Bastille

Bastille Unveils List of Top 10 Internet of Radios Vulnerabilities

List Coincides with New Poll that Finds a Significant Gap Between Internet of Things Security Awareness and Preparedness in the Enterprise

SAN FRANCISCO, Calif.– October 18, 2016 – Bastille, the leader in enterprise threat detection through software-defined radio, today released its list of "Top 10 Internet of Radios Vulnerabilities." The Internet of Radios is the combination of mobile, wireless, bring your own device (BYOD), and Internet of Things (IoT) devices operating within the radio frequency (RF) spectrum. The Top 10 list coincides with National Cyber Security Awareness Month as well as the results of the recent "Bastille Internet of Radios Security Poll" that indicates widespread recognition of potential threats in the enterprise, but limited adoption and enforcement of security policies.

Comprised by Bastille's lauded engineering and research team responsible for the MouseJack and KeySniffer discoveries, the "Top 10 Internet of Radios Vulnerabilities" are:

1. Rogue Cell Towers ('Stingrays', 'IMSI Catchers')
2. Rogue Wi-Fi HotSpots
3. Bluetooth Data Exfiltration (tethering)
4. Eavesdropping/Surveillance Devices (e.g. conference room bugs)
5. Vulnerable Wireless Peripherals (mice/keyboard)
6. Unapproved Cellular Device Presence
7. Unapproved Wireless Cameras
8. Vulnerable Wireless Building Controls
9. Unapproved IoT Emitters
10. Vulnerable Building Alarm Systems

In addition to the Top 10 list, Bastille has released results of the "Bastille Internet of Radios Security Poll." Nearly 300 global professionals took part in the poll, offering a snapshot into enterprise awareness and preparedness of Internet of Radios threats in the workplace. The poll was conducted July 26–August 3, 2016 and was comprised of visitors to the Bastille, KeySniffer and MouseJack websites. The majority of respondents (69%) reported they were employed in the IT and cybersecurity industries.

Key takeaways from the poll include:

- 78% of respondents believe the threat from the Internet of Radios will increase in the next 12 months.
- 50% of respondents believe IoT devices are already impacting security.

- 51% of respondents say their companies have adopted a BYOD policy, but only 24% say the policy is strictly enforced.
- 42% of respondents say their organization has not implemented a BYOD policy at all.
- 47% of respondents say their organization is not currently using a Mobile Device Management (MDM) system, compared to 41% that already have one in place.

"While it's encouraging to see that so many people are aware of IoT-related threats, it's discouraging to see that enterprises are not actively heeding the warning," said Chris Risley, CEO, Bastille. "Awareness is only half the battle; without proper security protocols in place, enterprises leave themselves and their customers vulnerable to an IoT-related attack. As this is Cyber Security Awareness Month, we urge all enterprises to adopt a clear IoT security policy as these emerging IoT threats are simply too numerous and dangerous to continue to ignore."

Bastille is the first cybersecurity company to detect and mitigate the rapidly emerging threats to the enterprise that are the unintended consequence of the Internet of Radios. The company's flagship solution, Bastille Enterprise, utilizes patented software-defined radio sensors backed by machine-learning technology to sense, identify and localize radio-based threats.

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

About Bastille
Launched in 2014, Bastille is the leader in enterprise threat detection through software-defined radio. Bastille provides full visibility into the known and unknown mobile, wireless and Internet of Things devices inside an enterprise's corporate airspace–together known as the Internet of Radios. Through its patented software-defined radio and machine learning technology, Bastille senses, identifies and localizes threats, providing security teams the ability to accurately quantify risk and mitigate airborne threats that could pose a danger 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