Sodinokibi Ransomware Publishes Stolen Data for the First Time

bleepingcomputer.com/news/security/sodinokibi-ransomware-publishes-stolen-data-for-the-first-time/

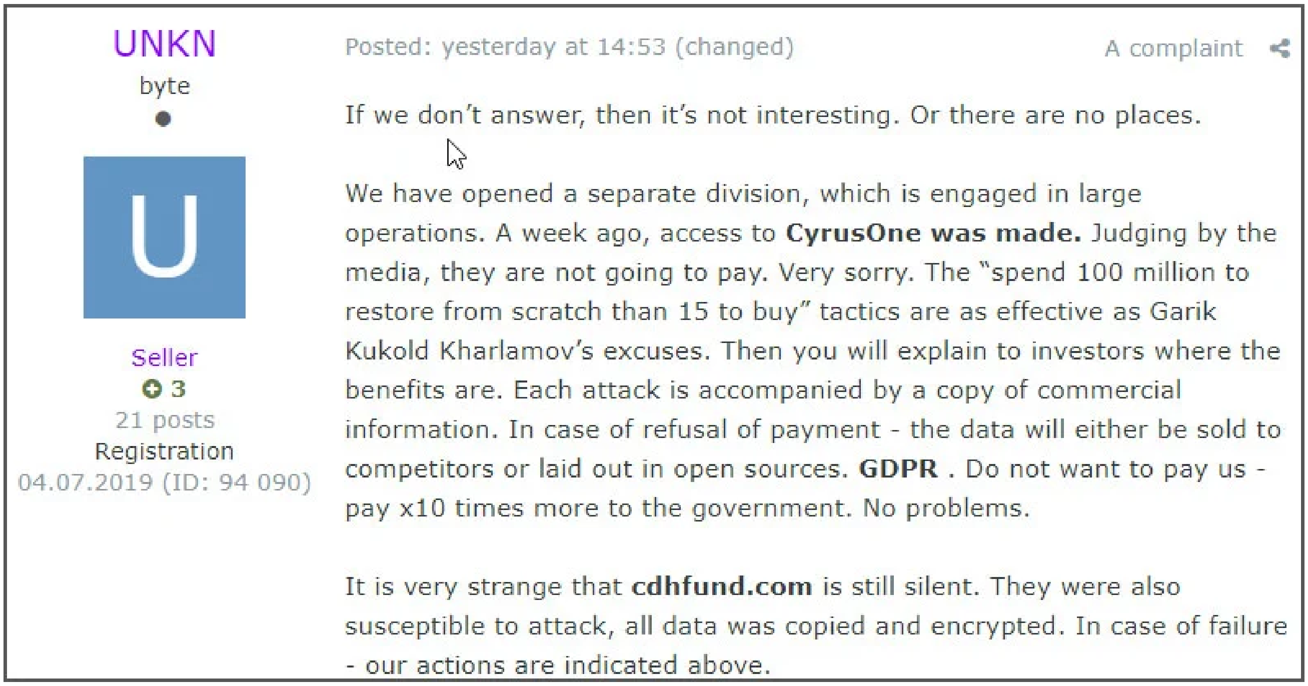
Lawrence Abrams

By
Lawrence Abrams

- January 11, 2020
- 06:07 PM
- 2

For the first time, the operators behind the Sodinokibi Ransomware have released files stolen from one of their victims because a ransom was not paid in time.

Since last month, the representatives of the Sodinokibi, otherwise known as REvil, have publicly stated that they would begin to follow Maze's example and publish data stolen from victims if they do not pay a ransom.



UNKN
byte
Seller
3
21 posts
Registration
04.07.2019 (ID: 94 090)

Posted: yesterday at 14:53 (changed)

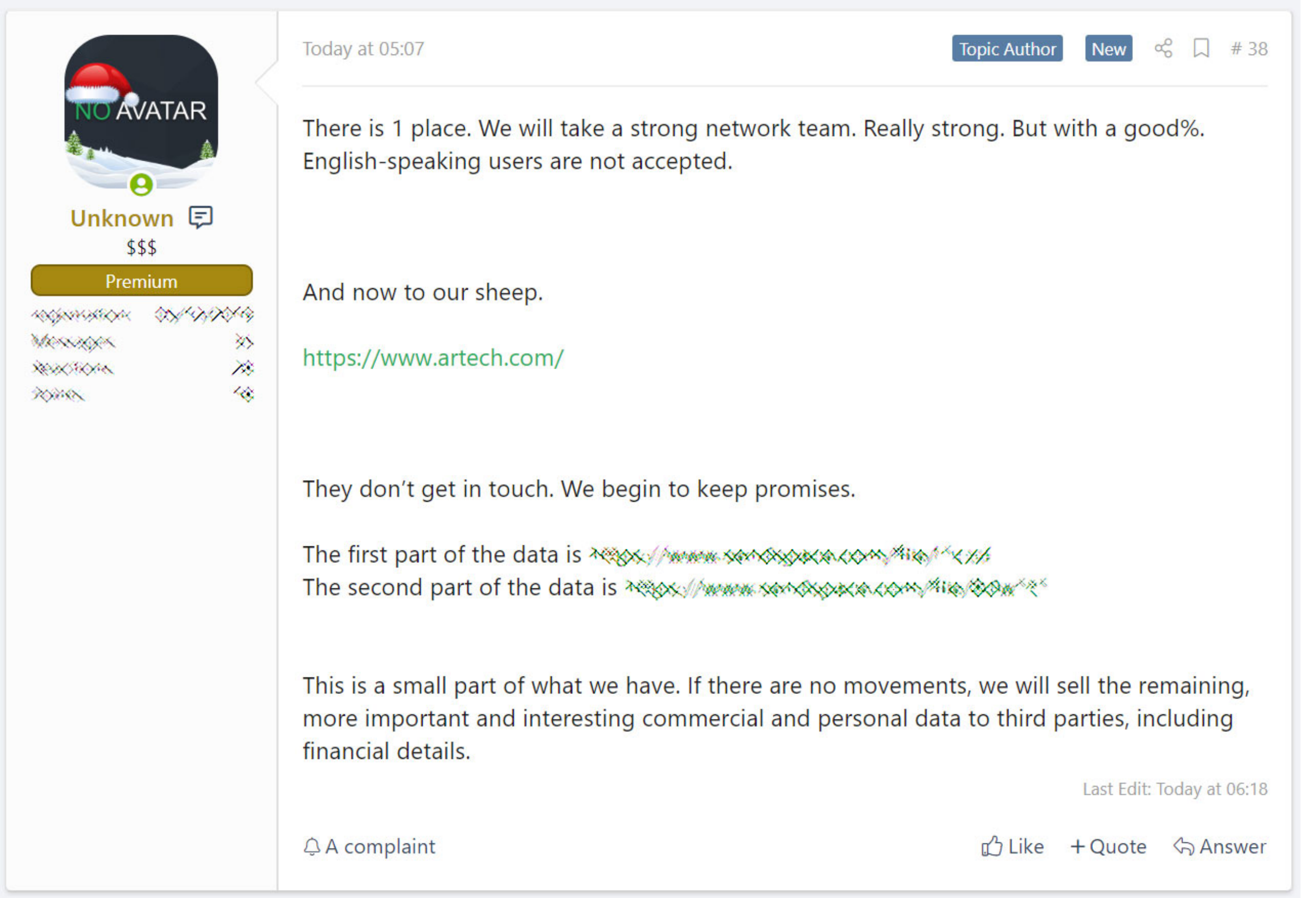
If we don’t answer, then it’s not interesting. Or there are no places.

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.

While there have been threats made against Travelex and CDH Investments, they have not carried through with them.

This all changed today when the public representative of Sodinokibi stated they beginning to "keep promises" as they posted links to approximately 337MB of allegedly stolen victim files on a Russian hacker and malware forum.



[redacted]

There is 1 place. We will take a strong network team. Really strong. But with a good%. English-speaking users are not accepted.

And now to our sheep.

https://www.artech.com/

They don't get in touch. We begin to keep promises.

The first part of the data is [redacted]
The second part of the data is [redacted]

This is a small part of what we have. If there are no movements, we will sell the remaining, more important and interesting commercial and personal data to third parties, including financial details.

Sodinokibi publishing victim's data
Source: Damien

They claim this data belongs to Artech Information Systems, who describe themselves as a "minority- and women-owned diversity supplier and one of the largest IT staffing companies in the U.S", and that they will release more if a ransom is not paid.

"This is a small part of what we have. If there are no movements, we will sell the remaining, more important and interesting commercial and personal data to third parties, including financial details."

At this time, Artech's site is down and it is not known if it is due to this attack. BleepingComputer has reached out to Artech with questions related to the ransomware attack, but have not heard back.

As we have been saying over and over, ransomware attacks need to be treated with transparency and as a data breach.

By trying to hide these attacks, and the theft of employee, company, and customer data, companies are not only risking fines and lawsuits but are also putting personal data at risk.

This practice of using stolen data as leverage is not going to go away and is only going to get worse.

Expect to see more ransomware operators began to utilize this practice as it becomes the norm in attacks.

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

- Data Exfiltration
- Extortion
- Ransomware
- REvil
- Sodinokibi

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

Comments

-

  thattimguy - 2 years ago

  -
  -

  I worked for Artech at a F.A.N.G. company, where they happen to be staffing large numbers of people. Slightly concerned.

-

  Lawrence Abrams - 2 years ago

  -
  -

  We have not heard back from them unfortunately.

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: