

Iranian “Dream Job” Campaign 11.24

CS clearskysec.com/irdreamjob24/

by ClearSky Research Team

November 12, 2024

ClearSky Cyber Security research identified a campaign named “Iranian Dream Job campaign”, in which the Iranian threat actor TA455 targeted the aerospace industry by offering fake jobs.

The campaign distributed the SnailResin malware, which activates the SlugResin backdoor. ClearSky attributes both malware programs to a subgroup of Charming Kitten.

However, some cyber research companies detected the malware files as belonging to the North Korean Kimsuky/Lazarus APT group.

The similar “Dream Job” lure, attack techniques, and malware files suggest that either Charming Kitten was impersonating Lazarus to hide its activities, or that North Korea shared attack methods and tools with Iran.

The Iranian “Dream Job” campaign has been active since at least September 2023. Mandiant had previously reported on suspected Iranian espionage activity targeting aerospace, aviation, and defense industries in Middle East countries, including Israel and the United Arab Emirates (UAE), as well as Turkey, India, and Albania.

The LinkedIn profiles of the fake recruiters in our report seem to be newer versions of the profiles Mandiant previously reported. For example, ClearSky discovered a profile associated with a fake company called “Careers 2 Find,” which previously worked for “1st Employer,” a fake recruiting website highlighted by Mandiant.

How the Campaign Works

TA455 uses fake recruiting websites and LinkedIn profiles to distribute a ZIP file containing malicious files. The ZIP file, which includes legitimate files, is downloaded from a domain impersonating a job recruiting website. Victims are given a detailed PDF guide on how to “safely” access the website in order to prevent them from making “mistakes” that might “prevent infection”. Once the ZIP file is downloaded, the victim clicks on a highlighted EXE file. The EXE loads the malicious DLL file “secur32[.]dll” via DLL side loading. The malware checks the victim’s IP address and downloads information from a GitHub account that contains the C&C server domain address.

For the full version of our report:

[Iranian Dream Job – ver1](#)

[Sitemap.xml](#) | Copyright 2025 © ClearSky Cyber Security