


Operation LiberalFace, MirrorFace - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 16:38:20 UTC

[Home](#) > [List all groups](#) > Operation LiberalFace, MirrorFace

APT group: Operation LiberalFace, MirrorFace

Names	Operation LiberalFace (ESET) MirrorFace (ESET)	
Country	 China	
Motivation	Information theft and espionage	
First seen	2019	
Description	<p>(ESET) ESET researchers discovered a spearphishing campaign, launched in the weeks leading up to the Japanese House of Councillors election in July 2022, by the APT group that ESET Research tracks as MirrorFace. The campaign, which we have named Operation LiberalFace, targeted Japanese political entities; our investigation revealed that the members of a specific political party were of particular focus in this campaign. ESET Research unmasked details about this campaign and the APT group behind it at the AVAR 2022 conference at the beginning of this month.</p> <p>This campaign may have been performed by Stone Panda, APT 10, menuPass.</p>	
Observed	Sectors: Government . Countries: Japan .	
Tools used	Anel , AsyncRAT , LODEINFO , MirrorStealer .	
Operations performed	Aug 2024	Operation “AkaiRyū” MirrorFace invites Europe to Expo 2025 and revives ANEL backdoor <https://www.welivesecurity.com/en/eset-research/operation-akairyu-mirrorface-invites-europe-expo-2025-revives-anel-backdoor/>
Information	<https://www.welivesecurity.com/2022/12/14/unmasking-mirrorface-operation-liberalface-targeting-japanese-political-entities/>	

<<https://www.bleepingcomputer.com/news/security/mirrorface-hackers-targeting-japanese-govt-politicians-since-2019/>>

Last change to this card: 21 April 2025

Download this actor card in [PDF](#) or [JSON](#) format

Source: <https://apt.etda.or.th/cgi-bin/showcard.cgi?u=366d8eb7-f1b3-4341-b20b-9853a82ed26d>