HC3: Alert

April 26, 2022 TLP: WHITE Report: 202204260900

Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure

Executive Summary

The cybersecurity authorities of the United States, Australia, Canada, New Zealand, and the United Kingdom are releasing this joint Cybersecurity Advisory (CSA). The intent of this joint CSA is to warn organizations that Russia's invasion of Ukraine could expose organizations both within and beyond the region to increased malicious cyber activity.

Report

Alert (AA22-110A) - Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure
https://www.cisa.gov/uscert/ncas/alerts/aa22-110a

Impact to HPH Sector

Evolving intelligence indicates that the Russian government is exploring options for potential cyberattacks. Additionally, some cybercrime groups have recently publicly pledged support for the Russian government. These Russian-aligned cybercrime groups have threatened to conduct cyber operations in retaliation for perceived cyber offensives against the Russian government or the Russian people. All critical infrastructure sectors are potentially impacted.

United States, Australian, Canadian, New Zealand, and United Kingdom cyber authorities urge critical infrastructure organizations to prepare for and mitigate potential cyber threats by immediately:

- Updating software, including operating systems, applications, and firmware, on IT network assets.
- Enforcing MFA to the greatest extent possible and require accounts with password logins, including service accounts, to have strong passwords.
- Securing and monitor them closely if you use RDP and/or other potentially risky services.
- Providing end-user awareness and training to help prevent successful targeted social engineering and spear phishing campaigns.

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. CISA also offers a range of no-cost cyber hygiene services to help organizations assess, identify, and reduce their exposure to threats. By requesting these services, organizations of any size could find ways to reduce their risk and mitigate attack vectors.

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