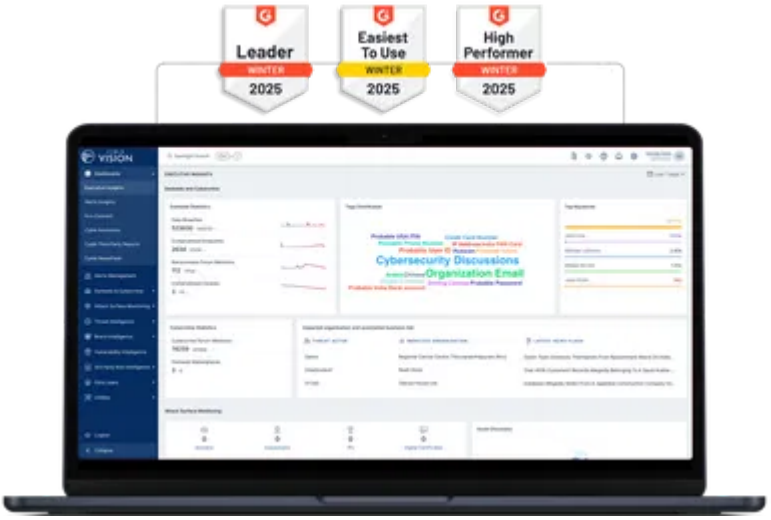
ALTOUFAN TEAM Hits Middle East Targets

Published: 2023-02-16 · Archived: 2026-04-05 18:24:04 UTC

Cyble analyzes recent Threat Actor activity targeting Bahraini & Israeli sites, protesting normalization of diplomatic relations.

Threat Actors target Bahraini & Israeli websites to protest normalization of relations

On February 13, 2023, the Threat Actor (TA) group **ALTOUFAN TEAM** on Telegram announced a campaign against Bahraini and Israeli websites to protest the normalization of relations between the two countries. The attacks coincided with events from February 14, 2011, attempted by the opposition to overthrow Bahrain's monarchy.



On February 14, 2023, the **ALTOUFAN TEAM** claimed to compromise Social Insurance Organization (SIO), Bahrain, on their Twitter account and Telegram channel.

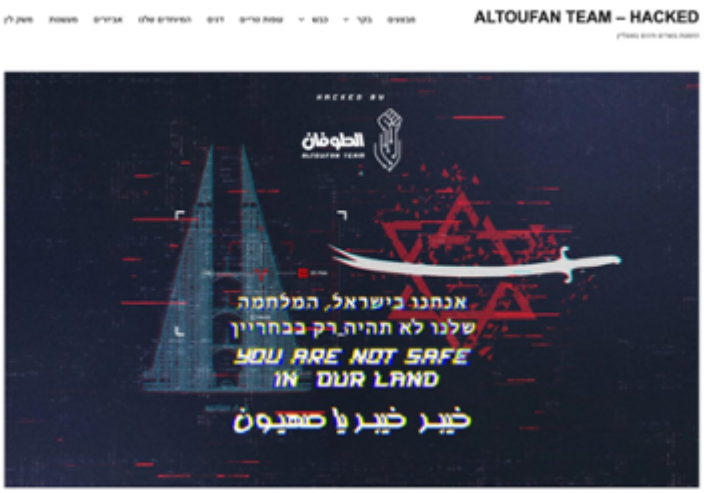


Figure 1: One site defaced by the group

The alleged attack was succeeded by a poll created by the hacktivist group that received maximum votes on the poll option – "**to increase the base pay for pensions**" – designating SIO as their next target organization. **ALTOUFAN** has since posted a video showcasing the **use of stolen credentials** to log into Bahrain's Social Insurance employer portal and modify base wages.

Timeline of Events

At approximately 11:49 PM Bahrain time, the TAs announced to target the SIO (the Social Insurance Organization), which was allegedly chosen through a Twitter poll.

Figure 2: TAs claim to increase the pay of pensioners

The TAs claimed they would carry out a hack to modify the pension wages of Bahrainis registered on the Social Insurance Organization “before dawn”.

Figure 3: TAs receive an error message on site indicating the amount of the raise is over 40% of base pay

At approximately 11:54 PM, The group shared a video as proof of compromise, claiming to have fully compromised the systems and servers of the Social Insurance Organization of Bahrain to raise the base wages of 4,000 insured and registered Bahraini citizens.

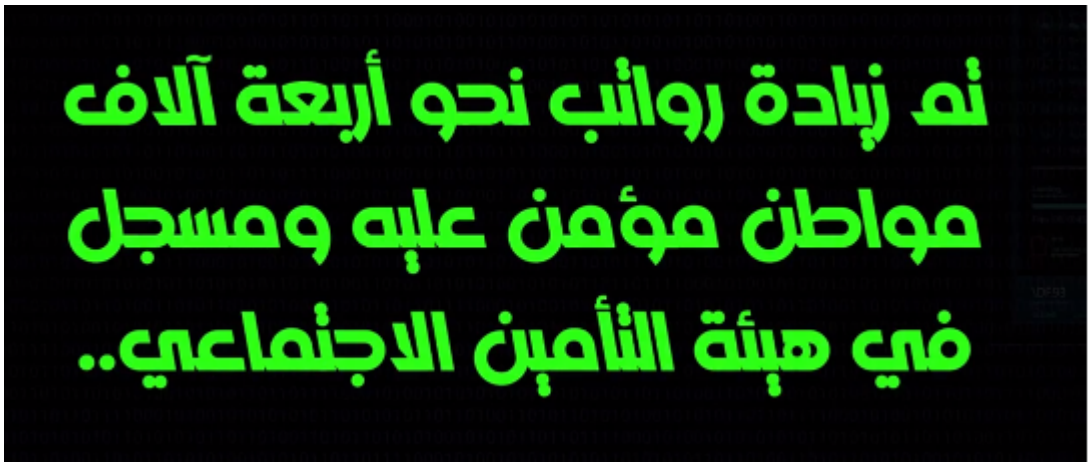


Figure 4: TAs claim to have modified 4,000 records of pensioners and insurees

While the TAs obtained access and modified records, the POC they shared displayed inputting credentials on the portal. The access to the portal was likely obtained through info-stealer malware logs (compromised endpoints) rather than a full server compromise.

We also found over 700 compromised credentials for the SIO employer portal domain on the Vision platform, supporting this conclusion.

Figure 5: Stealer logs found on Vision platform for SIO employer portal (left), TAs' compromise video (right)

Attack on Other Israeli and Bahraini Entities

The series of attacks began on February 13, 2022, with the news website “Akhbar Al Khaleej”. The TAs defaced the site’s landing page and claimed to have destroyed the site’s data.

Figure 6: Defacement of Akhbar AlKhaleej website

The defacement replaced the headlines with incendiary comments on the royal family and normalization with Israel and changed articles’ images to photos of opposition figures.

The TAs also included the keyword “Toufan” in the editor’s column title as their calling card. The group posted propaganda videos with political chants and a collage of exiled or jailed political figures from the opposition (e.g., Ali Salman, Abduljalil AlSingace, Hassan Mushaima, and others) next to the Pearl Monument.

Figure 7: Video with political chants and pearl monument symbol

The TAs also targeted the Bahrain Airport site. The website returned 504 and 404 errors at the time of this analysis, but it is currently up and running.

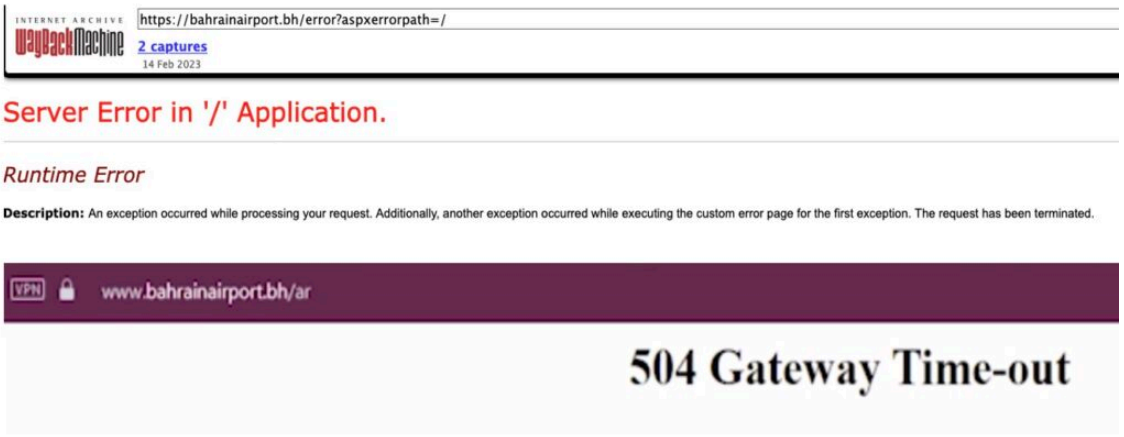


Figure 8: Wayback machine site capture and TA's screenshot

Furthermore, the group singled out the National Financial and Exchange Co website WLL, referencing public record information from Bahrain's commercial record registry to name and shame the owners.

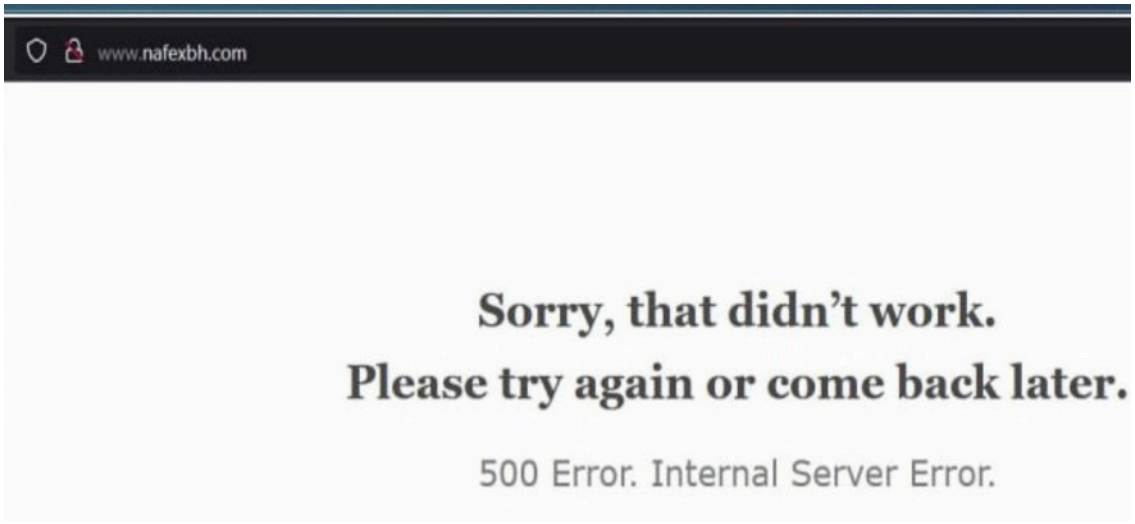


Figure 9: DDoS attack against nafexbh.com

Figure 10: TAs learning how to use public lookup sites

The TA group also performed DDoS attacks on the Bahrain News Agency website and the Bahrain Chamber of Commerce website, both of which are up at the time of this analysis.

Historic Exaggeration of Claims

The techniques allegedly leveraged by the group to gain access to SIO accounts were found improbable. The TAs did access the SIO employer portal, indicating a lack of protective measures such as OTP (One-Time Password). The Tactics, Techniques, and Procedures (TTPs) used in this campaign were basic.

However, the TAs utilized their exaggerated narratives to push a grand image of their campaign to influence amass. The group deliberately carried out the alleged SIO "hack" past midnight to prevent a quick response by

Bahrain CERT.

In November 2022, the same TA group attempted a disinformation campaign to dissuade citizens from voting in Bahrain's municipal elections. The TAs defaced and took down the House of Representatives website (nuwab.bh) and the Legislation and Legal Opinion Commission website (lloc.gov.bh) and sent fraudulent SMS messages claiming that the elections had been postponed due to the attacks.

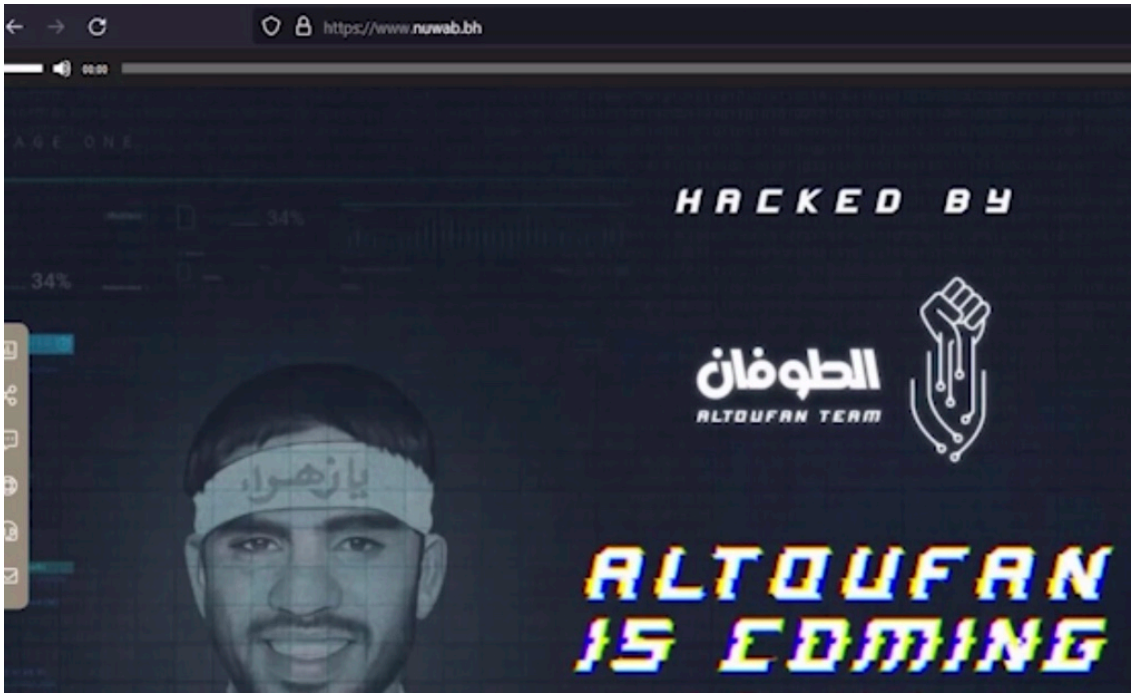


Figure 11: Altoufan's first defacement

At the time, the TAs had posted a propaganda video claiming to attack 16 prominent websites of government entities and stating that the leaks would be shared soon. The video showed a normal level of access to each site available to a logged-in user, indicating another instance of exaggeration using stealer logs.

Overview of the TA Group's Activities

ALTOUFAN isa group of politically motivated hacktivists with anti-Zionism, anti-monarchy, and pro-14-February movement sentiments.

Table 1 below lists the targeted websites and types of attacks.

Website URL	Type of Attack
AlKhaleej-news.com	Defacement, Data Deletion
BahrainAirport.bh	Denial of Service
Bna.bh	Denial of Service
Nafexbh.com	Denial of Service

Bahrainchamber.bh	**Denial of Service**
Sio.gov.bh	**Use of stolen credentials from stealer logs to modify records**
Abc-bahrain.com	**Defacement**
Btea.bh	**Defacement**
Mikapirsum.co.il	**Defacement**
Hawkshaifa.com/angos	**Defacement**
Zerpri.co.il	**Defacement**
Rotter.net	**Defacement**

Table 1: List of Cyberattacks on February 13 and February 14

The TA group uses a fist logo and iconography similar to the Iranian hacktivist groups “Moses’ Staff” and “Abraham’s Ax”. As with those groups, ALTOUFAN maintains a presence on the popular social media platforms Instagram, YouTube, Twitter, and Telegram and shares detailed montages and designs to spread their message.

The methodology of the attacks (DDoS, defacement), the promotion of the attacks, and clenched fist symbolism tie into Iranian hacktivist groups. Additionally, state-aligned Iranian Telegram channels picked up and promoted the then-unknown group after their first attack, indicating a possible connection.

Impact & Mitigation

Defacement and DDoS attacks result in lost revenue, reputational damage, misinformation campaigns, and promotion of TAs’ political agendas.

Mitigations for DDoS attacks include:

- Utilizing a WAF (Web Application Firewall) or DDoS (Distributed Denial of Service) protection service,
- Ensuring that production servers are not publicly accessible through the internet,
- Redirecting all traffic to go through the WAF,
- Rate-limiting traffic, for example, simultaneous SYN attacks by hosts which initiate a connection but never complete it, should receive a timeout past a certain period,
- Geo-blocking IP ranges that legitimate users would not have,
- Considering high-availability designs in development, such as utilizing a CDN and/or backup servers,
- Ensuring site data is backed up.
