Health-ISAC and HC3 Joint Bulletin: Potential Malicious Cyber Attacks from Russia - Credible Threats to US Critical Infrastructure Sectors

Threat Bulletins | TLP:WHITE | Alert ID : b4e3eb9d | Mar 22, 2022, 09:17 AM

The U.S. Department of Health & Human Services Health Sector Cybersecurity Coordination Center (HC3) and Health-ISAC are releasing this document to raise awareness of the Russia and Ukraine tensions, credible threats to US critical infrastructure sectors (not specifically healthcare) and potential mitigations for Russian cyberattacks.

On March 21, 2022, the White House released “FACT SHEET: Act Now to Protect Against Potential Cyberattacks.” The Biden-Harris Administration has warned repeatedly about the potential for Russia to engage in malicious cyber activity against the United States in response to the unprecedented economic sanctions we have imposed. There is now evolving intelligence that Russia may be exploring options for potential cyberattacks.

On March 22, the Cybersecurity and Infrastructure Security Agency (CISA) is hosting a Broad Stakeholder Call to address impacts of the Russia-Ukraine situation on the Homeland. Health-ISAC and HC3 encourage members to attend, and we will also share meeting notes with members following the call.

Date/Time: Tuesday, March 22, 2022 from 2 to 3 PM (EDT)
PARTICIPANTS Dial-in Information: **800-857-6546** | *Passcode:* **2824553**

Additional Info

The Biden Administration has prioritized strengthening cybersecurity defenses to prepare the US for threats. President Biden's Executive Order is modernizing the Federal Government defenses and improving the security of widely used technology. The President has launched public-private action plans to shore up the cybersecurity of the electricity, pipeline, and water sectors and has directed Departments and Agencies to use all existing government authorities to mandate new cybersecurity and network defense measures. Internationally, the Administration brought together more than 30 allies and partners to cooperate to detect and disrupt ransomware threats, rallied G7 countries to hold accountable nations who harbor ransomware criminals, and took steps with partners and allies to publicly attribute malicious activity.

The Administration accelerated their work in November of last year as Russian President Vladimir Putin escalated his aggression ahead of his further invasion of Ukraine with extensive brie ngs and advisories to U.S. businesses regarding potential threats and cybersecurity protections. The U.S. Government will continue efforts to provide resources and tools to the private sector, including CISA's Shields-Up campaign, and will defend the Nation and respond to cyberattacks. But the reality is that much of the Nation's critical infrastructure is owned and operated by the private sector and the private sector must act to protect the critical services on which all Americans rely.

Recommendations

HC3 and Health-ISAC urge organizations to:

- Have Business Continuity Plans in place and ensure those plans consider cascading impacts due to failures in other sectors (interruptions in telecommunications, electricity, fuel delivery, water, etc.).
- Understand your threat surface – what are all the areas your IT network may be vulnerable to unauthorized users or attackers who could exploit vulnerabilities to gain access to systems and confidential data.
- Be sure system default passwords are changed; use MFA everywhere possible.
- Share incident and threat information to collectively protect the healthcare community. Health-ISAC Members can share securely through Health-ISAC's HTIP, WeeSecrets or by emailing the Health-ISAC Threat Operations Center (TOC) at TOC@h-isac.org. Organizations can share information with HC3 by emailing HC3@hhs.gov.

The Administration urges companies to execute the following steps with urgency:

- Mandate the use of multi-factor authentication on your systems to make it harder for attackers to get onto your system;
- Deploy modern security tools on your computers and devices to continuously look for and mitigate threats;

- Check with your cybersecurity professionals to make sure that your systems are patched and protected against all known vulnerabilities, and change passwords across your networks so that previously stolen credentials are useless to malicious actors;
- Back up your data and ensure you have offline backups beyond the reach of malicious actors;
- Run exercises and drill your emergency plans so that you are prepared to respond quickly to minimize the impact of any attack;
- Encrypt your data so it cannot be used if it is stolen;
- Educate your employees to common tactics that attackers will use over email or through websites, and encourage them to report if their computers or phones have shown unusual behavior, such as unusual crashes or operating very slowly; and
- Engage proactively with your local FBI field office or CISA Regional Office to establish relationships in advance of any cyber incidents. Please encourage your IT and Security leadership to visit the websites of CISA and the FBI where they will find technical information and other useful resources.

Sources

White House Fact Sheet: Act Now to Protect Against Potential Cyberattacks

More information about HC3 can be found

here: https://www.hhs.gov/about/agencies/asa/ocio/hc3/index.html

More information about Health-ISAC can be found here: https://h-isac.org/

Reference | References

HHS.gov
cisa
Health-ISAC

Tags

White House Administration, Russia, Cyberattacks

Linked Alert(s)

4afc7072

Share Threat Intel: For guidance on sharing indicators with Health-ISAC via CSAP, please visit the Knowledge Base article CSAP “Share Threat Intel” Documentation at the link address

provided here: https://health-isac.cyware.com/webapp/user/knowledge-base Additionally, this collaborative medium provides opportunities for attributed or anonymous sharing across ISACs and other cybersecurity related entities.

Access the Health-ISAC Intelligence Portal: Enhance your personalized information-sharing community with improved threat visibility, alert notifications, and incident sharing in a trusted environment delivered to you via email and mobile apps. Contact membership@h-isac.org for access to Cyware.

For Questions or Comments: Please email us at toc@h-isac.org