مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

# Threat Actor UNC1549 targets aerospace and defense sectors in Israel and the Middle East

Tracking #:432315662
Date:29-02-2024

## EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed suspected Iran-linked threat actor UNC1549 targeting aerospace, aviation, and defense industries in the Middle East, specifically Israel and the UAE, with potential impacts on Turkey, India, and Albania.

## TECHNICAL DETAILS:

UNC1549 (a.k.a. Tortoiseshell, Smoke Sandstorm, Imperial Kitten) is an Iran state-sponsored group and has been active since at least early 2019, and pursues targets in the Energy & Utilities, Defense, Technology and Government sectors in Middle East region. The activities or techniques followed by UNC1549 overlaps with Tortoiseshell, and Smoke Sandstorm/BOHRIUM threat groups.

- Suspected Iranian espionage activity targeting the aerospace, aviation, and defense industries in Middle East countries, including Israel and the United Arab Emirates (UAE), and potentially Turkey, India, and Albania.
- This activity is attributed to the Iranian actor UNC1549, which overlaps with Tortoiseshell, a threat actor publicly linked to Iran's Islamic Revolutionary Guard Corps (IRGC). The focused targeting of Middle East entities affiliated with the aerospace and defense sectors is consistent with other Iran-nexus clusters of activity, some of which are affiliated with the IRGC.
- This campaign remains active as of February 2024, and targeted entities are related to defense, aerospace, and aviation in the Middle East, particularly in Israel and the UAE.
- The potential link between this activity and the Iranian IRGC is noteworthy given the focus on defense-related entities and the recent tensions with Iran in light of the Israel-Hamas war. observed an Israel-Hamas war-themed campaign that masquerades as the "Bring... In addition, the focused targeting of Middle East entities affiliated with the aerospace and defense sectors is consistent with other Iran-nexus clusters of activity, some of which are affiliated with the IRGC as well.
- Research indicates this campaign remains active as of February 2024, and targeted entities are related to defense, aerospace, and aviation in the Middle East, particularly in Israel and the UAE and potentially in Turkey, India, and Albania.
- The attacks involve the use of Microsoft Azure cloud infrastructure for command-and-control (C2) and social engineering. The evasion methods used in this campaign, such as tailored job-themed lures combined with the use of cloud infrastructure for C2, make it challenging for network defenders to prevent, detect, and mitigate this activity.
- UNC1549 uses spear-phishing emails with malicious attachments or links to websites designed to steal credentials and infect devices.
- Use of legitimate-looking websites and decoy documents.
- Malware includes custom backdoors and data exfiltration tools.

## INDICATORS OF COMPROMISE(IOCs):

- Attached in Excel File

## RECOMMENDATIONS:

- Block the attached IOCs on network and use the latest Threat Intelligence data to stay aware of actual TTPs and IOCs used by threat actors.
- Regularly update all software, including operating systems and applications, to patch vulnerabilities.
- Implement strong authentication methods, such as multi-factor authentication (MFA), for all critical systems and applications.
- Monitor network traffic for unusual or suspicious activities using intrusion detection systems (IDS) and intrusion prevention systems (IPS).
- **Network Security:** Review and enhance network security by closing unused ports, removing unnecessary applications, and monitoring for suspicious activity.
- **Endpoint Protection:** Install and maintain reputable endpoint protection solutions that include behavioral detection capabilities.
- **Secure Backups:** Maintain offline, immutable backups of critical data. Regularly test restoration procedures.
- **User Awareness Training:** Educate employees on phishing, social engineering, and secure password practices.

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.mandiant.com/resources/blog/suspected-iranian-unc1549-targets-israel-middle-east