مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

United Arab Emirates

"Dream Job" Campaign Targeting Aerospace and Defense Sectors

Tracking #:432316518

Date:15-11-2024

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed security researchers has uncovered a persistent and evolving cyber espionage campaign attributed to the Iranian APT group TA455,uses a highly sophisticated "Dream Job" lure targeting individuals in the aerospace, aviation, and defense industries.

TECHNICAL DETAILS:

Security Researchers has uncovered a persistent and evolving cyber espionage campaign attributed to the Iranian APT group TA455 (also known as Charming Kitten, APT35, Smoke Sandstorm, and BOHRIUM). The campaign, which has been active since at least September 2023, uses a highly sophisticated "Dream Job" lure targeting individuals in the aerospace, aviation, and defense industries

This campaign involves social engineering tactics through fake recruitment offers and malware distribution, particularly focusing on SnailResin malware, delivered via DLL side-loading attacks and hidden within ZIP files.

The group is employing advanced obfuscation techniques, leveraging trusted platforms like LinkedIn and Cloudflare to evade detection and maintain persistence. The campaign shares significant similarities with North Korean Lazarus Group operations, indicating possible cross-collaboration or shared tactics and tools. The targeted organizations are also located in the United Arab Emirates (UAE).

Threat Overview:

1. Iranian "Dream Job" Campaign:

The "Dream Job" campaign uses a combination of social engineering and malware delivery techniques to infiltrate organizations in sensitive industries. The adversary lures victims by offering fake job opportunities, primarily targeting individuals within the aerospace, aviation, and defense sectors.

2. Malware Deployment – SnailResin:

The malware used in this campaign, identified as SnailResin, is distributed through spear-phishing emails that contain malicious ZIP file attachments. The ZIP file (signedconnection[.]zip) is typically disguised as a job-related document and is hosted on fake recruitment websites like careers2find[.]com, which masquerades as a legitimate job board for aerospace industry professionals.

The malware is designed to exploit DLL side-loading vulnerabilities, enabling remote execution of the malicious payloads once the user interacts with the infected file. The SnailResin malware is a multi-stage infection that aims to establish persistent access and exfiltrate sensitive data.

3. Impersonation of Other Threat Actors:

TA455 is deliberately mimicking tactics used by North Korean APTs such as Lazarus and Kimsuky. This misattribution is designed to confuse threat intelligence efforts and hinder accurate identification of the Iranian group's activities. The use of similar attack scenarios, including the DLL search order hijacking technique, underscores the growing sophistication and adaptability of the TA455 group.

4. Techniques for Evasion and Persistence:
TA455 utilizes various techniques to evade detection and maintain persistent access within compromised networks:

Obfuscation: They employ high-level obfuscation and custom malware to bypass traditional detection tools and evade signature-based antivirus engines.
Use of Trusted Platforms: The group hides its infrastructure behind services like Cloudflare, GitHub, and Microsoft Azure, using legitimate traffic to conceal command-and-control (C2) communications.
Multi-Stage Infection: The malware undergoes multiple stages, where the initial payload retrieves further instructions and tools from compromised legitimate services, making detection more difficult.

Indicators of Compromise:

Files (SHA-1):
2a29ba7302024ec1255811abec2a532136d12fef
3a0b3426f4a2f85e0c82b2804aab7f5d5bb63fb7
1acd34fb6de5c645e03ded9875046979be7893c4
2e7fc6d63ce16075a3fe3584e03be24a9bc220e1
aa5fcea406edd406bd6e0a23e83beebe2b3582d1
c52beb64f7450fce923d15efaa1e5be4c0e43d2b
IP:
185[.]186[.]244[.]130
89[.]221[.]225[.]249
DOMAIN:
careers2find[.]com
xboxapicenter[.]com
SHA-256:
918e70e3f5fdafad28effd512b2f2d21c86cb3d3f14ec14f7ff9e7f0760fd760
bf308e5c91bcd04473126de716e3e668cac6cb1ac9c301132d61845a6d4cb362
88097e4780bfdc184b16c5a8a90793983676ad43749ffca49c9d70780e32c33a
73b95960a683a6c4ffc7e213b409e4089c70dc53020d7b04cf47c3db2a87bd3a
d6048c65e0dae602043c1d4b86477996cde46d084c30cb28723b93a2ff40fe4a
18ddf0b17618f91e922b5afa9b10a764df51cda4ddfd657f9da1c9dfb1e6442b

RECOMMENDATIONS:

- Implement Endpoint Protection and Network Monitoring:
  - Ensure that Endpoint Detection and Response (EDR) solutions are in place to detect and mitigate multi-stage infections and DLL side-loading attacks.
  - Enhance monitoring capabilities to detect suspicious activities, particularly those involving C2 communications through Cloudflare and GitHub.
- Educate and Train Employees:
  - Awareness training should be conducted to ensure employees are aware of the risks of spear-phishing and social engineering tactics. This includes being cautious about unsolicited job offers or communications from unknown recruiters.
  - Emphasize the importance of verifying LinkedIn profiles, especially those linked to job

offers in the aerospace, defense, and aviation sectors.

- Enhance Malware Detection:
  - Utilize advanced anti-malware solutions that can detect and block obfuscated malware and files disguised as legitimate documents (e.g., ZIP files with embedded malicious payloads).
  - Implement file integrity monitoring to detect unauthorized modifications to system files, particularly in areas where DLL side-loading attacks could occur.
- Strengthen Network Defenses:
  - Implement web application firewalls (WAFs) to block access to malicious domains such as careers2find[.]com and prevent C2 traffic from reaching attacker-controlled infrastructure.
  - Geo-fencing can be used to restrict access from high-risk regions or IP addresses known to be associated with adversary activity.
- Review and Update Threat Intelligence:
  - Stay informed by regularly reviewing cyber threat intelligence reports from sources to track evolving tactics, techniques, and procedures (TTPs) used by TA455 and other Iranian APT groups.
  - Subscribe to threat intelligence feeds that provide real-time updates on malicious domains and IP addresses associated with these attacks.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://www.clearskysec.com/wp-content/uploads/2024/11/Iranian-Dream-Job-ver1.pdf