

## China Cyber Threat Overview and Advisories

This page provides an overview of the Cybersecurity and Infrastructure Security Agency's (CISA's) assessment of the Chinese government's malicious cyber activities. The overview leverages publicly available, open-source intelligence and information regarding this threat. This page also includes [a complete list of related CISA publications](#), many of which are jointly authored with other U.S. government agencies (Note: unless specifically stated, neither CISA nor the U.S. Government attributed specific activity described in the referenced sources to Chinese government actors). Additionally, this page provides instructions on how to [report related threat activity](#).



The Chinese government—officially known as the People's Republic of China (PRC)—engages in malicious cyber activities to pursue its national interests. Malicious cyber activities attributed to the Chinese government targeted, and continue to target, a variety of industries and organizations in the United States, including healthcare, financial services, defense industrial base, energy, government facilities, chemical, critical manufacturing (including automotive and aerospace), communications, IT (including managed service providers), international trade, education, video gaming, faith-based organizations, and law firms. Additionally, Advisories published by CISA and other unclassified sources reveal that China is conducting operations worldwide to steal intellectual property and sensitive data from critical infrastructure organizations, including organizations involved in healthcare, pharmaceutical, and research sectors working on COVID-19 response.

According to the U.S. Office of the Director of National Intelligence 2021 Annual Threat Assessment, "China presents a prolific and effective cyber-espionage threat, possesses substantial cyber-attack capabilities, and presents a growing influence threat." The Assessment states that "China can launch cyber attacks that, at a minimum, can cause localized, temporary disruptions to critical infrastructure within the United States." Additionally, the Assessment states that "China'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."<sup>[1]</sup>

### Latest U.S. Government Report on Chinese Malicious Cyber Activity

On July 20, 2021, the U.S. Government attributed recent activity targeting industrial control systems to the PRC. CISA and FBI have released [Joint Cybersecurity Advisory: Chinese Gas Pipeline Intrusion Campaign, 2011 to 2013](#) to raise awareness of the risks to and improve the cyber protection of critical infrastructure.

On July 19, 2021, the [White House released a statement](#) attributing recent [Microsoft Exchange server exploitation activity](#) to the PRC and [the Department of Justice 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. Following up on the White House announcement, CISA Executive Assistant Director Eric Goldstein released a blog post, [Safeguarding Critical Infrastructure against Threats from the People's Republic of China](#). Additionally, CISA, the National Security Agency (NSA), and Federal Bureau of Investigation (FBI) released the following Joint Cybersecurity Advisories and CISA Insights:

- CISA and FBI [Joint Cybersecurity Advisory: TTPs of Indicted APT40 Actors Associated with China's MSS Hainan State Security Department](#): Helps network defenders identify and remediate APT40 intrusions and established footholds.
- CISA, NSA, and FBI [Joint Cybersecurity Advisory: Chinese Observed TTPs](#): 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 [CISA Insights: Chinese Cyber Threat Overview for Leaders](#): Helps leaders understand this threat and how to reduce their organization's risk of falling victim to cyber espionage and data theft.

The [Chinese Malicious Cyber Activity](#) section below lists all CISA Advisories, Alerts, and Malware Analysis Reports (MARs) on Chinese malicious cyber activities.

[Expand All Sections](#)

#### Chinese Malicious Cyber Activity

Much of the information contained in the Advisories, Alerts, and MARs listed below is the result of analytic efforts between CISA, the U.S. Department of Defense (DoD), and the Federal Bureau of Investigation (FBI) to provide technical details on the tools and infrastructure used by Chinese state-sponsored cyber actors. The publications below include descriptions of Chinese malicious cyber activity, technical details, and recommended mitigations. Users and administrators should flag activity associated with the information in the products listed in table 1 below, report the activity to [CISA](#) or [FBI Cyber Watch \(CyWatch\)](#)<sup>Ⓘ</sup>, and give the activity the highest priority for enhanced mitigation.

Table 1: CISA and Joint CISA Publications

Publication Date	Title	Description
July 20, 2021	<ul style="list-style-type: none"><li><a href="#">Joint Cybersecurity Advisory: Chinese Gas Pipeline Intrusion Campaign, 2011 to 2013</a></li></ul>	CISA and FBI released an advisory providing information on a spearphishing and intrusion campaign conducted by state-sponsored Chinese actors that occurred from December 2011 to 2013, targeting U.S. oil and natural gas (ONG) pipeline companies.
July 19, 2021	<ul style="list-style-type: none"><li><a href="#">Joint Cybersecurity Advisory: TTPs of Indicted APT40 Actors Associated with China's MSS Hainan State Security Department</a></li></ul>	CISA and FBI released an advisory to help network defenders identify and remediate APT40 intrusions and established footholds. See the July 19, 2021, <a href="#">Department of Justice press release</a> .
July 19, 2021	<ul style="list-style-type: none"><li><a href="#">Joint Cybersecurity Advisory: Chinese Observed TTPs</a></li></ul>	CISA, NSA, and FBI released an advisory describing 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.
July 19, 2021	<ul style="list-style-type: none"><li><a href="#">Joint CISA Insights: Chinese Cyber Threat Overview for Leaders</a></li></ul>	CISA, NSA, and FBI released a joint CISA Insights to help leaders understand this threat and how to reduce their organization's risk of falling victim to cyber espionage and data theft.
March 03, 2021	<ul style="list-style-type: none"><li><a href="#">CISA Alert: Mitigate Microsoft Exchange Server Vulnerabilities</a></li></ul>	CISA partners observed active exploitation of vulnerabilities in Microsoft Exchange Server products. This Alert includes tactics, techniques, and procedures and indicators of compromise associated with this activity. See the July 19, 2021 <a href="#">White House Statement</a> .
October 1, 2020	<ul style="list-style-type: none"><li><a href="#">CISA Alert: Potential for China Cyber Response to Heightened U.S.-China Tensions</a></li></ul>	In light of heightened tensions between the United States and China, CISA released an Alert providing specific Chinese government and affiliated cyber threat actor tactics, techniques, and procedures (TTPs). The Alert also includes recommended mitigations to the cybersecurity community to assist in the protection of our Nation's critical infrastructure.
September 14, 2020	<ul style="list-style-type: none"><li><a href="#">Joint Cybersecurity Advisory: Chinese Ministry of State Security-Affiliated Cyber Threat Actor Activity</a></li></ul>	CISA has consistently observed Chinese Ministry of State (MSS)-affiliated cyber threat actors using publicly available information sources and common, well-known TTPs to target U.S. government agencies. This advisory identifies some of the more common TTPs employed by cyber threat actors, including those affiliated with the Chinese MSS.
August 3, 2020	<ul style="list-style-type: none"><li><a href="#">MAR-10292089-1.v2 – Chinese Remote Access Trojan: TAIDQOR</a></li></ul>	CISA, FBI, and DoD released a MAR describing Chinese government actors using malware variants in conjunction with proxy servers to maintain a presence on victim networks and to further network exploitation.
May 13, 2020	<ul style="list-style-type: none"><li><a href="#">CISA and FBI Joint Public Service Announcement: People's Republic of China (PRC) Targeting of COVID-19 Research Organizations</a></li></ul>	CISA and FBI issued a Public Service Announcement warning healthcare, pharmaceutical, and research sectors working on the COVID-19 response of likely targeting and attempted network compromise by the PRC.
February 2019	<ul style="list-style-type: none"><li><a href="#">CISA Webinar: Chinese Cyber Activity Targeting Managed Service Providers</a><sup>Ⓙ</sup></li><li><a href="#">CISA Webinar Slide Deck: Chinese Cyber Activity Targeting Managed Service Providers</a></li></ul>	CISA provided a Webinar on Chinese state-sponsored cyber actors targeting managed service providers (MSPs) and their customers. This campaign is referred to as CLOUD HOPPER.
October 3, 2018	<ul style="list-style-type: none"><li><a href="#">CISA Alert: Advanced Persistent Threat Activity Exploiting Managed Service Providers</a></li><li><a href="#">CISA Alert: Using Rigorous Credential Control to Mitigate Trusted Network Exploitation</a></li></ul>	These Alerts address the CLOUD HOPPER Campaign. Since May 2016, APT actors have used various TTPs to attempt to infiltrate the networks of global MSPs for the purposes of cyber espionage and intellectual property theft. APT actors have targeted victims in several U.S. critical infrastructure sectors, including IT, Energy, Healthcare and Public Health, Communications, and Critical Manufacturing.
April 27, 2017	<ul style="list-style-type: none"><li><a href="#">CISA Alert: Intrusions Affecting Multiple Victims Across Multiple Sectors</a></li></ul>	This Alert provides information on a campaign in which Chinese government cyber threat actors exploited trust relationships between IT service providers—such as MSPs and cloud service providers—and their customers. Chinese cyber actors associated with the Chinese MSS carried out a campaign of cyber-enabled theft targeting global technology service providers and their customers. The actors gained access to multiple U.S. and global IT service providers and their customers in an effort to steal the intellectual property and sensitive data of companies located in at least 12 countries.

[Report Activity Related to This Threat](#)



[Mitigate and Detect This Threat](#)







[Respond to an Incident](#)



[References](#)



#### Contact Us

-  (888)282-0870
-  Send us email <sup>Ⓚ</sup>
-  Download PGP/GPG keys
-  Submit website feedback

#### Subscribe to Alerts

Receive security alerts, tips, and other updates.

Enter your email address

Sign Up

HSIN



[Report](#)