CHINA NEWS

Japan Says China-Linked Hackers Targeted National Security, Tech Entities

The Chinese hackers tried to steal information by sending emails containing malware to targets in Japan and by infiltrating networks, the NPA said.

24 3 Save

A man holds a laptop computer as cyber code is projected on him in this illustration picture taken on May 13, 2017. Kacper Pempel/Reuters

By Lily Zhou

1/9/2025 Updated: 1/9/2025

Print

Chinese cyberespionage group MirrorFace has been attempting to steal information on Japan’s national security and advanced technology since 2019, Japan’s National Police Agency (NPA) said on Jan. 8.

A security assessment has linked MirrorFace to an “organized cyberattack” campaign that is suspected to be connected to China, according to the NPA.

The agency detailed the group’s tactics in three campaigns, calling on government agencies and businesses to reinforce preventive measures.

The cyberespionage group was dubbed MirrorFace by Slovakia-based cybersecurity company ESET.

In December 2022, ESET said its researchers had detected a MirrorFace spearphishing campaign targeting politicians before the Japanese House of Councillors election in July 2022.

In a quarterly report published in November 2024, ESET said MirrorFace had “extended its operations to include a diplomatic organization in the European Union for the first time while continuing to prioritize its Japanese targets.”

According to the NPA, between December 2019 and July 2023, MirrorFace targeted sitting and retired government officials, other politicians, the media, and think tanks by sending emails with malware-laden attachments.

The senders often posed as former executives of an organization with which the recipient was or had been affiliated, or as experts in a field of interest to the recipient.

The emails' subjects generally referred to then-current affairs, with keywords such as "Japan–U.S. Alliance," "Taiwan Strait," "Russia–Ukraine War," and "Free and Open Indo–Pacific."

In some cases, hackers initially offered to send materials in their emails and later attached malware-infected files to entice the recipient to open them.

As a result of these emails, hackers were able to access some information until May 2024, the NPA said.

Since June 2024, MirrorFace actors have been conducting a separate email campaign. In the body of the email, they include links that prompt recipients to download a ZIP file containing malware-laced files. The targets include academia, think tanks, politicians, and the media.

In both email campaigns, in some cases, hackers impersonated others by gaining access to their legitimate email addresses.

Between February and October 2023, MirrorFace infiltrated internet-connected network devices, targeting academics and sectors such as semiconductors, manufacturing, aerospace, and information and communications. Intrusions believed to be caused by this campaign have continued as recently as June 2024, the NPA said.

The attacks included one on the Japan Aerospace and Exploration Agency, which in June, acknowledged that it had been targeted by a series of cyberattacks since 2023, though sensitive information related to rockets, satellites, and defense was not affected. The agency said in July that it had taken short-term measures and was working on permanent measures to further enhance security.

Experts have repeatedly raised concerns about the vulnerability of Japan's cybersecurity, especially as the country steps up its defense capabilities and works more closely with the United States and other partners to strengthen its cyber defenses.

In 2023, a cyberattack allegedly launched by the Russia-based LockBit ransomware group paralyzed the operations of a container terminal at a port in the city of Nagoya for three days.

More recently, Japan Airlines was hit by a cyberattack on Dec. 25, 2024, causing delays and cancellations to more than 20 domestic flights, though the carrier was able to restore its systems hours later, and there was no impact on flight safety.

In a report published in October 2024, Microsoft said Russia, China, and Iran were increasingly enlisting cybercriminals to target the United States and its allies.

On Dec. 10, 2024, the FBI said malware from Beijing-backed Salt Typhoon, Flax Typhoon, and Volt Typhoon were still embedded in some U.S. systems.

On Jan. 3, the Treasury sanctioned a Chinese cybersecurity company, Beijing-based Integrity Technology Group, saying Flax Typhoon actors operated a botnet of 200,000 devices worldwide using the company's infrastructure.

The Associated Press contributed to this report.

Lily Zhou
Author

Lily Zhou is an Ireland-based reporter covering China news for The Epoch Times.

Author's Selected Articles

Shein Representative Declines to Address China Cotton Questions at UK Hearing

Jan 08, 2025

CDC Monitoring HMPV Outbreak in China

Jan 07, 2025

Philippines Monitors Chinese ‘Monster Ship’ in South China Sea

Jan 07, 2025

DOD Adds Tencent, CATL to List of Companies Linked to Chinese Military

Jan 06, 2025

Cookies Settings