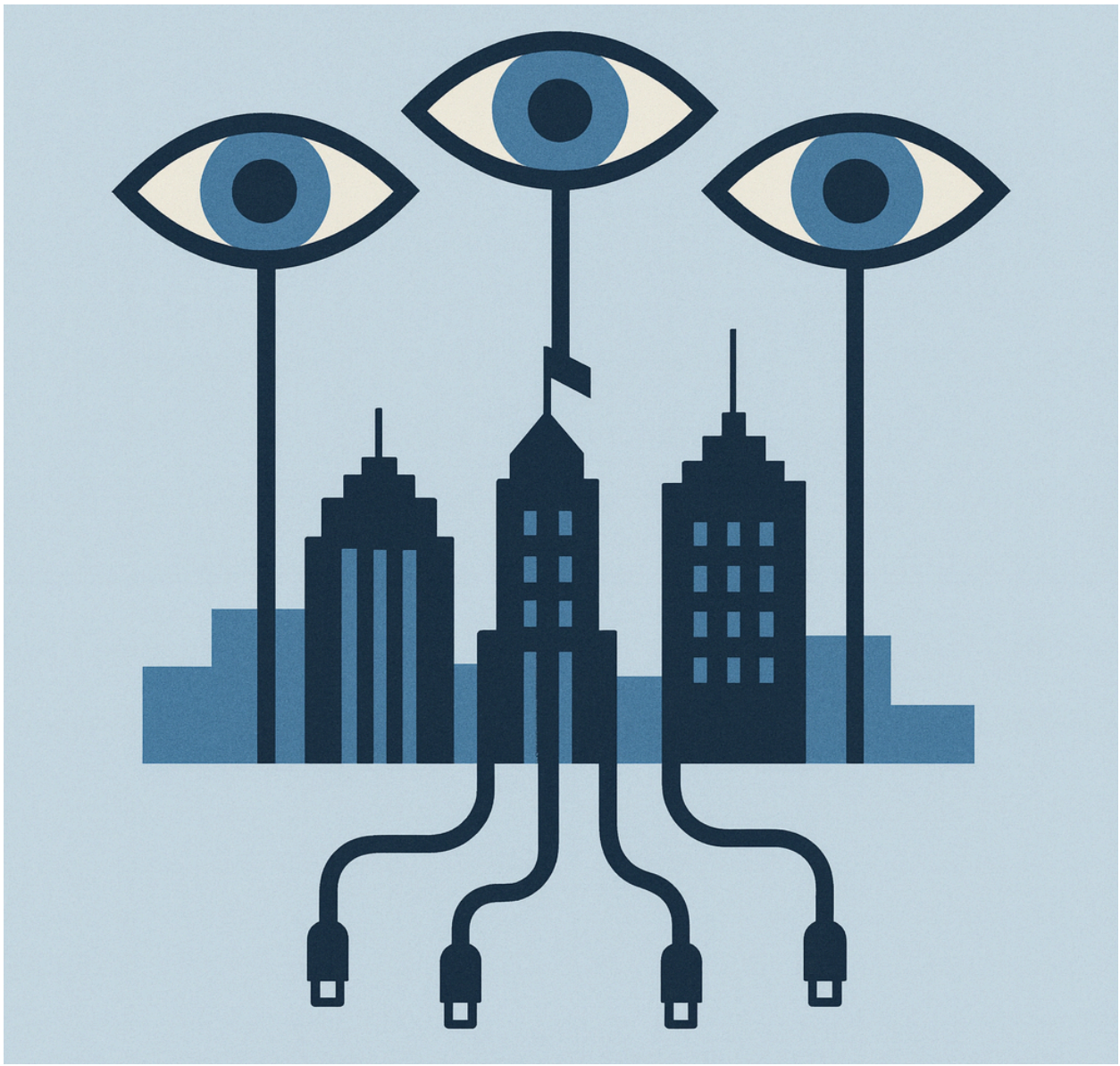
Policymaking and Institutional Mapping of Surveillance and Interception on Citizens under the Islamic Republic of Iran

Part 2: The Islamic Republic's Covert Mechanisms of Surveillance and Interception



Privacy Rights and Surveillance Monitoring (PRISM)
Holistic Resilience, Inc., December 2025

Policymaking and Institutional Mapping of "Surveillance and Interception" on Citizens under the Islamic Republic of Iran

***

Part 2: The Islamic Republic's Covert Mechanisms of Surveillance and Interception

---

This report focuses on the covert and deceptive mechanisms through which surveillance is operationalized in the Islamic Republic of Iran beyond formal legal frameworks. It documents the use of spyware, deceptive access tools, session hijacking, and platform capture to transform everyday connectivity into vectors of monitoring and control. The analysis demonstrates how censorship, user trust, and platform dependence are systematically exploited to enable persistent surveillance while remaining largely invisible to the public.

December 2025

Privacy Rights and Surveillance Monitoring (PRISM)

***

Holistic Resilience

Abstract

Policymaking and Institutional Mapping of "Surveillance and Interception" on Citizens under the Islamic Republic of Iran; Part 2: The Islamic Republic's Covert Mechanisms of Surveillance and Interception

This report examines the covert, deceptive, and extra-legal mechanisms through which the Islamic Republic of Iran operationalizes surveillance and interception beyond formal regulatory frameworks and publicly acknowledged infrastructures. Focusing on clandestine tools, social engineering techniques, and platform-level manipulation, Part 2 maps how surveillance is embedded into everyday digital practices through spyware, deceptive access tools, and the capture of trusted platforms.

Drawing on leaked internal documents, technical analyses, and disclosures related to state-aligned threat actors, this report documents the use of Remote Access Trojans (RATs), modular malware loaders, session hijacking frameworks, and spyware disguised as VPN services or benign applications. Particular attention is paid to operations linked to the Charming Kitten (APT35) ecosystem, whose tools and infrastructures reveal a systematic strategy of persistent access, behavioral monitoring, and scalable data extraction aligned with state intelligence objectives.

Beyond device-level compromise, the report analyzes how surveillance is extended to the application and platform layers. It details the cloning of foreign services, deployment of so-called "governance-compliant shells," and exploitation of authentication sessions to achieve durable control over user accounts without direct malware installation. These practices transform platforms themselves into instruments of surveillance, enabling continuous data collection while remaining largely invisible to users.

Part 2 further demonstrates how censorship, connectivity scarcity, and internet shutdowns are deliberately leveraged to channel users toward compromised access pathways. Attempts to evade filtering—through VPNs, alternative connectivity tools, or satellite internet lures—are systematically

repurposed into vectors of surveillance and espionage. In this model, access to the internet is not merely restricted but actively weaponized.

Taken together, the findings show that covert surveillance in the Islamic Republic is not an auxiliary or exceptional practice, but an integrated operational layer that complements formal interception infrastructures. By combining deception, platform capture, and state-aligned cyber operations, these mechanisms erode privacy and autonomy without relying on visible repression. This report provides a framework for understanding how covert technical practices function as instruments of governance, repression, and long-term social control.

Privacy Rights and Surveillance Monitoring (PRISM)
Holistic Resilience, Inc.
December 2025

Table of Contents

List of Abbreviations

Acronyms:	Full Term:

Islamic Republic of Iran Bodies:

CRA	Communications Regulatory Authority
FARAJA	Islamic Republic of Iran's Law Enforcement Forces; Police
FATA	Islamic Republic of Iran's Cyber Police
IRGC	Islamic Revolutionary Guard Corps
IRGC-IO	IRGC Intelligence Organization
ITO	Information Technology Organization of Iran
MIMT	Ministry of Industry, Mine and Trade
Ministry of ICT	Ministry of Information and Communications Technology
MOIS	Ministry of Intelligence
NCC	National Center for Cyberspace
NIN	National Information Network
NOCR	National Organization for Civil Registration of Iran
SCC	Supreme Council of Cyberspace
SCCR	Supreme Council of Cultural revolution
SCNS	Supreme Council of National Security
TCI	Telecommunication Company of Iran
TIC	Telecommunication Infrastructure Company

State-Controlled Surveillance and Interception Systems:

EMTA	E-commerce Customer Authentication System
HAMTA	Smart System of Communication Devices Registry
HODA	Iranian Digital Identity Authentication System
SAMAVA	National Identity and Verification Gateway
SANA	Online Judicial Authentication System
SHAHKAR	Users Authentication Network
SHAMSA	National lawful intercept data archive system
SIAM	Integrated System for Telecommunication Inquiries

General and Technical Terms:

AAA	Authentication, Authorization, Accounting
API	Application Programming Interface
APT	Advanced Persistent Threat
ETSI	European Telecommunications Standards Institute
IMEI	International Mobile Equipment Identity

IMSI	International Mobile Subscriber Identity
ISP	Internet Service Provider
MITM	Man-in-the-Middle
SSO	Single Sign-On
TTPs	Tactics, Techniques, Procedures
VPN	Virtual Private Network
3GPP	3rd Generation Partnership Project

Islamic Republic of Iran Groundplay and Main Actors

Introduction

The Government of the Islamic Republic of Iran has transformed internet services into an infrastructure for covert control and behavioral monitoring by deploying advanced surveillance techniques and developing interception systems. A wide range of tools are used to monitor citizens' online activities, some specifically built for interception and data collection, and others that appear to serve unrelated functions but enable various levels of access, tracking, and behavioral logging on users' devices. These include techniques such as man-in-the-middle (MITM) interception, so-called "governance-compliant shells," and spyware, including Remote Access Trojans (RATs), capable of covert data extraction and persistent monitoring.

Information leaks from the email servers of the Filtering Committee within the Office of the Prosecutor General have shown that state authorities have sought to deploy complex interception techniques, including MITM, to control citizens' access to the internet and foreign online services and to maintain comprehensive oversight of their online activity.[1] In December 2024, a resolution by the SCC recommended the implementation of "governance-compliant shells" for services such as YouTube, Telegram, and other platforms where negotiations with providers had failed.[2] In November 2025, further disclosures linked to the Charming Kitten (APT35) hacking group revealed the extensive use of RATs by this IRGC affiliated APT against Iranian and non-Iranian targets, as well as the aggregation of citizen data through a platform known as "Kashef."[3]

[1] IranWire; "Anonymous hack of Iran's Filtering Committee servers", Nov 5, 2022; Link, Archive

[2] Mehr News Agency; "Phased Plan to Lift Internet Filtering: From Reopening WhatsApp to Conditional Access to YouTube and Telegram"; Dec 25, 2024; Archive

[3] KittenBusters; "CharmingKitten"; September 2025; Link

Taken together, these practices reflect a dynamic and adaptive approach to the Islamic Republic's surveillance and interception architecture. Unlike centralized initiatives formally led by the Ministry of ICT, the development and deployment of these systems are largely overseen by security and military institutions, including the MOIS and IRGC-IO. Their shifting targets, evolving techniques, and layered operational structures demand increasingly sophisticated analytical frameworks. The sections that follow examine a number of these tools, previously exposed by cybersecurity researchers, that have been deployed to monitor, infiltrate, and operationalize surveillance over the private digital lives of citizens.

Man-in-the-Middle Interception as State Policy

In technical terms, a man-in-the-middle (MITM) attack refers to a form of active interception in which a third party covertly positions itself between two communicating endpoints in order to intercept, alter, or record the exchanged data without the knowledge or consent of either party. Within international cybersecurity and telecommunications standards, MITM is classified as a hostile or malicious activity, typically associated with cybercrime, espionage, or unauthorized network intrusion. As such, it is treated as a security threat to be detected and mitigated, not as a legitimate component of network governance.

In its criminal form, MITM is commonly used for phishing, credential theft, session hijacking, and financial fraud. These attacks exploit weaknesses in network configurations, certificate trust chains, or user behavior to gain unauthorized access to communications. By contrast, when adopted by authoritarian states, MITM shifts from an illicit technical exploit to a policy-enabled surveillance instrument. Instead of operating at the margins of the network,

state-driven MITM is embedded directly within national infrastructure, internet service providers, and regulatory frameworks, enabling interception at scale and with institutional authorization.

Governments resort to MITM techniques primarily because end-to-end encryption has rendered conventional content-based surveillance increasingly ineffective. As encrypted messaging platforms and HTTPS traffic severely limit direct access to communication content, interception at intermediary layers such as DNS resolution, TLS handshakes, or certificate validation becomes a strategic alternative. By asserting control over these intermediary points, the state can regain visibility into user behavior, metadata, and in certain cases even content, without requiring cooperation from foreign platforms or service providers.

This transformation of MITM from a technical exploit into a governance tool marks a critical shift in contemporary surveillance practices. It reflects a broader move away from targeted interception toward infrastructural control, where the architecture of the network itself becomes an instrument of monitoring, filtering, and behavioral regulation.

Institutional Drivers of MITM in Iran

The deployment of MITM interception in the Islamic Republic of Iran is not the result of isolated technical initiatives but is driven by a network of state institutions operating across judicial, regulatory, and security domains. Central to this process is the Filtering Committee, which functions under the authority of the Office of the Prosecutor General and plays a key role in defining enforcement priorities for content control and access restrictions. Through its coordination with internet service providers and infrastructure operators, the committee has

served as an institutional hub for translating policy objectives into technical interception practices.

Documents obtained through information leaks from the Filtering Committee's internal communications indicate that MITM interception has been treated not as an exceptional or temporary response, but as a practical solution to what authorities described as the loss of governmental control over encrypted communications and foreign platforms. In particular, MITM techniques were explored and endorsed in cases where conventional filtering and blocking mechanisms failed to achieve the desired level of control.[4]

Alongside judicial bodies, institutions responsible for internet governance have played a key role in legitimizing and expanding these practices. The Supreme Council of Cyberspace, as Iran's highest internet policymaking authority, has repeatedly stressed the necessity of enforceable mechanisms for asserting state sovereignty over online services. While these mechanisms are often presented in the language of regulation and compliance, in practice they rely on models of intermediary interception and infrastructural control that closely align with the logic of MITM surveillance.

Security and military institutions, including the MOIS and the IRGC-IO, have also played a parallel and often decisive role in the development and deployment of interception capabilities. Unlike centralized programs formally overseen by the Ministry of ICT, these initiatives are

[4] Abdolsamad Khoramabadi (then Deputy Prosecutor General for Cyberspace); "Report of the Cyberspace Deputy of the Office of the Prosecutor General on Certain Matters Related to the Internet", Fifteenth Semiannual Activity Report of the Filtering Committee, first half of 2017; Download.
The report states in part:

> ***Use of the MITM Method***
> *Given that some foreign websites and service providers, on the one hand, publish the public content of their websites in encrypted form, thereby depriving the state of the ability to exercise supervision and content filtering, and on the other hand do not comply with the laws and regulations of the country, a technically feasible short-term solution for filtering criminal content on such websites is the use of the method known as man-in-the-middle.*

typically classified, operationally flexible, and oriented toward intelligence collection rather than service regulation. Taken together, these judicial, regulatory, and security actors have formed an institutional ecosystem in which MITM interception has been normalized as a routine instrument of governance, law enforcement, and surveillance over citizens.

MITM within the National Information Network

The operational viability of man-in-the-middle interception in Iran is closely tied to the architecture of the National Information Network (NIN). Unlike ad hoc interception techniques, large-scale and persistent MITM requires structural control over key layers of network traffic, including routing, name resolution, and transport security. The NIN provides precisely this level of centralized oversight by concentrating traffic flows, standardizing access points, and enabling coordinated intervention across domestic infrastructure.

At the technical level, MITM within the NIN is facilitated through mechanisms such as DNS manipulation, TLS interception, and certificate injection. By controlling or influencing domain name resolution, authorities can redirect user traffic to intermediary nodes without explicit user awareness. Similarly, interception at the TLS handshake stage allows for the inspection or modification of encrypted sessions, particularly when combined with trusted or coerced certificate authorities and network-level deep packet inspection. These techniques shift interception upstream, embedding it within the fabric of network operation rather than applying it at the application layer.

Internet service providers and fixed communication providers (FCPs) play a critical role in enabling this model. As licensed operators, they are structurally positioned to enforce

interception policies mandated by judicial or regulatory bodies. Their integration with national routing infrastructure and compliance obligations allows MITM practices to be implemented uniformly and at scale. In this configuration, interception does not depend on targeting individual users but is applied across entire traffic segments, blurring the line between lawful interception and mass surveillance.

The National Information Network thus functions as a prerequisite for sustained MITM deployment. By consolidating control over traffic exchange points and reducing reliance on external routing paths, the NIN lowers the technical and operational costs of interception while increasing its coverage and persistence. This integration transforms MITM from a situational tactic into a systemic capability embedded in Iran's internet governance framework.

MITM interception in the Islamic Republic of Iran serves multiple, overlapping objectives that extend beyond content filtering or platform blocking. One primary function is controlling access to foreign platforms and services by selectively degrading, redirecting, or conditionally allowing traffic. Rather than relying solely on blunt blocking mechanisms, MITM enables granular intervention, allowing authorities to shape how, when, and under what conditions users can reach external services.

Another core function of MITM is the circumvention or weakening of encryption. While full decryption of end-to-end encrypted content is often infeasible, interception at intermediary layers allows the state to collect metadata, session identifiers, and behavioral signals associated with encrypted communications. These data points provide valuable insights into user networks, communication patterns, and levels of activity, even when message content remains inaccessible.

MITM interception also supports user and device identification across the network. By correlating traffic flows with technical identifiers such as IP addresses, device fingerprints, IMEI, and IMSI, authorities can link online behavior to specific individuals and physical devices. This capability enables cross-platform tracking and facilitates the integration of intercepted data with other surveillance systems, including identity registries and telecommunications databases.

More broadly, MITM functions as a behavioral monitoring tool. Continuous observation of connection attempts, protocol usage, and traffic anomalies allows for profiling user behavior, detecting circumvention efforts, and identifying targets for further action. In this way, MITM operates not merely as a surveillance technique but as an enforcement mechanism that reinforces filtering policies, supports selective repression, and feeds data into wider systems of control.

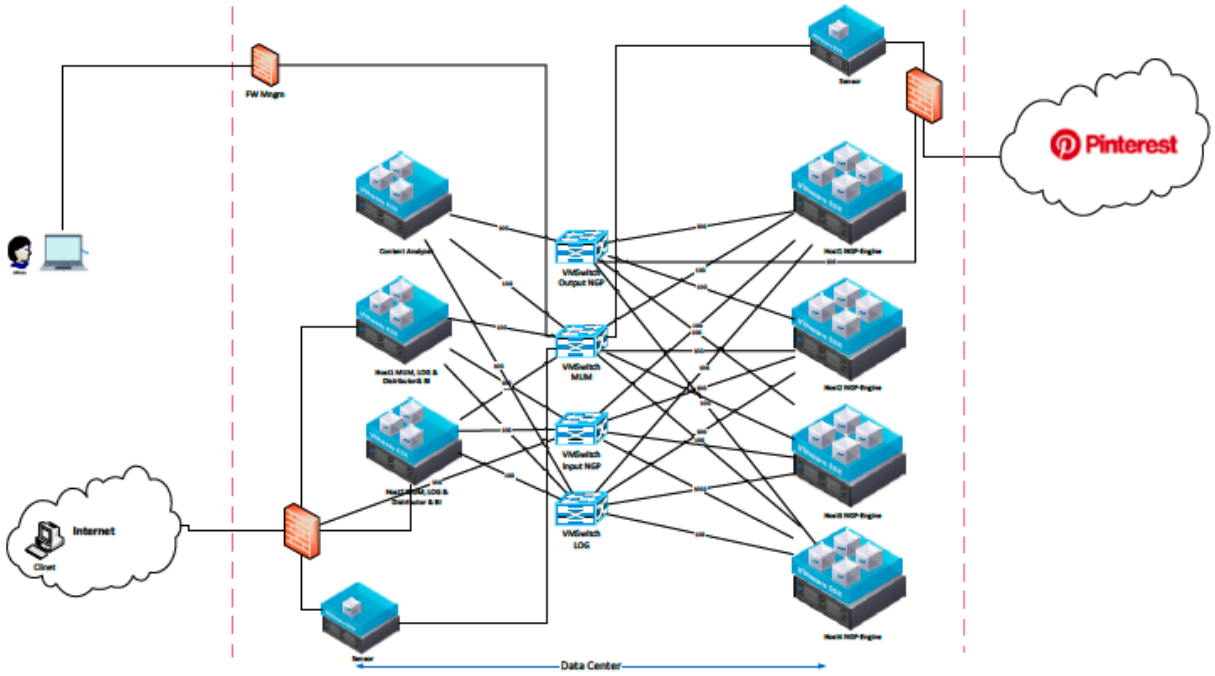
For instance, in 2020, a company named Yaftar Pazhouhan Pishtaz Rayanesh submitted a project titled “New Generation Proxy” to the Filtering Committee.[5] The proposal involved the creation of a fully cloned version of the Pinterest platform, designed to operate as a domestic intermediary proxy. Through this proxy, user requests were received, inspected, censored, and forwarded to the original service, while responses were intercepted, modified, and filtered before being delivered back to users. Marketed as a controlled access solution, the system enabled comprehensive logging of user searches, content preferences, and behavioral signatures.

This proxy-based cloning model, which closely resembles phishing at scale, extended far beyond content filtering. By routing user activity through a state-aligned intermediary, the

[5] Filterwatch; ‘Next-Generation Filtering; Phishing with Governable Templates Analytical”: Apr 26, 2024: Link

system enabled covert surveillance, behavioral profiling, and data extraction without users' informed consent. Such architectures transform popular foreign platforms into intelligence collection surfaces, exposing sensitive user data to analysis by security institutions. In doing so, they not only undermine user privacy but also introduce systemic risks to personal data security by embedding surveillance mechanisms directly into the access layer.

نحوه استقرار ماژول سنسور باید به گونه ای باشد که کمترین تاثیر و عوارض را از سخت افزارهای ماژول های اصلی سیستم بگیرد تا بتواند به بهترین نحو وضعیت کارکردی را بررسی و اشکال یابی کند. همانطور که در شکل هم مشخص است کارت شبکه یکی از سنسورها مانند کاربران قبل از ورود به شبکه و در Zone ورودی فایروال Input قرار گرفته و ارتباط دیگر آن نیز با VM-Switch MUMبرقرار خواهد شد. یک کارت شبکه از سنسور دوم نیز به Zone خارجی فایروال Output در اینترنت و کارت شبکه دوم آن نیز مانند سنسور اول با VM-Switch MUM بر قرار می شود.



شکل ۳ معماری استقرار و توپولوژی سامانه پروکسی Pinterest

The collaboration between Yaftar Pazhouhan Pishtaz Rayanesh Co. and the Prosecutor's Office in this project reflects the willingness of state institutions to expand control and surveillance over citizens' online activities.[6] The company operates as an affiliate within the "Association of Clean Cyberspace Developers" or the "Namdar Security Holding." This grouping brings together a network of policymakers and ICT actors in Iran who are commonly associated with the concept of "smart filtering." Prominent figures linked to this network include Rasoul Jalili, a professor at Sharif University of Technology and a member of the SCC,[7] and Issa Zarepour, the former Minister of ICT.[8]

Earlier efforts followed a similar logic. In the early 2010s, Viber was among the most popular communication platforms in Iran and became a target for platform-level exploitation. A private contractor submitted a proposal to the Filtering Committee detailing thirteen technical scenarios, including data exfiltration, psychological operations, honeypot account deployment, and remote payload delivery.[9]

These practices were publicly acknowledged by Kamal Hadianfar, then head of Iran's Cyber Police (FATA), who stated that private communications on platforms such as Viber were already under law enforcement control.[10] These statements, alongside projects carried out by companies such as Keysan, point to a systematic effort by the state to monitor, spy on, and manipulate users' information in the online space. These measures, particularly at a time when

[6] US Department of the Treasury; "Treasury Sanctions Iranian Officials and Companies Connected to Repression in Advance of the Anniversary of Mahsa "Zhina" Amini's Death"; Sep 15, 2023; Link
[7] Open Sanctions; "Rasoul Jalili"; Link
[8] Open Sanctions; "Issa Zarepour"; Link
[9] Filterwatch; "Internet Oppressors; A Look at the Office of Iran's Attorney General and its Contractors"; Jul 2023; Download
[10] ICTNA; "Chief of Cyber Police (FATA): Be aware that private messages on Viber and WhatsApp are controllable by the Cyber Police"; Sep 12, 2014; Archive

Viber was among the most popular messaging applications in Iran, illustrate widespread violations of privacy and the use of technology as an instrument of social control.

Session Hijacking as Platform-Level Control

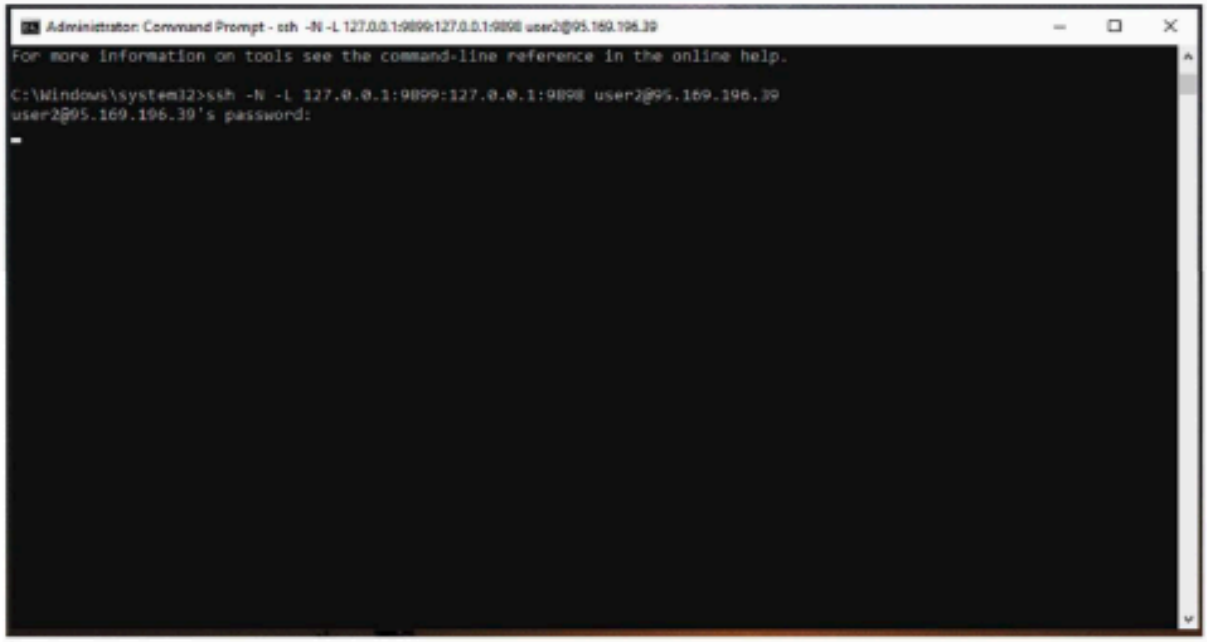
Beyond malware deployment and cloned applications, one of the most revealing techniques linking covert espionage to platform capture is session hijacking. Unlike traditional spyware, session hijacking does not require persistent access to a user's device. Instead, it targets the authentication layer of platforms by stealing or replaying active session tokens, cookies, or access credentials, allowing attackers to assume control over user accounts without triggering security alerts.

Findings from the Charming Kitten disclosures demonstrate how session hijacking can function as a substitute for platform-level access. In several documented campaigns, operators harvested session data through phishing frameworks and deceptive login flows, enabling direct entry into email accounts, cloud services, and social media platforms. Once a valid session was obtained, attackers could read private messages, download archives, modify account settings, and monitor ongoing activity, all while bypassing most end-to-end encryption protections.

This technique is particularly significant in the context of platform capture because it shifts surveillance away from device compromise toward account domination. Rather than installing implants, the attacker becomes the user from the platform's perspective (*the two following sections*). This mirrors the logic of governance-compliant shells and cloned services: control is achieved not by breaking encryption, but by positioning the state or its proxies inside trusted

access pathways. Unlike spyware or remote access trojans, this system is designed to capture active authentication sessions, cookies, and account metadata, allowing operators to access victims' Gmail accounts without installing malware or bypassing operating system protections.

مرحله 1 (اتصال SSH)



جهت دسترسی به صفحه لاگین سامانه نیاز است اتصال خود را به سرور سامانه از طریق پروتکل SSH برقرار کنید.

```
ssh -N -L 127.0.0.1:9899:127.0.0.1:9898 user2@95.169.196.39
```

برای این کار دستوری با عنوان SSH را از فایل پیوست در CMD خود کپی کرده و اجرا کنید سپس منتظر بمانید تا از شما پسورد بخواهد.

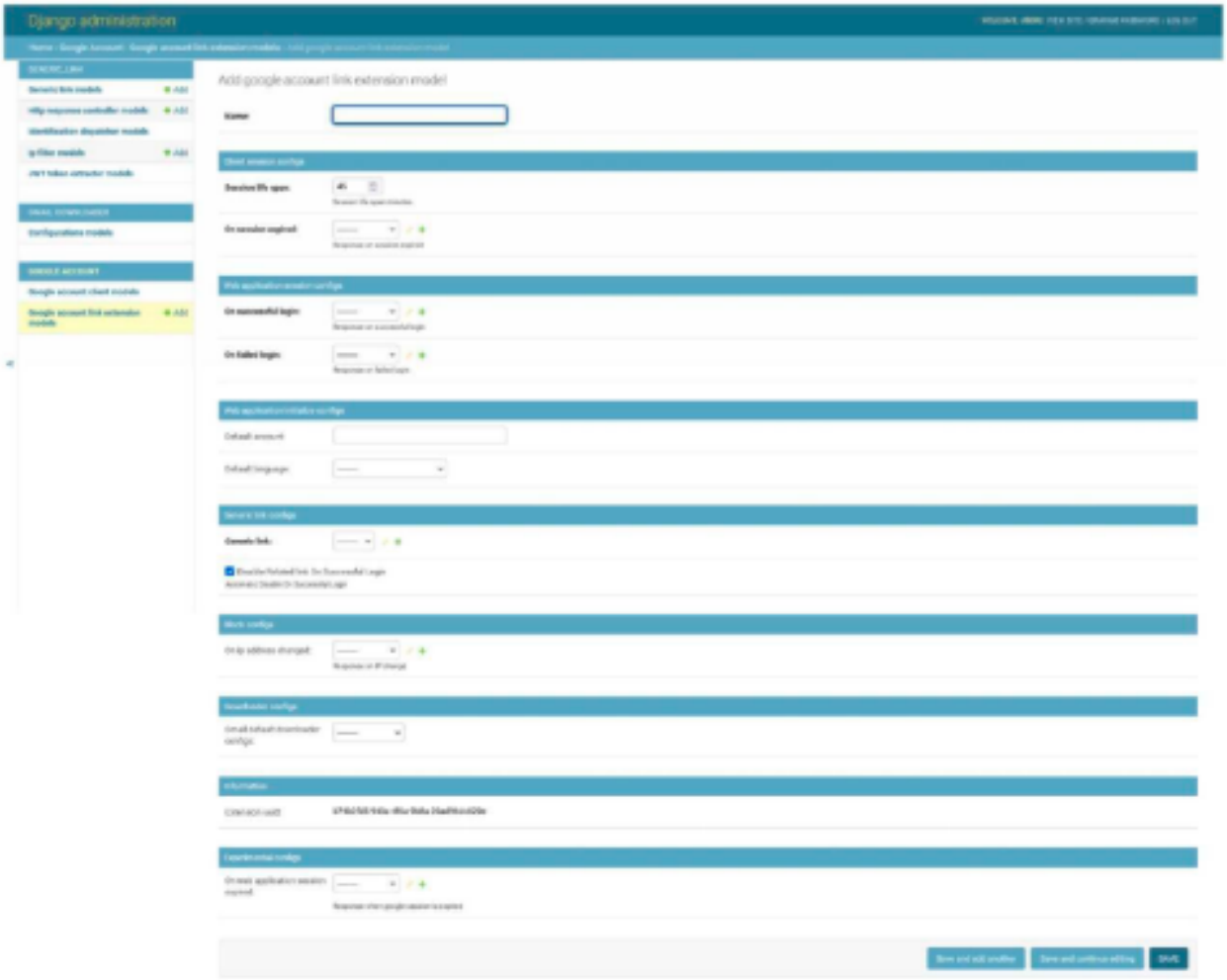
```
Pass: MyUltraSecurePassword#@758
```

*نکته: قبل از برقراری SSH از متصل بودن VPN خود مطمئن باشید.

پسورد مورد نظر را وارد نمایید، توجه کنید که پسورد به شما نمایش داده نمی‌شود. درصورتی که پسورد صحیح باشد و خطایی دریافت نکنید، (مانند تصویر) اتصال SSH برقرار شده و می‌توانید به صفحه وب لاگین سامانه دسترسی پیدا کنید.

Technical documentation shows a server-side infrastructure built around a Django-based control panel, dynamic phishing link generation, and session management modules. The framework supports the harvesting of authenticated sessions, user identifiers, IP addresses, and browser fingerprints, effectively bypassing two-factor authentication by reusing valid session cookies. Access to compromised accounts is facilitated through proxying and SSH tunneling to preserve the victim's network profile.

Session hijacking also enables scalable data extraction. A single compromised session can yield contact lists, communication histories, metadata, and authentication links to other services. In aggregate, such access supports the construction of identity-to-behavior graphs similar to those revealed in state-run databases like Shekar, but without requiring cooperation from the platform itself (*the subsequent sections of this chapter*).



In this sense, session hijacking represents a bridge between individual espionage operations and systemic platform surveillance. It illustrates how techniques developed by state-aligned threat actors can operationalize the same objectives pursued through formal platform capture policies: silent access, behavioral monitoring, and durable control over digital identities.

Legal and Technical Deviations from Global Standards

International frameworks governing lawful interception, including standards developed by ETSI[11] and 3GPP,[12] are built around principles of necessity, proportionality, target specificity, and judicial accountability. These frameworks define clear procedures for authorization, limit interception to identifiable targets, and require mechanisms for logging, auditing, and independent oversight. MITM interception, when assessed against these benchmarks, falls outside the scope of accepted lawful interception practices.

In the Islamic Republic of Iran, MITM interception diverges from these standards both legally and technically. Rather than being constrained by individualized warrants or narrowly defined targets, interception is applied at the infrastructure level, affecting broad segments of network traffic. Legal safeguards are opaque, judicial authorization mechanisms lack transparency, and there is no evidence of independent auditing or effective remedies for unlawful interception. This shifts interception from a rule-bound exception to a generalized condition of network access.

Technically, the deployment of MITM through DNS manipulation, TLS interception, and certificate injection bypasses the safeguards envisioned in international standards. These practices undermine trust models central to secure communications and collapse the distinction between targeted interception and mass surveillance. By embedding interception capabilities directly into national infrastructure and service provision, the state eliminates meaningful technical barriers to continuous monitoring.

---

[11] ETSI; “Lawful Intercept”; Link, Archive

[12] 3GPP; “Lawful Interception in mobile networks”, Aug. 08, 2022; Link, Archive

In the Islamic Republic of Iran, MITM interception is not an exceptional response to security threats but a structural component of internet governance, embedded in policy documents, filtering mechanisms, and national network architecture.

Deceptive Tools and the Transformation of Connectivity into Surveillance Infrastructure

As access to the internet has become increasingly restricted in the Islamic Republic of Iran, scarcity itself has been transformed into a mechanism of surveillance. Systematic filtering, bandwidth throttling, and platform blocking have created a demand for alternative access tools, particularly VPN services and circumvention applications. Within this environment, deceptive access tools have emerged as a core component of the state's covert surveillance strategy, exploiting users' attempts to bypass censorship as an opportunity for monitoring and data extraction.

A growing body of evidence indicates that a subset of VPN services operating in Iran are either directly aligned with state institutions or tolerated under regulatory and security oversight. These services function not merely as circumvention tools but as controlled gateways through which user traffic can be observed, logged, or redirected. By concentrating demand around a limited number of "functional" VPNs, authorities reduce uncertainty in user behavior and create chokepoints for surveillance, effectively turning access tools into instruments of interception.

Surveillanceware distributed through this ecosystem often leverages censorship pressure as its primary vector. Applications marketed as secure VPNs, privacy tools, or connectivity solutions frequently request excessive permissions, embed monitoring components, or establish persistent command-and-control channels. In some cases, these tools are promoted through semi-official channels or benefit from selective non-enforcement, blurring the line between tolerated services and covert surveillance operations.

More recently, deceptive access campaigns have expanded to include Starlink-themed malware and connectivity lures. By exploiting public interest in satellite internet as an alternative to domestic infrastructure, these campaigns distribute spyware disguised as configuration tools, installers, or activation software. Alongside these efforts, mobile and desktop spyware campaigns targeting Iranian users have intensified, deploying remote access trojans and data exfiltration tools capable of capturing communications, device identifiers, and behavioral data.

Together, these deceptive access tools represent a shift in surveillance strategy: rather than merely blocking unwanted connections, the state channels users toward compromised pathways. In doing so, attempts to evade censorship are systematically repurposed into opportunities for surveillance, infiltration, and behavioral monitoring

Deceptive VPN Campaigns Amid Internet Shutdowns and Protest-Related Disruptions

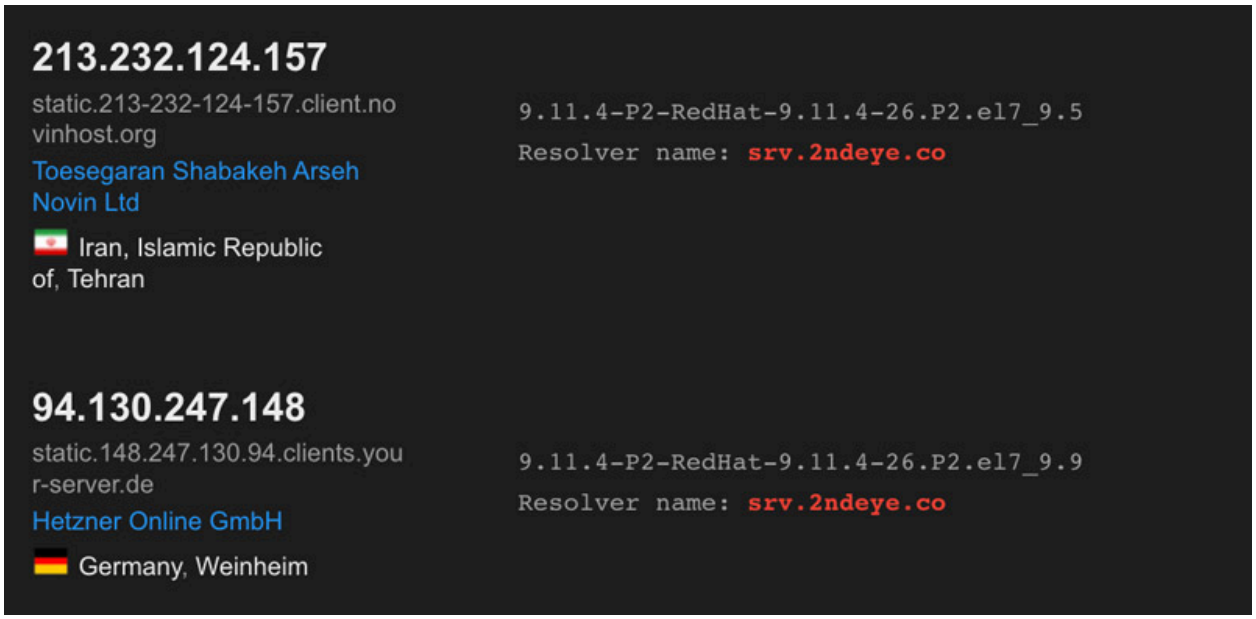
One of the most concerning evolutions in the Islamic Republic's surveillance arsenal is the deployment of state-aligned spyware through vanity VPN services, especially during periods of heightened digital repression such as the 2022–2023 protests (Women, Life, Freedom movement).[13] In a context where the government deliberately throttles internet access to force citizens toward unreliable circumvention tools, spyware-laced VPNs become both a technical weapon and a psychological trap.

[13] Netblocks; "Internet disrupted in Iran amid protests over death of Mahsa Amini"; Sep 19, 2022; Link

This tactic is grounded in a well-documented pattern: by creating a climate of digital desperation through heavy-handed censorship and blocking access to major platforms, the state indirectly pushes users toward unvetted VPN services. Once user trust has been corralled into domestic or rogue services, these apps can be weaponized for full-spectrum digital monitoring.

One of the most high-profile cases emerged during the 2022 nationwide protests, when cybersecurity researchers revealed a campaign involving a spyware family dubbed EyeSpy.[14] This malware was embedded in a widely used Iranian VPN app called 20Speed, marketed as a solution to access the free internet. In reality, it was a trapdoor into users' most sensitive data. Once installed, the app enabled keylogging, theft of files and documents, screen capture, and even exfiltration of passwords and cryptocurrency wallets. The spyware campaign peaked in September 2022, with Iranian users as the primary targets, followed by clusters in Germany and the United States.

[14] Janos Gergo SZELES; Bitdefender; "EyeSpy - Iranian Spyware Delivered in VPN Installers"; Jan. 11, 2023, Archive
Blackpoint Cyber; "Tech Tuesday: Eye Spy – The Dangers of Legal Malware"; Aug. 30, 2022; Archive



The EyeSpy/20Speed campaign is particularly noteworthy for its technical modularity and behavioral stealth. The malware was bundled with a legitimate VPN interface, often using obfuscated or dual-purpose code. Upon installation, it established persistent access, allowed remote command execution, and siphoned data to command-and-control servers operated from inside Iran. Analysts traced the infrastructure to an Iranian threat actor group known as SecondEye, which had a history of surveillance operations aligned with state objectives.

While the campaign mimicked the structure of a criminal spyware distribution operation, the targeting patterns, timing (during peak protests), and geopolitical context strongly suggest coordination or toleration by security agencies such as MOIS and IRGC-IO.

Starlink-Themed Lures and the Distribution of Surveillanceware via Fake Access Tools

What emerges is a strategy of digital entrapment: the Islamic Republic constructs artificial scarcity of free internet, then exploits the user base's turn to insecure channels for surveillance objectives. A more recent evolution of this technique has involved the weaponization of Starlink-themed apps and websites. In response to growing public interest in Starlink connectivity during government-imposed internet shutdowns, Iranian users began searching for ways to access the satellite-based network. The state and affiliated actors swiftly exploited this trend by releasing fake Starlink VPNs and mobile apps claiming to enable access to the service.[15]

[15] Lookout; "Lookout Discovers Iranian APT MuddyWater Leveraging DCHSpy During Israel-Iran Conflict"; Jul. 21, 2025, Archive

Title	Package Name	SHA1	Acquired Date
Earth VPN	com.earth.earth_vpn	556d7ac665fa3cc6e56070641d4f0f5c36670d38	02.07.2025
Comodo VPN	com.comodoapp.comodovpn	7010e2b424eadfa261483ebb8d2cca4aac34670c	25.06.2025
Earth VPN	com.earth.earth_vpn	8f37a3e2017d543f4a788de3b05889e5e0bc4b06	23.06.2025
Earth VPN	com.earth.earth_vpn	9dec46d71289710cd09582d84017718e0547f438	20.06.2025
حضرت عشق (Hazrat Eshq)	hazrateeshgh.apk	6c291b3e90325bea8e64a82742747d6cdce22e5b	2024-04-12
Hide VPN	com.hv.hide_vpn	7267f796581e4786dbc715c6d62747d27df09c61	2023-07-16

Researchers documented distributed APK files embedded with spyware payloads, including variants of DCHSpy and remote access tools capable of file system manipulation, call and SMS interception, and contact harvesting. In at least one case, malware-laced APKs advertised as “Starlink Activation Tools” were uploaded to Iranian app markets not subject to international scrutiny.

This operation highlights a sophisticated use of social engineering, exploiting both technical illiteracy and digital despair among Iranians. By framing these spyware tools as empowerment, attackers aligned themselves with user aspirations for uncensored connectivity, only to subvert those very goals through surveillance.

Deceptive Surveillanceware Disguised as a Harmless Utility

“Souvenir Photo” is a deceptive surveillance application documented in PRISM research as part of a broader ecosystem of state-aligned spyware targeting Iranian users.[16] Unlike full-scale remote access trojans, this tool relies on social engineering and visual deception rather than

[16] Raaznet; “An Android spyware called Aks-e Yadegari (Souvenir Photo) is spreading through Telegram, targeting Iranian cryptocurrency exchanges”; Nov 8, 2025; Link

persistent system-level control. It is distributed as a seemingly benign application, presented to users as a photo-related utility, while covertly collecting sensitive data from the device on which it is installed.

```
public String _vvvvvvv0(String str) throws Exception {
    String str2 = "";
    try {
        Regex regex = Common.Regex;
        String[] Split = Regex.Split("\\n", str);
        if (Split.length > 0) {
            String trim = Split[0].trim();
            if (trim.startsWith(" مشترک گرامی") && trim.endsWith(",")) {
                str2 = trim.replace(" مشترک گرامی", "").replace(",", "");
            } else if (trim.startsWith("ایرانسلی عزیز به شماره")) {
                str2 = trim.replace("ایرانسلی عزیز به شماره", "").trim();
            } else if (trim.startsWith("مشترک گرامی") && trim.contains("در  ، ")) {
                str2 = trim.substring(trim.trim().indexOf("مشترک گرامی"), trim.indexOf("در  ، ")).replace("مشترک گرامی", "").trim();
            } else if (trim.startsWith("همراه گرامی، شماره") && trim.contains("در تاریخ ")) {
                String replace = trim.replace("همراه گرامی، شماره", "");
                str2 = replace.substring(0, replace.indexOf("در تاریخ ")).trim();
            }
        }
    } catch (Exception e) {
        this.ba.setLastException(e);
        Common.LogImpl("713172754", BA.ObjectToString(Common.LastException(getActivityBA())), 0);
    }
```

Technical analysis shows that the application requests a range of permissions disproportionate to its declared functionality. Once installed, it is capable of accessing stored images, device identifiers, and contextual metadata, while also establishing outbound connections to remote servers under operator control. The collection process is largely silent and does not require continuous user interaction, allowing surveillance to take place without raising immediate suspicion.

```
public Object callSub(String str, Object obj, Object[] objArr) throws Exception {
    BA.senderHolder.set(obj);
    if (BA.fastSubCompare(str, "CHANGEICON")) {
        return _changeicon();
    }
    if (BA.fastSubCompare(str, "HIDEICON")) {
        return _hideicon(((Boolean) objArr[0]).booleanValue());
    }
    return BA.SubDelegator.SubNotFound;
}
```

What distinguishes “Souvenir Photo” from conventional malware is its reliance on trust rather than exploitation. The application does not depend on software vulnerabilities or advanced

exploits, but instead capitalizes on the social and political environment created by censorship, access scarcity, and fear. Users are encouraged to install the application through direct messaging or themed pretexts, turning everyday digital interactions into vectors of surveillance.

Charming Kitten (APT35): Deceptive Access, Espionage Toolchains, and State Control

In autumn 2025, a series of coordinated disclosures published by the KittenBusters project[17] provided the first systematic exposure of the operational infrastructure associated with the Charming Kitten advanced persistent threat (APT35).[18] Rather than focusing on isolated incidents or attribution claims, these disclosures mapped the group's active phishing domains, malware delivery pipelines, command-and-control infrastructure, and a portfolio of bespoke surveillance tools deployed across multiple campaigns. This shift toward infrastructure-level documentation marked a turning point in how Charming Kitten's operations could be understood, analyzed, and contextualized.[19]

[17] KittenBusters; "CharmingKitten"; September 2025; Link

[18] MITRE; "Magic Hound"; Link

[19] Nariman Gharib; "Massive Leak Exposes Inner Workings of Iranian Hacking Group Charming Kitten"; Sep 30, 2025; Link, Archive

Nariman Gharib; "Part two and three of the leaked Charming Kitten files reveal operations across five continents"; Oct 16, 2025; Link, Archive

Nariman Gharib; "Episode 4: Inside Charming Kitten's Financial Operations and Infrastructure Network"; Oct 28, 2025; Link, Archive

Associated Group Descriptions

Name	Description
TA453	[6][5][7]
COBALT ILLUSION	[4]
Charming Kitten	[8][9][10][2][6][7]
ITG18	[11]
Phosphorus	[12][13][14][3][6][7]
Newscaster	Link analysis of infrastructure and tools revealed a potential relationship between Magic Hound and the older attack campaign called Newscaster (aka Newscasters).[15][1]
APT35	[1][3][7]
Mint Sandstorm	[16]

Charming Kitten has long been assessed by independent researchers as a state-aligned threat actor operating in close coordination with Iranian security institutions. Multiple investigations have linked its campaigns, targeting priorities, and operational timing to the intelligence objectives of the IRGC Intelligence Organization, often referenced internally as Unit 40.[20] Unlike financially motivated cybercrime groups, Charming Kitten's operations consistently reflect strategic intelligence collection goals, including surveillance of journalists, activists, researchers, dissidents, and foreign policy targets. Its activity patterns indicate sustained, long-term engagement focused on access maintenance, persistence, and behavioral monitoring rather than rapid or opportunistic exploitation.

The significance of the KittenBusters disclosures lies not only in attribution, but in the rare visibility they provide into Charming Kitten's tactics, techniques, and procedures (TTPs). The

[20] Amirhadi Anvari; Iran International; "Charming Kitten exposed: spy unit led Iran's surveillance for deadly plots"; Nov 2025; Link, Archive
Nariman Gharib; "Department 40 Exposed: Inside the IRGC Unit Connecting Cyber Ops to Assassinations"; Nov 23, 2025; Link, Archive

leaked materials reveal a clear operational preference for deceptive access vectors: phishing frameworks designed to harvest credentials and active sessions, modular malware loaders, remote access trojans, and server-side tooling that enables scalable account takeover and data aggregation. These capabilities are not deployed in isolation, but as part of an integrated surveillance ecosystem in which access, persistence, and data extraction are tightly coupled.

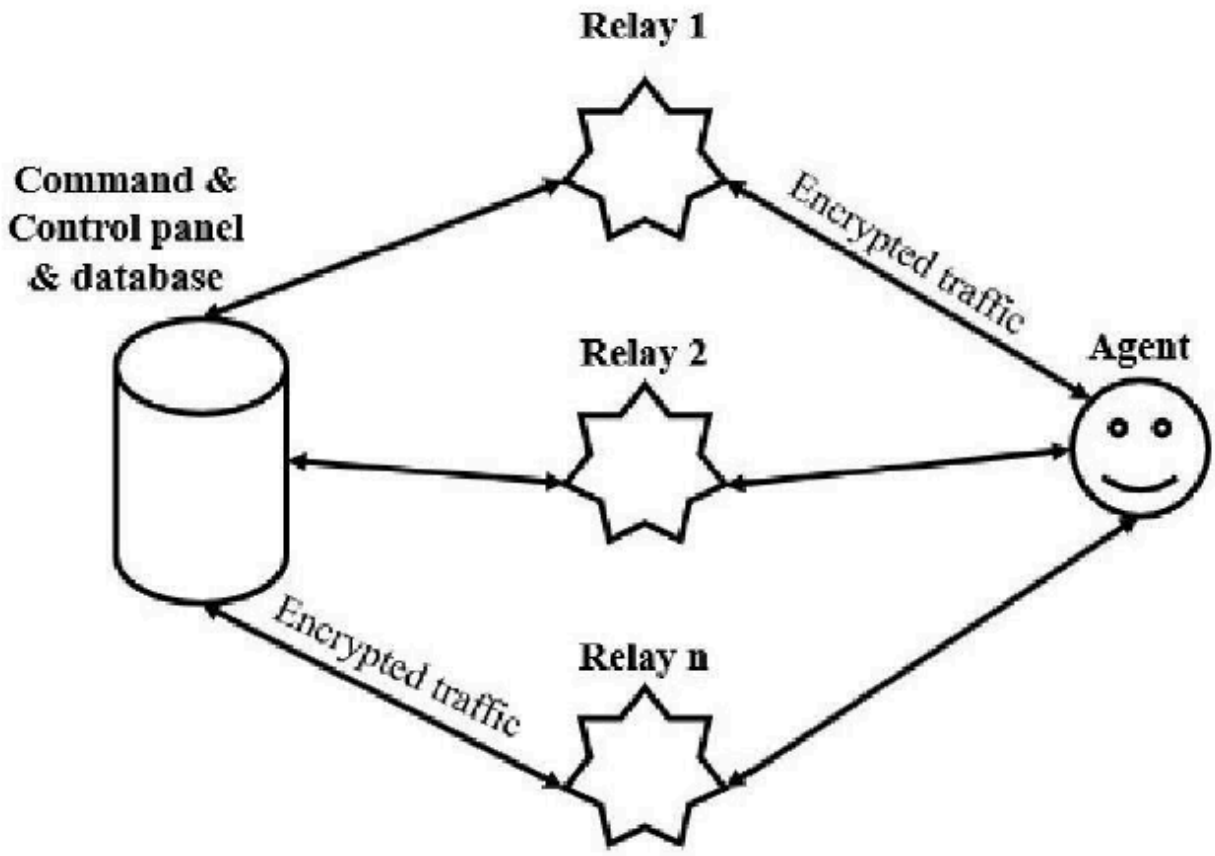
Subsequent leaks and analyses have further demonstrated how Charming Kitten's tooling intersects with broader Islamic Republic's surveillance strategies.[21] Rather than relying exclusively on zero-day exploitation, the group repeatedly weaponized user behavior under censorship pressure, exploiting demand for VPNs, cloud access, and alternative connectivity. This approach aligns closely with domestic interception policies and platform capture efforts, blurring the boundary between covert cyber espionage and institutionalized surveillance. The current wave of disclosures, including internal documentation and tool repositories, offers rare insight into how offensive cyber capabilities are operationalized in tandem with national internet control mechanisms.

Taken together, these leaks establish Charming Kitten not merely as a discrete threat actor, but as a key operational arm within a wider surveillance architecture. Its toolchains, infrastructure, and operational logic provide a concrete case study of how deceptive access, remote intrusion, and behavioral monitoring converge into a durable system of digital control. The following sections examine these tools in detail, tracing how individual implants and frameworks serve broader intelligence and governance objectives.

[21] Nariman Gharib; "Charming Kitten Leak Continues: Payroll Data and a Stolen IAEA Document"; Dec 9, 2025; Link, Archive

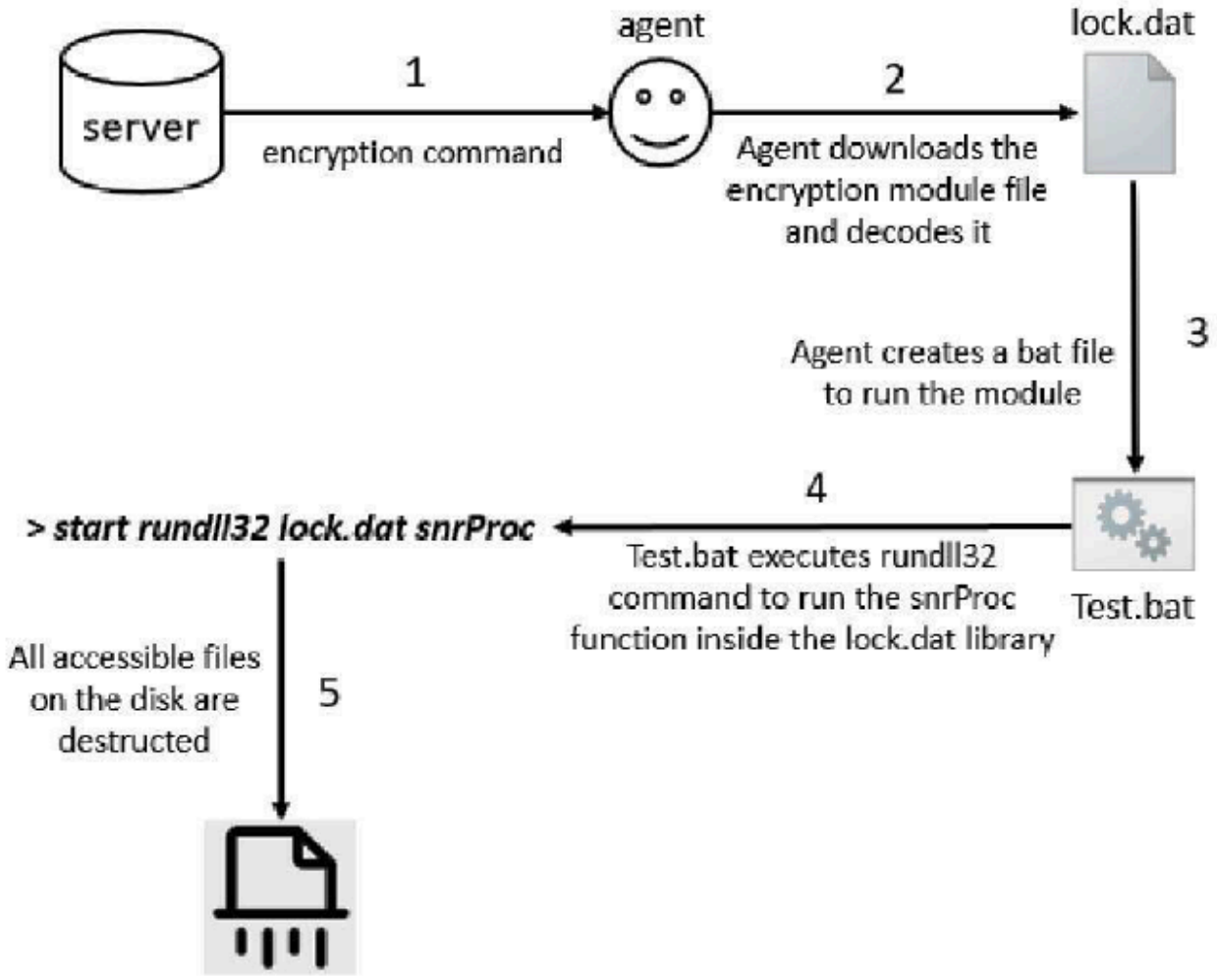
Modular Windows Remote Access Trojan with Relay-Based Command and Control

One of the core tools uncovered through the Charming Kitten internal disclosures is a Windows-based Remote Access Trojan (RAT) built around a modular architecture. The malware is composed of multiple interoperable components coordinated by a central controller module, commonly referred to as main. This primary module manages execution flow, communication with command-and-control (C2) infrastructure, and the activation of auxiliary modules responsible for data collection and system interaction.



The RAT supports both direct and indirect communication with its operators. In indirect mode, traffic is routed through intermediary relay servers, a design choice that obscures the origin of commands and increases operational resilience against takedowns and attribution. This relay-based C2 architecture enables sustained access even when individual nodes are disrupted.

Functionally, the malware provides full remote control capabilities, including command execution, file upload and download, and dynamic tasking. Its modular design allows operators to selectively deploy functionality depending on the target profile. Identified modules include components for credential harvesting, keylogging, browser data extraction, and targeted data collection from specific applications such as messaging platforms. Evidence of persistence mechanisms indicates that the malware is designed to survive system reboots and maintain long-term access to compromised devices.



Technical analysis shows that execution is frequently achieved through legitimate system utilities such as rundll32.exe, a technique commonly used to evade basic security controls by blending malicious activity with normal operating system behavior. Data collected from victims is stored locally in structured files and exfiltrated through the established C2 channels.

نام ماژول	عملکرد
central.dat	آخرین نسخه برنامه اصلی main است که در صورت به روزرسانی بدافزار دانلود خواهد شد.
creds.dat	ماژول استیلر فایرفاکس
lock.dat	ماژول رمزنگاری فایلها
logging.dat	ماژول کیلاگر
msg.dat	ماژول تلگرام

Taken together, this tool represents a mature, state-aligned surveillance implant rather than an opportunistic cybercrime utility. Its architecture, feature set, and operational discipline are consistent with long-term espionage objectives, reinforcing assessments that Charming Kitten functions as an advanced persistent threat engaged in sustained monitoring of targeted users.

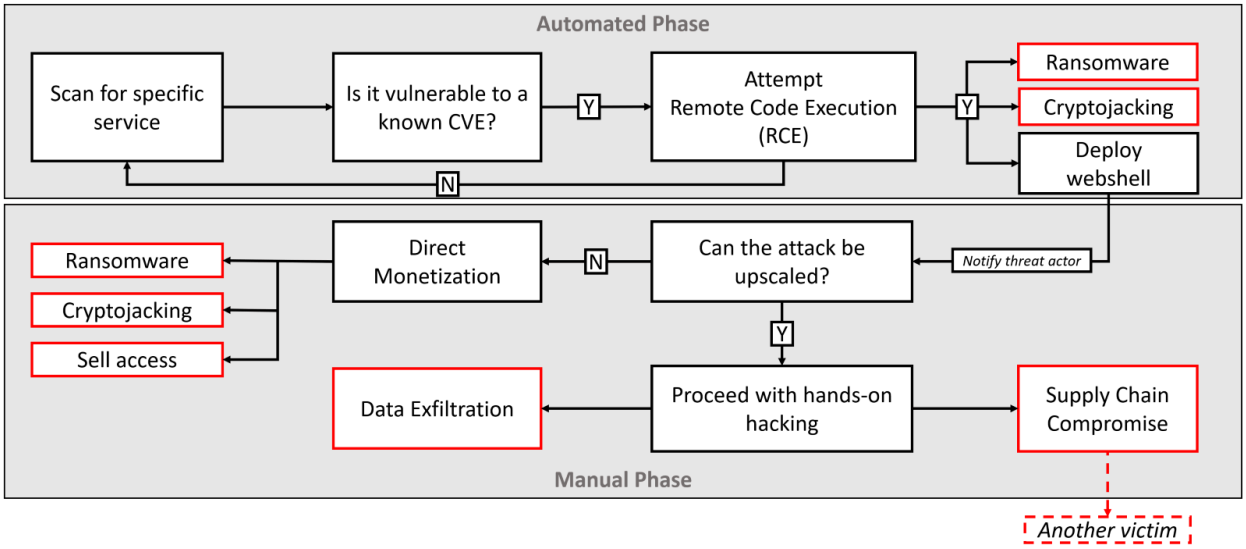
BellaCiao: Modular Windows Loader at the Core of Charming Kitten Operations

BellaCiao is a modular Windows-based malware framework that had previously been attributed to the Charming Kitten advanced persistent threat (APT35) through independent cybersecurity research, and whose attribution has now been confirmed through the KittenBusters project

leak.[22] Unlike full-featured remote access trojans, BellaCiao functions primarily as a loader and orchestration platform, designed to establish persistence, maintain stealthy access, and deploy additional surveillance payloads on demand.

Technical analysis shows that BellaCiao operates through a highly modular design, enabling operators to dynamically load and execute secondary components without modifying the core implant. This approach reduces detection risk and allows the malware to adapt to different operational requirements. The framework supports multiple execution modules, including components for command execution, file retrieval, system reconnaissance, and payload delivery. Communication with command-and-control infrastructure is typically encrypted and structured to blend into legitimate network traffic.

[22] Martin Zugec; Bitdefender; "Unpacking BellaCiao: A Closer Look at Iran's Latest Malware"; Apr 26, 2023; Link, Archive
Ravie Lakshmanan; The Hacker News; "Charming Kitten's New BellaCiao Malware Discovered in Multi-Country Attacks"; Apr 26, 2023; Link, Archive
Jai Vijayan; Dark Reading; "'BellaCiao' Showcases How Iran's Threat Groups Are Modernizing Their Malware"; Apr 28, 2023; Link, Archive
Jonathan Greig; The Record; "Iran APT using 'BellaCiao' malware against targets in US, Europe and Asia"; Apr 30, 2023; Link, Archive
Ravie Lakshmanan; The Hacker News; "Iran's Charming Kitten Deploys BellaCPP: A New C++ Variant of BellaCiao Malware"; Dec 24, 2024; Link, Archive



BellaCiao is commonly delivered through spear-phishing campaigns, often using weaponized documents or installer-style droppers that exploit user trust rather than software vulnerabilities. Once deployed, the malware establishes persistence using registry modifications and scheduled execution mechanisms, ensuring continued access even after system restarts. Its low-profile behavior and reliance on legitimate system processes allow it to evade many signature-based detection systems.

Security researchers have identified BellaCiao as a foundational component in several Charming Kitten campaigns, acting as a staging platform for more intrusive spyware and data-exfiltration tools. This separation between the initial implant and later payloads reflects a deliberate operational strategy: minimizing exposure during early compromise while retaining the ability to escalate surveillance capabilities when required.

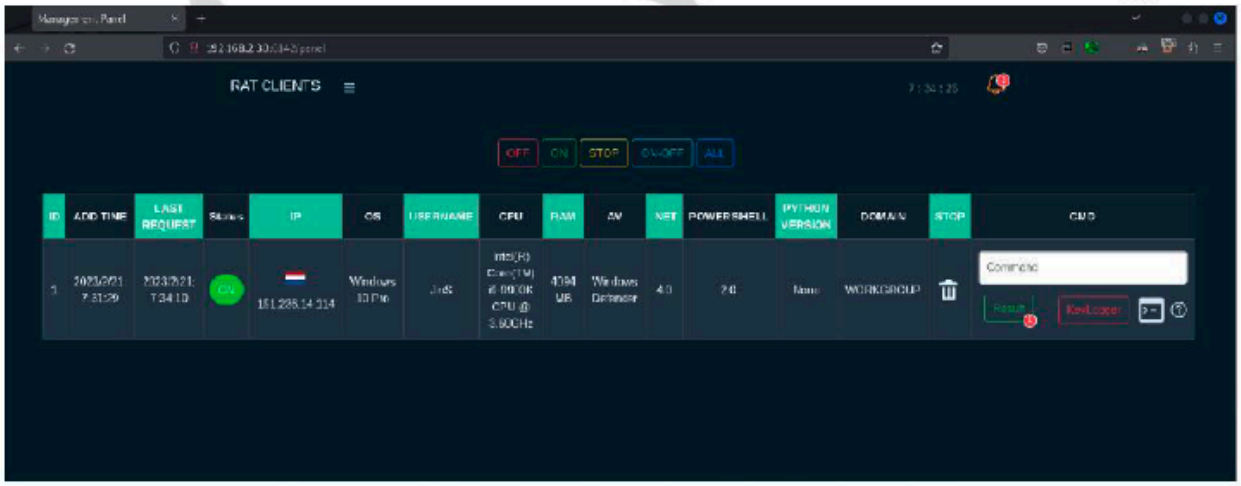
The use of BellaCiao underscores the evolution of Charming Kitten from isolated phishing operations toward a structured, multi-layered espionage framework. Rather than deploying monolithic spyware, the group relies on flexible loaders that integrate seamlessly into victims' systems and enable long-term monitoring aligned with intelligence collection objectives.

RAT-2Ac2; Preliminary Technical Report on a Modular Remote Access Tool

RAT-2Ac2 is documented in an internal “preliminary report” dated March 2023, which describes a fully operational remote access tool designed for victim device control and data collection. Rather than presenting a generic overview, the report details concrete implementation aspects, including system architecture, deployment requirements, operator-facing panels, and a catalog of supported commands and modules.

The report describes a client–server design in which the client component is implemented in .NET/C#, while the server backend is developed in Python using the Flask framework. Communication is routed over HTTPS and supported by a relay-based infrastructure, allowing operators to manage multiple infected clients through a centralized control panel.

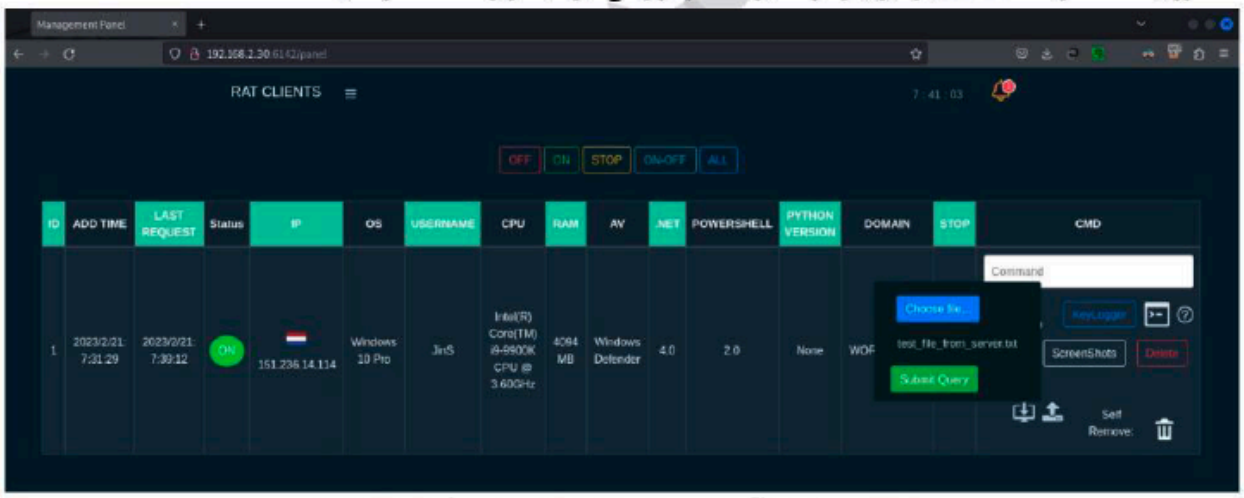
برای اجرا و راه‌اندازی امکان keylogger، می‌بایست در سامانه دستور keylogger ثبت شود. سپس دکمه keylogger در صفحه به رنگ قرمز در آمده و منتظر دریافت نتایج می‌شود. کاربر (Client) پس از دریافت این دستور اقدام به ثبت اطلاعات صفحه کلید در یک فایل به صورت مخفی کرده و نتایج را در پاسخ برای سامانه ارسال می‌کند. پس از دریافت این اطلاعات دکمه keylogger در سامانه به رنگ آبی در می‌آید و در صورت کلیک بر روی دکمه نتایج دریافتی نمایش داده می‌شود. (تصویر ۸)



تصویر ۸ – دستور KEYLOGGER پس از ثبت در سامانه و در حالت انتظار برای دریافت نتایج

Functionally, RAT-2Ac2 provides core surveillance and control capabilities commonly associated with remote access trojans. These include remote command execution via a shell interface, file upload and download, remote desktop control through VNC, and keystroke logging. The report also documents system profiling features, including the collection of device and environment attributes such as operating system details, hardware characteristics, network identifiers, and installed security products.

برای استفاده از قابلیت بارگذاری file بر روی سیستم هدف، ابتدا می‌بایست در سامانه اقدام به باگذاری file مدنظر و در قسمت ثبت دستورات در panel اقدام به وارد کردن عبارت UPLOAD=/path/to/file/yourfile.format، و به جای عبارت path to file آدرس و مسیر قرار گیری فایل مدنظر و نام فایل مدنظر قرار می‌گیرد. پس از ثبت این دستور فایل از روی سامانه توسط client بارگیری و در مسیر مدنظر قرار می‌گیرد.(تصویر ۱۳ ، ۱۴ و ۱۵)



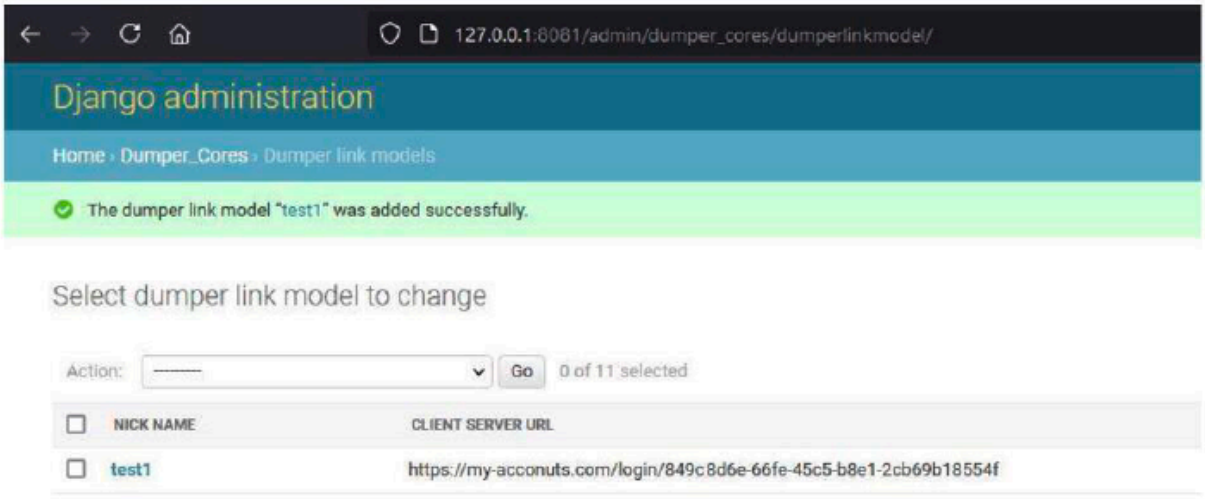
تصویر ۱۳- بارگذاری file مدنظر بر روی سامانه به منظور بارگیری آن توسط CLIENT

Beyond its core capabilities, the report highlights operational mechanisms intended to support stealth and traffic management, including configurable manipulation of network request headers. The inclusion of server setup instructions and deployment workflows indicates that RAT-2Ac2 is not a conceptual prototype, but a tool intended for real-world operational use, providing a structured interface for persistent access, continuous monitoring, and staged tasking against targets.

Deceptive Delivery Infrastructure Based on Image-Driven Lures

In another document from the same leak, a deceptive content delivery infrastructure is described which Charming Kitten uses to lure targets and control access to staged content prior to malware deployment. Rather than functioning as a surveillance implant or exploit, this

system operates as a controlled redirection and delivery platform, enabling operators to generate trusted-looking links, manage user sessions, and selectively serve files or payloads to targeted users.



در آدرس زیر میتوانیم لاگ های لینک ایجاد شده را مشاهده نماییم.

127.0.0.1:8081/google_account_v1/dumper_links

The infrastructure relies on web-based panels, SSH-managed servers, and configurable redirect chains, enabling operators to track access attempts, enforce conditional restrictions, and guide victims through multiple stages of interaction. By embedding malicious delivery within seemingly legitimate links or documents, this approach reduces suspicion and increases the likelihood of successful compromise. Such delivery mechanisms play a critical role in

Charming Kitten's operations by bridging social engineering with subsequent deployment of spyware and access tools.

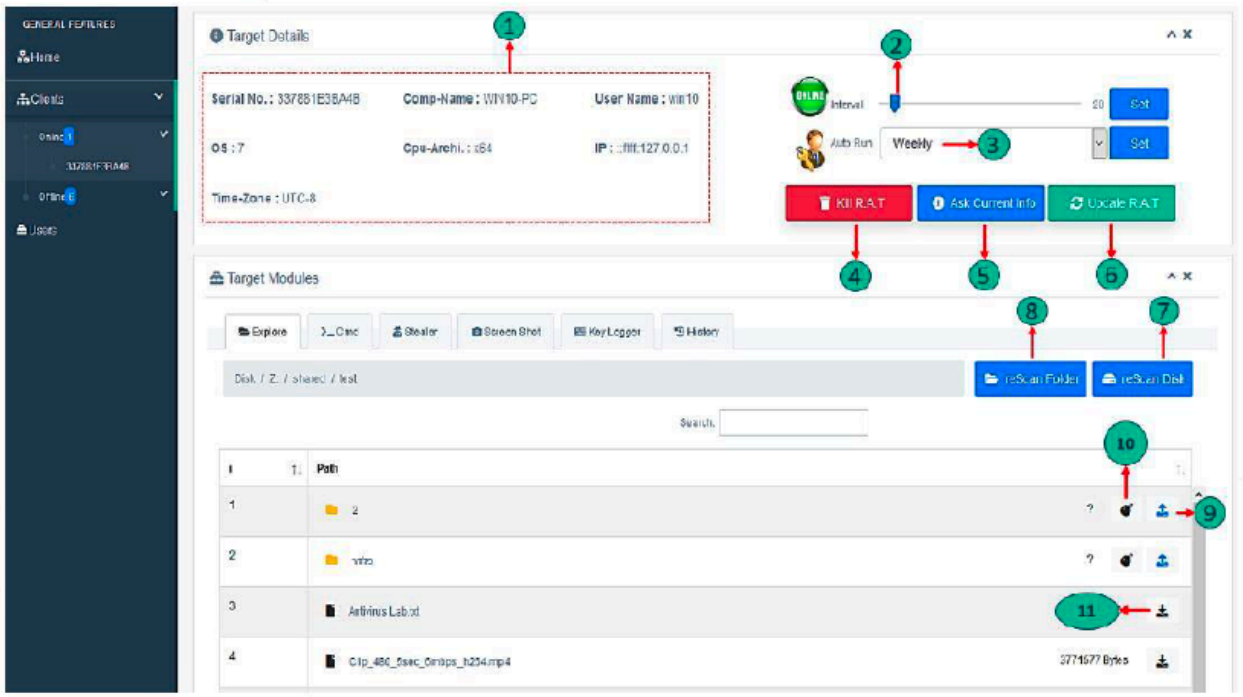
Thaqeb: A Remote Access Trojan Within Iran's Institutional Surveillance Architecture

"Thaqeb" (or Sagheb) is another full-featured Remote Access Trojan (RAT) documented in an internal technical report leaked from the Charming Kitten infrastructure. Unlike improvised malware or ad-hoc spyware, Thaqeb is presented as a structured surveillance platform, complete with a centralized management panel, modular client architecture, and a broad set of espionage and control capabilities. The documentation makes clear that Thaqeb is designed not merely for intrusion, but for sustained monitoring, behavioral tracking, and long-term control of infected systems.

At the technical level, Thaqeb operates through a classic command-and-control (C2) model, allowing operators to manage multiple compromised systems simultaneously. The malware supports remote command execution, file system access, keystroke logging, screenshot capture, and data exfiltration. It also includes specialized modules for harvesting credentials and extracting data from popular applications, including web browsers and messaging clients. These capabilities allow operators to reconstruct a detailed picture of a target's digital life, communications, and routines.

تصویر ۲ – صفحه اصلی سامانه ثاقب

A notable aspect of Thaqeb is its emphasis on persistence and stealth. The system is explicitly designed to remain undetected by security software, employing anti-debugging techniques, delayed execution logic, and obfuscation methods intended to evade antivirus detection. Communication with the C2 infrastructure is structured to minimize suspicion, and the documentation references the use of indirect routing mechanisms, including anonymization layers, to obscure operator activity.



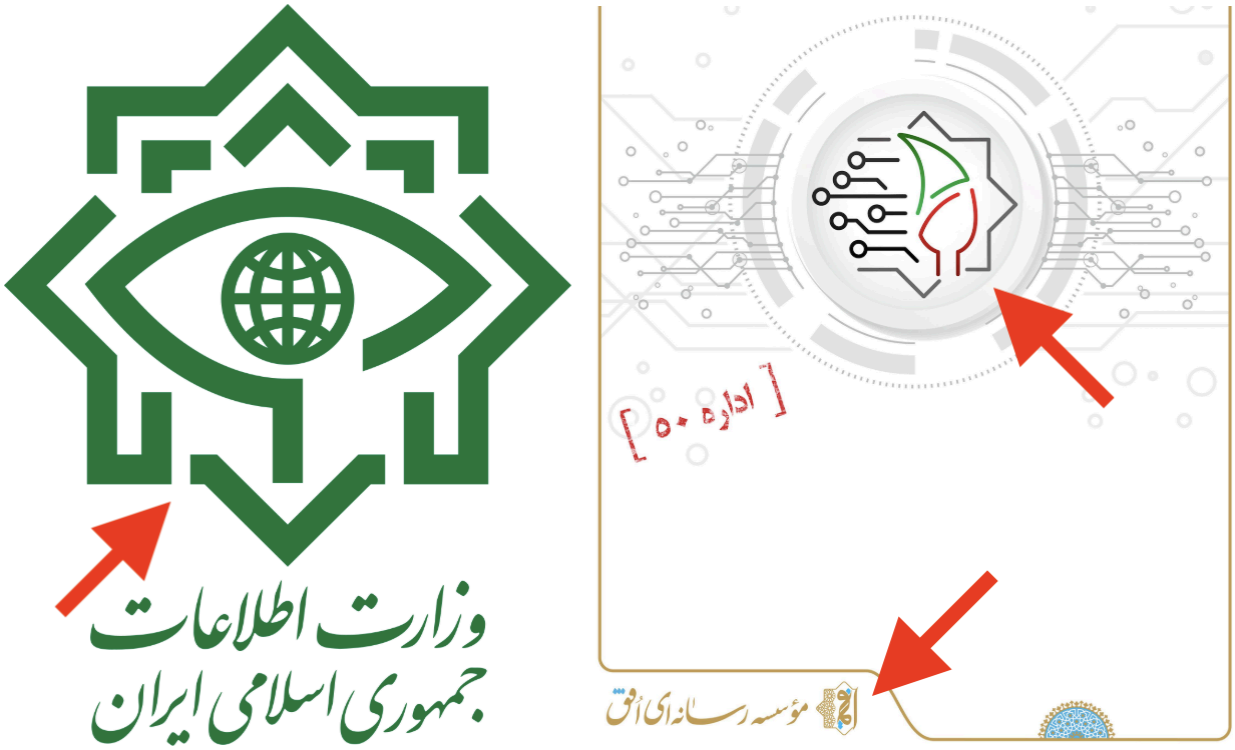
تصویر ۳ – پنل راهبری بدافزار ثاقب

Beyond its technical features, the leaked documentation reveals that Thaqeb is not a generic criminal tool but part of an organized surveillance workflow. The presence of user management features, logging systems, and client generation interfaces indicates deployment by trained operators rather than opportunistic attackers.

تصویر ۶ – صفحه Screen Shot در پنل راهبری بدافزار ثاقب

From a public interest perspective, Thaqeb illustrates how surveillance in the Islamic Republic of Iran extends far beyond filtering and platform control. Tools like Thaqeb enable direct intrusion into personal devices, bypassing legal safeguards and operating entirely outside transparent judicial oversight. The use of such spyware transforms private computers into sensors for intelligence collection, eroding privacy not through visible censorship, but through covert and continuous monitoring.

A final, revealing detail concerns visual identity. The branding associated with Thaqeb closely mirrors the official insignia of Iran's Ministry of Intelligence (MOIS), even though technical and contextual evidence links the tool's operational use to networks aligned with the IRGC-IO. This apparent mismatch is unlikely to be accidental; rather, it reflects a deliberate logic of institutional ambiguity, where symbols function as cover and attribution boundaries are intentionally blurred.



This pattern aligns with independent research findings. Case studies and subsequent analyses of Iran's hybrid cyber units demonstrate that cooperation, shared infrastructure, and tactical overlap between the MOIS and the IRG-IO are recurrent features of Iranian cyber espionage.[23] Within this framework, Thaqeb should be understood not as a standalone tool, but as an artifact of a layered institutional architecture in which tool development, operational deployment, and organizational deniability are tightly interwoven.

[23] Saher Naumaan; Proof Point; "Crossed wires: a case study of Iranian espionage and attribution"; Nov 5, 2025; Link, Archive

Platform Capture: Cloning, Governance-Compliant Shells, and Application-Level Control

Beyond spyware deployment and deceptive access tools, the Islamic Republic of Iran has pursued a more structural form of surveillance: the capture and manipulation of digital platforms themselves. Rather than relying on individual device compromise, this approach targets the application layer, exploiting users' trust in widely used services and transforming platforms into instruments of monitoring, control, and behavioral analysis.

This strategy has taken multiple forms, including traffic interception, reverse engineering of application behavior, large-scale data aggregation, and in some cases, full cloning of foreign platforms. Collectively, these efforts constitute a hidden ecosystem of platform-level surveillance, designed to extract identity, metadata, and behavioral patterns without the visibility typically associated with malware campaigns.

These trends reveal a coherent policy framework in which foreign digital platforms are treated as legitimate targets for infiltration, replication, and functional substitution. Unlike spyware implants that operate at the level of individual devices, platform capture operates structurally and at scale. Once users are redirected to state-controlled proxies or cloned services, granular data collection becomes seamless, encompassing search behavior, timestamps, content exposure, and device-level identifiers. This approach enables persistent surveillance while remaining largely invisible to the public, embedding control directly into the digital environments that users rely on daily.

Governance-Compliant Shells and Third-Party Surveillance Applications

In the Islamic Republic's digital control strategy, governance-compliant shells, state-approved versions of messaging platforms or social media apps, serve as structural instruments for monitoring user activity, intercepting private communications, and enforcing censorship. Rather than blocking access outright, these "shells" offer a familiar interface built on top of foreign services, but routed through domestic infrastructure that enables content filtering, metadata harvesting, and behavioral profiling.

The clearest examples are Golden Telegram and Hotgram, two modified versions of the Telegram app developed by the domestic firm Raahkaar Sarzamin Hooshmand. These apps gained widespread popularity after Telegram was blocked by judicial order in 2018, offering uncensored access, on the surface, while secretly enabling deep surveillance. Investigations revealed that both apps harvested sensitive user data, including identity verification codes, and were actively censoring content by blocking access to independent news channels such as BBC Persian and human rights organizations.[24] Telegram itself issued a warning about these apps, and they were eventually removed from Google Play for privacy violations.[25]

Despite official denials, leaked documents and public statements confirm state involvement in promoting these shells. A. Firouzabadi, then-Secretary of the SCC, publicly stated that these Telegram clones were supported by the Ministry of ICT to develop infrastructure independent of Telegram's servers. Although M. J. Azari Jahromi, then-Minister of ICT, denied these claims;

[24] Center for Human Rights in Iran; "Why Did Telegram Warn Users That Iranian Versions of the Telegram App - Talaeii and Hotgram - Are 'Unsafe'?"; Dec 17, 2018; Link, Archive

[25] Vitor Ventura; Cisco TALOS; "Persian Stalker pillages Iranian users of Instagram and Telegram"; Nov. 5, 2018; Link, Archive

however, Golden Telegram and Hotgram remained operational after Telegram's shutdown, enjoying de facto government endorsement .[26]

[26] Durov Post Pavel Durov post on X (formerly Twitter); Oct. 29, 2017; Link, Archive
IRNA; "Minister of ICT: We Do Not Confirm the Security of Iranian Telegram Versions"; Aug 12, 2018; Archive

سرزمین هوشمند

بسمه تعالی

شماره: ۹۶/۰۶۷۰
تاریخ : ۱۳۹۶/۰۷/۲۵

جناب آقای دکتر خرم آبادی

معاون محترم قضایی دادستان کل کشور در امور فضای مجازی

با سلام

احتراماً به عرض می رساند در راستای اجرای فیلترینگ و عرضه محتواهای مناسب بر بستر کلاینت ایرانی تلگرام، استارت آپ هایی تحت حمایت زیر مجموعه این شرکت اقداماتی که در ادامه توضیح داده خواهد شد انجام شده و یا در حال انجام می باشد که به شدت نیازمند کمک فکری آن مجموعه محترم می باشد.

موارد انجام شده ، درحال پیاده سازی و یا توسعه می باشد که شرح همه موارد به صورت زیر می باشد:

* **ایجاد بستر فیلتر کلمات در بخش جستجو :**

این بخش با استفاده از فیلترینگ هوشمند و بلک لیست کلمات جلوی سرچ موارد غیر اخلاقی را می گیرد که بانک استفاده شده به پیوست تحویل آن سازمان محترم می شود. در این بخش با استفاده از بات های نوشته شده در سمت این شرکت، امکان اضافه کردن کلمات جدید به لیست سیاه در کمترین زمان فراهم شده است. در این بخش بیش از ۱۰۰۰ کلمه در درون لیست موجود می باشد. که در همه لحظات در حال رشد و داده افزایی می باشد.

* **ایجاد بستر فیلتر کانال در بخش جستجو:**

در این بخش باتی طراحی شده است که با دریافت یک پست از کانال خاطی یا دریافت یوزر نیم کانال اقدام به حذف همه پستها و کانال مرتبط از لیست سرچ می کند.

* **ایجاد بستر فیلتر پست در بخش جستجو:**

در این بخش باتی طراحی شده است که با دریافت یک پست اقدام به حذف همه پستها از لیست سرچ می کند.

* **ایجاد بستر بلک لیست بر روی کلاینت ها :**

در این بخش لیستی وجود دارد که اسم هر کانالی که در آن قرار بگیرد بر روی هیچ یک از کلاینت های زیر مجموعه این شرکت باز نخواهد شد و این لیست می تواند از طریق یک بات، یک وب سرویس و به صورت دستی این لیست را تغذیه نمود.

The legal justification for these shells is rooted in SCC. In Resolution No. 96 of the Supreme Council of Cyberspace, various state bodies were tasked with examining "user access to beneficial foreign services through governance-compliant frameworks."[27] The same resolution defines concrete forms of governance compliance, including:

1. Access windows embedded within domestic platforms
2. Negotiations to establish in-country representation for foreign services
3. Diverse governance-compliant gateways developed through private-sector investment under state regulation

The term governance-compliant thus refers not merely to legal oversight, but to engineered control over what users can access, see, and share.

Beyond cloned apps, state institutions have explored 3rd party surveillance applications disguised as leg-tech or civic tools. In 2022, a team based at a government-affiliated accelerator submitted a proposal titled "DATAP: Evidence Documentation Platform" to the Filtering Committee.[28] The proposal claimed to support digital due process by creating a system for collecting and presenting electronic evidence to the judiciary.

The implementation, however, relied on covert infiltration: a 3rd party app designed to gain access to target users' chats, social media activity, and emails, often with deceptive consent prompts. The proposal stated:

[27] SCC; "Review of Measures to Increase the Share of Domestic Traffic and Counter Circumvention Tools"; Nov 13, 2024; Archive

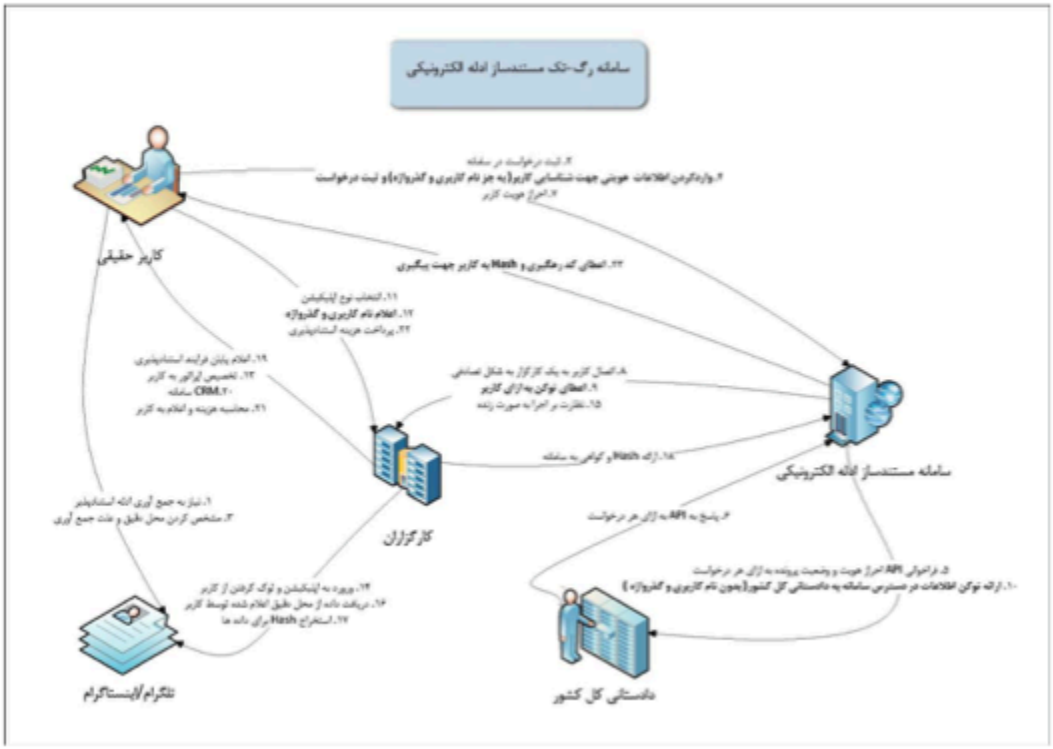
[28] Sharif RegTech Company; "Technical Proposal for the Electronic Evidence Documentation System"; Jul 5, 2022; Download

Factnameh; "Filtering Contractors in Iran"; Jan 28, 2024; Link, Archive

“This documentation system will use the 3rd party model to build trust between users and cyberspace and facilitate case review through reg-tech solutions.”

The needs assessment section called explicitly for: Screenshot capture of chats and posts, Access to account information across virtual platforms, And the ability to counter “misinformation.”

پروپوزال فنی "سامانه مستندساز ادله الکترونیکی"	
شرکت فناوری های تنظیم یار شریف	کارفرما : معاونت نظارت بر فضای مجازی دادستانی کل کشور



شکل ۵. نمودار جریان فرآیند ارتباط بین نهادی در اجرای راهکار با ایجاد سامانه نظارت بر مستندسازی ادله الکترونیک

This framing positioned mass surveillance as legal evidence gathering, enabling law enforcement to bypass platform-level security under the guise of civic regulation. The system further blurs the line between judicial oversight and intelligence surveillance.

Messaging App Exploits and Platform-Level Surveillance

One early example of such operations was an Instagram crawling bot deployed before the 2015 protocol upgrade, which allowed authorities to monitor user behavior across the platform. M.J. Azari Jahromi, later Minister of ICT, played a key role in launching this surveillance infrastructure.

جهرمی
برخی اشتباهات روبات اینستاگرام
To: amiri, Cc: karimi

March 14, 2015 at 10:24 PM
Details

با سلام
نتایج بررسی برای بهره برداری ارسال میگردد.

جهرمی

با سلام

نتایج بررسی به شرح ذیل تقدیم حضور می گردد.

- khaneye_maa نام قبلی ایشان hairmod بوده و تبلیغات غیر اخلاقی داشته است. رفع فیلتر شد
- which_brand به نظر خطای ربات بوده است. رفع فیلتر شد
- bolandgou نام کاربری قبلی ایشان bolandgou_creative_house بوده و صفحه ایشان پیشتر سفید تشخیص داده شده بود با این حال به سبب تکرار درج آگهی غیر اخلاقی در نام جدید سیاه شده بود. رفع فیلتر شد
- sepidclinic در تاریخ ۲۰۱۴/۰۵/۱۸ توسط دادستانی وارد پایگاه داده ها شده در نتیجه رفع فیلتر نشد.
- new.ideaa نام قبلی ایشان jok.zirnafi و نام کامل ایشان ++18 بوده است. نیازمند دستور برای رفع فیلتر
- lumpishs بیوگرافی قبلی ایشان Photo Fetish بوده نیازمند دستور برای رفع فیلتر
- zhesst نام قبلی ایشان pic_love_ بوده حاوی تصاویر غیر اخلاقی و در بیوگرافی تاکید داشته « بیجنبه ها فالو نکنن » . نیازمند دستور برای رفع فیلتر
- dokhtaro0ne به نظر خطای ربات بوده چرا که صفحه برای فروش بوده و همه نوع تصویری در آن یافت می شده است. رفع فیلتر شد.
- text irooni پیشتر رفع فیلتر شده بود.

One of the most notorious cases is the Shekar system, a database leaked in 2020 that exposed the private details of over 42 million Iranian Telegram users.[29] This included user IDs, phone numbers, and associated metadata. Although Telegram was officially banned by judicial order

[29] IranWire; “Hackers Claim Access to 42 Million Sepah Bank Records, Bank Denies Breach”; Mar 31, 2020; Archive
WebAmoz; “Who Is Responsible for the Disclosure of 42 Million Iranians’ Data on the Shekar System?”; Jun 20, 2020; Archive

in 2018, the platform remained widely used via circumvention tools, and it has long been subject to both policy-level pressure and covert monitoring. The Shekar leak revealed that Iranian authorities had quietly been building comprehensive identity-to-behavior maps, without any user consent or platform-level acknowledgment.

A broader proposal known as the SAAFTA Monitoring System, developed by a defense-affiliated institution and presented to the Attorney General's Office in 2017, outlined plans for persistent surveillance of Telegram traffic across Iran. SAAFTA aimed to categorize news channels, flag dissent, and classify behavioral patterns based on keyword detection and user interactions. The proposal's institutional origin, within the Ministry of Defense and Armed Forces Logistics, suggests military-grade interest in the strategic potential of social media surveillance.[30]

[30] Office of the Prosecutor General; "System for Monitoring and Tracking News and Telegram"; April 2017; download

Collectively, these efforts reflect a policy framework in which foreign platforms are treated as legitimate targets for both infiltration and replication, with the ultimate goal of maintaining social control through digital oversight. Unlike spyware implants which target individual users, these techniques are structural, systematic, and often invisible to the general public.

A key risk lies in the modular and scalable nature of such operations. Cloned platforms and proxy interfaces can be updated, scaled across services, or ported to mobile apps with minimal cost. Once users are rerouted to state-controlled versions of globally trusted services, granular

data capture becomes seamless, from search terms and timestamps to content curation and device fingerprinting.

User Data as an Intelligence Asset: Platforms, Backdoors, and State-Aligned Apps

In addition to wiretaps and spyware campaigns, a significant yet underexamined pillar of the Islamic Republic's surveillance apparatus is its access to user behavioral data generated by ordinary internet services. Rather than targeting individuals through implants or attacks, this layer of oversight relies on privileged access to backend systems of widely used Iranian platforms, often granted without legal authorization or judicial transparency.

Leaked documents from late 2022 revealed that several domestic internet companies had granted the Prosecutor's Office and the Filtering Committee special administrative access to user data dashboards.[31] These access points allowed the government to obtain identity records, usage patterns, and sensitive metadata without official court orders. Companies such as ZarinPal, Vigool, Aparat, Bam, and Cafe Bazaar were named among those offering such privileged access. While some firms later claimed these measures were intended to combat cybercrime, the absence of formal legal procedures casts serious doubt on these justifications.

[31] Anonymous OpIran; Post on Telegram; Nov. 3 2022; Archive

مهرداد قورچیان (Support)
[ArvanCloud] Re: مسدود سازی فوری
To: واحد نظارت بر ارائه دهندگان خدمات میزبانی,
Reply-To: Support
October 15, 2019 at 6:06 AM

##- لطفن جواب خود را در بالای این خط تایپ کنید -##

درخواست شما با شماره 23468 بروزرسانی شده است. برای پاسخ دادن نیز میتونید به این ایمیل reply ارسال کنید.

مهرداد قورچیان (ArvanCloud)
15 اکتبر، 15:36 (+0330)

با سلام و احترام

این وب سایت داخل آروان هاست نشده است و فقط از سرویس cdn استفاده می کند .
دسترسی این سرویس برای این دامنه مسدود گردید.

پایدار باشید

واحد نظارت بر ارائه دهندگان خدمات میزبانی
15 اکتبر، 15:07 (+0330)

مدیر عامل محترم ابر آرون

با سلام و احترام

بنابر اعلام دبیرخانه کارگروه تعیین مصادیق محتوای مجرمانه نشانی زیر وفق ماده 23 قانون جرایم رایانه ای جهت مسدود سازی اعلام می گردد:

lilak.org

با توجه به اینکه آی پی نشانی فوق الذکر به نام آن شرکت ثبت شده است و یا میزبانی آن بعهده آن شرکت محترم می باشد، مقتضی است سریعا اقدامات لازم در خصوص مسدودسازی نشانی اعلام شده بعمل آورده و نتیجه را از طریق پست الکترونیکی itc@dci.ir اعلام نمایید.

ضمنا از میزبانی محتوای مذکور تحت نشانی جدید تا دستور رفع انسداد دبیرخانه کارگروه تعیین مصادیق محتوای مجرمانه خودداری نمایید و چنانچه مدیر تارنما نسبت به مسدودسازی نشانی اعلام شده اعتراض و شکایت دارد می تواند جهت پیگیری از طریق نشانی internet.ir شکایت خود را به دبیرخانه کارگروه تعیین مصادیق محتوای مجرمانه ارسال نماید.

ضمناً در صورت تاخیر در اجرای دستور برای شما اعلام جرم می گردد.

با سپاس | واحد نظارت بر ارائه دهندگان خدمات میزبانی / دبیرخانه کارگروه تعیین مصادیق محتوای مجرمانه | تلفن : 02138582314 - نمابر : 02133111669

One illustrative case of data misuse involves the navigation app Balad, developed by the Hezar Dastan Group,[32] the same conglomerate behind Café Bazaar, Iran's largest Android app marketplace, and Divar, a widely used classified ads platform. In October 2022, Balad published a statement that indirectly acknowledged public concerns over potential government access to its user data.[33] The implications of this were far-reaching: if such access existed in Balad,

[32] Crunchbase; Ava Hamrah Hooshmand Hezardastan; Link, Archive

[33] Peivast; "Hazardastan Reports: Possible Shutdown of Balad After Year-End / Dozens of Layoffs"; Oct 25, 2022; Archive

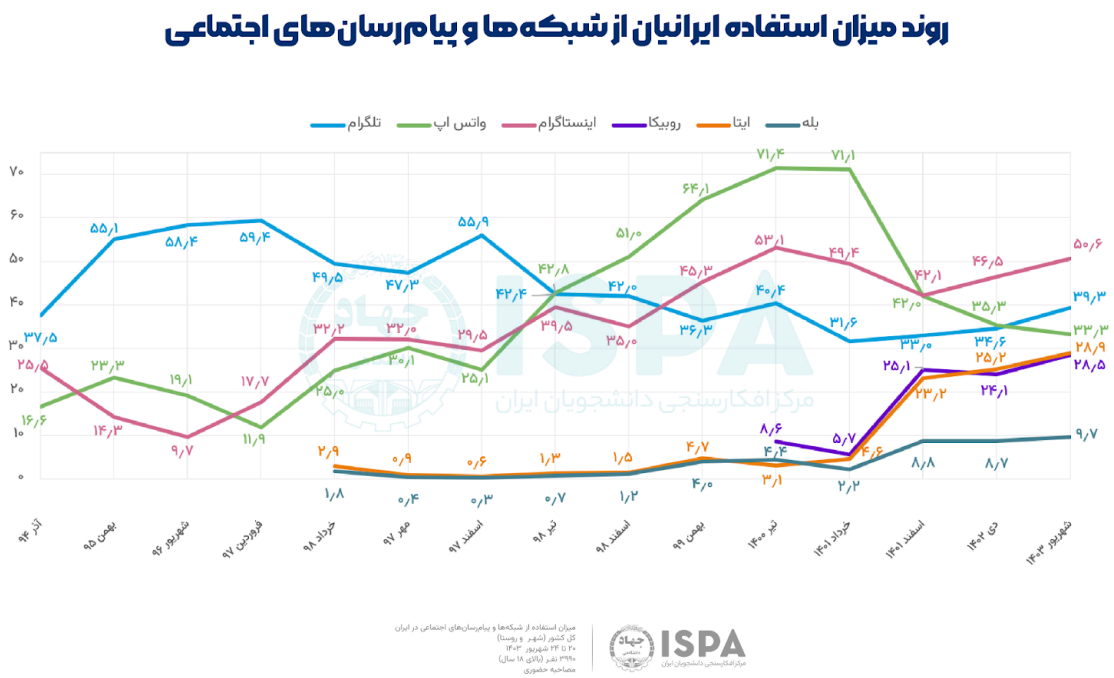
similar risks likely extended to Divar and Café Bazaar, given their shared backend infrastructure and ownership. This incident underscored the broader problem of user data exposure across dominant domestic platforms.

بیانیه گروه هزاردستان
در ارتباط با آینده فعالیت نقشه و مسیریاب بلد

بلد در پنجمین سال فعالیتش با وجود تیمی باانگیزه، کم‌نظیر و همدل و محصولی با بیش از ۱۰ میلیون کاربر فعال روزانه، به‌ناچار با ده‌ها نفر از همکارانش خداحافظی می‌کند. مدت‌هاست که راه‌های جذب سرمایه در فضای استارتاپی و بخش خصوصی کشور بسته مانده و ادامه دادن کسب‌وکارهایی که بازگشت سرمایه در بلندمدت را هدف خود قرار داده بودند و امکان رسیدن به نقطه سربه‌سر در کوتاه‌مدت را ندارند، سخت‌تر شده است. همچنان هیچ افق روشنی برای خروج سرمایه‌گذاران از کسب‌وکارهای بالغ‌تر اینترنتی وجود ندارد و این امید را برای آنها که سال‌های سال تا رسیدن به مرحله خروج فاصله دارند از بین برده است. از طرف دیگر ضمن نگرانی بابت محدودیت‌های اعمال شده بر اینترنت و امنیتی‌تر شدن فضا، آینده اینترنت در کشور چندان قابل پیش‌بینی نیست و برخی برخوردها به خصوص در ماه‌های اخیر ما را در درستی راهی که در پیش گرفته بودیم و توانایی خود در حفاظت از حقوق کاربران به شک انداخته است. ما بابت شرایط به وجود آمده برای همکاران‌مان متأسفیم و تمامی تلاش خود را به کار می‌گیریم که در فضای سخت و پرابهام فعلی، جابجایی این افراد توانمند و با استعداد در گروه، با سختی‌های کمتری همراه شود. ما ارائه خدمت توسط نقشه و مسیریاب بلد به کاربرانش را تا پایان سال جاری تضمین می‌کنیم. در عین حال به‌زودی در مورد آینده این محصول و تبعات آن برای میلیون‌ها کاربری که تمام این سال‌ها به آن اعتماد کرده‌اند اطلاع‌رسانی دقیق‌تر انجام خواهیم داد.

The Islamic Republic has invested heavily in cultivating a parallel ecosystem of state-aligned messaging platforms, including Rubika, Eitaa, Bale, iGap, Soroush, and Gap, under the guise of

“digital sovereignty.” These platforms operate under the financial and infrastructural backing of semi-governmental economic institutions and are intended not only to replace foreign apps but also to concentrate user communications within an environment of centralized control. While promoted as “national” alternatives, these apps have played an active role in granting privileged backend access to government entities, bypassing judicial oversight in the process. Recent surveys show Rubika, Eitaa, and Bale consistently rank among the most widely used messaging apps in Iran.[34]



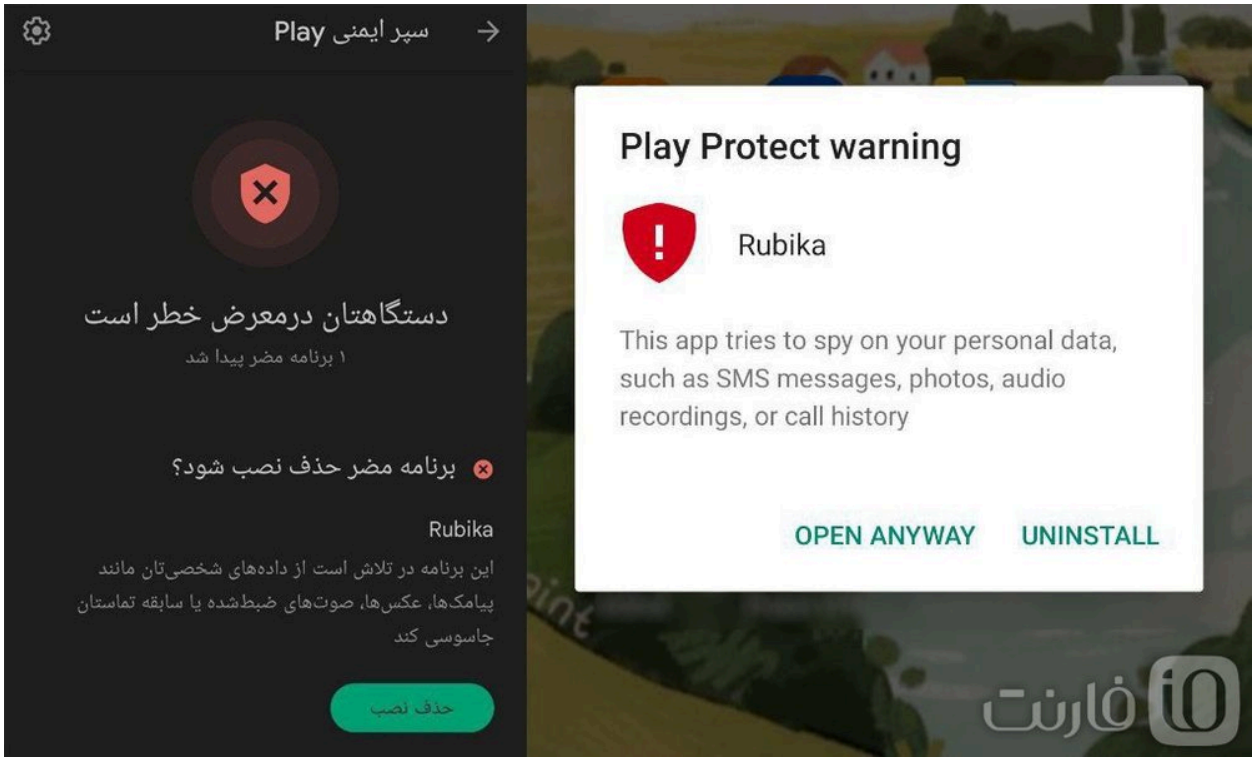
Independent technical audits, including a detailed investigation by the Open Technology Fund (OTF), have raised serious concerns about the privacy architecture of Rubika, Eitaa, and Bale.[35] None of these platforms adhere to basic international standards for secure messaging: data is

[34] ISPA; “Usage Rates of Messaging Apps and Social Media Among Iranians”; Sep 28, 2024; Archive

[35] Open Technology Fund; “Iranian Messaging Apps - Security Audit”; Archive

stored insecurely, cryptographic protocols are weak or improperly implemented, and app permissions are excessively broad. The findings suggest that these vulnerabilities are not accidental but structurally embedded, facilitating state access to sensitive communications under the guise of national infrastructure.

One of the most revealing moments came when Google Play flagged Rubika as a surveillance threat. The app, which had gained popularity in Iran for features like football betting and media streaming, was delisted due to violations of user privacy and potential spyware behavior. In retaliation, the Filtering Committee blocked access to Google Play itself, effectively shielding domestic apps from international scrutiny.[36] This episode illustrates the Islamic Republic's willingness to weaponize national infrastructure and platform policy in defense of surveillance-capable software.



[36] PC Jow; "Why did Rubica get a warning from Google's security shield?"; Oct. 3 2022; Archive

Iranian ICT and security officials have frequently cited this incident as evidence of foreign interference in domestic affairs, framing Google's action as part of a broader campaign against national platforms and they have not forgotten it.

Rubika was developed by semi-governmental economic holdings under the control of the Supreme Leader of the Islamic Republic, with the vision of becoming a national "super app" to rival foreign platforms. However, this ambition also enabled the platform to function as a surveillance proxy. By integrating backend access and enforcing opaque data practices, Rubika became a textbook example of how the state leverages private-sector façades for mass data extraction under the guise of domestic innovation.[37]

Bale has also faced serious privacy concerns, particularly following a major leak in which users' personal information, including private group content, was exposed.[38] The revelations showed that Bale administrators had access to private messages and user metadata, sparking public outrage and widespread criticism.

[37] Jamaran; "Whose Names Appear in 'Touska'?"; Mar 17, 2019; Archive
Khorasan Daily; "Touska's Monopoly Behind the Mask of MCI (Hamrah-e Aval)"; Mar 23, 2020; Archive
[38] Factnameh; "Ambiguities in the Bale Messenger's Statement on the Display of User Information"; Jul 23, 2023; Link, Archive

بیانیه اپلیکیشن بله دربارهٔ تصویر منتشرشده

بله

قبل از هر چیز همانطور که بارها خاطرنشان کرده‌ایم، امنیت و داده‌های شخصی کاربران، جزو خط قرمزهای بله است و با تمام وجود از آن حفاظت کرده، می‌کنیم و خواهیم کرد. این موضوع در این بیش از ۷ سال که از عمر بله می‌گذرد، همواره مورد تأکید بله بوده است.

بله، به عنوان یک پلتفرم، مانند تمام پلتفرم‌های دیگر موظف است تدابیر لازم را برای جلوگیری از کلاهبرداری‌ها و حفظ امنیت، دربارهٔ فعالیت کاربران خود در پلتفرم، اتخاذ کند. از این رو طبق سند قوانین و شرایط استفاده از بله که در آدرس terms.bale.ai منتشر شده «برای کانال‌ها و بازوهایی که به‌صورت عمومی در دسترس هستند، بله از الگوریتم‌های خودکار برای آنالیز پیام‌ها برای جلوگیری از انتشار محتوای مجرمانه استفاده می‌کند. همچنین کاربران می‌توانند درصورت مشاهدهٔ این موارد، گزارش آن را به بازوی پشتیبانی ارسال یا از گزینه «گزارش محتوای نامناسب» استفاده کنند. در این حالت بله این گزارش‌ها را بررسی می‌کند و درصورت تأیید مجرمانه‌بودن آن، طبق قانون، برخورد لازم انجام می‌شود. لازم به ذکر است با گروه‌هایی که بیش از هزار عضو داشته باشند، در حوزهٔ بررسی محتوا، مشابه کانال‌های عمومی رفتار می‌شود.»

آنچه در این تصویر از صفحهٔ مانیتور منتشر شده، مربوط به ابزار اجرایی همین موضوع است. این ابزار صرفاً حاوی محتوای منتشر شده در کانال‌های عمومی و گروه‌های بیش از ۱۰۰۰ عضو است که به‌صورت سیستمی و حسب نیاز کارشناسی، جهت مقابله با کلاهبرداری از کاربران مورد بررسی قرار می‌گیرد. بدیهی است که اطلاعات خصوصی کاربران، آی‌دی و شمارهٔ فرستندهٔ محتوا و مواردی از این قبیل **در جهت حفظ حریم خصوصی کاربران به عنوان خط قرمز بله**، در حیطهٔ این ابزار وجود ندارد و تنها محتوا به صورت بی‌نام در آن وجود دارد.

مجدداً تأکید می‌کنیم که حریم خصوصی کاربران خط قرمز ماست و با تمام وجود از آن حفاظت کرده و می‌کنیم و خواهیم کرد. **همچنین بله حق قانونی جهت پیگیری و برخورد با منتشرکنندگان این تصویر را برای خود محفوظ می‌دارد.**

Additional security vulnerabilities have been reported as well, including weak or absent encryption and unauthorized access to user data. These concerns have grown especially acute during periods of heightened government pressure for digital surveillance, fueling fears that Bale serves as a backchannel for state monitoring of sensitive communications.

In addition, other security problems have been reported in the Bale application. These problems include the lack of proper encryption and unauthorized access to user data. Especially at times when government pressure for monitoring online activities has increased, concerns about authorities' access to users' sensitive information have risen. The Eitaa messenger application has also been subject to concerns regarding privacy violations. In security investigations, similar problems to Rubika and Bale have been observed, including unauthorized access to user information.

The Eitaa messenger, another state-backed platform, has also been implicated in serious privacy concerns. Security audits and independent reports have flagged patterns of unauthorized data access, insecure transmission protocols, and embedded monitoring mechanisms. Like Rubika and Bale, Eitaa operates under close ties to government-affiliated investors and benefits from state promotion campaigns. However, its architecture reveals systemic vulnerabilities, including unencrypted data storage and administrative access to user content. These issues have become especially pressing during periods of heightened political repression, where metadata and message content from users, particularly journalists, activists, and protesters, could be harvested and analyzed. While the app brands itself as a secure domestic alternative, its operational model reflects a broader strategy of digital containment, turning communication tools into instruments of state control.

Collectively, these practices illustrate how the Islamic Republic has weaponized user data from both private sector startups and domestically promoted messaging platforms to construct an expansive, multi-tiered surveillance infrastructure. By exploiting backend access, opaque

partnerships, and the absence of meaningful legal safeguards, authorities have effectively bypassed judicial oversight to extract, monitor, and weaponize behavioral data. This hybrid model of public–private surveillance not only undermines user trust in domestic digital services but also redefines the role of technology firms as de facto extensions of the state's intelligence apparatus. As Iran's digital ecosystem becomes increasingly fragmented from global networks, the unchecked exploitation of user data represents a growing threat to civil liberties and digital autonomy.

Kashef System; Data Fusion, Relationship Mapping, and Operational Surveillance

Beyond individual surveillance operations, one of the most consequential dimensions of the Islamic Republic's digital control strategy is data aggregation. Rather than relying solely on isolated interceptions or targeted espionage, the state increasingly prioritizes the systematic collection, correlation, and analysis of user data across platforms, services, and identifiers. In this model, surveillance power derives not from single data points, but from the ability to fuse disparate datasets into coherent behavioral profiles.

Disclosures related to the Charming Kitten operations illustrate this logic in practice. The group's infrastructure was not limited to malware delivery or account compromise; it functioned as a data pipeline. Collected information including credentials, session tokens, metadata, contact networks, and content archives was stored, indexed, and cross-referenced over time. This enabled the construction of identity-to-behavior mappings that extend beyond individual incidents and support long-term monitoring objectives.

This aggregation-centric approach closely mirrors state-level practices observed across domestic platforms. Backend access to Iranian services such as messaging apps, marketplaces, navigation tools, and payment systems allows authorities to correlate behavioral signals across domains: communication patterns, location data, transaction histories, and social relationships. When combined, these datasets produce a level of visibility far exceeding that of conventional lawful interception.

Crucially, data aggregation collapses the distinction between targeted and mass surveillance. Even when access originates from discrete sources, the resulting datasets scale horizontally, capturing populations rather than individuals. This architecture transforms ordinary digital exhaust into an intelligence asset, enabling predictive analysis, social graph construction, and retrospective investigation without continuous active interception.

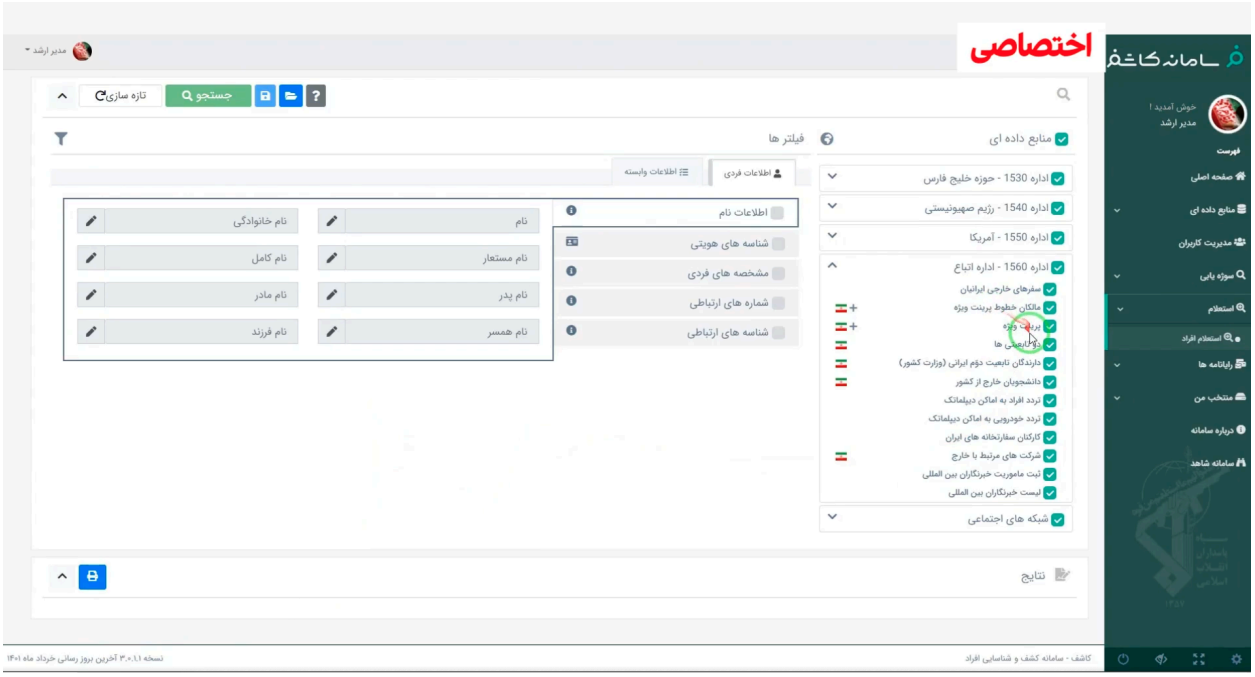
In this context, Charming Kitten should not be understood merely as a cyber-espionage actor, but as an operational prototype for data-driven surveillance. Its methods demonstrate how decentralized collection can feed centralized analysis, reinforcing a broader state strategy that treats user data as a strategic resource. The convergence of state-backed platforms, privileged backend access, and external data harvesting points toward an increasingly unified surveillance architecture, where aggregation itself becomes the primary mechanism of control.

One of the most consequential revelations about the Islamic Republic's covert surveillance ecosystem is the exposure of a platform known as Kashef, a centralized intelligence system designed to aggregate, correlate, and operationalize vast volumes of personal data.[39] Unlike the surveillance vectors discussed earlier in this section, Kashef does not rely on malware delivery, platform cloning, or direct user interaction. Instead, it functions as a back-end intelligence fusion engine that transforms disparate datasets into actionable relationship and behavioral maps.

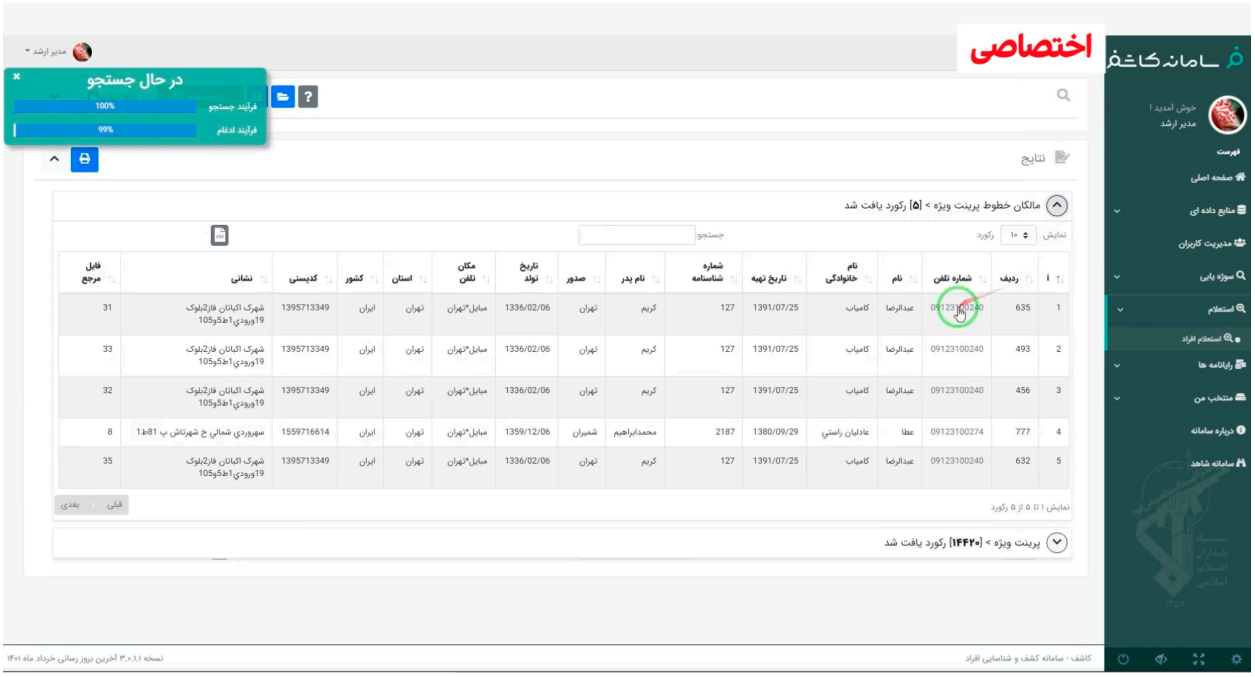
Investigations revealed that Kashef enables operators to input the identity of a target individual and retrieve a structured network of associations, including family members, frequent contacts,

[39] Nariman Gharib; "Department 40 Exposed: Inside the IRGC Unit Connecting Cyber Ops to Assassinations"; Nov 23, 2025; Link, Archive
Amirhadi Anvari; Iran International; "Charming Kitten exposed: spy unit led Iran's surveillance for deadly plots"; Nov 2025; Link, Archive

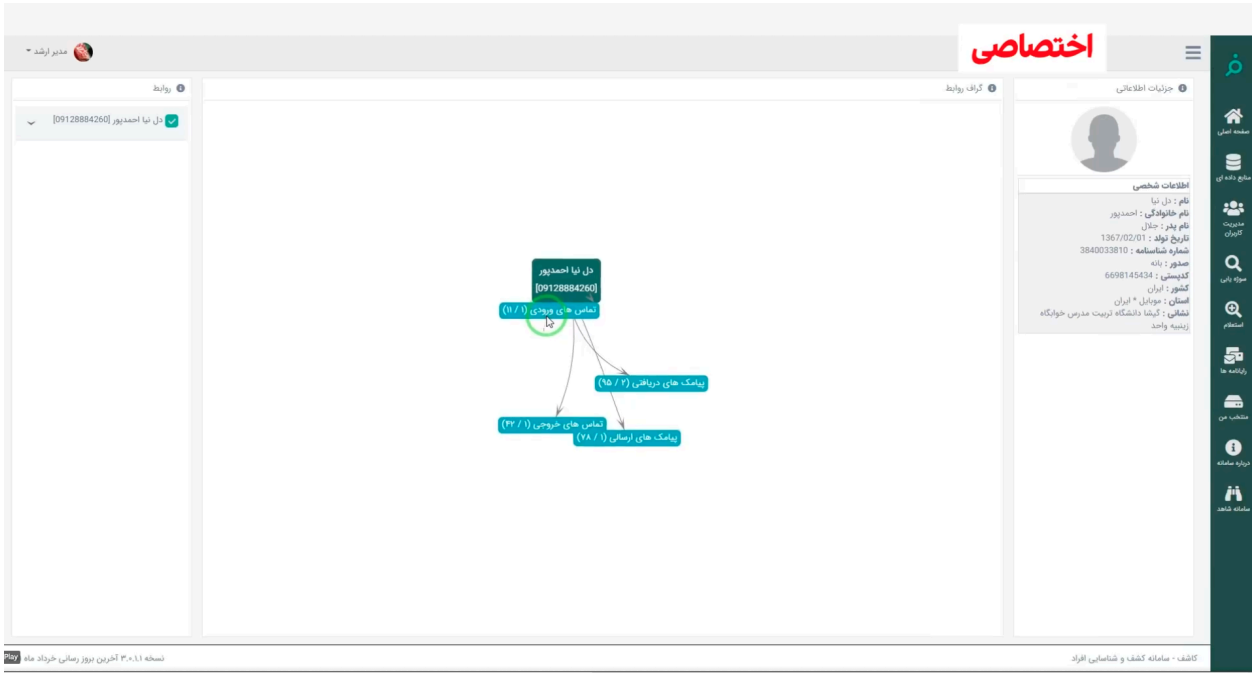
travel history, and geospatial presence. The system correlates metadata from multiple sources, such as mobile phone records, location data, airline manifests, and leaked or exfiltrated databases obtained through cyber operations. By combining these inputs, Kashef generates a dynamic graph of relationships that can be queried, expanded, and filtered based on investigative or operational needs.



According to available reporting, Kashef is used by security and intelligence units to identify social networks, trace indirect connections, and surface hidden links between individuals and locations. Rather than surveilling communications in real time, the platform reconstructs patterns of life after the fact, allowing authorities to infer trust relationships, logistical coordination, and movement patterns. This capability makes Kashef particularly valuable for intelligence-led policing, counter-dissent operations, and transnational targeting.



Crucially, Kashef appears to function as a downstream consumer of data collected through other surveillance mechanisms described in this report. Information harvested via spyware campaigns, administrative access to domestic platforms, lawful intercept systems, and cyber intrusions can be ingested into Kashef, where it is normalized and cross-referenced. In this sense, Kashef represents the convergence point of the Islamic Republic's surveillance stack: a system where interception, data access, and behavioral monitoring coalesce into a single analytical framework.



The architecture and use of Kashef illustrate a shift from fragmented surveillance toward integrated intelligence production. Rather than relying on isolated datasets or single-purpose tools, the Islamic Republic has invested in systems that enable long-term profiling and predictive inference. This model blurs the boundary between domestic surveillance and intelligence operations, enabling authorities to repurpose civilian data for security objectives without judicial transparency or meaningful oversight.

Kashef thus exemplifies the maturation of surveillance governance in the Islamic Republic: a move from monitoring communications to mapping societies. By transforming personal data into relational intelligence, the system operationalizes digital traces as instruments of control, extending the reach of state surveillance beyond individual platforms and into the structure of social life itself.

Appendix

Glossary