

Iranian “Dream Job” Cyber Campaign Targets Aerospace Sector

informationsecuritybuzz.com/iranian-dream-job-aerospace/

By Kirsten Doyle

November 15, 2024



In a new and sophisticated cyber campaign dubbed the “Iranian Dream Job Campaign,” the Iranian threat group TA455 is using deceptive job offers to infiltrate the aerospace industry, ClearSky Cyber Security reported.

The campaign relies on distributing SnailResin malware, which activates the SlugResin backdoor, a malware set ClearSky links to the well-known Iranian cyber actor subgroup Charming Kitten.

The deceptive nature of the operation has led some cyber research companies to mistakenly attribute the malware files to North Korea’s Kimsuky/Lazarus Advanced Persistent Threat (APT) group. The overlapping “Dream Job” recruitment tactics, attack methods, and malware signatures suggest that Charming Kitten may be masquerading as Lazarus to obfuscate its activities or that there could be an exchange of cyberattack tools and strategies between Iran and North Korea.

Extended Campaign Targets Aerospace, Aviation, and Defense

The campaign has been active since at least September 2023. It aligns with previously identified Iranian espionage activities targeting aerospace, aviation, and defense sectors in Middle Eastern countries, including Israel, the UAE, and beyond to Turkey, India, and Albania. Cybersecurity firm Mandiant had earlier identified similar activities involving Iran, highlighting the persistent nature of the country's interest in these sensitive industries.

ClearSky has identified LinkedIn profiles associated with fictitious recruiting firms, which are believed to be newer iterations of previously exposed profiles from Mandiant's reports. For example, ClearSky uncovered a profile linked to a fabricated firm named "Careers 2 Find," which reportedly succeeded an earlier fraudulent company called "1st Employer." Both profiles serve as bait for professionals in the aerospace sector.

Sophisticated Deception Tactics

TA455 lures victims through fake recruitment websites and LinkedIn profiles, providing a ZIP file that appears to contain legitimate job-related files. This ZIP file, downloaded from a website that mimics a legitimate recruiting domain, also contains the malicious executable file "secur32[.dll]" hidden in a DLL file. Victims are encouraged to follow a detailed PDF guide designed to ensure they "safely" access the job information, unknowingly executing the malware.

Upon activation, the SnailResin malware connects to a GitHub account to retrieve the Command and Control (C&C) server domain, which allows attackers to monitor and control the infected device remotely. This campaign leverages advanced social engineering tactics and uses legitimate-seeming tools to increase its effectiveness, posing a significant threat to high-value sectors globally.

TA455's Techniques for Evading Detection

TA455 intentionally seeks to mislead investigators by adopting tactics and tools commonly associated with other threat actors, particularly the North Korean Lazarus group. This involves using similar "Dream Job" lures, attack techniques, and malware files that resemble those used by Lazarus in DLL side-loading attacks. The goal of this misattribution is to create confusion and make accurate identification more difficult.

To disguise their infrastructure and command-and-control (C2) communications, TA455 blends into the traffic of reputable online services such as Cloudflare, GitHub, and Microsoft Azure cloud. By using Cloudflare for malicious domains like "careers2find[.com]," they obscure the actual server location and ownership, complicating tracking efforts. Similarly, they exploit GitHub to host encoded C2 server information, accessing it through seemingly benign accounts like "msdnedgesupport." This approach allows them to camouflage their activities within legitimate traffic, reducing the likelihood of detection.

TA455 also employs a sophisticated, multi-stage infection strategy to improve the success rate while limiting the chances of detection. Initial spearphishing emails likely contain malicious attachments disguised as job-related documents hidden within ZIP files containing a combination of legitimate and malicious files. This layered tactic is designed to bypass security scans and entice victims to execute the malware. Once activated, the malware carries out a series of staged actions, such as checking the victim's IP address and obtaining C2 server details from compromised GitHub accounts, making the attack harder to detect and analyze fully.

AI-Enabled Evolution in Attack Precision

This campaign highlights the lengths to which threat actors are willing to go in order to disguise their cyber espionage activities. The crossover with known North Korean tactics has raised concerns over potential collaboration between Iranian and North Korean APT groups, though conclusive evidence of direct cooperation remains elusive.

Industry-specific job-themed social engineering attacks from TA455 threat actors demonstrate an AI-enabled evolution in attack precision, making it economical to target sectors like aerospace where specialized talent and valuable intellectual property converge, says Stephen Kowski, Field CTO at SlashNext.

“We’ve seen historically these job campaigns were generalized and focused on university settings, where students eagerly seeking opportunities become prime targets for malicious actors using weaponized PDFs and harmful compressed archives. Modern security solutions capable of real-time detection of malicious content are crucial, as traditional email security often fails to catch these highly targeted attacks that masquerade as legitimate job offers and professional networking attempts. To combat this threat, organizations and job seekers must implement thorough verification processes for recruitment communications while deploying advanced security tools that can intercept social engineering attempts before user engagement.”

Exploiting the Desire for Career Advancement

Sarah Jones, Cyber Threat Intelligence Research Analyst at Critical Start, says APT actors, including state-sponsored ones, have often used job-themed social engineering tactics to target people and organizations. “These campaigns exploit the natural human desire for career advancement and new opportunities. Threat actors craft convincing job postings, set up seemingly legitimate front companies, and engage targets through professional channels like LinkedIn.”

She says the aim is to build trust and credibility, ultimately delivering malware payloads that provide persistent access to target systems and networks. This access can then be leveraged for espionage, data theft, and other malfeasance, often targeting industries and

sectors of strategic importance.

An Ounce of Prevention

To mitigate the risk of falling victim to these job lure campaigns, Jones says job applicants and employers must exercise vigilance and adopt robust security measures.

She advises job applicants to be cautious of unsolicited job offers, especially those that seem too good to be true, and to thoroughly research the company, role, and recruitment process before engaging. Also, they should verify the company's website, social media presence, and other publicly available information, and finally trust their instincts. "If something feels off, it's better to err on the side of caution."

When it comes to employers, Jones advises to implement comprehensive security awareness training for employees, educating them on social engineering tactics, and to monitor for suspicious activity, such as unusual job application patterns or unusual network traffic. Moreover, she says to maintain incident response plans, and collaborate with cybersecurity providers and threat intelligence sources. Finally, consider implementing additional security controls, such as email filtering, network segmentation, and multi-factor authentication.

By staying vigilant, verifying information, and leveraging a multilayered security approach, both job seekers and employers can enhance their resilience against these evolving job lure campaigns orchestrated by sophisticated threat actors like TA455, Jones ends.

About the Author



Kirsten Doyle

Information Security Buzz News Editor

Kirsten Doyle has been in the technology journalism and editing space for nearly 24 years, during which time she has developed a great love for all aspects of technology, as well as words themselves. Her experience spans B2B tech, with a lot of focus on cybersecurity, cloud, enterprise, digital transformation, and data centre. Her specialties are in news, thought leadership, features, white papers, and PR writing, and she is an experienced editor for both print and online publications.

The opinions expressed in this post belongs to the individual contributors and do not necessarily reflect the views of Information Security Buzz.