

Cyber Threat Reports

AI in the Service of Repression: From Targeted Phishing to Gender-Based Harassment

October 15, 2026 Filterwatch

Executive Summary and Key Trends

The fourth report in the *Cyber Threats in Iran* series examines data recorded by the Digital Security Helpline over the six-month period from 22 March to 22 September 2026. This period unfolded amid the continuing repercussions of the December 2025 - January 2026 protests, a wave of arrests and device seizures, widespread internet disruptions, and intensifying pressure on activists both inside and outside Iran.

The data show that digital repression not only persisted during this period but evolved into a combination of denial of access, targeted social engineering, malware, impersonation, coordinated harassment, and disruptive operations. At the same time, the use of artificial intelligence in digital repression expanded significantly, including its application to

enhancing phishing campaigns, cloning the voices of trusted individuals, generating fabricated sexual content, conveying threats, damaging reputations, and sowing discord within civil society networks.

From Total Blackout to Controlled Connectivity

Filterwatch's research shows that, rather than fully restoring internet access, the Islamic Republic expanded a system of restricted and unstable connectivity in which access to the open internet increasingly depended on users' identities, professional affiliations, and approval by state authorities.

This system has made internet access increasingly tiered, with different levels of access granted to different groups of users, while also making connectivity more expensive and subject to greater state control.

Key developments included:

- The continuation of the internet shutdown or severe restrictions on international connectivity at the beginning of the reporting period;
- The incomplete restoration of internet access after 88 days, with traffic remaining far below levels recorded before 8 January 2026;
- Bandwidth throttling, increased latency, and interference with network protocols and DNS without an apparent total shutdown;
- The expansion of tiered internet access through privileged "white" SIM cards and the "Internet Pro" service;
- Making internet access for business owners and academics conditional on identity verification and institutional approval;
- Increased control over data centres, servers, VPNs, and other censorship-circumvention tools;
- Intensified security measures against Starlink users and equipment vendors;
- Reduced internet use among users and rising costs of accessing the open internet;
- Efforts to link online activities and multiple digital identifiers to users' real identities;
- Persistent network instability, power outages at data centres, and disruptions affecting GPS and banking services.

Overall, during this period, Iran's internet shifted from a state of total shutdown to an ostensibly connected network that remained unstable,

tiered, costly, and subject to heightened surveillance.

Blurring the Boundary Between Repression in Public Life and Online Spaces

Helpdesk data indicate that the boundary between repression in public spaces and control across digital platforms has become increasingly blurred. Individuals' conduct in society—from their clothing and lifestyle to providing services to women who do not observe mandatory hijab—can result in their SIM cards being blocked, their internet access being disconnected, or their online accounts being seized. Conversely, content published on social media has been used to exert judicial, economic, and social pressure in the physical world.

Documented cases included:

- The seizure of Instagram accounts that published content portraying lifestyles inconsistent with the Islamic Republic's approved norms;
- Threatening the owners of shuttered businesses with arrest on charges of "propaganda against the state" if they publicised the authorities' actions on their Instagram accounts;
- The termination of home internet services belonging to some civil society activists, in addition to the blocking of their SIM cards.

The widespread blocking of users' SIM cards assumed a significantly broader scope during this period. It affected not only civil society activists, journalists, and student activists, but also a wider range of social and professional groups.

- Blocking the SIM cards of Instagram users for publishing content inconsistent with the Islamic Republic's approved lifestyle norms, with restoration of service made conditional on removing the content;
- Requiring some users to publish an image of the Islamic Republic's flag or other pro-government content as a condition for restoring their SIM cards;
- Blocking the SIM cards of people working in clothing, fashion, and beauty, and requiring them—on the orders of prosecutors—to report to the Fashion and Clothing Council and sign a written undertaking;
- Blocking the SIM cards of women who did not observe mandatory hijab in Isfahan until their cases had been heard by the courts;

- Blocking the SIM cards of journalists, political activists, and civil society activists;
- Blocking the SIM cards of labour activists, teachers, artists, and people working in media and cinema;
- Blocking the SIM cards of online business owners for publishing images deemed inconsistent with the Islamic Republic's dress regulations;
- Blocking users' SIM cards for publishing critical or political content on social media;
- Accompanying SIM-card blocking with calls or threats from security agencies, while making restored access conditional on deleting content, signing undertakings, or ending public activities.

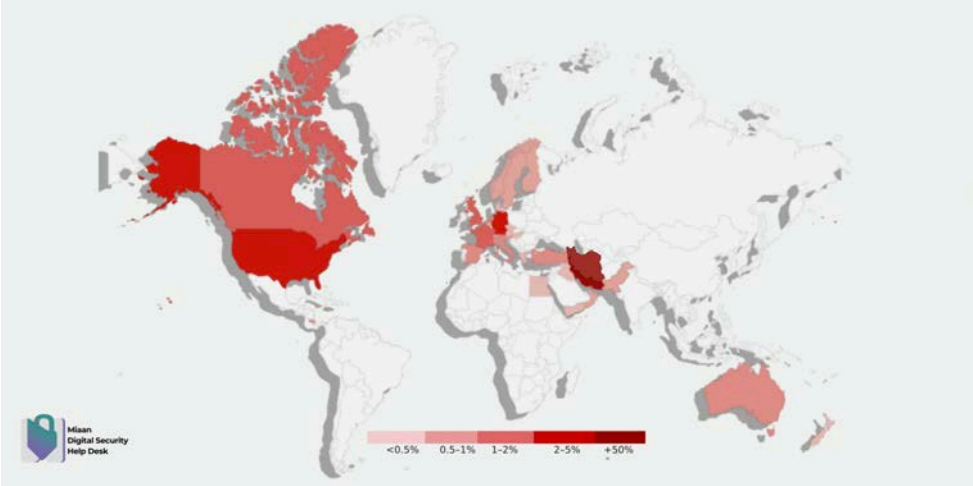
These cases demonstrate that repression is no longer confined to a single sphere: an individual's conduct in public can result in digital exclusion, while their online activity can lead to judicial action, business closures, or pressure to modify their behaviour in society. By blocking communications and seizing social media accounts, authorities have created a bridge between online and offline repression, using digital restrictions to pressure individuals to comply with government-imposed rules, force them to remove or publish certain content, and prevent them from exposing abuses by security forces.

Transnational Repression: Figures and Trends

The Islamic Republic's cyber operations targeting individuals and organisations outside Iran became increasingly sophisticated during the reporting period. Nearly 16% of all cases recorded between 22 March and 22 September 2026 involved Iranian civil society activists, journalists, and organisations based abroad. These cases revealed a growing reliance on targeted, multi-stage attacks involving impersonation, personalised social engineering deception, potentially AI-generated audio, malicious software, and attempts to take over online accounts. Attackers also used temporary websites and links to evade detection and facilitate their operations.

Geographical distribution of transnational targets:

The leading target countries during this period were the United States, with 30 cases; Germany, with 26; the United Kingdom, with 18; France, with 16; and Canada, with 12. Together, these five countries accounted for 102 cases, representing 64.6% of the 158 cases involving targets outside Iran.



Compared with the previous reporting period, the United States moved from second to first place, while Germany rose from fifth to second. The United Kingdom fell from first to third, and France moved from sixth to fourth.

Cases involving cyberattacks present a different picture. Targets outside Iran accounted for 66.7% of all cyberattack cases. Within this subset, the United States, the United Kingdom, and Germany recorded the highest numbers, with five cases each, followed by Italy with three. France, Sweden, Slovenia, and Spain each recorded one case. Together, the United States, the United Kingdom, and Germany accounted for 15 cases, representing 68.2% of the 22 cyberattack cases involving targets outside Iran.

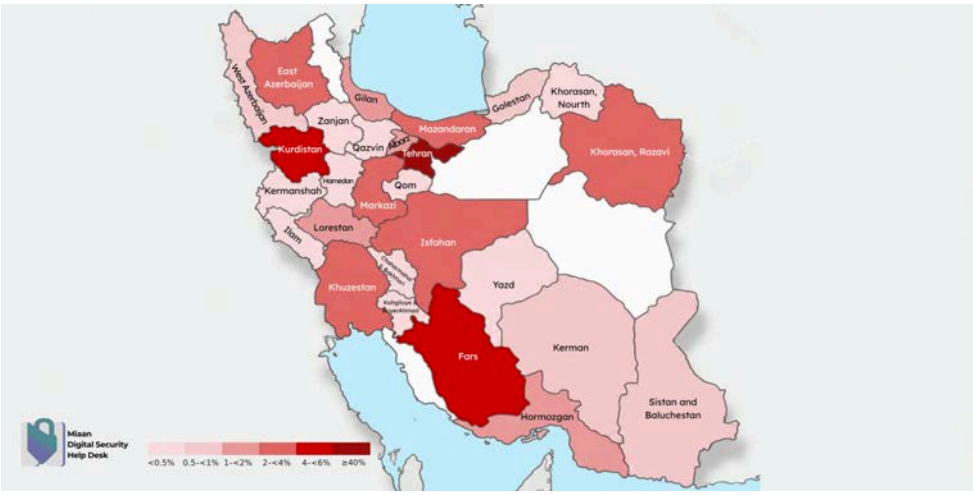
Journalists were the most frequently targeted group in cyberattack cases, with seven recorded cases. Digital rights organisations ranked second with five, followed by political activists with three. The targeting of journalists, media outlets, and digital rights organisations indicates that the media sector and Iran-related civil society networks remain among the principal targets of transnational attacks.

Requests submitted by civil society activists, journalists, and Iranian organisations based outside the country included the following:

- Reviewing messages, links, and webpages suspected of phishing or credential theft;
- Responding to attempts to obtain authentication codes and take over Telegram, Instagram, and other online accounts;
- Recovering and securing compromised or at-risk accounts, including reviewing active sessions and unauthorised login attempts;
- Identifying, reporting, and removing fraudulent accounts, channels, or pages impersonating activists, journalists, media executives, or civil society organisations;

- Examining files, Android applications, and links suspected of containing malware that had been sent through messaging platforms or trusted accounts;
- Analysing voice messages suspected of being artificially generated or manipulated for impersonation, threats, or the creation of conflict;
- Responding to doxxing, disclosure of personal information, and threats against diaspora activists on websites, Telegram channels, and Instagram accounts;
- Addressing coordinated harassment, online threats, psychological pressure, and calls for attacks or violence against activists and their family members;
- Reporting and following up on the distribution of private material, non-consensual sexual imagery, and fabricated or deepfake content intended to damage reputations;
- Investigating possible attacker access to private messages, contacts, organisational channels, or victims' networks;
- Responding to the misuse of compromised accounts belonging to friends, colleagues, or contacts to target additional members of a network;
- Investigating the misuse of organisations' names, domains, or infrastructure and mitigating resulting harm to their digital reputation;
- Countering artificial follower inflation, coordinated reporting, and attempts to restrict or remove accounts and channels;
- Providing security guidance, including enabling two-factor authentication, using a separate password, reviewing active sessions, and verifying identities through an independent communication channel.

Domestic Threats: The Geography of Repression in Iran



During the six-month period from 22 March to 22 September 2026, 82.5% of all cases recorded by the Helpdesk involved individuals or organisations inside Iran. This represented an increase of more than ten percentage points compared with the previous reporting period. The rise in domestic cases was primarily associated with requests concerning account access and security, account suspension or recovery, and emergency measures following arrests and device seizures.

- Provincial distribution: Tehran continued to account for the largest share of cases inside Iran, at 40.6%. This represented a decline of 6.4 percentage points from 47% in the previous period, although Tehran's share remained substantially higher than that of any other province. It was followed by Kurdistan at 5.7%, Fars at 4.1%, Mazandaran at 3.7%, Markazi at 3.6%, Isfahan at 3.3%, East Azerbaijan at 3.1%, Razavi Khorasan at 2.8%, and Khuzestan at 2.3%. Nearly 20% of domestic cases recorded during this period did not specify a province.
- Individuals: Account access and security represented the most frequently recorded area of need, accounting for approximately 75.9% of all domestic cases. Among account-related cases, account suspension or closure accounted for 51%, reactivation for 25.2%, appeals against suspension for 11.5%, and account recovery for 7.6%. Instagram was the most frequently cited platform in account-related cases, appearing in 46.2% of them.
- Device seizure as a tool of digital exclusion: Approximately 3.4% of the cases recorded during this period involved the seizure of mobile phones or other digital devices. Device seizure enables the Islamic Republic to

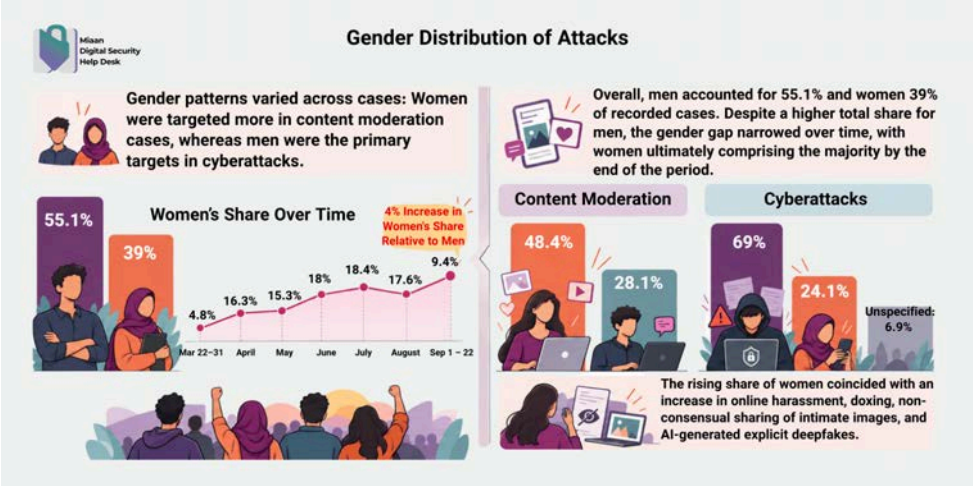
disrupt or prevent an individual's access to communications, online accounts, work tools, and support networks without holding them in prolonged detention and incurring the associated political, operational, and legal costs. Even after a person is released, the loss of a device—or concern that security agencies may have accessed the information stored on it—can bring their professional, journalistic, or civil society activities to a halt.

- Demand for Starlink support: Approximately 6.5% of requests recorded during this period concerned Starlink support. The volume of these requests may indicate both wider use of satellite internet and a growing preference for connectivity outside the communications infrastructure controlled by the state. Persistent restrictions, internet shutdowns and disruptions, extensive filtering, and concerns about surveillance or blocked communications have reduced some users' trust in the reliability and security of Iran's domestic internet infrastructure, increasing demand for alternative means of connectivity.

This growing demand for alternatives to state-controlled internet access was also acknowledged by Iranian officials. In September 2026, Behzad Akbari, Deputy Minister of Information and Communications Technology and CEO of the Telecommunication Infrastructure Company, stated that the number of Starlink terminals and users in Iran had increased, with growth accelerating since the war and the imposition of internet restrictions. He also noted that the effects of Starlink usage were visible in the country's network traffic, although precise user figures were available only to SpaceX.

Gender Distribution

Across the full reporting period, men accounted for 55.1% of recorded cases and women for 39%. Although men represented the larger share overall, the gap between men and women narrowed progressively, and by the end of the reporting period, women accounted for a greater proportion of cases than men.



At the beginning of the reporting period, men accounted for 67.1% of recorded cases and women for 27.1%. Women's share rose to 34.4% from mid-April to mid-May, 34.7% from mid-May to mid-June, 41.8% from mid-June to mid-July, and 43.4% from mid-July to mid-August. It declined slightly to 42.1% between mid-August and mid-September, before increasing to 48.1% between 1 and 22 September. During this final period, men accounted for 44.2% of cases, meaning that women represented the larger share of recorded cases for the first time during the reporting period.

Gender distribution also varied by type of request. In content-management cases, women accounted for 48.4%, compared with 28.1% for men. By contrast, in cyberattack cases, men represented 69% of identified targets and women 24.1%, while gender was not recorded in the remaining 6.9%.

The growing share of cases involving women coincided with an increase in gender-based harassment, disclosure of personal information, distribution of private content without consent, and the creation of fabricated sexual images and videos.

The Reach of Digital Pressure: From Protesters to Civil Society Organisations

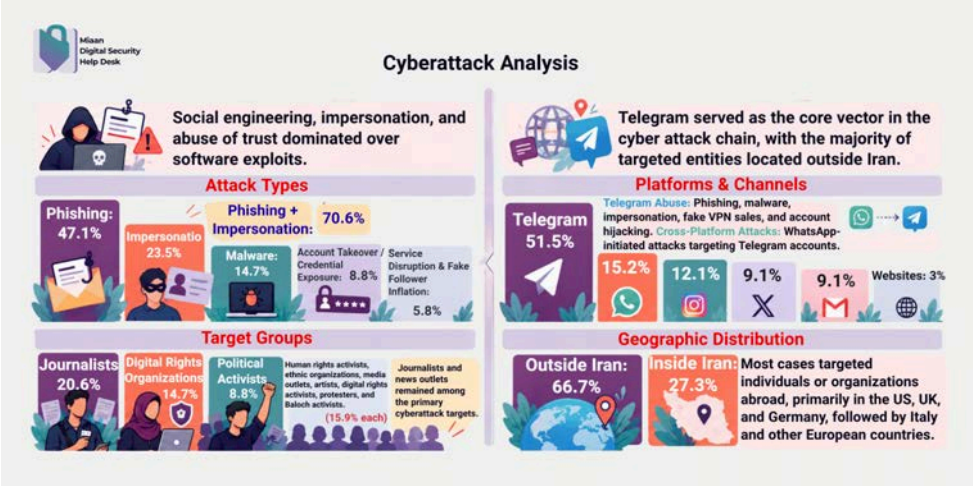
Among individual cases recorded during this period, protesters were the most frequently represented group. In cases involving organisations, human rights organisations accounted for the largest share, followed by organisations focused on the Kurdish ethnic minority, digital rights, and women's rights.



- Individual groups: Across the reporting period, protesters were the most frequently represented group, accounting for 22.9% of cases involving individuals. They were followed by political activists at 12.8%, protesters active on social media at 7.7%, journalists at 6.9%, and artists at 6%. This distribution shows that digital pressure extended beyond prominent political activists to people involved in protests and citizens who continued their protest-related activities on social media.
- Organisations: Among organisational cases recorded during the reporting period, human rights organisations accounted for the largest share, at 23.2%. Organisations associated with the Kurdish ethnic minority followed at 18.3%, digital rights organisations at 12.2%, and women's rights organisations at 9.8%.

Cyberattack Analysis

An examination of cyberattack-related cases indicates that the dominant threat pattern during this period relied less on exploiting software vulnerabilities and more on social engineering, impersonation, and the exploitation of trusted relationships.



- Attack types: Phishing was the most common attack method during this period, accounting for 47.1% of recorded attack classifications, followed by impersonation at 23.5%. Together, these two methods represented 70.6% of all attack classifications, underscoring the central role of social engineering and the exploitation of trust. Malware accounted for 14.7%, account takeover or credential exposure for 8.8%, while disruption to infrastructure access or reputation and artificial follower inflation each accounted for 2.9%.
- Target groups: Journalists were the most frequently targeted group, accounting for 20.6% of recorded targets. Digital rights organisations followed at 14.7%, and political activists at 8.8%. Human rights activists, ethnic minority organisations, media outlets and news agencies, artists, digital rights activists, protesters, and Baloch activists each accounted for 5.9% of target-group records. When journalists, media outlets, and news agencies are considered together, the media sector emerges as one of the most prominent targets during this period.
- Channels and platforms: Telegram appeared in 51.5% of cases, making it the most frequently recorded platform in the attack chain. WhatsApp followed at 15.2%, Instagram at 12.1%, X—formerly Twitter—and Gmail at 9.1% each, and websites at 3%. The use of Telegram was not limited to phishing; it also included malware distribution, account or channel impersonation, fraudulent VPN sales, and the misuse of compromised accounts. In some cases, the initial delivery channel differed from the asset ultimately targeted. For example, an attack might begin on WhatsApp while seeking to take over the victim's Telegram account.
- Geographical distribution: Targets outside Iran accounted for 66.7% of cyberattack-related cases, while 27.3% involved individuals or organisations inside Iran. The United States, the United Kingdom, and Germany each accounted for the largest share, at 15.2%, followed by Italy

at 9.1%. France, Sweden, Slovenia, and Spain each represented 3% of cases.

The concentration of cases involving targets outside Iran, together with the prominent targeting of journalists, media outlets, political activists, and digital rights organisations, is consistent with a pattern of digital transnational repression. The consequences of these attacks can extend well beyond the takeover of a single account, potentially giving attackers access to victims' contacts, conversations, and professional networks; enabling the sequential targeting of connected individuals; and damaging organisational reputations.

Use of Artificial Intelligence in Impersonation and Multi-Purpose Operations Against Civil Society Networks

During the reporting period, the Helpdesk documented several cases of targeted impersonation conducted through WhatsApp and Telegram. Attackers used the names, photographs, and professional identities of trusted individuals to create fraudulent accounts and contact activists, journalists, and members of civil society networks using AI-generated or manipulated audio recordings.

These attacks did not serve a single objective. Some cases were designed to steal authentication codes and take over Telegram accounts. In others, voice messages were used to threaten or intimidate targets, or to attribute divisive statements to well-known individuals. These activities therefore cannot be understood solely as a phishing campaign. The documented pattern combined targeted phishing, impersonation, threats, and attempts to undermine trust among members of the targeted networks.

In the phishing branch of the operation, the attacker established contact and built trust before sending a link disguised as an invitation to a meeting. The destination page instructed the victim to enter a code received from Telegram, falsely presenting it as a "meeting access code". In at least one case, submitting the code resulted in unauthorised access to the victim's Telegram account.

Other attacks, however, were aimed at intimidation and disruption rather than account theft. In these cases, threatening voice messages or audio falsely attributed to another individual could be used to create fear, damage

reputations, or undermine relationships within a network. Unlike phishing attacks, their success did not depend on a victim clicking a link or having an account compromised. Simply changing the victim's behaviour, generating mistrust, or disrupting communications could achieve the attacker's intended objective.

Key Findings:

- Fraudulent WhatsApp and Telegram accounts were created using the identities of trusted individuals.
- Messages were tailored to the victim's professional circumstances or personal network.
- In the phishing attacks, attackers typically gained victims' trust by inviting them to what appeared to be a legitimate meeting or professional discussion.
- The attacker used a webpage under their control to collect Telegram authentication codes.
- At least one case of unauthorised access to a Telegram account was confirmed.
- Voice messages were used in every documented case to reinforce the impersonation.
- Threatening voice messages and audio attributed to other individuals—apparently intended to generate conflict—were also reported.
- No malware delivery or exploitation of software vulnerabilities was documented within this cluster.
- The campaign used social-engineering techniques to impersonate the identity and voice of the person most likely to command the intended target's trust.

Multi-Stage Phishing and the Exploitation of Trust

The phishing attacks documented in this report followed an extended trust-building pattern. The phishing link was not necessarily sent in the initial message. Instead, the attacker first impersonated someone connected to the victim's professional field, establishing a plausible basis for contact before steering the conversation towards an invitation to a meeting or collaboration.

This method involved four principal stages:

Creating a fraudulent account using the name and photograph of a trusted individual;
Initiating a conversation through WhatsApp or Telegram;
Sending a meeting invitation and a link to a webpage controlled by the attacker;
Obtaining the victim's Telegram authentication code and using it to access the account.
In this attack chain, the authentication code was not intercepted through the telecommunications network. The attacker initiated the Telegram login process and persuaded the victim to enter the legitimate code they received into a fraudulent webpage. The attack therefore succeeded not because of a vulnerability in Telegram, but through the deceptive reframing of the authentication code's purpose.

This pattern is consistent with multi-stage phishing campaigns documented in previous Filterwatch reports: before presenting a link, the attacker establishes an apparently legitimate relationship through a professional or organisational invitation and raises the sensitive request only after gaining the victim's trust.

Use of Voice Messages and the Potential Role of Artificial Intelligence

Voice messages served at least three distinct purposes in these operations:

Reinforcing Impersonation

A voice attributed to a trusted individual can serve as apparent proof of identity. This method is particularly effective when the victim does not recognise the sender's phone number but finds the impersonated individual's voice or manner of speaking familiar.

Threats and Intimidation

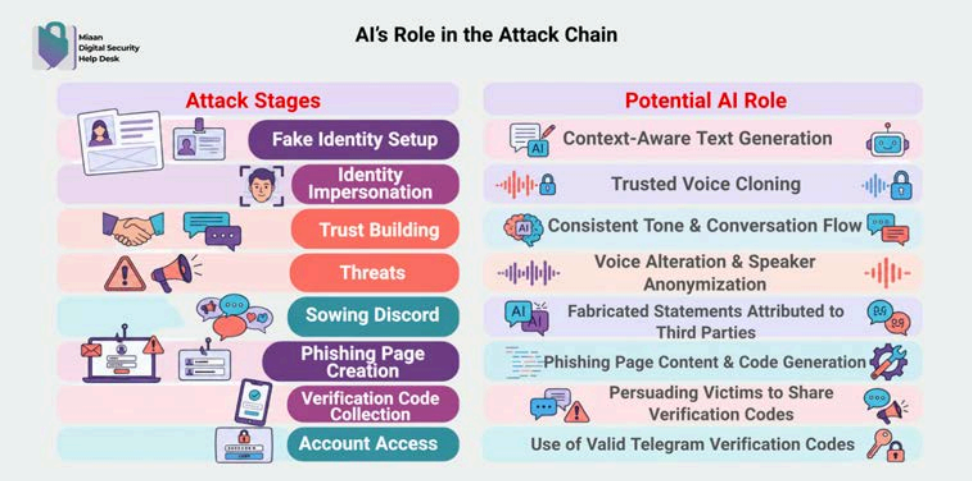
In some cases, the audio content was threatening in nature. In such scenarios, the objective may be to instill fear, exert psychological pressure, reduce the victim's public activity, or create the impression that the attacker has the ability to reach them.

Creating Conflict and Reputational Harm

A fabricated voice recording can be used to attribute offensive, confidential, or divisive statements to an individual. Disseminating such content may generate mistrust, end cooperation, or create tensions among members of a network, even when no account has been compromised.

The Role of Artificial Intelligence in the Operational Chain

The available evidence does not indicate that artificial intelligence exercised full control over the operations. Its likely role was to improve the quality, speed, and scale of deceptive content production.



Artificial intelligence did not create an independent method of compromise in these cases. Access to the account still depended on obtaining a valid Telegram authentication code, but synthetic content may have increased the likelihood that the victim would trust the attacker and continue the interaction.

Infrastructure Used

In the phishing cases, short-lived links and attacker-controlled webpages were observed. Some of this infrastructure relied on web services and Cloudflare tunnels. These services enable attackers to deploy webpages rapidly, use HTTPS, and replace addresses with relative ease.

The use of Cloudflare is not, by itself, an indicator of malicious activity. It acquires analytical value only when combined with other elements, including:

- Contact initiated from a fraudulent account;
- Impersonation of a trusted individual;

- An unexpected invitation to a meeting;
- Delivery of a short-lived link;
- A request to enter a Telegram authentication code on a webpage outside Telegram;
- The creation of a new session after the code has been disclosed.

Operational Impact

The most significant confirmed technical impact was unauthorised access to a Telegram account. Such access could expose the victim's contacts, accessible conversations, professional relationships, and the identities of potential secondary targets. However, the available data do not document the duration of the unauthorised session, the scope of information accessed, or the attacker's activities after gaining entry.

The disruptive branch produced a different category of harm. Its effects could include:

- Creating fear or psychological pressure;
- Damaging the reputation of the impersonated individual;
- Generating mistrust within the targeted network;
- Disrupting or reducing communication between individuals;
- Causing self-censorship or the suspension of activities;
- Preparing the victim for a subsequent attack.

These outcomes should not be assessed solely according to the technical criteria used for phishing. For example, an operation that did not result in an account takeover may still have succeeded as a disruptive information operation if it caused cooperation to end or led to the circulation of a fabricated voice recording.

Helpdesk Findings on the Abuse of Telegram in Malicious Operations

During the reporting period, the Helpdesk documented three categories of attacks involving the distribution of suspicious Android applications through Telegram. In each category, the attacker used a pretext tailored to the target's circumstances or interests to persuade them to install an APK file: government services, access to the open internet, or personal photographs.

The available evidence indicates that Telegram was used in these cases, at minimum, as a channel for contacting targets and delivering malicious files or links. In one sample, a string matching the structure of a Telegram Bot API token was also identified within the APK, raising the possibility that Telegram played a role in later stages of the operation.

Common Initial-Access Pattern

In all three cases, the attack began with a Telegram message. The attackers used two principal trust-building methods:

- Sending the message from an account known to the target;
- Presenting the application under a pretext tailored to the target's needs or circumstances.

In the "Jahad-e Keshavarzi" case, the attacker impersonated a government institution. In the Starlink/VPN case, the attacker exploited the need of users inside Iran for tools to circumvent internet restrictions. In the "Souvenir Photo" case, the message drew on a personal relationship and emotionally engaging content.

This pattern demonstrates that the attackers did not rely solely on the malware's technical capabilities. A critical part of the operation involved persuading the target to install an application from outside an official app store. A message sent from the account of a friend or former contact may indicate account compromise, but the available evidence is insufficient to confirm that these accounts had been hacked.

Potential Application Capabilities

The two samples whose Android manifests could be examined requested extensive permissions. These permissions could enable the applications to:

- Read SMS messages and authentication codes;
- Send SMS messages from the victim's device;
- Access the phone number and device information;
- View or modify contacts;
- Access stored images and files;
- View installed applications;
- Make telephone calls;
- Run services in the background;

- Resume activity after the device restarts;
- Communicate with external infrastructure over the internet.

The presence of these permissions alone does not prove that all of these capabilities were used in practice. However, the combination of permissions relating to SMS messages, contacts, internet access, background execution, and automatic startup—together with deceptive branding and targeted distribution—increases the risk of surveillance, account theft, and further propagation of the attack through the victim's contacts.

Identification of a String Resembling a Telegram Bot Token

In the Starlink/VPN APK, a string matching the format of a Telegram Bot API token was identified at assets/lb.txt. During testing, live validation returned a 401 Unauthorized response. This may indicate that the token had been revoked, replaced, or disabled by the time of analysis.

This finding is significant because a bot token can be used to authenticate an application with the Telegram API and enable automated communications. Potential uses could include transmitting device information, receiving configurations or commands, and reporting installation status. However, the presence of a token-like string alone does not demonstrate that it was operationally used. Confirmation would require identifying Telegram API calls in the code, network traffic, or the application's decrypted core components.

The complete token should not be published in a public report. Its numeric identifier, relevant timestamps, file path, and other necessary information may be shared with Telegram on a restricted basis through a secure channel for further investigation.

Obfuscation and Resistance to Analysis

Two samples employed techniques designed to make analysis more difficult. The Starlink/VPN APK contained a DPT-like native packing layer, obfuscated assets, architecture-specific loaders, and ZipCrypto protection. The "Souvenir Photo" file was also obfuscated in a manner that prevented analysts from fully extracting its manifest and principal capabilities.

These methods were likely intended to conceal the application's core components, prevent rapid detection, and increase the cost of analysis. However, similarities in obfuscation techniques or the use of publicly

available packing tools are insufficient to attribute the samples to a common threat actor.

Intelligence Assessment

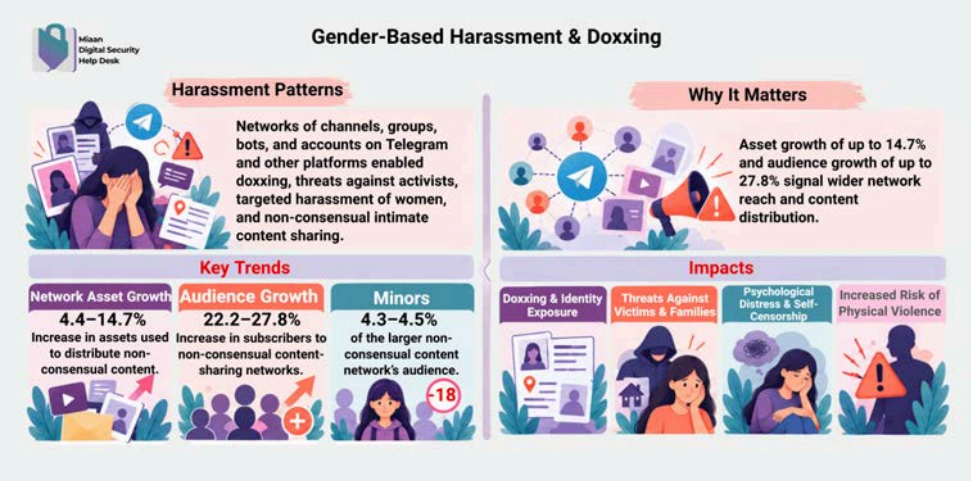
- Telegram was used in all three cases to contact the target and deliver an APK file or link.
- The “Ministry of Agriculture” and Starlink/VPN samples request sensitive permissions with the potential to enable surveillance, data theft or persistence.
- The Starlink/VPN sample contained a string matching the format of a Telegram bot token, although the token was invalid at the time of testing.
- The known accounts used to deliver the files may have been compromised.
- The applications were designed to collect information or maintain access to the victim’s device.
- The token identified in the Starlink/VPN sample was used for command and control.
- The three Helpdesk cases are linked to the same threat actor or operation.
- The Helpdesk cases are directly connected to Small Sieve or to public reporting on DCHSpy.

The cases examined show that Telegram can serve multiple functions in targeted operations against activists, protesters and journalists: establishing initial contact, exploiting trust between known contacts, delivering APK files, directing victims to download infrastructure and potentially providing an automated channel through which an application can communicate with the threat actor.

The most significant common pattern is the combination of social engineering tailored to the target’s circumstances with Android applications distributed outside official app stores. The identification of a string resembling a Telegram bot token in one sample raises the possibility that the Telegram API was used at a later stage of the operation, although this hypothesis requires further behavioural or network-level evidence.

Gender-Based Harassment and Disclosure of Personal Information

An examination of cases from this period reveals that a network of channels, groups, bots and accounts across Telegram and other platforms was used to disclose personal information, threaten activists, target women with harassment, and distribute private or sexual content without consent. These activities combined the publication of identifying information with degrading content, threats and calls for harassment, blurring the boundaries between digital violence, reputational harm and threats of physical violence.



Some of these networks published images of women opposing mandatory hijab, collected private information about them and their family members, and encouraged their audiences to engage in online harassment or acts of violence. Fabricated or AI-generated sexual images and videos were also used to humiliate and intimidate victims, damage their reputations and intensify psychological pressure.

- Expansion of non-consensual content networks: Between 1 August and 31 August 2026, the number of assets involved in distributing private or sexual content without consent increased by between 4.4% and 14.7% compared with the period from 1 July to 31 July.
- Growth in audience reach: The number of subscribers to networks distributing non-consensual content grew by between 22.2% and 27.8% in the second monitoring period. Audience growth outpacing the increase in the number of assets indicates that, alongside expanding structurally, existing networks also increased their reach and capacity to distribute content.
- Abuse involving minors: The audience of a separate network linked to the exploitation of minors was equivalent to approximately 4.3%–4.5% of the

audience of the larger non-consensual content network during the same period.

This trend indicates that gender-based harassment was not merely a collection of isolated attacks against individuals. Rather, it relied on networked infrastructure and large audiences to collect information, disseminate content and intensify pressure on victims. In this pattern, doxxing can enable coordinated harassment, threats against family members, offline stalking and an increased risk of physical violence. Fabricated sexual content can also cause reputational harm, self-censorship, reduced public engagement and psychological distress, even without compromising the victim's account or device.

Indicators of Compromise (IoCs)

Malicious Domains

- louisebatterseldom[.]com
- Hbscity[.]com
- ruv[.]de/service/doi/doi-check?id=s7PNg6pHDfZKXRLctDoZYN6wDQqdjoxg&v2=1
- Wajobfocus[.]com
- Domainlicense[.]my
- Datadataprotect[.]org
- Internetregisteredinternet[.]org
- Ct[.]ws
- votingglobal[.]ct[.]ws/en
- rfdedghmlktgfdklo[.]sfo3[.]digitaloceanspaces[.]com/1[.]html#cl/278230_md/1277/11128888/746/219/6720
- praxisioak[.]click

Malicious links

- rfdedghmlktgfdklo[.]sfo3.digitaloceanspaces[.]com/1[.]html
- Reproduction-sudden-generators-inspections[.]trycloudflare[.]com
- Examine-hopefully-batch-peers[.]trycloudflare[.]com
- Counting-retailer-special-islamic[.]trycloudflare[.]com
- www[.]google.com/url?q=https%3A%2F%2Fpraxisioak[.]click%2F83E7%2F&sa=D&source=calen

dar&ust=
1789842360000000&usg=AOvVaw3mRetNnUv7wOBmfT1no6Lt

IPs

- 209.85.220.69
- 104.21.41.127
- 44.239.46.73
- 52.202.199.209
- 31.22.4.234
- 209.85.220.41
- 138.68.34.161
- 172.67.194.155
- 104.21.52.28

Communication links

- bantaruland@gmail[.]com
- pwp-cbf349b79f117075b0533c6e9b57be01@privacyguardian[.]org
- 54221bb337154d11815f4b68b27641a2.protect@withheldforprivacy[.]com
- catalinatnucsfsjq46224@gmail[.]com
- katulisbrian@yahoo[.]com
- amirasmar.aratlantic@yahoo[.]com

Malicious applications

- LnDP8nXsjQ[.]apk
- SHA-256:
4e6d7f53733a77a989088160b68c8490a248dd9c63cf4f0d324712206f
9f0fd4
- Vision-35886[.]apk
- Md5: 4f1f2c61f39b1148401ef8b3a915eec5
- Sha256:
a1077d8d7b1ccaa87229a18dacb8897178757534c029e6aee3346df087e
cf078
- Vision[.]apk
- Md5: 1f2ec2b0f78c71609117ba8f1f1fd35d

- Sha256: e130a282cfa1ddff22bc7c41bdf139ac6b905c9437db0be82145c6248adcdba2
- عکس یادگاری[.]apk
- Md5: 90d02684aa70c9a0a8393e7f06a34e68

Get PDF

به فارسی
filter.wa