PREMIUM REPORTS

China's Massive Hacking Campaign Targeting the US

From espionage to intellectual property theft to sabotage, here's a look at 20 of the largest Chinese cyberattacks against the United States in the last decade.

39 21 Pause Save

Illustration by The Epoch Times, Getty Images

By Andrew Thornebrooke | January 03, 2025 Updated: January 04, 2025

China has dramatically increased its cyberattacks against the United States since Chinese Communist Party leader Xi Jinping came to power in 2012.

From espionage to intellectual property theft to sabotage, here is a look at 20 of the largest Chinese cyberattacks against the United States in the last 10 years.

August 2014: Community Health Systems Hack

A state-backed hacking group in China—referred to as APT18—launched an advanced malware attack against Tennessee-based Community Health Systems, one of the nation's largest hospital health care services.

The group succeeded in exfiltrating the sensitive personal information of more than 4.5 million patients, including their Social Security numbers, phone numbers, addresses, names, and birth dates.

(Left) FEMA Administrator Deanne Criswell addresses the media from the National Hurricane Center in Miami on May 31, 2023. (Right) United States Postal Service trucks in Farmingdale, N.Y., on April 12, 2020. Joe Raedle/Getty Images, Madalina Vasiliu/The Epoch Times

November 2014: NOAA and USPS Hacks

State-backed hackers in China launched malware and DDOS attacks against several government entities, including the U.S. Postal Service (USPS), the National Oceanic and Atmospheric Administration (NOAA), and the Office of Personnel Management.

The personal information of more than 800,000 employees at USPS, as well as that of customers who had called customer services, was exfiltrated. NOAA officials reported that they were immediately able to restore service to four affected websites but had not reported the incident for months, which was a violation of U.S. policy.

The entrance to the Theodore Roosevelt Federal Building that houses the Office of Personnel Management headquarters in Washington on June 5, 2015. U.S. investigators have said that at least four million current and former federal employees might have had their personal information stolen by Chinese hackers. Mark Wilson/Getty Images

June 2015: Office of Personnel Management Hack

The federal government's primary hiring agency was hacked by state-backed cyber actors in China. More than a million users' personal information, including names, addresses, and Social Security numbers, were stolen.

Those affected included current and former federal employees and contractors, as well as applicants for federal jobs and individuals listed on background check forms.

The attack was the third and largest of its kind in a matter of weeks and appeared to have specifically targeted data and applications related to U.S. security clearances. As such, the data stolen also included the financial histories and family information of those undergoing federal background checks at the time.

A Belgian plant of the U.S. chemicals group DuPont de Nemours in Mechelenon on April 13, 2004. Herwig Vergult/AFP via Getty Images

January 2016: Dupont Chemical Hack

Pangang Group, a Chinese state-owned steel manufacturer, was charged by the U.S. government for stealing trade secrets from

DuPont, a major chemical corporation. The group had obtained access to information on the U.S. company's computers.

Pangang worked with unidentified hackers to purchase trade secrets from a long-time DuPont employee, who stole the company's method for manufacturing titanium dioxide, a white pigment used in many applications, including semiconductors and solar panel cells.

The Aviation Industry Corporation of China (AVIC) logo is seen in during the International Paris Air Show in Le Bourget on June 25, 2017. Eric Piermont/AFP via Getty Images

April 2017: FAA, NASA Spearfishing Campaign

Song Wu, an employee for China's state-owned aerospace and defense corporation AVIC, allegedly began a multiyear spearfishing campaign against targets in the Federal Aviation Administration (FAA), National Aeronautics and Space Administration (NASA), U.S. Air Force, Navy, and Army.

Wu was later charged in 2024 for creating email accounts impersonating U.S.-based researchers and engineers to obtain restricted software used for aerospace engineering and computational fluid dynamics.

The U.S. government alleged that the software obtained could be used to develop advanced tactical missiles and aerodynamic designs for other weapons.

WANTED BY THE FBI
CHINESE PLA MEMBERS, 54TH RESEARCH INSTITUTE
Computer Fraud; Economic Espionage; Wire Fraud; Conspiracy to Commit Computer Fraud; Conspiracy to Commit Economic Espionage; Conspiracy to Commit Wire Fraud
Wang Qian
Xu Ke
Liu Lei
Wu Zhiyong
CAUTION
On January 28, 2020, a Grand Jury in the Northern District of Georgia returned an indictment charging Wang Qian, Xu Ke, Liu Lei, and Wu Zhiyong, with Computer Fraud, Economic Espionage, Wire Fraud, Conspiracy to Commit Fraud, Conspiracy to Commit Economic Espionage, and Conspiracy to Commit Wire Fraud. The defendants
Research Institute, which was a component of the People's Liberation Army ("PLA"), the
2017, and continuing through on or about
DEPARTMENT OF JUSTICE
WASHINGTON
JUSTITIA

A sign depicting the four members of China's military indicted on charges of hacking into Equifax Inc. and stealing data from millions of Americans is on display shortly after Attorney General William Barr held a press conference at the Department of Justice in Washington on Feb. 10, 2020. Sarah Silbiger/Getty Images

May 2017: Equifax Hack

Chinese military hackers breached the Equifax credit bureau in the largest-known theft of personal information.

More than 145 million Americans' sensitive personal data, including Social Security and driver's license numbers, were stolen. The hackers also obtained roughly 200,000 American credit card numbers.

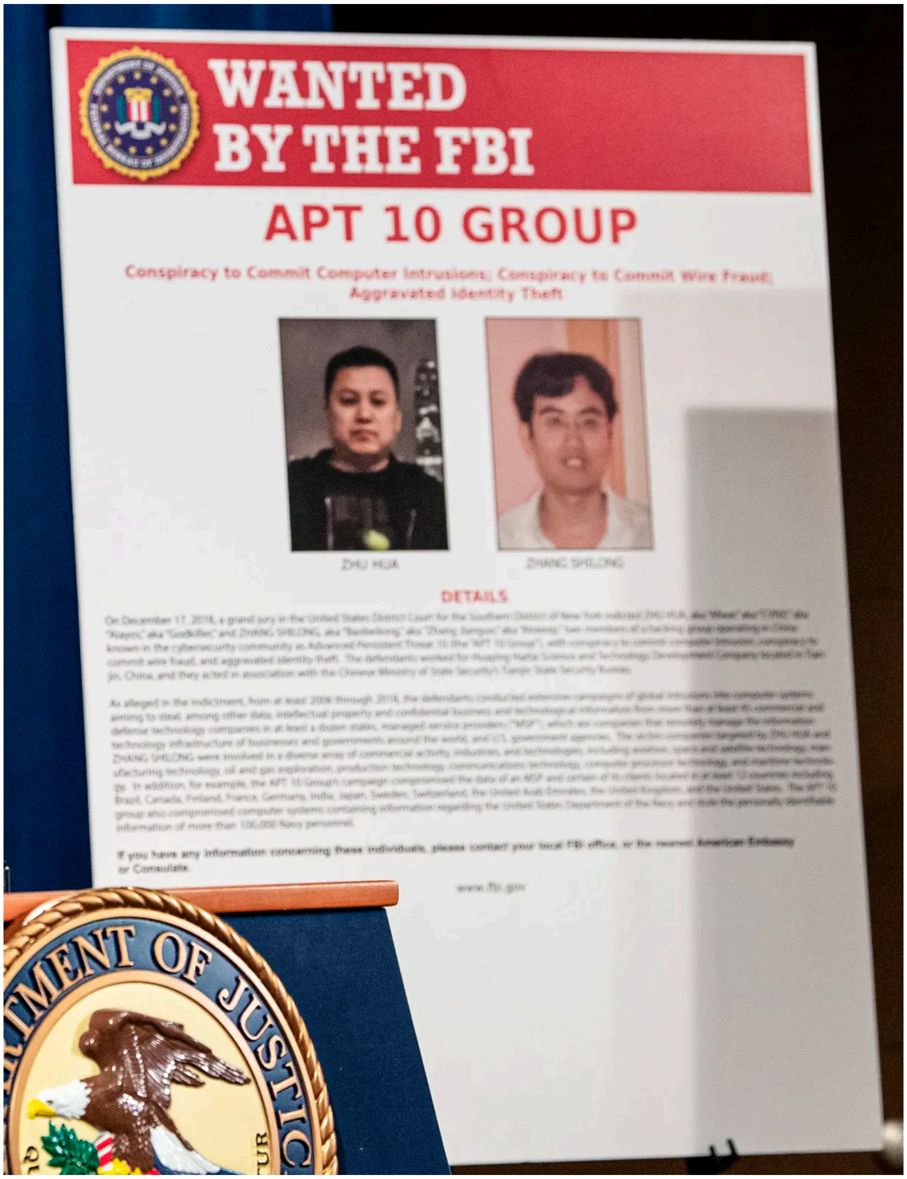
The hackers routed traffic through approximately 34 servers located in nearly 20 countries to obfuscate their true location.

The United States later indicted four members of China's military for the hack in 2020. As in most such cases, the hackers remain in China and have never been arrested.

January 2018: Navy Personnel, Technology Hacks

Chinese state-backed hackers allegedly compromised the computers of a U.S. Navy contractor and stole a large amount of highly sensitive data on undersea warfare, including U.S. plans for a supersonic anti-ship missile known as "Sea Dragon" for use on submarines, The Washington Post reported.

The hacked material also included signals and sensor data, information about submarine cryptographic systems, and electronic warfare documents from the Navy's primary submarine development unit.


WANTED
BY THE FBI
APT 10 GROUP
Conspiracy to Commit Computer Intrusions; Conspiracy to Commit Wire Fraud; Aggravated Identity Theft
ZHU HUA
ZHANG SHILONG
DETAILS
www.fbi.gov
TMENT OF JUSTIC

A sign depicting Chinese government hackers who allegedly targeted scores of companies in a dozen countries, at a press conference about Chinese hacking at the Justice Department in Washington on Dec. 20, 2018. Nicholas Kamm/AFP via Getty Images

June 2019: APT10 Utility Spearfishing Campaign

APT10, a hacking group directed by China’s Ministry of State Security, began a massive spearfishing and hacking campaign targeting U.S. aerospace, engineering, and telecommunications firms.

By using stolen passwords and malware, the hackers were able to steal records related to 130,000 Navy personnel.

Huntington Ingalls Industries, the largest builder of U.S. military ships and nuclear-powered submarines, acknowledged that it was targeted in the attack, and that computer systems owned by one of its subsidiaries were discovered connecting to a foreign server controlled by APT10.

Acting U.S. Attorney for the District of Columbia Michael R. Sherwin speaks to the media about charges and arrests related to a computer intrusion campaign tied to the Chinese government by a group called APT 41, at the Department of Justice in Washington on Sept. 16, 2020. Tasos Katopodis-Pool/Getty Images

August 2019: APT41 Hacks Revealed

China-based hacking group APT41 penetrated and spied on global tech, communications, and health care providers for China’s Ministry of State Security.

The group deployed rootkits, granting itself hard-to-detect control over computers, by compromising millions of copies of a utility called

CCleaner. APT41 also hijacked a software update pushed by Asus to reach 1 million computers, targeting a small subset of those users.

Moderna
COVID-19
Vaccine
NDC 80777-273-10
Suspension for Intramuscular Injection
For use under Emergency Use Authorization
Multiple-dose vial
(10 doses of 0.5 mL)

A nurse prepares a dose of the Moderna vaccine against COVID-19, donated by the United States, at a vaccination center in San Juan Sacatepequez, Guatemala, on July 15, 2021. Johan Ordonez/AFP via Getty Images

May 2020: Moderna COVID-19 Vaccine Espionage

Chinese regime-linked hackers targeted biotech company Moderna as it conducted research to develop a vaccine for COVID-19.

The effort involved conducting reconnaissance in order to steal proprietary research needed to develop a vaccine for the disease, which Moderna received nearly half a billion dollars to create from the U.S. government.

A U.S. indictment alleged that the China-based hackers probed public websites for vulnerabilities and scouted accounts of key personnel after gaining access to a network used by Moderna.

Paul Nakasone, director of the National Security Agency, looks at a hearing with the House Armed Services Subcommittee on Cyber, Innovative Technologies, and Information Systems in the Rayburn House Office Building in Washington on May 14, 2021. Anna Moneymaker/Getty Images

February 2021: Chinese Access to NSA Hacking Tools Revealed

Israeli researchers discovered that Chinese spies had stolen and deployed code first developed by the U.S. National Security Agency (NSA) to support their hacking operations.

The NSA hacking tools were leaked online in 2017. Still, cyber investigators found evidence that the Chinese communist-backed APT31 hacking group had deployed an identical tool as early as 2014. This suggests that China-based hackers had persistent access to the nation’s best national security cyber tools for years.

People walk by a Microsoft store in New York City on July 26, 2023. Samira Bouaou/The Epoch Times

March 2021: Silk Typhoon

A cyber-espionage group associated with China's Ministry of State Security stole emails and passwords from more than 30,000 organizations by exploiting flaws in Microsoft Exchange Servers.

The group, dubbed Silk Typhoon by Microsoft, worked closely with China-back APT40, leveraging a flaw in Microsoft's software to gain full access to emails hosted on more than 250,000 servers in the United States.

Among the organizations most affected by the hack were American pharmaceutical companies, defense contractors, and think tanks.

Attendees pass by an Alibaba.com display at a consumer technology trade show at the Las Vegas Convention Center in Las Vegas on Jan. 8, 2019. David Becker/Getty Images

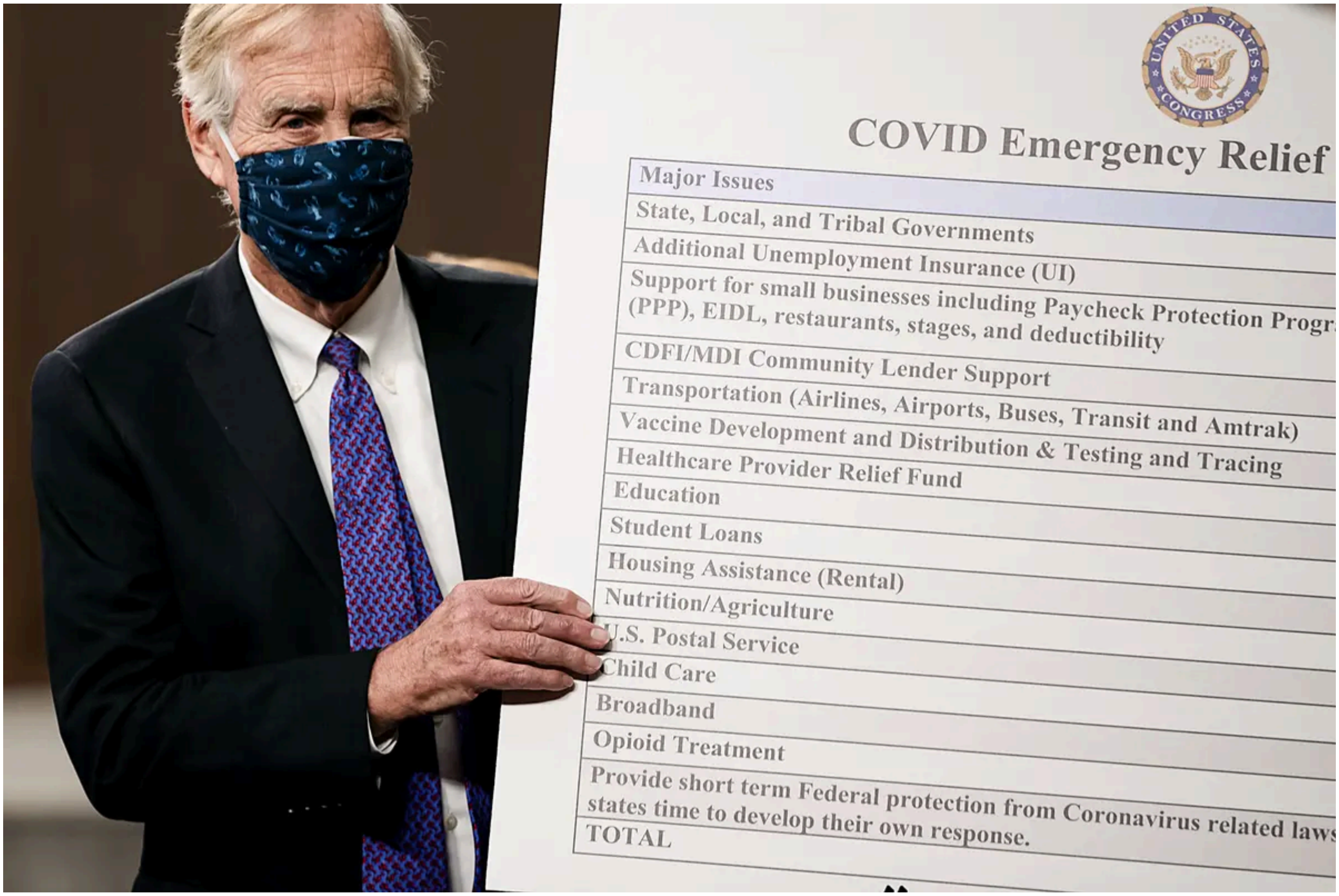
December 2021: Log4j Hacks

APT41 returned to action, leveraging a previously unknown vulnerability in commonly used open-source logging software Log4j. The group used the vulnerability to hack into at least six unspecified U.S. government agency networks over a nine-month period.

The vulnerability allowed APT41 to keep track of user chats and clicks and follow user link clicks to outside sites, allowing hackers to control a targeted server.

The hackers then used the hijacked networks to mine cryptocurrency, create botnets, send spam, and establish backdoors for future malware attacks.

Notably, the China-based company Alibaba first discovered the security flaw and privately reported it to Apache Software, which created the affected software. The Chinese Communist Party afterward punished Alibaba by revoking an information-sharing deal, as Chinese law requires security flaws to be reported to the regime.

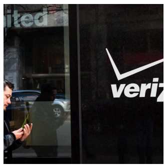

UNITED STATES CONGRESS
COVID Emergency Relief
Major Issues
State, Local, and Tribal Governments
Additional Unemployment Insurance (UI)
Support for small businesses including Paycheck Protection Progr
(PPP), EIDL, restaurants, stages, and deductibility
CDFI/MDI Community Lender Support
Transportation (Airlines, Airports, Buses, Transit and Amtrak)
Vaccine Development and Distribution & Testing and Tracing
Healthcare Provider Relief Fund
Education
Student Loans
Housing Assistance (Rental)
Nutrition/Agriculture
U.S. Postal Service
Child Care
Broadband
Opioid Treatment
Provide short term Federal protection from Coronavirus related laws
states time to develop their own response.
TOTAL

Sen. Angus King (I-Maine) sets up a sign alongside a bipartisan group of Democrat and Republican members of Congress as they announce a proposal for a COVID-19 relief bill on Capitol Hill on Dec. 1, 2020. Tasos Katopodis/Getty Images

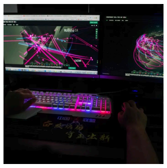
December 2022: COVID-19 Relief Fund Theft

APT41 stole millions of dollars worth of U.S. COVID-19 relief benefits, which were intended to help Americans who were negatively impacted by the government's economic shutdowns during the 2020 pandemic.

Premium Picks



China-Backed Salt Typhoon Hacking Group Remains Embedded in US …



What Could Cyber Attacks Like China's Volt Typhoon Do With Emplaced Malware?

The sum was part of a staggering estimated $280 billion in stolen COVID-19 relief, which was illicitly intercepted by foreign hackers and domestic fraudsters who used the Social Security numbers and personal information of deceased and incarcerated Americans to claim benefits illegally.

To date, the Justice Department has only successfully recovered about $1.5 billion of the stolen funds.

May 2023: Antique Typhoon

Antique Typhoon, a Chinese state-backed hacking outfit, forged digital authentication tokens to access the webmail accounts of 25 organizations, including numerous U.S. government agencies.

The hackers were able to obtain the emails of government officials, including Commerce Secretary Gina Raimondo, and members of Congress, including Rep. Don Bacon (R-Neb.). The hackers used persistent access to the email accounts only for exfiltrating data, suggesting that their purpose was primarily espionage.

半導體世紀對談
CW Semiconductor Forum:Global Chip Competition and Taiwan's Key Strengths

Taiwanese Vice President Lai Ching-te gives a speech at the CommonWealth Semiconductor Forum in Taipei, Taiwan, on March 16, 2023. Annabelle Chih/Getty Images

August 2023: HiatusRAT

China-backed hackers began targeting U.S. and Taiwanese military procurement systems, as well as semiconductor and chemical manufacturers.

The hackers leveraged a remote access tool to breach the system used to coordinate arms shipments from the United States to Taiwan. International open-source reporting suggests that the hackers' goal was to gain intelligence on future defense contracts between the two powers.

September 2023: BlackTech Router Attack

China-backed hacking group BlackTech began targeting major corporate headquarters throughout the United States. The group appeared to focus its attacks on gaining access to American and Japanese companies working in the defense sector.

U.S. and allied intelligence agencies announced that having penetrated the international subsidiaries of major companies, BlackTech was now using its access to grant itself entry to major corporate networks within the United States in order to exfiltrate data.

January 2024: Volt Typhoon

U.S. intelligence agencies announced that Volt Typhoon, a Chinese state-backed hacking group, was pre-positioning malware in critical infrastructure throughout the United States, including water, gas, energy, rail, air, and port infrastructure.

Unlike most other Chinese hacking efforts that focus on espionage or intellectual property theft, Volt Typhoon sought to position malware in U.S. infrastructure in order to sabotage it in the event of a conflict between the two nations. Such sabotage would result in mass casualties among American citizens.

U.S. intelligence agencies said that they have removed Volt Typhoon malware from thousands of systems but that it remains embedded in some privately owned infrastructure and has been present since at least 2021.

(Left) A sign is posted in front of an AT&T retail store in San Rafael, Calif., on May 17, 2021. (Right) A man on his cell phone walks past a Verizon Wireless store in Washington on Dec. 30, 2014. Justin Sullivan/Getty Images, Jim Watson/AFP via Getty Images

November 2024: Salt Typhoon

U.S. intelligence agencies acknowledged that Salt Typhoon, a Chinese state-backed hacking group, has compromised the infrastructure used by eight major telecommunications companies, including AT&T, CenturyLink, and Verizon.

Salt Typhoon appeared to have gained access to the backend infrastructure used to accommodate the U.S. government's own wiretapping efforts and thus gained access to virtually all calls and texts made using the affected networks.

Despite the wide-ranging access, China-based hackers appeared to have used the persistent access to target high-profile individuals, including President-elect Donald Trump and Vice President-elect JD Vance.

Congressional leaders have described the hack, which likely began in 2022, as among the most significant breaches in history. It is unclear how Salt Typhoon will be evicted from the infrastructure. The group retained access to U.S. telecommunications until late December.

Secretary of the Treasury Janet Yellen delivers remarks at Johns Hopkins University's School of Advanced International Studies in Washington on April 20, 2023. Anna Moneymaker/Getty Images

January 2025: US Treasury Department Hack

The Treasury Department revealed that Chinese state-backed hackers had breached the department's networks, gaining access to the servers of an office responsible for administering international sanctions.

The hackers also gained access to the department's networks by compromising third-party cybersecurity service provider BeyondTrust, stole an as-of-yet unknown number of unclassified documents, and targeted the accounts of Treasury Secretary Janet Yellen.

More Premium Reports See More

Trump Wants to Eliminate the Debt Ceiling—What Is It and How Did We Get Here?

US Health Insurance: What Are Its Problems and Potential Solutions?

Top 10 Moments From the 118th Congress

Trump Supporters Are Debating the H-1B Visa—What Is It?

A Look Back at 24 Moments That Helped Define 2024

How The New York Times Distorts Shen Yun's Success in Latest Attack Article

10 Things to Know About President Jimmy Carter

Increased Drone Sightings Highlight New Risks, Aviation Experts Say

California Makes World-Class Wines, but Industry Pressures Are Leaving Grapes to Die

How Shen Yun Was Born to Expose Persecution in China, Revive Traditional Culture

Cookies Settings