Cyberattack forces Iran steel company to halt production

27 June 2022, By ISABEL DEBRE

Credit: CC0 Public Domain

One of Iran's major steel companies said Monday it was forced to halt production after being hit by a cyberattack that also targeted two other plants, apparently marking one of the biggest such assaults on the country's strategic industrial sector in recent memory.

The Iranian government did not acknowledge the disruption or blame any specific group for the assault on the state-owned Khuzestan Steel Co. and Iran's two other major steel producers, which constitutes just the latest example of an attack crippling the country's services in recent months amid heightened tensions in the region.

An anonymous hacking group claimed responsibility for the attack on social media, saying it targeted Iran's three biggest steel companies in response to the "aggression of the Islamic Republic."

The group, calling itself "Gonjeshke Darande," shared what purported to be closed-circuit footage from the Khuzestan Steel Co. factory floor that showed a piece of heavy machinery on a steel billet production line malfunction and cause a massive fire.

"These companies are subject to international sanctions and continue their operations despite the restrictions," the group said, citing their links to Iran's paramilitary Revolutionary Guard.

A steel mill in the central Iranian town of Mobarakeh said that its system was struck too, while the the state-run IRAN newspaper reported that another factory in the southern Iranian port of Bandar Abbas was targeted in the cyberattack. Neither plant acknowledged any damage or work stoppage as a result.

Khuzestan Steel Co., meanwhile, said the factory had to stop work until further notice "due to technical problems" following "cyberattacks." The company's website was down on Monday.

However, CEO Amin Ebrahimi, claimed that Khuzestan Steel managed to thwart the cyberattack and prevent damage to production that would impact supply chains and customers. He said nothing of the explosion shown in the hacker group's footage.

"Fortunately with time and awareness, the attack was unsuccessful," the semiofficial Mehr news agency quoted Ebrahimi as saying, adding that he expected the company's website to be restored and everything to return to "normal" by the end of Monday.

A local news channel, Jamaran, meanwhile reported that the attack failed because the factory happened to be non-operational at the time due to an electricity outage.

Cyberattacks have become increasingly common in Iran in recent years. The country, long sanctioned by the West, has been slow to update its networks to counter the rising use of ransomware by

criminals, as well as intrusions by state actors.

In a major incident last year, a cyberattack on Iran's fuel distribution system paralyzed gas stations across the country, leading to long lines of angry motorists. The same anonymous hacking group, Gonjeshke Darande, claimed responsibility for the attack on fuel pumps.

Train stations in Iran have been hit with fake delay messages. Surveillance cameras in the country have been hacked. State-run websites have been disrupted. Footage showing abuse in the country's notorious Evin prison has leaked out.

Juan Andrés Guerrero-Saade, a principal threat researcher at SentinelOne, said it's still unclear who is behind the recent cyberattacks against Iran. But he said it's an escalation if the same groups are behind the alleged attack on the steel plants' industrial control system.

"Something has changed in the tone of these attacks," he said.

Lior Tabansky, a cybersecurity expert at Israel's Tel Aviv University, said that in the murky world of cybersecurity, it's often difficult to separate genuine claims of responsibility from false flags.

If it was indeed a cyberattack, suspicion would likely fall on Israel or the United States, he said. "However, if I were an Iranian senior official and I had problems in my ministry of steel or whatever, the best way out is to say well, the Zionists or American imperialists are cyber-attacking me."

Iran has previously accused the United States and Israel for cyberattacks that have impaired the country's infrastructure.

Iran disconnected much of its government infrastructure from the internet after the Stuxnet computer virus—widely believed to be a joint U.S.-Israeli creation—disrupted thousands of Iranian centrifuges in the country's nuclear sites in the late 2000s.

Khuzestan Steel Co., based in Ahvaz in the oil-rich southwestern Khuzestan province, has a monopoly on steel production in Iran along with two other major state-owned firms.

Founded before Iran's 1979 Islamic Revolution, the company for decades afterward had some production lines supplied by German, Italian and Japanese companies. Service has been continuous except during the catastrophic Iran-Iraq war of the 1980s, when Iraqi dictator Saddam Hussein sent his army across the border.

However, crushing sanctions on Iran over its nuclear program have forced the company to reduce its dependence on foreign parts.

The government considers steel a crucial sector. Iran is the leading producer of steel in the Middle East and among the top 10 in the world, according to the World Steel Association. Its iron ore mines provide raw materials for domestic production and are exported to dozens of countries, including Italy, China and the United Arab Emirates.

Iran's crude steel production, however, was only 2.3 million tons last month, the WSA said. Its concurrent drop in exports has been largely attributed to sanctions-hit Russia flooding Iran's Chinese buyers with discounted steel after losing access to Western markets amid the war on Ukraine.