Another Ransomware Will Now Publish Victims' Data If Not Paid

bleepingcomputer.com/news/security/another-ransomware-will-now-publish-victims-data-if-not-paid/

Lawrence Abrams

By
Lawrence Abrams

- December 12, 2019
- 03:20 PM
- 4

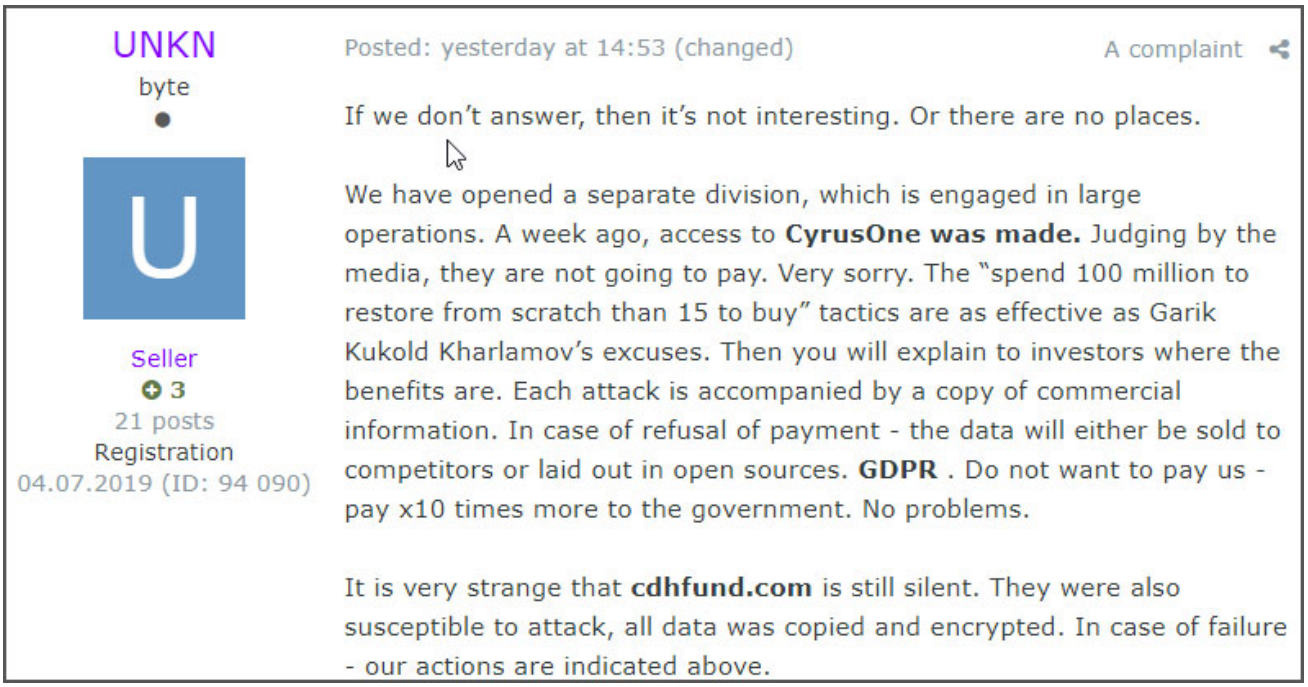
The operators of the REvil Ransomware, otherwise known as Sodinokibi, have announced that they will use stolen files and data as leverage to get victims to pay ransoms.

A new tactic by ransomware developers is to release a victim's data if they do not pay the ransom. While we have seen these threats in the past, only recently have Ransomware operators, such as Maze, actually followed through.

In a new post to a Russian malware and hacker forum shared with us by security researcher Damian, the public-facing representative of the REvil ransomware known as UNKN states that a new "division" has been created for large operations.

They claim that a recent operation from this group is the attack against the CyrusOne data center that was reported last week. As part of this operation, UNKN claims that they have stolen files from the company before encrypting their network.

REvil goes on to say that if a company does not pay the ransom, the ransomware actors will publicly release the stolen data or sell it to competitors. It is in their opinion that this would be more costly to the victim than paying the ransom.



Forum post by REvil operator

The original Russian text from the above post is below:

```
Если не отвечаем - значит не интересны. Либо мест нет.

Мы открыли отдельное подразделение, которое занимается крупными операциями. Неделю
назад был осуществлен доступ к CyrusOne. Судя по СМИ - платить они не собираются.
Очень жаль. Тактика "потратим 100 миллионов на восстановление с нуля, чем 15 на
выкуп" такая же эффективная, как и оправдания Гарика Куколда Харламова. Инвесторам
потом будете объяснять, где выгода. Каждая атака сопровождается копированием
коммерческой информации. В случае отказа выплаты - данные будут либо проданы
конкурентам, либо выкладываться в открытые источники. GDPR. Не хотите платить нам -
платите в x10 раз больше правительству. Нет проблем.

Очень странно, что cdhfund.com до сих пор молчат. Они также были подвержены атаке,
все данные скопированы и зашифрованы. В случае отказа - наши действия обозначены
выше.
```

The English translation via Google Translate can also be read below:

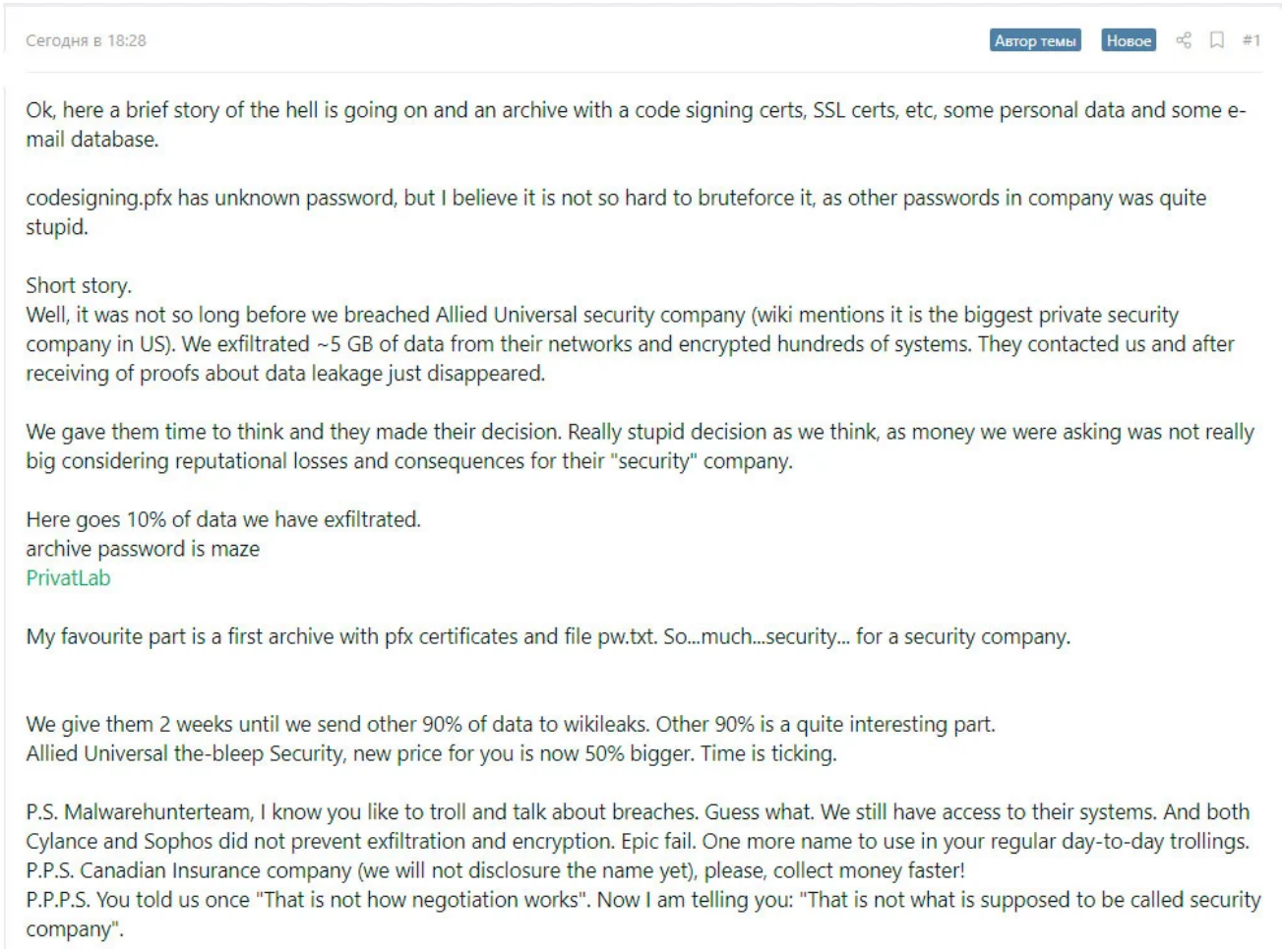
```
If we don't answer, then it's not interesting. Or there are no places.

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.
```

Ransomware attacks are now data breaches

For years, ransomware developers and affiliates have been telling victims that they must pay the ransom or stolen data would be publicly released.

While it has been a well-known secret that ransomware actors snoop through victim's data, and in many cases steal it before the data is encrypted, they never actually carried out their threats of releasing it.

This all changed at the end of November when Maze Ransomware threatened Allied Universal that if they did not pay the ransom, they would release their files. When they did not receive a payment, they released 700MB worth of data on a hacking forum.



Сегодня в 18:28 Автор темы Новое #1

Ok, here a brief story of the hell is going on and an archive with a code signing certs, SSL certs, etc, some personal data and some e-mail database.

codesigning.pfx has unknown password, but I believe it is not so hard to bruteforce it, as other passwords in company was quite stupid.

Short story.
Well, it was not so long before we breached Allied Universal security company (wiki mentions it is the biggest private security company in US). We exfiltrated ~5 GB of data from their networks and encrypted hundreds of systems. They contacted us and after receiving of proofs about data leakage just disappeared.

We gave them time to think and they made their decision. Really stupid decision as we think, as money we were asking was not really big considering reputational losses and consequences for their "security" company.

Here goes 10% of data we have exfiltrated.
archive password is maze
PrivatLab

My favourite part is a first archive with pfx certificates and file pw.txt. So...much...security... for a security company.

We give them 2 weeks until we send other 90% of data to wikileaks. Other 90% is a quite interesting part.
Allied Universal the-bleep Security, new price for you is now 50% bigger. Time is ticking.

P.S. Malwarehunterteam, I know you like to troll and talk about breaches. Guess what. We still have access to their systems. And both Cylance and Sophos did not prevent exfiltration and encryption. Epic fail. One more name to use in your regular day-to-day trollings.
P.P.S. Canadian Insurance company (we will not disclosure the name yet), please, collect money faster!
P.P.P.S. You told us once "That is not how negotiation works". Now I am telling you: "That is not what is supposed to be called security company".

Public disclosure of Allied Universal data

During ransomware attacks, some threat actors have told companies that they are familiar with internal company secrets after reading the company's files. Even though this should be considered a data breach, many ransomware victims simply swept it under the rug in the hopes that nobody would ever find out.

Now that ransomware operators are releasing victim's data, this will need to change and companies will have to treat these attacks like data breaches.

This is because employee medical records, personal information, termination letters, salaries, and much more can potentially be disclosed. Furthermore, if any third-party information is stolen, which is highly likely, then that requires further disclosure as well.

It is too soon to say whether these new tactics will push companies to treat ransomware attacks like data breaches, but as more ransomware developers publish stolen documents, we can expect lawsuits and public concern to rise.

Related Articles:

Industrial Spy data extortion market gets into the ransomware game

Snap-on discloses data breach claimed by Conti ransomware gang

Shutterfly discloses data breach after Conti ransomware attack

New RansomHouse group sets up extortion market, adds first victims

Ransomware attack exposes data of 500,000 Chicago students

- Data Breach
- 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

- 

Whalley_World - 2 years ago

  -
  -

Lawsuits? That's like the victims of an armed robbery being sued by other customers!

- 

Lawrence Abrams - 2 years ago

  -
  -

It's not unheard of for employees suing a company due to "poor" security after being hacked.

Here is an example: https://www.bleepingcomputer.com/news/security/citrix-sued-for-not-securing-employee-info-before-data-breach/

- 

  Pointless_noise - 2 years ago

  -
  -

  Hoping not to be a complete pedant but PII unrecoverable from a ransomware attack is already a data breach under article 4 paragraph 12. Also it could be argued that the encryption of data by a malicious 3rd party could be unlawful "alteration" therefore again a data breach in the eyes of the GDPR. My point being if you're company is not treating ransomware encrypting PII as a data breach it probably should be.

- 

  Lawrence Abrams - 2 years ago

  -
  -

  I 100% agree, but to make matters worse and what I alluded to in the story, it has been known for some time that ransomware attackers sift through company files in order to add information to their ransom notes that scare the victim into paying.

  It's just gotten worse with their willingness to actually publish data to public.

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: