Iran’s Cyber Threat Intelligence

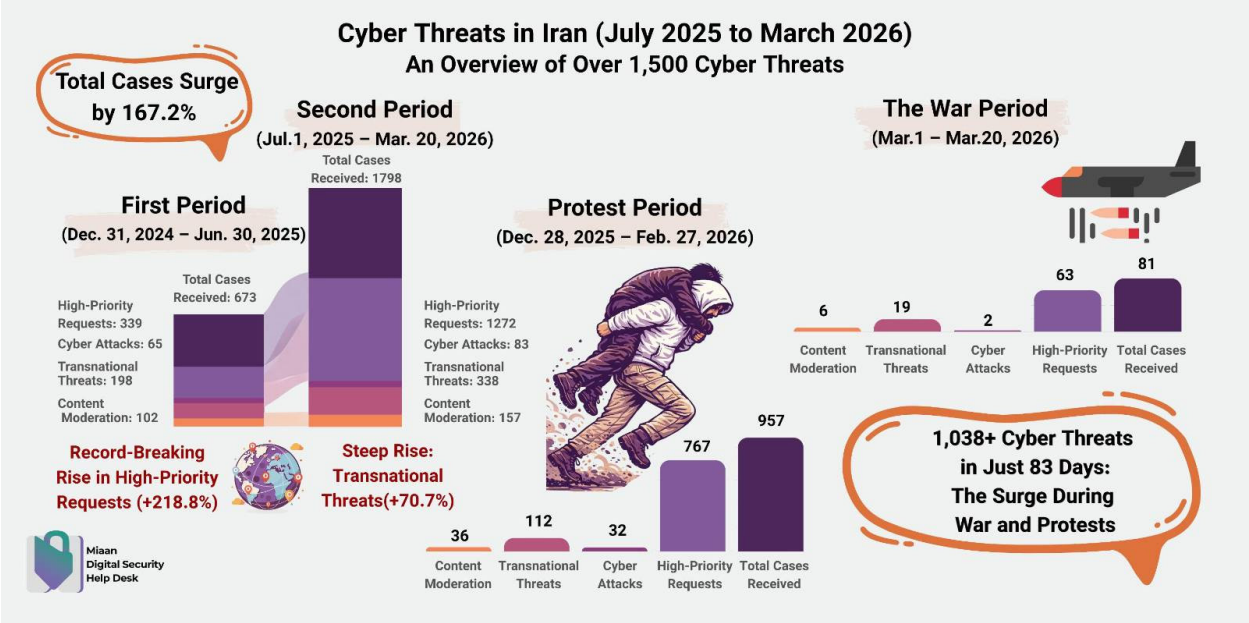
From Massacre to War;

Escalation of Cyber and Transnational Repression Amidst Digital Blackout

March 2026

Executive Summary and Trends

The third installment of the Iran Cyber Threats report series has been published following a delay caused by the rapid developments of the **Dey protests (late December 2025–January 2026)** and escalating military tensions. Given the sensitivity of this period and the emergence of new threat patterns, the data collection for this report was exceptionally expanded to cover an eight-month window from **July 2, 2025, to March 21, 2026**. This report is being released while Iranian users' right to internet access has been violated for more than 25 consecutive days during the ongoing conflict involving Israel, the United States, and Iran.



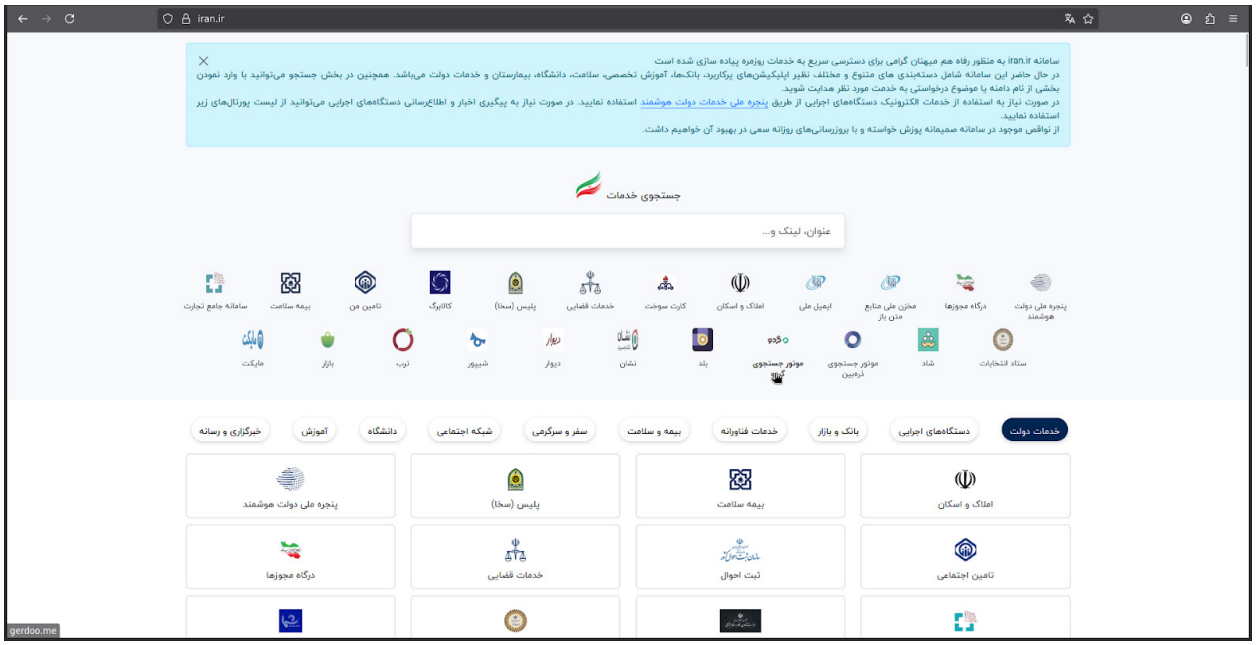
Data from July 2 to December 30, 2025, indicates a paradigm shift in digital repression, particularly regarding its transnational reach. During this period, the volume of cyber threats increased by 15% compared to the previous six months. At the same time, requests for digital security consultations surged by 67%, reflecting heightened anxiety among users—including those not personally targeted—both inside and outside of Iran.

A critical turning point occurred during the nationwide Dey protests (late December 2025–January 2026). Despite a total 10-day internet blackout, digital repression expanded beyond Iran's borders through various threats against activists abroad. Notably, digital rights violations during this month increased by 500% compared to the same period last year, demonstrating a powerful synergy between domestic and transnational repression tools.

From Blackout to Whitelist: Iran's Evolving Internet Control Strategy

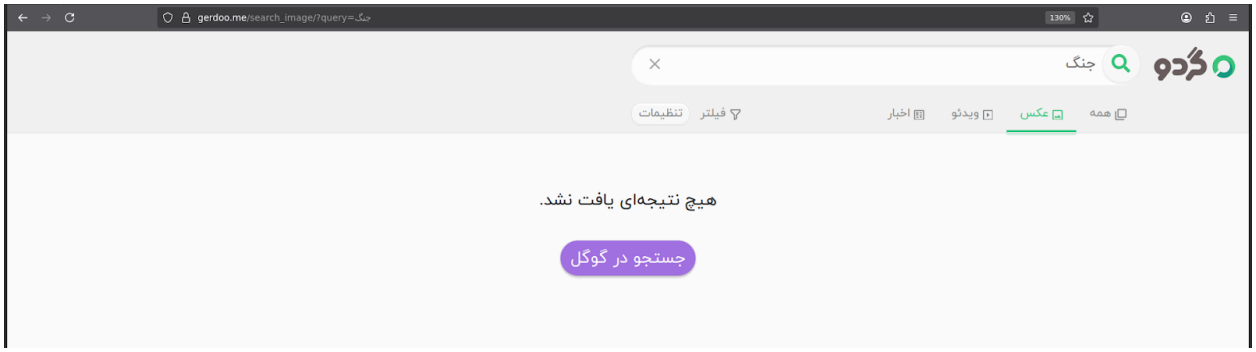
All of this is taking place under conditions where, from the protests in Dey (late December–January) until today, the internet in Iran has been shut down for more than 39 days.

Research by Filterwatch indicates that, given the Iranian government's new policies, there is no clear prospect of internet connectivity being restored. The government is rapidly expanding domestic services on the National Information Network (NIN). The website *Iran.ir* has become a central hub for this situation, with more services being introduced on it every day.

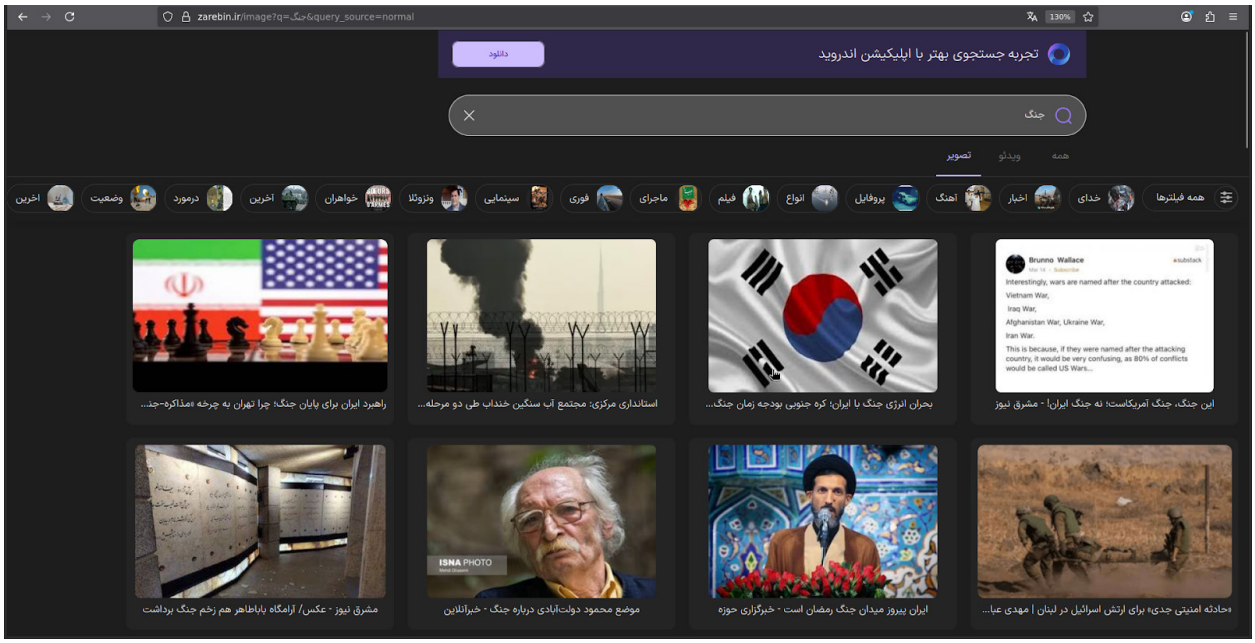


The development of whitelist-based access is ongoing, and this strategic shift from traditional censorship to a whitelist model has caused significant side effects: many domestic services either do not function properly or do not work at all. The National Information Network is extremely slow, and people are increasingly being pushed toward domestic platforms.

Severe censorship is being enforced on domestic search engines and all local platforms. Searching for keywords such as "war" or "ceasefire" on https://gerdoo.me/ yields no results in images, videos, or news sections—as if no war exists, not only in Iran but anywhere in the world.



In the https://zarebin.ir search engine, searching for the name "Mojtaba Khamenei" returns only results that focus on his power and wealth outside Iran. Similarly, searching for the keyword "war" produces content that presents a narrative of Iran's decisive victory in the conflict.



Each gigabyte of VPN access that can connect users to the internet—whether via whitelisted servers or Starlink—is being sold for between 1 and 3 million tomans (approximately 6–24 USD), a cost **5–20 times higher than the global average for one gigabyte**, effectively turning internet access into a luxury commodity that many people cannot afford.

At the same time, the price of internet packages offered by telecom operators has also increased, although this traffic does not provide access to the global internet and can only be used to access services on the National Information Network.

Most Significant Events:

- **Abduction Attempt:** A plot to deceive a London-based journalist and lure him to Iraq for the purpose of kidnapping.
- **Infiltration Attempts:** Targeting a London-based television network supportive of Reza Pahlavi.
- **Account Theft:** Targeted attempts to compromise the online accounts of Iranian-American and Iranian-British journalists in New York and London.
- **Website Disruption:** An attempt to disable the website of a Paris-based human rights organization affiliated with a prominent Iranian activist.
- **Impersonation:** Widespread impersonation of high-profile human rights advocates.
- **Malicious Code Delivery:** Distribution of malicious JavaScript via live television streaming links.
- **MahsaAlert Disruption:** Intentional interference with the MahsaAlert platform.

- **Regional Expansion:** Extension of transnational threats to Iraqi civil society groups opposing the Islamic Republic's regional policies.
- **Starlink Crackdown:** Numerous arrests related to Starlink usage; however, these primarily resulted from lapses in basic communication security rather than advanced technical tracking.
- **Android Malware:** Discovery of a large-scale cyberattack campaign utilizing sophisticated Android malware.

During this period, we witnessed the emergence and intensification of complex, multi-layered transnational threats. These began with Distributed Denial of Service (DDoS) attacks against the websites of prominent Iranian human rights activists—using infrastructure linked to the Iranian government—and extended to the targeted distribution of malware via platforms like Telegram.

Attackers also utilized phishing links to gain unauthorized access to the accounts of high-profile Iranian-American journalists, highlighting a clear focus on targets outside Iran's geographic borders. Furthermore, the use of Artificial Intelligence (AI) tools to generate and disseminate disinformation, along with the doxxing of activists and Iranians living abroad, has added new and dangerous dimensions to these threats.

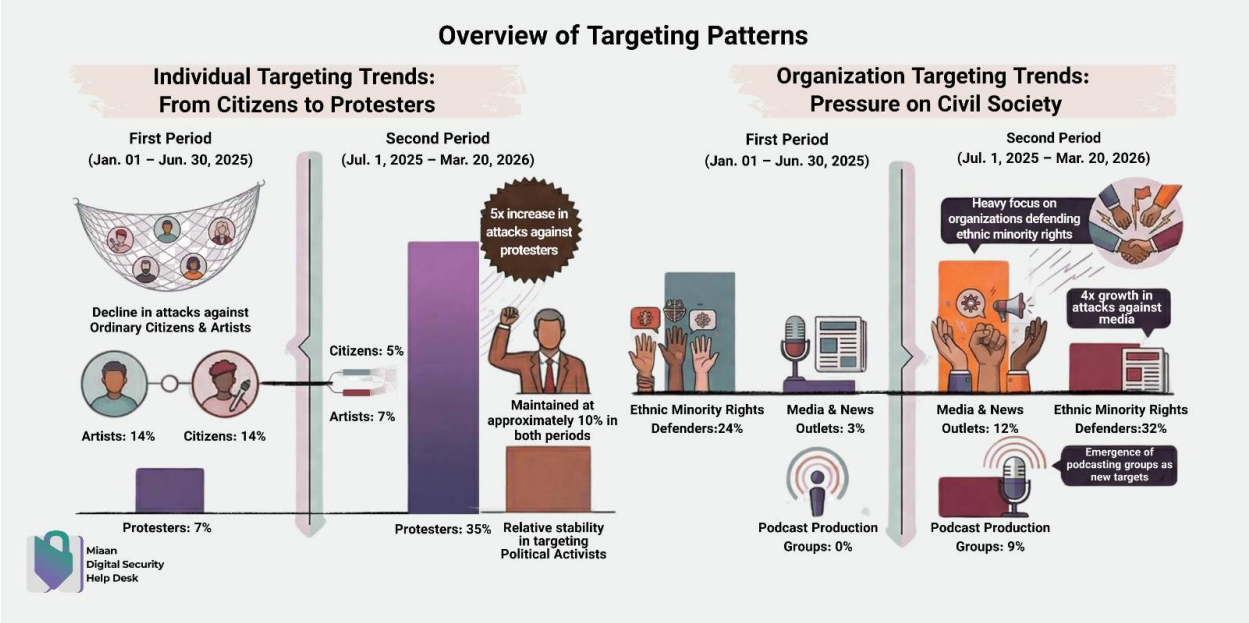
These actions, paired with public threats from Iranian officials on state-run radio and television, signify the emergence of a systematic pattern of "transnational repression". This phenomenon combines cyber, intelligence, and media tools to reach a level of complexity and scale that distinguishes it from previous years.

Dominant Attack Patterns:

- **Impersonation:** Posing as trusted platforms such as Meta, Facebook, WhatsApp, Gmail, and Telegram.
- **Infrastructure Abuse:** Exploiting legitimate or semi-legitimate infrastructure to increase the perceived credibility of the attack.
- **Infrastructure Masking:** Using newly registered domains, cloud email services, shortened links, and cover domains to hide malicious intent.
- **Targeting:** Concentrating efforts on activists, journalists, advocates, and individuals with public roles or sensitive professional connections.
- **State-Linked Evidence:** Technical and content-based indicators frequently suggest these attacks are linked to actors aligned with the Iranian government or utilize domestic Iranian infrastructure.

Transnational Repression: Statistics and Trends

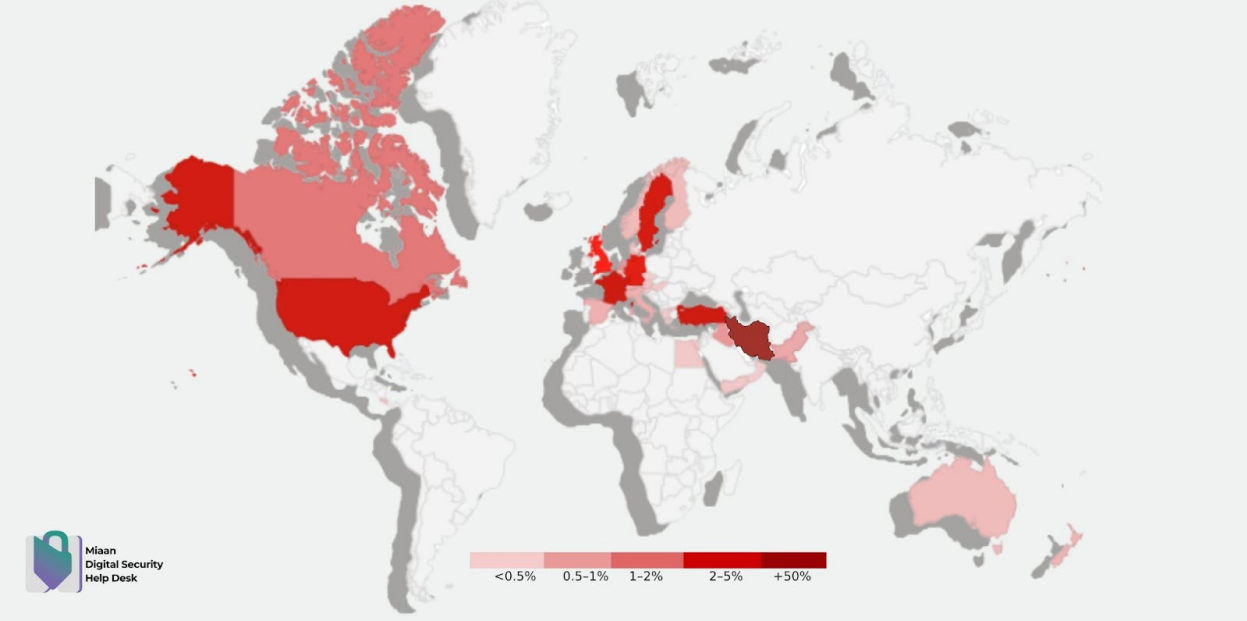
The Islamic Republic has significantly expanded its digital repression beyond Iran's borders. Nearly **30%** of all cases recorded between July 2 and December 30, 2025, involved diaspora civil activists and targets located outside of Iran.



Geographic Distribution and Growth

The report identifies a global reach for these threats, with the primary target countries being the United Kingdom, United States, Sweden, Turkey, Germany, and France.

- **United Kingdom**: Remains the top target due to the concentration of Persian-language media outlets.
- **Turkey:** Saw a 3.3% increase in the share of attacks, likely linked to the rising rate of Iranian migration and increased diaspora activity there.
- **Germany:** Recorded a significant rise in threats. Referrals from Germany increased by 15% starting in late December 2025 (Dey protests). This figure surged further to 26% during the Esfand war period (February–March 2026). This targeting is attributed to the high activity of opposition groups, including republicans and monarchists, residing there.
- **United States:** Saw a slight decrease of 2% in its share of total attacks compared to the first half of the year.



Expanding the Circle of Repression

Transnational threats are no longer limited to the Iranian diaspora. The reporting period revealed attacks targeting:

- **Iraqi Civil Society**: 2% of cases involved Iraqi activists opposed to the Islamic Republic's regional policies.
- **Afghan Journalists:** 1.6% of cases targeted Afghan journalists opposed to both the Taliban and the Islamic Republic.

Targeted Organizations and Emerging Trends

The data shows a strategic shift in who is being targeted organizationally:

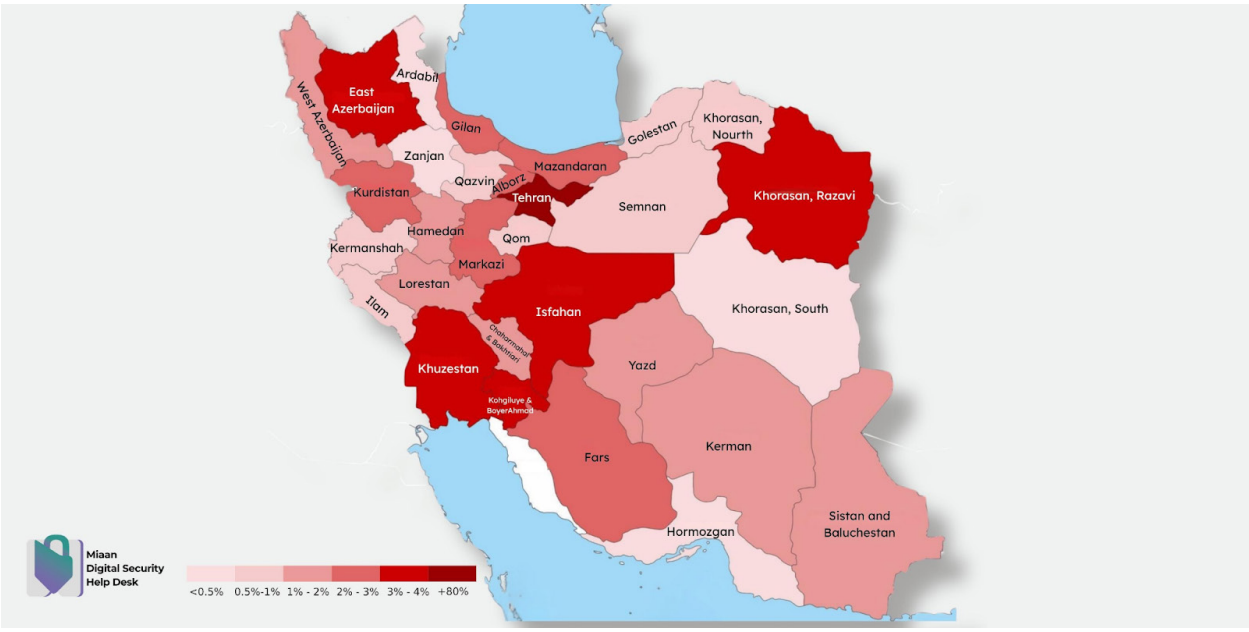
- **Ethnic Minority Rights Defenders:** Saw a heavy focus, with attacks increasing from 24% to 32%.
- **Media and News Outlets:** Experienced a 4x growth in attacks, rising from 3% to 12%.
- **Podcasting Groups:** Identified as a new target category, accounting for 9% of organizational attacks.

Special Case: Abduction Deception

A particularly alarming case involved an impersonation attempt designed to deceive a journalist and lure them to Iraq to facilitate a kidnapping or other transnational repression objectives.

Domestic Threats: Statistics and Trends

From July 2 to December 30, 2025, threats originating within Iran accounted for 71.6% of all recorded cases. This represents an 8% decrease compared to the previous period, with the shifting share of attacks moving toward targets in the United Kingdom and Turkey.



Provincial Distribution of Threats

While cyber threats were documented across the country, they remained concentrated in major political and economic centers:

- **Tehran Province**: Remains the primary target, accounting for 47% of all domestic reports, despite a 12% decrease compared to the first half of the year.
- **Secondary Hubs**: Following Tehran, the highest volumes of reports came from East Azerbaijan, Khuzestan, Isfahan, Kurdistan, and Sistan and Baluchestan.
- **Rising Growth:** The provinces of Fars, Markazi, and Khuzestan each saw a 3% increase in attack frequency.

Repression During the Protest Period (Late Dec. 2025 – Feb. 2026)

Concurrent with the nationwide Dey protests (late December 2025–January 2026), Miaan's "Emergency Help Desk" expanded its outreach, resulting in a shift in applicant patterns.

- **Surge in Enforcement:** Referrals related to arrests and device confiscations skyrocketed to 763 cases in just 31 days.

- **Geographic Breadth**: Requests were registered from 27 different provinces.
- **Major Reporting Centers:** Significant figures were recorded in Tehran (30%+), Isfahan, Razavi Khorasan, Kohgiluyeh and Boyer-Ahmad, and Alborz. Notably, 30% of applicants withheld their provincial location to ensure their personal security.

Repression During the "Esfand War" (Feb. – March 2026)

Following military escalations involving the U.S. and Israel, Tehran Province again saw a spike in activity.

- **Capital Surge:** Cases from Tehran rose by 2%, eventually constituting nearly 40% of all referred domestic cases.
- **Other Affected Regions:** High report volumes followed in Markazi, Isfahan, Mazandaran, Fars, Khuzestan, and Yazd.
- **Security Anonymity:** More than 32% of applicants chose not to disclose their province due to heightened security concerns during the conflict.

Digital Security Consultations and Public Anxiety

The reporting period saw a 67% jump in consultation requests, driven largely by state-sponsored disruptions and climate of fear.

- **Platform Specific Issues:** The primary drivers were account access and security failures, particularly on Instagram and WhatsApp.
- **Fear of Hacking:** Many users reported "suspicious activity" or account suspensions, leading to widespread fear that they were being actively targeted by security agencies.
- **OTP Blocking:** The Ministry of Communications intentionally blocked one-time-password (OTP) verification codes for the installation of Signal, Telegram, and Clubhouse, creating systemic obstacles for secure communication.
- **Device Checkups:** Following high-profile reports of hackers targeting journalists (such as those at Iran International), the Help Desk recorded a wave of requests for professional "device security checkups".

The Starlink Crackdown

The use of Starlink satellite internet was explicitly criminalized during the Twelve-Day War between Iran and Israel in June 2025. This provided a legal pretext for intensified judicial and security actions against satellite internet users during the total internet blackouts of both the Dey protests and the Esfand war.

Target Profiles: Individuals and Organizations

From July 2025 to March 2026, targeting patterns showed a clear focus on those with high social and professional capital:

- Individual Concerns: 35% of all requests related to general account security, followed by political activists at 11%.
- Organizational Targets: Ethnic minority rights organizations (32%) and human rights organizations (21%) remained at the top of the target list.
- Media Sector Growth: The share of attacks against media organizations rose sharply from 3% to 12%.
- Emerging Target: Podcast production groups were identified as a new target category, accounting for 9% of organizational attacks.

Attack Categorization

Phishing and Social Engineering

Phishing remained the most prevalent threat, accounting for approximately **39%** of all recorded cases between July 2 and December 30, 2025. The Help Desk recorded **54 unique cases**, representing a **45% growth** in phishing activity compared to the first half of the year.

Dominant Techniques and Success Rates

The primary vector for these attacks was the distribution of malicious links via Instagram direct messages, often using lures such as "art festival surveys" or "Meta copyright infringement notices." These campaigns achieved a 38% success rate, meaning nearly four out of every ten targets clicked the malicious link.

Miaan identified four key evolutionary patterns in these attacks:

1. **Platform Impersonation:** Attackers posed as support or legal teams from trusted brands like Meta, Facebook, WhatsApp, Gmail, and Telegram. Common themes included urgent warnings of account suspension, copyright claims, or fake job offers.
2. **Telegram-Specific Campaigns:** Sophisticated attempts were observed on Telegram, including the use of fake "support" bots (e.g., @AuthenticatorBot) and international phone calls to pressure victims into revealing credentials. In some instances, these led to full account takeovers and ownership transfers.
3. **Multi-Stage "Long Con" Phishing:** Some attackers avoided malicious links in the initial phase, instead focusing on building trust through believable pretexts such as university interviews, business collaborations, or invitations to human rights meetings. Once rapport was established, the attacker introduced the malicious link or request for sensitive data.

4. **Infrastructure Abuse:** Attackers bypassed security filters by exploiting legitimate digital trust chains, including the use of Amazon SES, link-shortening services (t.ly, shorten.ee), and high-reputation domains that successfully passed SPF, DKIM, and DMARC checks.

Malware

Android Malware

A report concerning a file named PDF.apk, which was suspiciously distributed via Telegram, was initially identified as an isolated sample. This file, designed to look like a standard PDF document, served as the starting point for the discovery of an extensive cyberattack campaign. Further analysis confirms this sample is part of a broader malware cluster rather than a stand-alone case. Evidence suggests additional undiscovered samples likely exist beyond those identified.

The identified samples are:

- PDF.apk
- Vision-3187.apk
- PDF-977.apk
- PDF-572.apk
- Unknown-8663.apk
- PhotoAi1.0 (1).apk
- Artificial Intelligence.apk
- PhotoAi-741.apk

All samples share the package name com.chvi.pool and belong to a single malware family and operational campaign, most likely managed by a specific individual or group.

Malware Cluster and Sample Correlation

Structural and behavioral analysis reveals that these samples are part of an integrated Android malware infrastructure managed by a common actor. Shared characteristics include the package name, similar runtime behavior, common server communication patterns, and shared infrastructure.

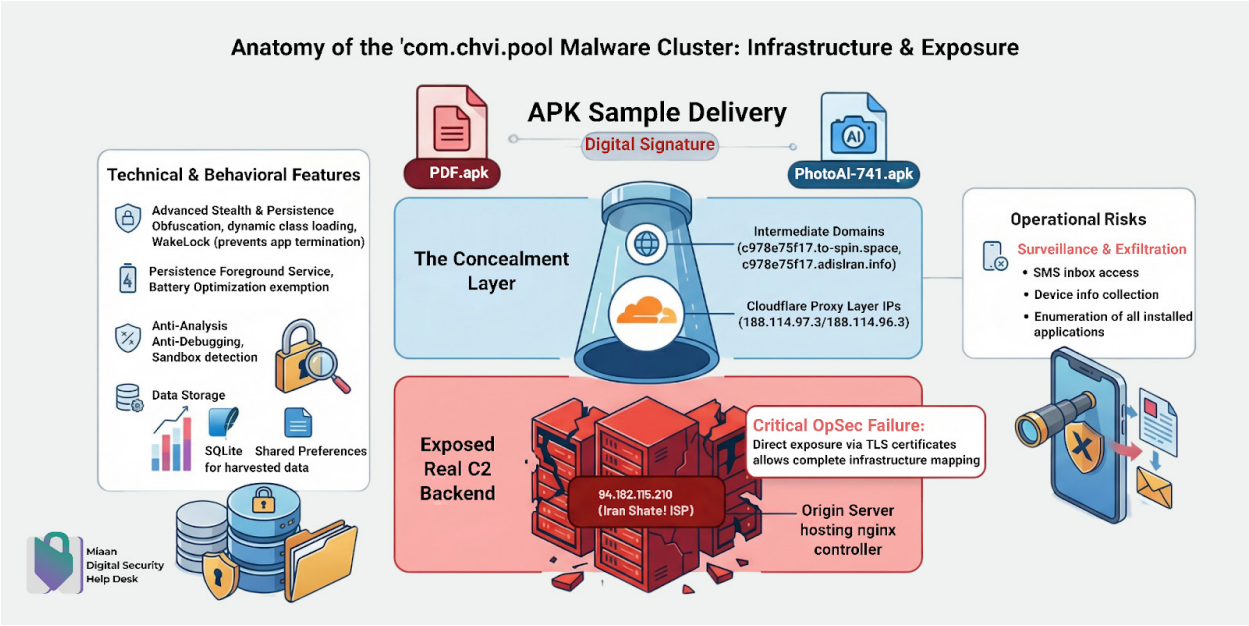
This infrastructure attempts to hide the real command-and-control (C2) infrastructure by using Domain Rotation techniques and Cloudflare as a reverse proxy. However, further analysis showed that in one of the samples, the real backend IP was exposed, making it possible to identify the main infrastructure.

Technical and Behavioral Features

Static and dynamic analysis of the samples shows that these malware samples have a set of advanced capabilities for concealment, persistence, and information gathering:

- **Concealment:** Obfuscation, code encryption, and dynamic class loading via Reflection.
- **Persistence:** Use of "Foreground Services" and "WakeLock" to prevent the application from being stopped by the system.

- **Anti-Analysis:** Detection of debuggers and sandbox environments to bypass conventional analysis tools.
- **Stealth:** In the PDF.apk sample, the application icon is hidden from the user immediately after execution.



In the PDF.apk sample, application icon-hiding behavior was also observed, such that the application becomes invisible to the user after execution. This behavior may also be present in the other samples, even if it was not activated in the Sandbox environment.

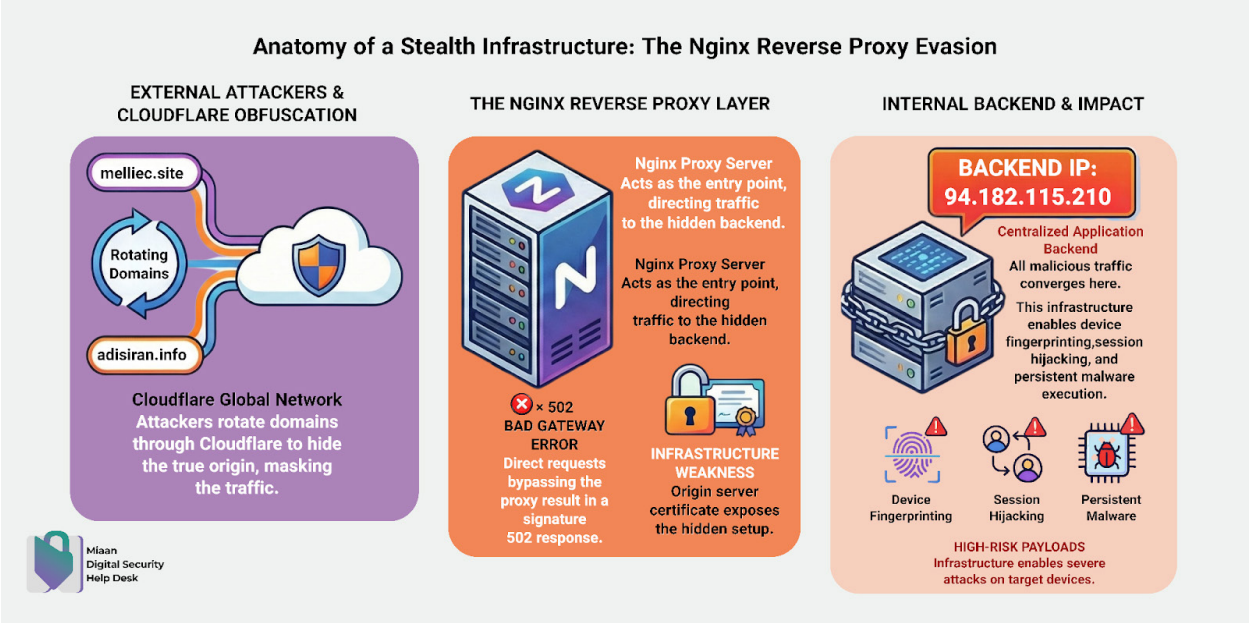
Surveillance Capabilities and Operational Risk

These samples are classified as hidden Android loaders with surveillance functionality. They are capable of receiving secondary payloads and focus heavily on data collection, including:

- **Monitoring:** Accessing SMS inboxes and monitoring user communications.
- **Data Theft:** Collecting device environment information and enumerating all installed applications.

Command and Control (C2) Infrastructure

The campaign utilizes a multilayered architecture to conceal its backend operations.



Layer One: C2 Domains

The following domains were observed in the samples:

- c978e75f17.tc-spin.space
- c978e75f17.adislran.info
- C978e75f17m.cs2-go.sbs
- c5acc344.geogo.cfd

In most cases, these domains resolved to Cloudflare IPs:

- 188.114.96.3
- 188.114.97.3

which indicates the use of Cloudflare as a proxy layer to hide the origin server.

Layer Two: Origin Backend Discovery

In the Pdf-812.apk sample and also PhotoAi-741.apk, one of the domains resolved to the following IP:

- 94.182.115.210

This IP belongs to an Iranian domestic internet provider, Shatel, and with a very high probability functions as the real origin backend of the C2.

Layer Three: Direct Analysis of the Backend Server

Direct examination of this IP showed:

- Operating system: Ubuntu
- Web server: nginx 1.24
- Active services: HTTPS and unusual ports (7000/7001)

- Use of TLS 1.3 and a Let's Encrypt certificate
- Most importantly: the TLS certificate presented on this server belongs to the domain melliec.site.

Connection to melliec.site

TLS analysis shows that:

- The backend server directly presents the certificate of the domain melliec.site
- This domain is also behind Cloudflare

But the origin server is still directly accessible

This indicates a weakness in OpSec implementation, because the backend is exposed to direct access without full isolation

Reverse Proxy Behavior

Sending direct requests to the backend with different Host values (including melliec.site and adislran.info) resulted in a 502 Bad Gateway response. This behavior shows that:

- The server acts as a reverse proxy (nginx)
- There is an internal backend (application layer)

At the time of testing, this backend:

- Either was unavailable
- Or responded only to specific requests

Infrastructure Summary

Based on all evidence:

- All samples are connected to a shared infrastructure.
- The attacker uses Domain Rotation and Cloudflare for concealment.
- The main backend is concentrated at IP 94.182.115.210.
- The domain melliec.site is connected to this backend, but its exact role (operational or auxiliary) is still not certain.
- The presence of the certificate on the origin indicates an operational weakness in infrastructure concealment.

Importance and Security Implications

This malware cluster indicates that threats have evolved beyond simple phishing to full device compromise. If successful, an attacker can establish persistence, activate surveillance, and execute secondary payloads, making this a high-risk espionage threat for targeted users.

Browser- and Web-Based Attacks

We have documented the execution of malicious JavaScript via a state-run live-streaming site.

- **Entry Point:** Attackers utilized a live-streaming website from the Islamic Republic of Iran Broadcasting (IRIB) as the primary entry point.
- **January 2026 Tactics (Dey Protests):** Following the complete shutdown of the international internet, a link to the **IRIB Channel Six** live stream was sent en masse to diaspora journalists. Attackers exploited the fact that these journalists were seeking information during the blackout to encourage clicks.
- **Attack Objectives:** This browser-based campaign was designed for device fingerprinting, behavior tracking, and potential session theft to prepare for more targeted phishing.
- **Technical Significance:** This method is particularly dangerous because it requires no file installation; merely visiting the page is sufficient to identify and track the target.

Disruptive Attacks and Infrastructure Repression

Application-Layer DDoS with Signs of Reconnaissance and Exploitation

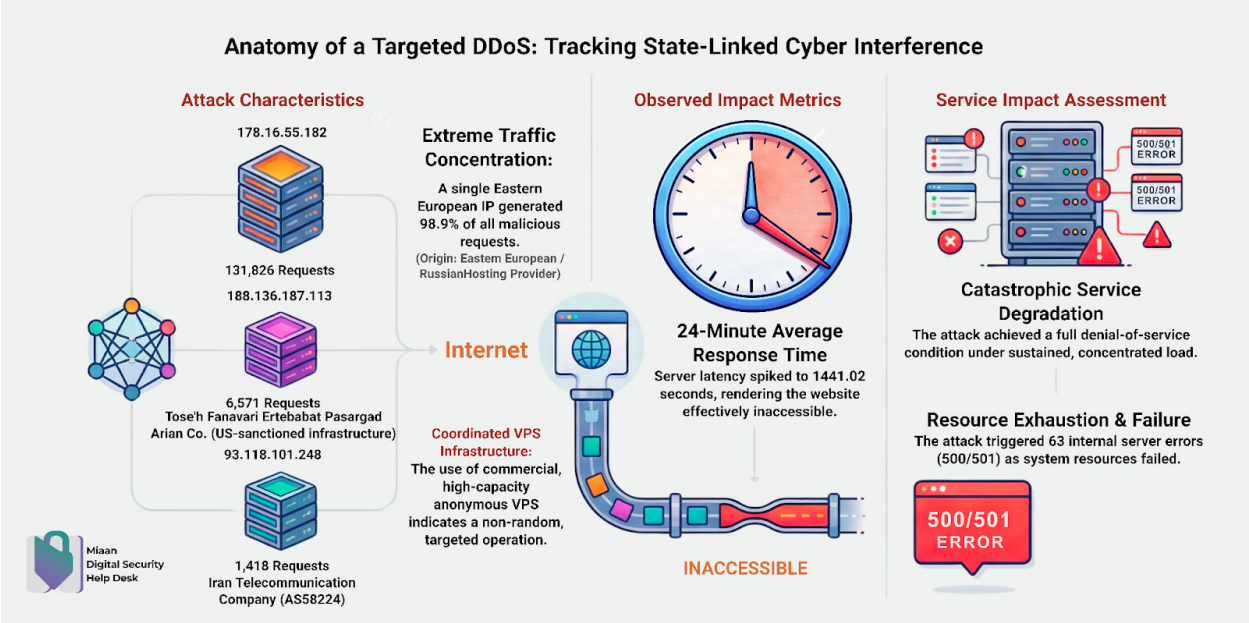
During this period, we identified a severe attack on the website of a prominent human rights institution. This was not a simple "flood" attack; our analysis observed the following sophisticated techniques:

- **Targeting of heavy paths:** Specifically /xmlrpc.php.
- **Scanning:** Active use of Nmap.
- **Vulnerability probing:** Abnormal requests designed to identify system weaknesses.
- **Injection patterns:** Presence of SQL Injection (SQLi) signatures.
- **User-Agent Spoofing:** Spoofing of standard browser User-Agents.

This attack represents a combination of DDoS, vulnerability reconnaissance, and attempted intrusion. Its goal was not merely to reduce service quality, but to impose digital censorship by disrupting access to a human rights platform registered in France belonging to a prominent Iranian activist. The attack was repeated a second time, indicating a determined effort by state-linked actors to silence this entity.

Technical Analysis

Analysis of the recorded data shows that the system in question was subjected to a distributed denial-of-service (DDoS) attack that led to severe disruption in service performance and ultimately rendered it inaccessible to ordinary users. A prominent feature of this attack is the very high concentration of traffic on one main source; the IP address 178.16.55.182 generated about 98.9 percent of all malicious requests. This pattern indicates a focused and targeted attack, not a dispersed one based on large botnets. The use of high-capacity and anonymous VPS infrastructure in Eastern Europe or Russia also indicates that the attacker used rented and scalable resources to execute the attack.



Alongside the main source, two other IPs were also observed in the attack, and they are particularly significant. The address 93.118.101.248 is linked to the infrastructure of the Telecommunication Company of Iran (AS58224), and the address 188.136.187.113 belongs to Tose'h Fanavari Ertebabat Pasargad Arian, or Fanap (AS206065), which was sanctioned by the United States on August 7, 2025.

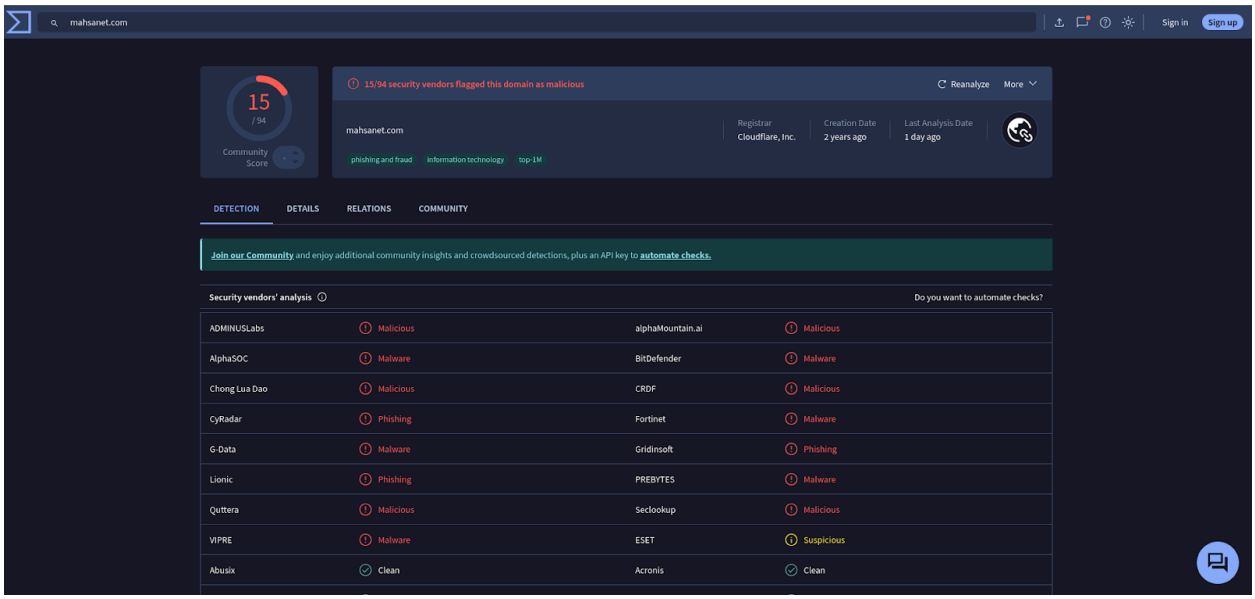
The involvement of these two sources, which are linked to state or semi-state infrastructure in Iran, in the attack on this website is a critical finding. It indicates the use of sensitive infrastructure alongside public resources to disrupt the activities of human rights organizations. This combination of anonymous infrastructure and infrastructure with sovereign ties may be a sign of an increased level of complexity in the design and execution of security agencies' operations in transnational repression.

From the perspective of impact, the data indicate a complete breakdown in service performance. The average server response time reached about 1441 seconds (nearly 24 minutes), which in practice means the service was unusable for ordinary users. Under such conditions, even if the website appears superficially available, the user experience is completely disrupted and public access is effectively lost. The recording of 63 instances of 500 and 501 errors also shows that, under excessive pressure, the server suffered a severe shortage of resources and lost the ability to process requests.

Overall, this attack can be described as a targeted DDoS attack with severe operational impact that, using a combination of rented infrastructure and infrastructure linked to telecommunications entities, was able to completely disable the service. The high concentration of traffic, the controlled attack pattern, and the level of destruction caused all indicate a planned and effective operation that goes beyond ordinary and scattered DDoS attacks.

Indirect Attack and Domain Poisoning: Disruption of Access to MahsaAlert

The public warning platform MahsaAlert is an information and crisis-mapping system created by Iranians outside the country and publishes information related to protests, arrests, and cases of human rights violations in Iran. With the start of tensions between the United States, Israel, and the Islamic Republic of Iran, this platform issued special wartime alerts in order to prevent collateral and indirect harm from war to civilians.



The MahsaAlert platform, without any actual intrusion into the server or being hacked, was effectively taken offline. Raznet's investigation shows that an individual or group created a real sample of Windows malware (RAT), embedded the domain mahsaalert.com in it as the command-and-control (C2) server, and uploaded the malware sample to platforms such as VirusTotal. When security engines and sandboxes executed this malware, the program's attempt to connect to this domain was recorded, and as a result many cybersecurity companies and cyber threat databases marked the domain as malware infrastructure.

This event is an example of an indirect attack: instead of infiltrating the server, the attacker manipulated automated cybersecurity systems, damaged the domain's reputation, and caused access to it to be blocked for users and networks. The aim of the report is to warn about a structural weakness in global threat intelligence systems: many systems regard domains as malicious solely on the basis of data correlation (such as malware connecting to a domain), without verifying the actual behavior of the server.

The key point of this report is that this happened without any real intrusion into the server and became possible solely through poisoning the domain's reputation.

Common Methods Used by Attackers

Across all analyzed cases, the following methods were dominant:

- **Impersonation:** Attackers posed as Telegram support, Meta/Facebook/WhatsApp, Gmail, organizational colleagues, researchers, or legal recruiters.
- **Technical Credibility Abuse:** Many phishing emails successfully passed SPF, DKIM, and DMARC checks, appearing technically valid to recipients.
- **Newly Registered Domains:** Attackers used professionally styled domains to build trust and conduct multi-stage attacks.
- **Legitimate Service Concealment:** Use of link shorteners (e.g., shorten.ee, t.ly), trackers, and cloud services to hide malicious destinations.
- **Multi-channel Attacks:** Combining messengers, phone calls, and threat emails to increase pressure on the victim.
- **Anti-analysis:** Use of manifest encryption, dynamic class loading, and Reflection to bypass security researchers.

Importance and Implications of These Attacks

These operations have evolved beyond simple deception:

1. **Beyond Deception:** Attacks resulted in full account takeovers, transfer of account ownership, and long-term access.
2. **Digital Trust as a Weapon:** Attackers turned the user's trust in legitimate brands and cloud infrastructure into a vulnerability.
3. **Repressive Function:** These attacks restrict expression, make communication networks feel unsafe, and impose heavy psychological costs, leading to self-censorship.
4. **Device-Level Compromise:** The discovery of the PDF.apk / Vision-3187.apk cluster shows a shift toward persistent, surveillance-oriented access at the hardware level.

Indicators of Connection to Iran and the Use of Iranian Infrastructure

In all cases, it is not possible to state with certainty which individual or entity carried out the attack. However, in several cases there is significant evidence that strengthens the possibility of a connection to actors aligned with the Islamic Republic or the use of Iranian infrastructure.

1. Direct presence of Iranian infrastructure in the DDoS attack: in the case of the attack on the human rights website, part of the attacker traffic came from the following infrastructures:
    a. AS58224 affiliated with Telecommunication Company of Iran

b. AS206065 affiliated with Tose'h Fanavari Ertebabat Pasargad Arian Co. PJS

This is one of the most important pieces of evidence in the entire collection, because it shows that, alongside foreign VPS infrastructure, domestic telecommunications infrastructure inside Iran was also observed in the attack.

- Attackers used impersonation of platforms, academic figures, organizational managers, and legal entities.
- A significant portion of the attacks relied on legitimate or apparently valid infrastructure.
- In several cases, the attack progressed to actual account takeover, transfer of ownership, and post-compromise threats.
- An Android malware cluster and a case of malicious JavaScript execution show that the threats are not limited to phishing.
- The DDoS attack, with reconnaissance and attempted intrusion components, indicates digital repression at the infrastructure level.
- In several cases, especially those related to Telegram, the DDoS attack, and Android malware, significant signs of a connection to Iran or the use of Iranian infrastructure were observed.

Overall, these data indicate the existence of a multilayered, adaptive, and in some cases successful threat environment directed against high-risk Persian-speaking users and institutions.

Content Moderation: The War of Narratives

Hate Speech and Targeted Campaigns

Between July 1 and December 31, 2025, we observed coordinated campaigns across various platforms targeting political activists and civil society. These campaigns typically involved groups of social media users, particularly on X (formerly Twitter), targeting well-known figures with threats of death or sexual violence.

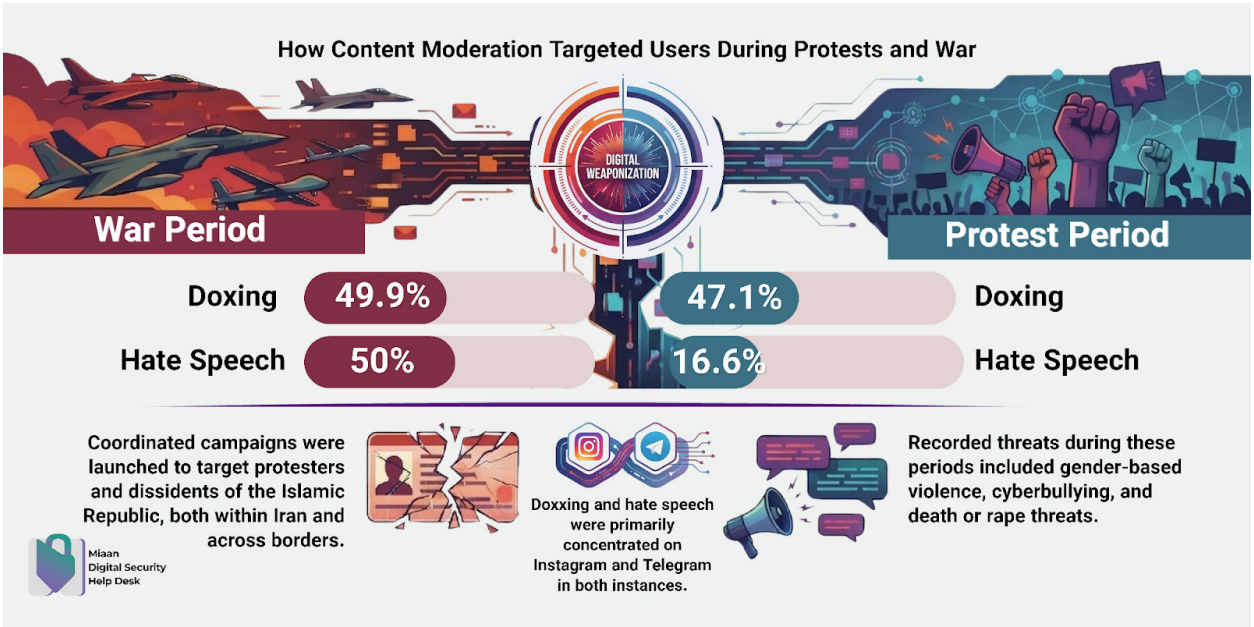
Impersonation Tactics

Attackers utilized impersonation to identify and compromise users in contact with credible entities. This was not limited to media outlets but extended to humanitarian sectors:

- Media and Citizen Journalists: Creating fake Instagram accounts or Telegram channels using slight variations in Latin character spelling.
- Charitable Organizations: Several charities were similarly targeted on Telegram and Instagram to map their networks of supporters and beneficiaries.

Comparative Analysis: Doxing During Protests vs. War

While both the Dey protests and the Esfand war saw surges in doxing and hate speech despite internet shutdowns, the two periods exhibited substantial strategic differences:



- **Nationwide Dey Protests (Late December 2025–January 2026):** Doxing was primarily decentralized and provincial. Telegram channels and Instagram accounts published phone numbers, home addresses, and workplace locations of protesters to incite local-level harassment.

- **Esfand War (February–March 2026):** Following U.S. and Israeli military actions, the focus shifted to a national level. Regime officials publicly threatened diaspora activists with property confiscation and revocation of citizenship for supporting humanitarian intervention. This was followed by a wave of information exposure targeting these activists across social networks.

Involvement of Official Media

A significant development during the war period was the direct involvement of official and semi-official media in doxing efforts:

- **Tabnak:** The official Tabnak Telegram channel was directly involved in targeting civil society activists outside of Iran.
- **Mehr News Agency:** The official account of Mehr News Agency was locked by platform after it published the private address of actress Leila Otadi in Dubai.

Policy Enforcement on Platform X

Following February 27, 2026, platform X implemented a visible policy shift, enforcing content moderation more strictly against users promoting the policies of the Islamic Republic. Significant removals included:

- **Mehr News Agency:** Accounts related to the outlet were removed following the publication of private information (doxing).
- **Regime Officials:** Accounts of several current officials, including Members of Parliament, were removed for supporting the Islamic Revolutionary Guard Corps (IRGC).
- **High-Profile Pro-Regime Users:** Accounts were suspended for threatening supporters of the military actions against Iran.

Gender-Based Violence and Psychological Pressure

In both periods of repression, hate speech remained a primary tool for silencing dissent.

- **Nature of Threats:** Campaigns included severe cyberbullying, threats of murder, and gender-based violence, specifically targeting women with threats of rape.
- **Coerced Support:** High-follower accounts and well-known figures were targeted by organized campaigns designed to pressure them into publicly supporting the policies of the Islamic Republic.

Indicators of Compromise

Domains

- smtp3707.org
- em557105.smtp3707.org
- onlineviewer.net
- confidential-mail.google.com
- cucps.k12.va.us
- amazonses.com
- awstrack.me
- joining-hosts-room.online
- shorten.ee
- louisebatterseldom.com
- gg.hls2.xyz
- c978e75f17.adislran.info
- c978e75f17.tc-spin.space
- C978e75f17m.cs2-go.sbs
- c5acc344.geogo.cfd

Telegram Accounts and Bots

- @AuthenticatorBot
- @abdallahsarayra06
- @mnzd12300

IP Addresses

- 84.32.84.32
- 103.2.141.104
- 87.248.110.82
- 76.223.140.188
- 91.195.240.19
- 178.16.55.182
- 93.118.101.248
- 188.136.187.113
- 209.85.220.65
- 209.85.220.41
- 188.114.96.3
- 188.114.97.3
- 94.182.115.210

Uniform Resource Locator (URL)

- https://shorten.ee/@help_center_6639
- https://t.ly/lZ6bU
- awstrack.me

File Hashes

PDF.apk

MD5: 873e3f275340fa1706b8e32026e6bedc

SHA1: 71b8262e239869d74cd84eb5632abcfb252dc79d

SHA256: 7ef0da4c8bd83a5eaaa4a250d027b4ffc168206923d9453f81b02454f58ab020

Vision-3187.apk

MD5: deae9dae9c418c2db3575c9f91823eb9

SHA1: 7201a304a4e90ea14af6e6bd4eef6a6965cae613

SHA256: 33dfa923c2047098170ca5ebdaa25494707dd2e77873be46f07851b60ea982b2

Pdf-812.apk

MD5: 4044E8EAA4548C72A41705386632FC61

SHA1: 66D5906CF5EBB54C4CDC5FCA65BBB6D8EC9DD694

SHA256: 3D6136E5CC81837B77B12FA73989C23A23F8F68E5CEEF304BA9097FB734B47C4

Package Names

- com.chvi.pool