New Iranian Espionage Campaign By “Siamesekitten” – Lyceum – ClearSky Cyber Security

Published: 2021-08-17 · Archived: 2026-04-05 12:44:59 UTC

At the beginning of May 2021, we detected the first attack by Siamesekitten on an IT company in Israel. Siamesekitten (also named Lyceum/Hexane) is an Iranian APT group active in the Middle east and in Africa that is active in launching supply chain attacks. To this end Siamesekitten established a large infrastructure that enabled them to impersonate the company and their HR personnel. We believe that this infrastructure was built to lure IT experts and penetrate their computers to gain accesses to the company’s clients.

This campaign is similar to the North Korean “Job seekers” campaign, employing what has become a widely used attack vector in recent years – impersonation. Many attack groups are executing this type of campaign, such as the North Korean Lazarus campaign we exposed in the summer of 2020 (Dream Job) and the Iranian OilRig campaign (APT34) that targeted Middle Eastern victims in the first quarter of 2021.

In July 2021, we detected a second wave of similar attacks against additional companies in Israel. In this wave, Siamesekitten upgraded their backdoor malware to a new version called “Shark” and it replaced the old version of their malware called “Milan”. Details of both versions are included in our report.

This report summarizes our findings regarding the latest Siamesekitten attacks and reviews the attack patterns and malware used in this campaign.

Read the full report:
