Whisper Forensic Analysis Details Large-Scale, Coordinated Shutdown of Iranian Internet Infrastructure

New analysis details "Filter-First, Route-Second" policy leading to widespread internet disconnection for 90 million people.

LONDON, UNITED KINGDOM, January 13, 2026 /EINPresswire.com/ -- Whisper, a predictive cybersecurity company, today published a detailed forensic analysis of the recent Iranian internet blackout, documenting a highly coordinated and centrally commanded shutdown that effectively removed the nation from the global internet. The report, titled "The Blackout," provides evidence that the five-day-long outage was a deliberate, protocol-level disruption of Iran's digital infrastructure.

> “The internet is a global commons, not a state tool. Connectivity is essential for modern society; we must reject the weaponization of infrastructure as a normalized tool of governance.”
>
> *Kaveh Ranjbar, CEO at Whisper Security, Former Board Member at ICANN*

Whisper's analysis of over 5.6 million BGP routing updates in a 24-hour period - a 368% spike from the baseline - shows the nation's core routers experienced significant, anomalous routing changes. The research indicates that on January 8th, 2026, at 03:00 UTC, every major network in Iran, including mobile carriers, fixed-line ISPs, and hosting providers, failed in unison. This synchronized event points to a centralized command executing a shutdown protocol, a finding supported by a joint statement from over 30 internet leaders, including ICANN founder Esther Dyson and cryptographer Bruce Schneier.

The investigation also uncovered a sophisticated, three-stage "Digital Kill Chain" used to identify and block circumvention tools like VPNs and encrypted messengers. Evidence shows DNS spoofing was used to block Session Messenger, while middleboxes on the national backbone manipulated HTTP headers to interfere with Psiphon. Furthermore, national authorities removed IPv6, the modern internet protocol, from the country, a move that indicates a strategy to isolate the population and revert to a more easily controlled, legacy internet infrastructure.

This period of widespread disconnection occurred during nationwide protests. Human rights organizations have reported a high number of casualties and arrests during this time.

Whisper's report concludes that the January 8th event was a stress-test for a "Filter-First, Route-Second" policy, a new paradigm of internet control that reconfigures the national network for information management. The company continues to monitor the situation in real-time via its WhisperGraph™ platform.

About Whisper
Founded in January 2025, Whisper is shifting cybersecurity from reactive to predictive. As AI-driven and multi-vector attacks accelerate, Whisper helps organizations anticipate threats before damage occurs. With a mission to stop cybercrime, Whisper is building a new generation of predictive cybersecurity solutions at scale.

Company Website: https://whisper.security/

Kaveh Ranjbar
Whisper Security
email us here
Visit us on social media:
LinkedIn
YouTube