The PIOGA Press

April 2022 • Issue 144

Biden administration, CISA, FBI and NSA respond to cybersecurity threats to critical infrastructure posed by Russia

On March 21, President Biden issued a statement in response to evolving intelligence that Russia is exploring options for malicious cyberattacks against the United States. The statement highlights the measures taken by the administration to strengthen cyber defenses within the federal government and, to the extent that it has authority, within critical infrastructure sectors.

Additionally, President Biden called on private sector critical infrastructure owners and operators to accelerate and enhance their cybersecurity measures, urging them to take advantage of public-private partnerships and initiatives, including those administered by the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA). Appended to President Biden's statement was a Fact Sheet (www.whitehouse.gov/briefing-room/statements-releas- es/2022/03/21/fact-sheet-act-now-to-protect-against- potential-cyberattacks), which outlines specific steps that companies can take to bolster cybersecurity across the nation, and refers readers to various resources compiled by CISA, as part of a cybersecurity campaign. In November, the Biden administration began ramping up its cybersecurity and defense measures in response to Russian President Vladimir Putin's escalating aggression toward Ukraine. On January 11, CISA, the Federal Bureau of Investigation (FBI) and the National Security Agency (NSA) issued Alert AA22-011A, "Understanding and Mitigating Russian State-Sponsored Cyber Threats to U.S. Critical Infrastructure" (www.cisa.gov/uscert/ncas/alerts/aa22-011a) which provided an overview of Russian state-sponsored cyber operations; commonly observed tactics, techniques and procedures (TTPs); detection actions; incident response guidance; and mitigations. The administration, CISA, FBI and NSA continued to monitor the level of risk posed by Russia, which recently escalated based on intelligence indicating that Russia is planning cyberattacks against the United States in response to economic sanctions that the United States has imposed.

Authors:

Justine Kasznica

Ember Holmes

-

Babst Calland

What is Shields Up?

Shields Up is a cybersecurity campaign formed out of the combined efforts of CISA and the FBI to help organizations prepare for, respond to and mitigate the impact of cyberattacks by Russia. Although the campaign is focused on critical infrastructure, CISA has emphasized that all organizations, regardless of sector or size, must be prepared to defend against and respond to disruptive cyber incidents.

On March 22, CISA hosted an Unclassified Broad Stakeholder Call to brief attendees on the escalating threat of cybersecurity attacks by Russia.

Jen Easterly (Director of CISA), Matt Hartman (Deputy Executive Assistant Director of Cybersecurity of CISA) and Tonya Ugoretz (Deputy Assistant Director of the FBI Cyber Division) addressed attendees, focusing their comments on the Shields Up campaign and highlighting most important actions that organizations can take to prevent, detect and respond to possible cyberattacks. A condensed list of these actions includes:

1. Familiarize yourself with your networks and actively patrol systems, including informational and operational technology, for perceived threats or unexpected events (identified TTPs, malware signatures, etc.).
2. Regularly scan public-facing programs, systems and software for vulnerabilities.
3. Secure your systems and credentials by using complex passwords, two-factor authentication, encryption, patching, etc.
4. Maximize resilience to cyberattacks by strengthening security of operating systems, software and firmware, and by scheduling automatic updates of these systems.
5. Prepare a cyber incident response plan that includes FBI contact information for reporting, as well as contact information for an incident response firm and outside legal counsel.
6. Report any incidents immediately and maintain a low threshold for reporting.

In addition to the foregoing broad, categorical guidance and advice, the Shields Up website (www.cisa.gov/shields-up) has valuable resources to assist those in the private sector with the development and implementation of enhanced security measures. These resources include technical guidance, a catalog of known exploited vulnerabilities, a catalog of free cybersecurity services and tools provided by the federal government, a catalog of free cyber hygiene services, a ransomware guide, and many other preparedness and response resources.