Educated Manticore Reemerges: Iranian Spear-Phishing Campaign Targeting High-Profile Figures

By matthewsu

Published: 2025-06-25 · Archived: 2026-04-02 11:03:50 UTC

Amid growing warnings from agencies like the FBI and DHS about Iranian cyber activity, Check Point Research is sharing fresh, real-world examples from the past few days to shed light on how these threats are playing out in practice. We've identified the reemergence of an active, global spear-phishing campaign attributed to the Iranian threat actor Educated Manticore, also tracked as APT42, Charming Kitten, and Mint Sandstorm. Associated with the IRGC Intelligence Organization, this group is known to target public figures around the world. Currently, the campaign is executing sophisticated credential theft operations against high-profile individuals in Israel, while the real scope of the campaign is likely much wider, both geographically and by industry.

Following the escalation in Iran–Israel tensions, the group has intensified its efforts, this time impersonating Israeli institutions, diplomats, and tech professionals.

Wide-Reaching, Highly Targeted Campaign
This campaign marks a broader scope of Iranian cyber ops, using tailored spear-phishing creating fictitious personas tied to existing entities, precise timing, and multi-channel outreach to extract credentials and bypass MFA.

High-Value Targets: Academics, Journalists, and Beyond
We have observed attacks against:

- Leading Israeli computer science academics and cyber security researchers
- rominent journalists known for covering geopolitical and intelligence topics

While recent activity focuses on Israeli targets, Educated Manticore has a broader history of global operations. In the past, the group has masqueraded as prominent international media outlets and NGOs — including *The Washington Post* (US), *The Economist* (UK), *Khaleej Times* (UAE), *Azadliq* (Azerbaijan), and others — to phish journalists, researchers, and geopolitical figures in regions aligned with Iran's strategic interests. These operations follow the same pattern: trust-building through impersonation, followed by credential harvesting and surveillance.

Over 100 Registered Phishing Domains
We've identified over 100 phishing domains tailored to each target, with phishing pages often mimicking:

- Google, Outlook, and Yahoo
- The links have since been blocked and are no longer available
- Event scheduling or meeting platforms such as Google Meet

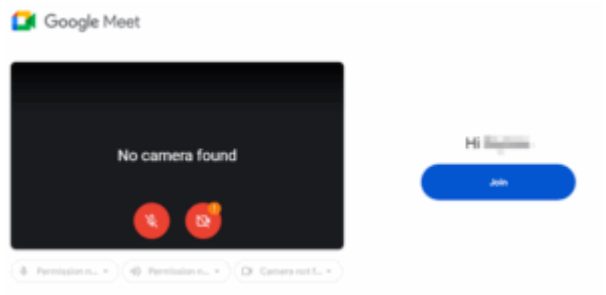

Figure 1: Fake image redirecting to the attackers' servers

Initial Contact Varies by Target

Attackers use multiple communication channels to initiate contact, including:

- Email addresses
- Private messaging apps (e.g., WhatsApp)

Figure 2: Fake image redirecting to the attackers' servers.

Figure 3: *A prominent reporter was targeted with messages purporting to be from one of the prime minister's advisors and a former Israeli ambassador to the United States (source: [Mako](#))*

The Phishing Flow: Fake Google Login or Meeting Invites
Once contact is established, victims are typically directed to:

- Fake Google sign-in pages, often pre-filled with their email address
- Fake Google Meet invitations hosted on phishing domains

These pages mimic legitimate login flows using advanced web development frameworks.

Bypassing 2FA: Social Engineering at Play
Educated Manticore also works to bypass 2FA by tricking victims into sharing them as part of the phishing chain, enabling full account takeover.

Proposal for Physical Meetings
In one incident, a target received a WhatsApp message inviting them to an in-person meeting in Tel Aviv. While the goal may have been to rush the victim to confirm an online session, this raises the concern that the campaign could extend beyond cyber space.

Tailored Impersonation: From Low-Level Staff to Major Institutions
The impersonation style is highly adaptive. In some cases, attackers pose as:

- Mid-level employees at major Israeli firms
- Staff from the Prime Minister's Office
- Professionals affiliated with well-known tech companies

Emails are grammatically correct, formally structured, and may have been assisted by AI tools. However, subtle inconsistencies, such as minor name misspellings, can give them away.

Recommendations
This evolving campaign poses a serious threat to academic, policy, and media sectors. Individuals should be cautious when receiving unsolicited meeting invitations, even from seemingly credible sources.

If You're in a High-Risk Sector:

- **Verify the identity of the sender or caller** using known channels like reliable social media accounts
- **Always verify the URL** before entering credentials into any site handling sensitive information
- **Enable and monitor 2FA** and be suspicious of any request to share codes
- **Report suspicious contact** to your organization's security team

Check Point Research continues to monitor this activity and will share updates as new indicators and techniques are uncovered. Check Point's Harmony Email and Collaboration and Zero Phishing protect customers by detecting and blocking such attacks and targeted phishing attempts.

Check out Check Point Research's report for a comprehensive understanding of the spear-phishing campaign.
