Expert doubts Altahrea Team's claims about Israel power plant fire

techmonitor.ai/technology/cybersecurity/alahrea-team-power-plant-fire-israel

July 14, 2022

The Altahrea Team hacking group has taken responsibility for a power plant fire in Israel today, saying it assumed control of the plant's remote management system ahead of the blaze. A security expert who spoke to *Tech Monitor* is highly dubious about the claims, and believes such an attack would be beyond the group's capabilities.

The Orot Yosef power plant in Southern Israel caught fire earlier today. No one was injured in the blaze, and the official cause has yet to be determined. Reporter Arnold Nataev, from Israeli radio station *Radio Darom 97*, tweeted from the scene that the source of the fire appears to have been an air filter.

"The fire and rescue service updates that it is the burning of an air filter in an IEC facility that endangers the nearby facilities," he wrote earlier today.

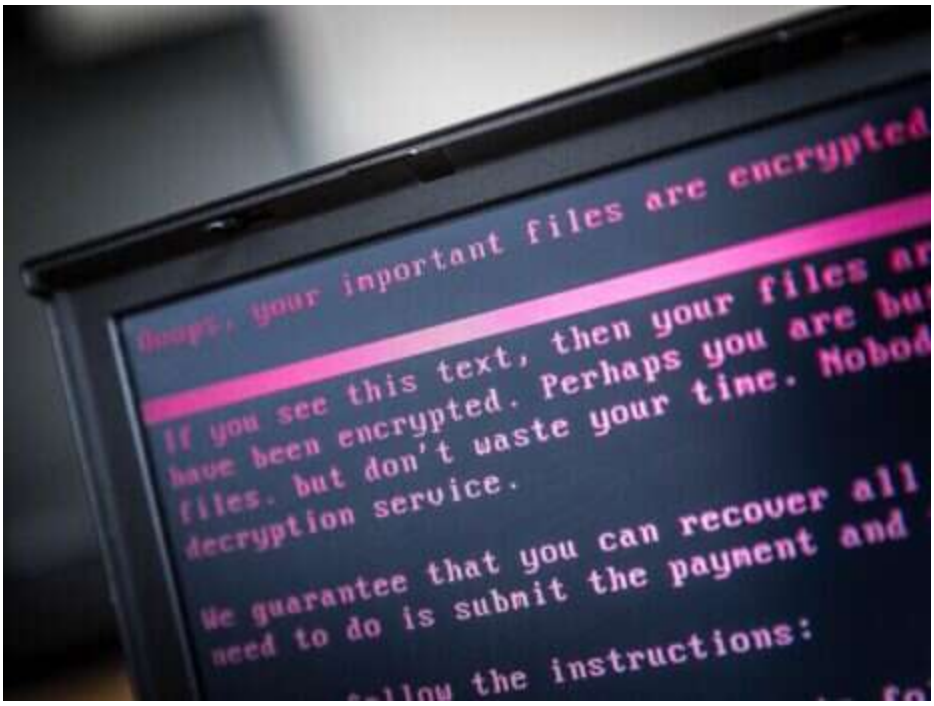
> בכבאות והצלה מעדכנים כי מדובר בשריפת פילטר אוויר במתקן חברת חשמל שמסכן את המתקנים הסמוכים. למקום הוזנקו כוחות רבים ורכבי אספקת מים, בשלב זה אין מידע על נפגעים.
>
> — ארנולד נטייב (@ArnoldNataev) July 14, 2022

However, Altahrea has claimed responsibility for the fire on its Telegram channel. The group says it hacked into the remote energy measuring system of the power plant prior to the blaze and shared the system's IP address online for anyone to access. It is unclear from the messages whether the group is claiming to have started the fire itself.

> 🌐 The Israeli power plant "Orot Yosef" was exploded🚨
>
> Earlier today, ALtahrea the Iranian 🇮🇷 hacking team claimed to hacked into the remote energy management of the power plant and shared the IP address of the EMpro system on their TG channel 🧐#ALtahrea pic.twitter.com/iFK53oGlqz
>
> — DarkFeed (@ido_cohen2) July 14, 2022

On the channel, Altahrea Team shared images of the power plant fire, and posted provocative statements like: "Do you smell gas or Benzen? Check the store," before leaving the number of the local fire department.

Yossi Reuven, security research team lead at Israeli security company SCADAfence, is sceptical about Altarhea's claims. "It is unlikely that this one is related to them [Altahrea] due to the high impact, sophistication and capabilities needed to execute this type of attack," he says.



Inside ransomware's hidden costs

The Orot Yosef plant is operated by Edeltech. It has been up and running since 1989 and has an output of 1,189mw of electricity. Tech Monitor has contacted Edeltech for comment on the fire.

View all newsletters Sign up to our newsletters Data, insights and analysis delivered to you By The Tech Monitor team

Who are the Altahrea Team?

Altahrea Team is thought to be made up of Iranian hackers, or Iraqi hackers supportive of Iran.

It is "known for multiple DDoS attacks on Israeli targets like the Jpost, Israeli 9 channel and the Israeli port authority," according to security company Check Point, which added that "these loud attacks appear to be politically motivated."

DDoS attacks are relatively simple to execute, meaning a complex operation such as taking control of a power plant remotely would be a significant departure for the gang.

Altahrea Team has not limited its operations to Israel. In May, *Tech Monitor* reported that it knocked out systems at the Port of London Authority offline with a DDoS attack, while in April it struck Turkish media outlet Anadolu Agency as well as Turkish President Recep Urdogan's website.

Cyber tensions have been running high between Israel and Iran, and last month hackers linked to Israel claimed to have taken control of systems at three state-owned steel companies in Iran.

Read more: Will closer ties with Israel impact cybersecurity in the UK?

Homepage image courtesy Oleksii Liskonih/iStock