MirrorFace hackers targeting Japanese govt, politicians since 2019

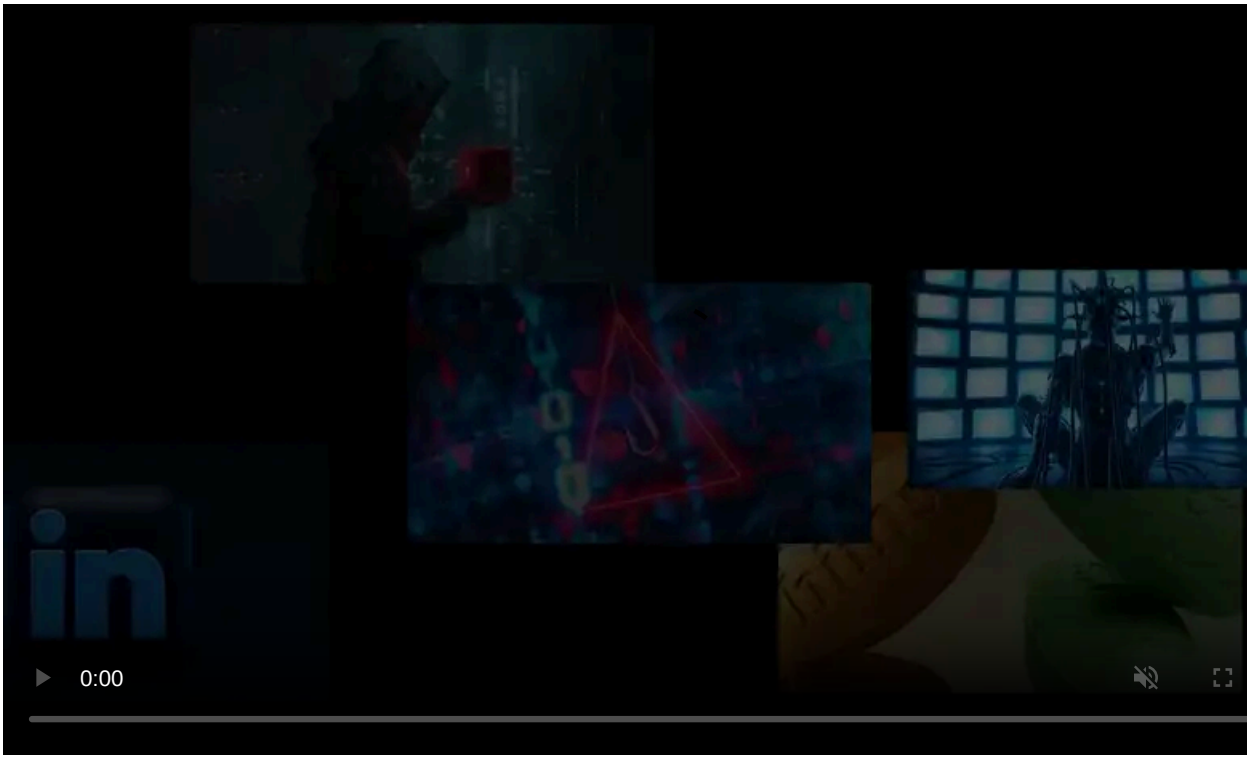
By Bill Toulas

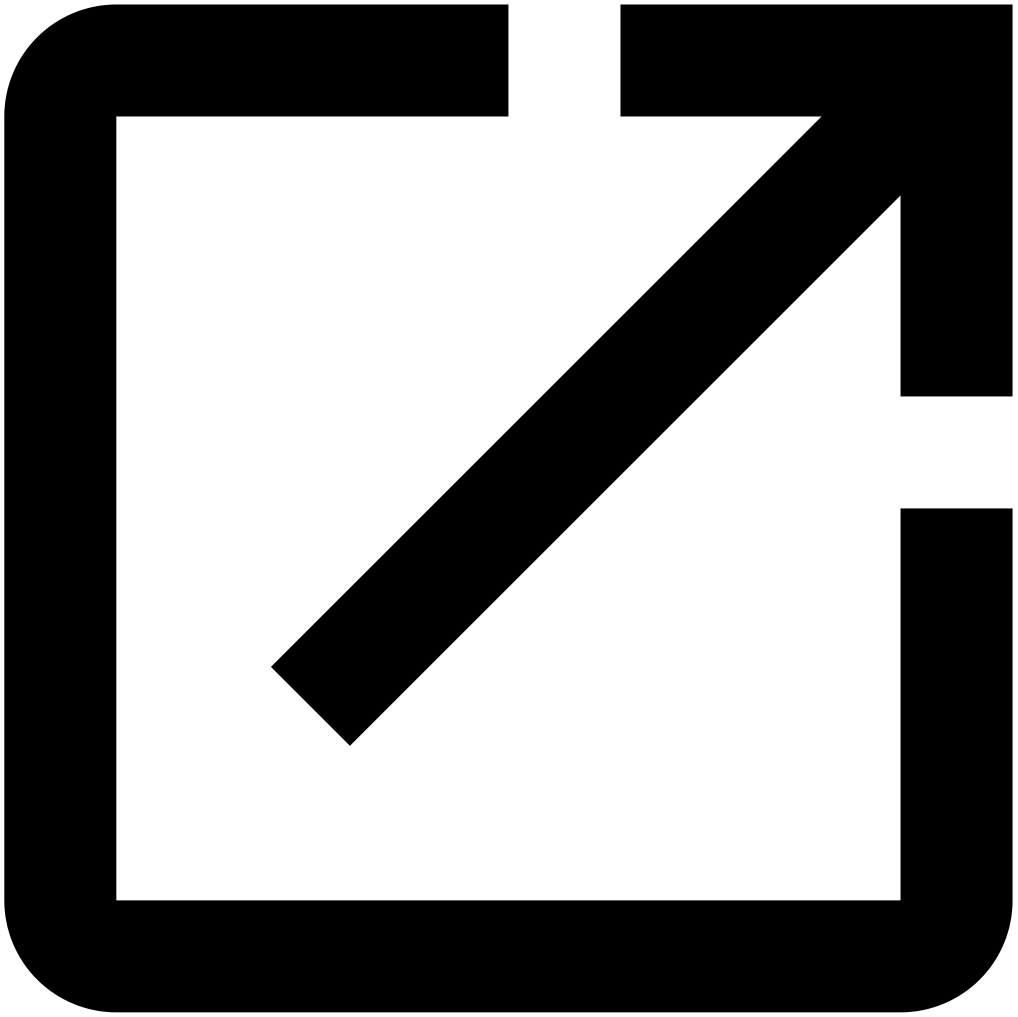
Published: 2025-01-09 · Archived: 2026-04-05 18:01:54 UTC

The National Police Agency (NPA) and the Cabinet Cyber Security Center in Japan have linked a cyber-espionage campaign targeting the country to the Chinese state-backed "MirrorFace" hacking group.

The campaign has been underway since 2019 and is still ongoing, while the Japanese investigators have observed distinct phases with differentiation of targets and attack methods.

In all cases, the primary goal is to steal information on valuable and advanced Japanese technology and gather national security intelligence.


0:00



MirrorFace, also known as "Earth Kasha," was previously observed by ESET conducting attacks on Japanese politicians before elections, using phishing emails to deploy a credential stealer dubbed 'MirrorStealer' and also the 'LODEINFO' backdoor.

Targeting government and technology

According to NPA's analysis of the MirrorFace activity, the Chinese hackers exploit flaws in networking equipment, including CVE-2023-28461 in Array Networks, CVE-2023-27997 in Fortinet appliances, and CVE-2023-3519 in Citrix ADC/Gateway.

After breaching the networks, the threat actors infect targeted computers with LODEINFO, ANEL, NOOPDOOR, and other malware families capable of data exfiltration and various backdoors for persistent long-term access.

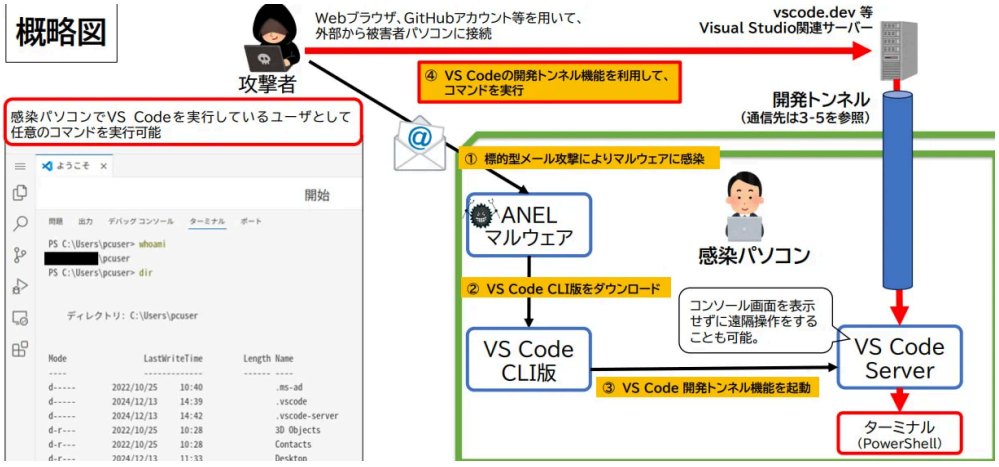
NPA identified three distinct campaigns conducted by the MirrorFace hackers:

- **Campaign A (2019–2023)**: Targeted think tanks, government entities, politicians, and media with malware-laden emails to steal information.
- **Campaign B (2023)**: Exploited software vulnerabilities in internet-connected devices, targeting Japan's semiconductor, manufacturing, ICT, academia, and aerospace sectors.
- **Campaign C (2024–present)**: Used malicious email links to infect academia, think tanks, politicians, and media with malware.

Evasion via VSCode and Windows Sandbox

The NPA highlights two evasion methods MirrorFace uses to persist in networks for extended periods without raising any alarms.

The first uses Visual Studio Code tunnels, which are set up by the ANEL malware on the compromised system. These tunnels are used to receive commands to execute on infected systems, which are usually PowerShell commands.



Using VSCode tunnels for covert communications
Source: NPA

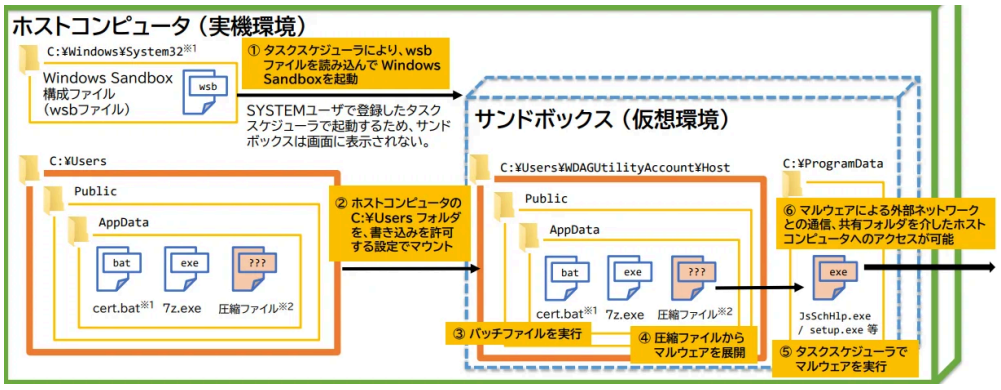
Reportedly, MirrorFace has been using VSCode tunnels since at least June 2024.

This is a documented tactic previously attributed to other Chinese state-sponsored hackers like STORM-0866 and Sandman APT.

The second evasion method, employed since June 2023, involves the use Windows Sandbox feature to execute LOADEINFO within an isolated environment, bypassing antivirus detection.

Windows Sandbox is a virtualized desktop environment that can safely execute commands and run programs isolated from the host operating system.

However, the host operating system, including Microsoft Defender, does not monitor this environment. This allows the threat actors to run malware that communicates with remote command and control (C2) servers while maintaining local filesystem access to the host via shared folders.



The Windows Sandbox evasion method

Source: NPA

Based on the above, the NPA recommends that system administrators monitor for suspicious PowerShell logs, unauthorized communications with VSCode domains, and unusual sandbox activity.

While it is not possible to log commands executed in Windows Sandbox, the NPA says you can configure Windows policies on the host to audit process creation to detect when the Windows Sandbox is launched and what configuration file was used.

This will allow organizations that do not usually use Windows Sandbox to detect its use and investigate further.

Automated pentesting proves the path exists. BAS proves whether your controls stop it. Most teams run one without the other.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.
