Eletrobras, Copel energy companies hit by ransomware attacks

By Ionut Ilascu

Published: 2021-02-05 · Archived: 2026-04-05 13:47:18 UTC

Centrais Eletricas Brasileiras (Eletrobras) and Companhia Paranaense de Energia (Copel), two major electric utilities companies in Brazil have announced that they suffered ransomware attacks over the past week.

State-controlled, both are key players in the country. Copel being the largest in the state of Paraná while Eletrobras is the largest power utility company in Latin America and also owns Eletronuclear, a subsidiary involved in the construction and operations of nuclear power plants.

Both ransomware attacks disrupted operations and forced the companies to suspend some of their systems, at least temporarily.


DIE LINKE.
0:00

Nuclear plants unaffected

In the case of Eletrobras, the incident occurred at its Eletronuclear subsidiary and was classified as a ransomware attack. It affected some of the administrative network servers and had no impact on operations at nuclear power plants Angra 1 and Angra 2.

Operations at the two plants are disconnected from the administrative network, for obvious security reasons, so the electricity supply to the National Interconnected System remained unaffected, the company says in a press release on Wednesday.

Upon detecting the attack, Eletronuclear suspended some of its systems to protect the integrity of the network. Together with the managed security services team, the company isolated the malware and restricted the effects of the attack.

The notification is scarce with details and does not clarify if the attack also doubles as a data breach, as it is common for ransomware operators to steal data from the victim network before deploying the encryption routine.

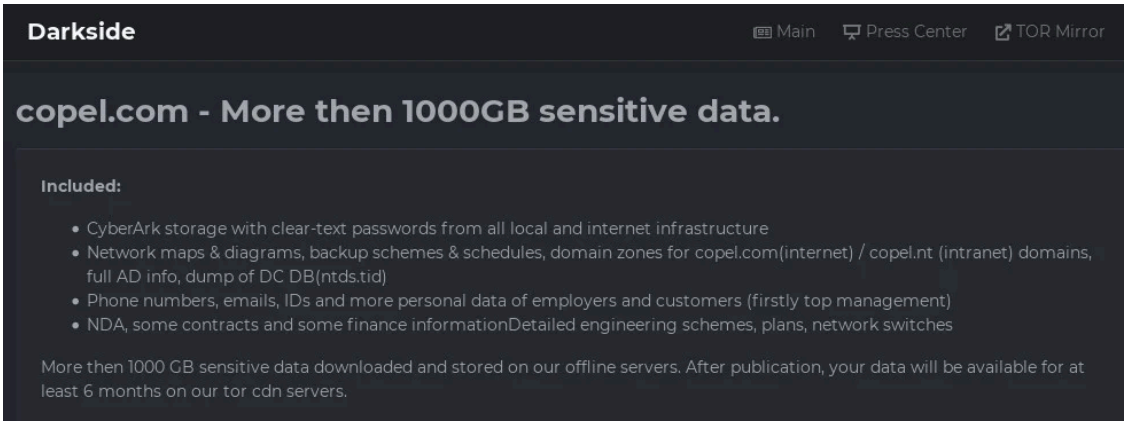
Copel leaks ahead

In the case of Copel, the attack is the work of the Darkside ransomware gang, who claims to have stolen more than 1,000GB of data and that the cache includes sensitive infrastructure access information and personal details of top management and customers.

According to the hackers, they gained access to the company's CyberArk solution for privileged access management and exfiltrated plaintext passwords across Copel's local and internet infrastructure.

Apart from this, Darkside says that they have more than 1,000GB of sensitive data belonging to Copel, which contains network maps, backup schemes and schedules, domain zones for Copel's main site, and the intranet domain.

They also claim to have exfiltrated the database that stores Active Directory (AD) data - NTDS.dit file, which includes information about user objects, groups, group membership, and password hashes for all users in the domain.



Although the AD database does not have plain text passwords, there are tools that could crack the hashes offline or use them in the so-called pass-the-hash attacks, where they function as the password itself.

Unlike other ransomware operators, Darkside does not provide stolen data on their leak site. Instead, they set up a distributed storage system to host it for six months.

Access to these caches is vetted by the gang members. This means that while Copel's data is not freely available, third parties including hackers can easily get it.

Main systems intact

Copel is the largest company in the state of Paraná and also the first Brazilian company in the electricity sector to be listed at the New York Stock Exchange.

The date of the intrusion remains undisclosed but Copel announced the incident in a filing with the Securities and Exchange Commission (SEC) on Monday, February 1st.

The company detected the attack and acted immediately to stop it from spreading across the network. An investigation was started to determine the full impact of the attack.

What is certain is that the main systems remained unaffected and the electricity supply along with telecommunications services continued to function normally.

“The operation and protection systems detected the attacks and, immediately, the Company followed the security protocols, including suspending the operation of its computerized environment to protect the integrity of the information. The full assessment of what happened is in progress and the Company is taking the necessary steps to restore normality” - Copel

It is unclear how many segments of the Copel network were impacted by the attack or if the hackers were able to deploy the encryption routine. BleepingComputer reached out to Copel with a request for comments and we will update the article when an official statement becomes available.

Source: https://www.bleepingcomputer.com/news/security/eletrobras-copel-energy-companies-hit-by-ransomware-attacks/