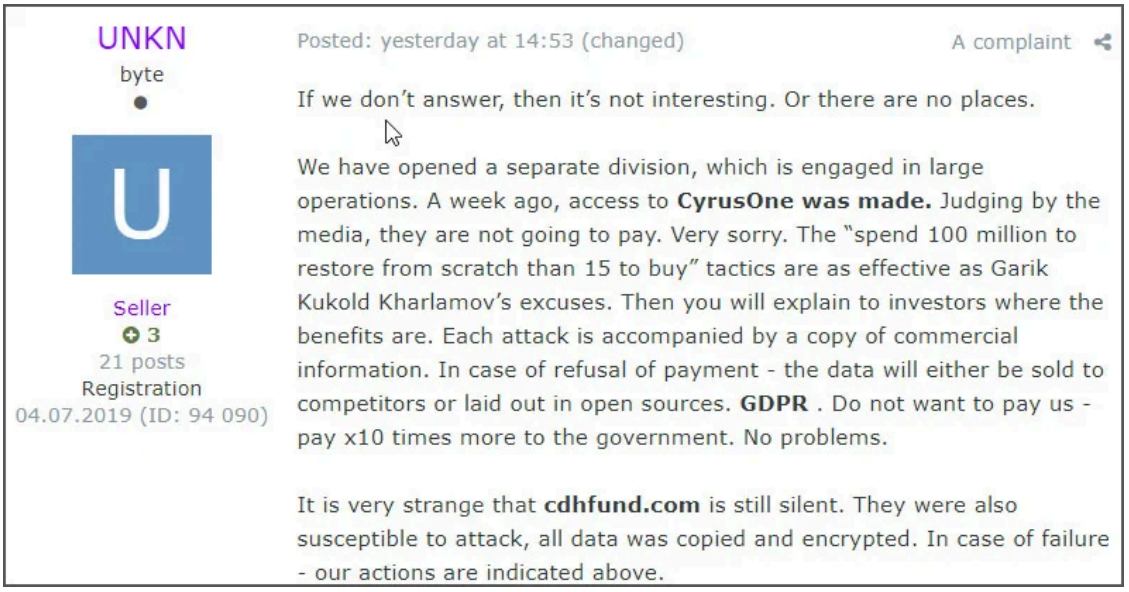
Sodinokibi Ransomware Publishes Stolen Data for the First Time

By Lawrence Abrams

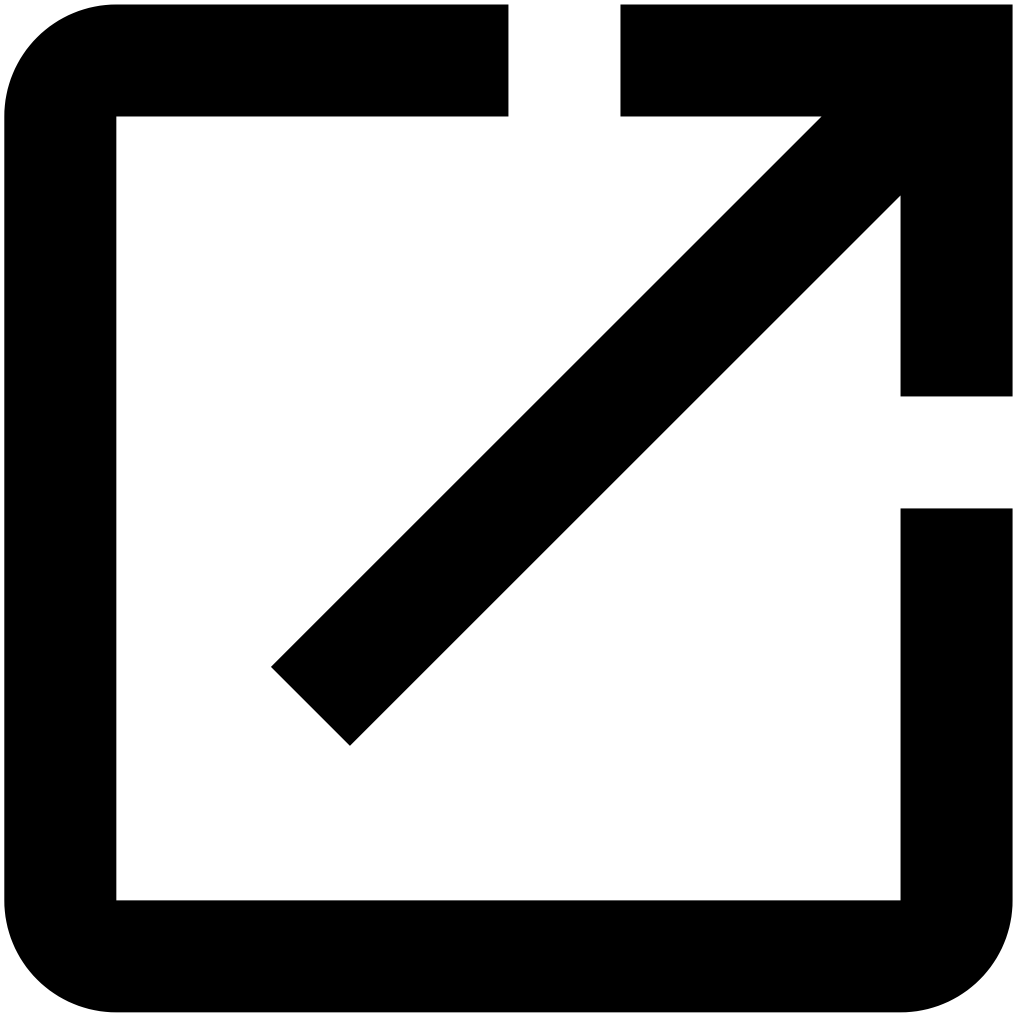
Published: 2020-01-11 · Archived: 2026-04-05 13:28:40 UTC

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.

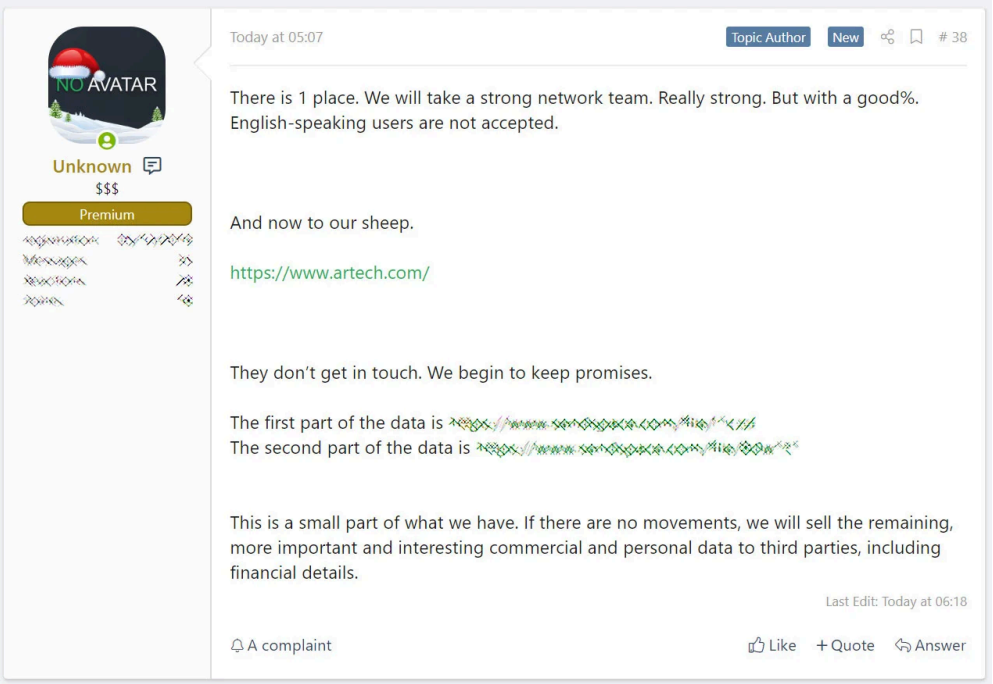



DIE LINKE.
0:00



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.



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.
