Trend Micro Reveals Top Ten Regions Affected by IoT Security Threats

Smart Home Devices such as routers are vulnerable to cybercriminals

Smart home devices and applications took center stage at many tech events in 2017 from CeBIT to Computex, and even MWC 2017, as cybersecurity threats have continued to grow hand in hand with the increase of connected devices. Trend Micro Incorporated (TYO: 4704; TSE: 4704), a global leader in cyber security solutions, today released the "Trend Micro 2017 1H Smart Home Network Security Summary," revealing the top 10 regions most affected by cyberattacks on a home router and identifying key factors for in-home cyber security threat

In the Internet of Things (IoT) ecosystem today, cyberattacks are becoming more diverse and sophisticated with cybercriminals taking over home network routers to launch attacks on smart home devices. Trend Micro's recent report shows more than 1.8 million cyberattacks have been conducted through home network routers in the past six months. Eight percent of these attacks were outbound attacks where hackers were able to access a home device, then remotely execute malware to obtain confidential information such as passwords or intercept contents transmitted by the affected devices.

"As the value of infecting connected devices continues to rise, these attacks will become increasingly prevalent, particularly impacting the countries outlined in this report," said Richard Ku, senior vice president, commercial IoT Business & market development, Trend Micro. "Our research shows that the use of connected devices for Bitcoin mining has nearly doubled in just a few months. The increased use for malicious gains paired with the significant growth of the industry makes an ideal market for cybercriminals to exploit."

The United States, China and the United Kingdom were the three top countries affected by smart home attacks by cyber criminals. Below is a list of the top ten affected countries, which account for approximately seventy percent of globally detected incidents on smart homes by Trend Micro*, further indicating that security issues of smart home devices are a global threat.

1. United States- 28 percent
2. China- 7 percent
3. United Kingdom-7 percent
4. Hong Kong- 5 percent
5. Canada- 5 percent
6. Australia- 4 percent
7. Sweden- 4 percent
8. Netherlands- 4 percent
9. Taiwan- 3 percent
10. Russia- 3 percent

* Trend Micro detected incidents are gathered from partners' home routers deployed internationally.

Inbound vs Outbound Attacks

Cybercriminals that attack home network systems classify the two main types of cyberattacks on home devices as inbound and outbound attacks. Inbound attacked are when hackers breach the home network on smart devices, such as game counsels, routers and smart TVs, from the internet. Outbound attacks are when hackers gain control of networking devices through inbound attackes and then use them to breach and attack other devices. Desktops, laptops and IP cameras are the most common targets for inbound attacks, while DNS amplification attack is the most common outbound attack. Nearly eighty percent of all attacks that occur on a home router are outbound attacks.

Trend Micro has found that the number of incidents where IoT devices are controlled by cybercriminals for Bitcoin mining has nearly doubled from February to June 2017. It is predicted that as the value of Bitcoin and Ethereum continues to rise, these type of related attacks will continue to become more prevalent.

Risks of Smart Home Devices

According to Trend Micro's research there are three major risks of smart home devices- long-term exposure to unprotected networks, no change of default password and low replacement rate of home devices (plus infrequent firmware/software updates). Comprehensive security protection, users' awareness to the importance of proper configuration and regular updates are critical to smart home security.

1. Long-term Exposure to Unprotected Networks: Most smart home devices connect to external networks via routers, and many consumers tend to overlook the routers security protection, which will allow hackers to exploit vulnerabilities of devices or home network and freely control all home connected devices. This further exposes all family members to

serious risks of personal information leaks.

2. No Change of Default Passwords: Devices used in smart homes such as routers and web cameras often share the same system so it can be conveniently managed. With this however, users leave their devices with default passwords, providing hackers an easy access to these devices.
3. Low Replacement Rate of Home Devices plus Infrequent Firmware/Software Updates: Most home-connected devices, like PC and smart TVs, the product life cycle is not short and will not be frequently replaced. The devices' software system is seldom updated. Overlooking the firmware and system updates both contribute to the increase of cyber security threats.

Trend Micro Smart Home Network Solution Provides Comprehensive Protection for Smart Homes

In the era of thriving IoT development, it is vital to enhance the security posture of connected devices to prevent ever-evolving cyberattacks. Trend Micro's Smart Home Network (SHN) solution provides a wide range of security protection through exclusive deep packet inspection (DPI) technologies, including intrusion protection, IP filtering and application control. In addition, SHN leverages virtual patching to prevent vulnerabilities ahead, protecting users against breaches of personal information or monetary loss. In the first half of 2017 alone, SHN has successfully prevented over five million attacks worldwide. Moving forward, Trend Micro will continue to provide the most advanced cybersecurity technologies for smart home users and deter any future threats.

About Trend Micro

Trend Micro Incorporated, a global leader in cyber security 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 5,000 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.

Media Contact:
Kateri Daniels
publicrelations@trendmicro.com