Trend Micro Warns of Ransomware Targeting Industrial Control Systems

Latest report highlights United States as the prime target of global threat actors

DALLAS, June 30, 2021 /PRNewswire/ -- Trend Micro Incorporated (TYO: 4704; TSE: 4704), a global cybersecurity leader, today released a new report highlighting the growing risk of downtime and sensitive data theft from ransomware attacks aimed at industrial facilities.

Click here to read a full copy of the report, *2020 Report on Threats Affecting ICS Endpoints*: https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/2020-report-ics-endpoints-as-starting-points-for-threats*.*

"Industrial Control Systems are incredibly challenging to secure, leaving plenty of gaps in protection that threat actors are clearly exploiting with growing determination," said Ryan Flores, senior manager of forward-looking threat research for Trend Micro. "Given the US government is now treating ransomware attacks with the same gravity as terrorism, we hope our latest research will help industrial plant owners to prioritize and refocus their security efforts."

Industrial Control Systems (ICS) are a crucial element of utility plants, factories and other facilities—where they're used to monitor and control industrial processes across IT-OT networks.

If ransomware finds its way onto these systems, it could knock out operations for days and increase the risk of designs, programs, and other sensitive documents finding their way onto the dark web.

Trend Micro's report found that Ryuk (20%), Nefilim (14.6%), Sodinokibi (13.5%) and LockBit (10.4%) variants accounted for more than half of ICS ransomware infections in 2020.

The report also revealed:

- Threat actors are infecting ICS endpoints to mine for cryptocurrency using unpatched operating systems still vulnerable to EternalBlue.
- Variants of Conficker are spreading on ICS endpoints running newer operating systems by brute-forcing admin shares.
- Legacy malware such as Autorun, Gamarue and Palevo are still widespread in IT/OT networks, spreading via removable drives.

The report urged closer cooperation between IT security and OT teams to identify key systems and dependencies such as OS compatibility and up-time requirements, with a view to developing more effective security strategies.

Trend Micro makes the following recommendations:

- Prompt patching is vital. If this is not possible, consider network segmentation or virtual patching from vendors like Trend Micro.
- Tackle post-intrusion ransomware by mitigating the root causes of infection via application control software, and threat detection and response tools to sweep networks for IoCs.
- Restrict network shares and enforce strong username/password combinations to prevent unauthorized access through credential brute forcing.
- Use an IDS or IPS to baseline normal network behavior to better spot suspicious activity.
- Scan ICS endpoints in air-gapped environments using standalone tools.
- Set up USB malware scanning kiosks to check the removable drives used to transfer data between air-gapped endpoints.
- Apply principle of least privilege to OT network admins and operators.

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. www.TrendMicro.com.

SOURCE Trend Micro Incorporated

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

---

https://newsroom.trendmicro.ca/2021-06-30-Trend-Micro-Warns-of-Ransomware-Targeting-Industrial-Control-Systems