ForeScout Reveals New Findings that Show Common Enterprise IoT Devices are Hackable in Under Three Minutes

In-depth analysis highlights the dangers posed by enterprise IoT devices, discovering that most can act as simple points of entry into critical enterprise networks

SAN JOSE, Calif. -- (Marketwired - October 25, 2016) – ForeScout Technologies, Inc., a leading Internet of Things (IoT) security company, today released its "IoT Enterprise Risk Report," led by one of the nation's leading ethical hackers, Samy Kamkar. The research findings offer new insight into how common enterprise IoT devices pose an inherent risk to the overall security posture of organizations.

"IoT is here to stay, but the proliferation and ubiquity of these devices in the enterprise is creating a much larger attack surface— one which offers easily accessible entry points for hackers," said Michael DeCesare, president and CEO, ForeScout Technologies, Inc. "The solution starts with real-time, continuous visibility and control of devices the instant they connect — you cannot secure what you cannot see."

Kamkar's research focused on seven common enterprise IoT devices, including IP-connected security systems, smart HVACs and energy meters, video conferencing systems and connected printers, among others. According to his observations from a physical test situation and analysis from peer-reviewed industry research, these devices pose significant risk to the enterprise because the majority of them are not built with embedded security. Of the devices that were outfitted with rudimentary security, Kamkar's analysis revealed many were found to be operating with dangerously outdated firmware.

Additionally, Kamkar's research included a physical hack into an enterprise-grade, network-based security camera. Entirely unmodified and running the latest firmware from the manufacturer, the camera proved itself vulnerable and ultimately allowed for the planting of a backdoor entryway that could be controlled outside the network. To view the hack in its entirety, please visit.

Key findings of the IoT Enterprise Risk Report:

- The identified seven IoT devices can be hacked in as little as three minutes, but can take days or weeks to remediate.

- Should any of these devices become infected, hackers can plant backdoors to create and launch an automated IoT botnet DDoS attack.

- Cybercriminals can leverage jamming or spoofing techniques to hack smart enterprise security systems, enabling them to control motion sensors, locks and surveillance equipment.

- With VoIP phones, exploiting configuration settings to evade authentication can open opportunities for snooping and recording of calls.

- Via connected HVAC systems and energy meters, hackers can force critical rooms (e.g. server rooms) to overheat critical infrastructure and ultimately cause physical damage.

The IoT footprint continues to expand, showing little to no signs of slowing down. Analyst firm Gartner predicts that 20 billion connected devices will be deployed by 2020, with as many as a third of these sitting unknowingly vulnerable on enterprise, government, healthcare and industrial networks around the globe.[1] In turn, hackers are now easily able to pivot on insecure devices into the secure network, and ultimately access other enterprise systems that could store bank account information, personnel files or proprietary business information.

To learn more about the research findings and the risks associated with adopting IoT-enabled devices within the enterprise, go here.

Research Methodology
Commissioned by ForeScout Technologies, Inc., the IoT Enterprise Risk Report employed the skills of Samy Kamkar, one of the world's leading ethical hackers, to investigate the security risks posed by IoT devices in enterprise environments. The report sought to uncover vulnerabilities in enterprise-grade technology utilizing both physical testing situations, as well as drawing from peer-reviewed industry research.

About ForeScout Technologies, Inc.
ForeScout Technologies, Inc. is transforming security through visibility. ForeScout offers Global 2000 enterprises and government organizations the unique ability to see devices, including non-traditional devices, the instant they connect to the network. Equally important, ForeScout lets you control these devices and orchestrate information sharing and operation among disparate security tools to accelerate incident response. Unlike traditional security alternatives, ForeScout achieves this without requiring software agents or previous device knowledge. The company's solutions integrate with leading network, security, mobility and IT management products to overcome security silos, automate workflows and enable significant cost savings. As of January 2016, more than 2,000 customers in over 60 countries improve their network security and compliance posture with ForeScout solutions. Learn more at www.forescout.com.

ForeScout Media Relations Contact
Elliott Suthers

[1] http://www.gartner.com/newsroom/id/3165317

Highwire PR
415 963 4174 ex. 6
ForeScout@Highwirepr.com