ANOMALI

Empowering Governors

Proactive Measures Against Foreign Cyber Threats

U.S. Governors Must Understand the Evolution of Foreign Cyber Threats Immediately

Governors have initiated a broad range of actions to protect their states from U.S. foreign adversaries. Recognizing rising international risks, U.S. Governors took proactive measures to mitigate those threats:

- Divested state pension funds from nations that seek to harm our national interests
- Banned foreign ownership of sensitive land
- Prohibited contracts with foreign nation-states that harm our interests
- Banned Tik-Tok from state devices

However, "advanced persistent threats" (APTs) to our nation's sensitive critical infrastructure from nation-states and their allies from China, Russia, Iran, and North Korea are quite common, according to the Cybersecurity & Infrastructure Security Agency (CISA), cybersecurity experts and our law-enforcement officials.

U.S. Governors must recognize that foreign threats are no longer limited to ransomware and financial crimes. In fact, they've escalated and could be used to disrupt water utilities, transportation networks, ports, and power generation facilities. Within the past six months, Russia, China, and Iran have all initiated various incursions into these sensitive facilities:

- A water utility serving a western Pennsylvania town was attacked by Iranian threat actors[1] who gained operational control of the system. Cybersecurity experts estimate that 70% or more of municipal water providers lack basic standards to prevent breaches and hacks.[2]
- A U.S. Naval Base in Guam was targeted by Chinese groups.[3]
- The Chinese Group Volt Typhoon has been documented inside water, power, and port networks throughout the United States.[4]
- Federal officials have warned U.S. ports that up to 80% of the cranes in operation, as well as their operating software, were manufactured in China.[5]
- A Texas utility adjacent to an Air Force base was disrupted.[6]

If attacked, American critical infrastructure could pose a life and safety risk to the public. Although most states have invested in technology, workforce, and processes to protect state networks from these types of attacks, the risks remain.

Additionally, sensitive networks run by private utilities or local governments are much more vulnerable. As smaller providers, they do not have the resources to identify, mitigate, or respond to the sophisticated attacks launched by hostile nation-states who wish to create chaos and do us harm.

Governors are uniquely positioned to convene and coordinate local governments and infrastructure providers to proactively plan for responses. Utilizing their National Guard and Emergency Management resources, governors can share information and facilitate coordination to prevent attacks. Cyber threat intelligence and analysis can help.

Defending Against Threats with a State-Led Information Sharing and Analysis Center (ISAC)

A mid-Atlantic state responded to international cyber threats by establishing a state-local information threat sharing platform. This ensured that state agencies, counties, and school boards automatically received real-time information about threats facing them and other governmental entities.

Rather than manually calling or emailing each other, the state and local governments were able to establish this innovative partnership to protect these sensitive networks from incursions.

Just as they protected their states from other types of foreign threats, governors can partner and collaborate with critical infrastructure providers and the private sector to protect critical infrastructure. Cyber threat intelligence and analysis software can facilitate up-to-the-minute intelligence about these foreign threats and help their agencies and partners in local government prevent these attacks from ever happening for a more secure tomorrow.

Anomali Empowers Your ISAC with Threat Intel and Remediation

Anomali offers immediate and comprehensive visibility into active threats, coupled with how and where specifically your infrastructure is at risk. By automatically containing and remediating threats in real time and immediately sharing this information with relevant ISACs, Anomali can enable state governments and their extended ecosystems to take preventative measures, stopping attacks before they gain traction.

Get Started with Anomali

Anomali offers an industry-leading AI-Powered solution that elevates your security operations and de-fense capabilities in one platform. We consolidate your tech stack, giving you never- before-seen speed, scale, and performance at a fraction of the cost. Anomali empowers your team and helps you retain talent. Simply different. http://www.anomali.com.

1. Exploitation of Unitronics PLCs used in Water and Wastewater Systems
2. Enforcement Alert: Drinking Water Systems to Address Cybersecurity Vulnerabilities
3. Chinese hackers behind Guam breach have been spying on US military for years
4. Volt Typhoon targets US critical infrastructure with living-off-the-land techniques
5. Chinese-made cranes at U.S. ports may pose a national security threat
6. China-Backed Hackers Threaten Texas Military Sites, Utilities