Securing the Nation's Critical Infrastructure | Action Plans to Defend Against Cyber Attacks

June 27, 2022
by Vikram Navali and Varun Anand

Industries around the globe increasingly rely on operational technology (OT) and industrial control systems (ICS) to support their mission-critical infrastructures while at the same time they are facing a significant increase in cyber threats.

According to the CISA, the Russian government is exploiting options for cyberattacks against critical infrastructure systems. Other threat actors have deliberately targeted critical infrastructure in the past and the challenge remains: how do we protect mission-critical cyber assets that are crucial to the nation's well-being?

Why Do Cybercriminals Target Critical Infrastructure?

There are several reasons why cybercriminals target critical infrastructure. Most of the malicious cyber activities on ICS and Supervisory control and data acquisition (SCADA) systems are financially or politically motivated.

Financially-motivated attackers seek to hit public services with ransomware, in part because such assets are often running on legacy hardware or software and may be vulnerable to known exploits. Ransomware operators also hope that the mission-critical nature of such targets will force organizations to pay the ransom in order to protect those that rely on the services they provide.

Politically-motivated attackers, meanwhile, seek to disrupt critical national infrastructure during times of crisis or when significant events are taking place, such as elections, health emergencies and wars. Such politically-motivated attacks often reach beyond their intended targets, causing collateral damage to other organizations. During Russia's invasion of Ukraine, for example, threat actors targeted essential organizational infrastructure within and beyond the region. These state-sponsored cyber operations have included distributed denial-of-service (DDoS) attacks and the deployment of destructive malware against the Ukrainian government and critical national infrastructure (CNI) organizations.

Targeting critical infrastructure to trigger a panic can include attacking the nation's financial and healthcare systems or electricity grids. Cybercriminals have attacked high-value organizations and those that provide critical services in several high-profile incidents. These included AcidRain, an attack on Viasat KA-SAT modems in Europe, Russian state-sponsored distributed denial-of-service (DDoS) attacks, the Colonial Pipeline attack, a ransomware attack on JBS Foods, and a supply chain attack on Kaseya Limited.

How Do Cybercriminals Exploit Critical Infrastructure?

Several factors have contributed to devastating organizational breaches. Here are some of the ways that cyber-criminals explore options for potential cyberattacks:

- Exploit vulnerable systems – Unpatched and misconfigured devices in the critical infrastructure pose a significant risk of being breached. Attackers look for vulnerabilities that exist in the standard and proprietary ICS protocols, including RMS (Manufacturing Message Specification), GOOSE (Generic Object Oriented Substation Event) by IEC 61850 standard, MODBUS (supervision and control), DNP3 (Energy and Water), BACNET (Building Automation), and IPMI (Baseboard Management Control). They know the mitigations may not always be possible and attempt to exploit these weaknesses.
- Perform denial-of-service (DDS) attacks – Attackers can gain access through a compromised IT system, perform reconnaissance activities and move laterally to the OT network to launch a denial-of-service attack.
- Deploy ransomware and/or wipers – a recent report from CISA shows an increase in sophisticated, high-impact ransomware incidents against critical infrastructure organizations globally. CISA, the FBI, and the NSA have observed incidents involving ransomware against 14 of the 16 U.S. critical infrastructure sectors, including the Defense Industrial Base, Emergency Services, Food and Agriculture, Government Facilities, and Information Technology Sectors. They also observed that several ransomware groups had developed code to stop critical infrastructure or industrial processes.

Recommended Action Plans to Protect ICS Systems

Securing infrastructure requires a new approach to mitigating cyber-attacks targeting OT/ICS systems vulnerabilities. Here are some recommended action plans that will help protect essential OT assets in today's interconnected world.

- Conduct security assessments of OT (ICS/SCADA) systems regularly.
- Identity OT and IT networks and implement network segmentation between IT and OT networks. Network segmentation limits the ability of adversaries to pivot to the OT network even if the IT network is compromised.
- Identify assets in the OT network and eliminate possible vulnerabilities across a comprehensive set of attack vectors.
- Protect endpoints to reveal any suspicious, malicious activity in industrial networks. Identify, detect, and investigate suspicious activity indicating lateral movements within IT and OT networks. Deploy endpoint-based solutions, such as Singularity Identity to detect lateral connections.
- Protect credentials. Russian state-sponsored APT actors have demonstrated their ability to maintain persistence using compromised credentials.
- Implement data backup procedures on both the IT and OT networks. Regularly test backup procedures and ensure that backups are isolated from network connections that could enable the spread of malware. Understand actual behavior, e.g., the type of device, what it is doing, and what it tries to connect to.

How Can the SentinelOne Identity Portfolio Help?

SentinelOne is the leader in Ransomware Anti-Encryption Technology and offers innovative ICS security solutions to protect critical infrastructure. Five of the Fortune 10's largest ICS/SCADA organizations have already widely deployed the company's comprehensive solutions. The PNNL(Pacific Northwest National Laboratory), a DoE national laboratory, also validated the security solutions protecting critical national infrastructure.

The Singularity™ Hologram solution provides comprehensive deception capabilities covering traditional enterprise IT and OT networks. The deception platform offers adaptive cybersecurity defense using machine learning to create deception campaigns that address the evolving attack surface. The platform supports a large subset of ICS protocols and allows customers to build emulations of various PLCs, SCADA nodes, medical equipment and more. Attackers targeting and exploiting vulnerabilities in Human Machine Interface (HMI) systems are common attack vectors. Customers can deploy decoy HMI systems using golden images.

The ICS security solution provides comprehensive deception capabilities covering traditional enterprise IT and OT networks. The platform projects deceptive decoys into SCADA, ICS, IoT, Point of Sale, and Medical Device networks, identifying attacker lateral movement and reconnaissance activity targeting production-critical systems. Additionally, the Singularity™ Identity solutions deploy deceptive credentials that can detect and report on cybercriminals leveraging their operations through remote services and exploiting ICS infrastructure.

Conclusion

Critical infrastructure is vital to public safety and health in many ways, but these essential services are often maintained by organizations with small budgets running legacy hardware and software.

To ensure the safety of mission-critical assets, organizations must put in place robust action plans that include autonomous endpoint security controls that can reduce the need for a large SOC while still continuously monitoring the ICS network for suspicious and malicious activity. To learn more about how SentinelOne can help, contact us or request a free demo.

Like this article? Follow us on LinkedIn, Twitter, YouTube or Facebook to see the content we post.

Read more about Cyber Security

- Rise in Identity-Based Attacks Drives Demand for a New Security Approach
- Detecting Unsanctioned Delegated Exposure in AD Environment
- Versus Ransomware | Zeolitus Spin-off Shows Sandboxization Isn't Necessary for Success
- Top 10 Ways to Protect Your Active Directory
- Detecting a Rogue Domain Controller – DCShadow Attack
- Protecting Your Active Directory from AdminSDHolder Attacks