Trend Micro Research Launches New Program to Help IoT Device Makers Tackle Risk at Source

ZDI’s expertise in vulnerability detection offers chance to combat connected device flaws

DALLAS--(BUSINESS WIRE)--Trend Micro Incorporated (TYO: 4704; TSE: 4704), a global leader in cybersecurity solutions, has reconfirmed its commitment to Internet of Things (IoT) security by leading the industry with a new program designed to leverage the global leadership of its Zero Day Initiative (ZDI) to minimize vulnerabilities as smart products are developed. Trend Micro also invites device manufacturers to submit their devices to get help assessing possible vulnerabilities before deploying devices to market, which will be carried out by the company’s world-leading research teams.

According to Gartner1, “The use of Industrial IoT (IIoT) in facilities and the rapid increase in the number of connected devices means that more often events in the binary world can have an effect in the physical world. Gartner predicts that approximately 25 billion IoT devices will be connected in 2021 and that number will continue to increase for the foreseeable future. Even if just a very limited percentage of those devices are IIoT devices controlling or monitoring industrial processes like manufacturing, the sheer number and the pervasiveness of IIoT will most likely lead to an increase in security incidents.”

Insecure devices are inadvertently fueling a range of emerging threats, including corporate data theft and network intrusions, ransomware-related outages, sabotage of industrial equipment, and botnet-driven DDoS and crypto-mining.

“As the success of Mirai, Brickerbot and other attacks have shown, cybercriminals and nation-state actors are increasingly turning their attention to exploiting vulnerabilities in IoT devices,” said Eva Chen, chief executive officer for Trend Micro. “The problem here is that patching flaws after their discovery is highly problematic. Many manufacturers may not have a software update mechanism in place, and even if patches can be issued, customers may have challenges applying them — especially large corporations with potentially thousands of IoT endpoints running in mission critical environments.”

Trend Micro’s ZDI is an industry-leading vulnerability research program that has been helping organizations become more secure for the past 13 years. Today it manages the largest vendor-agnostic bug bounty program in the world with more than 3,500 external researchers complementing the internal team’s efforts.

During the first half of 2018 alone, the ZDI published 600 advisories, a 33 percent increase compared to the same timeframe in 2017. SCADA and Industrial IoT (IIoT) vulnerabilities have comprised around 30 percent of submissions so far this year, with the ICS-CERT as the No. 1 supplier of SCADA/ICS flaws to ZDI.

“Thanks to our new program, device manufacturers gain immediate access to relevant and extensive IoT research, get help assessing possible vulnerabilities before deploying devices to market, and develop a vulnerability handling process to help them going forward,” continued Eva Chen. “Many IoT manufacturers may be struggling to fill key roles with skilled security professionals in-house, so it makes sense to work with the experts so your products come off the factory line as resilient as possible.”

Trend Micro Research and the ZDI is just one element of Trend Micro’s ecosystem approach to securing the Internet of Things. Alongside continued research into emerging threats in areas such as connected speakers, robotic systems, traffic management and connected cars, Trend Micro works with telecom companies, enterprise customers, embedded computing developers and other key stakeholders.

Trend Micro Deep Security provides comprehensive protection in the back-end data center, while Trend Micro Tipping Point intrusion prevention and Deep Discovery breach detection appliances improve security at the network layer. Trend Micro Safe Lock leverages lockdown security software to protect application-specific or legacy OS terminals in IIoT environments.

Trend Micro is fully committed to expanding its knowledge and leadership in understanding and securing risks associated with the fast-growing IoT security market by investing in research and development.

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.

1 *Gartner, Security and Engineering — Converging or Colliding? Published 18 June 2018 - ID G00348946*

Contact:

Trend Micro Incorporated
Kateri Daniels, 817-522-7911
media_relations@trendmicro.com

Public Company Information:

TOKYO:
4704
JP3637300009
NQB:
TMICY