Sodinokibi Ransomware Threatens to Publish Data of Automotive Group

bleepingcomputer.com/news/security/sodinokibi-ransomware-threatens-to-publish-data-of-automotive-group/

Sergiu Gatlan

By
Sergiu Gatlan

- January 23, 2020
- 02:00 AM
- 0

The attackers behind the Sodinokibi Ransomware are now threatening to publish data stolen from another victim after they failed to get in touch and pay the ransom to have the data decrypted.

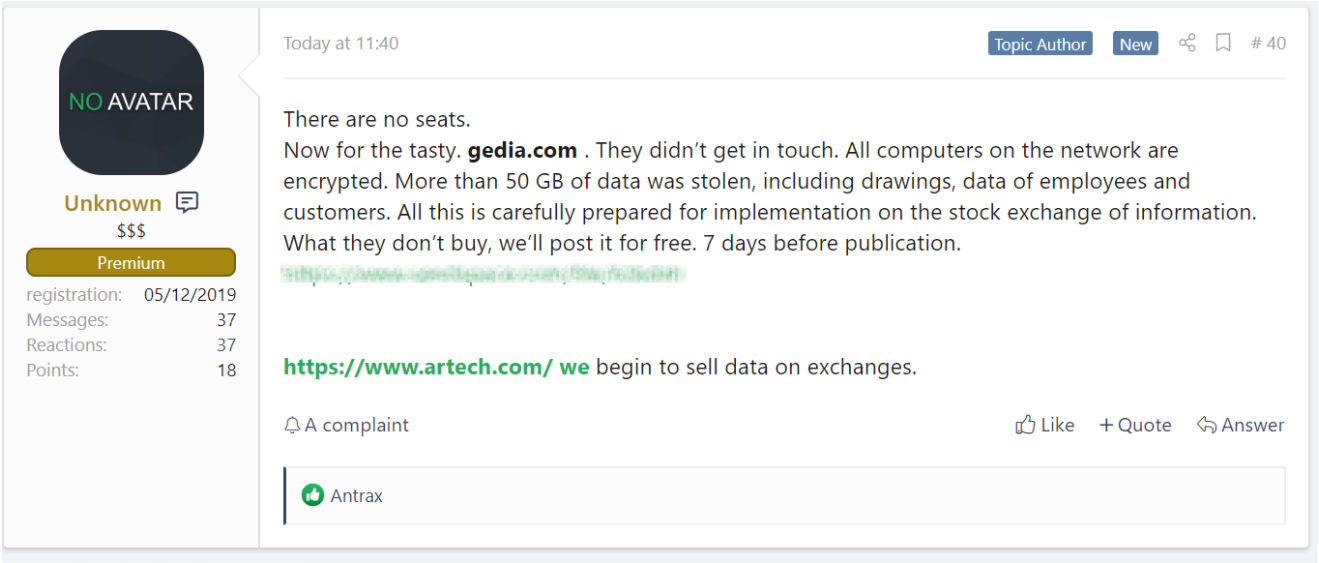
Sodinokibi claims that this data was stolen from GEDIA Automotive Group, a German automotive supplier with production plants in Germany, China, Hungary, India, Mexico, Poland, Hungary, Spain, and the USA.

GEDIA also has over 4,300 employees all around the world and it had an annual turnover of €600 million (over $665 million) in 2017.

The group published a Microsoft Excel spreadsheet containing an AdRecon report with information on an Active Directory environment.

The Sodin attackers appear to use Sense of Security's open-source AdRecon tool on each of their victims' AD environments as they have also released a similar spreadsheet for a previous victim named Artech Information Systems.

BleepingComputer asked GEDIA to confirm the ransomware attack but did not hear back at the time of publication.



"Now for the tasty. gedia.com . They didn't get in touch. All computers on the network are encrypted," as Sodinokibi said on a Russian hacker and malware forum. "More than 50 GB of data was stolen, including drawings, data of employees and customers.

All this is carefully prepared for implementation on the stock exchange of information. What they don't buy, we'll post it for free. 7 days before publication."

This happens after Sodinokibi posted download links to 337 MB worth of files supposedly stolen from Artech Information Systems, a "minority- and women-owned diversity supplier and one of the largest IT staffing companies in the U.S."

The operators behind Sodinokibi Ransomware also said that they'll begin selling the data they stole from Artech on data exchange platforms frequented by cybercriminals as they threatened on January 11.

Ransomware groups now behind potential data breaches

Exfiltrating data before encrypting ransomware victims' systems and leaking the stolen data is a new tactic recently adopted by ransomware gangs.

If their victims don't pay the ransom, the attackers will then slowly start leaking parts of the stolen data cache until they get paid or all the files have been released.

This new trend started by Maze Ransomware during late November 2019 and now adopted by Sodinokibi, as well as Nemty Ransomware and BitPyLock during January 2020 who are saying that they'll start stealing data before encrypting victims' devices.

Even though they would also sniff around their victims' files before publicly announcing it, ransomware groups never released any of the data they stole until Maze Ransomware leaked 700 MB worth of documents stolen from Allied Universal during late-November.

Companies that get hit by ransomware aren't yet treating such security incidents as data breaches even though a wide range of sensitive records containing personal, financial, and medical information now also gets swiped before being encrypted and ransomed.

This will most probably change in the near future, as lawmakers will take notice and will push out legislation also requiring data breach disclosures following ransomware attacks.

H/T Damian

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

The Week in Ransomware - March 18th 2022 - Targeting the auto industry