Sodinokibi Ransomware May Tip NASDAQ on Attacks to Hurt Stock Prices

By Lawrence Abrams

Published: 2020-02-27 · Archived: 2026-04-05 14:18:05 UTC

The operators of the Sodinokibi Ransomware (REvil) have started urging affiliates to copy their victim's data before encrypting computers so it can be used as leverage on a new data leak site that is being launched soon.

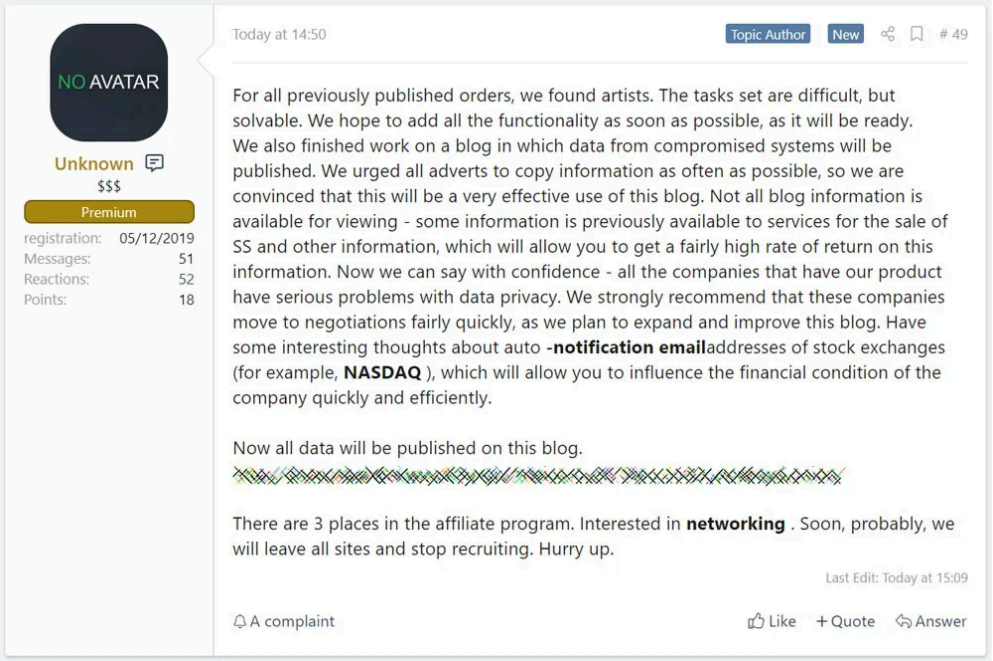
The Sodinokibi Ransomware ransomware operation is a Ransomware-as-a-Service where the operators manage the payment portal and development of the ransomware and third-party 'affiliates' distribute the ransomware.

The operators and affiliates then share the ransomware payment made by victims.


DIE LINKE.
0:00

Most likely spurred on by the release of DoppelPaymer's data leak web site this week, the public-facing representative of Sodinokibi, Unknown, outlined their plans for the further extortion of victims on a Russian malware and hacker forum.

According to the post shared with BleepingComputer by Damian, the ransomware operators have finished a 'blog' that will be used to distribute unpaid victim's stolen data, with some data like Social Security numbers being held back to be sold on dark markets for a 'fairly high rate of return'.



Sodinokibi plans for their data leak site

Unknown states that the companies who are encrypted by REvil have "serious problems with data privacy" and should move to negotiations quickly.

Further laying their plans out in the open, Unknown speculates on other ways that they can further pressure victims to pay a ransom.

One idea they are thinking about is to auto-email stock exchanges, such as NASDAQ, to let them know about the company's attack and hurt the value of their stock.

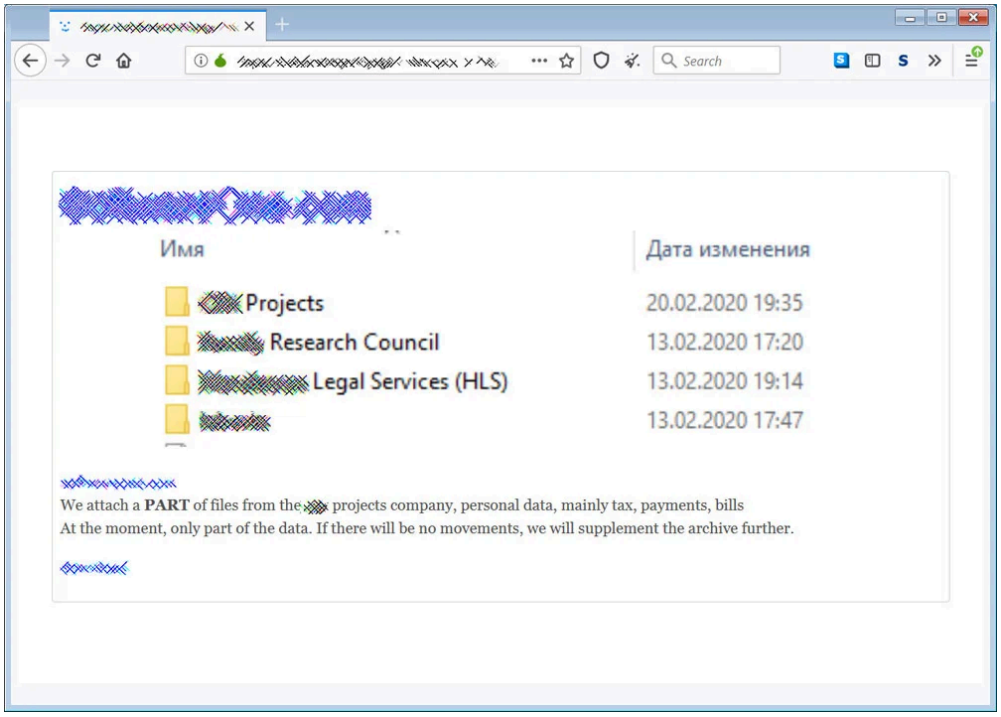
The full posted translated from Russian can be read below:

```
 For all previously published orders, we found artists. The tasks set are difficult, but solvable. We hope to add all the
We also finished work on a blog in which data from compromised systems will be published. We urged all adverts to copy in

Now all data will be published on this blog.
xxx

There are 3 places in the affiliate program. Interested in networking . Soon, probably, we will leave all sites and stop
```

As part of this post, they also linked to a 10MB stolen data dump of one of their victims that they claim contains financial and tax information. They go on to state that they will add more to this data dump if the victim does not pay.



Leaked data of a victim

BleepingComputer will not be naming the victim until we confirm the validity of the alleged attack.

Ransomware attacks are data breaches!

This feels like a daily statement from BleepingComputer, but all ransomware attacks are now data breaches and must be treated as such.

The files that were stolen by ransomware operators not only contain company data but also the personal information of its employees.

By not disclosing these attacks and what has been stolen, company's put their employees at risk of identity theft, fraud, and other malicious attacks.

This could lead to fines by government agencies and lawsuits from employees whose data has been compromised.

Be smart and transparent about ransomware attacks. It is better in the long run.

Source: https://www.bleepingcomputer.com/news/security/sodinokibi-ransomware-may-tip-nasdaq-on-attacks-to-hurt-stock-prices/