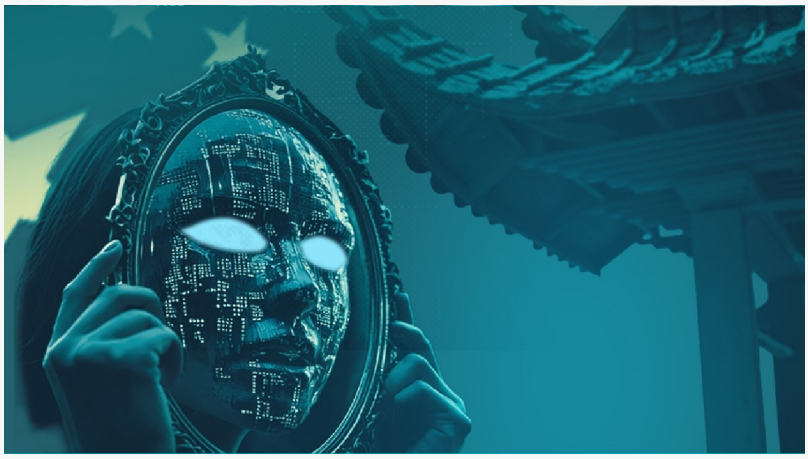
ESET Research uncovers Operation AkaiRyū: China-aligned MirrorFace targets European diplomats using Expo 2025 as a lure



DUBAI, UNITED ARAB EMIRATES, March 20, 2025 /EINPresswire.com/ -- ESET researchers have detected cyberespionage activity carried out by the China-aligned MirrorFace APT group against a Central European diplomatic institute in relation to Expo 2025, which will be held this year in Osaka, Japan. Known primarily for its cyberespionage activities against organizations in Japan, to the best of our knowledge, this is the first time MirrorFace has shown intent to infiltrate a European entity. The campaign was uncovered in Q2 and Q3 of 2024 and named Operation AkaiRyū (Japanese for RedDragon) by ESET; it showcases refreshed TTPs that ESET Research observed throughout last year.

“MirrorFace targeted a Central European diplomatic institute. To our knowledge, this is the first, and, to date, only time MirrorFace has targeted an entity in Europe,” says ESET researcher Dominik Breitenbacher, who investigated the AkaiRyū campaign.

MirrorFace operators set up their spearphishing attack by crafting an email message that references a previous, legitimate interaction between the institute and a Japanese NGO. During this attack, the threat actor used the upcoming World Expo 2025 – to be held in Osaka, Japan – as a lure. This further shows that even considering this new broader geographic targeting, MirrorFace remains focused on Japan and events related to it. Before the attack on this European diplomatic institute, MirrorFace targeted two employees at a Japanese research institute, using a malicious, password-protected Word document delivered in an unknown manner.

During the analysis of Operation AkaiRyū, ESET discovered that MirrorFace has significantly refreshed its TTPs and tooling. MirrorFace started using ANEL (also referred to as UPPERCUT) – a backdoor considered exclusive to APT10 – that was believed to be abandoned years ago;

however, the latest activity strongly suggest that the development of ANEL has restarted. ANEL supports basic commands for file manipulation, payload execution, and taking screenshots.

“The use of ANEL also provides further evidence in the ongoing debate about the potential connection between MirrorFace and APT10. The fact that MirrorFace has started using ANEL, along with the other previously identified information, such as similar targeting and malware code similarities, led us to make a change in our attribution: we now believe that MirrorFace is a subgroup under the APT10 umbrella,” adds Breitenbacher.

Additionally, MirrorFace deployed a heavily customized variant of AsyncRAT, embedding this malware into a newly observed, intricate execution chain that runs the RAT inside Windows Sandbox. This method effectively obscures the malicious activities from security controls abilities to detect the compromise. In parallel to the malware, MirrorFace also started deploying Visual Studio Code (VS Code) to abuse its remote tunnels feature. Remote tunnels enable MirrorFace to establish stealthy access to the compromised machine, execute arbitrary code, and deliver other tools. Finally, MirrorFace has continued to employ its current flagship backdoor, HiddenFace, further bolstering persistence on compromised machines.

Between June and September 2024, ESET observed MirrorFace conducting multiple spearphishing campaigns. Based on ESET data, the attackers primarily gained initial access by tricking targets into opening malicious attachments or links, then they leveraged legitimate applications and tools to stealthily install their malware. Specifically, in Operation AkaiRyū, MirrorFace abused both McAfee-developed applications and also one developed by JustSystems to run ANEL. ESET was unable to determine how MirrorFace exported the data, and whether or how the data was exfiltrated.

ESET Research collaborated with the affected Central European diplomatic institute and performed a forensic investigation. The close collaboration with the affected organization provided a rare, in-depth view of post-compromise activities that would have otherwise gone unseen. ESET Research presented the results of this analysis at the Joint Security Analyst Conference (JSAC) in January 2025.

For a more detailed analysis and technical breakdown of MirrorFace’s Operation AkaiRyū, check out the latest ESET Research blogpost “Operation AkaiRyū: MirrorFace invites Europe to Expo 2025 and revives ANEL backdoor” on WeLiveSecurity.com. Make sure to follow ESET Research on Twitter (today known as X) for the latest news from ESET Research.

About ESET
ESET® provides cutting-edge digital security to prevent attacks before they happen. By combining the power of AI and human expertise, ESET stays ahead of known and emerging cyberthreats — securing businesses, critical infrastructure, and individuals. Whether it’s endpoint, cloud or mobile protection, our AI-native, cloud-first solutions and services remain highly effective and easy to use. ESET technology includes robust detection and response, ultra-secure encryption,

and multifactor authentication. With 24/7 real-time defense and strong local support, we keep users safe and businesses running without interruption. An ever-evolving digital landscape demands a progressive approach to security: ESET is committed to world-class research and powerful threat intelligence, backed by R&D centers and a strong global partner network. For more information, visit www.eset.com or follow us on LinkedIn, Facebook, and X.

Sanjeev Kant
Vistar Communications
+971 55 972 4623
email us here