

Enel Group hit by ransomware again, Netwalker demands \$14 million

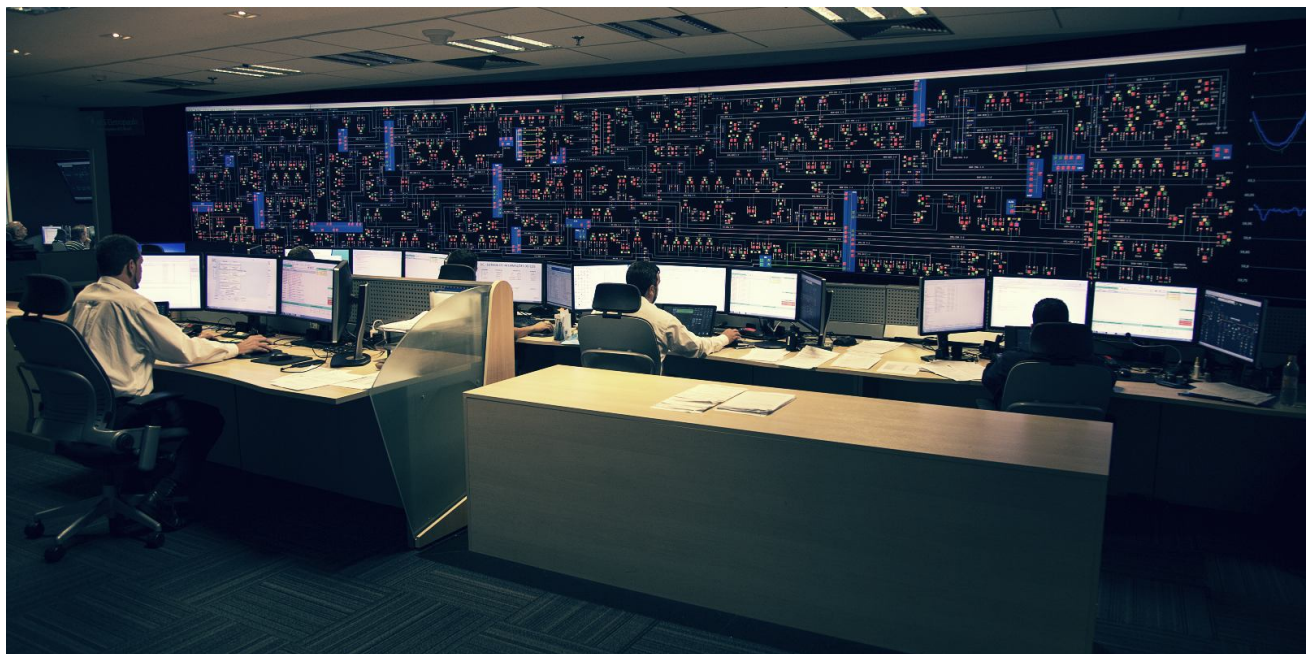
bleepingcomputer.com/news/security/enel-group-hit-by-ransomware-again-netwalker-demands-14-million/

Ionut Ilascu

By

[Ionut Ilascu](#)

- October 27, 2020
- 01:12 PM
- 0



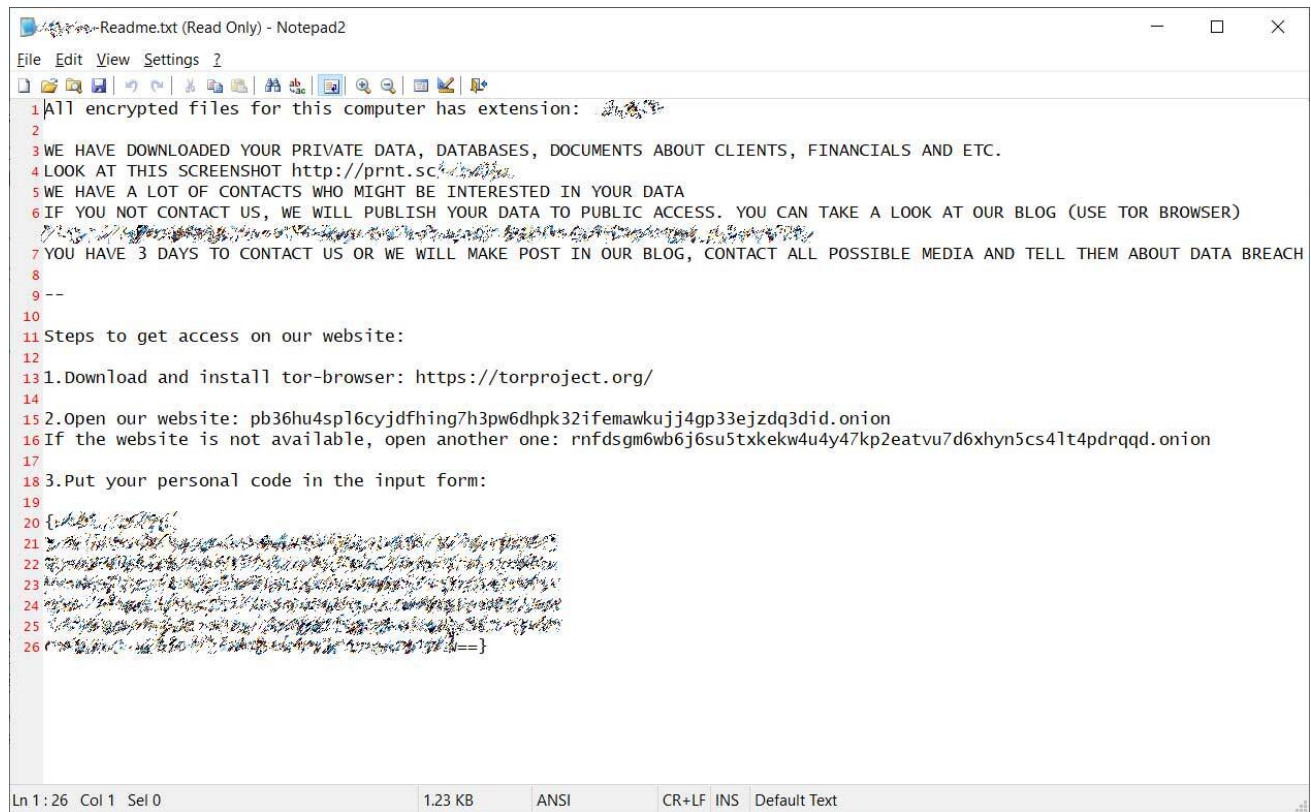
Multinational energy company Enel Group has been hit by a ransomware attack for the second time this year. This time by Netwalker, who is asking a \$14 million ransom for the decryption key and to not release several terabytes of stolen data.

Enel is one of the largest players in the European energy sector, with more than 61 million customers in 40 countries. As of August 10, it ranks 87 in Fortune Global 500, with a revenue of almost \$90 billion in 2019.

Enel hit with Netwalker Ransomware attack

In early June, Enel's internal network was attacked by Snake ransomware, also referred to as EKANS, but the attempt was caught before the malware could spread.

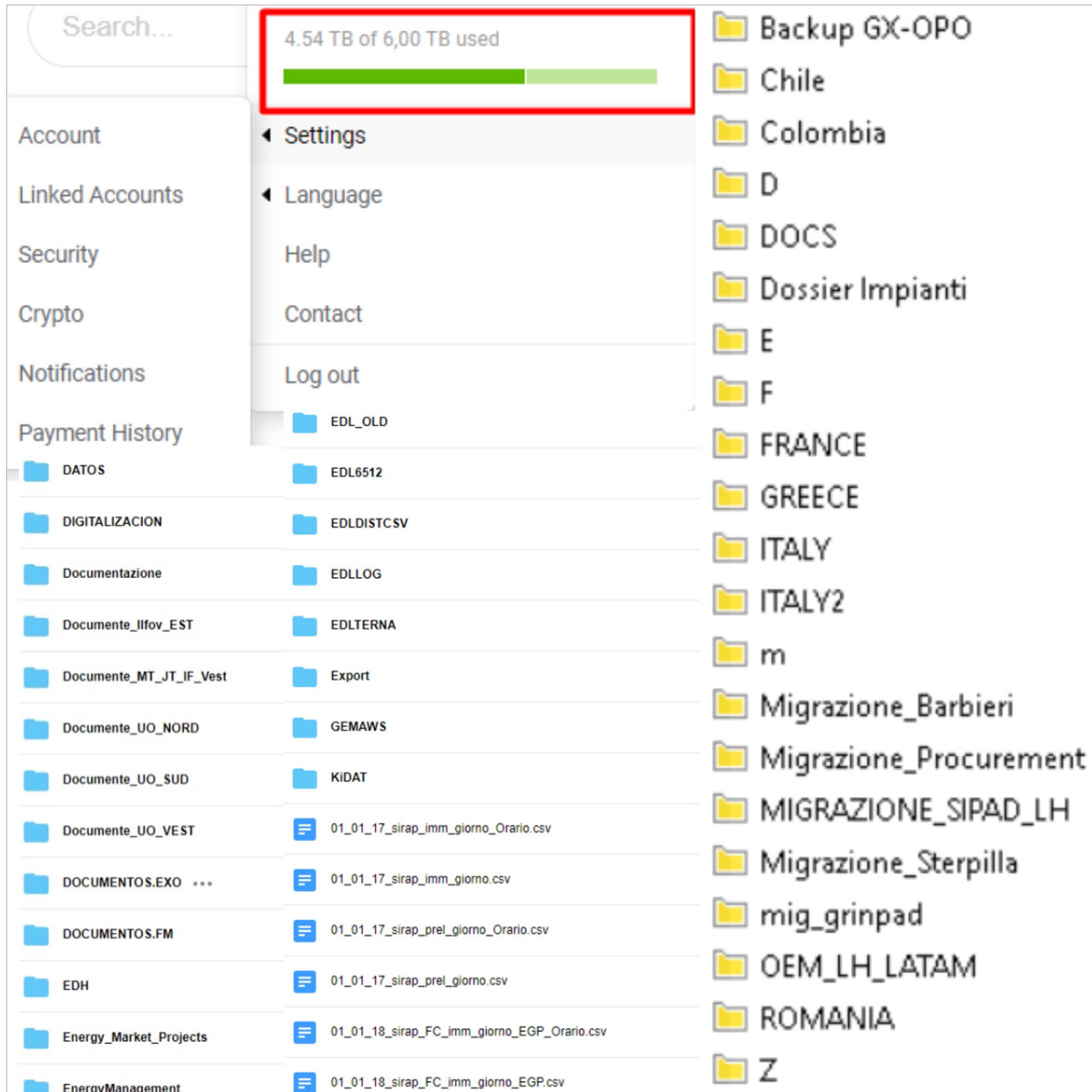
On October 19th, a researcher shared a Netwalker ransom note with BleepingComputer that appeared to be from an attack on Enel Group.



```
1 All encrypted files for this computer has extension:
2
3 WE HAVE DOWNLOADED YOUR PRIVATE DATA, DATABASES, DOCUMENTS ABOUT CLIENTS, FINANCIALS AND ETC.
4 LOOK AT THIS SCREENSHOT http://prnt.sc/
5 WE HAVE A LOT OF CONTACTS WHO MIGHT BE INTERESTED IN YOUR DATA
6 IF YOU NOT CONTACT US, WE WILL PUBLISH YOUR DATA TO PUBLIC ACCESS. YOU CAN TAKE A LOOK AT OUR BLOG (USE TOR BROWSER)
7 YOU HAVE 3 DAYS TO CONTACT US OR WE WILL MAKE POST IN OUR BLOG, CONTACT ALL POSSIBLE MEDIA AND TELL THEM ABOUT DATA BREACH
8
9 --
10
11 Steps to get access on our website:
12
13 1.Download and install tor-browser: https://torproject.org/
14
15 2.Open our website: pb36hu4spl6cyjdfhing7h3pw6dhpk32ifemawkujj4gp33ejzdzq3did.onion
16 If the website is not available, open another one: rnfdsqm6wb6j6su5txkek4u4y47kp2eatvu7d6xhyn5cs41t4pdrqqd.onion
17
18 3.Put your personal code in the input form:
19
20 {
21
22
23
24
25
26 }
```

Netwalker ransom note for Enel Group

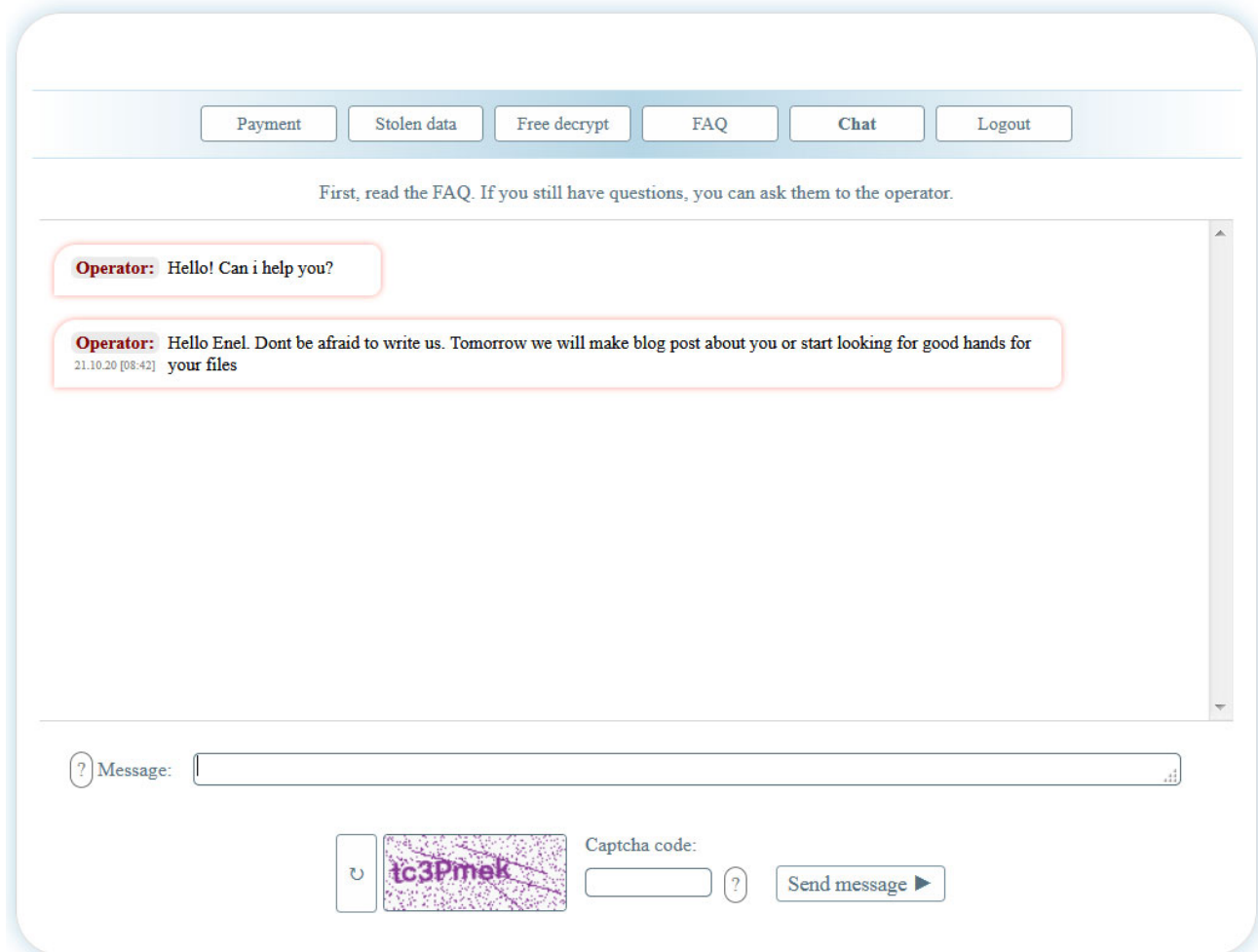
Included in the ransom note, was a link to a <http://prnt.sc/> URL that showed data stolen from the attack. Based on the names of the employees in the folders, it was determined that the attack was on Enel Group.



Screenshot of stolen data shared in ransom note

BleepingComputer emailed Enel Group last week regarding the attack but never heard back.

A few days later, Netwalker confirmed that the victim was Enel Group after they added a message to their support chat, stating "Hello Enel. Dont be afraid to write us."




Netwalker chat section for Enel victim page


Typically, if the company does not engage the ransom operator in any way, the ransom doubles after a while. It appears that this is what happened with Enel, too, as the private chat provided by the attacker has no conversation from the company.

The attacker used this channel to announce that they would initiate the first step towards leaking the stolen data. This means publishing proof that they have the goods, an attempt to pressure the company into paying the ransom, which is now \$14 million (1234.02380000 BTC).

[Payment](#) [Stolen data](#) [Free decrypt](#) [FAQ](#) [Chat](#) [Logout](#)

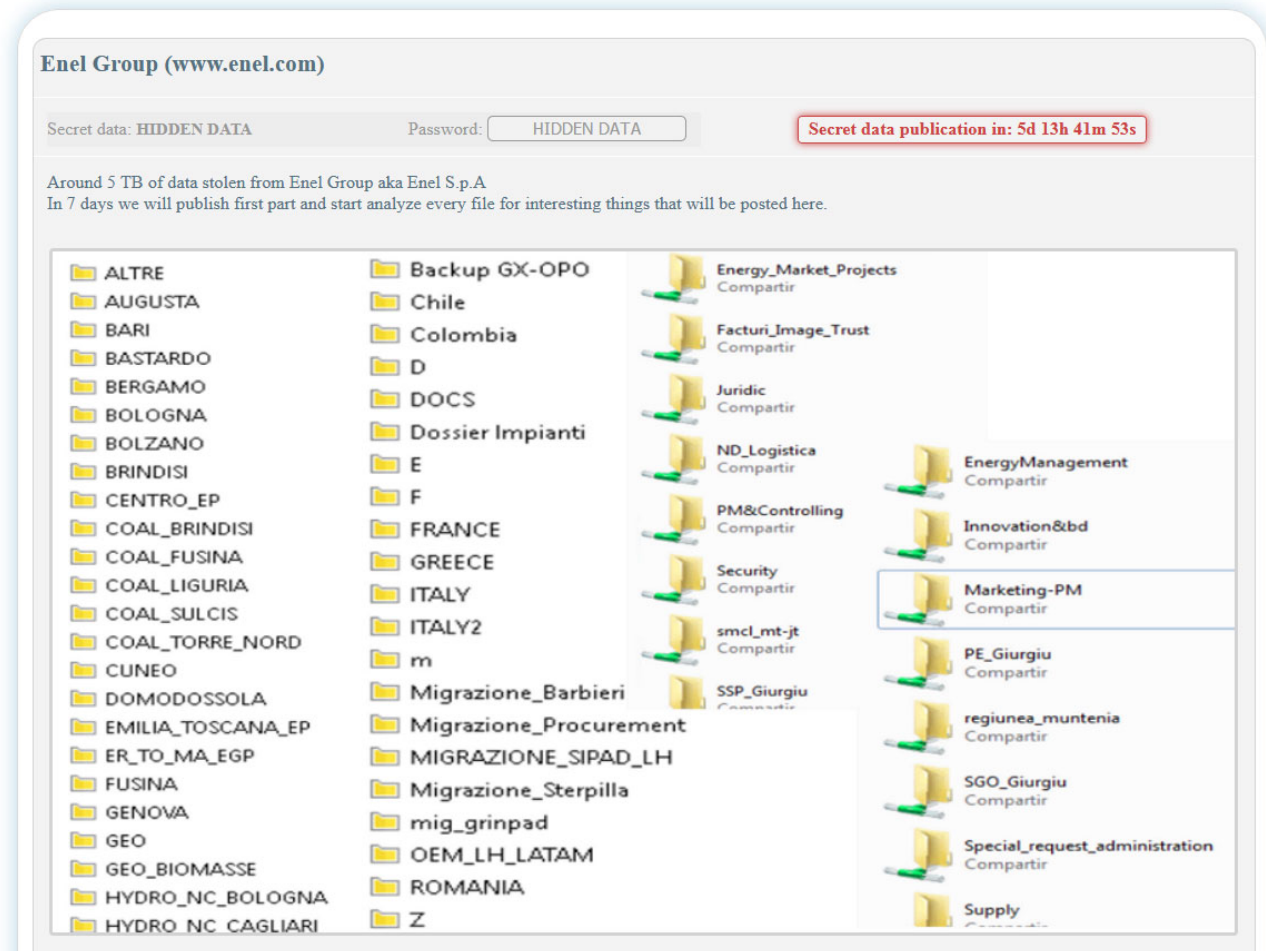
All your files are encrypted..
The only way to decrypt your files, is buying the decryptor.
Your user key is: , you can use it to log in again.
The system is automated. After you make the payment and transaction have 3 network confirmations, you'll be able to download decryptor.

Note: We saw alot of companies spending time and money, trying to recover their files, but in last case they still come and ask our help.
Cooperating with us, you will avoid damaging your company reputation.

Invoice for payment	EXPIRED	Status: Waiting for payment
You can buy the decrypter program for your network.		
Payment expired! New price: 14000000\$ (1234.02380000 BTC)		
Decrypter for: ALL NETWORK / ALL COMPUTERS / ALL FILES		
Bitcoin address: 	Amount for payment: 1234.02380000 BTC	
	You payed: 0.00000000 BTC	

\$14,000,000 million ransom demand

Today, the Netwalker ransomware gang added Enel Group to their data leak site and shared screenshots of unencrypted files from the company during this month's cyberattack.



According to Netwalker, they stole about 5 terabytes of data from Enel and are ready to make public a piece of it in a week. They also said they would "analyze every file for interesting things" and publish it on their leak site.

This tactic is meant to add pressure and force payment from the victim company. In many cases, this works to the advantage of the attacker.

Related Articles:

[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](#)

[New 'Cheers' Linux ransomware targets VMware ESXi servers](#)

[SpiceJet airline passengers stranded after ransomware attack](#)

- [Netwalker](#)

- [Ransomware](#)

[Ionut Ilascu](#)

Ionut Ilascu is a technology writer with a focus on all things cybersecurity. The topics he writes about include malware, vulnerabilities, exploits and security defenses, as well as research and innovation in information security. His work has been published by Bitdefender, Netgear, The Security Ledger and Softpedia.

- [Previous Article](#)
- [Next Article](#)

Post a Comment [Community Rules](#)

You need to login in order to post a comment

Not a member yet? [Register Now](#)

You may also like:
