Trend Micro Research Exposes Risk of Supply Chain Attacks to Water and Energy Systems

Many systems found vulnerable to significant cyber risk within critical industries

DALLAS--(BUSINESS WIRE)--Trend Micro Incorporated (TYO: 4704; TSE: 4704), a global leader in cybersecurity solutions, today published research revealing how exposed human machine interface (HMI) systems in thousands of critical water and energy organizations around the world could be exploited, causing significant real-world impacts, such as contaminating the water supply.

HMIs are a key part of industrial IT systems that allow human operators to interact with supervisory control and data acquisition (SCADA) environments. A large majority of the identified exposed systems are from smaller energy and water organizations that feed the major enterprise supply chain, which serves the general public. With access to an exposed HMI system, an attacker is not only able to see all the information about critical systems, but can also interact with and abuse these interfaces.

“Critical infrastructure is a national focal point for cybersecurity – and for cybercriminals, who can pinpoint and exploit the weakest link in these connected systems,” said Mark Nunnikhoven, vice president of cloud research for Trend Micro. “That’s troubling, as Trend Micro Research continues to find critical devices, and the networks that they connect to, needlessly exposed. This exposure, combined with the record number of ICS vulnerabilities reported through the Zero Day Initiative this year, highlights a growing risk that extends into each of our communities.”

Many of these HMIs are legacy systems that were not initially designed to be connected to a network in this way. Today, connectivity is being added to many legacy operational technology systems, which have long lifespans and are very difficult to patch, exacerbating the risk of attack.

In the report, Trend Micro researchers detail potential attack scenarios that would have substantial real-world impacts to critical infrastructure using information found in the exposed systems. This information includes the type of device, physical location, and other system-level information, which can all be used to inform a potential attack.

Attackers may soon turn their attention to exploiting these exposed systems due to an increase in new vulnerabilities found this year. Trend Micro’s Zero Day Initiative has published nearly 400 SCADA-related vulnerability advisories in 2018 so far – a 200 percent increase compared to the same time last year.

Based on a recent survey by Trend Micro, operational technologies like these have not typically been managed by IT or security teams. The ongoing confusion around who in an organization is responsible for securing connected devices often leaves them more at risk.

To protect HMI systems against the risk of attack, security leaders must ensure the interfaces are properly secured if they must be connected to the internet. Likewise, there should be as much isolation as possible in place between these devices and the corporate network, which maintains operational needs while eliminating the risk of exposure and exploitation.

“If we hadn’t found the command and control malware in our SCADA environment, our toxic gases monitoring systems could have been compromised and may put human lives in danger,” said Ireneo Demanarig, chief information officer, CEITEC S.A. “Security must be at the core of our company. Trend Micro not only provides comprehensive security solutions, but they are a great partner in automating threat intelligence sharing that makes our lives easier.”

Trend Micro’s industry-leading security solutions are used to protect customers globally against SCADA network threats. For more information on Trend Micro’s findings and the risks facing critical infrastructure, please visit: https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/exposed-and-vulnerable-critical-infrastructure-the-water-energy-industries

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.

Contact:

Trend Micro Incorporated
Erin Johnson, 817-522-7911
media_relations@trendmicro.com

Public Company Information:

TOKYO:
4704
JP3637300009
NQB:
TMICY

---

https://newsroom.trendmicro.ca/2018-10-30-Trend-Micro-Research-Exposes-Risk-of-Supply-Chain-Attacks-to-Water-and-Energy-Systems