Bastille

Bastille Unveils Unprecedented Solution to Protect Enterprises From Internet of Radios-Based Security Threats

Company's Patented Software-Defined Radio and Machine-Learning Technology Senses, Identifies and Localizes Threats in the Corporate Airspace

San Francisco, CA – October 18, 2016 – Bastille, the leader in enterprise threat detection through software-defined radio, today announced the General Availability of its new service to protect enterprises from information and physical security threats. Bastille's solution utilizes patented software-defined radio sensors backed by machine-learning technology to provide enterprises with full visibility into mobile, wireless and Internet of Things (IoT) - The Internet of Radios - devices inside their corporate airspaces. The ability to sense, identify and localize potential threats enables security teams to take swift action and preemptively remove those threats before harm is done.

"Your corporate airspace can either be a hugely vulnerable attack surface or it can be a new contributor to your security situational awareness. With the mobile world and unwired communications creating thousands of new threat vectors, enterprises have never been more vulnerable to a radio-based attack simply because you can't protect what you can't see," said Chris Risley, CEO, Bastille. "At the same time, almost every person in or near your facility now carries a radio transmitter in the form of a mobile phone. The Bastille solution scans the entire corporate airspace to sense, identify and localize emerging threats and behavioral anomalies resulting in full visibility of any airborne risks in your environment."

Bastille pairs sophisticated software-defined radio sensors with machine learning cloud analytics. It continuously scans the full spectrum from 60MHz to 6GHz, including all Wi-Fi, Bluetooth, cellular and IoT protocols, the Internet of Radios, to provide real-time situational awareness for all wireless infrastructure in the enterprise. With two patents issued and 12 patents pending, the Bastille solution is built upon three areas of technology that result in the ability to Sense, Identify and Localize threats:

SENSE: Collaborative Bandit Sensing quickly and accurately scans the spectrum for emitters and threats. Utilizing the multi-armed bandit Prediction Algorithm and machine-learning techniques, Bastille's sensors intelligently make distributed decisions about whether to observe a known signal versus scanning another part of the spectrum to find unknown signals.

IDENTIFY: Bayesian Device Fingerprinting is used to detect and identify devices in an enterprise's airspace. It leverages Probabilistic Graph Models to resolve emitter, device and people-device entities to produce never-before-seen situational awareness of an enterprise's airborne (RF) and physical space.

LOCALIZE: Distributed Tomographic Localization provides actionable position information of all emitters in the corporate airspace. This technology passively localizes any emitter within an industry-leading 1metre of accuracy, enabling customers to geo-fence emitters and set localization-based alerts for sensitive areas.

Bastille is providing three separate service offerings of its solution to meet the needs of the enterprise:

- **Bastille Enterprise:** This is a full solution deployment from one floor to enterprise-wide to discover and localize device/threat sources. Sensors are installed at the same density as WiFi hotspots, with 4-6 sensors minimum per area recommended for premium threat localization. The solution can determine all radio-capable devices in the environment, their threat capabilities and any active threats.

- **Bastille Audit:** This one-month audit focuses on the airborne threats in a single area of an enterprise's environment up to 25,000 square feet. Utilizing a maximum of 10 sensors, Bastille provides organizations with a point-in-time detailed analysis and thorough report of the current threats in their environment.

- **Bastille Desktop:** This one-week audit of airborne threats in a small area gives enterprises a trial of the Bastille solution. Featuring a desktop sensor, enterprises can see the different types of radio-borne threats that enter their airspace on a daily basis.

Bastille is the first company to offer a complete security solution for the Internet of Radios, which includes the world of mobile, wireless, BYOD and the Internet of Things. Bastille has been lauded for its groundbreaking research and discoveries including MouseJack, a massive vulnerability in wireless mice and keyboards, and KeySniffer, a security flaw in low-cost wireless keyboards. The company has also received several industry honors including being named a 2016 Gartner "Cool Vendor," a 2016 Red Herring Top 100 North America award winner, and a finalist for RSA Conference's Innovation Sandbox Contest 2016. Bastille's launch of its flagship solution coincides with the company's 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 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