CISA Cybersecurity Resources: Geopolitical Tensions

OVERVIEW

Given the increased focus on the geopolitical landscape, CISA is proactively leaning forward to ensure that our industry partners are aware of all CISA resources available to combat potential threats.

On Jan. 11, 2022, we released a joint cybersecurity advisory (CSA) with the FBI and NSA about the Russian threat to U.S. critical infrastructure, including specific tactics, techniques, and procedures associated with Russian actors. We followed this advisory with an executive-level product urging every organization to take urgent, near-term steps to reduce the likelihood and impact of a potentially damaging compromise.

CYBERSECURITY ALERTS

CISA, the FBI, and NSA encourage the cybersecurity community—especially critical infrastructure network defenders—to adopt a heightened state of awareness and to conduct proactive threat hunting, as outlined in the Detection section of the joint CSA. Additionally, CISA, the FBI, and NSA strongly urge network defenders to implement the recommendations detailed in the linked pdf. These mitigations will help organizations improve their functional resilience by reducing the risk of compromise or severe business degradation:

1. **Be prepared**. Confirm reporting processes and minimize personnel gaps in IT/OT security coverage. Create, maintain, and exercise a cyber incident response plan, resilience plan, and continuity of operations plan so that critical functions and operations can be kept running if technology systems need to be taken offline.
2. **Enhance your organization's cyber posture**. Follow best practices for identity and access management, protective controls and architecture, and vulnerability and configuration management.
3. **Increase organizational vigilance**. Stay current on information pertaining to this threat. Subscribe to CISA's mailing list and feeds to receive notifications when CISA releases information about a security topic or threat.

You can find all of our recent alerts and advisories on our alerts web page, including AA22-011A : Understanding and Mitigating Russian State-Sponsored Cyber Threats to U.S. Critical Infrastructure and AA21-200B : Chinese State-Sponsored Cyber Operations: Observed TTPs. CISA also maintains a dedicated public webpage providing an overview of the Russian government's malicious cyber activities as well as all of our advisories and products on Russian state-sponsored cyber threats.

CRITICAL INFRASTRUCTURE

Today's threats take the form of hybrid attacks targeting both physical and cyber assets. The adoption and integration of Internet of Things devices have led to an increasingly interconnected mesh of cyber-physical systems, which expands the attack surface and blurs the once clear functions of cybersecurity and physical security. Meanwhile, efforts to build cyber resilience and accelerate the adoption of advanced technologies can also introduce or exacerbate security risks in this evolving threat landscape. A successful cyber or physical attack on connected industrial control systems and networks can disrupt operations or even deny critical services to society.

The *Cybersecurity and Infrastructure Security Convergence Action Guide* describes the complex threat environment created by increasingly interconnected cyber-physical systems, and the impacts that this interconnectivity has on an organization's cybersecurity and physical security functions. It also provides information that organizations can consider to adopt a holistic cyber-physical security approach through a flexible framework. The CISA Services Catalog provides information about all of the tools and resources CISA offers for both cyber and physical security.

Report a ransomware incident to the FBI

Report a cyber incident to CISA