Sodinokibi Ransomware Says Travelex Will Pay, One Way or Another

bleepingcomputer.com/news/security/sodinokibi-ransomware-says-travelex-will-pay-one-way-or-another/

Lawrence Abrams

By
Lawrence Abrams

- January 9, 2020
- 12:19 PM
- 0

The attackers behind the Sodinokibi Ransomware are applying pressure on Travelex to pay a multi-million dollar ransom by stating they will release or sell stolen data that allegedly contains customer's personal information.

In a New Year's Eve ransomware attack on Travelex, the Sodinokibi Ransomware operators allegedly stole 5GB of unencrypted files and then proceeded to encrypt the foreign currency exchange company's entire network.

In a conversation with BleepingComputer, the Sodinokibi Ransomware actors state that they were demanding a $3 million ransom or they would release the data containing "DOB SSN CC and other". This amount was later changed to $6 million.

In a statement by Travelex, the currency exchange company is stating that there is no evidence that any data was stolen.

"Whilst the investigation is still ongoing, Travelex has confirmed that the software virus is ransomware known as Sodinokibi, also commonly referred to as REvil. Travelex has proactively taken steps to contain the spread of the ransomware, which has been successful. To date, the company can confirm that whilst there has been some data encryption, there is no evidence that structured personal customer data has been encrypted. Whist Travelex does not yet have a complete picture of all the data that has been encrypted, there is still no evidence to date that any data has been exfiltrated."

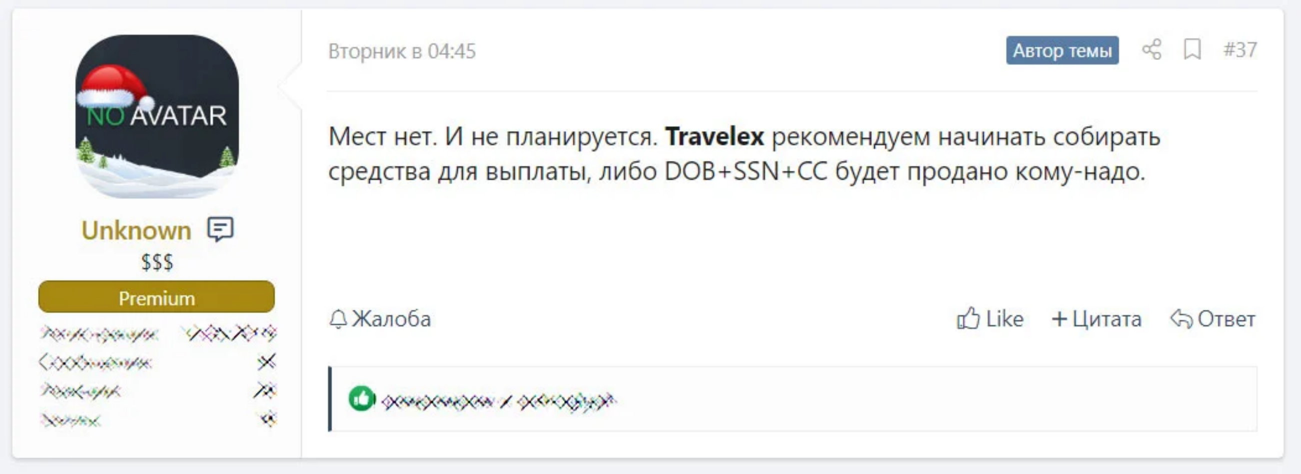
The Sodinokibi actors, though, paint a different picture.

When told that Travelex was denying any data was stolen, they told BleepingComputer that they were currently negotiating the ransom price with Travelex and that they would benefit even if a ransom is not paid.

"If this were true, they would not bargain with us now. On the other hand, we do not care. We will still benefit if they do not pay. Just the damage to them will be more serious."

When we were told this, it was not 100% clear how the ransomware operators would benefit.

This became clear in a recent forum post to a Russian hacker and malware forum where the public representative for the REvil/Sodinokibi Ransomware stated that if Travelex does not pay the ransom, they will sell the stolen PII information of their customers to other attackers.



[redacted]

Мест нет. И не планируется. **Travelex** рекомендуем начинать собирать средства для выплаты, либо DOB+SSN+CC будет продано кому-надо.

[redacted]

Sodinokibi post to a Russian hacker forum

This post translated to English as:

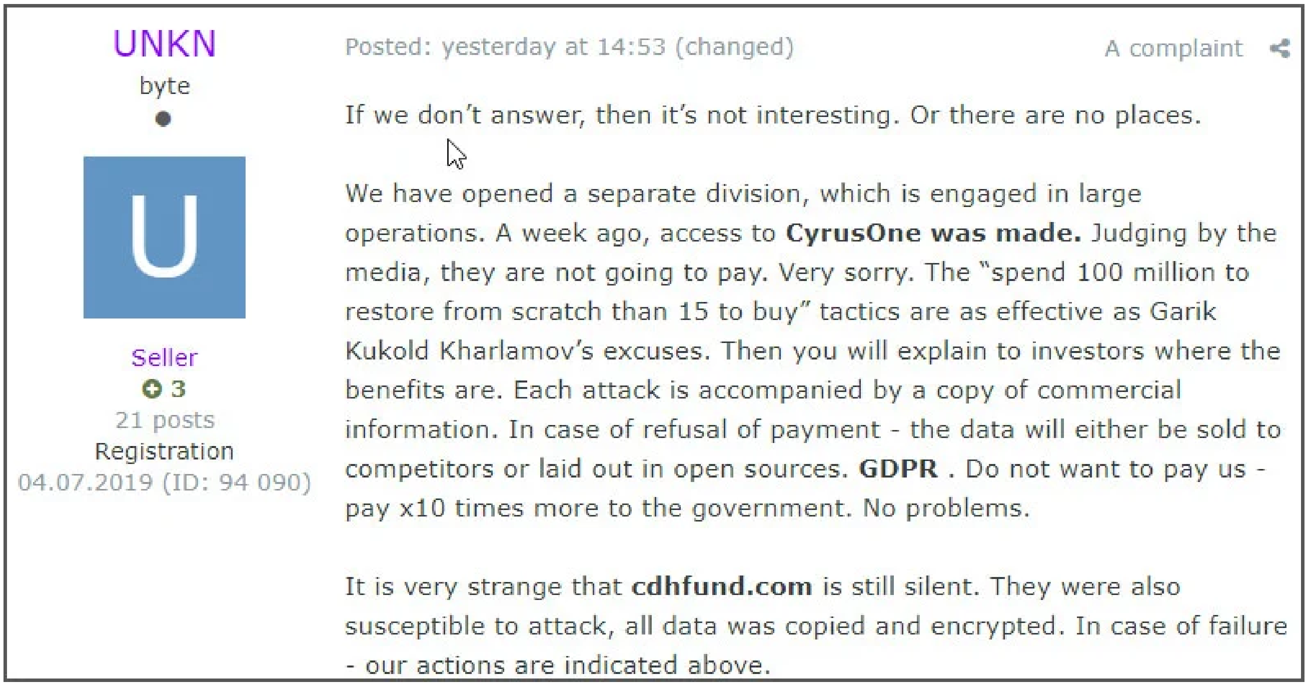
```
There are no seats. And not planned. Travelex recommend starting to raise funds for
payment, or DOB + SSN + CC will be sold to anyone.
```

The statement "There are not seats." in Unknown's post means that REvil is not accepting any new affiliates at this time.

The user named 'Unknown' is the public-facing representative of the Sodinokibi Ransomware and has made forum posts in the past when the ransomware first launched and they began building a team of affiliates composed of veteran malware distributors.

Ransomware operators have been threatening to release stolen data for some time, but none carried out their threats until the Maze Ransomware group released the stolen data of Allied Universal.

Since then, Unknown has also stated that Sodinokibi Ransomware will adopt the tactic of releasing stolen data as leverage to get victims to pay.



Posted: yesterday at 14:53 (changed)

If we don't answer, then it's not interesting. Or there are no places.

We have opened a separate division, which is engaged in large operations. A week ago, access to **CyrusOne was made.** Judging by the media, they are not going to pay. Very sorry. The "spend 100 million to restore from scratch than 15 to buy" tactics are as effective as Garik Kukold Kharlamov's excuses. Then you will explain to investors where the benefits are. Each attack is accompanied by a copy of commercial information. In case of refusal of payment - the data will either be sold to competitors or laid out in open sources. **GDPR** . Do not want to pay us - pay x10 times more to the government. No problems.

It is very strange that **cdhfund.com** is still silent. They were also susceptible to attack, all data was copied and encrypted. In case of failure - our actions are indicated above.

Unknown's post about releasing stolen data

To this date, Sodinokibi has not released any stolen data and it is not known for sure if they will release Travelex's if the ransom is not paid.

However, if the data is released, it will open up a whole new world of business problems for Travelex

The Sodinokibi actors are right, too. No matter what happens, Travelex will incur further damage; either through the payment of a ransom, the public release of their data, or by the data being sold to other threat actors.

If the data is released, the attack will need to be classified as a data breach, notifications and free monitoring services will need to be offered, GDPR fines would be likely as are the risks of class action lawsuits.

BleepingComputer has contacted Travelex with questions regarding this story, but has not heard back.

Transparency in ransomware attacks is necessary

When an organization suffers a ransomware attack, they usually try to hide the attack or downplay its impact to prevent customer concerns, damage to brand image, and a plunging stock price.

This commonly, though, backfires as the severity of the attacks ultimately leak and make the company look worse than if they had been transparent about it in the first place.

Now that many ransomware attackers are claiming to steal data before encrypting devices, it is more important than ever to be transparent about these attacks as they could now be classified as data breaches.

By hiding this information, companies are more likely to be hit with government fines and lawsuits as customers' personal information is compromised.

Instead, companies should follow Norsk Hydro's lead and be fully transparent during a ransomware attack by providing timely updates, customer notifications, and public information.

This approach not only made Norsk Hydro customers feel better but also increased their brand image.

Related Articles:

Industrial Spy data extortion market gets into the ransomware game

New RansomHouse group sets up extortion market, adds first victims

The Week in Ransomware - May 6th 2022 - An evolving landscape

Conti, REvil, LockBit ransomware bugs exploited to block encryption

Quantum ransomware seen deployed in rapid network attacks

- Blackmail
- Data Exfiltration
- Extortion
- Ransomware
- REvil
- Sodinokibi
- Travelex

Lawrence Abrams

Lawrence Abrams is the owner and Editor in Chief of BleepingComputer.com. Lawrence's area of expertise includes Windows, malware removal, and computer forensics. Lawrence Abrams is a co-author of the Winternals Defragmentation, Recovery, and Administration Field Guide and the technical editor for Rootkits for Dummies.

- 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: