Threat Intelligence Report

Threats to Operational Technology in Critical Infrastructure Sectors

Critical infrastructure sectors are among the most at-risk targets for major cyber attacks from both cyber criminals and nation-state threat actors, largely due to the significant and widespread disruptions these attacks can cause. Many critical infrastructure sectors, namely energy, manufacturing, and water, are dependent on operational technology (OT) to carry out basic functions.[1] However, the security of OT systems is often de-prioritized compared to that of information technology (IT) systems. OT has become more vulnerable to cyber attacks as systems have undergone a digital transformation, frequently adopting protocols from IT. Threat actors have been observed exploiting insecure and misconfigured OT systems in North American and European critical infrastructure sectors as recently as April 2024.

THREAT ACTIVITY

- In April 2024, US government agencies advised of nation-state hacktivists known to target and compromise modular, Internet-exposed OT through remote access software and default passwords. Outdated and misconfigured systems can be infiltrated with less sophisticated measures, making them an easier target for threat actors.
- In February 2024, global cybersecurity and law enforcement directorates published an advisory about a nation-state threat actor seeking to pre-position themselves for cyber attacks against US critical infrastructure. The group is known to have stolen multiple files related to OT equipment, including SCADA systems, relays, and switchgear.
- As OT systems become increasingly connected with IT environments, they are vulnerable to downstream impact from “traditional” cyber attacks, like ransomware. In 2023, cyber attacks against two major manufacturers, both of which operate in critical infrastructure sectors, caused significant disruptions to manufacturing processes. In total, the incidents cost the companies $49 million and $27 million, respectively.

THREAT ASSESSMENT

Governing agencies across critical sectors have identified increased cybersecurity risks facing critical infrastructure, especially from nation-state and ransomware threat actors.

- On April 30, 2024, the Biden-Harris administration announced a new National Security Memorandum on critical infrastructure, detailing how the US government is working to get ahead of threat actors to "enhance our collective resilience to disasters before they happen."
- On April 4, 2024, the Cybersecurity and Infrastructure Security Agency published a Notice of Proposed Rulemaking requiring "substantial cybersecurity incidents" in the critical infrastructure sector be reported within 72 hours and ransomware payments be reported within 24 hours.
- The Department of Transportation Maritime Administration released a 2023 report detailing the increasing cyber risks facing U.S. ports due to the large number of stakeholders involved in their operation and risks identified within OT systems.

RECOMMENDED ACTION

- Segment networks into distinct zones to control traffic flow between OT and IT networks.
- Use role-based access controls and least privilege principles to ensure that users only have access to necessary systems and data.
- Ensure that all systems and software versions are up-to-date and patched.
- Require the use of Multi-Factor Authentication for remote access solutions used to access OT environments.
- Actively monitor the OT estate to identify suspicious user behavior and respond appropriately.
- Implement allowlisting, limiting access to only authorized IP addresses.
- Develop and regularly update an incident response plan tailored to the OT environment.
- Assess the security practices of third-party vendors who have access to your OT network.

1. Operational technology refers to hardware and software responsible for direct monitoring and/or control of industrial equipment, assets, processes and events. OT also encompasses Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition (SCADA) systems.

SOURCES

Sources include open-source information from public and private industry reporting.

- Defending OT Operations Against Ongoing Pro-Russia Hacktivist Activity
- Biden admin, U.S. ports prep for cyberattacks as nationwide infrastructure is targeted
- Biden-Harris Administration Announces New National Security Memorandum on Critical Infrastructure
- 2023-002-Worldwide-Maritime Port Vulnerabilities - Foreign Adversarial Technological, Physical, and Cyber Influence
- Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements
- Canadian Centre for Cybersecurity Cyber Threat Bulletin: The Cyber Threat to Operational Technology
- Clorox Says Cyberattack Costs Exceed $49 Million
- PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure

Why FTI Cybersecurity

Multidisciplinary Expertise

Intelligence-led, expert-driven, strategic approach to cybersecurity challenges

Core team from intelligence agencies, law enforcement, prosecuting offices, and global private sector institutions

Globally Positioned

Ability to respond anywhere in the world

Ability to staff the largest and most complex engagements and investigations

Relationships with the top global intelligence agencies, regulatory authorities, and private agencies

Integrated & Comprehensive

Comprehensive services include crisis communications, e-discovery, forensic investigations, and more

Seamless integration of FTI Consulting's expertise across service offerings

FTI Cybersecurity Global Offices

Americas

Atlanta
Boston
Chicago
Dallas
Houston
Irvine
Los Angeles
Mexico City
Miami
New York
Philadelphia
Roseland
San Francisco
Sao Paulo
Seattle
Toronto
Washington, DC
Wayne

EMEA

Berlin
Brussels
Cape Town
Dubai
Dublin
Dusseldorf
Frankfurt
Johannesburg
London
Madrid
Mumbai
Munich
Paris
Zurich

APAC

Brisbane
Hong Kong
Melbourne
Perth
Shanghai
Singapore
Sydney
Tokyo

CONTACT FTI CYBERSECURITY

Email: #fticybersecurity@fticonsulting.com

Phone: +1-844-CYBR-FTI (+1-844-292-7384)