CISA INSIGHTS

DEFEND TODAY, SECURE TOMORROW

July 19, 2021

Chinese Cyber Threat Overview and Actions for Leaders

The Cybersecurity and Infrastructure Security Agency (CISA), National Security Agency (NSA), and Federal Bureau of Investigation (FBI) assess that the People's Republic of China (PRC) leverages cyber operations to assert its political and economic development objectives. Chinese state-sponsored cyber actors aggressively target U.S. and Allied political, economic, military, educational, and critical infrastructure (CI) personnel and organizations to steal sensitive data, emerging and key technology, intellectual property, and personally identifiable information (PII).

This joint analysis provides a summary of the Chinese state-sponsored cyber threat to the U.S. Federal Government; state, local, tribal, and territorial (SLTT) governments; CI organizations; and private industry and provides recommendations for organization leadership to reduce the risk of cyber espionage and data theft.

CHINESE MALICIOUS CYBER ACTIVITY

In 2021, the U.S. Intelligence Community assessed that the PRC presents a prolific and effective cyber-espionage threat, possesses substantial cyberattack capabilities, and presents a growing influence threat. The PRC's cyber-espionage operations have included compromising telecommunications firms, providers of managed services and broadly used software, and other targets potentially rich in follow-on opportunities for intelligence collection, attack, or influence operations.

The PRC's cyber-espionage operations and coordinated theft of information and technology places U.S. government, CI, and private industry organizations at risk of loss of sensitive data and technology, trade secrets, intellectual property, and PII. CISA, NSA, and FBI have observed increasingly sophisticated Chinese state-sponsored cyber activity targeting political, economic, military, educational, and CI personnel and organizations. Target sectors include managed service providers, semiconductor companies, the Defense Industrial Base (DIB), universities, and medical institutions. During the past several years, the Department of Justice has charged, indicted, or sentenced PRC-affiliated cyber actors with computer intrusion campaigns targeting multiple CI and private sector organizations. Some of these actors attempted to obtain and transfer sensitive U.S. software and technology to China.

ACTIONS FOR LEADERS

Leaders of organizations should:

1. **Drive a culture of cybersecurity investment and strategy.** As a leader committed to the cybersecurity of your organization, ensure your company follows best practices for cybersecurity including employing multi-factor authentication (MFA) and keeping software up to date. Refer to CISA Cyber Essentials Starter Kit: The Basics for Building a Culture of Cyber Readiness and NSA's Top 10 Mitigation Strategies for best practices.
2. **Ensure your organization has incident response plans**. Ensure personnel are familiar with the key steps they need to take during an incident, have the accesses they need, and are positioned to act in a calm and unified manner. 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. Join other industry leaders and report incidents to help serve as part of CISA's early warning system (see the Contact Information below). For guidance on responding to an incident, refer to Joint Cybersecurity Advisory AA20-245A: Technical Approaches to Uncovering and Remediating Malicious Activity.

3. **Stay informed about Chinese malicious cyber activity.** Ensure security personnel monitor key internal security capabilities and can identify anomalous behavior. Flag any known Chinese state-sponsored indicators of compromise (IOCs) and tactics, techniques, and procedures (TTPs) for immediate response. Use technical resources on Chinese malicious activity, such as us-cert.cisa.gov/china and nsa.gov/What-We-Do/Cybersecurity/Advisories-Technical-Guidance, to help ensure your security personnel possess the information to identify and report malicious cyber activity.

CONTACT INFORMATION

To report suspicious or criminal activity related to information in this CISA Insights, contact your local FBI field office at fbi.gov/contact-us/field-offices, or the FBI's 24/7 Cyber Watch (CyWatch) at (855)292-3937 or by email at CyWatch@fbi.gov. When available, please include the following information regarding the incident: date, time, and location of the incident; type of activity; number of people affected; type of equipment used for the activity; the name of the submitting company or organization; and a designated point of contact. To request incident response resources or technical assistance related to these threats, contact CISA at Central@cisa.gov.