ANALYST1

# RANSOMHOUSE:

## STOLEN DATA MARKET, INFLUENCE OPERATIONS & OTHER TRICKS UP THE SLEEVE

By Anastasia Sentsova

# Contents

# Executive Summary

- This research aims to identify connections between RansomHouse, and other groups based on the investigation of multiple crossclaims of victims. Emerging after the Babuk source code leak in late 2021, RansomHouse has been linked to multiple groups, including **White Rabbit, Mario ESXi, RagnarLocker,** and **Dark Angels (Dunghill Leak)**.

- Investigation of the RansomHouse data leak site (DLS) also revealed multiple crossclaims with other groups, indicating potential cooperation. According to the analysis of RansomHouse's dataset (**May 9, 2022**, to **February 28, 2024**) of entities posted on its DLS, **11** out of **73** claimed victims were crossclaimed by other groups.

- Further investigation revealed potential associations of RansomHouse with **Alphv/BlackCat, LockBit 3.0, BianLian,** and **RagnarLocker**. Through our findings and corroborated by open-source reporting from other researchers, including the identification of shared emails and a consistent timeline of crossclaims, there is evidence suggesting potential collaboration among these syndicates.

- **Snatch** and **Stormous**, singled out in a separate case, were identified as closely cooperating with RansomHouse and/or Dark Angels, engaging in hybrid ransomware/hacktivist activities that blend ransomware with influence operations under the guise of hacktivism. While Dark Angels and RansomHouse primarily function as ransomware groups, Snatch and Stormous align themselves with hacktivists. Observed causes include pro-Palestine and pro-Russia sentiments, with a focus on attacking US and European entities, also involving associated individuals, particularly government officials.

- The analysis of the geopolitical alignment indicates that RansomHouse, Snatch, and Stormous are likely aligned with Russia. This is based on the observed infrastructure analysis revealing connections originating from servers based in Russia and other artifacts. Additionally, an analysis of major pro-Russian media channels reveals strong support for these groups, reinforcing their narratives in a way that aligns with and supports the broader agenda of the Russian state.

- Data sharing among ransomware groups introduces new challenges. Previously stolen data is reused in extortion attempts, creating false impressions of new attacks. The integration of hacktivist-like activities by groups like Snatch and Stormous also underscores the need for enhanced security measures to protect sensitive data and mitigate reputational damage at governmental and individual levels.

# Introduction

One of the main aspects of ransomware operations, often determining the success of their extortion efforts, is the utilization of data leak sites. These platforms are crucial in supporting double-extortion tactics, where actors not only encrypt the victim's data but also threaten to publicly release it unless a ransom is paid.

Recent observations within the realm of Russian-speaking ransomware highlight a notable trend: multiple groups claiming to have breached the same victim. While it is theoretically possible for multiple syndicates to simultaneously target the same victim, the frequency of such cross-claims suggests a higher likelihood of collaboration in data sharing among the actors involved.

The rise of Russian-speaking ransomware has indeed been significant, with its impact extending across former Soviet Union countries where the language is historically spoken. In this report, however, our focus is primarily on groups with geopolitical alignment with Russia. Therefore, to maintain clarity and specificity, we will refer to subjects of our analysis as Russian groups or actors.

In this research, we mainly focused on the RansomHouse group, which drew our attention due to the high number of crossclaims with various other groups compared with the total number of entities posted on their DLS. To uncover RansomHouse's operations, we delved into the group's history, tracing its emergence back to May 2021 when the Babuk source code was leaked, giving rise to multiple other syndicates, including RansomHouse.

Through analyzing the patterns and dynamics surrounding these crossclaims between RansomHouse and other groups, we aimed to delve into the extent of collaboration within the Russian ransomware ecosystem. Our analysis suggests significant data-sharing collaborations among multiple groups, with RansomHouse prominently involved. These collaborative efforts also implicate groups like Snatch and Stormous, which engage in hybrid operations blending traditional ransomware activities with what we name as hacktivist-like activities, masking influence operations under this guise.

Identifying data-sharing collaborations among ransomware groups is a significant finding that has important implications for incident response actions. It also underscores the interconnected nature of the Russian ransomware landscape and enhances our understanding of its ecosystem.  By recognizing the potential for collaboration, organizations can implement more robust defense measures to mitigate the impact of such attacks and extortion attempts.

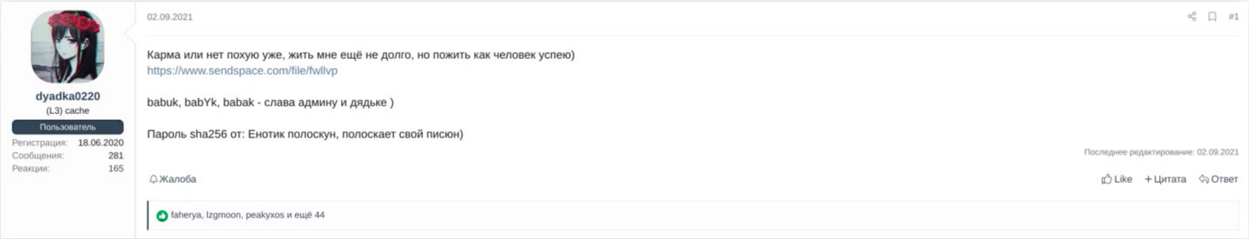
# Babuk Code Leak & Emergence of RansomHouse

The attribution of RansomHouse and its emergence history, has sparked considerable debate and speculation within the cybersecurity community. Indeed, in an environment where ransomware groups frequently undergo rebranding, attributing attacks to specific groups can be challenging.

The group's emergence began with the leak of Babuk source code. On **September 2, 2021**, a prominent member of the Russian-speaking DarkWeb forum XSS operating under the moniker **dyadka0220**, published the code. Babuk, also referred to as Babyk was first observed approximately at the beginning of 2021. Throughout their operations, Babuk actors targeted numerous high-profile victims, getting away with millions of dollars of ransom payments.

The leak became a Pandora's box, spawning several new groups, including **RansomHouse**, and being adopted by existing groups at that time such as **Conti** and **Alphv/BlackCat**. The Babuk Locker "builder" became attractive to hackers due to its functionality in targeting ESXi servers, which are widely popular among large corporations and businesses. According to the Cybersecurity and Infrastructure Security Agency (CISA) advisory published on February 8, 2023, 3,800 VMware ESXi servers have been compromised globally.

The backstory behind the leak is also intriguing and provides valuable insights into the Russian ransomware underground. The incident followed an internal dispute between dyadka0220 and boriselcin (aka wazawaka), key members of Babuk. Boriselcin was later identified as Mikhail Matveev and sanctioned by the DOJ, with actions announced on May 13, 2023. Among approximately 65 identified victims, the Metropolitan Police Department in Washington D.C. was one of them, targeted on April 26, 2021.



dyadka0220
(L3) cache
Пользователь
Регистрация: 18.06.2020
Сообщения: 281
Реакции: 165

02.09.2021 #1

Карма или нет похую уже, жить мне ещё не долго, но пожить как человек успею)
https://www.sendspace.com/file/fwllvp

babuk, babYk, babak - слава админу и дядьке )

Пароль sha256 от: Енотик полоскун, полоскает свой писюн)

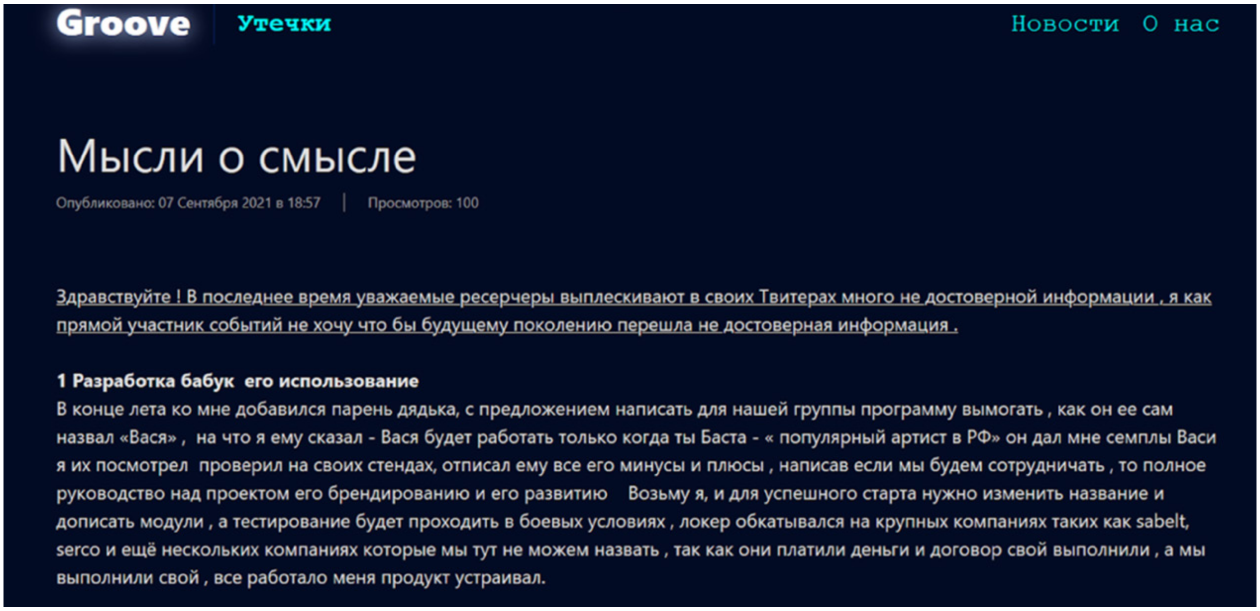
Последнее редактирование: 02.09.2021

faherya, lzgmoon, peakyxos и ещё 44

*Figure 1: dyadka0220 leaks Babuk source code in a message posted on September 2, 2021*
*Source: XSS forum*

Metropolitan Police became the subject of a dispute between actors, likely occurring sometime in May of 2021 when the Babuk shutdown was announced, eventually leading to a split. On **July 11, 2021**, Matveev launched a ransomware forum **RAMP**, first operating under the moniker **TetyaSluha**, which was soon changed to **Orange**. Soon after, on **August 22, 2021**, a new ransomware group named **Groove** was announced on RAMP, describing itself as ***"an aggressive financially motivated criminal organization dealing in industrial espionage."***

Four days after the Babuk source code leak, on **September 7, 2021**, Matveev posted a blog on his Groove data leak site explaining the situation surrounding the group. According to the blog, Matveev claimed that the negotiation failed due to the lack of pressure on the victim and ***"unprofessionalism"*** by their affiliate. The actor then decided to end the business relationship with their former colleagues. It was agreed that Matveev would retain Babuk's DLS domain, where the first RAMP forum was built (eventually, Matveev rebuilt RAMP on a different domain), while their affiliate would keep the source code.



Мысли о смысле

Опубликовано: 07 Сентября 2021 в 18:57 | Просмотров: 100

Здравствуйте ! В последнее время уважаемые ресерчеры выплескивают в своих Твитерах много не достоверной информации , я как прямой участник событий не хочу что бы будущему поколению перешла не достоверная информация .

**1 Разработка бабук его использование**

В конце лета ко мне добавился парень дядька, с предложением написать для нашей группы программу вымогать , как он ее сам назвал «Вася» , на что я ему сказал - Вася будет работать только когда ты Баста - « популярный артист в РФ» он дал мне семплы Васи я их посмотрел проверил на своих стендах, отписал ему все его минусы и плюсы , написав если мы будем сотрудничать , то полное руководство над проектом его брендированию и его развитию Возьму я, и для успешного старта нужно изменить название и дописать модули , а тестирование будет проходить в боевых условиях , локер обкатывался на крупных компаниях таких как sabelt, serco и ещё нескольких компаниях которые мы тут не можем назвать , так как они платили деньги и договор свой выполнили , а мы выполнили свой , все работало меня продукт устраивал.

*Figure 2: Matveev posted a message explaining its split with Babuk*
*Source: Groove data leak site*

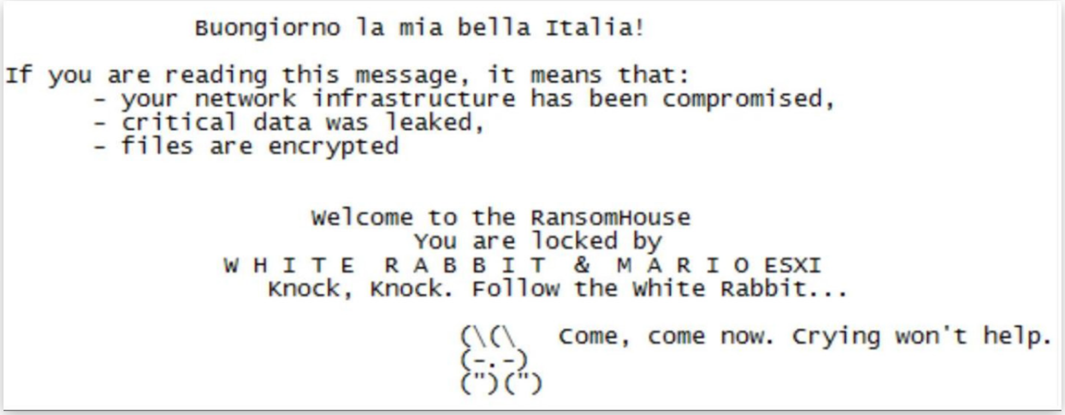
These events provide a compelling example of the interconnected nature of the Russian ransomware ecosystem. They also serve as a reminder that the investigation of ransomware involves much more than just the technical aspects, as its landscape is often shaped by various internal and external factors. With constant rebranding and the launching of new groups, the underlying reason in some cases may indeed be as simple as actors being unable to get along with each other.

It is important to highlight that this behavior and interconnectedness between groups are particularly prevalent among Russian actors. This may also explain why Russian ransomware continues to flourish, as well as the success of the Ransomware-as-a-Service (RaaS) business model, wherein an affiliate responsible for a breach can collaborate with numerous other groups. Driven by financial motivation and bolstered by the foundation of established personal relationships – essential in Russian society – the ransomware ecosystem thrives. Mikhail Matveev, for example, was identified as participating across at least three variants: LockBit, Babuk, and Hive.

Such cultural characteristics that foster strong support for close collaboration might also contribute to and explain instances of crossclaims of victims we observed, which is the main focus of our research. But first, let's take a closer look at the operations of RansomHouse.

## RansomHouse: The Beginning – The SLGA Case

With its emergence approximately in late 2021, RansomHouse promoted itself as a Ransomware-as-a-Service (RaaS). Since the beginning of RansomHouse operations, it has been alternatively referred to as **White Rabbit** and **Mario ESXi**, creating confusion and adding layers of intrigue to their identity. The explanation, however, is simple: both Mario ESXi and White Rabbit strains are used by actors in their attacks. In ransom notes shared with the victims, the actors refer to themselves as Mario ESXi or White Rabbit and, in some cases, by all three names.

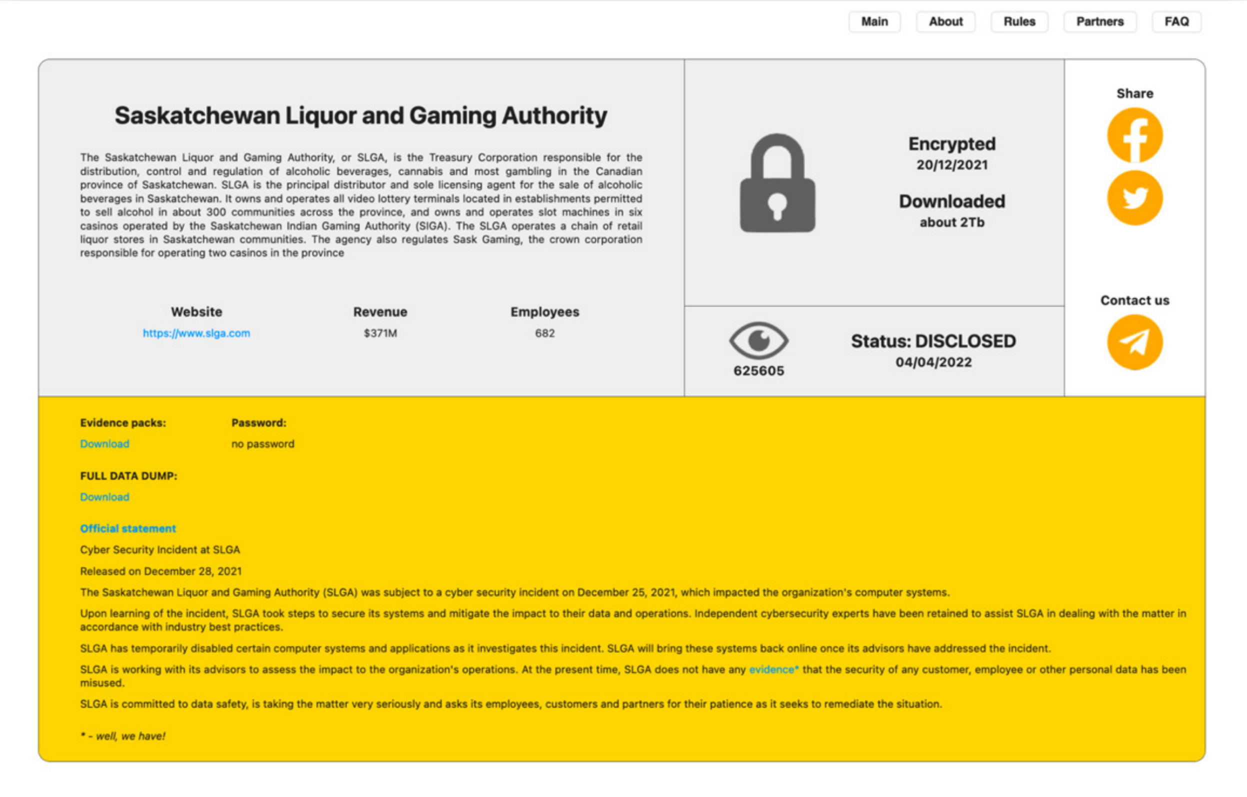


```
             Buongiorno la mia bella Italia!

If you are reading this message, it means that:
      - your network infrastructure has been compromised,
      - critical data was leaked,
      - files are encrypted


                     Welcome to the RansomHouse
                            You are locked by
               W H I T E  R A B B I T  &  M A R I O ESXI
                  Knock, Knock. Follow the White Rabbit...

                                (\(\    Come, come now. Crying won't help.
                                (-.-)
                                (")(")
```

*Figure 3: Ransom note that was shared with the Italian entity that was attacked by RansomHouse in August 2022. Source: Analyst1*

Their first victim is believed to be the Saskatchewan Liquor and Gaming Authority (SLGA) which reported a ransomware attack on **December 25, 2021**. SLGA was also the first victim publicly claimed by RansomHouse, which was published on their data leak site on **April 4, 2022**. The SLGA, a Treasury Board, is responsible for overseeing the distribution, control, and regulation of alcoholic beverages, cannabis, and most gambling in the Canadian province of Saskatchewan. According to the SLGA investigation report released on **November 10, 2022**, the attackers exploited a critical vulnerability in the CMS platform software.

Forensic analysis revealed that the actors initially breached SLGA's IT environment in November 2021. However, SLGA only became aware of the attack on December 25, 2021, when they received a ransom demand. As a result of this attack, ***"approximately 40,000 individuals were affected by this privacy breach, including current and past employees, dependents of the employees, and regulatory clients."***



Saskatchewan Liquor and Gaming Authority

The Saskatchewan Liquor and Gaming Authority, or SLGA, is the Treasury Corporation responsible for the distribution, control and regulation of alcoholic beverages, cannabis and most gambling in the Canadian province of Saskatchewan. SLGA is the principal distributor and sole licensing agent for the sale of alcoholic beverages in Saskatchewan. It owns and operates all video lottery terminals located in establishments permitted to sell alcohol in about 300 communities across the province, and owns and operates slot machines in six casinos operated by the Saskatchewan Indian Gaming Authority (SIGA). The SLGA operates a chain of retail liquor stores in Saskatchewan communities. The agency also regulates Sask Gaming, the crown corporation responsible for operating two casinos in the province

| Website | Revenue | Employees |
|---|---|---|
| https://www.slga.com | $371M | 682 |

Encrypted
20/12/2021

Downloaded
about 2Tb

625605

Status: DISCLOSED
04/04/2022

Evidence packs: Download

Password: no password

FULL DATA DUMP: Download

Official statement

Cyber Security Incident at SLGA

Released on December 28, 2021

The Saskatchewan Liquor and Gaming Authority (SLGA) was subject to a cyber security incident on December 25, 2021, which impacted the organization's computer systems.

Upon learning of the incident, SLGA took steps to secure its systems and mitigate the impact to their data and operations. Independent cybersecurity experts have been retained to assist SLGA in dealing with the matter in accordance with industry best practices.

SLGA has temporarily disabled certain computer systems and applications as it investigates this incident. SLGA will bring these systems back online once its advisors have addressed the incident.

SLGA is working with its advisors to assess the impact to the organization's operations. At the present time, SLGA does not have any evidence* that the security of any customer, employee or other personal data has been misused.

SLGA is committed to data safety, is taking the matter very seriously and asks its employees, customers and partners for their patience as it seeks to remediate the situation.

** - well, we have!*

*Figure 4: RansomHouse data leak site displays SLGA being claimed as a victim*
*Source: RansomHouse DLS*

The gap between December 25, 2021, when the actors initially contacted SLGA, and April 4, 2022, when they posted the company on their leak site, was a period during which they engaged in extortion. To bolster their double-extortion efforts, the actors utilized various methods, including a data leak site and reaching out to the media when negotiations stalled.

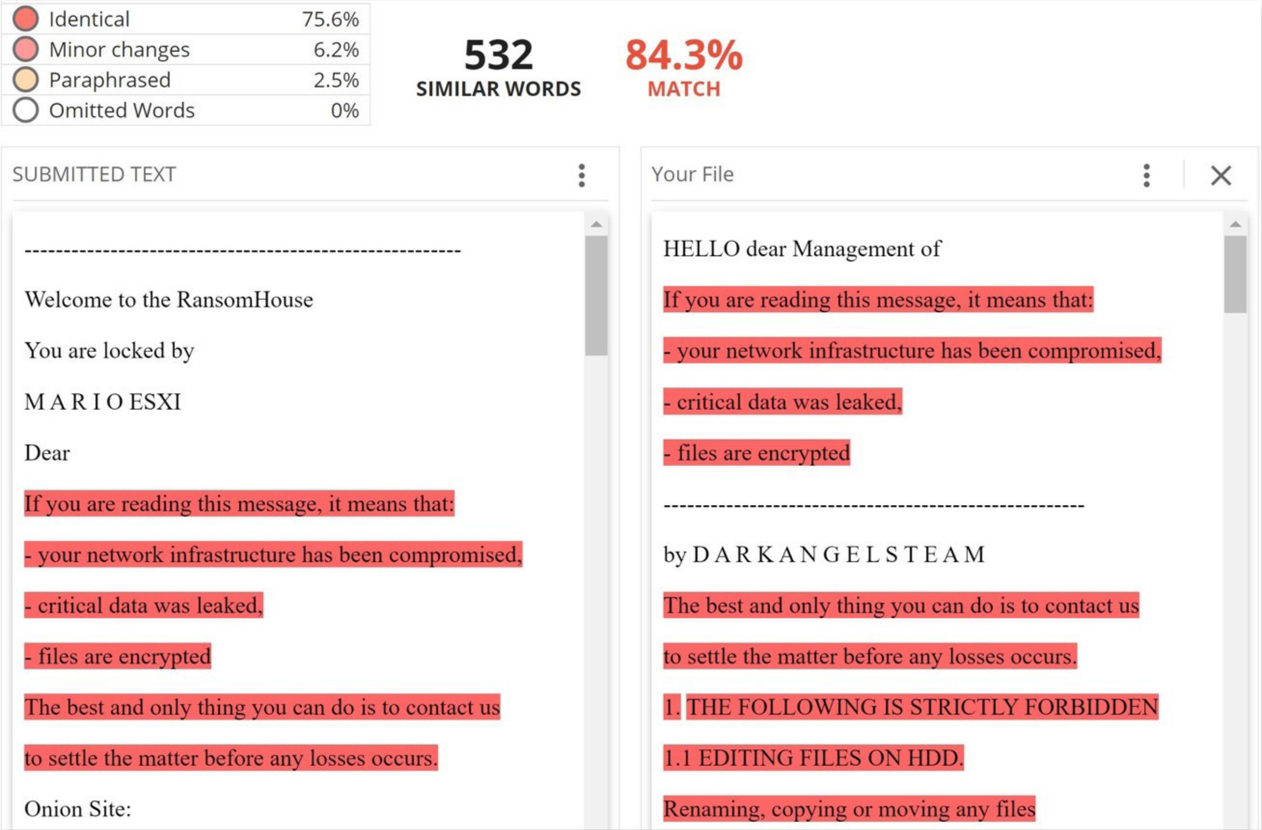
At some point during these three months of negotiations, the actors contacted CBC to disclose the breach and seek media visibility. ***"We tried to reach the company to provide them this information and to start negotiations. They said they don't care about the problem,"*** claimed the individual, identifying themselves as **Jason Walmart** to a reporter. They shared a data sample purportedly stolen from SLGA, including bank records, budgets, contracts, employee data, and supplier agreements Negotiations seemingly made no progress. Eventually, RansomHouse published claimed stolen data on its leak site.

The narrative of victim blaming is clearly observed throughout RansomHouse's operations. We will delve deeper into analyzing these tactics used by the group later. Let's proceed to the next section, examining RansomHouse's association with other groups. The wide and calculated actions taken by the actors during its very first case — SLGA and other following attacks clearly indicated that they had established a team that was well-experienced and had been operating for a significant period. The question arises: to which groups exactly RansomHouse associated, and to what extent?

The narrative of victim blaming is clearly observed throughout **RansomHouse's** operations

## RansomHouse & Other Groups: RagnarLocker, Dark Angels, Dunghill and More

Researchers have drawn connections between RansomHouse and other prominent groups, with one of them being **Dark Angels** first seen approximately in **May 2022**. On **March 7, 2023,** Will Thomas, a threat intelligence researcher at Equinix, observed similarities between the ransom notes of both RansomHouse's Mario ESXi and Dark Angels. According to the analysis, similarities in wording were identified, accounting for approximately 84.3%.



| | | |
|---|---|---|
| ● | Identical | 75.6% |
| ● | Minor changes | 6.2% |
| ● | Paraphrased | 2.5% |
| ○ | Omitted Words | 0% |

532
SIMILAR WORDS

84.3%
MATCH

SUBMITTED TEXT

---------------------------------------------------------

Welcome to the RansomHouse

You are locked by

MARIO ESXI

Dear

If you are reading this message, it means that:

- your network infrastructure has been compromised,

- critical data was leaked,

- files are encrypted

The best and only thing you can do is to contact us

to settle the matter before any losses occurs.

Onion Site:

Your File

HELLO dear Management of

If you are reading this message, it means that:

- your network infrastructure has been compromised,

- critical data was leaked,

- files are encrypted

-------------------------------------------------------

by DARKANGELSTEAM

The best and only thing you can do is to contact us

to settle the matter before any losses occurs.

1. THE FOLLOWING IS STRICTLY FORBIDDEN

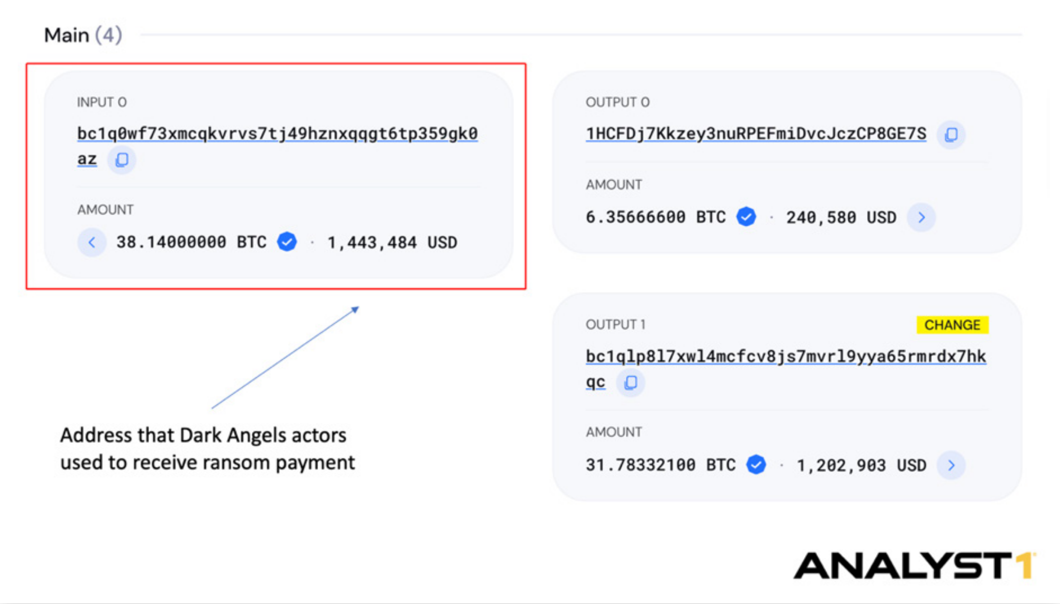
1.1 EDITING FILES ON HDD.

Renaming, copying or moving any files

*Figure 5: Similarities between ransom notes of RansomHouse and Dark Angels indicate matching in wording. Source: Will Thomas' Twitter*

Notably, both RansomHouse and Dark Angels were named one of the most active ransomware groups in 2023 by Chainalysis, a blockchain analytics company. Another valuable finding is the median ransom size versus its frequency of payouts, which shows that Dark Angels' median payment size is close to **USD 1.5 million**, while the frequency of payouts stays relatively low. This means that Dark Angels generates higher profit with fewer payouts compared to other strains, such as Phobos for example. Phobos has the highest frequency of payouts, while its median size payment, which is less than **USD 1,000,** remains the lowest.

Based on the investigation of a known BTC address <**bc1q0wf73xmcqkvrvs7tj49hznxqqgt6tp359gk0az**>, by Analyst1, Dark Angels actors received nearly **38 BTC** ransom payment (equivalent to USD ~1.5 million  at the time of the transaction) on May **4, 2022**. In comparison to a RansomHouse, a known BTC address <**1MmkNa1gRUmVSocZic8wJhehef8NW4GzDZ**> reported by Trellix and attributed to RansomHouse was used to receive a ransom payment in a similar amount of nearly USD 1.2 million received on **December 12, 2023**. According to the report, the initial ransom was set to USD 2.56 million with an apparent 50% discount agreed at the end.



Main (4)

INPUT 0
bc1q0wf73xmcqkvrvs7tj49hznxqqgt6tp359gk0az
AMOUNT
38.14000000 BTC · 1,443,484 USD

OUTPUT 0
1HCFDj7Kkzey3nuRPEFmiDvcJczCP8GE7S
AMOUNT
6.35666600 BTC · 240,580 USD

OUTPUT 1 CHANGE
bc1qlp8l7xwl4mcfcv8js7mvrl9yya65rmrdx7hkqc
AMOUNT
31.78332100 BTC · 1,202,903 USD

Address that Dark Angels actors used to receive ransom payment

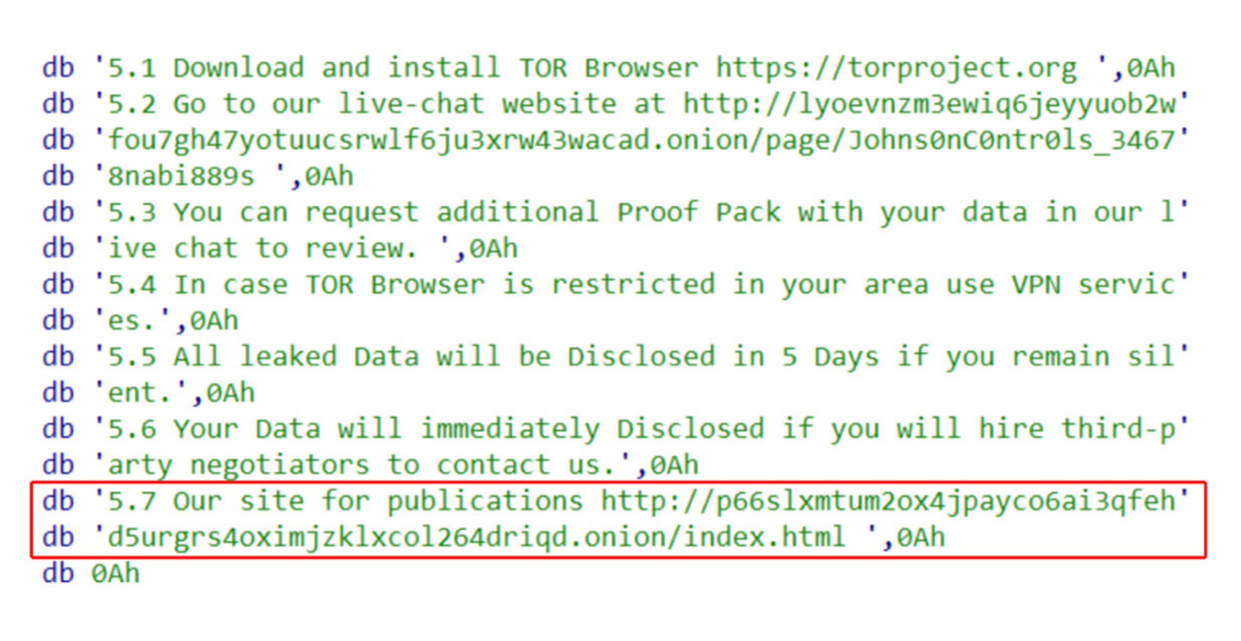
*Figure 6: Dark Angels actors received a ransom payment in the amount of nearly USD 1.5 million on May 4, 2022. Source: blockchair.com*

Johnson Controls International (JCI) which became one of the victims of Dark Angels shed light on connection between Dark Angels and two other groups: **Dunghill Leak** and **RagnarLoker**. JCI is a company specializing in manufacturing industrial control systems, physical security systems, and facility-related technology and infrastructure and does extensive business with U.S. federal agencies and the defense industrial base sector.

According to Bleeping Computer sources, actors stole over 27TB of confidential data and demanded USD 51 million  to provide a file decryptor and to delete stolen data. As it was later disclosed by JCI through an SEC filing submitted in December 2023, an attack occurred during the weekend of September 23, 2023.

Based on the reporting, **“The cybersecurity incident consisted of unauthorized access, data exfiltration and deployment of ransomware by a third party to a portion of the Company’s internal IT infrastructure.”** The attack resulted in a significant financial loss of nearly USD 27 million, consisting of ***“expenses associated with the response to, and remediation of, the incident, and are net of insurance recoveries.”*** It is unknown if any of the portion of these USD 27 million in expenses was partially a ransom paid to actors.

The connection between Dark Angels and Dunghill Leak was established through investigation of a ransom note shared by Dark Angels with JCI. According to the ransom note shared by threat researcher Gameel Ali on September 27, 2023, with the remainder shared with Analyst1 later, it was identified that during its double-extortion phase, actors directed the victim to the Dunghill Leak data leak site.



```
db '5.1 Download and install TOR Browser https://torproject.org ',0Ah
db '5.2 Go to our live-chat website at http://lyoevnzm3ewiq6jeyyuob2w'
db 'fou7gh47yotuucsrwlf6ju3xrw43wacad.onion/page/Johns0nC0ntr0ls_3467'
db '8nabi889s ',0Ah
db '5.3 You can request additional Proof Pack with your data in our l'
db 'ive chat to review. ',0Ah
db '5.4 In case TOR Browser is restricted in your area use VPN servic'
db 'es.',0Ah
db '5.5 All leaked Data will be Disclosed in 5 Days if you remain sil'
db 'ent.',0Ah
db '5.6 Your Data will immediately Disclosed if you will hire third-p'
db 'arty negotiators to contact us.',0Ah
db '5.7 Our site for publications http://p66slxmtum2ox4jpayco6ai3qfeh'
db 'd5urgrs4oximjzklxcol264driqd.onion/index.html ',0Ah
db 0Ah
```

*Figure 7: Ransom note sent to JCI showing a Dunghill data leak address named "our site for publications" note. Source: Analyst1*

The first victim was posted on the Dunghill Leak site in April 2024. Interestingly enough, the Dark Angels launched a separate data leak site at approximately the same time as the group's appearance in May 2022; however, no victims were ever posted for several months of its existence. Instead, actors seemed to use a Dunghill Leak instead of where their victims are being directed, including the JCI attack.

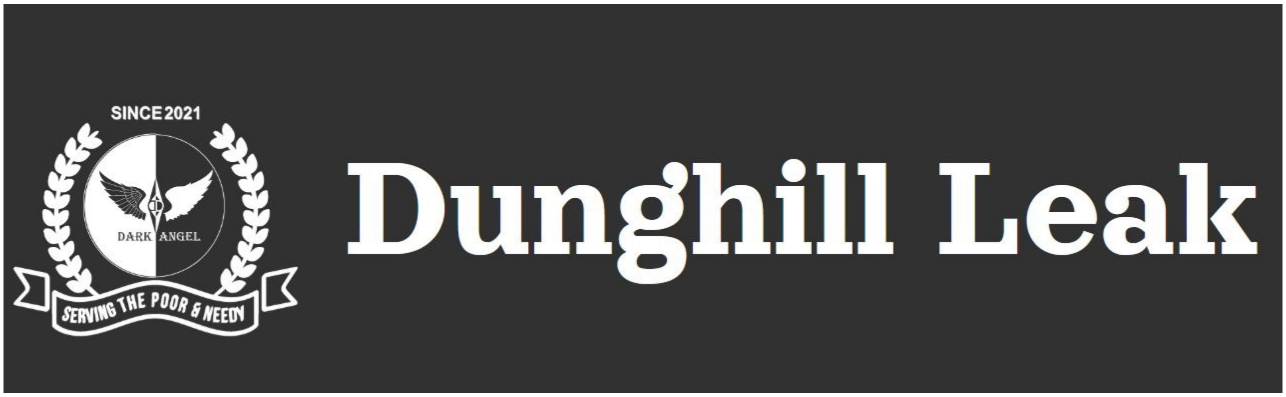
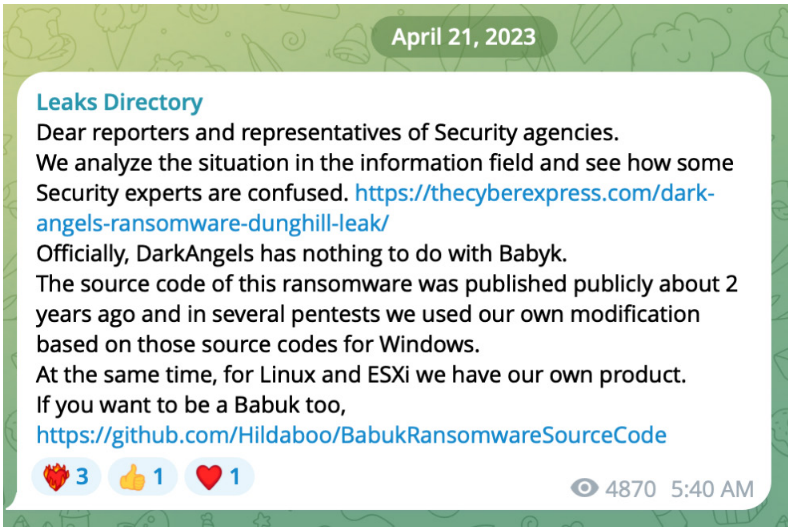


*Figure 8: Main image on Dunghill Leak data leak site also includes Dark Angel in their logo Source: Dunghill DLS*

In addition to the DLS, the Telegram channel **"Leaks Directory"** was registered on **January 15, 2023,** where actors would post claimed victims' names and files with the stolen data. According to the Analyst1 cross-reference analysis of Telegram and Dunghill Leak DLS, posts and identified claimed victims match on both platforms. In some cases, entities were posted on the same day, while in others, they were first posted on Telegram and then on the data leak site, or vice versa.

For example, their first victim posted on DLS on April 24, 2024, was posted on their Telegram channel on January 23, 2024, nearly two months earlier. Their Telegram channel was also used to clarify some ***"confusion among researchers"*** about Dark Angels being associated with Babuk. On **April 21, 2023,** Dark Angels posted a message denying any associations with Babuk by stating that leaked Babuk code was adapted by them and that they have their ***"own product"*** for Linux and ESXi.



April 21, 2023

Leaks Directory

Dear reporters and representatives of Security agencies.
We analyze the situation in the information field and see how some Security experts are confused. https://thecyberexpress.com/dark-angels-ransomware-dunghill-leak/
Officially, DarkAngels has nothing to do with Babyk.
The source code of this ransomware was published publicly about 2 years ago and in several pentests we used our own modification based on those source codes for Windows.
At the same time, for Linux and ESXi we have our own product.
If you want to be a Babuk too,
https://github.com/Hildaboo/BabukRansomwareSourceCode

❤‍🔥 3 👍 1 ❤️ 1 👁 4870 5:40 AM

*Figure 9: Dark Angels made a statement of not being associated with Babuk on its TG channel on April 21, 2021. Source: Telegram*

Another connection between RansomHouse (Dark Angels) and **RagnarLocker** was also uncovered during the investigation of the JCI attack. Similarities between Dark Angels and RagnarLocker were identified, with Dark Angels observed using RagnarLocker's original ESXi encryptor in the JCI attack. Later, we will further discuss the potential association of actors from both groups as RagnarLocker was identified in one of the crossclaim cases with RansomHouse.

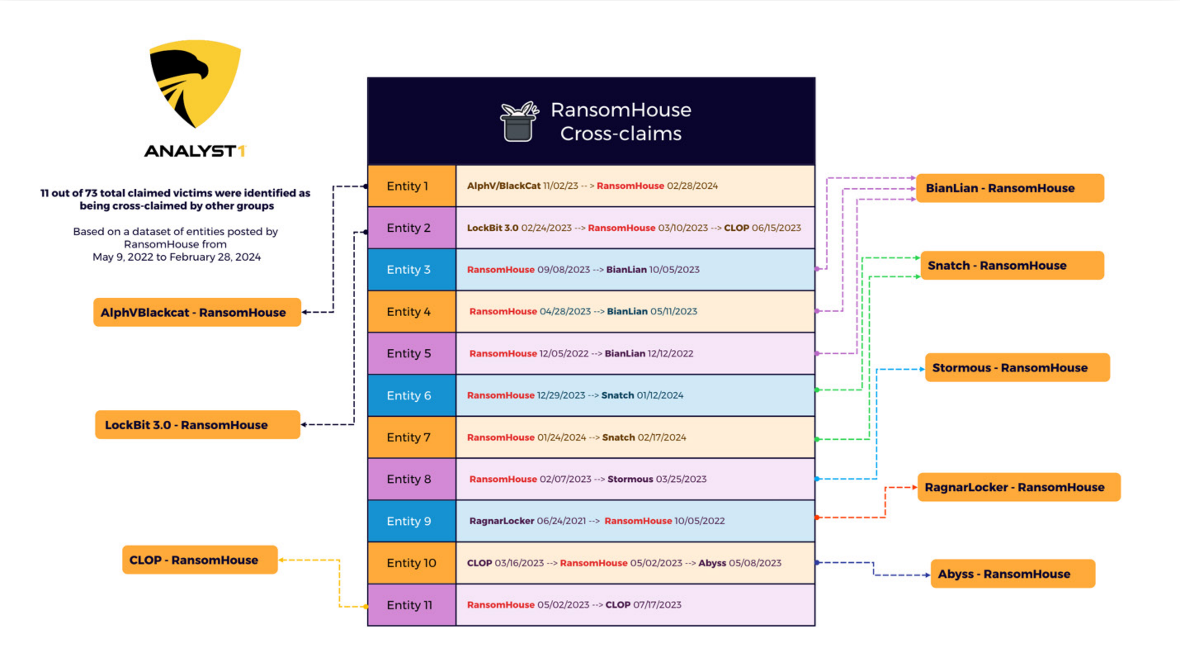
Indicators of associations between RansomHouse (White Rabbit & Mario ESXi), Dark Angels (Dunghill), and RagnarLocker groups suggest cross-collaboration among actors, with the high possibility of involving the same actors in operations of all three groups. The existence of such links might explain our findings of crossclaims between RansomHouse, considering their potential collaboration. In the following two sections, we will analyze crossclaim cases, also exploring the motivation behind data sharing among ransomware groups and its impact on incident response strategies.

# Investigating RansomHouse's Crossclaims

**Crossclaims** occur when the same victim is claimed multiple times by different ransomware groups on their DLS. Understanding the nature of crossclaims is crucial as it plays a pivotal role in guiding incident response actions effectively. Although we take threat actors' claims with a high degree of skepticism considering established cases of false claims, this source overall provides a good understanding of actors' victims' preferences and overall activity.

Investigating the RansomHouse group, we analyzed a dataset of entities posted by the group from **May 9, 2022**, to **February 28, 2024**. Based on our findings, **11** out of **73** total victims were identified as being cross-claimed by other groups. We observed crossclaims cases between **RansomHouse** and **Alphv/BlackCat**, **LockBit 3.0**, **BianLian**, **Snatch**, **Stormous**, **RagnarLocker**, **Abyss** and **CLOP**.

Looking at the timeline of crossclaims, we observe two scenarios involving RansomHouse. In the first scenario, RansomHouse claims an entity initially, followed by other syndicates making subsequent claims. Entities involved in this scenario include BianLian, Snatch, Stormous, and Abyss. In the **second scenario**, RansomHouse claims the same entity after it has already been claimed by other groups, as seen in cases involving Alphv/BlackCat, LockBit 3.0, and RagnarLocker.


ANALYST1
11 out of 73 total claimed victims were identified as being cross-claimed by other groups
Based on a dataset of entities posted by RansomHouse from May 9, 2022 to February 28, 2024
AlphVBlackcat - RansomHouse
LockBit 3.0 - RansomHouse
CLOP - RansomHouse
BianLian - RansomHouse
Snatch - RansomHouse
Stormous - RansomHouse
RagnarLocker - RansomHouse
Abyss - RansomHouse

RansomHouse Cross-claims

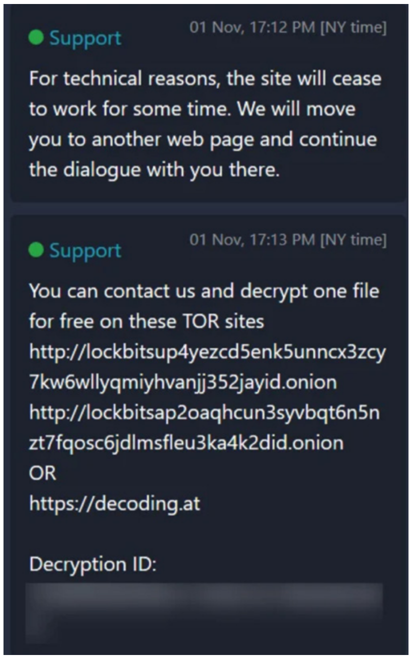
| | |
|---|---|
| Entity 1 | **AlphV/BlackCat** 11/02/23 -- > **RansomHouse** 02/28/2024 |
| Entity 2 | **LockBit 3.0** 02/24/2023 --> **RansomHouse** 03/10/2023 --> **CLOP** 06/15/2023 |
| Entity 3 | **RansomHouse** 09/08/2023 --> **BianLian** 10/05/2023 |
| Entity 4 | **RansomHouse** 04/28/2023 --> **BianLian** 05/11/2023 |
| Entity 5 | **RansomHouse** 12/05/2022 --> **BianLian** 12/12/2022 |
| Entity 6 | **RansomHouse** 12/29/2023 --> **Snatch** 01/12/2024 |
| Entity 7 | **RansomHouse** 01/24/2024 --> **Snatch** 02/17/2024 |
| Entity 8 | **RansomHouse** 02/07/2023 --> **Stormous** 03/25/2023 |
| Entity 9 | **RagnarLocker** 06/24/2021 --> **RansomHouse** 10/05/2022 |
| Entity 10 | **CLOP** 03/16/2023 --> **RansomHouse** 05/02/2023 --> **Abyss** 05/08/2023 |
| Entity 11 | **RansomHouse** 05/02/2023 --> **CLOP** 07/17/2023 |

*Figure 10: Timeline of crossclaims between RansomHouse and other ransomware groups*
*Source: Analyst1*

Additionally, CLOP ransomware appears in both scenarios. However, we exclude the CLOP variable from our analysis (although such collaboration is still possible) of potential data sharing between groups, as all entities cross-claimed with RansomHouse were confirmed to be breached by CLOP in separate cases during the exploitation of a zero-day exploit of Progress Software's MOVEit in May 2023.

LockBit, Alphv/BlackCat and RagnarLocker were identified as crossclaiming the same victims as RansomHouse among other groups. These cases follow the same scenario: LockBit 3.0, RagnarLocker, and Alphv/BlackCat claim the victim first and follow with a subsequent claim by RansomHouse.

For example, the collaboration between LockBit and BlackCat is not new, and we've seen such cases in the past. This cooperation extends to the sharing of infrastructure, including data leak sites. A noteworthy illustration of collaboration is the case of BlackMatter, formerly known as DarkSide, which transferred their victims to LockBit while undergoing a shutdown and rebranding process back in November 2021, eventually rebranding as Alphv/BlackCat later that year.



● Support 01 Nov, 17:12 PM [NY time]

For technical reasons, the site will cease to work for some time. We will move you to another web page and continue the dialogue with you there.

● Support 01 Nov, 17:13 PM [NY time]

You can contact us and decrypt one file for free on these TOR sites
http://lockbitsup4yezcd5enk5unncx3zcy7kw6wllyqmiyhvanjj352jayid.onion
http://lockbitsap2oaqhcun3syvbqt6n5nzt7fqosc6jdlmsfleu3ka4k2did.onion
OR
https://decoding.at

Decryption ID:
[redacted]

*Figure 11: Message shared by BlackMatter of moving communication to the LockBit site*
*Source: BleepingComputer*

Notably, a RansomHouse — Alphv/BlackCat crossclaim occurred during the time of another shutdown that BlackCat actors decided to make as the result of law enforcement actions. HAL Allergy was claimed by Alphv/BlackCat on **November 2, 2023**. Nearly a month later, on December 19, 2023, BlackCat's Data Leak Site was prominently taken down, displaying a seizure notice. This occurred due to a joint international operation of law enforcement agencies. According to The United States Department of Justice (DOJ), as a result of the operation, the FBI offered a decryption tool to over 500 victims worldwide, with additional victims encouraged to come forward.

Almost two months after BlackCat's claim, on **February 28, 2024**, RansomHouse claimed HAL Allergy. The company reported an attack confirming that on the morning of February 19, 2024, it was targeted by ransomware. It is unclear what strain was used to encrypt the victim's network and whether BlackCat assisted RansomHouse in any way to access HAL Allergy. However, considering the established cooperation of BlackCat actors with other groups, the timing of both claims suggests that such an instance might have taken place.

The crossclaim involving RansomHouse and LockBit 3.0 presents yet another instance of potential collaboration. Delaware Life Insurance was claimed by LockBit 3.0 on **February 24, 2023**, and by RansomHouse on **March 10, 2023**, while also being claimed by CLOP on **June 15, 2023**. According to notifications shared with its clients, the company reported only two ransomware incidents in 2023: first between May 29 and May 30, 2023, attributed to the CLOP attack exploiting the MOVEit vulnerability, and second on February 9, 2023. As mentioned earlier, we are excluding CLOP crossclaims from our analysis due to the nature of the breach, which likely has no association with breaches of the same victim claimed by LockBit and RansomHouse.

Considering the timeline of the reported attack on February 9, 2023, and the subsequent claim by LockBit 3.0, it is likely that LockBit actors were responsible for the initial attack. The outcome of negotiations with Delaware Life Insurance is unclear, but the appearance of the company on the data leak site suggests that the victim refused to cooperate with the actors. Subsequently, the data may have been shared with RansomHouse, which then claimed the company on their data leak site approximately two weeks after LockBit 3.0's initial claim.

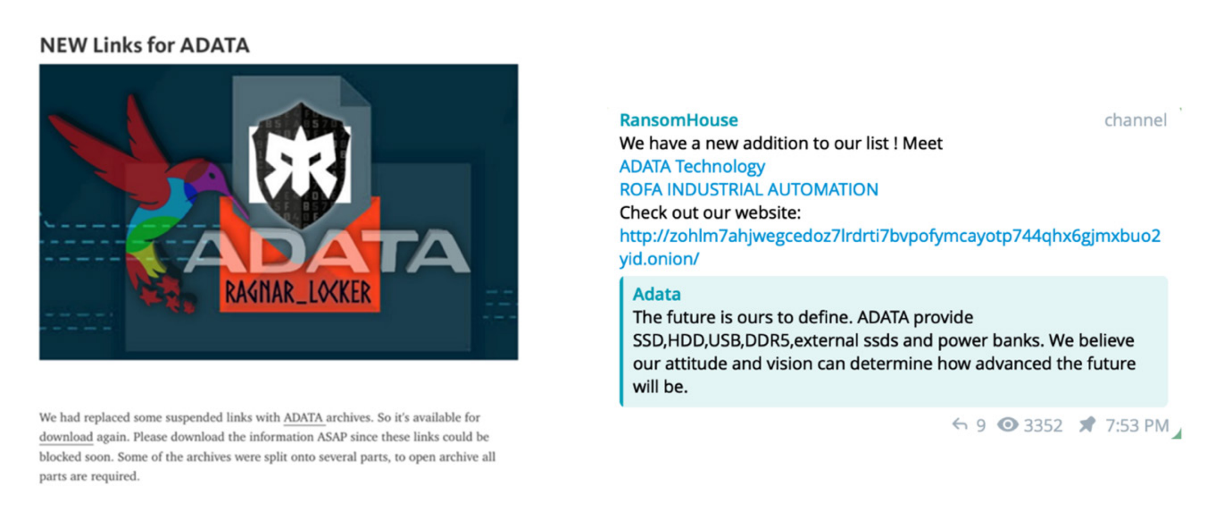
It is possible that a single actor might utilize data under a different syndicate's brands, a common occurrence in the realm of RaaS, where affiliates often partner with multiple groups. However, we are more inclined to believe in a well-established relationship between groups connected on multiple levels rather than just one single actor working with both syndicates.

It is also important to consider that these groups are geopolitically aligned with Russia, suggesting that their composition belongs to the same community. One of the key characteristics of the Russian ransomware ecosystem is a collectivist mindset and close interpersonal relationships that serve as the foundation for their "business" operations.

Given the current geopolitical climate, actors may find themselves increasingly connected and supportive of each other, pooling their resources against entities they perceive as the state's enemies.

The crossclaim between **RagnarLocker** and **RansomHouse** presents an intriguing case that suggests potential data sharing between two groups or even the involvement of the same actors in the operations of both groups. Like LockBit 3.0 and Alphv/BlackCat, RagnarLocker initially claimed a victim, with RansomHouse later doing the same. Specifically, Entity #9 on our graph, a Taiwanese chip maker ADATA was first claimed by RagnarLocker on **June 24, 2021**, on its data leak site following a ransomware attack on May 23, 2021, during which the entity refused to pay a ransom, resulting in a data leak.

Subsequently, on **October 5, 2022,** RansomHouse made a claim on ADATA, alleging possession of 1TB worth of sensitive data. Three days prior to that, actors also claimed ADATA as a victim on their Telegram channel. However, in a statement to a BleepingComputer, ADATA denied the claim of a RansomHouse attack, asserting that the leaked files were from a May 2021 RagnarLocker breach, during which 1.5TB of data was stolen.


NEW Links for ADATA

We had replaced some suspended links with ADATA archives. So it's available for download again. Please download the information ASAP since these links could be blocked soon. Some of the archives were split onto several parts, to open archive all parts are required.

RansomHouse
channel
We have a new addition to our list ! Meet
ADATA Technology
ROFA INDUSTRIAL AUTOMATION
Check out our website:
http://zohlm7ahjwegcedoz7lrdrti7bvpofymcayotp744qhx6gjmxbuo2yid.onion/

> Adata
> The future is ours to define. ADATA provide SSD,HDD,USB,DDR5,external ssds and power banks. We believe our attitude and vision can determine how advanced the future will be.

*Figure 12: From left to right is a claim of ADATA by RagnarLocker and a subsequent claim of an entity by RansomHouse Source: RagnarLocker DLS & RansomHouse Telegram Channel*

The exact nature of the data presented to ADATA by RansomHouse remains unclear, raising questions about whether it was the same data leaked/stolen previously by RagnarLocker. In addition to the scenario where RansomHouse actors are not in fact linked to RagnarLocker and acquired the data leaked from the ADATA breach in 2021, falsely presenting it as a new attack, we also explore an alternative scenario to address such coincidence of this crossclaim.

One possibility is that there was collaboration between actors, involving the sharing of data either freely or for a fee between two ransomware groups. Alternatively, it's possible that the same actor(s) who previously operated under the RagnarLocker brand eventually transitioned to RansomHouse.

The transition could have occurred during the arrests of RagnarLocker actors in October 2021 across multiple countries, including Ukraine and France. Despite RagnarLocker continuing its operations until October 2023, when its data leak site was seized by law enforcement, some RagnarLocker actors might have moved to other groups during the initial arrests in 2021. There is also a possibility that RansomHouse emerged as a new project for actors involved in RagnarLocker operations as they sought to continue their criminal activities under a different brand.

It can also explain instances of similarities between Dark Angels, which is suspected to be closely associated with RansomHouse, and RagnarLocker. Dark Angels was observed using RagnarLocker's original ESXi encryptor in the JCI attack mentioned earlier in the report. While similarities in source code do not definitely confirm the involvement of the same actors in the operations of both groups, as it could have been purchased from actors, the coincidence of both groups claiming the same victim might potentially suggest such a scenario.

Moving forward to **BianLian**, we observed three instances of crossclaims to be made by these two groups, with RansomHouse first claiming the victim and then BianLian claiming the same entity. BianLian has been operating since approximately June 2022. The indication of potential association and involvement of the same actors in both RansomHouse and BianLian operations was reported by Resecurity on December 15, 2023, which noticed the same email used by both groups in their communication with victims. Thus, swikipedia@onionmail[.]org was observed to be shared by RansomHouse with one of the victims, while the same email was attributed by CISA to BianLian. Artifacts such as emails and other indicators are valuable evidence for establishing connections between multiple groups within the ransomware landscape, which is likely the case in BianLian-RansomHouse's potential association.

In the case of **Abyss-RansomHouse**, there was a single claim concerning AvidXchange, a financial software company based in the US. The company has claimed a total of three times in 2023: one by CLOP on **March 16, 2023**, another by RansomHouse on **May 2, 2024**, and one by Abyss on **May 8, 2023**. According to the Office of the Maine Attorney General, the breach occurred on March 2, 2023, and likely referred to a CLOP attack based on the data leak timeline. No other official reports on additional attacks occurring in 2023 were found.

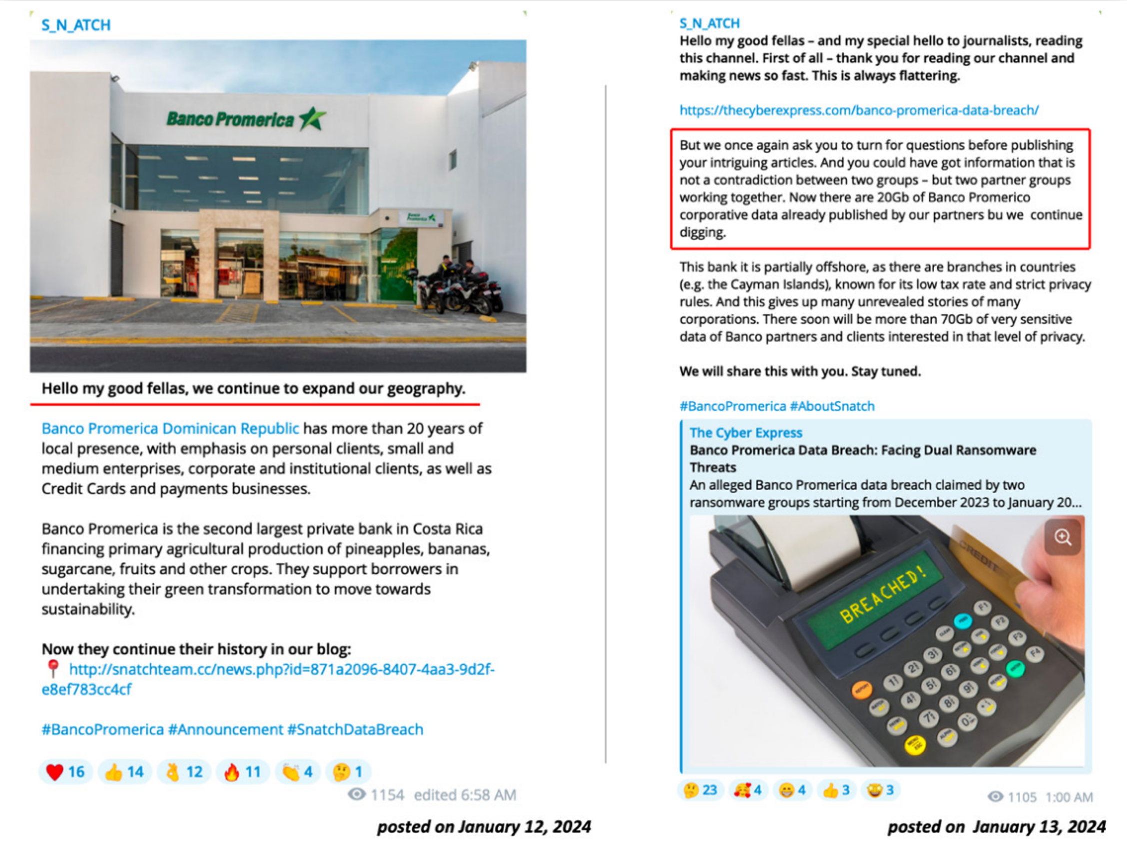
The connection between RansomHouse and Abyss remains unclear, as does whether the claimed attacks on AvidXchange were separate incidents or if, in fact, they ever took place. Abyss shares many similarities with RansomHouse, including using different strains for both Linux and Windows systems. Given the timeline of claims and similar modus operandi of both groups, there is a possibility of collaboration between syndicates.

While it is possible that a victim may be targeted independently by separate actors exploiting different vulnerabilities, the prevalence of cross-claims suggests a deeper underlying dynamic: collaboration and data sharing among threat actors. Our investigation into a potential link between RansomHouse and the above-mentioned groups is ongoing. In the next section we will look at the intriguing case of potential collaboration between RansomHouse with Stormous and Snatch and involving influence operations, which we uncovered during our investigation.

## RansomHouse, Stormous & Snatch: Ransomware, Hacktivist-Like Hybrid

We've singled out Stormous and Snatch for a specific reason: their involvement in influence operations introduces a different dimension. Our previous research on Snatch shed light on its activity. From our observations, Snatch actors appear to engage in hacktivist-like operations, leveraging their ransomware resources to conduct covert influence campaigns, primarily targeting Europe and the United States. Snatch actors have openly admitted to engaging in data reuse, claiming to ***"specialize exclusively in leaked sensitive data"*** and collaborating with other ransomware groups responsible for data breaches.

Interestingly enough, Snatch openly admitted its partnership with RansomHouse while commenting on an incident involving Banco Promerica de la República Dominicana, a victim claimed first by RansomHouse on December 29, 2023, and then by Snatch on January 11, 2024. On January 12, 2024, Snatch actors responded to an article published by The Cyber Express, highlighting a dual attack by RansomHouse and Snatch, stating, ***"That is not a contradiction between two groups — but two partner groups working together."*** Not only did Snatch post details of the victim on its data leak site, but it also shared information about the entity on its Telegram channel. Over five messages posted from January 12, 2024, to June 2, 2024, Snatch shared sensitive information related to their victim, including personal details of individuals associated with it.



S_N_ATCH

**Hello my good fellas, we continue to expand our geography.**

Banco Promerica Dominican Republic has more than 20 years of local presence, with emphasis on personal clients, small and medium enterprises, corporate and institutional clients, as well as Credit Cards and payments businesses.

Banco Promerica is the second largest private bank in Costa Rica financing primary agricultural production of pineapples, bananas, sugarcane, fruits and other crops. They support borrowers in undertaking their green transformation to move towards sustainability.

**Now they continue their history in our blog:**
📍 http://snatchteam.cc/news.php?id=871a2096-8407-4aa3-9d2f-e8ef783cc4cf

#BancoPromerica #Announcement #SnatchDataBreach

❤️ 16 👍 14 👌 12 🔥 11 👏 4 🤔 1
👁 1154 edited 6:58 AM

***posted on January 12, 2024***

S_N_ATCH

**Hello my good fellas – and my special hello to journalists, reading this channel. First of all – thank you for reading our channel and making news so fast. This is always flattering.**

https://thecyberexpress.com/banco-promerica-data-breach/

But we once again ask you to turn for questions before publishing your intriguing articles. And you could have got information that is not a contradiction between two groups – but two partner groups working together. Now there are 20Gb of Banco Promerico corporative data already published by our partners bu we continue digging.

This bank it is partially offshore, as there are branches in countries (e.g. the Cayman Islands), known for its low tax rate and strict privacy rules. And this gives up many unrevealed stories of many corporations. There soon will be more than 70Gb of very sensitive data of Banco partners and clients interested in that level of privacy.

**We will share this with you. Stay tuned.**

#BancoPromerica #AboutSnatch

The Cyber Express
**Banco Promerica Data Breach: Facing Dual Ransomware Threats**
An alleged Banco Promerica data breach claimed by two ransomware groups starting from December 2023 to January 20...

🤔 23 🥰 4 😁 4 👍 3 🤩 3
👁 1105 1:00 AM

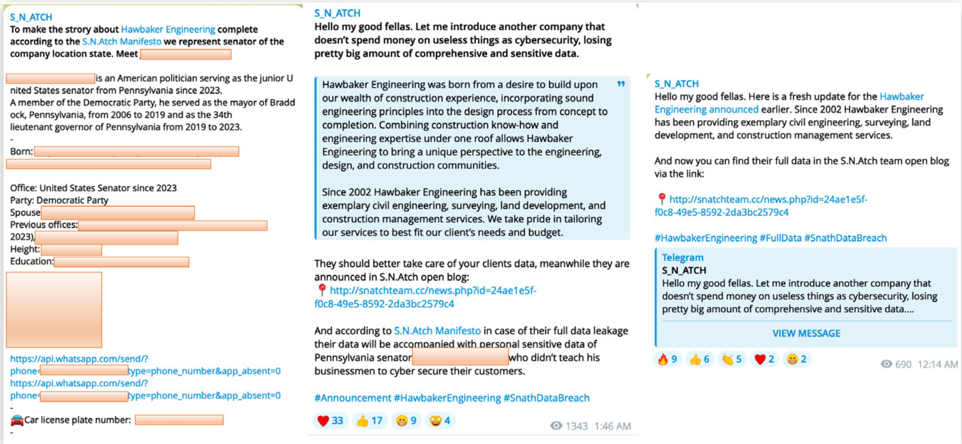
***posted on January 13, 2024***

*Figure 13: Snatch posted messages on its Telegram channel. Source: Telegram*

On **February 17, 2024,** Snatch posted Hawbaker Engineering on its data leak site and Telegram channel, marking another crossclaim with RansomHouse, which posted the entity earlier on January 24, 2024.

During this period, from February 14, 2024, to February 26, 2024, Snatch shared sensitive information related to the company in a series of messages. This wasn't merely a routine ransomware leak; in typical Snatch fashion, it targeted government officials associated with the state where the company is located. The message conveyed in these posts once again criticized the entity and associated individuals, aligning with the so-called Snatch manifesto that justifies their actions under the guise of addressing "weak security practices."

***From Snatch Manifesto:* "Business and power are united and go hand in hand. And each leak has its own name and face, both from the side of the business that allowed it and from the side of the authorities covering this business. That's why from now on each of our publications will be accompanied by personal data of presidents (owners of companies) and personal data of representatives of authorities assigned to this region."**



S_N_ATCH
**To make the strory about Hawbaker Engineering complete according to the S.N.Atch Manifesto we represent senator of the company location state. Meet [redacted]**

[redacted] is an American politician serving as the junior United States senator from Pennsylvania since 2023.
A member of the Democratic Party, he served as the mayor of Braddock, Pennsylvania, from 2006 to 2019 and as the 34th lieutenant governor of Pennsylvania from 2019 to 2023.
-
Born: [redacted]

Office: United States Senator since 2023
Party: Democratic Party
Spouse [redacted]
Previous offices: [redacted]
2023), [redacted]
Height: [redacted]
Education: [redacted]

[redacted]

https://api.whatsapp.com/send/?phone=[redacted]type=phone_number&app_absent=0
https://api.whatsapp.com/send/?phone=[redacted]type=phone_number&app_absent=0
-
🚘Car license plate number: [redacted]
-

S_N_ATCH
**Hello my good fellas. Let me introduce another company that doesn't spend money on useless things as cybersecurity, losing pretty big amount of comprehensive and sensitive data.**

> Hawbaker Engineering was born from a desire to build upon our wealth of construction experience, incorporating sound engineering principles into the design process from concept to completion. Combining construction know-how and engineering expertise under one roof allows Hawbaker Engineering to bring a unique perspective to the engineering, design, and construction communities.
>
> Since 2002 Hawbaker Engineering has been providing exemplary civil engineering, surveying, land development, and construction management services. We take pride in tailoring our services to best fit our client's needs and budget.

They should better take care of your clients data, meanwhile they are announced in S.N.Atch open blog:
📍 http://snatchteam.cc/news.php?id=24ae1e5f-f0c8-49e5-8592-2da3bc2579c4

And according to S.N.Atch Manifesto in case of their full data leakage their data will be accompanied with personal sensitive data of Pennsylvania senator [redacted] who didn't teach his businessmen to cyber secure their customers.

#Announcement #HawbakerEngineering #SnathDataBreach

❤️ 33 👍 17 😁 9 🤩 4 1343 1:46 AM

S_N_ATCH
Hello my good fellas. Here is a fresh update for the Hawbaker Engineering announced earlier. Since 2002 Hawbaker Engineering has been providing exemplary civil engineering, surveying, land development, and construction management services.

And now you can find their full data in the S.N.Atch team open blog via the link:

📍 http://snatchteam.cc/news.php?id=24ae1e5f-f0c8-49e5-8592-2da3bc2579c4

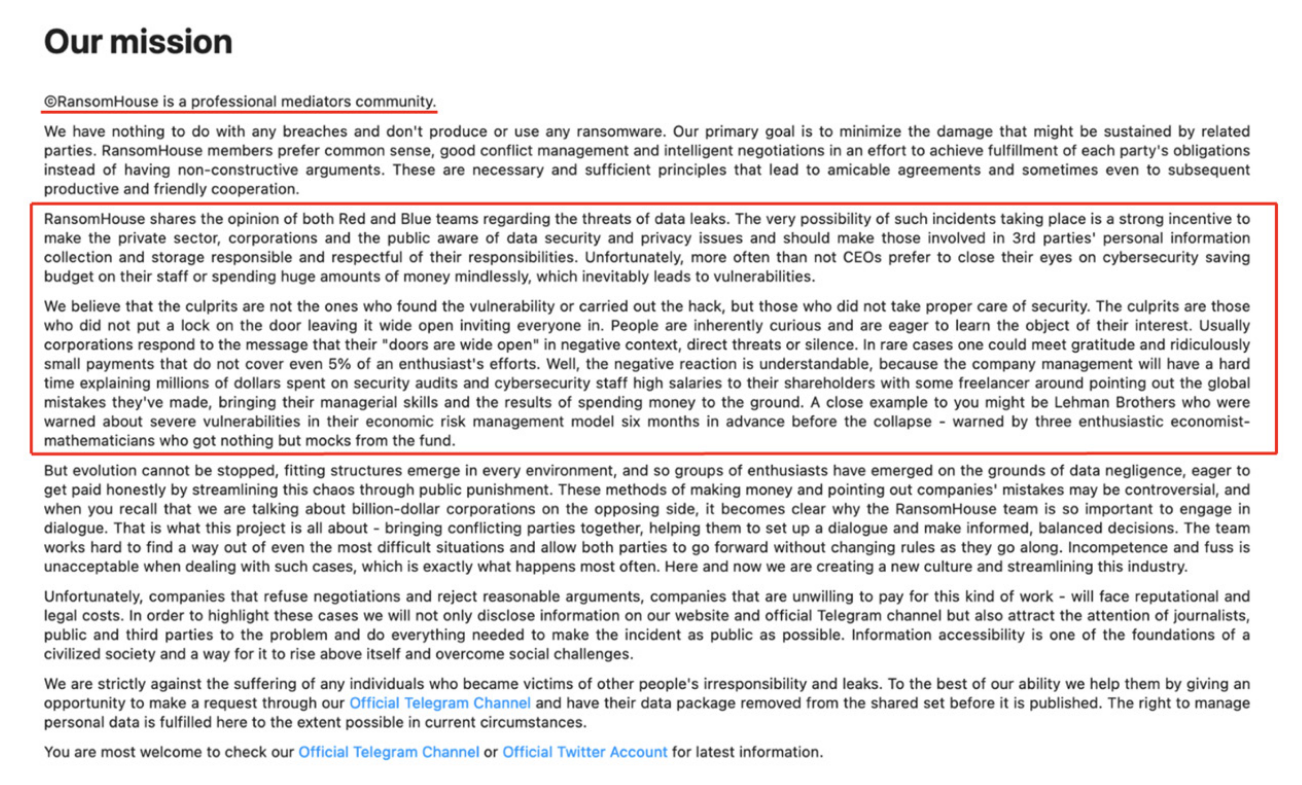
#HawbakerEngineering #FullData #SnathDataBreach

> Telegram
> S_N_ATCH
> Hello my good fellas. Let me introduce another company that doesn't spend money on useless things as cybersecurity, losing pretty big amount of comprehensive and sensitive data....
>
> VIEW MESSAGE

🔥 9 👍 6 👏 5 ❤️ 2 😁 2 690 12:14 AM

*Figure 14: Messages posted by Snatch on its Telegram channel. Source: Snatch Telegram channel*

Two groups also seem aligned with the narratives of victim-blaming they are pushing to the public. RansomHouse, similar to Snatch, claims that its primary goal is to ensure digital safety by educating its audience on various subjects. On their leak site's mission section, RansomHouse actors describe themselves as a ***"professional mediators community"*** committed to safeguarding personal information. They assert, "***We believe that the culprits are not the ones who found vulnerabilities or carried out the attacks, but those who did not prioritize security."***



## Our mission

©RansomHouse is a professional mediators community.

We have nothing to do with any breaches and don't produce or use any ransomware. Our primary goal is to minimize the damage that might be sustained by related parties. RansomHouse members prefer common sense, good conflict management and intelligent negotiations in an effort to achieve fulfillment of each party's obligations instead of having non-constructive arguments. These are necessary and sufficient principles that lead to amicable agreements and sometimes even to subsequent productive and friendly cooperation.

RansomHouse shares the opinion of both Red and Blue teams regarding the threats of data leaks. The very possibility of such incidents taking place is a strong incentive to make the private sector, corporations and the public aware of data security and privacy issues and should make those involved in 3rd parties' personal information collection and storage responsible and respectful of their responsibilities. Unfortunately, more often than not CEOs prefer to close their eyes on cybersecurity saving budget on their staff or spending huge amounts of money mindlessly, which inevitably leads to vulnerabilities.

We believe that the culprits are not the ones who found the vulnerability or carried out the hack, but those who did not take proper care of security. The culprits are those who did not put a lock on the door leaving it wide open inviting everyone in. People are inherently curious and are eager to learn the object of their interest. Usually corporations respond to the message that their "doors are wide open" in negative context, direct threats or silence. In rare cases one could meet gratitude and ridiculously small payments that do not cover even 5% of an enthusiast's efforts. Well, the negative reaction is understandable, because the company management will have a hard time explaining millions of dollars spent on security audits and cybersecurity staff high salaries to their shareholders with some freelancer around pointing out the global mistakes they've made, bringing their managerial skills and the results of spending money to the ground. A close example to you might be Lehman Brothers who were warned about severe vulnerabilities in their economic risk management model six months in advance before the collapse - warned by three enthusiastic economist-mathematicians who got nothing but mocks from the fund.

But evolution cannot be stopped, fitting structures emerge in every environment, and so groups of enthusiasts have emerged on the grounds of data negligence, eager to get paid honestly by streamlining this chaos through public punishment. These methods of making money and pointing out companies' mistakes may be controversial, and when you recall that we are talking about billion-dollar corporations on the opposing side, it becomes clear why the RansomHouse team is so important to engage in dialogue. That is what this project is all about - bringing conflicting parties together, helping them to set up a dialogue and make informed, balanced decisions. The team works hard to find a way out of even the most difficult situations and allow both parties to go forward without changing rules as they go along. Incompetence and fuss is unacceptable when dealing with such cases, which is exactly what happens most often. Here and now we are creating a new culture and streamlining this industry.

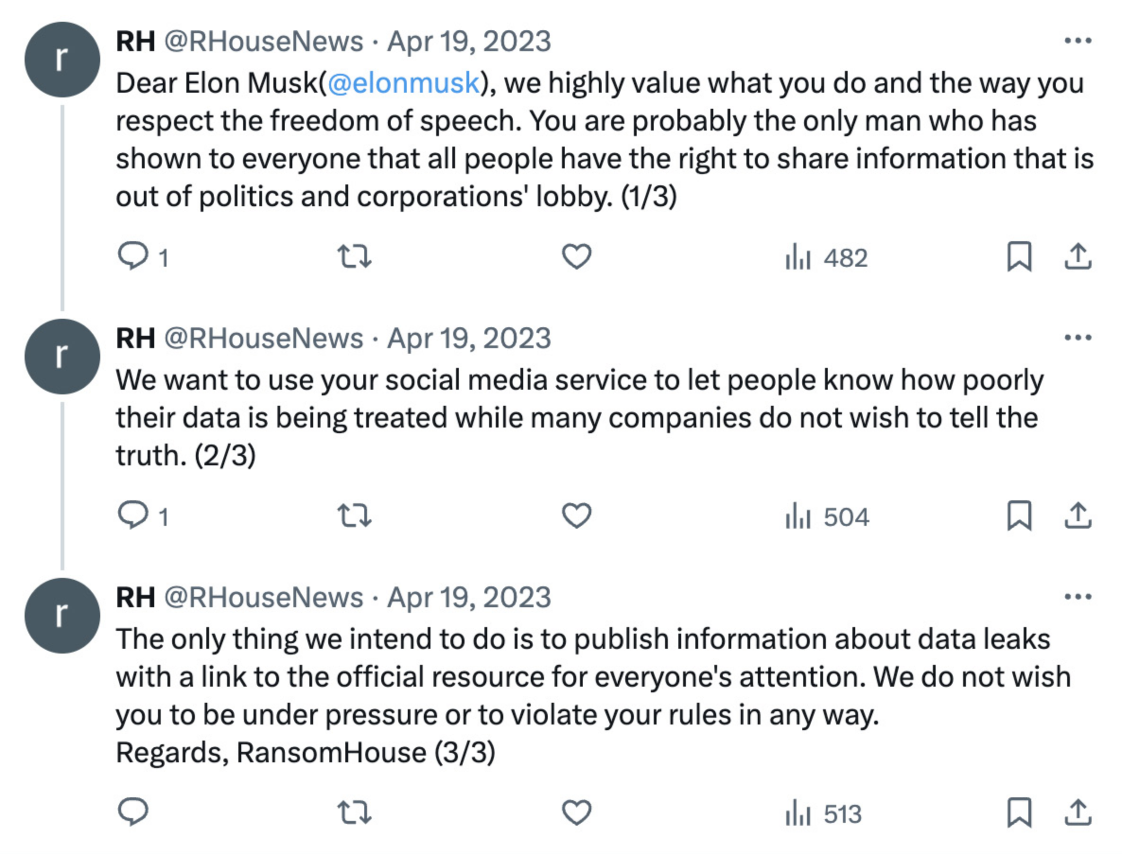
Unfortunately, companies that refuse negotiations and reject reasonable arguments, companies that are unwilling to pay for this kind of work - will face reputational and legal costs. In order to highlight these cases we will not only disclose information on our website and official Telegram channel but also attract the attention of journalists, public and third parties to the problem and do everything needed to make the incident as public as possible. Information accessibility is one of the foundations of a civilized society and a way for it to rise above itself and overcome social challenges.

We are strictly against the suffering of any individuals who became victims of other people's irresponsibility and leaks. To the best of our ability we help them by giving an opportunity to make a request through our Official Telegram Channel and have their data package removed from the shared set before it is published. The right to manage personal data is fulfilled here to the extent possible in current circumstances.

You are most welcome to check our Official Telegram Channel or Official Twitter Account for latest information.

*Figure 15: RansomHouse's mission statement. Source: RansomHouse DLS*

To increase visibility, RansomHouse takes this victim-blaming narrative a step further by pushing a similar message through their X account, tagging the platform's CEO, Elon Musk. In a post dated **April 19, 2023**, the actors state, ***"We want to use your social media service to let people know how poorly their data is being treated while many companies do not wish to tell the truth."***



**RH** @RHouseNews · Apr 19, 2023

Dear Elon Musk(@elonmusk), we highly value what you do and the way you respect the freedom of speech. You are probably the only man who has shown to everyone that all people have the right to share information that is out of politics and corporations' lobby. (1/3)

**RH** @RHouseNews · Apr 19, 2023

We want to use your social media service to let people know how poorly their data is being treated while many companies do not wish to tell the truth. (2/3)

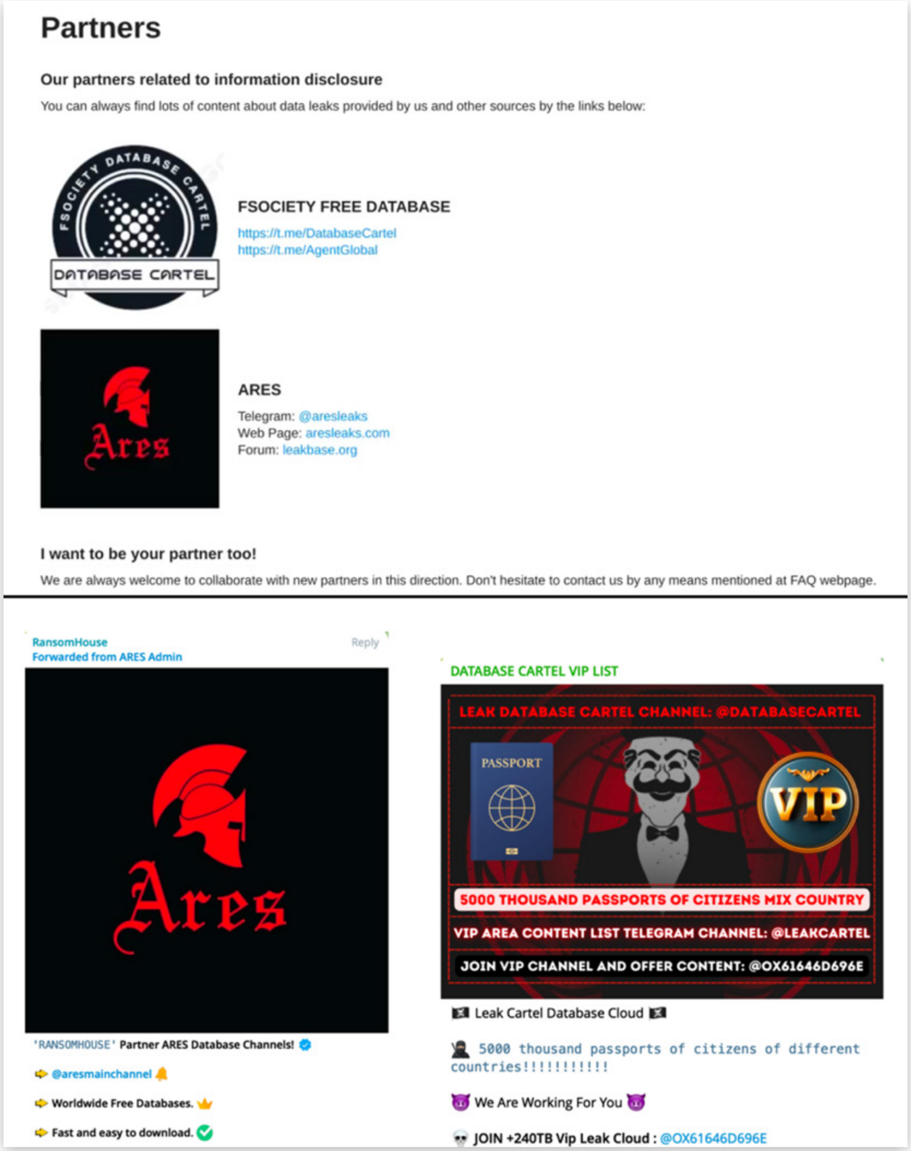
**RH** @RHouseNews · Apr 19, 2023

The only thing we intend to do is to publish information about data leaks with a link to the official resource for everyone's attention. We do not wish you to be under pressure or to violate your rules in any way.
Regards, RansomHouse (3/3)

*Figure 16: RansomHouse posts on Twitter tagging Elon Musk, CEO of X (former Twitter)*
*Source: Twitter*

The same narrative is also evident in the announcement of RansomHouse's partnership on its data leak site's **"Partners"** page. Here, **Database Cartel** and **Ares Leaks** are called their ***"partners related to information disclosure"*** activities. This tactic clearly serves as an attempt to justify their criminal actions of disclosing personal data as a form of punishment for victims who failed victims of their attacks.

Upon investigating Ares Leaks and Database Cartel activities, we discovered that their primary operation revolves around a stolen data market. These groups frequently post updates about their claimed victims and offer the stolen data for sale on their Telegram channels. Initially, Ares Leaks also operated a forum, which now appears inaccessible.


FSOCIETY DATABASE CARTEL
DATABASE CARTEL
Ares
Ares
LEAK DATABASE CARTEL CHANNEL: @DATABASECARTEL
PASSPORT
VIP
5000 THOUSAND PASSPORTS OF CITIZENS MIX COUNTRY
VIP AREA CONTENT LIST TELEGRAM CHANNEL: @LEAKCARTEL
JOIN VIP CHANNEL AND OFFER CONTENT: @OX61646D696E
Reply

Partners

Our partners related to information disclosure

You can always find lots of content about data leaks provided by us and other sources by the links below:

FSOCIETY FREE DATABASE
https://t.me/DatabaseCartel
https://t.me/AgentGlobal

ARES
Telegram: @aresleaks
Web Page: aresleaks.com
Forum: leakbase.org

I want to be your partner too!

We are always welcome to collaborate with new partners in this direction. Don't hesitate to contact us by any means mentioned at FAQ webpage.

RansomHouse
Forwarded from ARES Admin

'RANSOMHOUSE' Partner ARES Database Channels!

➪ @aresmainchannel

➪ Worldwide Free Databases.

➪ Fast and easy to download. ✓

DATABASE CARTEL VIP LIST

Leak Cartel Database Cloud

5000 thousand passports of citizens of different countries!!!!!!!!!!!

We Are Working For You

JOIN +240TB Vip Leak Cloud : @OX61646D696E

*Figure 17: RansomHouse's post about their partners is shown at the top, with Ares Leaks and Database Cartel offering stolen data on Telegram visible in the bottom image*
*Source: RansomHouse DLS/Telegram*

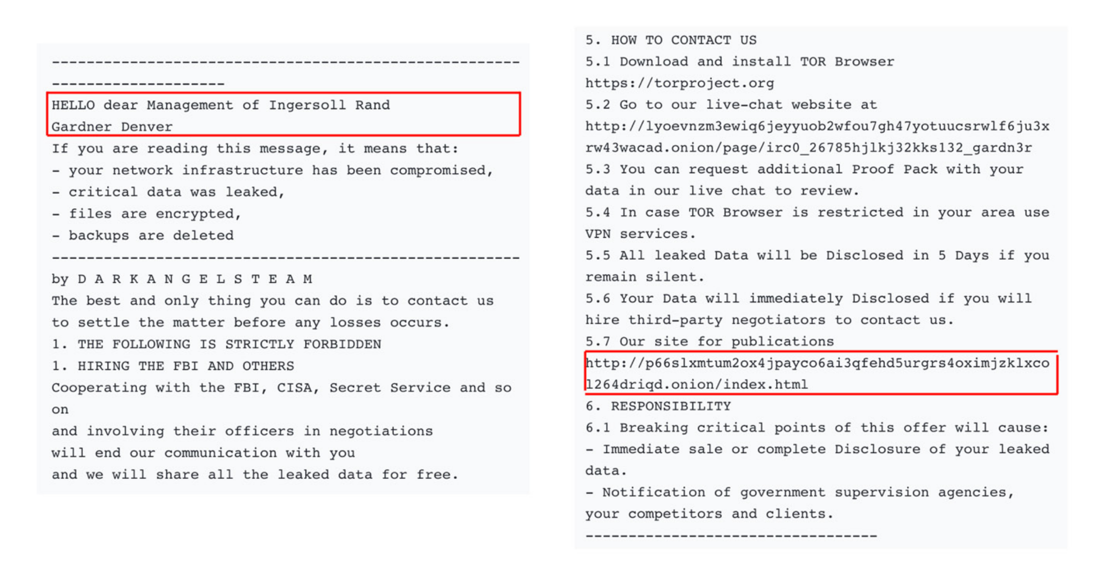
We also observe a very similar operational, hacktivist-like activity and tactics employed when analyzing Stormous. In addition to the website on Tor serving as a data leak site, the group also established a presence across Telegram and X (Twitter), with their accounts eventually being disabled on both platforms. It is worth adding that their DLS also became inaccessible approximately on May 11, 2024, and still is as of the day of this report on June 6, 2024.

Such an alignment in tactics might also indicate potential cooperation and explain what initially drew our attention: a case of cross-claims observed between Stormous and RansomHouse. According to our analysis, there is one instance of a cross-claim involving

The Dubai Gold & Commodities Exchange (DGCX), a UAE entity claimed first by RansomHouse on **February 7, 2023**, and then by Stormous on **March 25, 2023**. A cyber incident was confirmed by a DGCX spokesperson on February 9, 2023, stating that an unauthorized third party accessed some files, but it did not impact day-to-day operations or its trading platform.

When exploring potential connections between groups, we found a noteworthy detail that may indicate such a scenario. Specifically, a ransom note was submitted on VirusTotal on April 28, 2024, by Dark Angels (whose association with RansomHouse we've established earlier), allegedly extorting one of their victims, Ingersoll Rand.

However, the most intriguing aspect emerged when we checked Dunghill Leak, which Dark Angels included in their note, and found no claims of Ingersoll Rand. What we found instead was Stormous claiming this entity on **March 27, 2023**, on its data leak site. Although the possibility of Stormous and RansomHouse targeting the same company theoretically might exist, it is likely that two groups were cooperating with each other, including this particular case or, in additional cases, are likely subgroups of a bigger group.



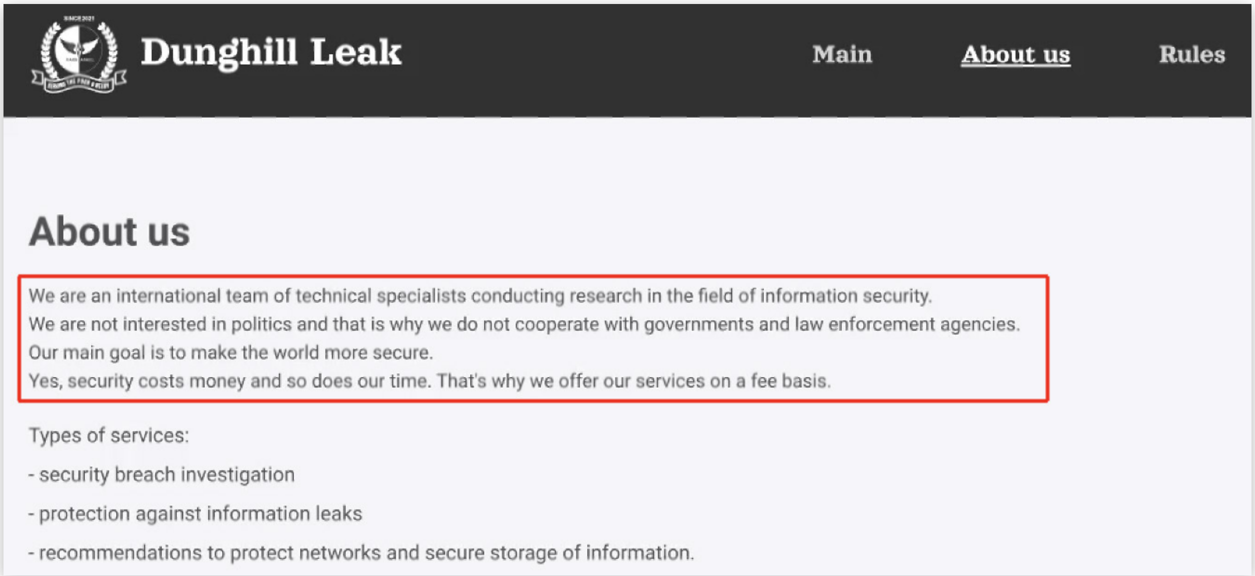
```
-------------------------------------------------------
--------------------
HELLO dear Management of Ingersoll Rand
Gardner Denver
If you are reading this message, it means that:
- your network infrastructure has been compromised,
- critical data was leaked,
- files are encrypted,
- backups are deleted
-------------------------------------------------------
by D A R K A N G E L S T E A M
The best and only thing you can do is to contact us
to settle the matter before any losses occurs.
1. THE FOLLOWING IS STRICTLY FORBIDDEN
1. HIRING THE FBI AND OTHERS
Cooperating with the FBI, CISA, Secret Service and so
on
and involving their officers in negotiations
will end our communication with you
and we will share all the leaked data for free.
```

```
5. HOW TO CONTACT US
5.1 Download and install TOR Browser
https://torproject.org
5.2 Go to our live-chat website at
http://lyoevnzm3ewiq6jeyyuob2wfou7gh47yotuucsrwlf6ju3x
rw43wacad.onion/page/irc0_26785hjlkj32kks132_gardn3r
5.3 You can request additional Proof Pack with your
data in our live chat to review.
5.4 In case TOR Browser is restricted in your area use
VPN services.
5.5 All leaked Data will be Disclosed in 5 Days if you
remain silent.
5.6 Your Data will immediately Disclosed if you will
hire third-party negotiators to contact us.
5.7 Our site for publications
http://p66slxmtum2ox4jpayco6ai3qfehd5urgrs4oximjzklxco
l264driqd.onion/index.html
6. RESPONSIBILITY
6.1 Breaking critical points of this offer will cause:
- Immediate sale or complete Disclosure of your leaked
data.
- Notification of government supervision agencies,
your competitors and clients.
----------------------------------
```

*Figure 18: Ransom note shared by Dark Angels with one of their victims*
*Source: Virus Total*

Given the suspected affiliation between Dark Angels and RansomHouse and the possibility of them sharing data and resources, such an intersection makes sense. This alignment is further supported when examining the tactics used by these groups. In particular, Dark Angels/Dunghill and RansomHouse demonstrate many similarities in their position, employing a victim-blaming strategy.

Their data leak site's **"About Us"** page states, ***"We are an international team of technical specialists conducting research in the field of information security. We are not interested in politics and therefore do not cooperate with governments and law enforcement agencies. Our main goal is to make the world more secure. Yes, security costs money, and so does our time. That's why we offer our services on a fee basis."***



About us

We are an international team of technical specialists conducting research in the field of information security.
We are not interested in politics and that is why we do not cooperate with governments and law enforcement agencies.
Our main goal is to make the world more secure.
Yes, security costs money and so does our time. That's why we offer our services on a fee basis.

Types of services:

- security breach investigation
- protection against information leaks
- recommendations to protect networks and secure storage of information.

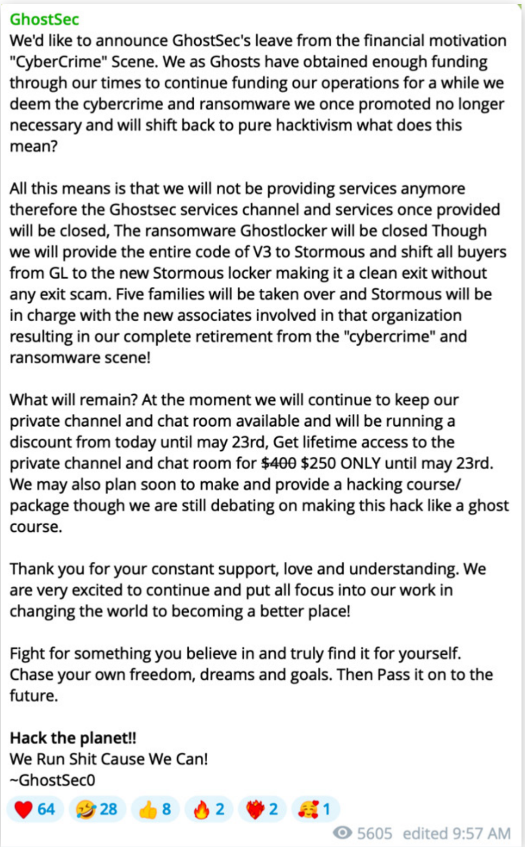
*Figure 19: Dark Angels (Dunghill Leak) "About Us" page on their DLS reflects their mission statement*
*Source: Dark Angels DLS*

When examining Stormous's timeline and nature of operations, the group emerged around mid-2021 initially as a typical ransomware group engaging in RaaS (Ransomware-as-a-Service). Over time, however, they adjusted their operations and became increasingly vocal about their political stance.

On **March 1, 2022,** four days after the invasion of Ukraine started, Stormous posted a message: ***"The STORMOUS team has officially announced its support for the Russian government. And if any party in different parts of the world decides to organize a cyber-attack or cyber-attacks against Russia, we will be in the right direction and will make all our efforts to abandon the supplication of the West, especially the infrastructure. Perhaps the hacking operation that our team carried out for the government of Ukraine and a Ukranian airline was just a simple operation but what is coming will be bigger!!!"***

In **July 2023,** Stormous publicly aligned themselves with GhostSec, **a hacktivist-like group. Both later became** part of the so-called "Five Families" in August 2023, which included four hacktivist groups: GhostSec, ThreatSec, SiegedSec, and BlackForums, a forum dedicated to the selling of stolen data. An overview of their activity suggests their alignment with various causes, including pro-Palestine, pro-Russia, and other geopolitically aligned actors, often correlating with global events and conflicts. In this research, however, we deliberately refrained from focusing on the activity of these groups, including the geographical distribution of entities claimed by actors. Instead, we prioritize the investigation of the infrastructure involved in the operations of these groups, which lays the groundwork and provides a logical explanation of the cooperation between ransomware and hacktivist-like entities.

The integration of ransomware into hacktivist-like operations was publicly introduced in July 2023 through the announcement of a joint project, **StmX|GhostLocker**, between GhostSec and Stormous, declaring a ransomware/hacktivist alignment and pooling of resources. ***“We’re very proud to announce with our continuous work together the new blog that belongs to us, stormous, and the remaining partners.”***, a Ghost Telegram message said on August 20, 2023. On **May 15, 2024,** GhostSec announced that they would no longer participate in ransomware and shift back to pure hacktivism. ***“To be 100% clear all this means is our full focus and shift back into pure hacktivism/Political hacking.”***, they added in the following message.



GhostSec

We'd like to announce GhostSec's leave from the financial motivation "CyberCrime" Scene. We as Ghosts have obtained enough funding through our times to continue funding our operations for a while we deem the cybercrime and ransomware we once promoted no longer necessary and will shift back to pure hacktivism what does this mean?

All this means is that we will not be providing services anymore therefore the Ghostsec services channel and services once provided will be closed, The ransomware Ghostlocker will be closed Though we will provide the entire code of V3 to Stormous and shift all buyers from GL to the new Stormous locker making it a clean exit without any exit scam. Five families will be taken over and Stormous will be in charge with the new associates involved in that organization resulting in our complete retirement from the "cybercrime" and ransomware scene!

What will remain? At the moment we will continue to keep our private channel and chat room available and will be running a discount from today until may 23rd, Get lifetime access to the private channel and chat room for ~~$400~~ $250 ONLY until may 23rd. We may also plan soon to make and provide a hacking course/ package though we are still debating on making this hack like a ghost course.

Thank you for your constant support, love and understanding. We are very excited to continue and put all focus into our work in changing the world to becoming a better place!

Fight for something you believe in and truly find it for yourself. Chase your own freedom, dreams and goals. Then Pass it on to the future.

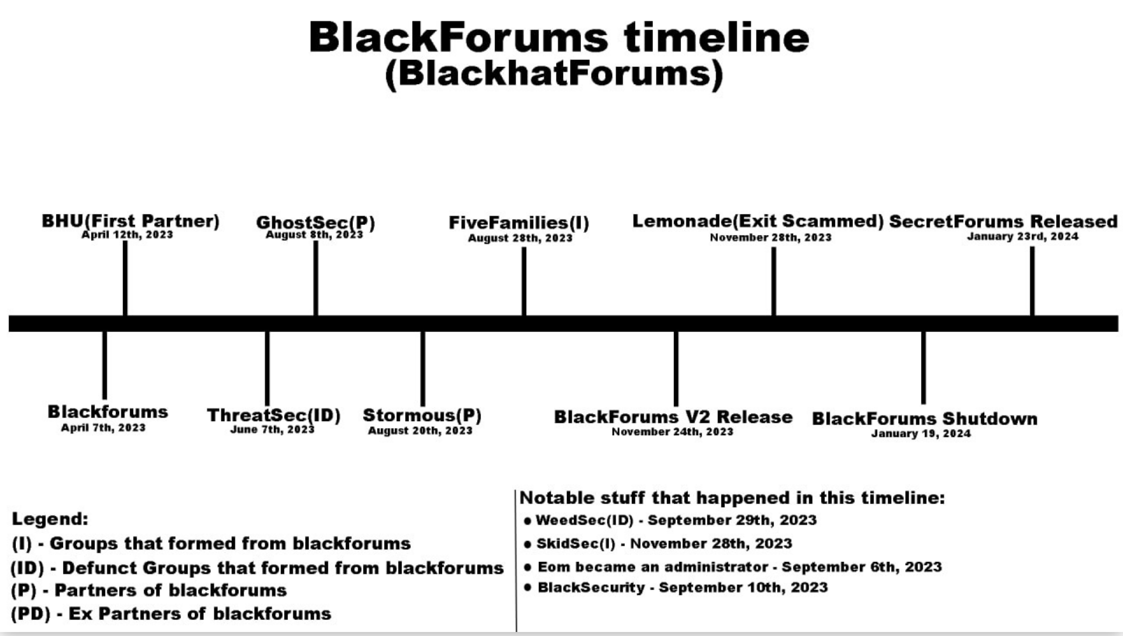
**Hack the planet!!**
We Run Shit Cause We Can!
~GhostSec0

*Figure 20: GhostSec posted a message announcing the ending their participation in ransomware*
*Source: Telegram*

This announcement is unsurprising considering the observed behavior of such hacktivist-like groups. This underscores a complex ecosystem where actors frequently launch new projects, shut down others, and announce new partnerships under different names. These maneuvers serve dual purposes: evading detection by researchers and law enforcement and projecting a larger community presence than what actually exists. This strategy also serves the purpose of obscuring the clear collaboration between ransomware groups that supply stolen data to these hacktivist-like entities.

When examining the operations of RansomHouse with its suspected relationships with Dark Angels, as well as Snatch and Stormous, we observe a well-structured model where resources are efficiently combined between groups and utilized across ransomware, influence operations camouflaged as hacktivism and data markets. Considering the ransomware operations involved, the presence of data markets is not coincidental, as it signifies a deliberate integration of ransomware into broader activities.

BlackForums, announced as a part of Five Families, operated from approximately April 2023 to January 2024, after which it was replaced by a new forum called **SecretForums**. The founder and admin, known by the alias “**Astounding**,” posted a detailed graph explaining the project’s evolution during its existence. ***“I wanted to give out a bit more of an insight to BlackForums and SecretForums so i have created a timeline (it isn’t the whole timeline). I made this for the new comers and OGs to see how we operated.”***, Astounding said on Telegram.

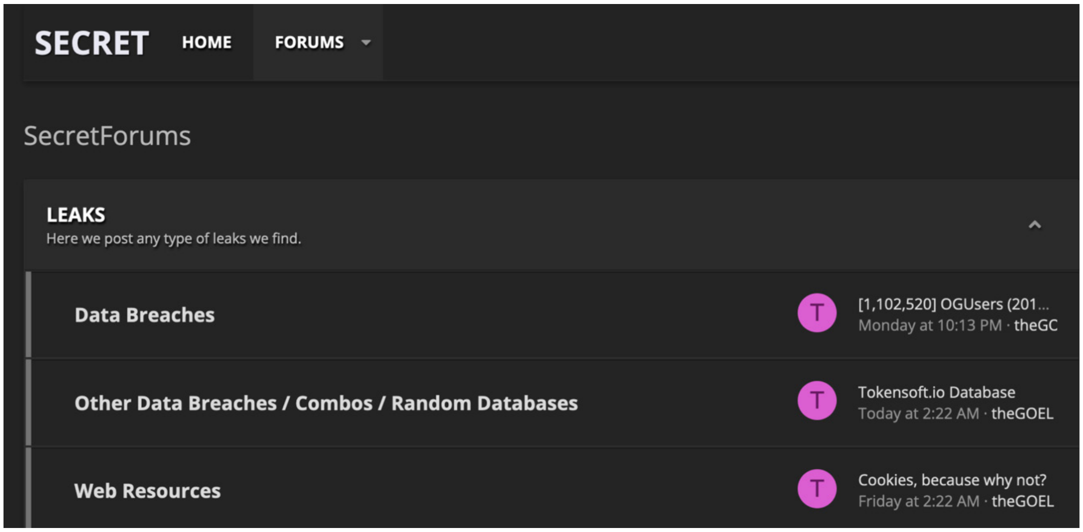


Legend:
(I) - Groups that formed from blackforums
(ID) - Defunct Groups that formed from blackforums
(P) - Partners of blackforums
(PD) - Ex Partners of blackforums

Notable stuff that happened in this timeline:
- WeedSec(ID) - September 29th, 2023
- SkidSec(I) - November 28th, 2023
- Eom became an administrator - September 6th, 2023
- BlackSecurity - September 10th, 2023

*Figure 21: A graph of BlackForum’s timeline of operations posted by its Admin Astounding*
*Source: Telegram*

The SecretForums, launched in January 2024, is currently active with approximately **4,364** registered members and a **total of 1,377 threads across various sections such as "Hacking," "Leaks," "Coding," "Marketplace," "Cracking," and "Social"** as of May 22, 2024. The involvement of data markets also highlights a particular framework in place, featuring data markets that not only secure additional ransomware revenue streams but also serve as a public justification for groups like Snatch and Stormous to claim ownership of data supposedly shared by other groups. While these groups present an illusion of open data access, the shared data is likely carefully curated to tailor information against specific entities of interest.



SecretForums

LEAKS
Here we post any type of leaks we find.

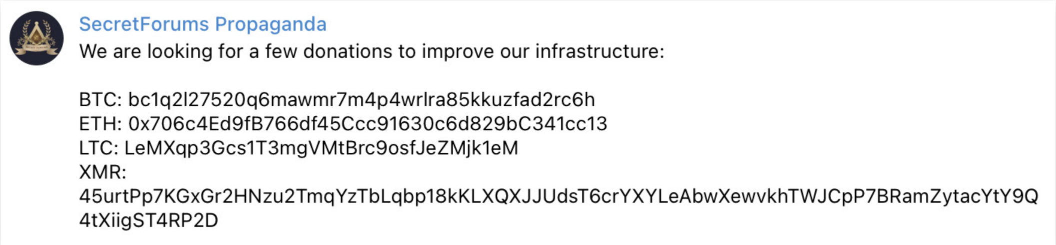
Data Breaches — [1,102,520] OGUsers (201... Monday at 10:13 PM · theGC

Other Data Breaches / Combos / Random Databases — Tokensoft.io Database Today at 2:22 AM · theGOEL

Web Resources — Cookies, because why not? Friday at 2:22 AM · theGOEL

*Figure22: SecretForums front page. Source: Analyst1*

Additionally, SecretForums maintains a presence on Telegram through its channel **"SecretForums Propaganda."** An ironic detail is the forum's attempt to solicit donations for their project despite the substantial revenue likely generated from selling stolen data. This gesture may not purely be driven by greed but rather an attempt to align with the perceived image of hacktivist-like groups that these modern Frankenstein ransomware/ hacktivist hybrids seem to embody.

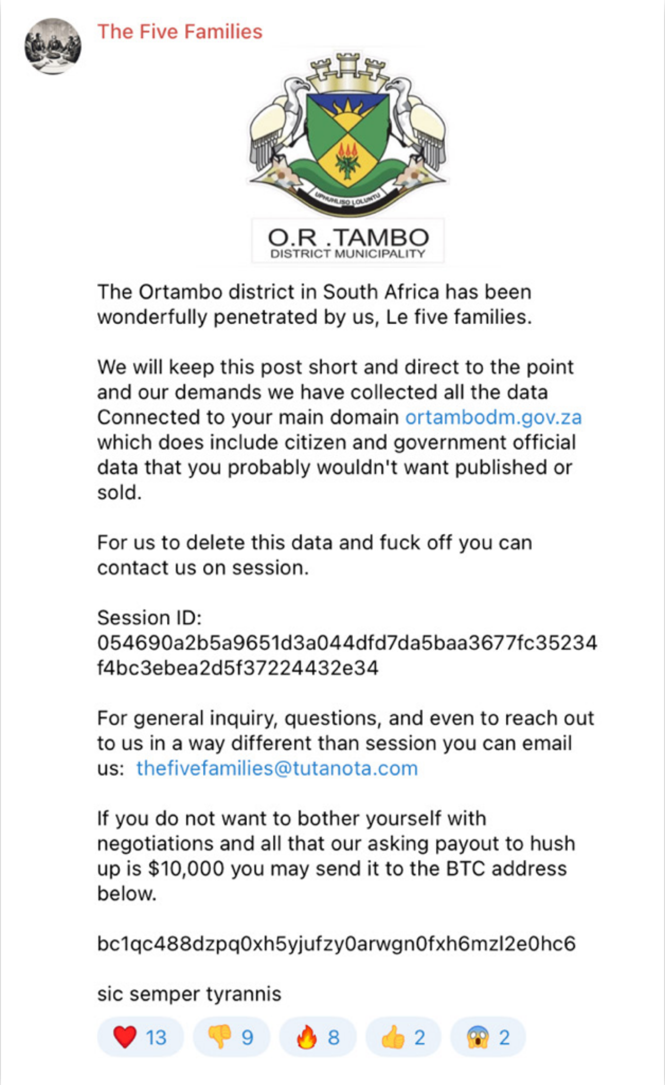


SecretForums Propaganda
We are looking for a few donations to improve our infrastructure:

BTC: bc1q2l27520q6mawmr7m4p4wrlra85kkuzfad2rc6h
ETH: 0x706c4Ed9fB766df45Ccc91630c6d829bC341cc13
LTC: LeMXqp3Gcs1T3mgVMtBrc9osfJeZMjk1eM
XMR:
45urtPp7KGxGr2HNzu2TmqYzTbLqbp18kKLXQXJJUdsT6crYXYLeAbwXewvkhTWJCpP7BRamZytacYtY9Q
4tXiigST4RP2D

*Figure 23: SecretForums actors providing cryptocurrency addresses in an attempt to solicit donations Source: Telegram*

This hacktivist-like behavior is not coincidental but rather a carefully planned strategy. Another example is a ransomware attack claimed by Five Families on September 29, 2023. Stating Ortambo district in South Africa as a victim, the actors asserted they had access to the data of its citizens and government officials. They demanded a ransom of USD 10,000, publicly sharing a BTC address for ransom. We emphasize the deliberate public sharing of a BTC address. In typical attacks, ransom addresses are kept private and shared with the victims in a closed chat. Exposing the address publicly indicates an attempt to garner attention and visibility rather than purely financial motivation.



The Five Families

The Ortambo district in South Africa has been wonderfully penetrated by us, Le five families.

We will keep this post short and direct to the point and our demands we have collected all the data Connected to your main domain ortambodm.gov.za which does include citizen and government official data that you probably wouldn't want published or sold.

For us to delete this data and fuck off you can contact us on session.

Session ID:
054690a2b5a9651d3a044dfd7da5baa3677fc35234f4bc3ebea2d5f37224432e34

For general inquiry, questions, and even to reach out to us in a way different than session you can email us: thefivefamilies@tutanota.com

If you do not want to bother yourself with negotiations and all that our asking payout to hush up is $10,000 you may send it to the BTC address below.

bc1qc488dzpq0xh5yjufzy0arwgn0fxh6mzl2e0hc6

sic semper tyrannis

❤️ 13 👎 9 🔥 8 👍 2 😱 2

*Figure 23: Five Families posted a message claiming the South African entity as a victim and demanding a ransom. Source: Telegram*

With this extensive activity, the question arises: what are these actors' motivations, and to whom can these groups be attributed? Let's analyze this in the next section.

# Attributing Ransomware/Hacktivist Activity: What Are Motivations?

Based on the observed activities, it is evident that these groups are attempting to present themselves as hacktivist organizations by adopting typical characteristics associated with hacktivist activities: making political statements, soliciting donations, maintaining a strong social media presence, and creating an illusion of a larger group to attract public engagement and influence public opinion.

The reality behind these operations likely involves a well-established workflow: initial ransomware attacks likely involve Dark Angels and RansomHouse acquiring data, which is then passed down the chain. Snatch and Stormous, evolving into hybrid ransomware/hacktivist groups, repurpose this data for covert influence operations under the guise of hacktivism.

In the graph below, we categorized groups based on their observed activities, suggesting that many may be subgroups of a larger entity. Dark Angels and RansomHouse are primarily classified as ransomware operators, while Snatch and Stormous are dual-labeled as both ransomware and hacktivist groups. By categorizing them as hacktivists, we highlight their distinctive approach, where influence operations are disguised under hacktivist-like activities.

The graph also illustrates Stormous's affiliation with recognized hacktivist groups as part of Five Families, which are involved in the joint StmX|GhostLocker ransomware project. Additionally, it identifies entities operating as Data Markets in two instances: BlackForums and SecretForums for Five Families and Ares Leaks and Database Cartel for RansomHouse.

Identifying a geopolitical alignment with a particular state is crucial to analyzing these groups' activities and predicting their operations' trajectory. Drawing upon our knowledge and investigation of these groups' activities, it's evident that many syndicates identified in cross-claims with RansomHouse, including Snatch and Stormous, are predominantly composed of Russian-speaking actors with a geopolitical alignment towards Russia.

Based on our previous research on Snatch, attribution analysis suggested they have roots in a Russian region for two primary reasons. Firstly, the group comprises Russian-speaking actors, as evidenced by the language used. Additionally, various artifacts point to this connection, such as using a command and control (C2) server hosted on a Russian

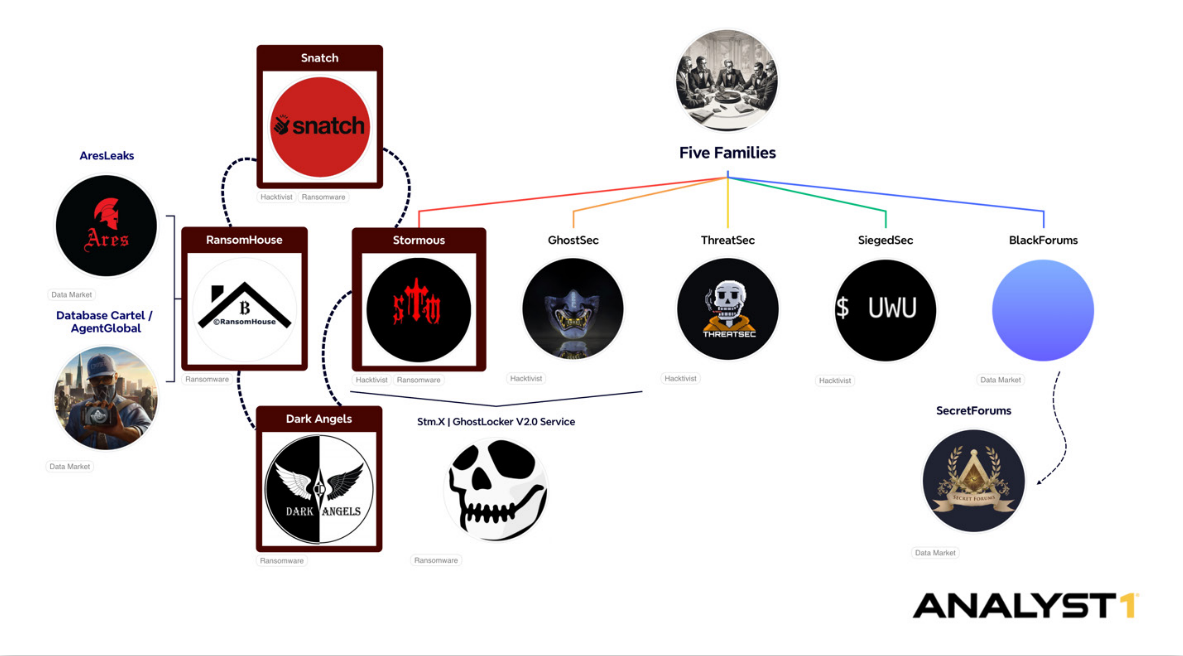
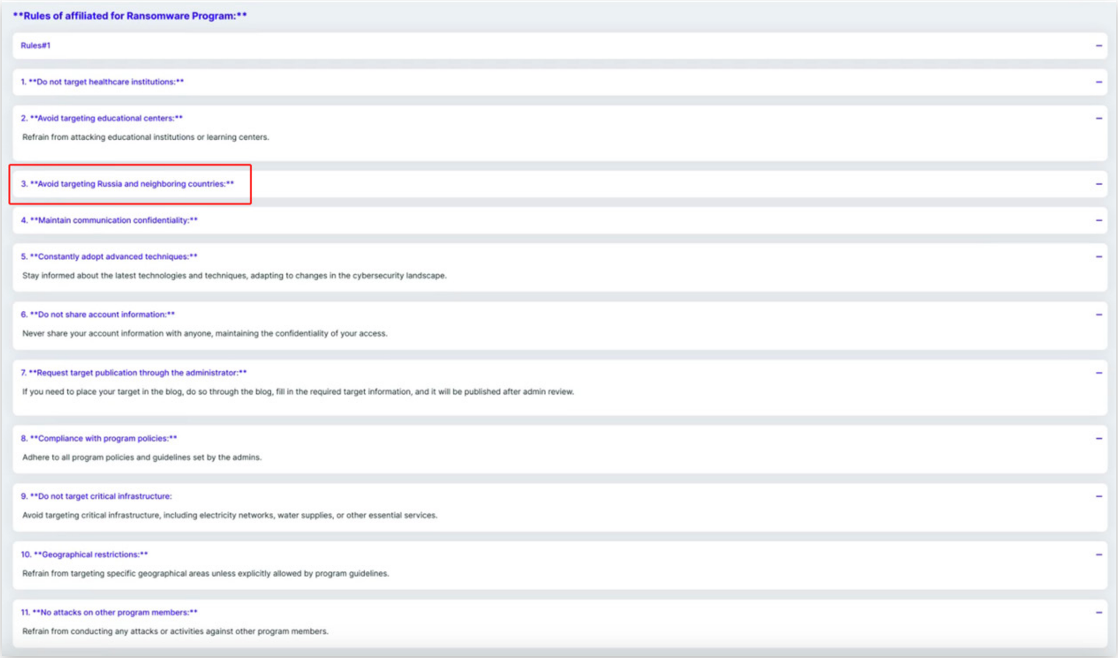


*Figure 24: Graph shows connections between groups with labels assigned as per their observed activities. Source: Analyst1*

bulletproof hosting service to execute attacks on their targets. Furthermore, according to a CISA report on the group, IP traffic analysis from event logs provided by victims indicates that Snatch establishes connections originating from servers based in Russia and through other virtual private network (VPN) services.

Similarly, in the case of Stormous, our investigation indicates a likely geopolitical alignment with Russia. Stormous, in particular, has always been vocal regarding its support of the Russian state. ***"We are designing our own ransomware (StormousX) which will be a corporate hell! Another point, we will launch our dark web site (.onion) this month. There is also a shop where we can sell the data of some important companies! Our own goals: America 80%, Ukraine 60%, India 58%, Peru 50%, Vietnam 12%)."***, reads a message posted on the Stormous Telegram channel on **July 2, 2022.** Among their affiliates, rules later listed on their DLS would include a warning not to attack Russia and Russia's neighboring countries, indicating a geopolitical alignment with the Russian state.

The increased use of social media is another tactic adopted by hacktivist-like groups, particularly with the emergence of hybrid operations by groups like Snatch and Stormous, which exhibit hacktivist-like activities alongside traditional ransomware operations. Many of these groups now maintain a robust presence on platforms such as Twitter (now known as X) and Telegram, using these channels to disseminate their messages and narratives, including information about victims and narratives that often involve victim blaming.



**Rules of affiliated for Ransomware Program:**

Rules#1

1. **Do not target healthcare institutions:**

2. **Avoid targeting educational centers:**
Refrain from attacking educational institutions or learning centers.

3. **Avoid targeting Russia and neighboring countries:**

4. **Maintain communication confidentiality:**

5. **Constantly adopt advanced techniques:**
Stay informed about the latest technologies and techniques, adapting to changes in the cybersecurity landscape.

6. **Do not share account information:**
Never share your account information with anyone, maintaining the confidentiality of your access.

7. **Request target publication through the administrator:**
If you need to place your target in the blog, do so through the blog, fill in the required target information, and it will be published after admin review.

8. **Compliance with program policies:**
Adhere to all program policies and guidelines set by the admins.

9. **Do not target critical infrastructure:
Avoid targeting critical infrastructure, including electricity networks, water supplies, or other essential services.

10. **Geographical restrictions:**
Refrain from targeting specific geographical areas unless explicitly allowed by program guidelines.

11. **No attacks on other program members:**
Refrain from conducting any attacks or activities against other program members.

*Figure 25: Affiliates rules of StormousX Raas partner program listed on Stormous' DLS*

*Source: Stormous DLS*

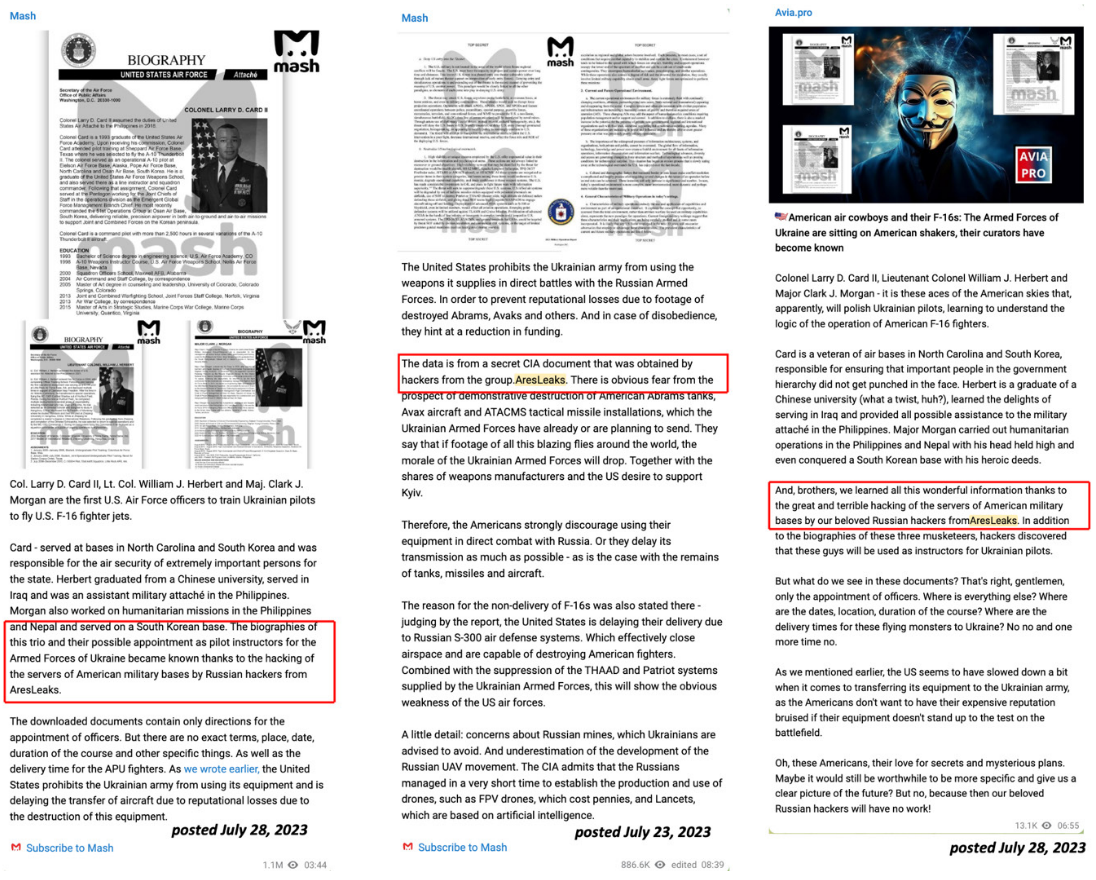
Analyzing these groups' activity across social media provides valuable insights into their alignment with particular states. Such geopolitical alignment can be explored by examining their portrayal by pro-Russian media and the narratives propagated therein. A closer examination involves tracking the frequency and amplification of content these hacktivist-like groups share within large pro-Russia news channels which are pivotal in amplifying narratives that align with Russia's geopolitical agenda.

The overall support by pro-Russia media for geopolitical agendas, particularly in contexts such as the Russia-Ukraine conflict, offers extensive justification for the state's actions. Telegram, in particular, has emerged as a significant communication channel, competing with traditional media and serving as a potent tool for disseminating narratives to the broader public. Pro-Russia channels disseminate messages portraying defenders against perceived enemies of the state, contributing to a wider narrative of resistance and defense aligned with Russia's interests.

In recent years, particularly since the invasion of Ukraine, these defenders also include Russian hackers, a phenomenon that has gained prominence within Russia since 2016 with allegations of involvement in the US election. Their positive image has increased significantly since the invasion of Ukraine, with their activities perceived as supporting the broader agenda of the Russian state. Pro-Russia media channels often portray hacker groups favorably, highlighting their actions as part of a larger struggle or defense against adversaries.

Channels like Mash (with approximately 2.9 million subscribers) and Avia Pro (with around 55 thousand subscribers) have included coverage of AresLeaks, a group announced as a partner by RansomHouse. These channels shared documents and details of sensitive information allegedly stolen from US government entities and individuals in claimed attacks in a series of messages.

***"Thanks to the hacking of American military base servers by Russian hackers from AresLeaks,"*** and "The data is from AresLeaks," ***"Brothers, we learned all this wonderful information thanks to the great and terrible hacking of the servers of American military bases by our beloved Russian hackers from AresLeaks"*** are among the messages shared by Mash and Avia Pro. These portrayals celebrate the hackers' actions, presenting them as uncovering valuable information and acting heroically to support Russia's interests.



Mash

Col. Larry D. Card II, Lt. Col. William J. Herbert and Maj. Clark J. Morgan are the first U.S. Air Force officers to train Ukrainian pilots to fly U.S. F-16 fighter jets.

Card - served at bases in North Carolina and South Korea and was responsible for the air security of extremely important persons for the state. Herbert graduated from a Chinese university, served in Iraq and was an assistant military attaché in the Philippines. Morgan also worked on humanitarian missions in the Philippines and Nepal and served on a South Korean base. The biographies of this trio and their possible appointment as pilot instructors for the Armed Forces of Ukraine became known thanks to the hacking of the servers of American military bases by Russian hackers from AresLeaks.

The downloaded documents contain only directions for the appointment of officers. But there are no exact terms, place, date, duration of the course and other specific things. As well as the delivery time for the APU fighters. As we wrote earlier, the United States prohibits the Ukrainian army from using its equipment and is delaying the transfer of aircraft due to reputational losses due to the destruction of this equipment.

***posted July 28, 2023***

Subscribe to Mash

1.1M 03:44

Mash

The United States prohibits the Ukrainian army from using the weapons it supplies in direct battles with the Russian Armed Forces. In order to prevent reputational losses due to footage of destroyed Abrams, Avaks and others. And in case of disobedience, they hint at a reduction in funding.

The data is from a secret CIA document that was obtained by hackers from the group.AresLeaks. There is obvious fear from the prospect of demonstrative destruction of American Abrams tanks, Avax aircraft and ATACMS tactical missile installations, which the Ukrainian Armed Forces have already or are planning to send. They say that if footage of all this blazing flies around the world, the morale of the Ukrainian Armed Forces will drop. Together with the shares of weapons manufacturers and the US desire to support Kyiv.

Therefore, the Americans strongly discourage using their equipment in direct combat with Russia. Or they delay its transmission as much as possible - as is the case with the remains of tanks, missiles and aircraft.

The reason for the non-delivery of F-16s was also stated there - judging by the report, the United States is delaying their delivery due to Russian S-300 air defense systems. Which effectively close airspace and are capable of destroying American fighters. Combined with the suppression of the THAAD and Patriot systems supplied by the Ukrainian Armed Forces, this will show the obvious weakness of the US air forces.

A little detail: concerns about Russian mines, which Ukrainians are advised to avoid. And underestimation of the development of the Russian UAV movement. The CIA admits that the Russians managed in a very short time to establish the production and use of drones, such as FPV drones, which cost pennies, and Lancets, which are based on artificial intelligence.

***posted July 23, 2023***

Subscribe to Mash

886.6K edited 08:39

Avia.pro

**🇺🇸American air cowboys and their F-16s: The Armed Forces of Ukraine are sitting on American shakers, their curators have become known**

Colonel Larry D. Card II, Lieutenant Colonel William J. Herbert and Major Clark J. Morgan - it is these aces of the American skies that, apparently, will polish Ukrainian pilots, learning to understand the logic of the operation of American F-16 fighters.

Card is a veteran of air bases in North Carolina and South Korea, responsible for ensuring that important people in the government hierarchy did not get punched in the face. Herbert is a graduate of a Chinese university (what a twist, huh?), learned the delights of serving in Iraq and provided all possible assistance to the military attaché in the Philippines. Major Morgan carried out humanitarian operations in the Philippines and Nepal with his head held high and even conquered a South Korean base with his heroic deeds.

And, brothers, we learned all this wonderful information thanks to the great and terrible hacking of the servers of American military bases by our beloved Russian hackers fromAresLeaks. In addition to the biographies of these three musketeers, hackers discovered that these guys will be used as instructors for Ukrainian pilots.

But what do we see in these documents? That's right, gentlemen, only the appointment of officers. Where is everything else? Where are the dates, location, duration of the course? Where are the delivery times for these flying monsters to Ukraine? No no and one more time no.

As we mentioned earlier, the US seems to have slowed down a bit when it comes to transferring its equipment to the Ukrainian army, as the Americans don't want to have their expensive reputation bruised if their equipment doesn't stand up to the test on the battlefield.

Oh, these Americans, their love for secrets and mysterious plans. Maybe it would still be worthwhile to be more specific and give us a clear picture of the future? But no, because then our beloved Russian hackers will have no work!

13.1K 06:55

***posted July 28, 2023***

*Figure 26: Messages mentioning Ares leaks posted by major pro-Russian Telegram media channels*

*Source: Telegram*

The question of state involvement remains uncertain and requires additional strong evidence to make a definitive judgment. However, considering the overall observed activity, including the visible presence of substantial resources and high levels of coordination that align with the Russian state's broader geopolitical agenda, it is likely possible.

The alignment of their activities with state objectives, the support from pro-Russian media channels, and the historical precedent of state-supported cyber activities all point towards the likelihood of potential state involvement. As such, understanding the potential state backing behind these groups is crucial for developing effective countermeasures and mitigating the impact of their operations.

# Conclusion

The analysis of data sharing among ransomware groups highlights the emergence of new challenges in cybersecurity. Traditionally, ransomware attacks involve encryption and data exfiltration, with some cases involving data theft without encryption. However, the collaboration among groups like RansomHouse, Dark Angels and others introduces a novel approach where stolen data is recycled among threat actors, leading to deceptive extortion attempts that simulate new attacks. This phenomenon underscores the importance for organizations to enhance their cybersecurity measures to protect against initial breaches and mitigate the risks posed by subsequent misuse of stolen data.

Moreover, the involvement of groups like Snatch and Stormous in influence operations, camouflaged under the guise of hacktivism, adds another layer of complexity. These operations target sensitive data and aim to manipulate public opinion and influence geopolitical narratives. Defending against these threats requires a comprehensive approach that includes robust cybersecurity defenses, rigorous data protection protocols, and strategic responses to mitigate reputational damage at both governmental and individual levels.

Addressing these challenges will necessitate collaboration between cybersecurity experts, law enforcement agencies, and policymakers to develop effective strategies that can adapt to the evolving tactics of ransomware and hacktivist-like groups. Organizations can better safeguard their data, integrity, and resilience in an increasingly digital and interconnected world by understanding and countering these sophisticated threats.

## ABOUT US:

**Analyst1**, engineered by cyber threat analysts, offers an enterprise-scale platform that operationalizes threat intelligence and enables security teams and analysts to focus on deeper analysis and response. With **Analyst1**, organizations gain visibility into advanced persistent threats attempting to infiltrate their networks.

@UseAnalyst1 **analyst1.com/blog**

Any technical information that is made available by Analyst1 is the copyrighted work of Analyst1 and is owned by Analyst1.

NO WARRANTY . The technical information is being delivered to you as is and Analyst1 makes no warranty as to its accuracy or use. Any use of the technical documentation or the information contained herein is at the risk of the user. Documentation may include technical or other inaccuracies or typographical errors. Analyst1 reserves the right to make changes without prior notice.