ANALYST1®

RANSOMWARE GOES POLITICAL

and Other Extortion Activity of 2023

By Anastasia Sentsova

Contents

Executive Summary

- Double-extortion tactics employed by ransomware actors involve threatening to leak claimed stolen data to pressure the victim into paying a ransom. This report uncovers insights into the extortion activity in 2023, incorporating data observed across Data Leak Sites (DLS) and human-driven techniques used by actors.
- For our statistial analysis of DLS activity, we include data observed from DLS in both 2023 and 2022. In our report "**claim**" is referred to as an event of a company name being published on DLS.
  - The number of claims in **2023** increased by nearly **73%** compared with **2022** (4,**611** and 2,**662** respectively).
  - The United States is leading by the number of claims by **47%** in **2023**. It seems to be a recurring trend when compared with **2022** when the US took nearly **41%** of total claims.
  - **LockBit 3.0, AlphVM/BlackCat, CLOP, PLAY, 8BASE, Black Basta, Akira, Medusa, BianLian**, and **Royal** are the top 10 groups responsible for nearly **70%** of total claims. Among these, the top 3 groups are LockBit 3.0 (**1,038** claims), AlphVM/BlackCat (**422** claims), and CLOP (**386** claims).
- In 2023, a new human-driven extortion tactic emerged, exemplified by AlphVM/BlackCat filing claims with the Security Exchange of Commissions (SEC) to report breached victims allegedly non-compliant with the law. This tactic aims to increase pressure on victims and sow fear among potential targets. We assess that this tactic will likely persist in 2024.
- In addition, we've witnessed the emergence of groups whose actions appear more aligned with influence operations than traditional ransomware activities, which we highlight in our case study of Snatch. Our analysis reveals that this group operates Telegram channels, primarily targeting English-speaking audiences from Europe and the United States. They utilize data claimed to be stolen from breaches conducted by other syndicates to propagate a narrative of inadequate protection practices by businesses associated with these regions. Moreover, these actors employ derogatory language when referencing governments and government officials, aiming to undermine their credibility.

In a time of multiple ongoing military conflicts such as Russia–Ukraine and Palestine–Israel, these actions contribute to the actors' intentions of manipulating the informational landscape. Constant monitoring of such activity is essential to identify influence operations attempts and address them with strategic planning.

Introduction

Ransomware activity persisted as a major concern throughout 2023, marked by a series of high-profile attacks worldwide. Addressing ransomware threats presents multifaceted challenges, both in technical defense as well as adapting to the constantly evolving, human-driven extortion strategies employed by attackers. This report provides a detailed analysis of both quantitative and qualitative analysis, of the extortion activities observed in 2023.

The "**Double-Extortion**" technique, popularized among ransomware actors since 2020, remains widespread. This tactic is exerted through the threat of publishing the victim's stolen data on a so-called Data Leak Site (DLS) to force the entity into paying a ransom.

While actors use various platforms such as Telegram for data leaks, dedicated DLS continue to remain prevalent. In our analysis of DLS, we deliberately remove the word "**ransomware attack**" from our vocabulary and replace it with "**claim**." Removing the term is a methodological choice aimed at ensuring accuracy and objectivity, treating actors' statements as claims until the ransomware attack is officially confirmed. Our 2023 analysis includes a statistical summary of activity observed across DLS, alongside comparative data from previous years, highlighting the number of claims, including the most impacted countries, and the top 10 syndicates.

Actors constantly evolve and adapt, employing novel, human-driven strategies to intensify their extortion campaigns. Previously, actors relied on psychological manipulation — blaming victims for breaches due to the lack of protection of their network. Moreover, they targeted individuals associated with victims by direct contact or releasing personal information. In 2023, they took this further by weaponizing legal frameworks against victims. For instance, AlphVM/BlackCat filed claims with the SEC to report victims who failed to notify about a breach as required by law, according to threat actors.

The year 2023 also demonstrated a substantial shift in motivation, moving away from purely monetary gain to the intention of influencing political outcomes. This trend is particularly noticeable in the context of ongoing military conflicts such as those related to

Palestine-Israel and Russia-Ukraine. We've observed the rise of groups whose activities seem to resemble influence operations more than traditional ransomware activities we're familiar with. To illustrate these tactics and techniques, we provide a case study focusing on the Snatch group.

Analyst1 aims to contribute to a safer digital space. We believe that our findings will be valuable to the general public as well as decision-makers who seek to protect their assets and combat ransomware threats effectively.

Data Leak Sites, 2023 Facts & Numbers

This section includes a statistical summary of activity observed across DLS in 2023, alongside comparative data from previous years, highlighting the number of claims, including the most impacted countries, and the top 10 syndicates.

When analyzing a DLS or any other platforms that actors use for data leaks, it is crucial to use clear and objective vocabulary and avoid making statements that confirm ransomware attacks solely based on the appearance of an entity's name on these sites. **To keep ransomware attack statistics accurate, we refer to the term "claim" as an event where the company's name is being published on a DLS.**

Number of Claims Increased by 73% in 2023

The number of claims in **2023** increased by nearly **73%** compared with **2022** (**4,611** and **2,662** respectively). **LockBit 3.0, AlphVM/BlackCat, CLOP, PLAY, 8BASE, Black Basta, Akira, Medusa, BianLian and Royal** are top 10 groups responsible for nearly **70%** of total claims (see further analysis in the section below).

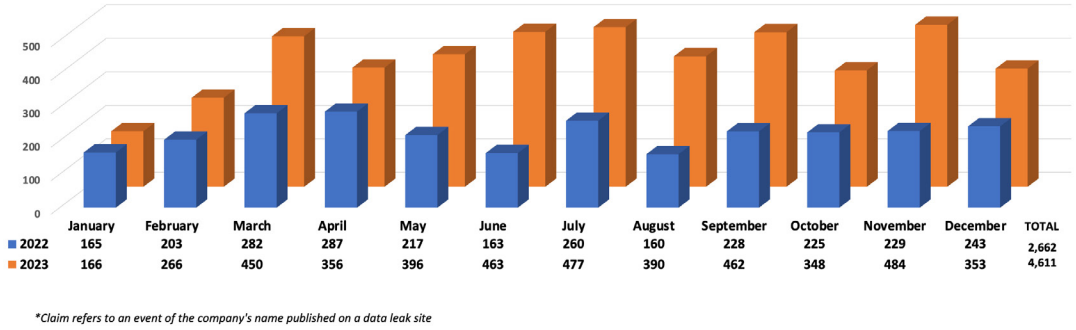
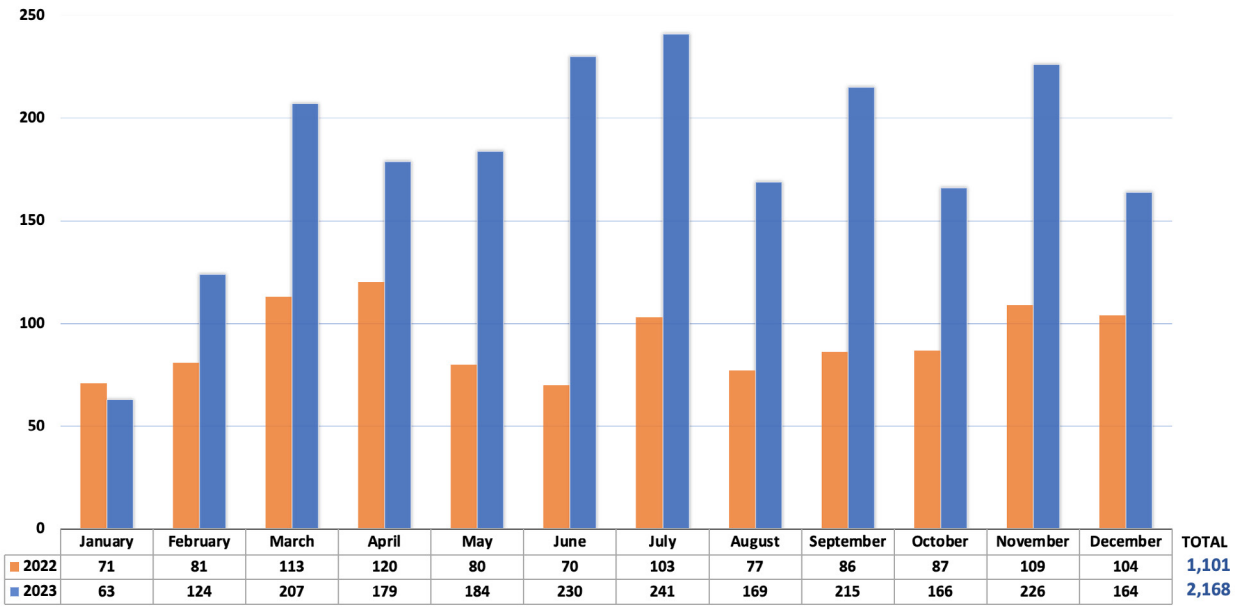


Figure 1: Graph shows monthly distribution of claims for 2022 – 2023
Graph: Analyst1 / Data Source: ecrime.ch

The United States is the Most Affected Country Leading by 47%

The United States is leading by the number of claims taking nearly **47%** of total claims in **2023**. It seems to be a recurring trend when compared to **2022** when the US took nearly **41%** of total claims.

- Top 10 groups that claimed the United States as a victim:
  - **LockBit 3.0** — 393 claims
  - **CLOP** — 235 claims
  - **AlphVM/BlackCat** — 222 claims
  - **PLAY** — 168 claims
  - **Black Basta** — 116 claims
  - **Akira** — 111 claims
  - **8BASE** — 105 claims
  - **BianLian** — 88 claims
  - **Royal** — 86 claims
  - **Medusa** — 52 claims



	January	February	March	April	May	June	July	August	September	October	November	December	TOTAL
2022	71	81	113	120	80	70	103	77	86	87	109	104	1,101
2023	63	124	207	179	184	230	241	169	215	166	226	164	2,168

Figure 2: Graph shows monthly distribution by claims for United States in 2022 – 2023
Graph: Analyst1 / Data Source: ecrime.ch

Top 10 Groups Drive Nearly 70% of Activity of Total Claims

LockBit 3.0 is the most active group by the number of claims leading by nearly **22%** (1,038 claims) and followed by AlphVM/BlackCat (**9%** or **422** claims) and CLOP (**8%** or **386** claims).

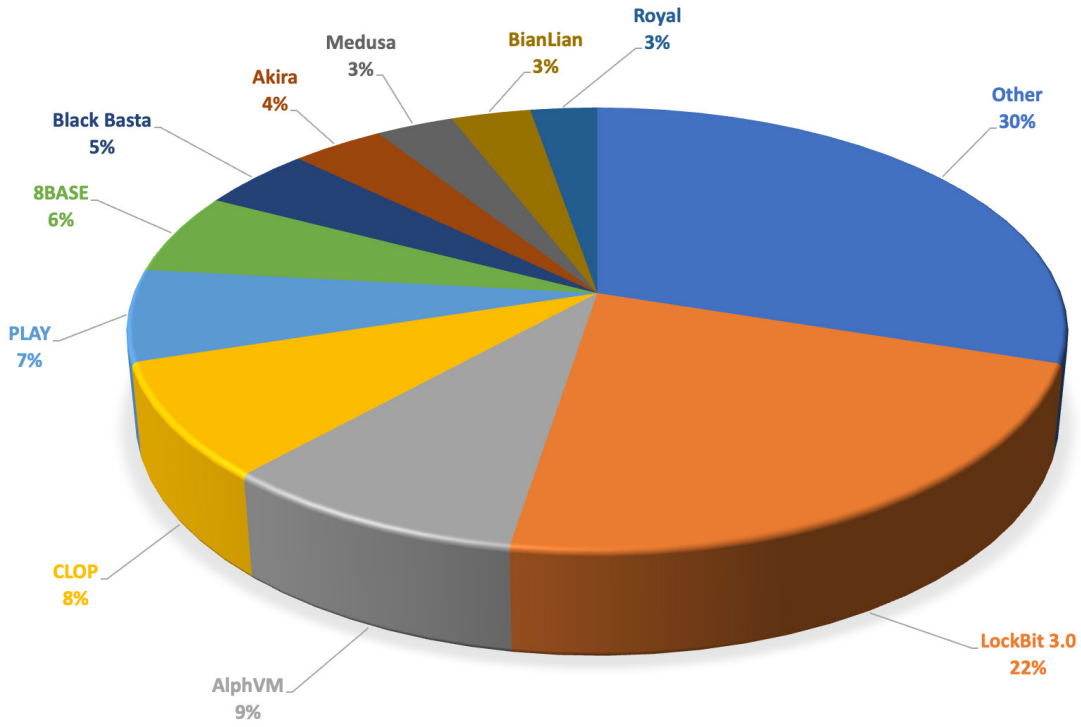


Figure 3: Graph shows distribution of claims across top 10 groups
Graph: Analyst1 / Data Source: ecrime.ch

The analysis of data leak sites is complex, particularly when there is a lack of official confirmation from entities that are claimed to be victims. It is also important to remember that even if actors' claims are confirmed, these numbers only represent a fraction of ransomware attacks, as many of them go unreported. As we delve deeper into this report, we will highlight instances where ransomware groups have made false attack claims, emphasizing the importance of maintaining a clear vocabulary when analyzing data leaks sites. This practice ensures we convey information without contributing to the narrative crafted by ransomware actors.

We will now direct our attention towards human-driven extortion techniques that actors employ to secure ransom payments. By exploring these techniques, we aim to show the intricacies of how actors exploit psychological and strategic elements to achieve their extortion objectives and gain deeper insights into the evolving landscape of ransomware.

Double Extortion. Psychological Games.

Ransomware actors use a variety of human-driven extortion tactics which involve calculated psychological and strategic planning to intensify extortion campaigns. Understanding these tactics is critical for establishing an effective strategic response. In this section, we will review previously utilized tactics that continue to be prevalent among actors. These tactics include 1) attributing blame to victims by highlighting their network's perceived protection inadequacies and 2) targeting individuals associated with victims by direct contact or releasing personal information. Additionally, we will analyze a newly adapted tactic by AlphVM/BlackCat, who seek to manipulate a legal framework to embarrass and pressure their victims. This is exemplified by their filing of claims with the SEC to report victims they claimed to breach, asserting non-compliance with the law.

1. Name and Blame

Ransomware actors often call their data leak sites "**wall of shame**", employing this deliberate tactic to exert pressure on victims. By doing so actors try to shift the blame onto the targeted companies by accusing them of lack of protection, thereby diverting attention from the actors' own criminal actions.

The use of explicit and derogatory language such as referring to their victims as "***customers***" or referring to attack as "***forced unscheduled audit of network vulnerabilities***", is a psychological tactic aimed at intimidating and emotionally manipulating affected entities into compliance. By leveraging these tactics, ransomware actors aim to create an environment where the victims feel compelled to act swiftly and comply with ransom demands to avoid reputational damage.

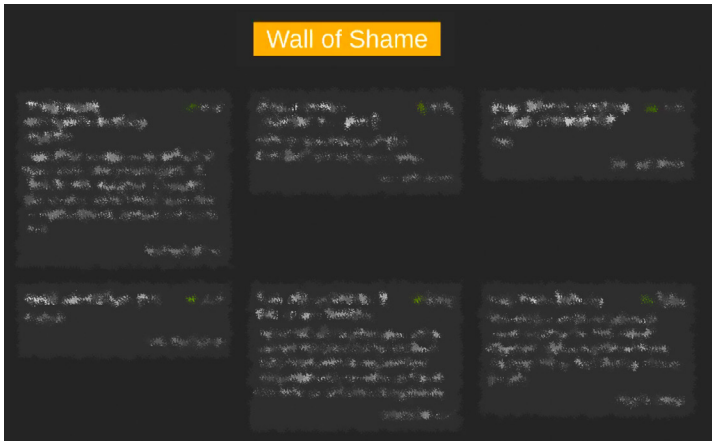


Figure 4: Monti Data Leak Site Shows the list of victims with a "Wall Shame" sign on top
Source: Analyst1

> *"The best thing you can do is to follow our instructions to get back to your daily routine, by cooperating with us you will minimize the damage that might be done. Those who choose different path will be shamed here publicly," reads Akira's data leak site.*

The message by Akira is a good example of coercive tactics used by actors. By suggesting that cooperation is the best route to minimize potential damage, they create an urge and a narrative where compliance with their demands seems like the only option. The language employed, such as "get back to your daily routine" points to the urgency of restoring operations disrupted by actors. Meanwhile, the implicit threat of public shaming adds to the psychological pressure.

Figure 5: Akira site reflect a "welcome" message with threats against victims in a case of non-compliance. Source: Analyst1

2. Make It Personal

Breached companies aren't the only ones bearing the costs of attacks. In efforts to escalate pressure, actors reach out to entities associated with the victim, including partners, customers, and employees. This tactic serves two main reasons: Firstly, it exerts pressure on the victims by leveraging stolen personal data, which legally holds breached companies accountable. Secondly, it aims to amplify the attack's visibility and publicity. This approach not only increases the pressure on the victim but also broadens the scope and impact of the breach, amplifying its consequences.

> *"Below is the list of companies that either have considered their financial gain to be above the interests of their partners/individuals who have entrusted their data to them or have chosen to conceal the fact that they have been compromised," says 8BASE's data leak site.*

This crafted message devised by actors aims to emphasize the victim's accountability for data privacy and security.

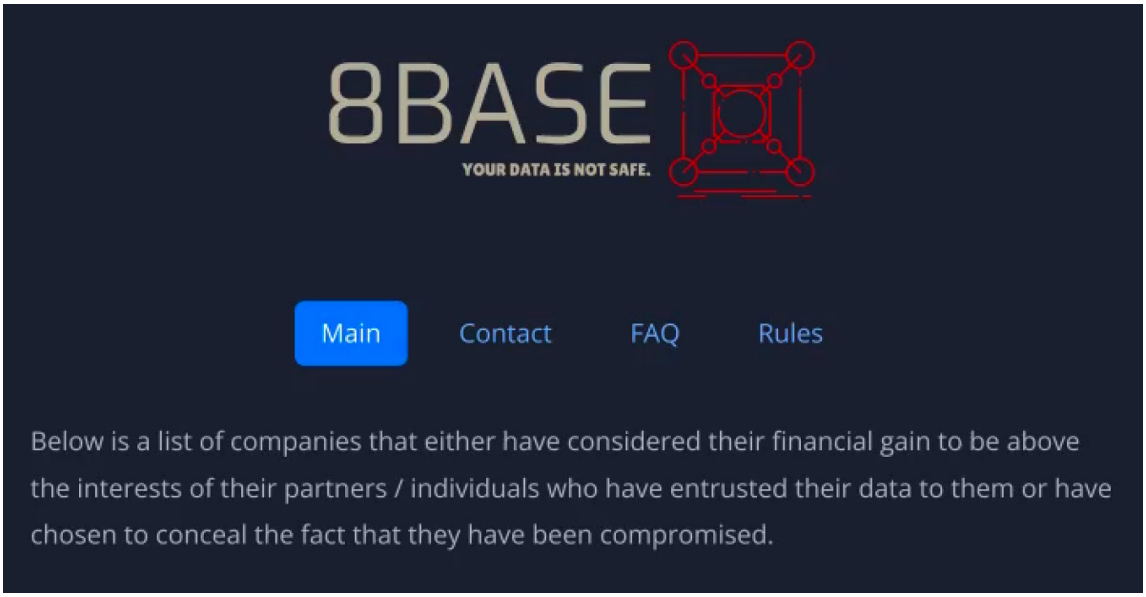


Figure 6: 8BASE site displays the message pointing to the victim's accountability for data privacy. Source: Analyst1

In many instances, actors go a step further by directly referencing associated entities on their data leak sites by publishing pieces of stolen PII (Personal Identifiable Information) like we see in the below example of Monti actors posting an individual's SSN on their data leak site.

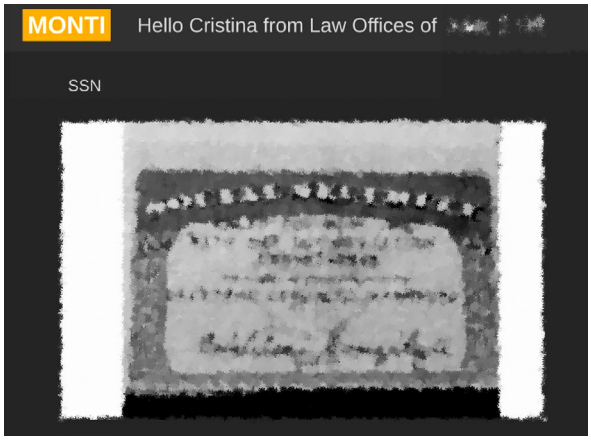


Figure 7: Monti actor post SSN of an entity associated with the breached company on its data leak site to intimidate the victim. Source: Analyst1

3. Threaten by Legal Consequences — Pay to Get Away

As the ransomware threat evolves, so does the legal framework surrounding it. Regulations differ across jurisdictions but share the common objective: to oversee data privacy and safeguard shareholders' rights. Businesses understand the potential legal ramifications of data breaches, and ransomware actors are equally aware. Deliberately selecting sensitive personal information during the exfiltration phase, actors will later use it to manipulate the victim.

One notable incident we observed in 2023 involved AlphVM/BlackCat filing complaints with the Security and Exchange Commission (SEC).

> *"Despite the significant cybersecurity disclosure requirements set forth by the Security and Exchange Commission (SEC), **victim** (name redacted) failed to promptly report a material cybersecurity incident involving patient data as mandated. To address the new criteria for a persons reporting an incident, an employee of **victim** has agreed to file a report after a productive talk with his family," reads AlphVM/BlackCat post on its data leak site.*

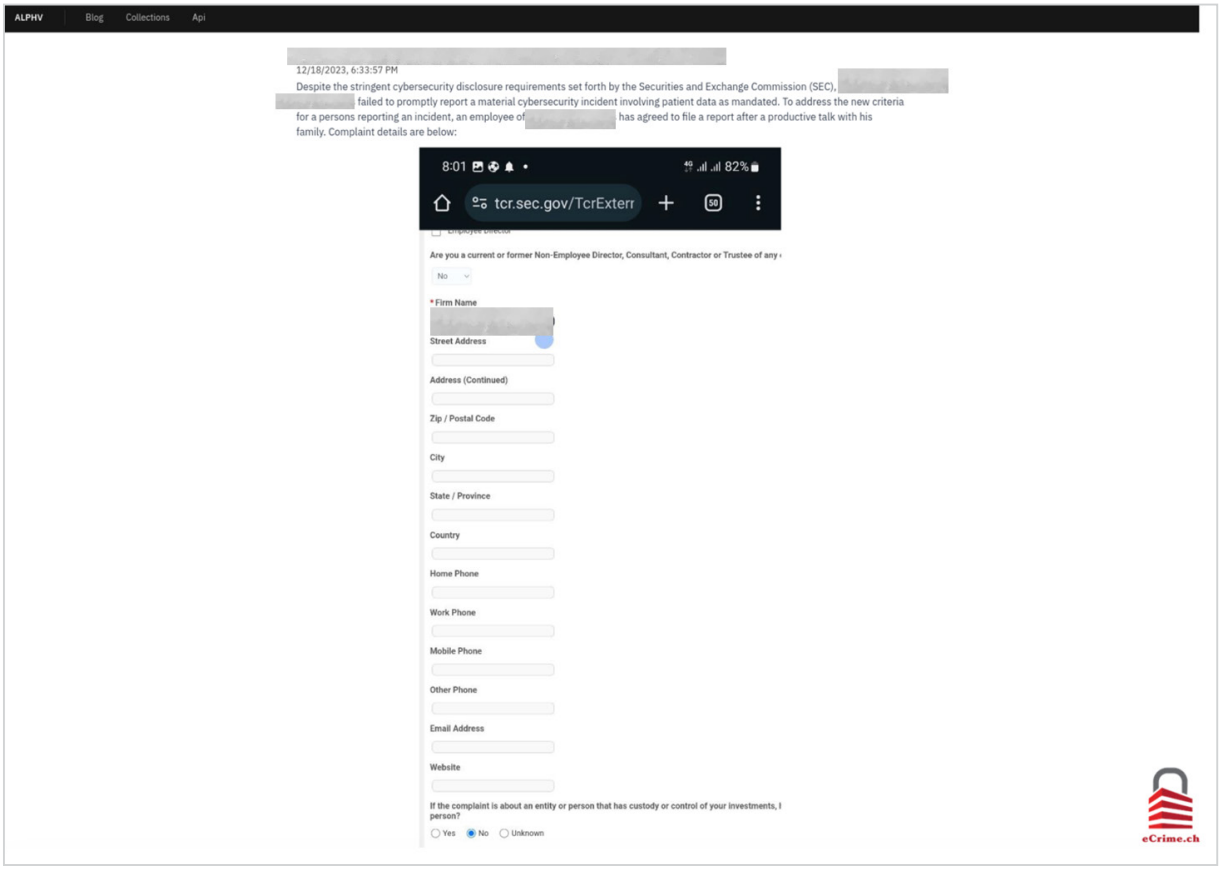


Figure 8: AlphVM/BlackCat posted a message about submitting to the SEC for one of its claimed victims and attached a screenshot as a proof in its submission. Source: ecrime.ch

This move was prompted by a recently established requirement by the SEC, which came into effect on December 18, 2023, mandating that public companies must report cybersecurity incidents. This tactic is used by actors to set a public example for their future victims and is also as an attempt to increase the visibility and publicity of an attack. We assess that this tactic will likely persist in 2024.

Referring to legal obligations itself isn't a novel tactic; we've seen it before. For instance, the GDPR, a legal framework that imposes obligations on European entities regarding data privacy violations, is frequently cited by actors in their threats. Below is another example of LockBit 3.0 weaponizing laws against victims by threatening them with legal repercussions. "***You will receive fines from the government such as the GDPR and many others, you can be sued by customers of your firm for leaking information that was confidential,***" reads a LockBit 3.0 ransom note. To further intensify pressure, ransomware actors point to the potential consequences of data leaks.

This note also serves as a great example of the behind-the-scenes activities in which ransomware actors engage. Ransom payments are not the sole revenue stream derived from attacks. Even if actors assure the deletion of stolen data upon ransom payment, they will likely repurpose it for various types of cybercrime. As perfectly detailed by LockBit actors themselves, these activities include 1) leveraging employees' data for social engineering and future re-infiltration of victim's network 2) using data for identity theft, creating fake profiles to "KnowYourCustomer" (KYC) procedures on exchanges in support of money laundering efforts and engaging in financial fraud, such as loan applications.

When facing ransomware attacks and extortion attempts, it is critical to have an established and effective strategic response. This plan serves as a guiding framework, offering a structured approach to navigate the complexities of the incident. During the extortion phase, regaining control over the network and maintaining coherence among the affected team and decisionmakers is crucial. While threat actors aim to create chaos and push victims into making a rash decision and paying the ransom, the primary goal for the victim should be to remain composed.

Confirming the occurrence of a breach is one of the most crucial aspects when mitigating an incident. The ever-changing landscape of ransomware requires a nuanced approach, considering the possibility that actors might engage in deception through false claims. As we transition to the next section of this report, we will illustrate an instance where a ransomware group makes false claims of a ransomware attack by using previously stolen data from other syndicates. This example underscores the need for organizations to exercise vigilance and conduct thorough verifications before taking any responsive actions.

```
>>>>> What are the dangers of leaking your company's data.

First of all, you will receive fines from the government such as the GDRP and many
others, you can be sued by customers of your firm for leaking information that was
confidential. Your leaked data will be used by all the hackers on the planet for
various unpleasant things. For example, social engineering, your employees'
personal data can be used to re-infiltrate your company. Bank details and
passports can be used to create bank accounts and online wallets through which
criminal money will be laundered. On another vacation trip, you will have to
explain to the FBI where you got millions of dollars worth of stolen
cryptocurrency transferred through your accounts on cryptocurrency exchanges. Your
personal information could be used to make loans or buy appliances. You would
later have to prove in court that it wasn't you who took out the loan and pay off
someone else's loan. Your competitors may use the stolen information to steal
technology or to improve their processes, your working methods, suppliers,
investors, sponsors, employees, it will all be in the public domain. You won't be
happy if your competitors lure your employees to other firms offering better
wages, will you? Your competitors will use your information against you. For
example, look for tax violations in the financial documents or any other
violations, so you have to close your firm. According to statistics, two thirds of
small and medium-sized companies close within half a year after a data breach. You
will have to find and fix the vulnerabilities in your network, work with the
customers affected by data leaks. All of these are very costly procedures that can
exceed the cost of a ransomware buyout by a factor of hundreds. It's much easier,
cheaper and faster to pay us the ransom. Well and most importantly, you will
suffer a reputational loss, you have been building your company for many years,
and now your reputation will be destroyed.
```

Figure 9: LockBit Ransom Note referring to legal consequences in case of non-compliance
Source: ransomware.live

Evolving from Monetary to Political Motivations. Snatch Case Study.

In 2023, we observed a shift among Russian-speaking ransomware groups' operations, indicating an alignment aimed at influencing political outcomes rather than solely seeking monetary gain. This trend became especially noticeable amid ongoing military conflicts such as those related to Palestine–Israel and Russia–Ukraine.

When analyzing ransomware, it's evident that groups, especially Russian-speaking syndicates, aren't entirely apolitical. For instance, actors' target preferences and the unspoken rule of not attacking CIS (Commonwealth of Independent States) suggest the actors' adherence to certain guidelines that align with the Russian state and its political agenda.

The first significant confirmation of an actor's political stance and alignment with a state occurred in February 2022. This was during the initial stages of Russia's invasion of

Ukraine when Conti, the leading group at that time, publicly announced its support for the Russian state. In response, an unknown individual leaked internal information linked to the group's operations. Following the statement, Conti refrained from issuing further announcements. Shortly after the leak, the group underwent rebranding into multiple groups and continued its extortion activities, with a focus on monetary gain.

When analyzing Russian-speaking ransomware landscape, it is crucial to acknowledge that specific state involvement is highly likely but remains unconfirmed. In addition, the behaviors of actors within Russian-speaking underground are naturally influenced by the multinational nature of this community. Primarily consisting of individuals from countries within the former Soviet Union regions where Russian language is historically spoken. This diversity encompasses a range of national and cultural backgrounds and might include a spectrum of political views among the actors. The varied perspectives among these actors highlight the complex and multifaced nature of their motivations and operations.

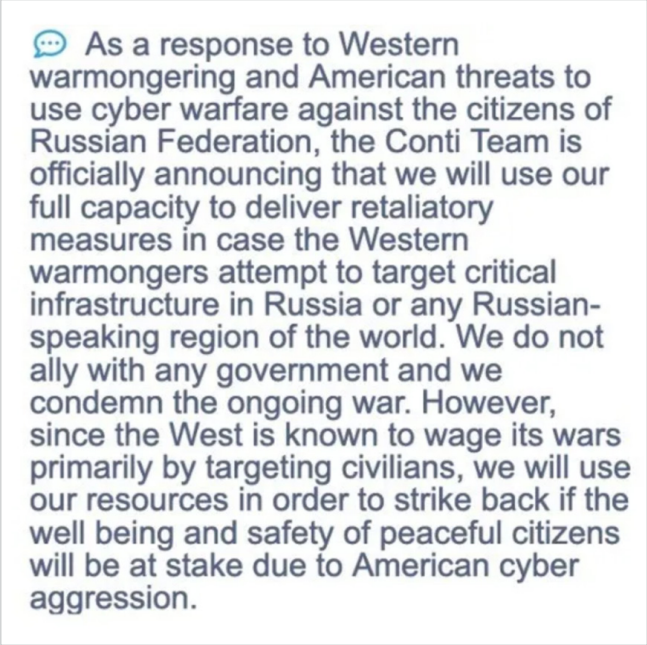


Figure 10: Conti announcement of supporting Russian State
Source: Analyst1

Snatch Case Study

Snatch is a noteworthy example in the realm of ransomware in showcasing the evolution of primary motivation. The group has undergone notable changes over its years of existence. Beginning its operations around 2018, the group initially followed the traditional Ransomware-as-a-Service (RaaS) model. According to a CISA report, originally

the group was referred to as Team Truinger, based on the moniker of a former GandCrab syndicate, a predecessor of notorious REvil group responsible for the supply-chain attack on Kaseya in June of 2021.

Our attribution analysis of Snatch suggests they have roots to a Russian region based on two aspects. Firstly, the group is comprised of Russian-speaking actors, evident from the language spoken. Additionally, several artifacts point to this connection, including the use of a command and control (C2) server located on a Russian bulletproof hosting service to launch attacks on their victims. Moreover, a CISA report on the group notes that, based on IP traffic from event logs provided by victims, Snatch initiates connections from the Russia-based server and through other virtual private network (VPN) services.

Snatch actors operate data leak site, which they utilize to support the double-extortion technique. Over the past three years, the group has claimed **127** victims, consisting of **24** in **2021**, **39** in **2022**, and **64** in **2023**. When compared to other syndicates, however, Snatch's activity appears to have a comparatively lower volume. In 2023 alone, the group didn't even rank among the top 20 most active groups.

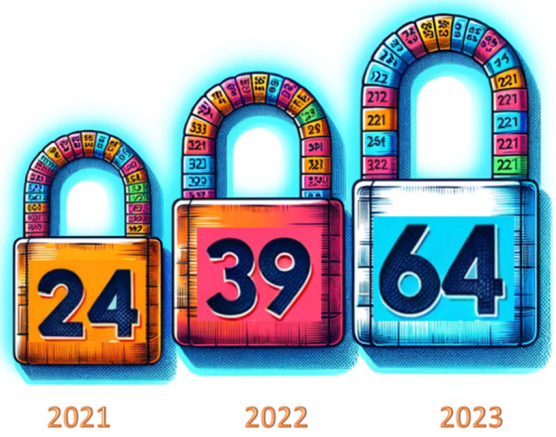


Figure 11: Number of claims by Snatch in 2021, 2022 and 2023
Graph Source: Analyst1 / Data Source: ecrime.ch

The legitimacy of the victims listed on the actors' leak site and the authenticity of the data have raised significant doubts. Snatch actors have been observed engaging in the purchase of previously stolen data from various ransomware variants in an attempt to pressure victims into paying a ransom. Valery Marchive's report further confirms these instances of Snatch using its platform for publishing data stolen from attacks conducted by other syndicates. According to the report, there was an identified correlation in multiple instances where victims claimed by other syndicates, such as Nokoyawa, LockBit 3.0, Quantum, and Medusa, were subsequently claimed by Snatch.

Snatch actors themselves acknowledged such instances of data reuse through their Telegram channels claiming to "***specialize exclusively in leaked sensitive data***". Actors admitted to collaborating with other ransomware groups responsible for data breaches, utilizing data leaked by these groups. Furthermore, actors stated that they started their operations a year ago and have no affiliation with the Snatch group which "***appeared in 2019 and existed for about 2 years***", asserting that the only commonality between them is the name. Based on the timing of this post, the actors' operations began approximately a year ago, around August 2022. They also added that "Snatch" stands for "***Security Notification Attachment (SNAtch).***" *(see screenshot on the left below)*

The actors' claim of not being affiliated with the original Snatch group appears contradictory, especially considering the activity across their Telegram channels. For instance, a message posted on **September 11, 2023**, featured an article about the original Snatch group published by ThreatPost on **December 10, 2019**, which uncovers its operations. By sharing this article and underscoring media interest, the actors attempt to enhance their notoriety by asserting, "***Social media admits Snatch Team***". However, for a group attempting to distance itself from the "original" Snatch group, this move appears contradictory. *(see screenshot on the right)*

Figure 12: Snatch messages posted on two of their Telegram channels referring to the "true" nature of their operations. Source: Analyst1

This accidental mistake sheds a light on why actors persist in operating under their own name. It also serves as a reminder of the ransomware phenomenon itself — a threat that has evolved into what is believed to be an unstoppable and destructive force that is hard to oppose. Actors leverage their own established name and ransomware reputation, capitalizing on the widespread interest and media attention, particularly in Europe and the United States, which seem to be the target audience for the group.

To conduct covert influence operations and disseminate their message, Snatch actors operate two Telegram channels. One was created in July 2023, garnering nearly 2,600 followers as of January 16, 2024, while another was launched in September 2023 and currently has nearly 10,200 followers. A notable detail is the actors' primary communication is in English, with occasional snippets in Russian. Considering that the group is believed to comprise Russian-speaking actors, this suggests a deliberate effort to appoint an English-fluent individual to convey their message effectively to the target audience.

This suggests a deliberate effort to appoint an English-fluent individual to convey their message effectively to the target audience.

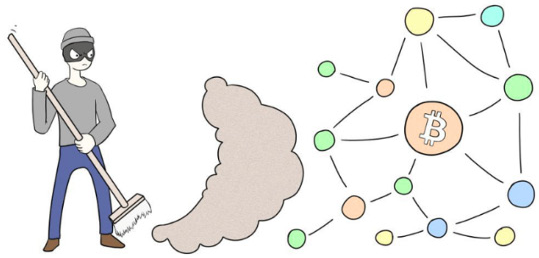
According to the actors, their primary goal is to ensure digital safety by educating their audience on a various subject. Their posts often include advice on protection measures, details about different fraud and attack schemes, and guidance on safeguarding against them. To validate their advice, which appears contradictory to their claimed nature of working for the greater good, actors provide details about multiple data leaks, referencing victims by name and including personal information of individuals associated with the breach, such as their addresses, emails, and other personal details.

Despite massive interrogative efforts and personal attacks aimed mainly at European or United States entities, the actors claim to be entirely apolitical. "***Unlike, for example, KillNet or pro-Ukrainian hacker groups, we do not make loud statements and do not indicate our position on what is happening in the world***," actors say in a message posted on October 8, 2023.

Actors refer to two ongoing conflicts, Russia–Ukraine and Palestine–Israel, stating their intent to remain neutral without taking sides. "***Never on our portals you will find neither Russian, nor Ukrainian, nor Israeli, nor Palestinian targets. And we will ban with no mercy those who try to post them. We want to prevent an imminent catastrophe, the name of which is World War III. And this war will not be as you are used to seeing it — explosions, deaths, bombings.***"

S_N_ATCH

BITCOIN DUST ATTACK



A trace amount of crypto, called dust, sent to thousands — or hundreds of thousands — of wallet addresses. This attack is deployed in order to track these addresses to "un-mask" or de-anonymize them.

Should You Be Worried About Getting Dusted?
In short - Yes.

Criminals have used dusting attacks to de-anonymize large cryptocurrency holdings. Those with large holdings can be targeted in a number of ways, including through phishing scams and cyber-extortion. Users with large crypto holdings in high-risk areas could also be physically targeted, or even have a family member kidnapped for a cryptocurrency ransom.

Tax or law enforcement agency may also perform a dusting attack in order to connect a person or group to an address. Specifically, they may target gangs that deal in contraband, large criminal networks, money launderers, or tax evaders. Mass dusting is also used by blockchain analytics firms, who study crypto dust for academic purposes or have contracts with government agencies.

#CryptoHygiene

Security Notification ATtaCHment

Here are some more security tips you should remind yourself of.

👀Use Two-Factor Authentication (2FA)

The first layer of protection between your account and someone else accessing it is your password. The second layer is two-factor authentication (2FA). You should be using it to add an extra blanket of security to your accounts.

2FA is, at its most basic, an identity verification software. If you (or the threat actor) enter the correct password to your account, 2FA will kick in and require you to verify your identity, most often by entering a series of random numbers or letters sent to you via SMS (cellphone texts) or by an app.

You can (and should) use 2FA for all of your accounts, Amazon, eBay, Nintendo, Twitter, Reddit, Instagram, and any other account you may have.

👀Double-Check That Link Before You Click

Phishing is one of the most common forms of cyber attack. Phishing is a form of cyberattack that is delivered mainly by email, but also by SMS. The threat actor tries to entice you to click a bogus link that will take you to a website that's masquerading as an official entity, or even download a virus on your device.

Before you click any link, double-check that it's the true source you want to visit. The difference can be as minor as "arnazon.com" and "amazon.com".

#CyberSecurity #SnatchTips #SecurityTips

Figure 13: Snatch posts provide some advice on safeguarding digital assets as a part of their "official" educating efforts. Source: Analyst1

Their official stance of abstaining from politics is intentional. The actors aim to avoid overtly aligning themselves with any political agenda, strategically presenting themselves as regular individuals. This deliberate choice allows them to conduct their coercive influence operations, subtly sharing their opinions under the guise of an ordinary person. This approach seeks to resonate with a wider audience as they attempt to portray themselves as relatable figures.

A further indication of the actors' underlying agenda and political inclinations becomes apparent in their deliberate choice of targets. Despite claiming neutrality, their significant focus on two specific regions, Europe and the United States, contradicts this claim. Additionally, the actors' distinct referencing of government and related government officials, is characterized by the frequent use of derogatory language and extensive engagement in discussions regarding government policies.

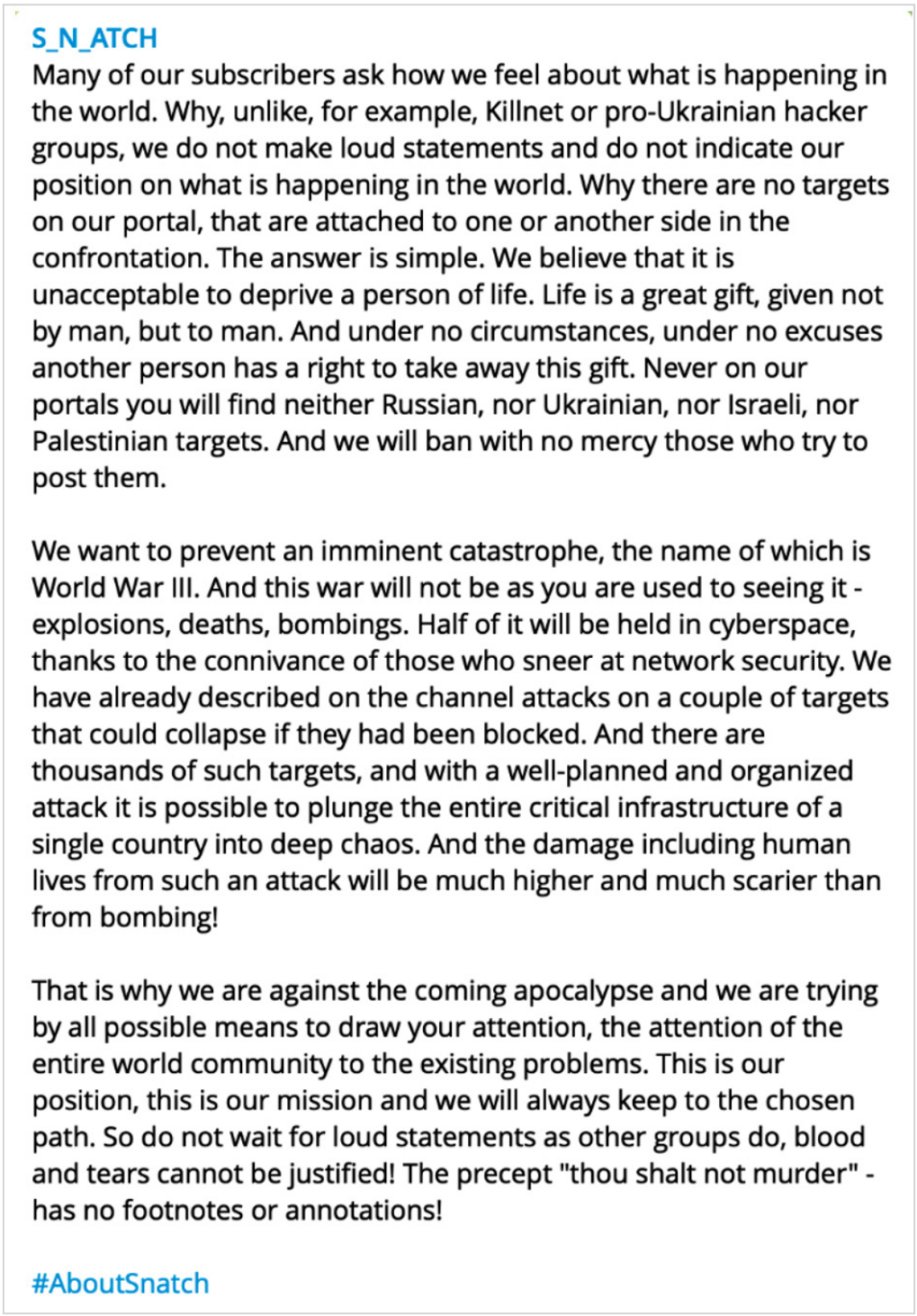


Figure 14: Actor claim to be apolitical in their Telegram post. Source: Analyst1

They utilize data claimed to be stolen from breaches conducted by other syndicates to propagate a narrative of inadequate protection practices by businesses associated with these regions. This tactic seems to be aimed at undermining both the credibility of these entities and the states themselves.

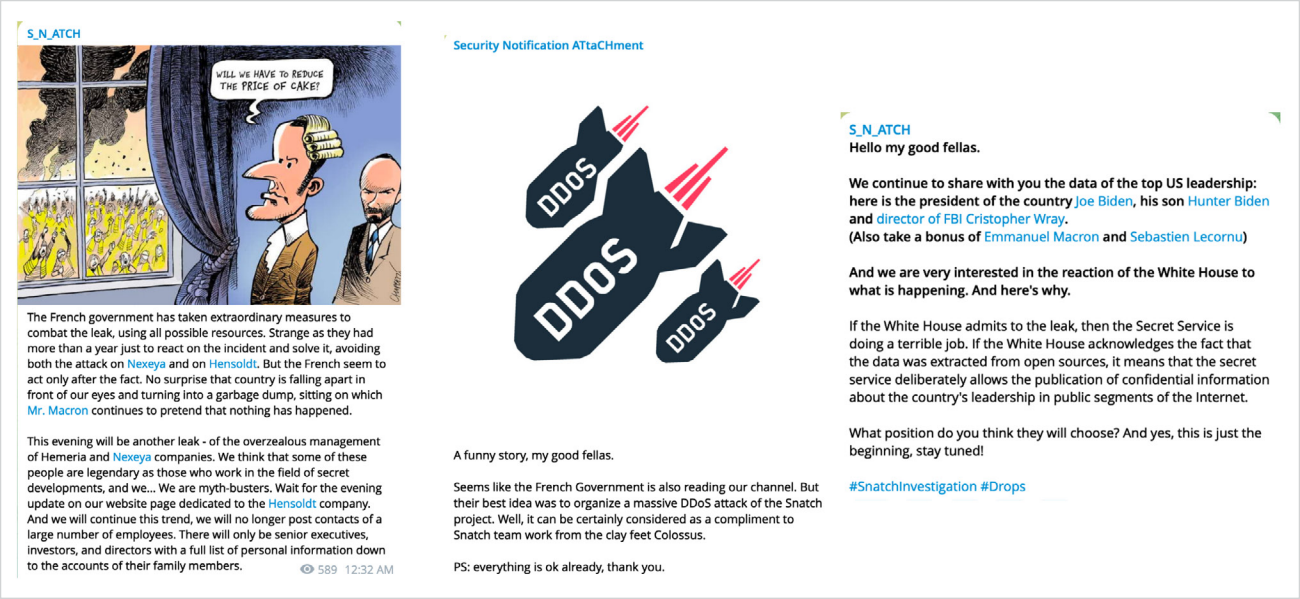


Figure 15: Snatch actors are attempting to persuade the public about the French government's weak policies and suggesting alleged retaliatory actions, using this to lend credibility to their claims (screenshot #1 & #2 from left to right). In a screenshot #3, actors refer to the United States officials using derogatory language aimed to undermine entities' credibility. Source: Analyst1

Another strong indicator that the group's motivations extend beyond monetary gain is the apparent lack of profitability. Based on our analysis and what is publicly shared by the actors themselves, their reliance on repurposing data obtained from other groups significantly diminishes their chances of successfully extorting a ransom. While their success receiving a ransom remains uncertain, their chances are likely close to zero. When faced with two claims of a breach from separate groups and lacking encryption in one case, victims are more likely to dismiss that particular claim, leaving Snatch actors without any potential profit.

However, despite understanding their slim chance of obtaining a ransom, the persistence of Snatch actors in their activity indicates alternative motivations and suggests a pursuit beyond monetary gain. Rather than solely seeking financial rewards, they appear to try for different outcomes, leveraging the attention garnered to communicate their ideas through their communication channels.

Stay Calm and Keep Fighting.

A ransomware attack is a disruptive event that can result in significant financial losses and damage to an entity's reputation, sometimes even leading to the loss of business

altogether. Alongside various consequences such as operational downtime, the extortion phase further intensifies the pressure. During the extortion phase, regaining control over the network and maintaining coherence among the affected team and decisionmakers is crucial. While threat actors aim to create chaos and push victims into making a rash decision and paying the ransom, the primary goal for the victim should be to remain composed. The recommended course of action consists of a strategic response plan, if available, and to promptly coordinate with law enforcement and incident response companies.

When dealing with ransomware actors, it is important to remember that any agreements made with them are unreliable and likely to be broken. This is especially true when actors promise to delete stolen data exfiltrated during the attack. For financially motivated ransomware actors, stolen data, which is highly marketable on the DarkWeb, serves as a secondary revenue stream after the ransom payment itself. Thus, engaging in deals with actors might only delay the exposure of a victim's name on a data leak site but doesn't guarantee the secrecy of a breach as stolen data might surface later.

The Snatch case study provides valuable insights for responding to extortion attempts. When approached by actors, it's crucial to thoroughly confirm whether a data breach occurred. Similar to the Snatch case, where data was repurposed from previous breaches and presented as a new attack, verifying the authenticity and cross-referencing the data against previously confirmed breaches is vital for mitigating potential reputational damage. This example also highlights the importance of using precise data leak analysis terminology, to avoid labelling the actors' claims as ransomware attacks and to prevent further misinformation.

The analysis of Snatch activity also points to the evolution of ransomware as a threat that has undergone a significant transformation in the past two years, with actors aligning their operations based on their affiliations with specific states. Threat actors now leverage the threat of ransomware attacks as a means to gain attention and validate its claim against a victim. The claim itself has evolved into a potent Ransomware-as-a-Weapon, used strategically by actors to attempt to influence operations. These influence attempts operate on two fronts: shaping public opinion and exerting pressure on higher echelons of authority to impact political decisions. In a time of multiple ongoing military conflicts such as Russia-Ukraine and Palestine-Israel, these actions contribute to the actors' intentions of manipulating the informational landscape. Constant monitoring of such activity is essential to identify influence operations attempts and address them with strategic planning.

Maintaining control over the narrative is crucial, and this responsibility should rest in the hands of Cyber Threat Intelligence (CTI) professionals and media. When dealing with information related to ransomware activity, it is important to conduct a careful assessment to avoid simply echoing the narratives pushed by ransomware groups, which may be designed to sway public opinion. This measured approach is essential for both public understanding and effective cybersecurity communication. Analyst1 continues to monitor ransomware landscape to contribute to a safety of a digital space.

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**