HC3: Alert

March 25, 2022 TLP: WHITE Report: 202203251200

State-Sponsored Russian Cyber Actors Targeted Energy Sector from 2011 to 2018

Executive Summary

On March 24, 2022, CISA, the Federal Bureau of Investigation, and the Department of Energy released a joint Cybersecurity Advisory (CSA) detailing campaigns conducted by state-sponsored Russian cyber actors from 2011 to 2018 that targeted U.S. and international Energy Sector organizations. The CSA highlights historical tactics, techniques, and procedures (TTPs) as well as mitigations Energy Sector organizations can take now to protect their networks. On March 24, 2022, the U.S. Department of Justice unsealed indictments of three Russian Federal Security Service (FSB) officers and a Russian Federation Central Scientific Research Institute of Chemistry and Mechanics (TsNIIKhM) employee for their involvement in the following intrusion campaigns against U.S. and international oil refineries, nuclear facilities, and energy companies. This CSA provides the TTPs used by indicted FSB and TsNIIKhM actors in cyber operations against the global Energy Sector.

Report

Alert (AA22-083A) Tactics, Techniques, and Procedures of Indicted State-Sponsored Russian Cyber Actors Targeting the Energy Sector
https://www.cisa.gov/uscert/ncas/alerts/aa22-083a

Impact to HPH Sector

While this joint Cybersecurity Advisory (CSA) is related to Russian cyber actors targeting the global Energy Sector, the TTPs and corresponding mitigations may be applicable to Healthcare and Public Health (HPH) organizations. The report details TTPs associated with the Havex and Triton malware families targeting ICS/SCADA systems. Furthermore, HPH entities such as hospitals heavily rely on energy supply for critical day-to-day operations and the healthcare sector is a major energy consumer, responsible for an estimated five to eight percent of global energy consumption, according to a 2019 study.

CISA offers a range of no-cost cyber hygiene services to help organizations assess, identify, and reduce their exposure to threats, including ransomware. By requesting these services, organizations of any size could find ways to reduce their risk and mitigate attack vectors. All organizations should immediately report incidents to CISA at https://us-cert.cisa.gov/report , a local FBI Field Office, or U.S. Secret Service Field Office.

References

Links to additional references and resources can be found in the above referenced report.

Contact Information

If you have any additional questions, please contact us at HC3@hhs.gov.

We want to know how satisfied you are with our products. Your answers will be anonymous, and we will use the responses to improve all our future updates, features, and new products. Share Your Feedback