Two more cyber-attacks hit Israel's water system

First attack hit in April when hackers tried to modify water chlorine levels, officials said.

By Catalin Cimpanu for Zero Day | July 20, 2020 -- 09:44 GMT (02:44 PDT) | Topic: Security

MORE FROM CATALIN CIMPANU

Security
DDoS extortionists target NZX, Moneygram, Braintree, and other financial services

Security
Twitter takes down 'Dracula' botnet pushing pro-Chinese propaganda

Security
A quarter of the Alexa Top 10K websites are using browser fingerprinting scripts

Security
Two members of movie piracy group

PDFmyURL

Two more cyber-attacks have hit Israel's water management facilities, officials from the Water Authority said last week.
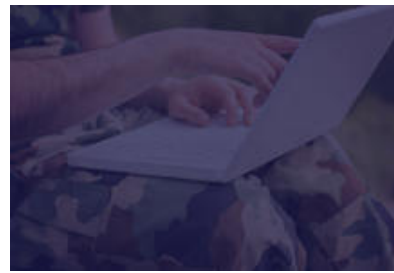
Officials said the attacks took place last month, in June, and didn't cause any damage to the attacked organizations.

The first attack hit agricultural water pumps in upper Galilee, while the second one hit water pumps in the central province of Mateh Yehuda, local media reported last week.

"These were specific, small drainage installations in the agriculture sector that were immediately and independently repaired by the locals, causing no harm or any real-world effects," the Water Authority said in a statement.

The two attacks come after Israel suffered a first cyber-attack on its water supply system in April.

Initial reports played down the April attack, but a Financial Times report from June citing Western intelligence sources claimed that hackers had gained access to some of Israel's water treatment systems and tried altering water chlorine levels before being detected and stopped. If the attack had been successful and water chlorine levels had been adjusted, attackers could have caused mild poisoning of the local population served by the affected treatment facility.

Following the intrusion, the Israel National Cyber-Directorate (INCD) and the Water Authority sent out an alert urging water treatment facilities to change the passwords of their internet-connected equipment "with emphasis on operational systems and chlorine control devices in particular."

Israeli officials never attributed the April attack, but the Washington Post, citing foreign intelligence officials, said the intrusion was linked to Iran.

Two weeks later, in mid-May, a cyber-attack crippled the port of Shahid Rajaei in the Iranian city of Bandar Abbas, which the Washington Post, citing the US intelligence sources, linked to Israel, as a likely payback for the April attack.

The attack on Israel's water utility seems, however, to have been an important moment between the two countries, as it also marked the start of a series of mysterious accidents and explosions detected across Iran's critical infrastructure -- such as petrochemical plants, nuclear fuel enrichment centers, power plants, ports, and more.

> Lots of "accidents" all over the country. Iran seems to be very unlikely lately https://t.co/5kJOOmfBFt
>
> — Dmitri Alperovitch (@DAlperovitch) July 19, 2020

The world's most famous and dangerous APT...   SEE FULL GALLERY

SECURITY

Top exploits used by ransomware gangs are VPN bugs, but RDP still reigns supreme

Free photos, graphics site Freepik discloses data breach impacting 8.3m users

Best security keys in 2020: Hardware-based two-factor authentication for online protection

Best password managers for business in 2020: 1Password, Keeper, LastPass, and more

Cyber security 101: Protect your privacy from hackers, spies, and the government

White hat hacker reveals the real job of an infosec pro (ZDNet YouTube)

Top 6 cheap home security devices in 2020 (CNET)

What are IT pros concerned about in the new normal? (TechRepublic)

RELATED TOPICS:

SECURITY TV

DATA MANAGEMENT

CXO

DATA CENTERS

By Catalin Cimpanu for Zero Day | July 20, 2020 -- 09:44 GMT (02:44 PDT) | Topic: Security

🗨 SHOW COMMENTS

Topics

Galleries

Videos

Sponsored Narratives

CA Privacy/Info We
Collect

CA Do Not Sell My Info

About ZDNet

Meet The Team

All Authors

RSS Feeds

Site Map

Reprint Policy

Newsletters

Site Assistance

ZDNet Academy

TechRepublic Forums

Visit other CBS Interactive sites: Select Site ▼