Introduction

As new ransomware groups emerge by the day, most of them operate the same business model and same techniques.

And as we all know, one of the main techniques of ransomware groups is to encrypt valuable assets belonging to the victim.

Over the past weeks, a new and slightly odd ransomware group has emerged named RansomHouse. At glance, it looks like any other ransomware group, but claims to be something other than what we are used to seeing.

The group first emerged at the end of March and has already amassed four victims on their Onion site (Figure 1).

Figure 1: RansomHouse homepage

A New Type of Agenda

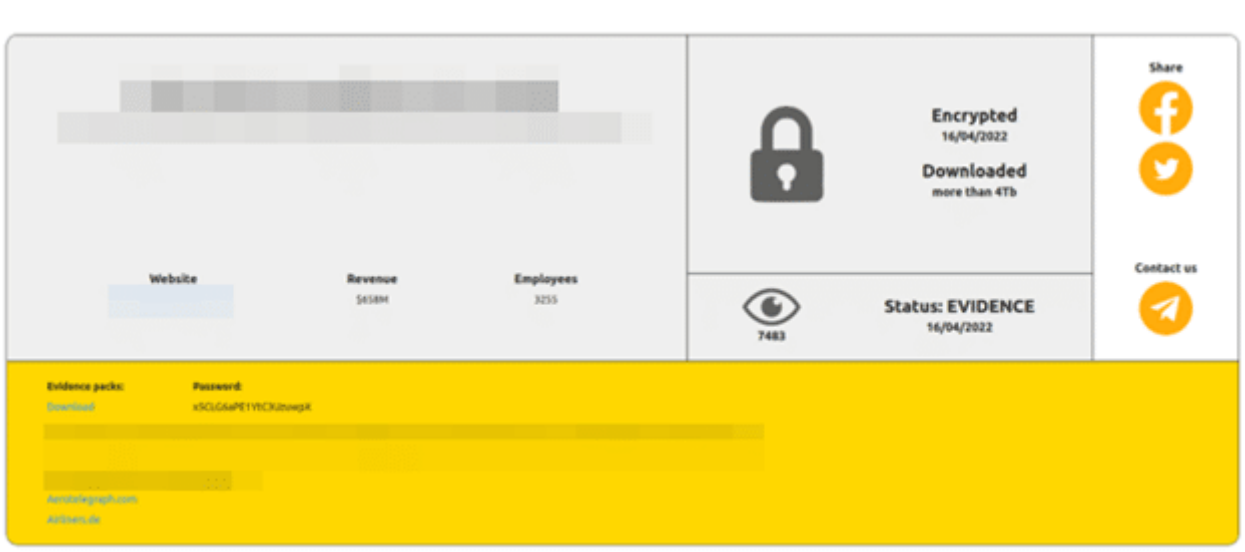
One of Cyberint's predictions about the ransomware landscape in 2022 is that ransomware groups will develop and make efforts, when possible, to request payment for stolen data only, and eliminate the encryption phase in their campaigns.

RansomHouse is one of the groups that has adopted this type of technique, as they are claiming that they do not use any encryption in their campaigns.

What is interesting about this unique group is the purpose they claim to have for their actions. When we look at the detailed "About" section on the group's Onion site, we are introduced to a new ransomware group profile, or business module, if you will.

One of the main characteristics of the group is that they claim to fulfil a higher purpose with their campaigns, labeling the organizations they compromise as the real villains who are not willing to protect themselves and their customers properly.

According to RansomHouse, many businesses and companies are not willing to invest as much money as required to fortify their infrastructures, while they ignore or do not institute enough bug bounty plans. Bug bounty are programs that encourage individuals to search for bugs and vulnerabilities in the organization's infrastructure and report them, and in return, the individual is rewarded with a payment. The group claims that these organizations put their assets and, most importantly, their customers' information at risk.



Published compromised victim data

Figure 2: Published compromised victim data

RansomHouse to the Rescue

Because they have established the fact that organizations not protecting themselves with state-of-the-art technologies are the bad guys in our story, RansomHouse introduces themselves as the public messengers and target any organization that is not protecting itself properly or does not reward and respect bug bounty programs.

Throughout their entire introduction process, RansomHouse sees themselves as the ones who do what's right and makes excuses such as "the organizations are the ones to lead us to these actions" as they are avoiding taking any responsibility.

RansomHouse is practically forcing "penetration testing services" on organizations that never used their services or rewarded bug bounties, and once they find any vulnerabilities, they fully exploit them to steal as much sensitive data as possible.

Ironically, RansomHouse announced on their Onion site that they are pro-freedom and support the free market, but on the other hand, they punish organizations that choose to not invest in their protection systems.

Techniques

RansomHouse campaigns focus on data exfiltration only; they do not possess or develop any encryption modules. In their words: "nothing to do with breaches and don't produce or use any ransomware".

It seems that the group operates manually and focuses on one victim at a time. They keep their actions simple and precise as they invest all their resources in vulnerability research and data exfiltration, which makes their task much simpler than encrypting the victim's assets.

The position the group generally puts the victim in is to pay the ransom or being shamed in their blog for not "caring enough" to pay the ransom to protect its customers' valuable information, which could cast a negative light on the victim in front of its customers and shareholders.

Communication Channels

RansomHouse has two basic and popular communication channels: Telegram and Onion.

Currently, they operate three Telegram channels. The first is the group's announcements about new victims, but mostly, the reaction of the victims, and which organization played the part of the caring and responsible organization, and which didn't in the negotiation process.

The second Telegram channel is a chat in which followers can communicate with the group's admins and talk to each other, although it doesn't seem to have much traffic.

RansomHouse truly respects journalists and promotes themselves as a great partner to work with as they have opened a new Telegram channel dedicated to journalists only (Figure 3).

RansomHouse opens a Telegram channel for journalists

Figure 3: RansomHouse opens a Telegram channel for journalists

The second communication channel is the group's Onion page, which is where the group announces its current victim list along with some sections explaining the group's intentions, etc.

As the group gains a reputation, mainly via Telegram, we can already see other potential threat actors reaching out to the group to join the cause (Figure 4).

Potential threat actor looks to help the team and offers partnership

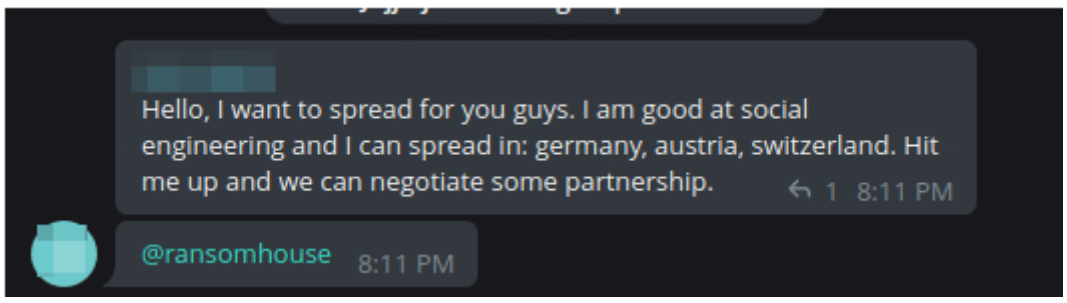
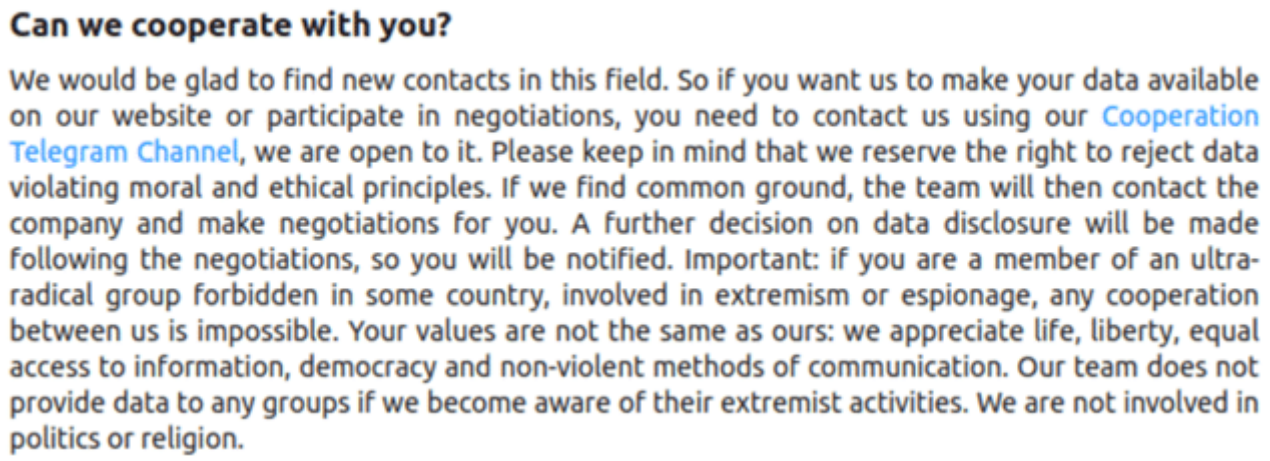


Figure 4: Potential threat actor looks to help the team and offers partnership

Reaching out to the group is not unusual given the fact that they are looking to expand and grow their operation as they recruit new members (Figure 5).



RansomHouse recruiting announcement

Figure 5: RansomHouse recruiting announcement

Some Respect Among Thieves?

As the new group tries to compromise as many organizations as possible, they also try to draw a picture, to both for victims and the general community, that they are an honest group that, once paid, will help the organization protect itself from future attacks and will provide a full report on how and what vulnerabilities were exploited in the process. They also promise to delete any information they stole, along with any evidence of the compromised organization even being on their victims list. Lastly, RansomHouse claims that they will also delete any backdoors they currently have on the victim's network (Figure 6).

RansomHouse commitments list after a successful negotiation

3. Post-transaction guarantees

3.1. All uploaded information will be removed from the team's servers;
3.2. All posts/websites/pages etc. posted by the team and associated with the data leak will be removed;
3.3. All backdoors exploited by the team will be removed;
3.4. Personal data will not be shared with third parties by the team;
3.5. A list of information security recommendations will be provided to the head of the company;
3.6. Decryption software, guidance and support will be provided if required;
3.7. Current vulnerabilities will never be used by the team for further attacks. In case new vulnerabilities will be discovered, the company will be notified.

Figure 6: RansomHouse commitments list after a successful negotiation

Overall, RansomHouse tries to introduce itself as a group that is trying to create a better future for the cybersecurity world as they force their "bug bounty" programs on organizations.

Team Members

Examining the methods and goals of the team, along with the way they operate and communicate, it seems that the group might have a blue and red team background and might even be disgruntled bug bounty hunters looking to be taken more seriously by organizations.

This profile of bug bounty hunters going rogue is very likely given the fact that many of the bug bounty hunter community members have been complaining for some time now about companies that do not want to pay the bounty for their hard labor while still enjoying its fruits, and also about bug bounty programs that increase their commissions making the bug bounty hunter a very frustrating profession.

It seems that the group is focused on their goal. They speak politely on both their blog and various Telegram channels, and do not get swept into irrelevant discussions. Furthermore, they claim to be very liberal and pro-freedom. They do not want to mix business and politics and announced that they will never work with radical hacktivists or espionage groups. Although the group's obvious drive is personal gain, they try to make it as painless as possible for their victims and conduct themselves in a straightforward manner.

Lapsus$ Connection?

An interesting finding that we found in Argos Edge™ was the relationship the group had with the Lapsus$ Telegram chat group. One of the difficulties of a new group is, of course, publicity. It seems that the group took the initiative to promote themselves in the Lapsus$ gang's dying Telegram channel (Figure 7), talking about their exploits and publishing their blog.

At some point, it seems that the channel's admins did not approve of these actions and muted the RansomHouse account.

RansomHouse announcement of a new victim in Lapsus$ Telegram channel found in Argos Edge™

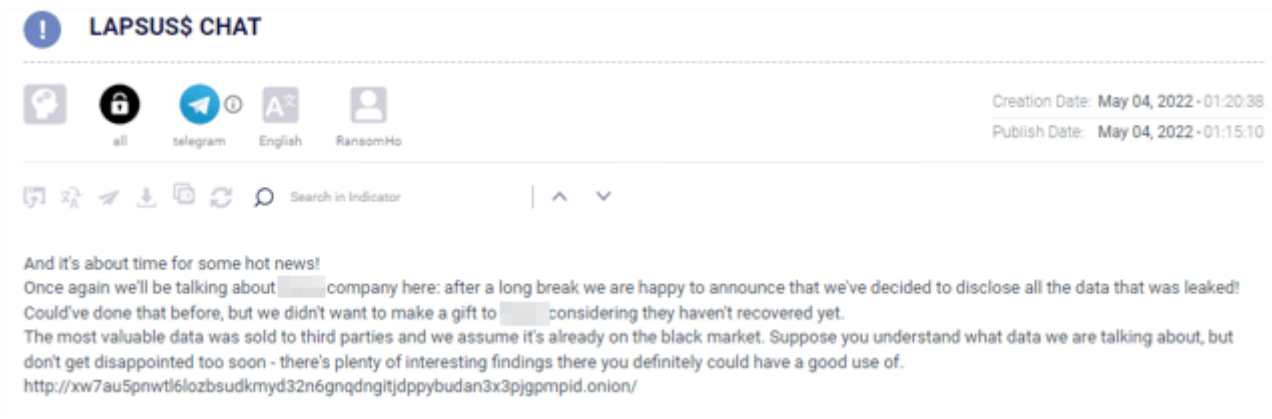


Figure 7: RansomHouse announcement of a new victim in Lapsus$ Telegram channel found in Argos Edge™

Summary

In recent months, especially after the Russia-Ukraine conflict began, we have seen new threat groups swarming into our lives with different agendas as Twitter and Telegram continue to give them a voice and act as their mouthpiece.

RansomHouse is another new creature emerging within this reality. A group of talented red and blue teamers that has two faces — the pro-freedom, liberal and anti-radicalism, and the face of a group that is terrorizing organizations and forcing them to pay or be shamed.

Their sense of mission aligns with the rise of many wolves in sheep's clothing threat actors who look to gain approval for their actions from society as they try to put their victims in a bad light.

Finally, the group is putting its best efforts into growing and becoming a dominant player in the cybercrime industry, but for the moment, they are still at an early age. However, unlike other groups that have emerged lately with a “higher purpose” such as BlueHornet, clearly, personal gain is their main motive.