INFORMATIONAL

Indictment and Several Advisories Detailing Chinese Cyber Threat Activity

TLP:WHITE

Jul 19, 2021

On July 19, the Cybersecurity and Infrastructure Security Agency (CISA) has uploaded the Current Activity regarding the release of an indictment and several advisories detailing Chinese cyber threat activity.

CISA, the Federal Bureau of Investigation (FBI), and the National Security Agency (NSA) have observed increasingly sophisticated Chinese state-sponsored activity targeting U.S. political, economic, military, educational, and critical infrastructure personnel and organizations.

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.

The White House has released a statement attributing recent Microsoft Exchange server exploitation activity to the People's Republic of China (PRC).

The Department of Justice has indicted four Chinese cyber actors from the advanced persistent threat (APT) group APT40 for malicious cyber activities, carried out on orders from PRC Ministry of State Security (MSS) Hainan State Security Department (HSSD). These activities resulted in the theft of trade secrets, intellectual property, and other high-value information from companies and organizations in the United States and abroad, as well as from multiple foreign governments.

CISA and FBI have released Joint Cybersecurity Advisory: TTPs of Indicted APT40 Actors Associated with China's MSS Hainan State Security Department to help network defenders identify and remediate APT40 intrusions and established footholds.

CISA, NSA and FBI have released Joint Cybersecurity Advisory: Chinese Observed TTPs, which describes Chinese cyber threat behavior and trends and provides mitigations to help protect the Federal Government; state, local, tribal, and territorial governments; critical infrastructure, defense industrial base, and private industry organizations.

CISA, NSA and FBI have released CISA Insights: Chinese Cyber Threat Overview for Leaders to help leaders understand this threat and how to reduce their organization's risk of falling victim to cyber espionage and data theft.

Reference(s)	cisa, whitehouse, cisa, US Department of Justice, cisa, cisa, cisa, cisa, cisa

Release Date
Jul 19, 2021

Sources
https://us-cert.cisa.gov/ncas/current-activity/2021/07/19/us-government-releases-indictment-and-several-advisories-detailing
https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/19/the-united-states-joined-by-allies-and-partners-attributes-malicious-cyber-activity-and-irresponsible-state-behavior-to-the-peoples-republic-of-china/
https://us-cert.cisa.gov/ncas/alerts/aa21-062a
https://www.justice.gov/opa/pr/four-chinese-nationals-working-ministry-state-security-charged-global-computer-intrusion

https://us-cert.cisa.gov/ncas/alerts/aa21-200a
https://us-cert.cisa.gov/ncas/alerts/aa21-200b
https://www.cisa.gov/publication/chinese-cyber-threat-overview-and-actions-leaders
https://www.cisa.gov/blog/2021/07/19/safeguarding-critical-infrastructure-against-threats-peoples-republic-china
https://us-cert.cisa.gov/china

Alert ID 5909417e

View Alert

Tags PRC, NSA, CISA, FBI, China

TLP:WHITE Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

For Questions or Comments Please email us at toc@h-isac.org

Download Health-ISAC's Information Sharing App. 

For more update and alerts, visit: **https://health-isac.cyware.com**