# Ransomware Threatens to Reveal Company's 'Dirty' Secrets

bleepingcomputer.com/news/security/ransomware-threatens-to-reveal-companys-dirty-secrets/

Lawrence Abrams

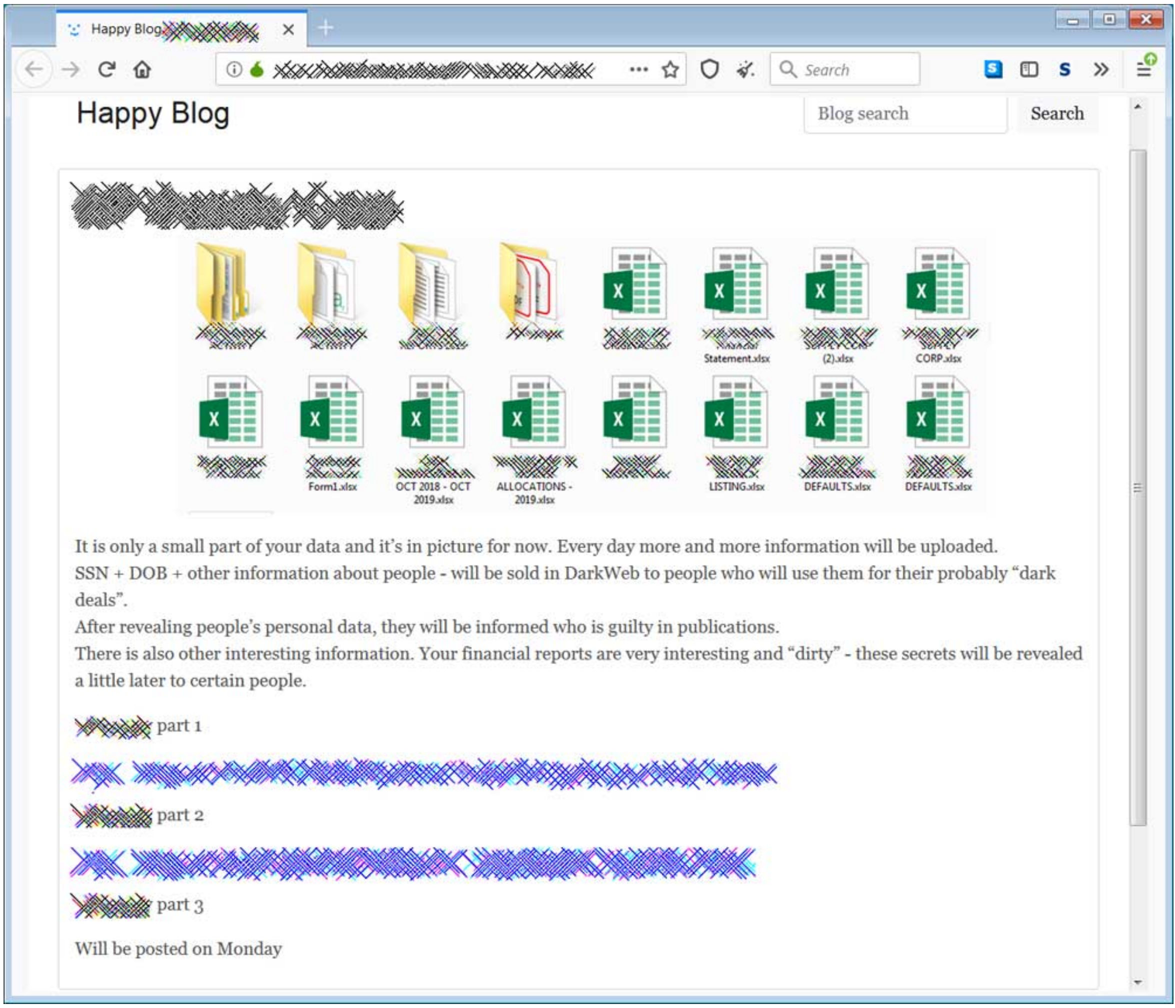
By
Lawrence Abrams

- March 7, 2020
- 10:15 AM
- 0

The operators of the Sodinokibi Ransomware are threatening to publicly share a company's "dirty" financial secrets because they refused to pay the demanded ransom.

As organizations decide to restore their data manually or via backups instead of paying ransoms, ransomware operators are escalating their attacks.

In a new post by the Sodinokibi operators to their data leak site, we can see that attackers are not only publishing victim's data but also sifting through it to find damaging information that can be used against the victim.



It is only a small part of your data and it's in picture for now. Every day more and more information will be uploaded.
SSN + DOB + other information about people - will be sold in DarkWeb to people who will use them for their probably "dark deals".
After revealing people's personal data, they will be informed who is guilty in publications.
There is also other interesting information. Your financial reports are very interesting and "dirty" - these secrets will be revealed a little later to certain people.

[redacted] part 1

[redacted]

[redacted] part 2

[redacted]

[redacted] part 3

Will be posted on Monday

**Entry on Ransomware data leak site**

In the above post, the attackers are threatening to sell the Social Security Numbers and date of births for people in the data to other hackers on the dark web.

They also intimate that they found "dirty" financial secrets in the data and threaten to disclose it.

"It is only a small part of your data and it’s in picture for now. Every day more and more information will be uploaded.
SSN + DOB + other information about people - will be sold in DarkWeb to people who will use them for their probably “dark deals”.
After revealing people’s personal data, they will be informed who is guilty in publications.
There is also other interesting information. Your financial reports are very interesting and “dirty” - these secrets will be revealed a little later to certain people."

These new extortion attempts further illustrate how victims need to treat ransomware attacks very seriously.

It is no longer only about getting your data back, but also the risk of very private and personal data being exposed and sold to other attackers.

This not only puts the company's who were attacked at risk but also their employees whose data is disclosed.

While companies should not pay a ransom if it could be avoided, even if data is published, they should disclose these attacks as data breaches so employees can protect themselves.

BleepingComputer has contacted the company for a public statement but has not heard back as of yet.

## Related Articles:

Industrial Spy data extortion market gets into the ransomware game

New RansomHouse group sets up extortion market, adds first victims

Quantum ransomware seen deployed in rapid network attacks

Karakurt revealed as data extortion arm of Conti cybercrime syndicate

Snap-on discloses data breach claimed by Conti ransomware gang

- Data Exfiltration
- Extortion
- Ransomware
- 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

## You may also like: