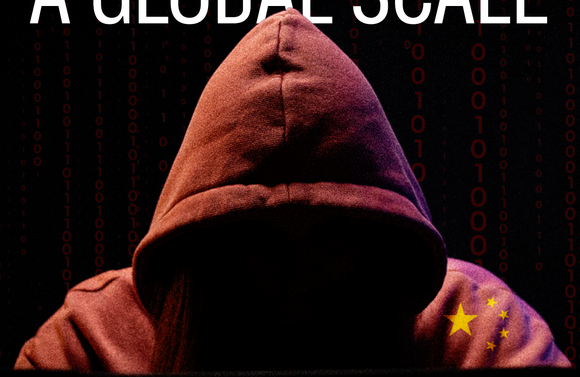
CCP HACKERS

CYBERWARFARE ON A GLOBAL SCALE



The Chinese regime runs the largest network of hackers in the world, and the United States is its most prominent target

China is the most prolific cybersecurity threat in the world, with nearly 200 hacker groups catalogued by various cybersecurity firms. The Chinese Communist Party (CCP) uses hacking not just for espionage, but also as a part of its broader agenda of unrestricted warfare. State-sponsored Chinese hackers target specific industries to steal the intellectual property of foreign companies on a mass scale. The information is then provided to Chinese companies and research establishments, siphoning hundreds of billions in value from the U.S. economy. The CCP also uses hackers to spy on and harass overseas critics and dissidents, including media and lawmakers. CCP cyberattacks have targeted critical infrastructure in the United States and around the world, possibly preparing to cripple life-sustaining services in the case of an open conflict. With the repeated hacking of U.S. government agencies, health insurance providers, and telecommunications companies, the CCP has been able to collect vast troves of Americans' personal data. The regime may be, quite literally, keeping tabs on every American.

HOW HACKERS GAIN ACCESS

Zero-Day Vulnerability

A weak spot in system code that can be exploited for unauthorized use of the system. "Zero-day" means the vendor or developer has just discovered the flaw and hasn't had time yet to fix it. Some Chinese hacker groups have been known to use multiple zero-day vulnerabilities.

Known Vulnerability

A weak spot in system code that can be exploited for unauthorized use of the system. "Known" means the flaw is known in the cybersecurity community and typically has already been patched; however, it can still be exploited on unpatched systems. Especially in large networks, it can be difficult to keep all computers and systems patched all the time. CCP hackers have been extremely successful in exploiting known vulnerabilities, taking advantage of lax security maintenance. One often-used tactic is to target a vulnerability right after it has been discovered and publicly disclosed, with the aim of exploiting it before a patch is broadly adopted.

Managed Service Provider

A managed service provider (MSP) is a company that manages computer networks and services for other companies. Some Chinese hacker groups have been known to target MSPs, using them as a bridge to compromise the computer networks of the MSPs' clients.

Spear Phishing

An attempt to trick an individual into installing malicious code on his computer. It often uses emails with attachments or hyperlinks that, if clicked on, install the malicious code. Compared to regular phishing, which is often sent to a broad audience and is usually easy to recognize, spear phishing is tailored to specific targets. An employee, for example, may receive an email that looks like it was sent by his manager or his company's HR department, asking him to click on a link or open an attachment to complete a work-related task. Spear phishing emails have also been disguised as invitations to seminars, conferences, retreats, and other events

commonly advertised to the targeted individuals. Sometimes, hackers set up innocuous-looking but infected fake websites, to which the phishing emails then link. Chinese hacker groups have been known to gather intelligence on their targets in order to craft convincing phishing emails.

Watering Hole

An indirect attack that compromises a website likely to be used by the intended target. An individual with access to the targeted system may, for example, frequent a particular online forum. Hackers would then target the forum's website and infect it with malicious code, waiting for the target to access it. Some Chinese hacker groups have been known to use this method, especially more recently, as victims have been getting more adept at spotting phishing scams.

Notable Hacker Groups

1 PLA UNIT 61398
AKA APT1

Active since at least 2002

Likely based in Pudong, Shanghai

Sometimes called the Comment Crew because of its technique of hiding communication with compromised systems in HTML comments—snippets of text inserted in website code, often as explanatory notes. In 2014, the Department of Justice (DOJ) indicted five officers from the unit on hacking charges.

SIGNATURE ACCESS METHOD: Highly personalized spear phishing, watering hole.

TARGETS: Governments, defense, shipping, aeronautics, energy, manufacturing, engineering, electronics, financial, and software industries.

PROMINENT PAST TARGETS: Lockheed Martin.

2 PLA UNIT 61486
AKA APT2

Active since at least 2007.

Likely based in Zhabei, Shanghai.

Known to send out fake conference invitations and job offerings.

SIGNATURE ACCESS METHOD: Spear phishing.

TARGETS: Space, aerospace, and satellite industries.

PROMINENT PAST TARGETS: Canada's National Research Council.

3 BUCKEYE
AKA APT3

Active since at least 2007.

Allegedly based at Guangzhou Bo Yu Information Technology Co.

In 2017, the DOJ indicted three members on hacking charges.

SIGNATURE ACCESS METHOD: Phishing, spear phishing.

TARGETS: Defense, telecom, transportation, and advanced technology companies; since about 2015, Hong Kong political figures.

PROMINENT PAST TARGETS: Siemens, Moody's Analytics.

4 SALMON TYPHOON
AKA APT4

Active since at least 2007.

Usually described as "China-affiliated" or "state-sponsored." In 2024, Microsoft and OpenAI disclosed that the group was using their AI services for research, translation, and possible target reconnaissance.

SIGNATURE ACCESS METHOD: Spear phishing.

TARGETS: U.S. defense contractors, government agencies, aerospace, telecom, and hardware and Technology Development Co. in Tianjin and acting in association with the Chinese Ministry of State Security's Tianjin State Security Bureau.

PROMINENT PAST TARGETS: Smart card system used by the Department of Defense and other agencies.

5 RED APOLLO
AKA APT10

Active since at least 2006.

Likely based in Tianjin.

In 2018, the DOJ indicted two members working for Huaying Haitai Science

SIGNATURE ACCESS METHOD: Spear phishing targeting MSPs.

TARGETS: Commercial and defense technology companies, MSPs, and government agencies.

PROMINENT PAST TARGETS: U.S. Navy.

6 NUMBERED PANDA
AKA APT12

Active since at least 2009.

Likely affiliated with the PLA.

SIGNATURE ACCESS METHOD: Spear phishing.

TARGETS: Companies, governments, and individuals mostly in East Asia, particularly Taiwan and Japan.

PROMINENT PAST TARGETS: The New York Times.

7 DEPUTYDOG
AKA APT17

Active since at least 2009.

Likely a contractor of the Jinan bureau of the Chinese Ministry of State Security.

SIGNATURE ACCESS METHOD: Spear phishing.

TARGETS: U.S. government, defense industry, IT companies, mining companies, nongovernmental organizations, law firms.

PROMINENT PAST TARGETS: Google, Northrop Grumman, Amnesty International.

8 DYNAMITE PANDA
AKA APT18

Active since at least 2009.

Likely part of the PLA Navy.

SIGNATURE ACCESS METHOD: Spear phishing using recently discovered vulnerabilities.

TARGETS: Health care, defense, high tech, aerospace, and telecom companies.

PROMINENT PAST TARGETS: Community Health Systems.

9 CODOSO TEAM
AKA APT19

Active since at least 2013.

Likely freelancers working for the Chinese regime.

SIGNATURE ACCESS METHOD: Spear phishing, watering hole.

TARGETS: U.S. government, health care, defense, finance, law, energy, pharmaceutical, telecom, high tech, education, and manufacturing companies.

PROMINENT PAST TARGETS: U.S. Office of Personnel Management, Anthem, Premera Blue Cross, CareFirst Blue Cross.

Notable Hacker Groups

10 TURBINE PANDA
AKA APT26

Active since at least 2010.

Likely part of the Jiangsu branch of the Ministry of State Security.

In 2018, the DOJ indicted several Chinese intelligence officers from the Jiangsu branch for hacking an aerospace company developing turbofan engines for commercial airliners. In 2012, APT26 hacked the Council on Foreign Relations website to use as a watering hole.

SIGNATURE ACCESS METHOD: Watering hole.

TARGETS: Aerospace, aviation, government, think-tanks, nonprofits, health care, defense, energy, agriculture.

PROMINENT PAST TARGETS: Capstone Turbine Corp.

11 ZIRKONIUM
AKA APT31

Active since at least 2016.

Known to target air-gapped—physically or logically separated—systems through malware spread via USB devices. In 2024, the U.S. Treasury linked the group to Wuhan Xiaoruizhi Science and Technology Co. and sanctioned it as a front for the Chinese Ministry of State Security's hacking campaign targeting U.S. officials and critical infrastructure, including defense contractors and an energy company.

SIGNATURE ACCESS METHOD: Phishing links that download malware from GitHub.

TARGETS: U.S. and European governments, defense and energy companies.

PROMINENT PAST TARGETS: President Joe Biden's 2020 campaign; governments of Norway, Finland, and Czech Republic.

12 DOUBLE DRAGON
AKA APT41

Active since at least 2012.

A group of hackers who seem to be freelancers conducting their activities partly for the Chinese regime and partly for direct financial gain. In 2020, the DOJ indicted seven members for allegedly targeting more than 100 victims around the world.

SIGNATURE ACCESS METHOD: Compromising web applications, supply chain attacks, spear phishing impersonating tax agencies.

TARGETS: Governments, universities, nonprofits, think tanks, and telecom, video game, hardware, software, and social media companies.

PROMINENT PAST TARGETS: At least six U.S. state governments.

13 SILK TYPHOON
AKA HAFNIUM

Active since at least 2021.

Likely tied to the Chinese Ministry of State Security.

Allegedly responsible for a series of attacks on Microsoft Exchange email servers in 2021. In 2025, a Chinese national was arrested in Italy for allegedly being a member of the group.

SIGNATURE ACCESS METHOD: Zero-day and known vulnerabilities, sometimes through third-party software providers.

TARGETS: Infectious disease researchers, law firms, universities, defense contractors, think tanks, and nongovernmental organizations.

PROMINENT PAST TARGETS: U.S. Treasury.

14 VOLT TYPHOON
AKA REDFLY

Active since at least 2020.

Possibly run by the PLA Cyberspace Force.

Allegedly focuses on stealthily compromising U.S. critical infrastructure systems and gathering intelligence for potential future attacks.

SIGNATURE ACCESS METHOD: Compromising Fortinet FortiGuard devices (patches were issued).

TARGETS: U.S. government, communications, manufacturing, utility, transportation, construction, maritime, information technology, and education companies.

PROMINENT PAST TARGETS: Utility companies supplying U.S. military bases.

15 FLAX TYPHOON
AKA ETHEREAL PANDA

Active since at least 2021.

In 2024, the FBI announced it had disrupted a Flax Typhoon botnet of more than 200,000 devices, including cameras, camcorders, and office routers.

SIGNATURE ACCESS METHOD: Known server vulnerabilities.

TARGETS: Government agencies, universities, telecom and media companies, nongovernmental organizations.

PROMINENT PAST TARGETS: Taiwanese government.

16 SALT TYPHOON
AKA GHOSTEMPEROR

Active since at least 2020.

Likely operated by the Chinese Ministry of State Security.

Known for a massive breach of U.S. telecom companies discovered in 2024, in which the hackers stole text messages, voicemails, and even some phone calls of high-profile clients, including President Donald Trump.

SIGNATURE ACCESS METHOD: Known vulnerabilities in network infrastructure, such as routers.

TARGETS: U.S. government, telecom companies.

PROMINENT PAST TARGETS: Verizon, AT&T, T-Mobile.

17 UNC3886
AKA FIRE ANT

Active since at least 2021.

Described as a "China-nexus" actor.

Known for deploying multiple layers of malware to maintain access even when detected.

SIGNATURE ACCESS METHOD: Zero-day vulnerabilities in Fortinet devices and VMWare virtualization software (patches were issued).

TARGETS: Defense, technology, and telecom companies.

PROMINENT PAST TARGETS: Singaporean critical infrastructure.

ALL PHOTOS BY GETTY IMAGES, FBI, DOJ