Subject: Joint Cybersecurity Advisory on tactics Used by Russian State-sponsored Actors to target US and International Energy Sector Organizations

---

Critical Infrastructure Partners,

The Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), and the Department of Energy (DOE) announced a joint Cybersecurity Advisory today with information on Russian state-sponsored cyber actors that conducted multiple intrusion campaigns targeting U.S. and international energy sector organizations from 2011 to 2018. This advisory is being published in conjunction with the U.S. Department of Justice announcement of unsealed indictments today.

The advisory titled, "Tactics, Techniques, and Procedures of Indicted State-Sponsored Russian Cyber Actors Targeting the Energy Sector," provides the technical details about a global energy sector intrusion campaign using Havex malware, and a compromise of a Middle East-based energy sector organization using TRITON malware. In both instances, the threat actors were also involved in activity targeting U.S. energy sector companies.

While this advisory documents historical cyber activity, CISA, FBI and DOE assess that state-sponsored Russian cyber operations continue to pose an ongoing threat to U.S. Energy Sector networks. Actions that executives and leaders can take now to protect to their networks are:

- Implementing and ensuring robust network segmentation between information technology and industrial control systems (ICS) networks;
- Enforcing multifactor authentication to authenticate into a system; and
- Managing the creation of, modification of, use of, and permissions associated with privileged accounts.

In addition to reviewing this new advisory, CISA encourages critical infrastructure executives and senior leaders to review our "Shields Up" webpage at www.cisa.gov/shields-up. Also, organizations should report incidents and unusual activity to CISA 24/7 Operations Center at report@cisa.gov or (888) 282-0870 and/or to the FBI via your local FBI field office or the FBI's 24/7 CyWatch at (855) 292-3937 or CyWatch@fbi.gov.

We encourage you to share this information widely.

Cybersecurity and Infrastructure Security Agency

Thank you,

Connect with us at CISA, Facebook, Twitter, LinkedIn, and YouTube

Subscribe to receive CISA alerts and updates

Subscribe to receive DHS information, alerts, & updates