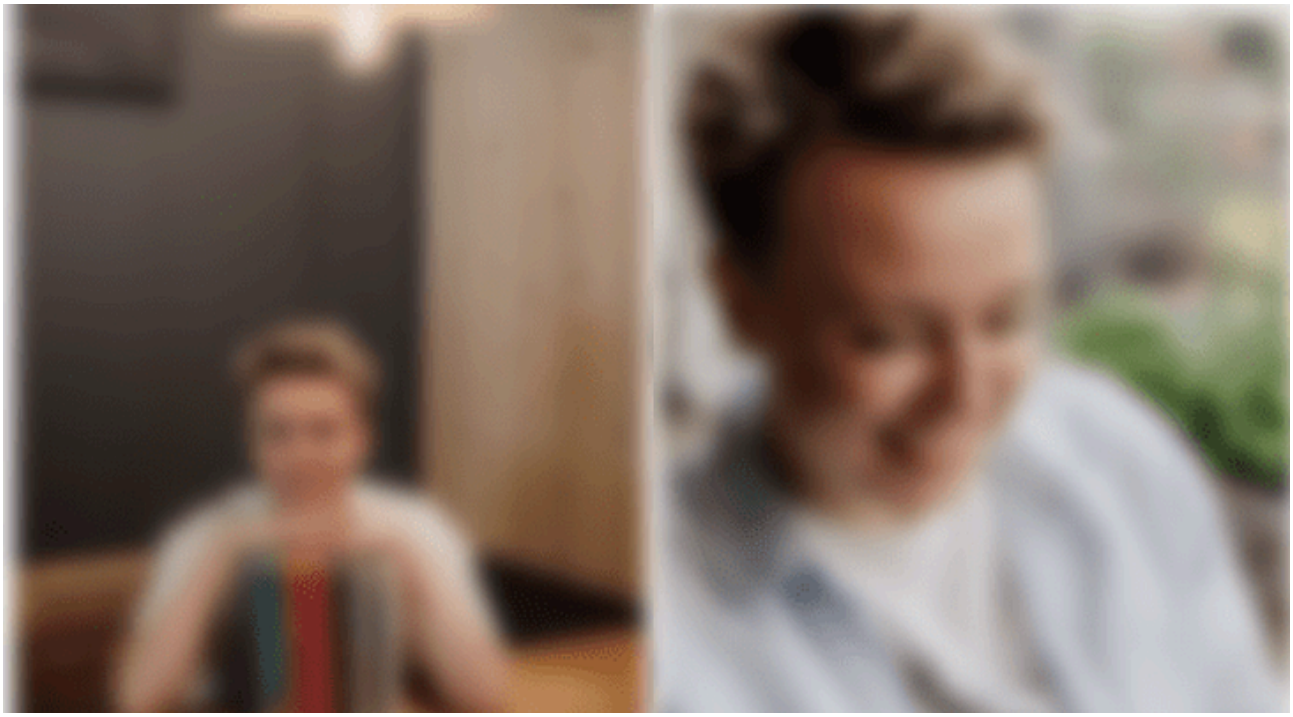
Iranian Hackers Target Women Involved in Human Rights and Middle East Politics

By The Hacker News

Published: 2023-03-09 · Archived: 2026-04-05 17:35:15 UTC



Iranian state-sponsored actors are continuing to engage in social engineering campaigns targeting researchers by impersonating a U.S. think tank.

"Notably the targets in this instance were all women who are actively involved in political affairs and human rights in the Middle East region," Secureworks Counter Threat Unit (CTU) said in a report shared with The Hacker News.

The cybersecurity company attributed the activity to a hacking group it tracks as **Cobalt Illusion**, and which is also known by the names APT35, Charming Kitten, ITG18, Phosphorus, TA453, and Yellow Garuda.

The targeting of academics, activists, diplomats, journalists, politicians, and researchers by the threat actor has been well-documented over the years.

The group is suspected to be operating on behalf of Iran's Islamic Revolutionary Guard Corps (IRGC) and has exhibited a pattern of using fake personas to establish contact with individuals who are of strategic interest to the government.

"It is common for Cobalt Illusion to interact with its targets multiple times over different messaging platforms," SecureWorks said. "The threat actors first send benign links and documents to build rapport. They then send a malicious link or document to phish credentials for systems that Cobalt Illusion seeks to access."

Chief among its tactics include leveraging credential harvesting to gain control of victims' mailboxes as well as employing custom tools like HYPERSCRAPE (aka EmailDownloader) to steal data from Gmail, Yahoo!, and Microsoft Outlook accounts using the stolen passwords.

Another bespoke malware linked to the group is a C++-based Telegram "grabber" tool that facilitates data harvesting on a large scale from Telegram accounts after obtaining the target's credentials.

The latest activity involves the adversary passing off as an employee of the Atlantic Council, a U.S.-based think tank, and reaching out to political affairs and human rights researchers under the pretext of contributing to a report.

To make the ruse convincing, the social media accounts associated with the fraudulent "Sara Shokouhi" persona (@SaShokouhi on Twitter and @sarashokouhii on Instagram) have been tweeting or engaging with posts that are supportive of ongoing protests in Iran. The bios also claim Shokouhi has a PhD in Middle East politics.

What's more, the profile photos in these accounts, per Secureworks, are said to have been taken from an Instagram account belonging to a psychologist and tarot card reader based in Russia.

It's not immediately clear if the effort resulted in any successful phishing attacks. The Twitter account, created in October 2022, remains active to date as is the Instagram account.

"Phishing and bulk data collection are core tactics of Cobalt Illusion," Rafe Pilling, principal researcher and Iran thematic lead at Secureworks CTU, said in a statement.

"The group undertakes intelligence gathering, often human focused intelligence, like extracting the contents of mailboxes, contact lists, travel plans, relationships, physical location, etc. This intel is likely blended with other sources and used to inform military and security operations by Iran, foreign and domestic."

Found this article interesting? Follow us on Google News, Twitter and LinkedIn to read more exclusive content we post.
