JOINT ADVISORIES

CISA, NSA, and FBI published a Joint Cybersecurity Advisory (CSA) to detail various Chinese state- sponsored cyber techniques used to target U.S. and Allied networks. This advisory, "Chinese State-Sponsored Cyber Operations: Observed TTPs", is a deep dive into the techniques used when targeting U.S. and Allied networks.

CISA and FBI published a Joint Cybersecurity Advisory on a Chinese Advanced Persistent Threat (APT) group known in open-source reporting as APT40. This advisory provides APT40's tactics, techniques, and procedures (TTPs) and indicators of compromise (IOCs) to help cybersecurity practitioners identify and remediate APT40 intrusions and established footholds. This accompanies action by the U.S. Department of Justice (DOJ) today with unsealing indictments against four APT40 cyber actors for their illicit computer network exploitation (CNE) activities via front company Hainan Xiandun Technology Development Company (Hainan Xiandun).

"CISA Insights: Chinese Cyber Threat Overview for Leaders" is a joint analysis from CISA, FBI, and NSA that provides recommendations to organizational public and private sector leadership to reduce the risk of cyber espionage and data theft from Chinese state-sponsored cyber actors. 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).

CISA also encourages users and administrators to review the blog post, Safeguarding Critical Infrastructure against Threats from the People's Republic of China, by CISA Executive Assistant Director Eric Goldstein and the China Cyber Threat Overview and Advisories webpage.