INTELLIGENCE INSIGHTS

EXPERT INSIGHTS ON NATIONAL SECURITY DEVELOPMENTS

FEBRUARY 2020

Amidst Reports of Rising Cyber Threats from State Actors, U.S. Private Sector Can Take Protective Measures

PRESENTED BY INSA'S CYBER COUNCIL

CYBER COUNCIL

In response to the increased risk of nation-state sponsored cyberattacks on the U.S. private sector, INSA's Cyber Council has consolidated key guidance to help organizations strengthen their cyber defenses.

On January 6, 2020, the Cybersecurity and Infrastructure Security Agency (CISA), the Department of Homeland Security's cybersecurity arm, posted Alert AA20-006A, "Potential for Iranian Cyber Response to U.S. Military Strike in Baghdad,"[1] which serves as a reminder of Iran's history of retaliatory cyber activities. The actions CISA recommends organizations take include:

- **Adopt a state of heightened awareness.** This includes minimizing coverage gaps in personnel availability, more consistently consuming relevant threat intelligence, and making sure emergency call trees are up to date.
- **Increase organizational vigilance.** Ensure security personnel are monitoring key internal security capabilities and that they know how to identify anomalous behavior.
- **Confirm reporting processes.** Ensure personnel know how and when to report an incident. The well-being of an organization's workforce and cyber infrastructure depends on awareness of threat activity.
- **Exercise organizational incident response plans.** Ensure personnel are familiar with the key steps they need to take during an incident. Do they have the accesses they need? Do they know the processes? Are your various data sources logging as expected?

RISK ASSESSMENT

U.S. companies have long been under significant risk of attack by foreign intelligence agencies or their proxies. This is particularly true for industries with highly sensitive data - such as the advanced technology, defense, legal and finance sectors - and for operators of U.S. critical infrastructure.

"Make no mistake, American companies are squarely in the cross-hairs of well-financed nation-state actors, who are routinely breaching private sector networks, stealing proprietary data, and compromising supply chains," National Counterintelligence and Security Center (NCSC) Director William Evanina said in a recent statement." The attacks are persistent, aggressive, and cost our nation jobs, economic advantage, and hundreds of billions of dollars."[2]

[1] *Cybersecurity and Infrastructure Security Agency, Alert AA20-006A, January 6, 2020. At https://www.us-cert.gov/ncas/alerts/aa20-006a.*

[2] *Bill Gertz, "National Counterintelligence and Security Center Warns of Foreign Hacking," Washington Times, January 9, 2019. At https://www.washingtontimes.com/news/2019/jan/9/foreign-hacker-threat-grows-for-private-sector/.*

Nation states targeting private companies, either directly or through proxies, include Russia, China, and North Korea, as well as Iran. Foreign state threats to the U.S. private sector will always exist, and to varying degrees the Iranian escalation represents a heightened threat environment for U.S. and allied interests. The targeting of individual businesses, universities or other organizations by malign actors with nation state resources presents a significant mismatch in cyberspace, whether the threat is Iran or another country.

In light of recent U.S. military activities in Iraq, U.S. public and private sector organizations face a heightened threat of offensive cyberattacks from Iran via its official offensive cyber organizations and paid proxies, sympathizers or supporters around the world. While Iranian hackers have attacked U.S. government entities and private companies since as far back as 2011, its tactics and techniques have become extremely advanced, and it is believed that many of Iran's cyberattacks are intended to lay the groundwork for denial of service and, potentially, kinetic attacks.

U.S. cybersecurity professionals have since been discussing the nature and likelihood of an event, and following the release of the CISA alert, Christopher Krebs, the director of CISA stated that "Iran has the capability and the tendency to launch destructive attacks."

RESOURCES FOR ACTION

Fortunately, government resources are available to help any organization protect and defend itself from nation-state-sponsored cyberattacks, including many that improve collective cyber defenses by fostering public-private collaboration.

National Counterintelligence and Security Center (NCSC)
"Know the Risk, Raise Your Shield"

In January 2020, the NCSC launched a new campaign to help better protect private industry from threats posed by nation-state actors. Its "Know the Risk, Raise Your Shield" campaign includes materials that explain how individual organizations can mitigate threats and raise awareness of the most common threats faced by the private sector. These include risks related to the corporate supply chain, spear-phishing e-mails, social media deception, foreign travel, and mobile devices. NCSC materials can be found at www.dni.gov/ncsc/knowtherisk/tools

DHS Cybersecurity and Infrastructure Security Agency (CISA)
National Cyber Awareness System

CISA offers a wide variety of information designed to inform businesses about cyber threats facing U.S. companies today, while also offering tips and advice about common security issues for non-technical computer users. CISA has posted its information at

www.us-cert.gov/ncas.

Intelligence and National Security Alliance (INSA)
INSA's Cyber Council combines the knowledge of industry, government, and academic experts to provide authoritative and influential insights regarding national security challenges in the cyber domain. Council members work to promote a greater understanding of the cyber threats, challenges, and opportunities that can be addressed effectively through public-private collaboration. Additional information can be found on the INSA website at www.insaonline.org/councils/cybersecurity.