Trend Micro Research Identifies Critical Industry 4.0 Attack Methods

Research report outlines advanced attack scenarios and recommendations for OT operators

DALLAS--(BUSINESS WIRE)--Trend Micro Incorporated (TYO: 4704; TSE: 4704), a global leader in cybersecurity solutions, today released research describing how advanced hackers could leverage unconventional, new attack vectors to sabotage smart manufacturing environments.

For this report, Trend Micro Research worked with Politecnico di Milano in its Industry 4.0 lab, which houses real manufacturing equipment from industry leaders, to demonstrate how malicious threat actors can exploit existing features and security flaws in Industrial IoT (IIoT) environments for espionage of financial gain.

“Past manufacturing cyber attacks have used traditional malware that can be stopped by regular network and endpoint protection. However, advanced attackers are likely to develop Operational Technology (OT) specific attacks designed to fly under the radar,” said Bill Malik, vice president of infrastructure strategies for Trend Micro. “As our research shows, there are multiple vectors now exposed to such threats, which could result in major financial and reputational damage for Industry 4.0 businesses. The answer is IIoT-specific security designed to root out sophisticated, targeted threats.”

“Politecnico di Milano is fully committed to supporting Industry 4.0 in addressing crucial aspects related to security and reliability of automated and advanced controls, especially as they gain relevance in all production sectors and increasingly impact business,” said Giacomo Tavola, Contract Professor in Design and Management of Production Systems and Stefano Zanero, Associate professor in Advanced Cybersecurity Topics for Politecnico di Milano.

Critical smart manufacturing equipment relies primarily on proprietary systems, however these machines have the computing power of traditional IT systems. They are capable of much more than the purpose for which they are deployed, and attackers are able to exploit this power. The computers primarily use proprietary languages to communicate, but just like with IT threats, the languages can be used to input malicious code, traverse through the network, or steal confidential information without being detected.

Though smart manufacturing systems are designed and deployed to be isolated, this seclusion is eroding as IT and OT converge. Due to the intended separation, there is a significant amount of trust built into the systems and therefore very few integrity checks to keep malicious activity out.

The systems and machines that could be taken advantage of include the manufacturing execution system (MES), human machine interfaces (HMIs), and customizable IIoT devices. These are potential weak links in the security chain and could be exploited in such a way to damage produced goods, cause malfunctions, or alter workflows to manufacture defective products.

The report offers a detailed set of defense and mitigation measures, including:

- Deep packet inspection that supports OT protocols to identify anomalous payloads at the network level
- Integrity checks run regularly on endpoints to identify any altered software components
- Code-signing on IIoT devices to include dependencies such as third-party libraries
- Risk analysis to extend beyond physical safety to automation software
- Full chain of trust for data and software in smart manufacturing environments
- Detection tools to recognize vulnerable/malicious logic for complex manufacturing machines
- Sandboxing and privilege separation for software on industrial machines

To find out more and read the full report, please visit:https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/threats-and-consequences-a-security-analysis-of-smart-manufacturing-systems.

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.

About Politecnico di Milano

Politecnico di Milano is a scientific-technological university which trains engineers, architects and industrial designers. The University has always focused on the quality and innovation of its teaching and research, developing a fruitful relationship with business and productive world by means of experimental research and technological transfer. Research has always been linked

to didactics and it is a priority commitment which has allowed Politecnico di Milano to achieve high quality results at an international level as to join the university to the business world. Research constitutes a parallel path to that formed by cooperation and alliances with the industrial system. For more information, visit www.polimi.it.

Contact:

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

Public Company Information:

TOKYO:
4704
JP3637300009
OTC Pink:
TMICY

---

https://newsroom.trendmicro.ca/2020-05-11-Trend-Micro-Research-Identifies-Critical-Industry-4-0-Attack-Methods