A session of the Supreme Council of Iran's Judiciary on February 19, 2024

Hacktivist Group Breaches Iranian Judiciary Servers

Tuesday, 02/20/2024

Iran International Newsroom

The hacktivist group Edalat-e Ali has disclosed a major breach in the servers of the Iranian judiciary, boasting access to a vast repository comprising millions of files and a treasure trove of confidential documents.

The documents encompass a spectrum of sensitive subjects, ranging from internal deliberations within the National Security Council following the death of Mahsa Amini to efforts aimed at quelling unauthorized VPN vendors, protests against the 2020 employment examination, and cases related to economic corruption.

The group unveiled a series of documents suggesting the complicity of the Iranian government in prosecuting prominent public figures during the 2022 uprising and preceding events.

Edalat-e Ali exposed **document highlighting the Iranian regime's clandestine endeavors to exert control over public figures**, particularly those occupying influential positions in the realms of entertainment and sports. Financial sanctions, bank freezes, travel bans and more have hit celebrities across the board.

They revealed a list encompassing 29 cinema and television figures alongside football stars accused of crimes including "anti-government propaganda activity" and allegations of "conspiracy and collusion against national security."

Actress Katayoun Riyahi, known for her public appearances without compulsory hijab during the uprising following Mahsa Amini's killing, faces charges encompassing “conspiracy, anti-government activities, and inciting moral corruption through her actions.”

(Clockwise) Actresses Katayou Riyahi and Hemgameh Ghaziani, and footballers Voria Ghafouri and Ali Daei

Similarly, football icons like Ali Daei, Aref Gholami, and Voria Ghafouri have been accused of fomenting dissent and engaging in activities deemed against national security.

The document, authored by Mohammad Mehdi Heidarian, the then head of the Joint Working Group on Celebrity Management and advisor to the Minister of Culture in 2019, outlines a comprehensive strategy involving multiple government entities tasked with overseeing and managing public figures, thus underscoring the regime's efforts to suppress dissent and enforce conformity.

Edalat-e Ali's ascendancy to prominence traces back to August 2021, marked by their penetration of **the surveillance infrastructure at Evin Prison**, supporting the ongoing protests and voicing advocacy for the release of political detainees.

The group's previous revelations, including documents implicating security forces in acts of sexual assault and extrajudicial violence against protesters, underscore the gravity of the situation and the need for accountability within Iran's governing apparatus.

The latest hacking is one in a long line of cyber attacks on the regime. The incidents have escalated since the 2022 uprising. From breaches in the judiciary's servers to infiltrations of surveillance infrastructure at Evin Prison and servers belonging to the Islamic Republic of Iran Broadcasting (IRIB), these hacks have underscored the vulnerability of Iran's digital infrastructure.

Each breach has not only exposed confidential information but also served as a catalyst for heightened scrutiny of the regime's activities and policies. The frequency and scale of the hacks reflect the ongoing tensions within Iranian society and the determination of hacktivists to challenge the status quo.

In the past year, MEK-affiliated hackers have targeted the portals of several other government agencies including Tehran Municipality, the Presidential Office, and the ministries of Foreign Affairs, Agriculture, and Culture as well as the parliament and published thousands of documents. In December, a cyberattack paralyzed much of the country's network of gas stations.

This week, documents were leaked following the hack of the Iranian parliament’s media arm, revealing a wide range of **Tehran’s strategies to circumvent US sanctions**.

Last week, hacktivist group **Uprising till Overthrow** took responsibility for the recent cyberattack on the Khaneh Mellat News Agency, the media arm of the Iranian Parliament.In a statement released by the group, closely affiliated with the Albania-based opposition Mujahideen-e Khalq (MEK) organization, it was disclosed that the attack reached 600 of the the main servers of the parliament, commission servers, main chamber servers, parliament assistant servers, parliament bank server, and other servers related to administrative functions.

Cybersecurity specialist Amin Sabeti claims Iran will continue facing increasing cyberattacks due to “structural defects” in their cyber defense systems. He claimed that many projects aimed at developing what the regime terms “domestic services” have failed due to their reliance on corrupt connections and nepotism rather than meritocracy and expertise.

It has led to domestic criticism in the face of the regime's weakness. Shahriar Heydari, deputy chairman of the National Security and Foreign Policy Commission of the Iranian parliament, stated that the National Organization for Passive Defense and the Intelligence Ministry should be held accountable for the recent cyberattacks.“Cyberspace is a war of information. Every country needs to secure its systems against hacking and data theft,” Heydari said.

More News

Khatami's Election Abstention Sparks Debate In Iran

Iran Denounces Meta’s Suspension Of Khamenei’s Accounts