HC3: Alert

January 11, 2022 TLP: White Report: 202201111700

Understanding and Mitigating Russian State-Sponsored Cyber Threats to U.S. Critical Infrastructure

Executive Summary

This Joint Cybersecurity Advisory - authored by the Cybersecurity and Infrastructure Security Agency (CISA), Federal Bureau of Investigation (FBI), and National Security Agency (NSA) - provides an overview of Russian state-sponsored cyber operations; commonly observed tactics, techniques, and procedures (TTPs); detection actions; incident response guidance; and mitigations. This overview is intended to help the cybersecurity community reduce the risk presented by these threats.

Report

Alert (AA22-011A) - Understanding and Mitigating Russian State-Sponsored Cyber Threats to U.S. Critical Infrastructure
https://www.cisa.gov/uscert/ncas/alerts/aa22-011a

Impact to HPH Sector

As Russia continues to act as a major cyber threat against the U.S. Healthcare and Public Health (HPH) Sector, it is extremely important to both know AND apply the information included in this Alert.

Reducing your organization's attack surface to the greatest extent possible is the primary goal, and this Alert provides many ways to do that. Notably:

- Ensure the listed vulnerabilities are patched.
- Use multi-factor authentication.
- Establish a robust data backup program.
- Consider signing up for CISA's cyber hygiene services.

References

Links to numerous 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