Trend Micro Creates Factory Honeypot and Traps Malicious Attackers

Six-month investigation results can help inform protection strategy for industrial environments

DALLAS--(BUSINESS WIRE)--Trend Micro Incorporated (TYO: 4704; TSE: 4704), a global leader in cybersecurity solutions, today announced the results of a six-month honeypot imitating an industrial factory. The highly sophisticated Operational Technology (OT) honeypot attracted fraud and financially motivated exploits.

The six-month investigation revealed that unsecured industrial environments are primarily victims of common threats. The honeypot was compromised for cryptocurrency mining, targeted by two separate ransomware attacks, and used for consumer fraud.

“Too often, discussion of cyber threats to industrial control systems (ICS) has been confined to highly sophisticated, nation-state level attacks designed to sabotage key processes. While these do present a risk to Industry 4.0, our research proves that more commonplace threats are more likely,” said Greg Young, vice president of cybersecurity for Trend Micro. “Owners of smaller factories and industrial plants should therefore not assume that criminals will leave them alone. A lack of basic protections can open the door to a relatively straightforward ransomware or cryptojacking attack that could have serious consequences for the bottom line.”

To better understand the attacks targeting ICS environments, Trend Micro Research created a highly realistic, industrial prototyping company. The honeypot consisted of real ICS hardware and a mix of physical hosts and virtual machines to run the factory, which included several programmable logic controllers (PLCs), human machine interfaces (HMIs), separate robotic and engineering workstations and a file server.

Trend Micro urges smart factory owners to minimize the number of ports they leave open and to tighten access control policies, among other cybersecurity best practices. In addition, implementing cybersecurity solutions designed for factories, like those offered by Trend Micro, can help further mitigate the risk of attack.

To read more about the research, including the design and deployment of the honeypot itself, please visit: https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/fake-company-real-threats-logs-from-a-smart-factory-honeypot.

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
OTC Pink:
TMICY
