TLP: WHITE
MS-ISAC CYBERSECURITY ALERT

TO: All MS-ISAC Members, EI-ISAC Members, and Partners

DATE ISSUED: December 20, 2018

SUBJECT: U.S. Government Announcement on Chinese Malicious Cyber Activity

Sent on behalf of the U.S. Department of Homeland Security (DHS). Recipients are encouraged to broadly share this information within the state, local, tribal, and territorial (SLTT) government community.

Today the U.S. Government announced that a group of Chinese cyber actors associated with the Chinese Ministry of State Security has carried out a campaign of cyber-enabled theft targeting global technology service providers and their customers. Over the past four years, these actors have gained access to multiple U.S. and global managed-service and cloud providers and their customers in an effort to steal the intellectual property and sensitive data of companies located in at least 12 countries. The U.S. Government is taking steps to hold the Chinese government accountable for these unacceptable actions and help victim organizations secure their networks and data.

In 2017, the Cybersecurity and Infrastructure Security Agency (CISA) within the Department of Homeland Security (DHS) issued a Technical Alert (TA17-117) that described an emerging, sophisticated campaign using multiple malware implants. Among other services, CISA provided mitigation techniques, including recommending monitoring activity of domains and IP addresses listed in the technical alert, as well as scanning for evidence of the file hashes as potential indicators of infection.

In the coming weeks, CISA will provide additional support and mitigation tips to assist service providers in securing their infrastructure and help end-customers understand and manage risks associated with outsourced services. In the meantime, organizations and the public should visit the US-CERT website for information and resources regarding this malicious activity: https://www.us-cert.gov/China.

We encourage any questions or feedback related to this activity. Related activity can be reported to CISA NCCIC at NCCICcustomerservice@hq.dhs.gov or 888-282-0870 and the FBI Cyber Watch (CyWatch) at CyWatch@fbi.gov or 855-292-3937.

24×7 Security Operations Center
Multi-State Information Sharing and Analysis Center (MS-ISAC)
Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC)
31 Tech Valley Drive
East Greenbush, NY 12061
SOC@cisecurity.org - 1-866-787-4722

MS-ISAC® Multi-State Information Sharing & Analysis Center®
Elections Infrastructure ISAC