Trend Micro Research Finds Serious Business Risks Due to Smart Buildings

As buildings and homes are more connected, enterprise businesses face new physical and data security threats

DALLAS--(BUSINESS WIRE)--Trend Micro Incorporated (TYO: 4704; TSE: 4704), a global leader in cybersecurity solutions, today announced new research revealing that IoT automation platforms in smart buildings are presenting attackers with new opportunities for both physical and data compromise. The findings have serious implications for organizations operating inside smart buildings, including spying on users, unlocking doors and stealing data, as well as employees working from smart home environments.

The new report, *Cybersecurity Risks in Complex IoT Environments: Threats to Smart Homes, Buildings and Other Structures*, warns that automation platforms are increasingly being used to chain multiple devices together to create user-friendly smart applications. This inadvertently creates new and unpredictable attack surfaces that can be hard to manage.

“IoT devices, their uses and the environments in which they are used have all gotten more complex very quickly, but security is still not built into these devices,” Greg Young, vice president of cybersecurity for Trend Micro. “Today, personal and corporate data may cross many routers, an IoT control, various IoT protocols and more all within a day’s work. This creates an ideal situation for criminals – why attack a robust enterprise when the remote worker’s smart home is exceptionally vulnerable.”

Whether a smart building is purpose-built to support IoT or not, there are three main types of automation systems outlined in the report: local standalone servers, cloud-based servers, and virtual assistant-based servers. The first category is the most common, so Trend Micro Research accordingly set up two types, FHEM and Home Assistant servers, to control 100 test connected devices over two sites.

A recent Gartner report estimates that, by 2021, there will be 25.1 billion internet-connected devices, growing at a rate of 32% per year. This report also points out that, “This rapid expansion of connected-device solutions can be summarized as follows: Everything that can be connected to the internet will be — eventually.”1

Researchers found the biggest issue with automation rules is that they become increasingly complex as more devices and actions are added. They are prone to logic errors, and it becomes more challenging to manage, track, and debug actions, especially if there are functional overlaps between rules.

The research reveals a variety of new threats specific to complex IoT environments, including: cloning a user’s voice to issue commands via a voice assistant speaker; adding a phantom device to fool presence detection checks in smart locks to keep doors unlocked; and inserting logic bugs to switch off smart alarms and more.

The research also warns that many IoT automation servers are exposed on the public internet, including 6,200 Home Assistant servers found via a simple Shodan search. Attackers could exploit this security oversight to break into smart buildings, or reprogram automation rules, steal hardcoded sensitive data including router log-ins, add new devices, infect devices with malware, and conscript devices into botnets.

Trend Micro recommends a list of precautionary measures to help mitigate the new threats presented by complex IoT environments, including:

- Enable password protection
- Change default settings
- Do not jailbreak devices or install applications from unverified third-part marketplaces
- Update device firmware
- Enable encryption in both disk storage and communication platforms
- Make regular backups of the configuration and automation rule files of your IoT automation server

For the complete report, please visit: https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/threats-and-risks-to-complex-iot-environments.

About Trend Micro

Trend Micro Incorporated, a global leader in cybersecurity solutions, helps to make the world safe for exchanging digital information. Our innovative solutions for consumers, businesses, and governments provide layered security for data centers, cloud environments, networks, and endpoints. All our products work together to seamlessly share threat intelligence and provide a connected threat defense with centralized visibility and control, enabling better, faster protection. With more than 6,000 employees in over 50 countries and the world’s most advanced global threat intelligence, Trend Micro enables organizations to secure their journey to the cloud. For more information, visit www.trendmicro.com.

1 Gartner, How to Secure the Enterprise Against the Internet of Things Onslaught, Jon Amato, Mark Judd, 14 December 2018

Contact:

Erin Johnson
817-522-7911
media_relations@trendmicro.com

Public Company Information:

TOKYO:
4704
JP3637300009
NQB:
TMICY
