Trend Micro Finds IoT Is a Hot Topic in Cybercriminal Underground

Global underground analysis reveals monetization of IoT attacks is increasing

DALLAS--(BUSINESS WIRE)--Trend Micro Incorporated (TYO: 4704; TSE: 4704), a global leader in cybersecurity solutions, today released new research detailing a fast-growing market for IoT attacks. Cybercriminals from around the world are actively discussing how to compromise connected devices, and how to leverage these devices for moneymaking schemes.

Trend Micro Research analyzed forums in the Russian, Portuguese, English, Arabic, and Spanish language-based underground markets to determine how cybercriminals are abusing and monetizing connected devices. The results reveal that the most advanced criminal markets are Russian- and Portuguese-speaking forums, in which financially driven attacks are most prominent. In these forums, cybercriminal activity is focused on selling access to compromised devices – mainly routers, webcams and printers – so they can be leveraged for attacks.

“We’ve lifted the lid on the IoT threat landscape to find that cybercriminals are well on their way to creating a thriving marketplace for certain IoT-based attacks and services,” said Steve Quane, executive vice president of network defense and hybrid cloud security for Trend Micro. “Criminals follow the money – always. The IoT market will continue to grow, especially with landscape changes like 5G. While IoT attacks are still in their infancy, we also found criminals discussing how to leverage industrial equipment for the same gain. Enterprises must be ready to protect their Industry 4.0 environments.”

According to Trend Micro’s findings, most conversations and active monetization schemes are focused on consumer devices. However, discussions on how to discover and compromise connected industrial machinery are also occurring, especially the vital programmable logic controllers (PLCs) used to control large-scale manufacturing equipment. The most likely business plan to monetize attacks against these industrial devices involves digital extortion attacks that threaten production downtime.

Additionally, the report predicts an increase in IoT attack toolkits targeting a broader range of consumer devices, such as virtual reality devices. The opportunities for attackers will also multiply as more devices are connected to the internet, driven by 5G implementations.

Trend Micro urges manufacturers to partner with IoT security experts to mitigate cyber-related risks from the design phase. End users and integrators should also gain visibility and control over connected devices to be aware of and curb their cyber risk.

The full report, *The Internet of Things in the Criminal Underground,* can be found here: https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/the-internet-of-things-in-the-cybercrime-underground.

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 secures your connected world. For more information, visit www.trendmicro.com.

Contact:

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

Public Company Information:

TOKYO:
4704
JP3637300009

NQB:
TMICY

---

https://newsroom.trendmicro.com/2019-09-10-Trend-Micro-Finds-IoT-Is-a-Hot-Topic-in-Cybercriminal-Underground