COBALT ILLUSION Masquerades as Atlantic Council Employee

secureworks.com/blog/cobalt-illusion-masquerades-as-atlantic-council-employee

Counter Threat Unit Research Team

The phishing campaign targets researchers who document the suppression of women and minority groups in Iran. Thursday, March 9, 2023 *By: Counter Threat Unit Research Team*
Secureworks® Counter Threat Unit™ (CTU) researchers are investigating suspicious activity reported via Twitter on February 24, 2023. Multiple individuals involved in Middle Eastern political affairs research tweeted that than an individual claiming to work for the U.S. Atlantic Council think tank had contacted them about contributing to an Atlantic Council report in progress. This individual used the name Sara Shokouhi and the @SaShokouhi (archived) Twitter account (see Figure 1).

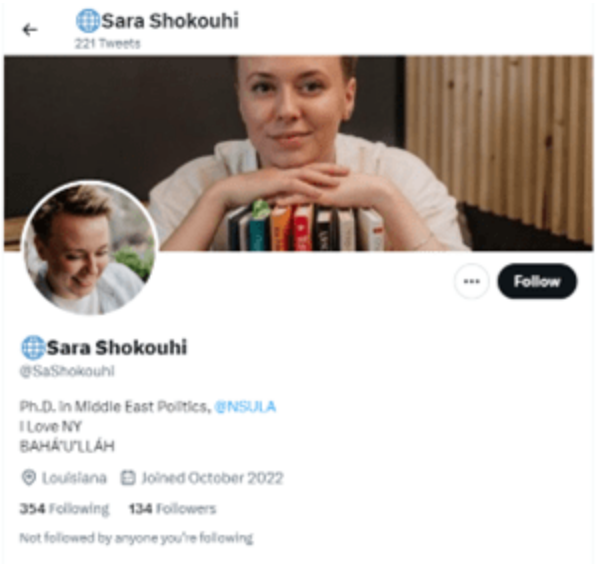

Figure 1. Twitter profile for Sara Shokouhi (@SaShokouhi). (Source: Secureworks)

In these solicitations, the SaShokouhi persona claimed to work with Holly Dagres, an Atlantic Council Senior Fellow. Dagres has publicly denied working with Shokouhi (see Figure 2).

Figure 2. Holly Dagres publicly denying that Sara Shokouhi is a colleague. (Source: Secureworks)

CTU™ researchers discovered that the individual in these photos is not Sara Shokouhi. The image belongs to a psychologist and tarot card reader based in Russia. The threat group responsible for the fake Sara Shokouhi persona stole these images from an Instagram account (see Figure 3) and used them as the basis for the SaShokouhi Twitter account and a corresponding Instagram account (@sarashokouhii). The fake Instagram profile claims Shokouhi was studying for or holds a “PhD in Middle East Polotics [sic]”.

Figure 3. Photos stolen from Instagram to create the @SaShokouhi Twitter persona. Secureworks blurred the images for privacy purposes. (Source: Secureworks)

Multiple hallmarks of this activity suggest involvement of the Iranian COBALT ILLUSION threat group (also known as Charming Kitten, APT42, Phosphorous, TA453, and Yellow Garuda), which is suspected of operating on behalf of the Intelligence Organization of the

Islamic Revolutionary Guard Corp (IRGC-IO) in Iran. COBALT ILLUSION targets a wide range of individuals and is particularly interested in academics, journalists, human rights defenders, political activists, intergovernmental organizations (IGOs), and non-governmental organizations (NGOs) that focus on Iran. The threat actors create a fake persona and then use it to contact a target with a request for an interview, assistance on a report, or to discuss a shared interest. Over a period of days or weeks, COBALT ILLUSION develops a rapport with the target and then attempts to phish credentials or deploy malware to the target's computer or mobile device. The UK National Cyber Security Centre (NCSC) issued an advisory in January that included details of COBALT ILLUSION spearphishing activity.

This would not be the first time the threat actors masqueraded as Atlantic Council employees. In September 2022, CERTFA identified numerous real individuals that COBALT ILLUSION impersonated, including an Atlantic Council employee. In that campaign, the group attempted to engage targets in video calls and delivered phishing links via the chat function at an appropriate point in the conversation.

The @SaShokouhi account has been operating since October 2022. It tweets or retweets posts supportive of the Mahsa Amini protests in Iran. To appear sympathetic to the protestors' interests and demands, the account owner has posted cynical content such as images of dead children, physical abuse suffered by protesters, anti-Iranian government commentary, and anti-Iranian symbolism.

CERTFA Lab reported a set of phishing indicators related to this suspicious activity. As of this publication, CTU researchers cannot independently verify an association between the CERTFA indicators and the @SaShokouhi account. However, these indicators align with patterns observed in past COBALT ILLUSION activity.

Multiple targets reported that the SaShokouhi persona engaged them in discussion (see Figure 4). The interactions included requests to visit multiple links.

Figure 4. Twitter user reporting that SaShokouhi had contacted them. (Source: Secureworks)

It is common for COBALT ILLUSION to interact with its targets multiple times over different messaging platforms. 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. These systems include online email services, social media services, and other systems used by the target.

Phishing and bulk data collection are core tactics of COBALT ILLUSION operations. In August 2022, Human Rights Watch reported that COBALT ILLUSION targeted their staff and obtained user credentials. The threat actors then used the Google Takeout service to export data from the various services associated with the compromised account, including email, cloud data storage, and contacts. This information could feed into additional rounds of phishing attacks, targeting users of interest who have had contact with the initial victim. In December 2021, the Google Threat Analysis Group (TAG) reported on COBALT ILLUSION's use of the custom HYPERSCRAPE (also known as EmailDownloader) tool to steal user data from Gmail, Yahoo, and Microsoft accounts. PwC identified a similar tool called TelegramGrabber that enabled bulk data collection from Telegram accounts after the threat actor had obtained the victim's credentials. Data stolen from victims' accounts could be used to inform intelligence priorities for the IRGC-IO and other COBALT ILLUSION customers.

To mitigate exposure to this malware, CTU researchers recommend that organizations use available controls to review and restrict access using the indicators listed in Table 1. Note that IP addresses can be reallocated. The domains and IP addresses may contain malicious content, so consider the risks before opening them in a browser.

Indicator	Type	Context
148.251.130.18	IP address	COBALT ILLUSION indicator published by CERTFA

Indicator	Type	Context
88.198.96.214	IP address	COBALT ILLUSION indicator published by CERTFA
46.4.95.242	IP address	COBALT ILLUSION indicator published by CERTFA
88.198.96.210	IP address	Hosting COBALT ILLUSION domains
88.198.96.211	IP address	Hosted COBALT ILLUSION domains
88.198.96.213	IP address	Hosted COBALT ILLUSION domains
node-dashboard.site	Domain name	COBALT ILLUSION indicator published by CERTFA
node-panel.site	Domain name	COBALT ILLUSION indicator published by CERTFA
stellar-stable-faith.top	Domain name	COBALT ILLUSION indicator published by CERTFA
funeral-engineering-expression.top	Domain name	COBALT ILLUSION indicator published by CERTFA
compact-miracle-abounds.top	Domain name	COBALT ILLUSION indicator published by CERTFA
live-redirect-system.top	Domain name	Suspected COBALT ILLUSION infrastructure
bonny-marvels-authentic.top	Domain name	Suspected COBALT ILLUSION infrastructure
review-status-plan.online	Domain name	Suspected COBALT ILLUSION infrastructure
sincerely-sensation-outdo.top	Domain name	Suspected COBALT ILLUSION infrastructure
progress-captivate-amply.top	Domain name	Suspected COBALT ILLUSION infrastructure

Table 1. Indicators for this threat.

Read more about Iranian threats in the 2022 State of the Threat report. If you need urgent assistance with an incident, contact the Secureworks Incident Response team.

Stay Informed

Get the latest in cybersecurity news, trends, and research

SEND ME UPDATES

Secureworks Taegis™

Security Analytics +
Human Intelligence
Delivers Better
Security Outcomes

About Taegis

Latest Report

Reports

2022 State of the Threat Report