CYBERATTACKS & DATA BREACHES

DARKREADING GLOBAL

Breaking cybersecurity news, news analysis, commentary, and other content from around the world, with an initial focus on the Middle East & Africa.

Iran's APT34 Hits UAE With Supply Chain Attack

The prolific APT, also known as OilRig, was caught targeting an IT company's government clients in the region, with the aim of carrying out cyber espionage.

Dan Raywood, Senior Editor, Dark Reading

August 3, 2023

2 Min Read

The Iran-linked advanced persistent threat known as APT34 is at it again, this time mounting a supply chain attack with the ultimate goal of gaining access to government targets inside the United Arab Emirates (UAE).

Maher Yamout, lead security researcher of the EEMEA Research Center at Kaspersky, says the attackers used a malicious IT job recruitment form as a lure. APT34 (aka OilRig) created a fake website to masquerade as an IT company in the UAE, sent the recruitment form to a target IT company, and when the victim opened the malicious document to presumably apply for the advertised IT job, info-stealing malware executed.

Yamout says the malware collected sensitive information and credentials that allowed APT34 to access the IT company clients' networks. He explains that the attacker then specifically looked to target government clients, using the victim IT group's email infrastructure for command-and-control (C2) communication and data exfiltration. Kaspersky couldn't verify if the government attacks were successful due to its limited downstream visibility, but "we assess to medium-high confidence" that they were, Yamout says, given the group's typical success rate.

According to the research by Kaspersky, the malware samples used in the UAE campaign resembled those used in a previous APT34 supply chain intrusion in Jordan that used similar tactics, techniques, and procedures (TTPs), including targeting government entities. In that instance, Yamout says he suspected LinkedIn was used to deliver a job form while impersonating an IT company's recruitment effort.

The job recruiter gambit is a tactic that has been used by numerous cyberattack outfits over the years, including by North Korea's Lazarus group in more than one instance, and cyberattackers purporting to be military recruiters.

Actions From a Repeat Cyberattack Offender

APT34 is an Iranian threat group operating primarily in the Middle East by targeting organizations in this region that are in a variety of different industries. It has previously been linked to other cyber-surveillance activities, such as an attack on UAE earlier this year.

It often carries out supply chain attacks, where the threat group leverages the trust relationship between organizations to attack their primary targets, systematically targeting specific organizations that appear to be carefully chosen for strategic purposes.

compromised accounts, sometimes coupled with social engineering tactics.

"We assess that APT34 works on behalf of the Iranian government based on infrastructure details that contain references to Iran, use of Iranian infrastructure, and targeting that aligns with nation-state interests," Mandiant noted in its report. It's an assessment shared by the US government, which sanctioned Iran last year over APT34's activities.

Read more about:

DR Global Middle East & Africa

About the Author(s)

Dan Raywood, Senior Editor, Dark Reading

With more than 20 years experience of B2B journalism, including 12 years covering cybersecurity, Dan Raywood brings a wealth of experience and information security knowledge to the table. He has covered everything from the rise of APTs, nation-state hackers, and...

You May Also Like

More Insights

Webinars

What's In Your Cloud?
JAN 17, 2024

Everything You Need to Know About DNS Attacks
JAN 18, 2024

Tips for Managing Cloud Security in a Hybrid Environment
FEB 01, 2024

Top Cloud Security Threats Targeting Enterprises
FEB 08, 2024

DevSecOps: The Smart Way to Shift Left
FEB 14, 2024

More Webinars

Events

Black Hat Asia - April 16-19 - Learn More

Black Hat Spring Trainings - March 12-15 - Learn More

Cyber Resiliency 2023: How to Keep IT Operations Running, No Matter What

More Events