Palestinian Hackers Hit 100 Israeli Organizations in Destructive Attacks

By Ionut Arghire

Published: 2024-01-03 · Archived: 2026-04-02 11:38:01 UTC

Over the past several months, a hacking group named Cyber Toufan has hit over 100 public and private organizations in Israel, as part of an aggressive campaign fueled by the intensifying geopolitical tensions in the region.

Bearing the hallmarks of a sophisticated threat actor and claiming to be formed of Palestinian state cyber warriors, Cyber Toufan rose to fame fast, executing complex cyberattacks against high-profile Israeli entities.

The group's tactics suggest that Cyber Toufan is likely sponsored by a government, with evidence pointing to potential Iranian involvement, Check Point reported in early December.

"The group has demonstrated superior capabilities compared to other pro-Palestinian linked Hamas hacking groups. Their activities, which focus on breaching servers, databases, and leaking information, strongly suggest support from a nation-state, with indications pointing towards Iran as the likely supporter," the International Institute for Counter-Terrorism (ICT) was noting in late November.

Security researchers have tracked over 100 intrusions associated with Cyber Toufan's operations, characterized by the exfiltration of large amounts of data, including personal information, and its release on the web.

"Their attacks have not only led to substantial data leaks but have also served as a form of digital retaliation, aligning with broader strategic objectives in the region," threat intelligence firm SOC Radar wrote in a report two weeks ago.

To date, security researcher Kevin Beaumont says, the group has leaked on its Telegram channel the data of 59 organizations. However, it likely compromised 40 more in an attack targeting a managed service provider (MSP).

“Data they have published includes a complete server disk image, SSL certificates with private keys to a host of domains (which still haven’t been revoked and are still in use), SQL and CRM dumps. Even WordPress backups, as apparently people build CRMs on WordPress nowadays,” Beaumont says.

Cyber Toufan’s victims include the Israeli National Archive, Israel Innovation Authority, Homecenter Israel, Israel Nature and Parks, The Academic College of Tel Aviv, Israel Ministry of Health, Ministry of Welfare and Social Security, Israel Securities Authority, Allot, MAX Security & Intelligence, Radware, and Toyota Israel.

Some of the victims, Beaumont says, have not been able to recover from the cyberattacks and have been offline for several weeks, likely because the attackers target Linux systems with a wiper.

According to the researcher, Cyber Toufan uses Shred, a legitimate tool, to “delete files in an unrecoverable fashion”. For that, the group runs Shred using their own shell script, to ensure that the tool continues to run even if the process is killed by an administrator.

The group was also seen emailing the victim organizations’ clients, to spread propaganda, and appears to be coordinating with other hacking groups in larger collective operations.

Related: Spyware Caught Masquerading as Israeli Rocket Alert Applications

Related: Hackers Join In on Israel-Hamas War With Disruptive Cyberattacks

Related: Irrigation Systems in Israel Disrupted by Hacker Attacks on ICS
