TLP:WHITE

TLP:WHITE

Information For

- Control System Users

  Information for industrial control systems owners, operators, and vendors.

- Government Users

  Resources for information sharing and collaboration among government agencies.

- Home and Business

  Information for system administrators and technical users about latest threats.

Chinese Malicious Cyber Activity

The information contained on this page is the result of analytic efforts of the Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) to provide technical details on the tactics, techniques, and procedures used by Chinese government cyber threat actors. These threat actors are actively exploiting trust relationships between information technology (IT) service providers—such as managed service providers and cloud service providers—and their customers. The intent of sharing this information is to enable network defenders to identify and reduce exposure to Chinese malicious cyber activity. However, mitigation for this activity can be complex and there is no single solution that will fully alleviate all aspects of the threat actor activity.

At this time, all known victims of this activity have been notified by CISA and/or the Federal Bureau of Investigation (FBI). However, because there may be additional victims not yet identified, CISA recommends all IT service providers and their customers follow the recommendations, tools, and actions described in this page and in Alerts TA17-117A and TA18-276A, referenced below. Organizations and individuals that determine their risk to be elevated—either because they are in one of the targeted sectors, or because unusual activity is detected—should conduct a dedicated investigation to identify if any of this malicious activity is in their networks.

For more information on Chinese malicious cyber activity, see:

- April 27, 2017: Alert (TA17-117A) – Intrusions Affecting Multiple Victims Across Multiple Sectors

Guidance for IT Service Provider Customers

- Organizations that rely on IT service providers should ensure their providers have conducted a review to determine if there is a security concern or compromise, and have implemented appropriate mitigation and detection tools for this cyber activity.
- IT service provider customers should also
  - Review and verify all connections between customer systems, service provider systems, and other client enclaves;
  - Verify service provider accounts in their environment are being used for appropriate purposes and are disabled when not actively being used;
  - Ensure contractual relationships with all service providers implement
    - Security controls as deemed appropriate by the client,
    - Appropriate monitoring and logging of client systems provided by the service provider,
    - Appropriate monitoring of service provider's presence, activities, and connections to the customer network, and
    - Notification of confirmed or suspected security events and incidents occurring on the provider's infrastructure and administrative networks.
  - Integrate system log files—and network monitoring data from IT service provider infrastructure and systems—into customer intrusion detection and security monitoring systems for independent correlation, aggregation and detection.
- IT service provider customers should consult the APTs Targeting IT Service Provider Customers site page that includes the following tools and alerts:
  - Tools To Detect Network Intrusions and Identify Compromised Systems
    - Sogu File Search Tool
    - Australian Cyber Security Center Sysmon and Windows Management Instrumentation Tools
  - October 3, 2018: Alert (TA18-276B) - Advanced Persistent Threat Activity Exploiting Managed Service Providers
  - October 3, 2018: Alert (TA18-276A) - Using Rigorous Credential Control to Mitigate Trusted Network Exploitation

Guidance for IT Service Providers

- Providers should fully implement the mitigation actions available on the APTs Targeting IT Service Provider Customers site page to protect against this malicious activity.
- Providers should implement the following specific actions:
  - Apply the principle of least privilege to their environment, which means customer data sets are separated logically, and access to client networks is not shared;
  - Implement robust network and host-based monitoring solutions that looks for known malicious activity and anomalous behavior on the infrastructure and systems providing client services;
  - Ensure that log information is aggregated and correlated to enable maximum detection capabilities, with a focus on monitoring for account misuse; and
  - Work with their customers to ensure hosted infrastructure is monitored and maintained, either by the service provider or the client.

- Providers may consult the following private industry report:
    - Operation Cloud Hopper - CISA does not endorse any commercial products or services identified in this report. Any hyperlinked websites do not constitute endorsement by CISA of the website or the information, products, or services contained therein.

Additional DHS Partner Resources

- December 20, 2018
    - U.S. Department of Justice: Deputy Attorney General Rod J. Rosenstein Announces Charges Against Chinese Hackers
    - Canadian Centre for Cyber Security: Malicious Cyber Activity Targeting Information Technology Managed Service Providers
    - Australian Minister for Foreign Affairs: Attribution of Chinese cyber-enabled commercial intellectual property theft
    - United Kingdom government: UK and allies reveal global scale of Chinese cyber campaign
    - New Zealand National Cyber Security Centre: Cyber campaign attributed to China