Trend Micro Report Reveals 65% of Manufacturing Environments Run Outdated Operating Systems

Latest research details the unique business-critical threats facing converged IT-OT systems

DALLAS--(BUSINESS WIRE)--Trend Micro Incorporated (TYO: 4704; TSE: 4704), a global leader in cybersecurity solutions, today announced new research that demonstrates the threats facing manufacturing networks still running outdated technology, including risks to intellectual property and production processes.

The report, *Securing Smart Factories: Threats to Manufacturing Environments in the Era of Industry 4.0*, outlines the security dimension of a new era for manufacturing driven by IoT and connectivity everywhere. Manufacturers are heavily investing in the convergence of traditional operational technology (OT) with IT networks in 2019, adding new technology to environments that are still vulnerable to more than 10-year-old issues, like Conficker.

“Industry 4.0 offers unparalleled opportunities to increase productivity, enhance process efficiencies, and realize on-demand manufacturing, but it also dramatically alters the threat risk model for these facilities,” said Steve Quane, Executive Vice President, Network Defense and Hybrid Cloud Security for Trend Micro. “As this research outlines, the convergence of IT and OT could unwittingly have a serious impact on production lines, and could lead to the loss of IP and competitive advantage. Trend Micro will continue to support the industry by providing innovative AI-driven solutions to protect business critical data and processes across the connected world.”

The report highlights the unique triple threat facing manufacturing, including the risks associated with IT, OT and IP. Previously isolated operations networks are being connected to the IT network to drive efficiencies, but this exposes insecure proprietary protocols and potentially decades-old OT equipment that is often not patched frequently enough because of its criticality. There is a harsh disparity between the significant operations performed by these devices and the fact that they operate for years with known vulnerabilities.

According to Gartner1, “OT networks and assets, and their security implications, were undiscovered and unmanaged for many years. As a result, current OT networks are unsegmented with a mix of production protocols, unidentified assets, legacy systems and devices. These industrial components have many unsecure communication channels to corporate/IT networks, and they utilize different vendor architectures and security standards.”

In addition to maintaining legacy infrastructure with known weaknesses, new vulnerabilities are being discovered more frequently than ever before in these systems. Zero-day vulnerabilities purchased in human-machine interfaces (HMIs) of industrial control systems increased by more than 200 percent in 2018 compared to the previous year.

Manufacturers are thus exposed to both targeted and commodity malware, including cryptocurrency mining attacks that could harm key production processes by consuming processing power and causing network latency. Ransomware is also a major threat to manufacturers if the attack affects production.

To help mitigate the impact of Industry 4.0 threats, Trend Micro recommends manufacturers remember the basics of cybersecurity, such as restricting user access and disabling directory listings, as well as identifying and prioritizing key assets to protect.

To find out more, read the complete report here: https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/security-in-the-era-of-industry-4-dealing-with-threats-to-smart-manufacturing-environments.

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 workloads, networks, and endpoints. All our products work together to seamlessly share threat intelligence and provide a connected threat defense with centralized visibility and investigation, enabling better, faster protection. With more than 6,000 employees in 50 countries and the world’s most advanced global threat research and intelligence, Trend Micro enables organizations to secure their connected world. For more information, visit www.trendmicro.com.

1 *Gartner, Inc., 2018 Strategic Roadmap for Integrated IT and OT Security, Saniye Burcu Alaybeyi, 3 May 2018*

Contact:

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

Public Company Information:

TOKYO:
4704
JP3637300009
NQB:
TMICY

---

https://newsroom.trendmicro.com/2019-04-03-Trend-Micro-Report-Reveals-65-of-Manufacturing-Environments-Run-Outdated-Operating-Systems