker, General Electric, and EagleTec. Vulnerable keyboards are easy for hackers to detect as they are always transmitting, whether or not the user is typing. Consequently, a hacker can scan a room, building, or public area for vulnerable devices at any time.

A History of Wireless Keyboard Attacks:

In 2010, the KeyKeriki team exposed weak XOR encryption in certain Microsoft wireless keyboards. In 2015, Samy Kamkar's KeySweeper exploited Microsoft's vulnerability. Both of those vulnerabilities utilized a weakness in Microsoft's encryption.

The KeySniffer discovery is different in that it reveals that manufacturers are actually producing and selling wireless keyboards with no encryption at all. Bluetooth keyboards and higher-end wireless keyboards from manufacturers including Logitech, Dell, and Lenovo are not susceptible to KeySniffer.

As part of its disclosure policy, Bastille notified affected vendors to provide them the opportunity to address the KeySniffer vulnerability. Most, if not all, existing keyboards impacted by KeySniffer cannot be upgraded and will need to be replaced. To be safe, Bastille advises the use of a wired or Bluetooth keyboard. For a complete list of affected devices, go to www.KeySniffer.net.

Bastille's discovery of KeySniffer comes just months after the company unveiled MouseJack, a vulnerability affecting millions of wireless mice. This latest find coincides with the company's ongoing mission to completely secure the Enterprise by identifying airborne threats and allowing for a preemptive response.

For more information on Bastille, visit www.bastille.net and follow them on Twitter @bastillenet and LinkedIn.

About Bastille
Launched in 2014, Bastille is pioneering Internet of Things (IoT) security with next-generation security sensors and airborne emission detection, allowing corporations to accurately quantify risk and mitigate 21st century airborne threats. Through its patented proprietary technology, Bastille helps enterprise organizations protect cyber and human assets while providing unprecedented visibility of wireless IoT devices that could pose a threat to network infrastructure. For more information, visit www.bastille.net and follow them on Twitter @bastillenet and LinkedIn.

Media Contact:
Noe Sacoco
LMGPR
408.340.8130
noe@lmgpr.com