New Ransomware Group: RansomHouse – Is it Real or Fake?

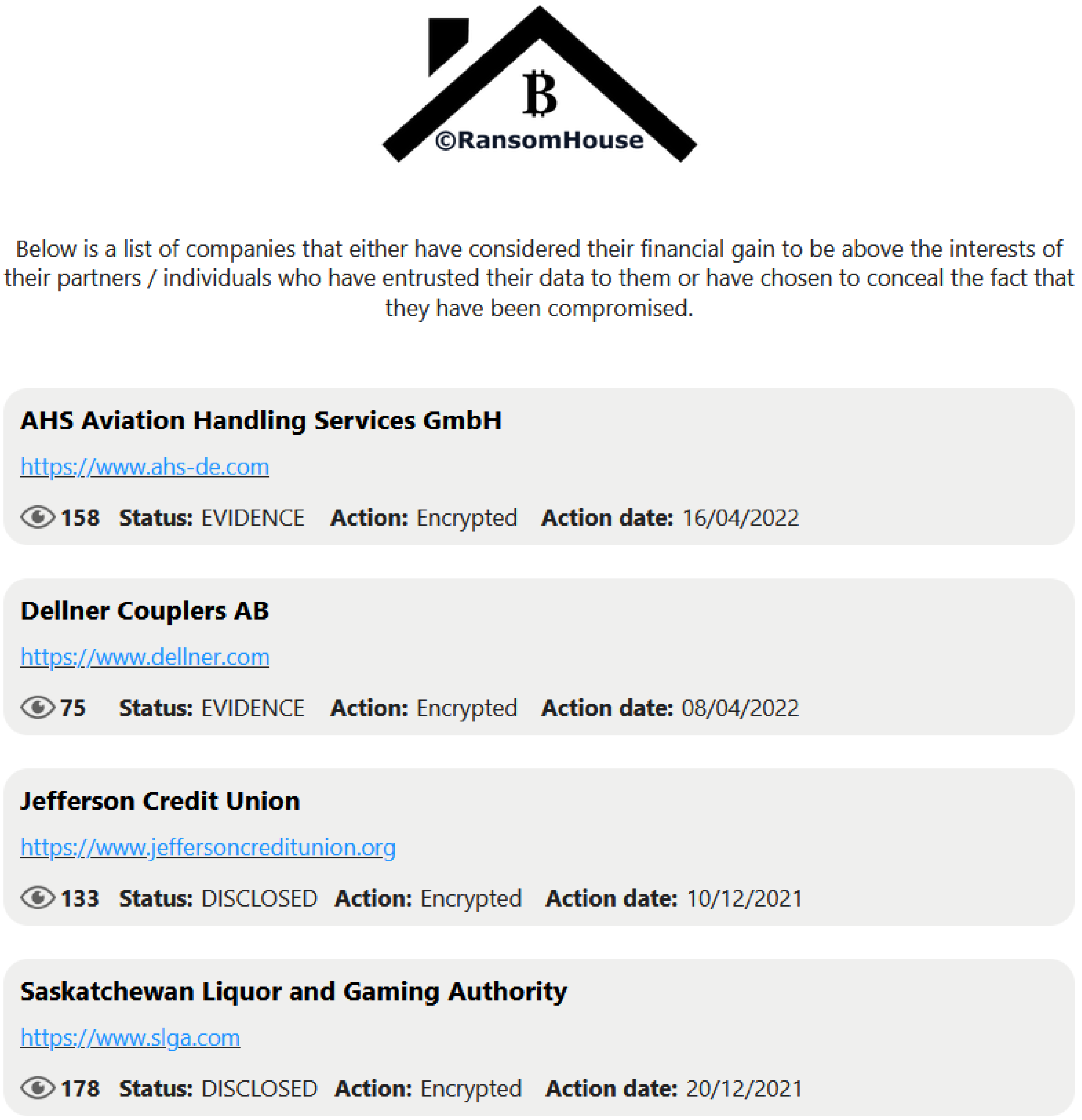
The first quarter of 2022 has seen a lot of cyberattacks, with RaaS (Ransomware as a Service) being the most common form of cyberattacks these days.

The deep and dark web continues to be a favorite space for new ransomware gangs, whether they are brand new groups with new infrastructure or re-brand of an existing group. Whether they are old or new, most ransomware groups operate very similarly. For example, some of those have already built their own Tor site, where they publish the targeted organizations they've allegedly attacked, including leaking some of the databases they claim to have compromised (assuming that the negotiation for getting a ransom by the victim failed).

But a question that has been recently raised is whether **these are real or fake ransomware gangs?**

One of the new ransomware groups whose credibility has been put in question is **RansomHouse**. So far, the group has published 4 samples of alleged stolen data from 4 companies (see image below) on their site on Tor. These companies are:

- SLGA, a local Canadian liquor and gaming authority
- Jefferson CU, a local U.S. bank
- AHS, a German handling service provider
- Dellner, a Swedish railroad equipment manufacturer



©RansomHouse

Below is a list of companies that either have considered their financial gain to be above the interests of their partners / individuals who have entrusted their data to them or have chosen to conceal the fact that they have been compromised.

AHS Aviation Handling Services GmbH
https://www.ahs-de.com
👁 **158** **Status:** EVIDENCE **Action:** Encrypted **Action date:** 16/04/2022

Dellner Couplers AB
https://www.dellner.com
👁 **75** **Status:** EVIDENCE **Action:** Encrypted **Action date:** 08/04/2022

Jefferson Credit Union
https://www.jeffersoncreditunion.org
👁 **133** **Status:** DISCLOSED **Action:** Encrypted **Action date:** 10/12/2021

Saskatchewan Liquor and Gaming Authority
https://www.slga.com
👁 **178** **Status:** DISCLOSED **Action:** Encrypted **Action date:** 20/12/2021

A

screenshot of the Tor site operated by the RansomHouse gang

Users on Twitter, Telegram, and dark web forums have been debating whether RansomHouse is a real ransomware gang that is responsible for attacking and stealing those databases, or an extortion group that buys leaked databases from a third party and tries to extort the victims by demanding a ransom fee in return for not leaking the data to the public.

How can you verify whether a ransomware group is real or fake?

Step #1: Use Publicly available records and announcements

The very first step should be to check the details that are publicly available. For example, have the companies suffered a ransomware attack?

According to an announcement made by Jefferson Credit Union, they admitted that they were hit by a ransomware attack, in which the company's files were encrypted. According to CBC News, RansomHouse affiliates contacted SLGA, claiming to have encrypted the authority’s system using ransomware.

As for AHS, they were targeted by a cyberattack but whether it was a ransomware attack remains unknown. Deliner has not yet clarified whether they suffered a cyberattack at all.

None of these announcements are damning evidence that the RansomHouse group was behind the attack. They could’ve hired ransomware from a different gang to carry out the attack, or they could not have even been involved in these attacks at all.

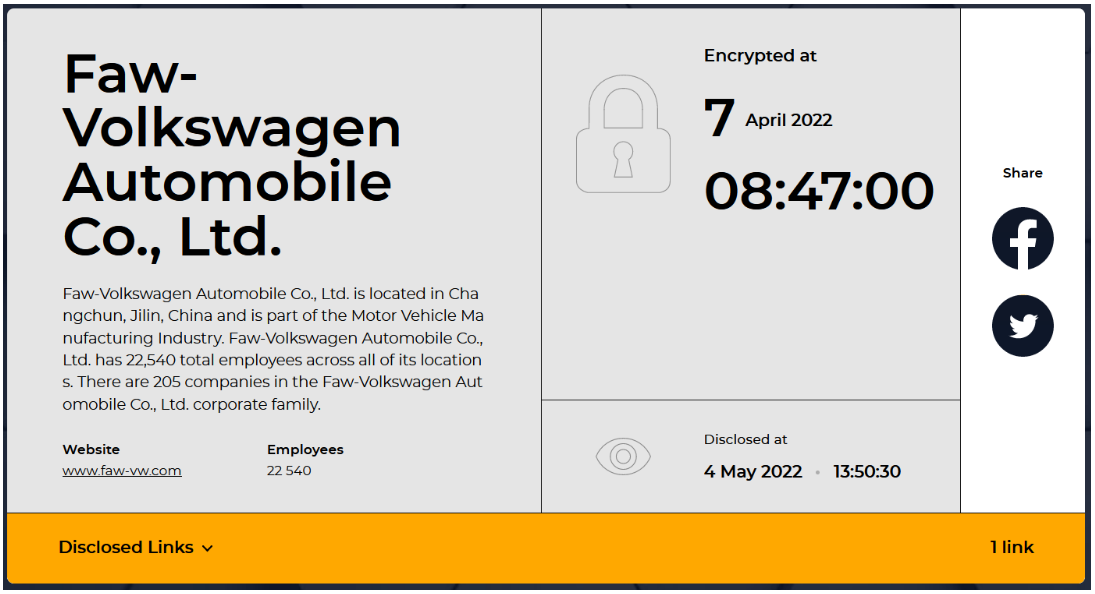
In order to get proof that this ransomware group is a valid, real ransomware group, we need to turn to the spaces where ransomware and other cybercriminal groups operate every day – the deep and dark web. Using Webz.io’s Cyber API, we took a closer look at RansomHouse in an effort to trace their activities and find out whether they are a real ransomware group or not.

Step #2: Use Deep and Dark Web to trace the activities of ransomware groups

There are various places on the deep and dark web where you can start studying ransomware groups more closely. We first started with the obvious option- their site.

The site of the RansomHouse group

We found the official site of the RansomHouse group on the Tor network. Here was the very first unusual finding we traced. If you look at the images below, you can see a strong resemblance between the design and layout of the site used by the RansomHouse group and the one Hive ransomware gang uses. Some would say that it could be an indication that the RansomHouse group is either an extension of Hive or that they work for a group that is also behind the Hive ransomware.



Faw-Volkswagen Automobile Co., Ltd.

Faw-Volkswagen Automobile Co., Ltd. is located in Changchun, Jilin, China and is part of the Motor Vehicle Manufacturing Industry. Faw-Volkswagen Automobile Co., Ltd. has 22,540 total employees across all of its locations. There are 205 companies in the Faw-Volkswagen Automobile Co., Ltd. corporate family.

Website	Employees
www.faw-vw.com	22 540

Encrypted at

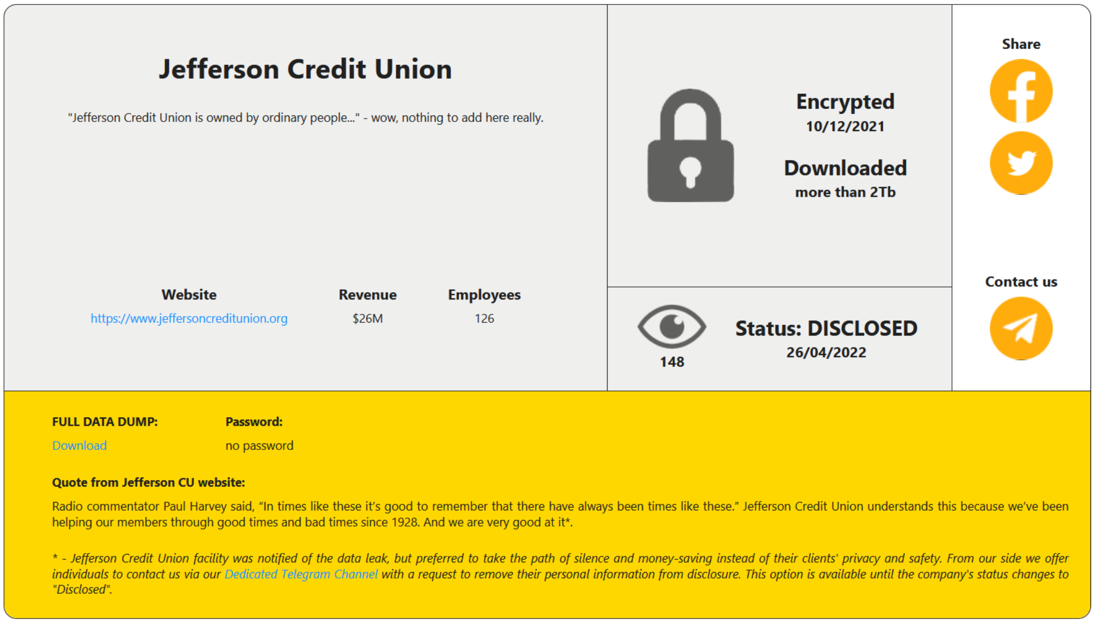
7 April 2022

08:47:00

Disclosed at

4 May 2022 · 13:50:30

A compromised enterprise that is posted on the Hive ransomware site



Jefferson Credit Union

"Jefferson Credit Union is owned by ordinary people..." - wow, nothing to add here really.

Website	Revenue	Employees
https://www.jeffersoncreditunion.org	$26M	126

Encrypted
10/12/2021

Downloaded
more than 2Tb

148

Status: DISCLOSED
26/04/2022

FULL DATA DUMP: Download

Password: no password

Quote from Jefferson CU website:

Radio commentator Paul Harvey said, "In times like these it's good to remember that there have always been times like these." Jefferson Credit Union understands this because we've been helping our members through good times and bad times since 1928. And we are very good at it*.

** - Jefferson Credit Union facility was notified of the data leak, but preferred to take the path of silence and money-saving instead of their clients' privacy and safety. From our side we offer individuals to contact us via our Dedicated Telegram Channel with a request to remove their personal information from disclosure. This option is available until the company's status changes to "Disclosed".*

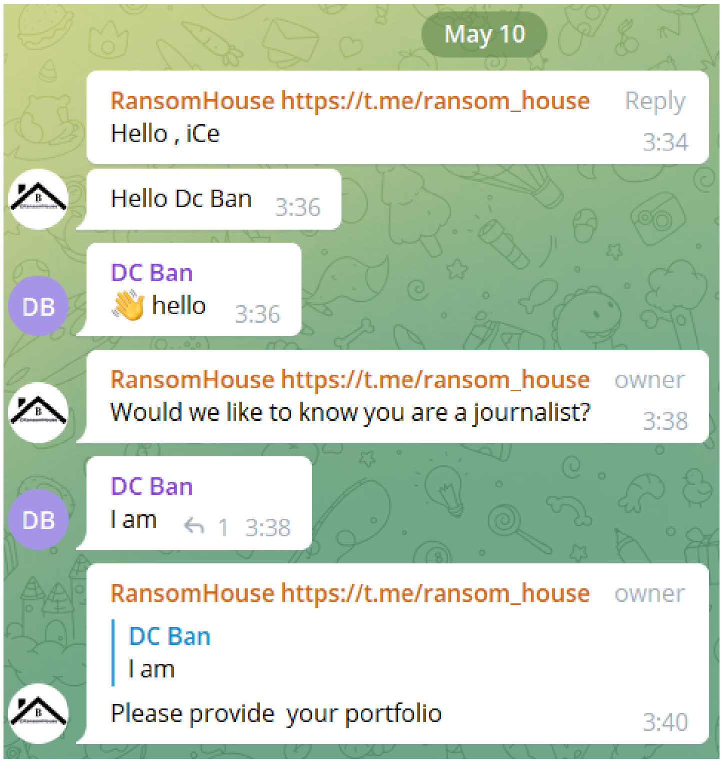
A compromised enterprise that is posted on the RansomHouse ransomware site

RansomHouse on Telegram

Next, we turned to the deep web and took a look at Telegram, where RansomHouse, like many other cybercriminals groups, including ransomware gangs, also operates.

How do they use Telegram?

1. **A private user** – the group is operating a private user on Telegram to allegedly communicate and negotiate with the victims regarding the ransom fee
2. **A Telegram channel** – is used to announce the names of the companies they attacked and threaten to expose their data.
3. **A group – this is a highly unusual group** RansomHouse use for PR relations, where they're communicating with verified journalists and share exclusive information a few hours or even days before the leak is published on the platforms they maintain.



May 10

RansomHouse https://t.me/ransom_house Reply
Hello , iCe 3:34

Hello Dc Ban 3:36

DC Ban
👋 hello 3:36

RansomHouse https://t.me/ransom_house owner
Would we like to know you are a journalist? 3:38

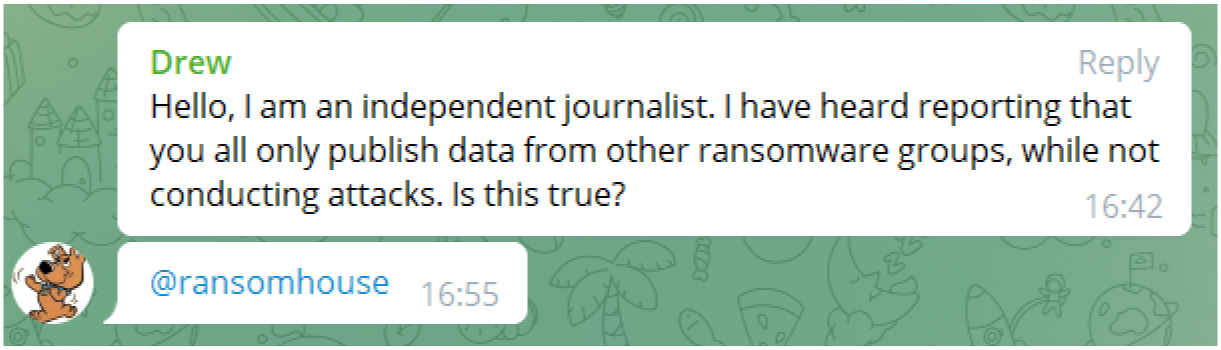
DC Ban
I am ↩ 1 3:38

RansomHouse https://t.me/ransom_house owner
> DC Ban
> I am

Please provide your portfolio 3:40

Messages that were sent in the PR group of RansomHouse, where they are trying to verify the identity of a person who identifies as a journalist.

In the image below, you can see that one of the members on the PR group RansomHouse maintains on Telegram, has recently asked the ransomware group if they are responsible for the cyberattacks they mention on their platforms or if they just publish data from other ransomware groups. So far, RansomHouse hasn't responded.

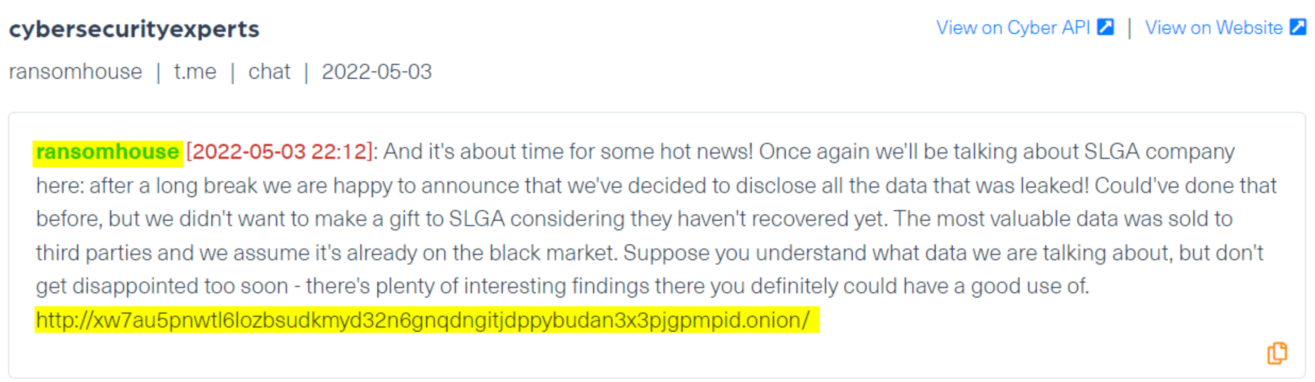


Drew Reply
Hello, I am an independent journalist. I have heard reporting that you all only publish data from other ransomware groups, while not conducting attacks. Is this true? 16:42

@ransomhouse 16:55

The group also uses Telegram for other PR campaigns. For example, they post messages on several cyber groups on Telegram where they announce the names of the latest data leak victims and publicize their Tor sites and Telegram groups.

You can see an example of these types of "PR campaigns" on Telegram in the following image, where RansomHouse gang announces that the leak of SLGA's data is up on the "Cyber Security experts" group on Telegram:



cybersecurityexperts

View on Cyber API | View on Website

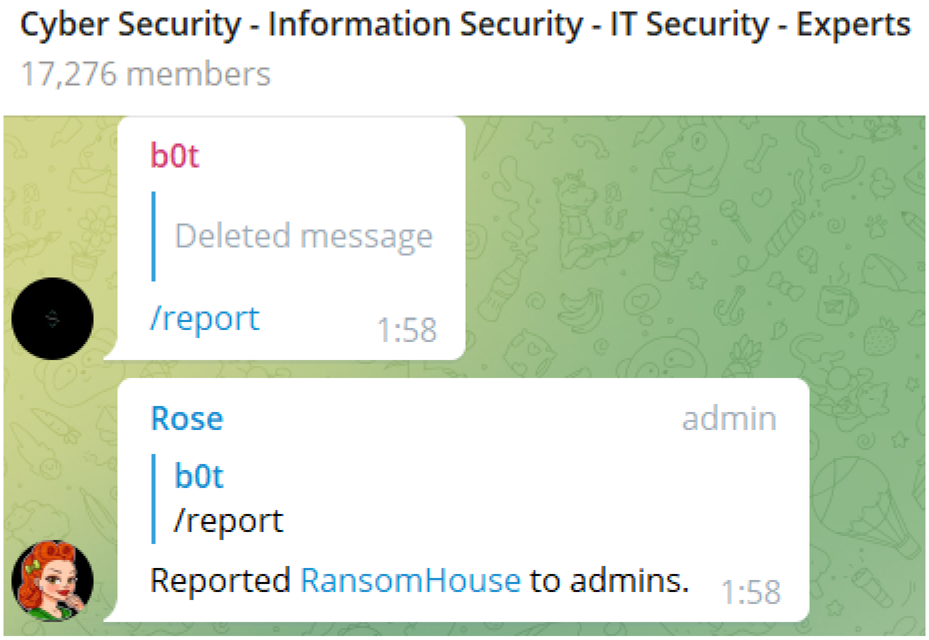
ransomhouse | t.me | chat | 2022-05-03

ransomhouse [2022-05-03 22:12]: And it's about time for some hot news! Once again we'll be talking about SLGA company here: after a long break we are happy to announce that we've decided to disclose all the data that was leaked! Could've done that before, but we didn't want to make a gift to SLGA considering they haven't recovered yet. The most valuable data was sold to third parties and we assume it's already on the black market. Suppose you understand what data we are talking about, but don't get disappointed too soon - there's plenty of interesting findings there you definitely could have a good use of. http://xw7au5pnwtl6lozbsudkmyd32n6gnqdngitjdppybudan3x3pjgpmpid.onion/

The screenshot was taken from our Cyber API UI.

Many of these posts were quietly removed by the admins of the groups, shortly after they were published. Because even on the dark and deep web, threat actors are reported and blocked if they violate the terms of the community.

In the next image you can see how several members reported on Ransomhouse on one of the Telegram groups they posted their “PR messages”:



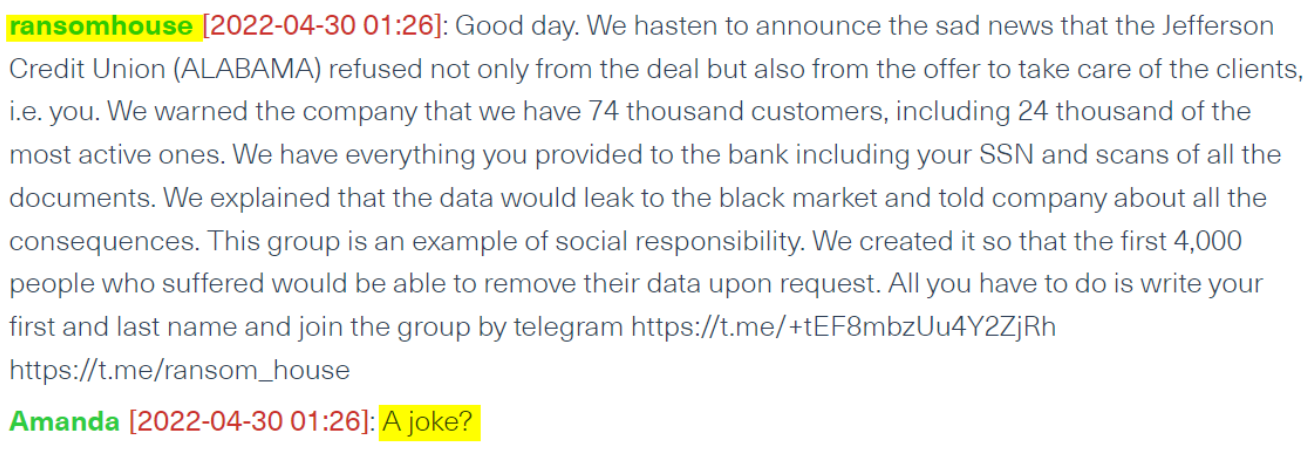
Cyber Security - Information Security - IT Security - Experts
17,276 members

b0t
Deleted message
/report 1:58

Rose admin
b0t
/report
Reported RansomHouse to admins. 1:58

A Telegram group, where RansomHouse was reported to the admins and blocked after publishing their messages there.

It is important to note that RansomHouse have never explicitly claimed that they were the group who hacked the victims, which puts in question their status as a “ransomware group”.



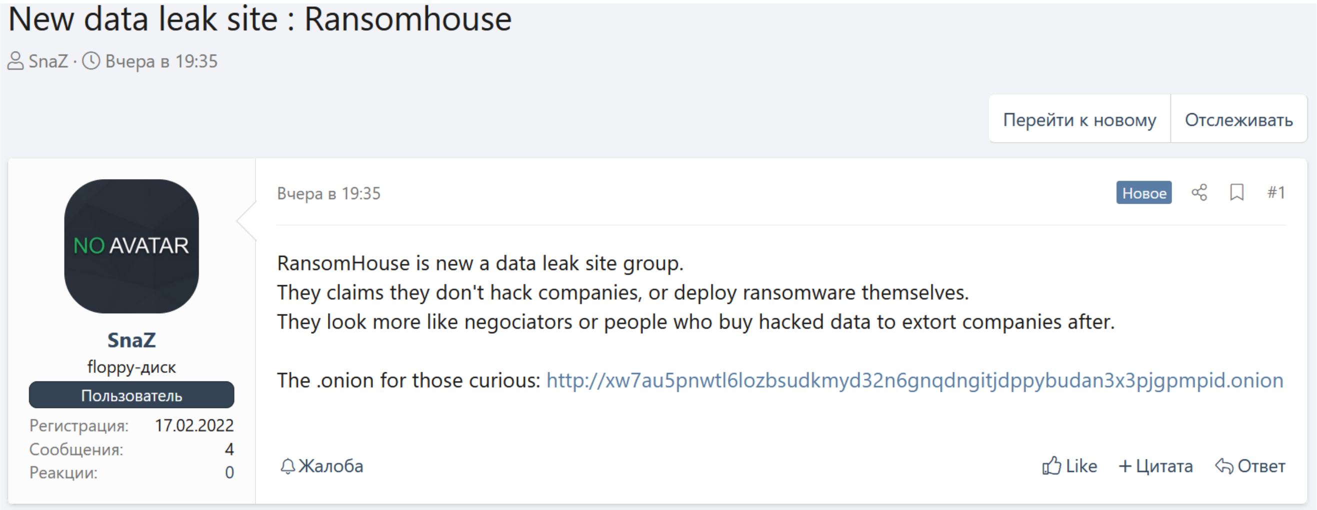
ransomhouse [2022-04-30 01:26]: Good day. We hasten to announce the sad news that the Jefferson Credit Union (ALABAMA) refused not only from the deal but also from the offer to take care of the clients, i.e. you. We warned the company that we have 74 thousand customers, including 24 thousand of the most active ones. We have everything you provided to the bank including your SSN and scans of all the documents. We explained that the data would leak to the black market and told company about all the consequences. This group is an example of social responsibility. We created it so that the first 4,000 people who suffered would be able to remove their data upon request. All you have to do is write your first and last name and join the group by telegram https://t.me/+tEF8mbzUu4Y2ZjRh https://t.me/ransom_house

Amanda [2022-04-30 01:26]: A joke?

The screenshot was taken from our Cyber API UI.

Because of their avoidance of the topic and the lack of clear proof that they are hacking unknowing victims, the debate continues to roll on the deep and dark web.

For example, a user of a popular hacking forum, XSS.IS, called Snaz claims that RansomHouse is only a data leak site, which is pretty common these days:



New data leak site : Ransomhouse

SnaZ · Вчера в 19:35

RansomHouse is new a data leak site group.
They claims they don't hack companies, or deploy ransomware themselves.
They look more like negociators or people who buy hacked data to extort companies after.

The .onion for those curious: http://xw7au5pnwtl6lozbsudkmyd32n6gnqdngitjdppybudan3x3pjgpmpid.onion

Whether RansomHouse is responsible for the attacks or not, it's very important to closely monitor their activities and the activity of other cybercriminal groups. A broad coverage of the deep and dark web helps conduct deep actor profiling and gain relevant context to prevent emerging cyber threats.

hacking forumsRansomware Groups

Hagar Margolin

Cyber Analyst