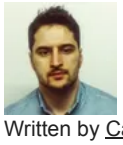
Croatia's largest petrol station chain impacted by cyber-attack

zdnet.com/article/croatias-largest-petrol-station-chain-impacted-by-cyber-attack/

Home Innovation Security

A ransomware attack is believed to have impaired the chain's ability to issue invoices and accept loyalty cards.



Written by Catalin Cimpanu, Contributor on Feb. 20, 2020

-
-
-
-
-

Image: andreas160578 on Pixabay

See als

10 dangerous app vulnerabilities to watch out for (free PDF)

A security incident described as "a cyber-attack" has crippled some business operations at INA Group, Croatia's biggest oil company, and its largest petrol station chain.

The attack took place last Friday, on February 14, at 22:00, local time, the company said.

Multiple sources have told ZDNet the cyber-attack is a ransomware infection that infected and then encrypted some of the company's backend servers.

The incident did not impact the company's ability to provide petrol fuel to its customers, nor its ability to handle payments.

It did, however, impact its ability to issue invoices, register loyalty card use, issue new mobile vouchers, issue new electronic vignettes, and allow customers to pay gas utility bills (INA is also a natural gas provider in Croatia).

The INA Group, which is part of the MOL Group and lists the Croatian government as its biggest shareholder, publicly disclosed the incident over the weekend and apologized to customers.

A company spokesperson did not return emails or phone calls for additional details.

In a message posted on its website, the company said it was working to restore all systems, however, its services were still down today.

Suspected CLOP ransomware attack

A source familiar with the incident has told ZDNet this week that the ransomware incident has been caused by an infection with the CLOP ransomware strain.

While we couldn't get INA to confirm, open-source reporting supports our source's tip. For example, hours before INA reported being infected, a Sophos malware analyst reported a new malware command-and-control server going live and being involved in CLOP-related operations.

Furthermore, this week, security researchers have also spotted new versions of the CLOP ransomware on VirusTotal, an aggregated malware scanning service [1, 2, 3].

The use of the CLOP ransomware in the attack against INA also fits the bill when it comes to CLOP's regular modus operandi.

According to BleepingComputer, a tech news site specialized in ransomware news and research, the operators of the CLOP ransomware switched tactics in March 2019 from targeting end-users to targeting companies.

The CLOP gang is now what security researchers call "big-game ransomware," which is a term referring to criminal groups that specifically target companies to infect their networks, encrypt data, and ask for extremely large ransom demands.