SECURITYWEEK NETWORK:

- Cybersecurity News
- Infosec Island
- Virtual Events

Security Experts:

WRITE FOR US

SECURITY WEEK
CYBERSECURITY NEWS, INSIGHTS & ANALYSIS

- Subscribe
- 2021 CISO Forum
- ICS Cyber Security Conference
- Contact

- Malware & Threats
  - Vulnerabilities
  - Email Security
  - Virus & Malware
  - IoT Security
  - Threat Intelligence
  - Endpoint Security
- Cybercrime
  - Cyberwarfare
  - Fraud & Identity Theft
  - Phishing
  - Malware
  - Tracking & Law Enforcement
- Mobile & Wireless
  - Mobile Security
  - Wireless Security
- Risk & Compliance

- Risk Management
- Compliance
- Privacy
- Supply Chain

- Security Architecture
  - Cloud Security
  - Identity & Access
  - Data Protection
  - Network Security
  - Application Security
- Security Strategy
  - Risk Management
  - Security Architecture
  - Disaster Recovery
  - Training & Certification
  - Incident Response
- ICS/OT
- IoT Security

Home › Cybercrime

Apparent Iran-Linked Hackers Breach Israeli Internet Firm

By AFP on October 30, 2021

Hackers believed to be linked to Iran have breached an Israeli internet hosting company, taking down several of its sites, local media reported.

The cyberattack hit websites including of Israeli public transport companies Dan and Kavim, a children's museum and public radio's online blog, with none of the sites available to users by midday Saturday.

The hacking group known as **Black Shadow** claimed responsibility for the attack and published what it said was client data, including the names, email addresses and phone numbers of Kavim clients, on the Telegram messaging app.

"Hello Again! We have news for you," the hackers wrote in a message on Telegram on Friday night.

"You probably could not connect to many websites today. 'Cyberserve' company and their customers (were) hit by us," it said.

"If you don't want your data leak(ed) by us, contact us SOON."

Later another message read: "They did not contact us... so (the) first data is here," with the group dumping the information online.

Israeli media said Black Shadow is a group of Iran-linked hackers who use cyberattacks for criminal ends.

The group breached Israel's Shirbit insurance firm in December last year, stealing a trove of data.

It demanded a $1 million ransom and began leaking the information when the firm refused to pay.

The new attack comes after an unprecedented, unclaimed cyberattack wrought havoc on Iran's petrol distribution system this week.

Iranian media have pointed the finger at government opponents abroad.

Iran and Israel have been engaged in a so-called "shadow war", including several reported attacks on Israeli and Iranian ships that the two have blamed on each other, as well as cyberattacks.

In 2010 the Stuxnet virus -- believed to have been engineered by Israel and its ally the US -- infected Iran's nuclear programme, causing a series of breakdowns in centrifuges used to enrich uranium.

Related: Iran Struggles to Relaunch Petrol Stations After Cyberattack

Related: Iran Blames Israel for Sabotage at Natanz Nuclear Site

Previous Columns by AFP:

Apparent Iran-Linked Hackers Breach Israeli Internet Firm
Ransomware Attack Hits PNG Finance Ministry
India's Top Court Orders Probe Into Pegasus Snooping
US Dismisses Assange Suicide Risk in Extradition Appeal
US Bans China Telecom Over National Security Concerns

Tags:

NEWS & INDUSTRY Cybercrime

Search

Get the Daily Briefing