Predatory Sparrow: Who are the hackers who say they started a fire in Iran?

bbc.com/news/technology-62072480

By Joe Tidy

By Joe Tidy
Cyber reporter

Published

7 days ago

Image source, Predatory Sparrow
Image caption,
The steel factory shortly before the fire

It's extremely rare for hackers, who operate in the digital world, to cause damage in the physical world.

But a cyber-attack on a steel maker in Iran two weeks ago is being seen as one of those significant and troubling moments.

A hacking group called Predatory Sparrow said it was behind the attack, which it said caused a serious fire, and released a video to back up its story.

The video appears to be CCTV footage of the incident, showing factory workers leaving part of the plant before a machine starts spewing molten steel and fire. The video ends with people pouring water on the fire with hoses.

In another video that surfaced online, factory staff can be heard shouting for firefighters to be called and describing damage to equipment.

Predatory Sparrow, also known by its Persian name, Gonjeshke Darande, says this was one of three attacks it carried out against Iranian steel makers on 27 June, in response to unspecified acts of "aggression" carried out by the Islamic Republic.

Media caption,
The moment when Predatory Sparrow says it caused the fire

The group has also started sharing gigabytes of data it claims to have stolen from the companies, including confidential emails.

On its Telegram page Predatory Sparrow posted: "These companies are subject to international sanctions and continue their operations despite the restrictions. These cyber-attacks, being carried out carefully to protect innocent individuals."

That last sentence has pricked the ears of the cyber-security world.

Clearly the hackers knew that they were potentially putting lives in danger, but it seems they were at pains to ensure the factory floor was empty before they launched their attack - and they were equally eager to make sure everyone knew how careful they had been.

This has led many to wonder whether Predatory Sparrow is a professional and tightly regulated team of state-sponsored military hackers, who may even be obliged to carry out risk assessments before they launch an operation.

- Iran says foreign country hacked petrol stations
- Iranian hackers posed as British-based academic

"They claim themselves to be a group of hacktivists, but given their sophistication, and their high impact, we believe that the group is either operated, or sponsored by, a nation state," says Itay Cohen, head of cyber research at Check Point Software.

Image source, Predatory Sparrow

Image caption,
Predatory Sparrow has a Telegram channel, Twitter account and even a logo

Iran has been the victim of a spate of recent cyber-attacks that have had an impact in the real world but nothing as serious as this.

"If this does turn out to be a state sponsored cyber-attack causing physical - or in the war studies jargon 'kinetic' damage - this could be hugely significant," says Emily Taylor, Editor of the Cyber Policy Journal.

"Historically the Stuxnet attack on Iran's uranium enrichment facilities in 2010, has been highlighted as one of the few - if not the only known - example of a cyber-attack causing physical damage."

Stuxnet was a computer virus first discovered in 2010 that damaged or destroyed centrifuges at Iran's uranium enrichment facility in Natanz, hampering its nuclear programme.

Since then there have been very few confirmed cases of physical damage.

Image source, EPA

Image caption,
Natanz is heavily protected, with its most sensitive machinery housed deep underground

Possibly the only one came in 2014 in Germany. In the annual report of the German cyber authority it was stated that a cyber-attack caused "massive damage" to a steel factory, causing an emergency shutdown, but no further details have ever been given.

There have been other cyber-attacks that could have caused serious damage but didn't succeed. For example, hackers have tried but failed to add chemicals to the water supply by taking control of water treatment facilities.

It's more common for cyber-attacks to cause disruption - to transport networks for example - without causing real physical damage.

Emily Taylor says it's a significant distinction because if a state is proven to have caused physical damage to the Iranian steel factory it may have violated international laws prohibiting the use of force, and provided Iran with legal grounds to hit back.

So if Predatory Sparrow is a state-sponsored military hacking group, which country does it represent? Its name, a play on the name of the Iranian cyber-warfare group, Charming Kitten, could be a clue, suggesting that it's a country with a strong interest in Iran.

The Stuxnet attack is widely thought to have been carried out by Israel, with support from the US. And this time the murmurings linking the Predatory Sparrow attack with Israel have been loud enough to prompt a response from the Israeli government.

According to Israeli media reports, Defence Minister Benny Gantz has ordered an investigation into leaks that led to Israeli journalists heavily hinting that Israel is behind the hack.

The minister is reportedly concerned that Israel's "ambiguity policy" on its operations against Iran might have been broken.

"If this cyber-attack is state-sponsored then of course Israel is the prime suspect. Iran and Israel are in a cyber-war, and officially both states acknowledge this," says Ersin Cahmutoglu from ADEO Cyber Security Services in Ankara.

"Both states mutually organise cyber-attacks through their intelligence services and everything has escalated since 2020 when retaliation came from Israel after Iran launched a failed cyber-attack on Israeli water infrastructure systems and attempted to interfere with the chlorine level."

Image caption,
Predatory Sparrow hijacked road signs to spread chaos in Iran

In October last year Predatory Sparrow claimed responsibility for taking Iran's national fuel station payment system offline. The group also said it had been behind a hack that hijacked digital billboards on roads, making them display a message saying, "Khamenei, where is our fuel?" - a reference to the country's supreme leader, Ayatollah Ali Khamenei.

Again, the hackers showed a degree of responsibility by warning Iran's emergency services in advance about the potential chaos that could result.

Check Point researchers say they have also found code in the malicious software used by Predatory Sparrow that matches code used by another group, called Indra, that hacked Iranian train station displays in July last year.

According to Iranian news reports, hackers indicated on information boards at stations across the country that trains were cancelled or delayed, and urged passengers to call the supreme leader.

But experts say the steel factory attack is a sign that the stakes are getting higher.

Image source, FARS

Image caption,
In August 2021 train station displays were hacked causing confusion to rail users

According to the CEO of Mobarakeh Steel Company, where the fire apparently took place, the plant's operations were not affected by the attack and no-one was hurt. The two other companies targeted also said they experienced no problems.

Nariman Gharib, a UK-based opposition Iranian activist and independent cyber-espionage investigator, is convinced the video is genuine. He notes that two other videos of the fire were also posted on Twitter.

"The attack was real, as workers recorded video from another angle and we saw a statement posted on one company's Telegram channel regarding the suspension of the production line, which was later denied."

He fears a threshold has now been crossed.

"If Israel is behind these attacks, I think they are showing that they can do real damage rather than just disrupting a service. It shows how things can quickly escalate."

More on this story

How cyber-attacks could be deadly

25 September 2020