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

BACKGROUND

This piece consolidates key information regarding cyber threats related to the death of Quds Force Commander, General Qasem Soleimani, and draws attention to resources organizations can use to enhance their cybersecurity. On January 6, 2020, the Cybersecurity and Infrastructure Security Agency (CISA), the Department of Homeland Security's cybersecurity arm, posted Alert AA20-006A entitled, "Potential for Iranian Cyber Response to U.S. Military Strike in Baghdad."[1]

The CISA alert serves as a reminder of Iran's history of retaliatory cyber activities and informs organizations in the U.S. private sector of actions they should be taking during this time of heightened tensions. Recommended actions include:

- adopting an elevated state of awareness
- increasing vigilance across the organization
- refreshing and confirming the internal reporting process
- reviewing or exercising incident response plans.

[1] *Cybersecurity and Infrastructure Security Agency, "Potential for Iranian Cyber Response to U.S. Military Strike in Baghdad," Alert AA20-006A, January 6, 2020. At https://www.us-cert.gov/ncas/alerts/aa20-006a.*

RISK ASSESSMENT

NATION-STATE CYBER THREATS TO THE PRIVATE SECTOR

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]

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.

IRANIAN CYBER THREATS TO THE PRIVATE SECTOR

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.

In a private report after the storming of the U.S. embassy in Iraq and the death of General Soleimani, cybersecurity researchers assessed that hackers supporting Iran's Islamic Revolutionary Guards Corps vandalized websites related to the cities of Minneapolis, Minnesota and Tulsa, Oklahoma, with images honoring General Suleimani.[3]

Even before the recent escalations in the wake of the killing of General Soleimani, Iran has been escalating the destructiveness and scope of its attack preparation for U.S. critical infrastructure targets. In November 2019, cyber threat intelligence researchers reported that the Iranian hacker group APT33 had begun activity focused on "manufacturers, suppliers, or maintainers of industrial control system equipment" which could result in dangerous attacks on U.S. critical infrastructure.[4]

[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/.*

[3] *Zolan Kanno-Youngs and Nicole Perlroth, "Iran's Military Response May Be 'Concluded,' but Cyberwarfare Threat Grows," New York Times, updated January 14, 2020. At https://www.nytimes.com/2020/01/08/us/politics/iran-attack-cyber.html.*

[4] *Andy Greenberg, "A Notorious Iranian Hacking Crew Is Targeting Industrial Control Systems," Wired, November 20, 2019. At https://www.wired.com/story/iran-apt33-industrial-control-systems/.*

Although not confirmed and not as dangerous as threats to IT networks associated with industrial control systems, hackers claiming to be associated with Iran defaced the website of the Federal Depository Library Program, a division of the U.S. Government Publishing Office, replacing it with pro-Iranian, anti-American messaging.[5]

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. You need to get in the head space that the next breach could be your last."[6]

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 https://www.dni.gov/index.php/ncsc-how-we-work/ncsc-know-the-risk-raise-your-shield/ncsc-awareness-materials.

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.

[5] *John Bacon, "US Government Website Hacked With Pro-Iranian Messages, Image of Bloodied Trump," USA Today, January 5, 2020. At https://www.usatoday.com/story/news/nation/2020/01/05/iran-hack-homeland-security-website-hacked-image-bloody-trump/2818308001/.*

[6] *Kanno-Youngs and Perlroth, January 14, 2020.*

INTELLIGENCE AND
NATIONAL SECURITY
ALLIANCE

ACKNOWLEDGEMENTS

INSA expresses its appreciation to the INSA members and staff who contributed their time, expertise, and resources to this piece.

INSA MEMBERS

Andrew Borene, JD, CISSP,
President & CEO, Cipherloc Corporation

Jim Keffer, *Chair, INSA Cyber Council*

Scott Lawler, CISSP-ISSAP, ISSMP,
Chairman & CEO, LP3

Jason Swope, *INSA Cyber Council*

INSA STAFF

Suzanne Wilson Heckenberg, *President*

Larry Hanauer, *Vice President of Policy*

ABOUT INSA

The Intelligence and National Security Alliance (INSA) is a nonpartisan, nonprofit forum for advancing intelligence and national security priorities through public-private partnerships. INSA's government and private sector members collaborate to make government more effective and efficient through the application of industry expertise and commercial best practices. INSA's 160+ member organizations are leaders in intelligence collection and analysis, data analytics, management consulting, technology development, cybersecurity, homeland security, and national security law, and its 4,000 individual and associate members include leaders, senior executives, and intelligence experts in government, industry, and academia.