

# RagnarLocker ransomware hits EDP energy giant, asks for €10M

---

[bleepingcomputer.com/news/security/ragnarlocker-ransomware-hits-edp-energy-giant-asks-for-10m/](https://bleepingcomputer.com/news/security/ragnarlocker-ransomware-hits-edp-energy-giant-asks-for-10m/)

Sergiu Gatlan

By

[Sergiu Gatlan](#)

- April 14, 2020
- 01:35 PM
- 0



Attackers using the Ragnar Locker ransomware have encrypted the systems of Portuguese multinational energy giant Energias de Portugal (EDP) and are now asking for a 1580 BTC ransom (\$10.9M or €9.9M).

EDP Group is one of the largest European operators in the energy sector (gas and electricity) and the world's 4th largest producer of wind energy.

The company is present in 19 countries and on 4 continents, it has over 11.500 employees and delivers energy to more than 11 million customers.

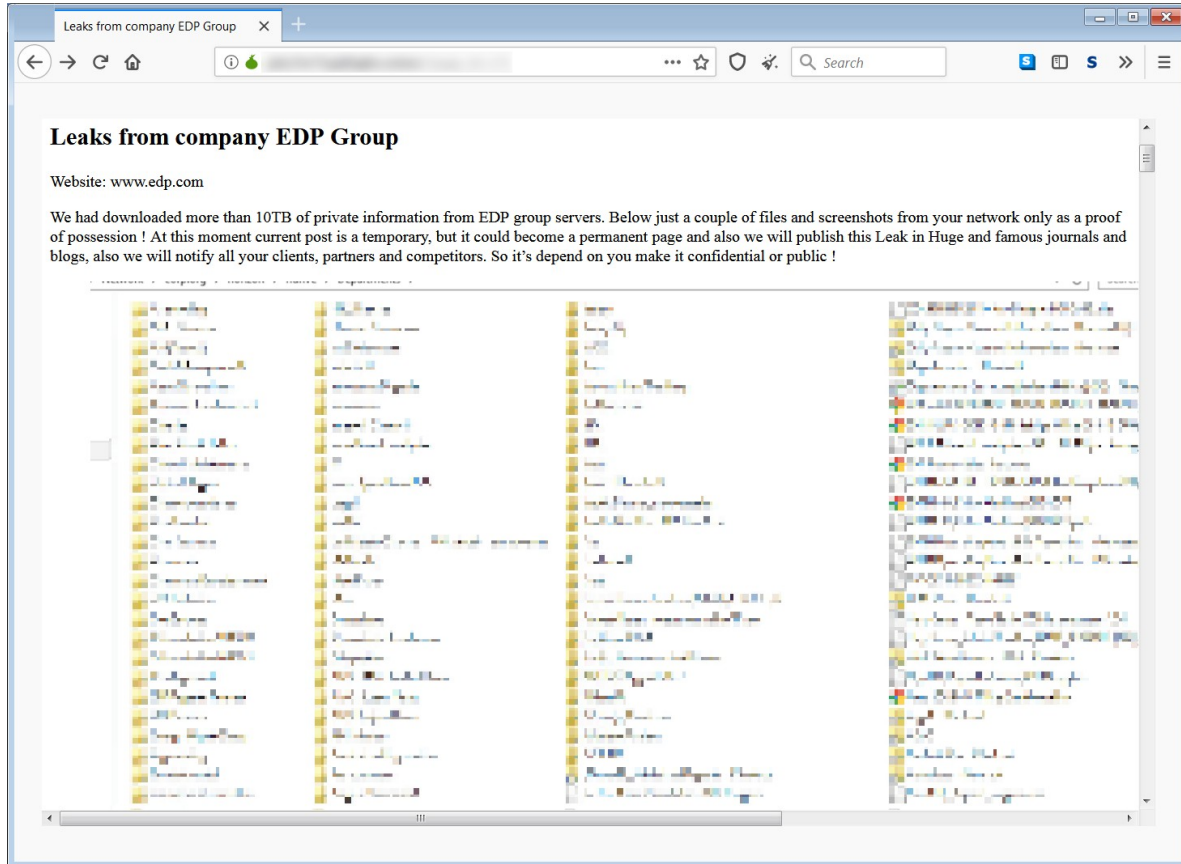
## Attackers threaten to leak 10 TB of stolen documents

---

During the attack, the [Ragnar Locker ransomware](#) operators claim to have stolen over 10 TB of sensitive company files and they are now threatening the company to leak all the stolen data unless the ransom is paid.

"We had downloaded more than 10TB of private information from EDP group servers," a new post on Ragnarok's leak site says.

"Below just a couple of files and screenshots from your network only as a proof of possession! At this moment current post is a temporary, but it could become a permanent page and also we will publish this Leak in Huge and famous journals and blogs, also we will notify all your clients, partners and competitors. So it's depend on you make it confidential or public !"



Among the already leaked files published as a sign of what's to come, the attackers included an edpradmin2.kdb file which is a KeePass password manager database.

When clicked on the leak site, the link leads to a database export including EDP employees' login names, passwords, accounts, URLs, and notes.

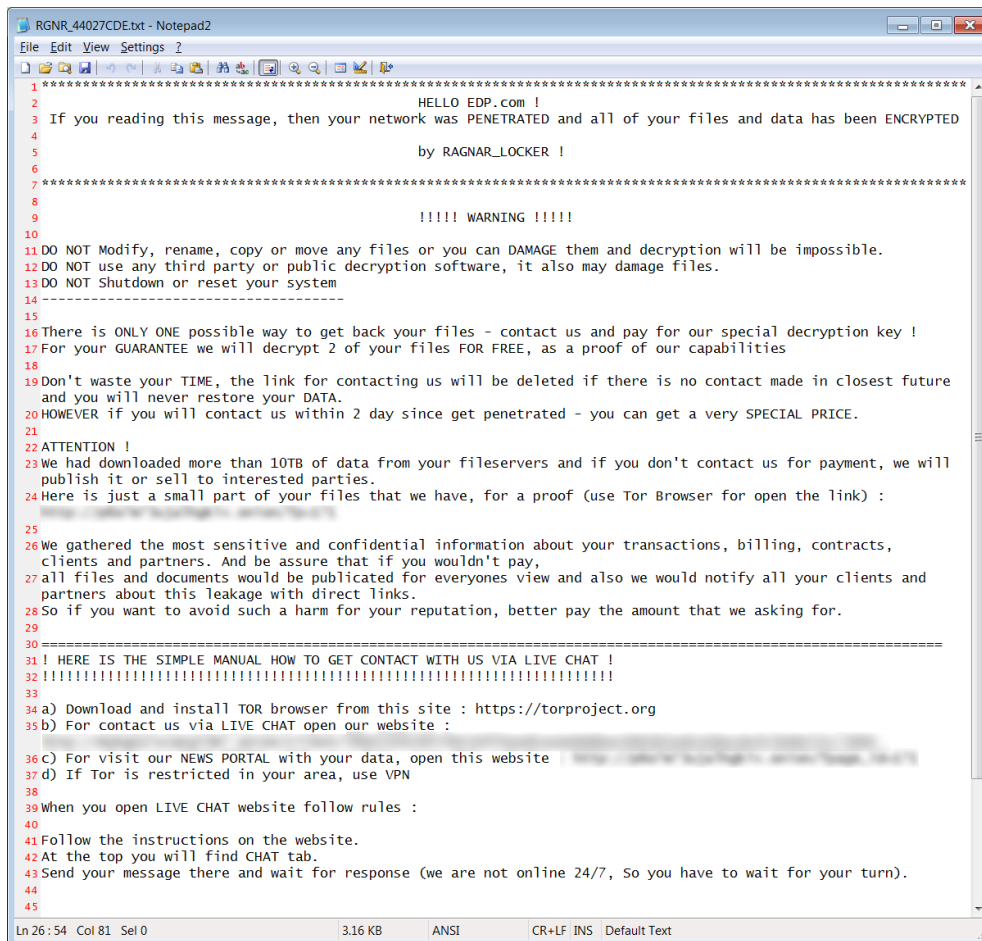
List of files Archive	<a href="#">Link to download</a>
List of files Archive 2	<a href="#">Link to download</a>
edpradmin2.kdb	<a href="#">Link to download</a>
Public.rar	<a href="#">Link to download</a>
Public2.rar	<a href="#">Link to download</a>

The Ragnar Locker ransomware sample used in this attack was found by MalwareHunterTeam and BleepingComputer was able to also find the ransom note and the Tor payment page where the attackers detail the decryption process and the ransom amount.

According to the ransom note dropped on the EDP encrypted systems, the attackers were able to steal confidential information on billing, contracts, transactions, clients, and partners.

"And be assure that if you wouldn't pay, all files and documents would be publicated for everyones view and also we would notify all your clients and partners about this leakage with direct links," the ransom note reads.

"So if you want to avoid such harm for your reputation, better pay the amount that we asking for."

A screenshot of a Notepad2 window titled 'RGNR\_44027CDE.txt - Notepad2'. The window contains a ransom note with the following text:

```
1 *****
2 HELLO EDP.com !
3 If you reading this message, then your network was PENETRATED and all of your files and data has been ENCRYPTED
4
5 by RAGNAR_LOCKER !
6
7 *****
8
9          !!!!! WARNING !!!!!
10
11 DO NOT Modify, rename, copy or move any files or you can DAMAGE them and decryption will be impossible.
12 DO NOT use any third party or public decryption software, it also may damage files.
13 DO NOT Shutdown or reset your system
14 -----
15
16 There is ONLY ONE possible way to get back your files - contact us and pay for our special decryption key !
17 For your GUARANTEE we will decrypt 2 of your files FOR FREE, as a proof of our capabilities
18
19 Don't waste your TIME, the link for contacting us will be deleted if there is no contact made in closest future
20 and you will never restore your DATA.
21 HOWEVER if you will contact us within 2 day since get penetrated - you can get a very SPECIAL PRICE.
22
23 ATTENTION !
24 We had downloaded more than 10TB of data from your fileservers and if you don't contact us for payment, we will
25 publish it or sell to interested parties.
26 Here is just a small part of your files that we have, for a proof (use Tor Browser for open the link) :
27
28 We gathered the most sensitive and confidential information about your transactions, billing, contracts,
29 clients and partners. And be assure that if you wouldn't pay,
30 all files and documents would be publicated for everyones view and also we would notify all your clients and
31 partners about this leakage with direct links.
32 So if you want to avoid such a harm for your reputation, better pay the amount that we asking for.
33
34 -----
35 ! HERE IS THE SIMPLE MANUAL HOW TO GET CONTACT WITH US VIA LIVE CHAT !
36 !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
37
38 a) Download and install TOR browser from this site : https://torproject.org
39 b) For contact us via LIVE CHAT open our website :
40
41 c) For visit our NEWS PORTAL with your data, open this website :
42 d) If Tor is restricted in your area, use VPN
43
44 When you open LIVE CHAT website follow rules :
45
46 Follow the instructions on the website.
47 At the top you will find CHAT tab.
48 Send your message there and wait for response (we are not online 24/7, So you have to wait for your turn).
49
50
```

## EDP taunted in the live chat room

As also seen BleepingComputer, the Ragnar Locker operators taunted EDP in a live chat "client room" used by the attackers to communicate with their victims, asking them to "check the article about your company" on the data leak site and if the company is "ready to see your private information, at the breaking need, tech-blogs, and stockmarket sites."

They also added that the "timer is not waiting" and warned EDP not to attempt to decrypt their data using any other software besides the decryption tool provided by the Ragnar Locker operators as they risk damaging or losing it.

The attackers offered EDP a "special price" if they reach out within two days of their systems having been encrypted, however, they also warned that the company will have to wait for their turn as the ransomware's live chat is not online 24/7.

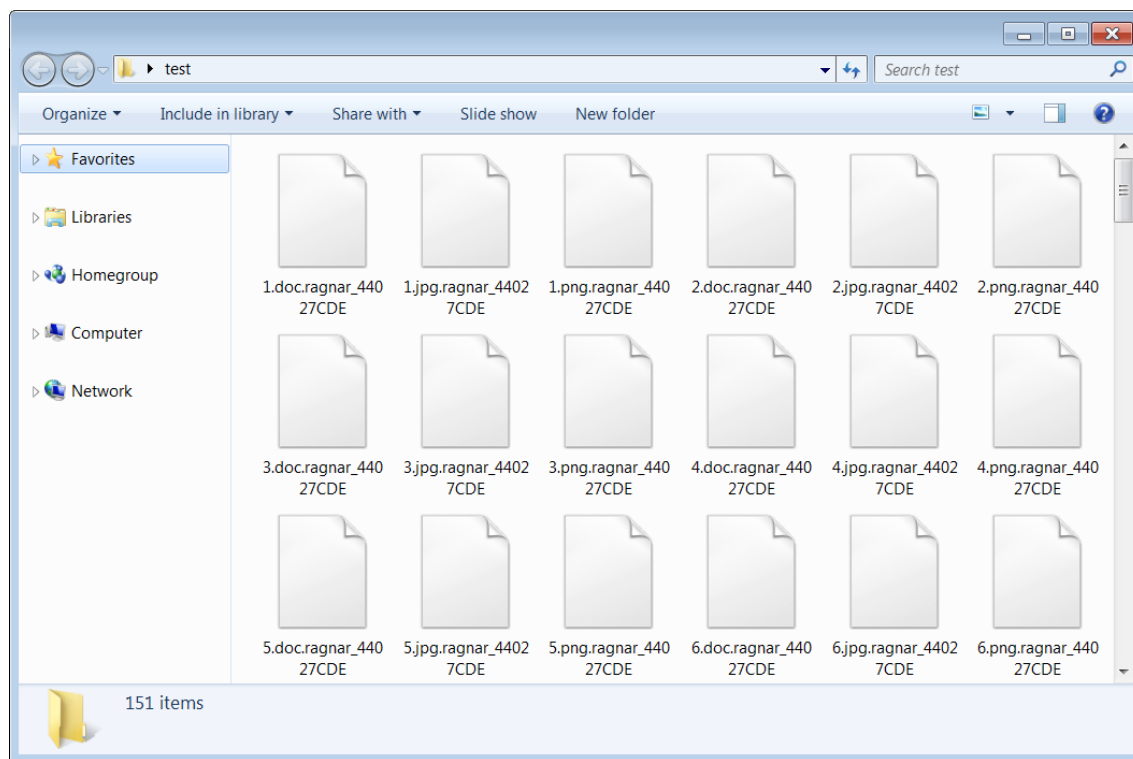
BleepingComputer has reached out to EDP for comment and additional details but had not heard back at the time of this publication. This article will be updated when a response is received.

## Delivered via MSP enterprise support tools

Ragnar Locker ransomware was first spotted while being used as part of attacks against compromised networks towards the end of December 2019.

The Ragnar Locker operators target software regularly used by managed service providers to prevent their attack from being detected and blocked.

Kyle Hanslovan, the CEO of MSP security firm Huntress Labs, told BleepingComputer in February of his company seeing Ragnar Locker being deployed via the MSP software ConnectWise.



After reconnaissance and pre-deployment stages, the attackers drop a highly targeted ransomware executable that adds specific extension to encrypted files, features an embedded RSA-2048 key, and drops custom ransom notes.

The ransom notes include the victim's company name, a link to the Tor site, and the data leak site with the victim's published data.

BleepingComputer has previously seen multiple ransom notes for Ragnar Locker with ransoms ranging from \$200,000 to roughly \$600,000.

---

**Update April 16, 09:21 EDT:** An EDP spokesperson told BleepingComputer that the attack did not impact the company's power supply service and critical infrastructure.

EDP was the target of a computer attack on its corporate network this Monday, April 13th, which conditioned part of its services and operations. The power supply service and critical infrastructure, however, have never been compromised and we continue to ensure this operation as normal.

The situation is currently being assessed and we have teams dedicated to restoring the normal functioning of the systems as soon as possible, which is our priority.

EDP is working with the authorities, that were immediately notified of the attack to identify the origin and anatomy of the attack. At this moment, we have no knowledge of this alleged ransom demand - we have only seen this information disclosed in the media, which we cannot verify.

## **Related Articles:**

---

[Ransom payment is roughly 15% of the total cost of ransomware attacks](#)

[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](#)

- [Energy Supplier](#)
- [Ragnar Locker](#)
- [Ransom](#)
- [Ransomware](#)
- [Renewable Energy](#)

[Sergiu Gatlan](#)

Sergiu Gatlan is a reporter who covered cybersecurity, technology, Apple, Google, and a few other topics at Softpedia for more than a decade. Email or Twitter DMs for tips.

- [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:**

---