Cyber-Attacks on Industrial Assets Cost Firms Millions

Trend Micro study reveals the impact of threats to ICS/OT environments

DALLAS, June 2, 2022 /PRNewswire/ -- Trend Micro Incorporated (TYO: 4704; TSE: 4704), a global cybersecurity leader, today announced new research* revealing that 89% of electricity, oil & gas, and manufacturing firms have experienced cyber-attacks impacting production and energy supply over the past 12 months.

To read a full copy of the research, *The State of Industrial Cybersecurity*, please visit: https://resources.trendmicro.com/IoT-survey-report.html

Trend Micro study reveals the impact of cyber threats on ICS/OT organizations.

"Across the globe, industrial locations are going digital to drive sustainable growth. But this has invited a deluge of threats which they are ill-equipped to mitigate, causing major financial and reputational damage," said William Malik, vice president of infrastructure of strategies at Trend Micro. "Managing these heavily networked IT and OT environments effectively requires an experienced partner with the foresight and breadth of capabilities needed to deliver best-in-class protection across both environments."

The findings come a year after the Colonial Pipeline ransomware attack, which forced OT systems at the provider offline for several days, leading to major fuel shortages up and down the US East Coast. It is still the largest critical infrastructure (CNI) attack of its kind.

Around half of the industrial sector organizations affected by CNI attacks made efforts to improve cybersecurity infrastructures but do not always have sufficient resources or knowledge in place to defend against future threats.

Of the responding organizations that suffered cyber disruption to their industrial control systems and operational technology (ICS/OT), the average financial damages amount to approximately $2.8 million, with the oil & gas industry suffering the most.

Almost three-quarters (72%) of respondents admitted they experienced cyber disruption to their ICS/OT environments at least six times during the year.

The research also found that:

- 40% of respondents could not block the initial attack
- 48% of those who say there have been some disruptions do not always make improvements to minimize future cyber risks.
- Future investments in cloud systems (28%) and private 5G deployments (26%) were the top two drivers of cybersecurity among respondents.
- The OT security function tends to be less mature than IT on average in terms of risk-based security.

The addition of cloud, edge, and 5G in the mixed IT and OT environments has rapidly transformed industrial operations and systems. Organizations must stay ahead of the curve and take security measures to protect business assets. Improving risk and threat visibility is a curtail first step to a secure industrial cloud and private network.

"Trend Micro exceeded our expectations right from the start, and we haven't looked back since," said David Levine, vice president of Information Security and CISO, Ricoh USA. "With Trend Micro, you get an immediate reaction, escalation, and communication. It's about effective, innovative tools, coupled with a great partnership."

Trend Micro's unified cybersecurity platform provides streamlined detection and response, adaptive to ICS and 5G, to equip organizations in the complex industrial environment where different technologies and applications are integrated to support business operations. To learn more about Trend Micro ICS/OT security, please visit: https://www.trendmicro.com/en_us/business/solutions/iot/ics-ot.html#tabs-c89bc2-6

** Trend Micro polled 900 ICS cybersecurity leads in Germany, the US, and Japan's manufacturing, oil & gas, and electricity sectors to compile its new study.*

About Trend Micro
Trend Micro, a global cybersecurity leader, helps make the world safe for exchanging digital information. Fueled by decades of security expertise, global threat research, and continuous innovation, Trend Micro's cybersecurity platform protects hundreds of thousands of organizations and millions of individuals across clouds, networks, devices, and endpoints. As a leader in cloud and enterprise cybersecurity, the platform delivers a powerful range of advanced threat defense techniques optimized for environments like AWS, Microsoft, and Google, and central visibility for better, faster detection and response. With 7,000 employees across 65 countries, Trend Micro enables organizations to simplify and secure their connected world.

employees across 65 countries, Trend Micro enables organizations to simplify and secure their connected world. www.TrendMicro.com.

SOURCE Trend Micro Incorporated

For further information: Trend Micro Communications, 817-522-7911, media_relations@trendmicro.com

---

https://newsroom.trendmicro.com/2022-06-02-Cyber-Attacks-on-Industrial-Assets-Cost-Firms-Millions