Energy group ERG reports minor disruptions after ransomware attack

bleepingcomputer.com/news/security/energy-group-erg-reports-minor-disruptions-after-ransomware-attack/

Sergiu Gatlan

By
Sergiu Gatlan

- August 4, 2021
- 05:34 PM
- 0

Image: RawFilm

Italian energy company ERG reports "only a few minor disruptions" affecting its information and communications technology (ICT) infrastructure following a ransomware attack on its systems.

While the Italian renewable energy group only reffered to the incident as a hacker attack, La Repubblica reported that the attack was coordinated by the LockBit 2.0 ransomware group.

The LockBit ransomware gang started operating in September 2019 and announced the launch of the LockBit 2.0 ransomware-as-a-service in June 2021.

No downtime after attack

"Concerning the recent rumours in the media on hacker attacks on institutions and companies, ERG reports that it has experienced only a few minor disruptions to its ICT infrastructure, which are currently being overcome, also thanks to the prompt deployment of its internal cybersecurity procedures," the company said today.

"The company confirms that all its plants are operating smoothly and have not experienced any downtime, thus ensuring continuous business operations."

ERG is the leading Italian wind power operator and among the top ten onshore operators on the European market, with a growing presence in France, Germany, Poland, Romania, Bulgaria, and the United Kingdom.

The group operates in the wind energy, hydroelectric energy, solar energy, and high-yield thermoelectric cogeneration energy sectors.

On Monday, Enel, Europe's largest utility company, agreed to buy ERG's hydroelectric power asset portfolio as part of a €1 billion ($1.18 billion) deal.

An ERG spokesperson was not available for comment when contacted by BleepingComputer earlier today.

> The company confirms that all its plants are operating smoothly and have not experienced any downtime, thus ensuring continuous business operations (2/2)
>
> — ERG (@ERGnow) August 4, 2021

Lazio ransomware attack

In related news, the Italian Lazio region has suffered a likely RansomEXX ransomware attack that has disabled the region's IT systems, including the Salute Lazio health portal used for COVID-19 vaccine registration.

"On the night between Saturday and Sunday the Regione Lazio suffered a first cyber attack of criminal matrix. We don't know who is responsible and their goals," Nicola Zingaretti, the President of the Lazio region, said in a statement.

"The systems are all disabled including all of the Salute Lazio portal and the vaccine network. All defense and verification operations are under way to avoid the misappropriation. Vaccination operations may experience delays," the region said in a statement.

The RansomEXX gang, the main suspect behind the Lazio attack, started operating as Defray in 2018 but, in June 2020, it rebranded as RansomEXX and started to focus on targeting large corporate organizations.

Once RansomEXX threat actors gain access to a victim's network, they spread laterally through the network while stealing sensitive documents to be used as extortion leverage.

Related Articles:

Online library app Onleihe faces issues after cyberattack on provider

LockBit victim estimates cost of ransomware attack to be $42 million

BlackCat/ALPHV ransomware asks $5 million to unlock Austrian state

Windows 11 KB5014019 breaks Trend Micro ransomware protection

Industrial Spy data extortion market gets into the ransomware game