Iranian Cyber Actors Impersonate Model Agency in Suspected Espionage Operation

unit42.paloaltonetworks.com/iranian-attackers-impersonate-model-agency/

May 7, 2025

Executive Summary

Unit 42 recently identified suspected covert Iranian infrastructure impersonating a German model agency. This infrastructure hosted a fraudulent website designed to mimic the authentic agency's branding and content.

Visitors unknowingly triggered obfuscated JavaScript designed to capture detailed visitor information, such as:

- Browser languages
- Screen resolutions
- IP addresses
- Browser fingerprints

Attackers likely collected these data points to enable selective targeting.

The website replaces a real model's profile with a fake one, including a currently inactive link to a private album. This suggests preparation for targeted social engineering attacks, likely using the fake profile as a lure. We have not yet observed direct victim interaction, though it is possible victims would arrive at the fake website through spear phishing.

The operation's complexity, methods and targeting lead us to believe with high confidence that these are the actions of an Iranian threat group. With lower confidence, we suspect a group overlapping with Agent Serpens, also known as APT35 or Charming Kitten, is behind this campaign. This group is known for conducting espionage campaigns against Iranian dissidents, journalists and activists, particularly those living abroad.

In this article, we will cover details of the fake website's functionality, including the obfuscated data collection routines and the fictitious profile likely used for social engineering.

Individuals and organizations, particularly those involved with Iranian activist communities, should remain vigilant for similar operations and treat unsolicited contacts cautiously before engaging.

Palo Alto Networks customers are better protected through the following products and services:

- Advanced URL Filtering and Advanced DNS Security identify known domains and URLs associated with this activity as malicious.
- Advanced Threat Prevention has an inbuilt machine learning-based detection that can detect exploits in real time.

If you think you might have been compromised or have an urgent matter, contact the Unit 42 Incident Response team.

Related Unit 42 Topics **Iran**, **Phishing**

Technical Analysis of the Fake Mega Model Agency Site

While monitoring infrastructure we assess is likely tied to Iranian cyber actors, we discovered the domain megamodelstudio[.]com. This domain was registered on Feb. 18, 2025, and has resolved to 64.72.205[.]32 since March 1, 2025. This domain hosts a website impersonating the Hamburg-based Mega Model Agency, as illustrated in Figure 1.

Figure 1. Fake Mega Model Agency website.

This actor-created website closely replicates the actual website's branding, layout and content. However, the clone includes an obfuscated script designed to harvest detailed visitor information and potentially lure specific targets to a fictitious model's profile.

This fake website exhibits the hallmarks of social engineering attacks performed by known Iranian advanced persistent threat groups (APTs). Most notably, it appears to link to Agent Serpens, a threat actor that the security community has widely reported to perform espionage campaigns against individuals and organizations critical of the Iranian regime, including in Germany [PDF].

Upon visiting any page of the fake website, obfuscated JavaScript code runs in the victim's browser. The likely goal of the code is to enable selective targeting by determining sufficient device- and network-specific details about visitors.

The script performs the following tasks:

- Enumerating browser languages and plugins, retrieve screen resolution and collect timestamps to track a visitor's locale and environment
- Revealing the user's local and public IP address using WebRTC-based IP address leaking
- Leveraging canvas fingerprinting, using SHA-256 to produce a device-unique hash
    - Canvas fingerprinting is a technique that uses the HTML5 canvas element to identify unique characteristics about a user's device and generate a corresponding fingerprint
- Structuring the collected data (e.g., language, screen size, canvas hash) as JSON and delivering it to the endpoint /ads/track via a POST request
    - This naming convention suggests an attempt to disguise the collection as benign advertising traffic rather than storing and processing potential target fingerprints

In addition to its data collection routines, the fake website contains functionality designed to dynamically alter on-page references to a specific model and replace them with details and images of a model named "Shir Benzion." We assess that this replacement profile is likely fictitious and part of a social engineering tactic.

Attackers also inject a link to a private album into the profile for this fictitious model, though it appears to be non-functional at the time of writing. We assess that this is likely a placeholder intended for targeted social engineering attacks, potentially serving as a mechanism for harvesting credentials or delivering malware payloads. We illustrate these observations in Figures 2 and 3.

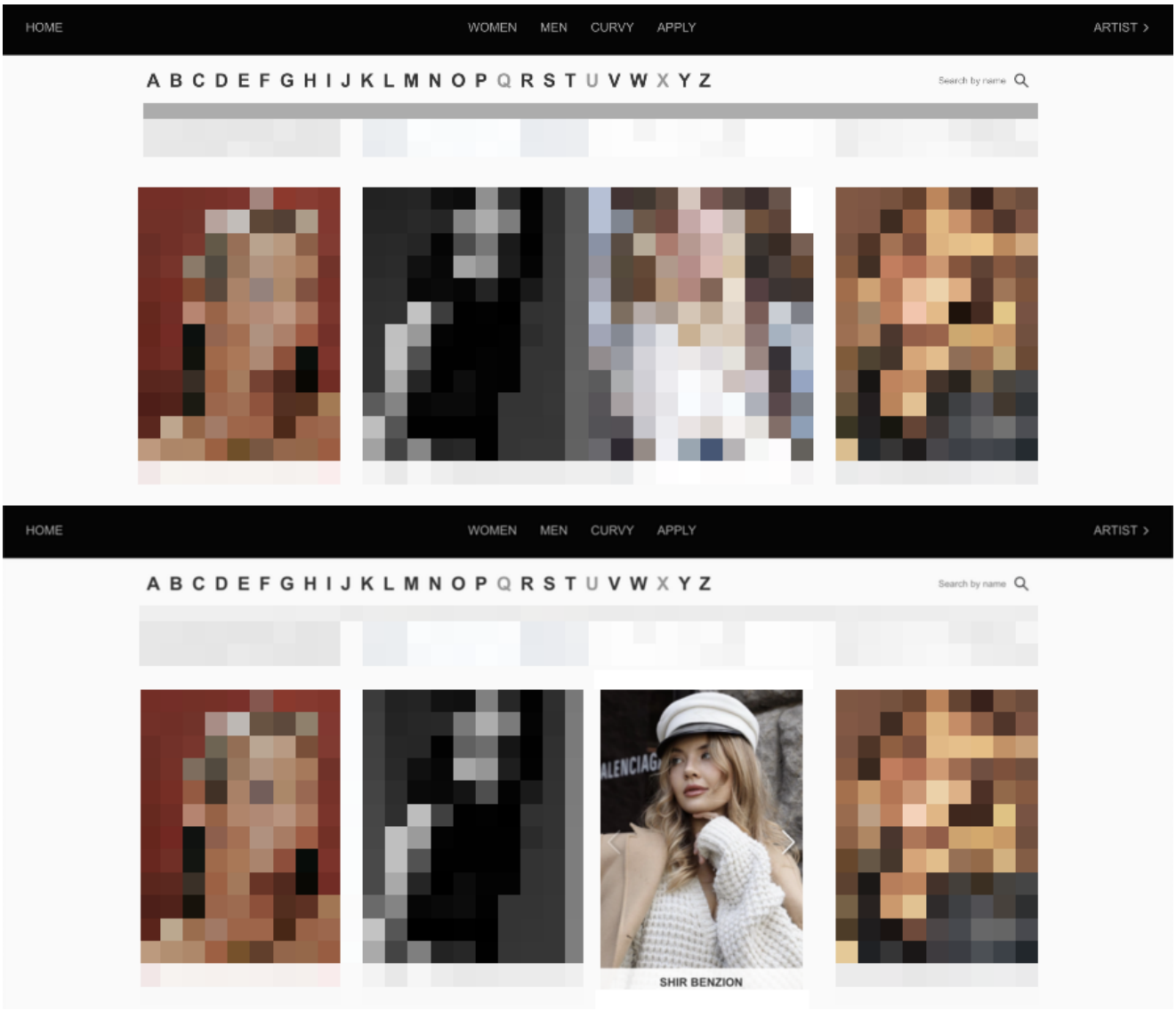

Figure 2. Top: Legitimate Mega Model Agency women's page. Bottom: Fake page with profile of a real model replaced by the fictitious "Shir Benzion" profile.

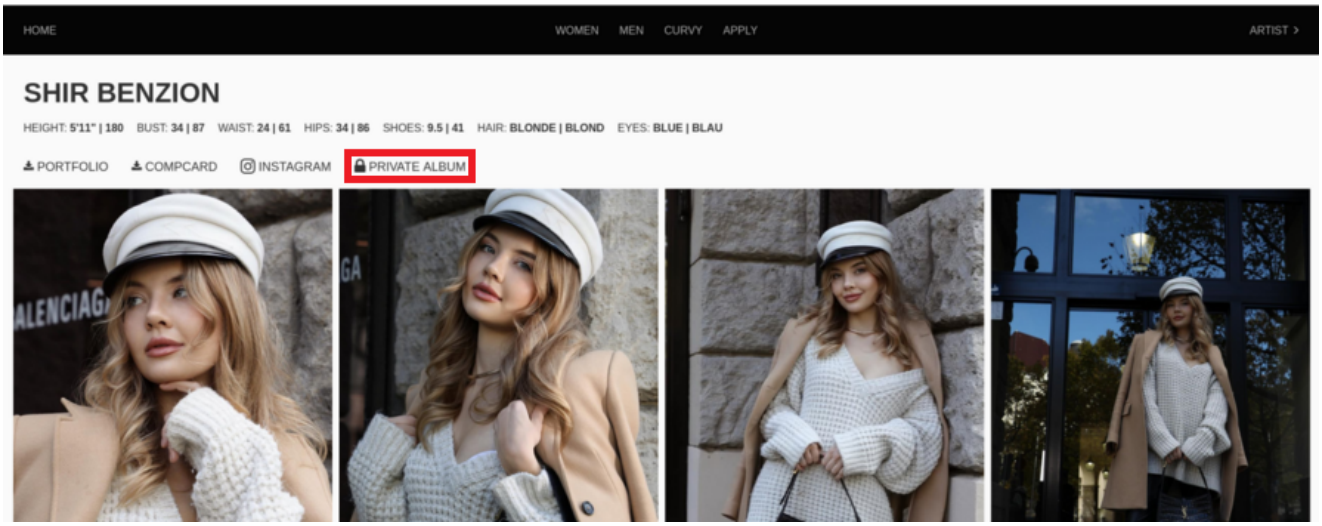

Figure 3. Fictitious "Shir Benzion" profile with private album lure.

The fake website's current functionality, combined with the potential for further malicious development, indicates that this campaign is both an ongoing and evolving threat.

Conclusion

This operation, involving detailed visitor profiling and sophisticated impersonation tactics, demonstrates a continued escalation in suspected Iranian cyberespionage activity. Such activities present significant risks to various organizations and individuals, such as those advocating for or supporting Iranian dissidents.

Individuals and organizations should treat unsolicited contacts offering seemingly appealing opportunities cautiously. People should independently verify the legitimacy of contacts, websites and offers before engaging or sharing sensitive information.

Palo Alto Networks customers are better protected from the threats discussed in this article through the following products and services:

- Advanced URL Filtering and Advanced DNS Security subscriptions for the Next-Generation Firewall identify known domains and URLs associated with this activity as malicious.
- Advanced Threat Prevention has an inbuilt machine learning-based detection that can detect exploits in real time.

If you think you may have been compromised or have an urgent matter, get in touch with the Unit 42 Incident Response team or call:

- North America: Toll Free: +1 (866) 486-4842 (866.4.UNIT42)
- UK: +44.20.3743.3660
- Europe and Middle East: +31.20.299.3130
- Asia: +65.6983.8730
- Japan: +81.50.1790.0200
- Australia: +61.2.4062.7950
- India: 00080005045107

Palo Alto Networks has shared these findings with our fellow Cyber Threat Alliance (CTA) members. CTA members use this intelligence to rapidly deploy protections to their customers and to systematically disrupt malicious cyber actors. Learn more about the Cyber Threat Alliance.

Indicators of Compromise

- Domain: megamodelstudio[.]com
- Description: The domain pointing to the website impersonating Mega Model Agency
- IP address: 64.72.205[.]32

- Description: The IP address of the server hosting the fake Mega Model Agency website
- URL: hxxps://www.megamodelstudio[.]com/model
- Description: The URL for the main page of the fake Mega Model Agency website
- URL: hxxps://www.megamodelstudio[.]com/women
- Description: The URL for the women's page of the fake Mega Model Agency website
- URL: hxxps://www.megamodelstudio[.]com/women/Shir-Benzion
- Description: The URL for the fictitious "Shir Benzion" profile

Additional Resources

[PDF] — Bundesamt für Verfassungsschutz (Federal Office for the Protection of the Constitution)