FEBRUARY | 2024

Arete

Annual Crimeware Report

2023 Trends and Highlights

Table of Contents

Executive Summary

At Arete, our global teams glean data and insights from every aspect of the threat lifecycle. From forensics and restoration to threat actor communications and compliance, this comprehensive visibility informs our understanding and analysis of the threat landscape. Leveraging data collected during incident response engagements, we can see the rise and fall of ransomware variants, notable trends in ransom demands and payments, industries targeted by ransomware attacks, and what may be coming next.

Throughout 2023, Arete observed threat actors continually evolve their operations to become faster, stealthier, and wealthier. These changes ranged from new methods to bypass security defenses to new techniques for exfiltrating and posting stolen data. Arete also observed threat actors becoming more aggressive in negotiation techniques, demanding notably larger ransoms as fewer victims were willing to pay ransoms. Internal challenges and disorganization drove operators to implement more stringent policies on negotiation and demand amounts.

In this report, we explore the big names in ransomware, the most frequently targeted sectors, trends in data exfiltration, and which malware and tools are leveraged by ransomware operators. This data creates insights into how organizations can better protect their environments from cyberattacks.

The 2023 threat landscape was characterized by a combination of mainstay threat actors and new or reemerging groups. While top variants continue evolving to maintain dominance, the widespread impact of newer groups demonstrates the constant evolution of today's threats and the need for adaptable defenses and increased cyber resilience.

Threat actors faced increased pressure from law enforcement, including the successful disruption of the Hive operation and a temporary ransomware takedown of ALPHV/BlackCat. These high-profile disruptions may result in more stringent vetting of affiliates and a splintering of larger ransomware groups in 2024 as ransomware groups look to evade this unwanted attention.

Looking ahead to 2024, ransomware groups will likely continue evolving their operations to more effectively access, steal, and encrypt victim data. New malware, leaked source code and builders, and an influx of AI tools will continue to lower the barrier of entry into cybercrime. As defenses and backups continue to improve, disruptions to operations will likely be the leading driver for victims to pay ransoms. Preventing and detecting cyber threats will require an increasingly comprehensive, data-driven approach. Arete is committed to providing our clients and partners with actionable data and insights to effectively combat cybercrime.

2023 Highlights From Arete's Incident Response Cases

Using frontline data from incident response engagements, Arete identified and analyzed notable trends and shifts that highlight the evolving state of the cyber threat landscape.

TOP RANSOMWARE VARIANTS OBSERVED

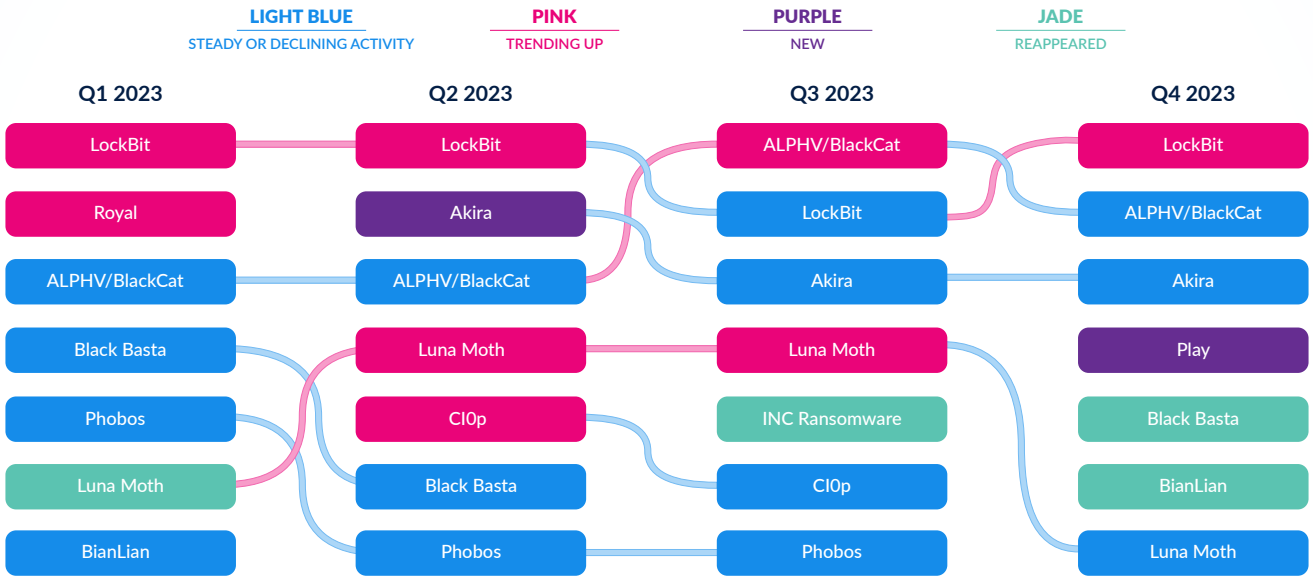

Figure 1: Top ransomware variants observed from Q1 2023 to Q4 2023

The 2023 threat landscape was characterized by a combination of mainstay threat actors and newly developed groups. Nearly all the most frequently observed threat actors in 2023 appeared consistently throughout the entire year, and all but Akira have operated since at least 2022. Figure 1 shows the top ransomware variants observed over the past four quarters and is color-coded according to each variant's current state of activity.

LockBit and ALPHV/BlackCat retained the top three spots in 2023, showcasing their continued dominance. In Q2 2023, we observed the emergence of Akira, a new ransomware group that maintained a strong presence throughout the rest of the year. Q4 saw an increase in variants, including Play, Black Basta, and BianLian, significantly impacting the threat landscape as they expanded operations.

Arete's data covers victims in eight countries, spanning 85 states and provinces in those countries. The majority of organizations Arete supported in 2023 were headquartered in the major population centers in the United States, including California, New York, Florida, and Texas. These organizations were not without defenses—nearly 90% of victims had an Endpoint Detection and Response (EDR) tool or anti-virus in place, and nearly 30% of victims were warned of or logged a potential security concern prior to ransomware being deployed in their environment.

While these defenses protected the victims from some attacks, insecure deployments, lack of management, and slow response times allowed determined threat actors to subvert these defenses.

Additionally, 50% of victims had some form of multi-factor authentication and backups in place. However, nearly 30% of victims had their backups either encrypted or deleted. In these cases, misconfigured or insufficiently managed defenses left holes that threat actors found and exploited. These statistics demonstrate that most victims were not without defenses, but their existing defenses were not enough to stop skilled and stealthy crimeware groups looking to profit by encrypting and stealing data.

Arete's data covers victims in 85 states and provinces across eight countries.

Arete's Incident Response and Managed Detection and Response teams understand that implementing defenses alone is not enough. The continued management of defenses and speed of remediation is critical to stopping threat actors. Actively managed security-in-depth, including multiple layers of controls, is required to disrupt and defeat cyber threats.

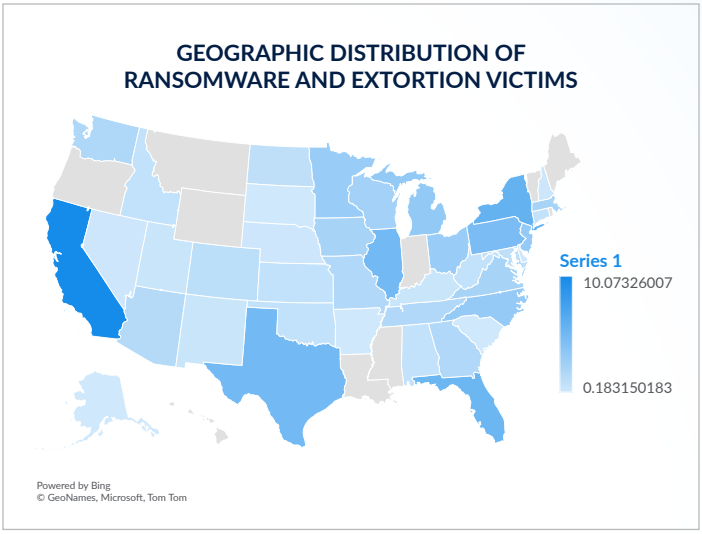

Figure 2: Geographic distribution of ransomware and extortion victims in the U.S. observed by Arete in 2023

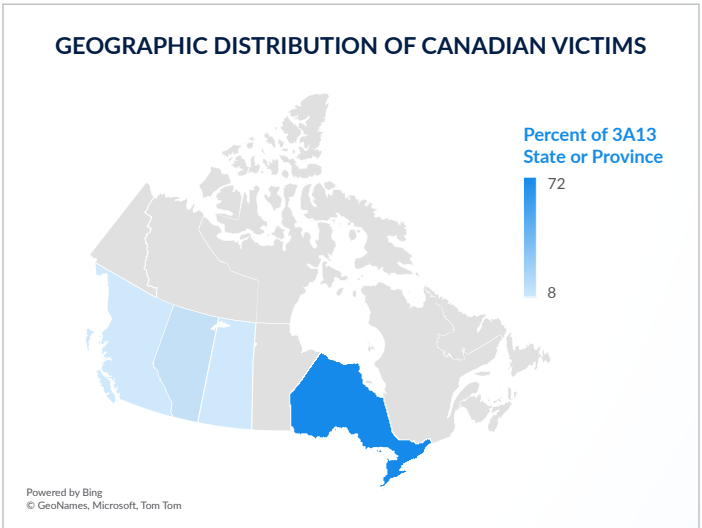

Figure 3: Geographic distribution of ransomware and extortion victims in Canada observed by Arete in 2023

Threat Actor Insights

Tactics, techniques, and procedures (TTPs) and analysis on the top ten threat actor ransomware groups observed during 2023.

75	Over 50	41
Total Named Threat Actors Tracked	**Unnamed Unique Threat Actors Monitored**	**Ransomware Data Leak Sites Tracked**

LockBit

Accounting for 17% of ransomware engagements conducted by Arete in 2023, LockBit remains a prominent player in today's threat landscape. With fast encryption and data exfiltration features, the group continues to demonstrate intent and capability to compromise organizations across many industries and countries. As the self-proclaimed "world's fastest and most stable ransomware,"[1] LockBit has continued its pursuit to monopolize the ransomware sector by expanding its attack surface by implementing encryptors such as:

- LockBit targeting MacOS environments
- LockBit targeting Linux environments
- LockBit Green using leaked Conti ransomware source code to attract former Conti affiliates

Throughout the year, LockBit faced a multitude of challenges, including inefficiencies in adding victims to their data leak site (DLS), encryption issues, and general management issues. Following a brief hiatus, the group issued more stringent negotiation guidelines, outlining how much ransom to demand and setting the maximum percentage of discount off the initial demand (For more information on LockBit negotiation practices, see page 15). Thus far, it appears LockBit affiliates have complied with the guidelines set by the Ransomware-as-a-Service (RaaS) group.

LockBit issued more stringent guidelines, outlining how much ransom to demand and setting the maximum percentage of discount off the initial demand.

ALPHV/BlackCat

As one of the oldest currently operating ransomware brands, ALPHV/BlackCat represented 14% of Arete's engagements in 2023, with a significant uptick in Q3. First identified attacking victims in November 2021, ALPHV/BlackCat has remained a formidable RaaS enterprise since its onset. The group demonstrates continuous innovation, regularly incorporating new discovery techniques, defense evasion, and various post-compromise activities.

Programmed in Rust, the BlackCat encryptor already features some built-in multiplatform encryption capabilities. While LockBit appears to focus primarily on adding capabilities, BlackCat strives to raise the ceiling of extortion techniques to pressure victims into paying the ransom.

BlackCat has always pushed the boundaries of extortion, making their DLS searchable, mimicking the clear web websites of victims to serve as DLS, and posting medical procedures to embarrass victims. In July 2023, BlackCat was the first threat actor to implement API functionality into their DLS to increase pressure on victims.

Prior to law enforcement's attempted takedown of ALPHV/BlackCat in December 2023 (further discussed on page 29), Arete observed shifts in ALPHV/BlackCat's attacks and negotiations, including a decrease in the quality of affiliates and negotiations. In October 2023, negotiations with several BlackCat affiliates led to the conclusion that Arete's Threat Actor Communications team was interfacing directly with affiliates rather than with a centralized negotiation team, as was previously assessed through dealings with the threat actor. Arete saw attacks in which the ransom demands did not follow the typical ALPHV/BlackCat pattern, but the threat actor provided screenshots of a draft post to the ALPHV/BlackCat DLS, leading to the hypothesis that ALPHV/BlackCat was opening its DLS to other affiliates.

ALPHV/BlackCat demonstrates continuous innovation, regularly incorporating new discovery techniques, defense evasion, and various post-compromise activities.

The FBI seized the ransomware group's DLS on December 19, 2023, and obtained victim-specific decryption keys for over 500 BlackCat victims. Despite this disruption to ALPHV/BlackCat's infrastructure, the group quickly resumed operations and posted new rules for its affiliates, allowing more permissive attacks against organizations like hospitals. However, since the announcement, Arete has not observed any ALPHV/BlackCat affiliates adhering to these new rules.

Akira

Despite emerging in mid-Q2, Akira was one of the top three threat actors in Q2, Q3, and Q4. Akira operates as a RaaS and appeared to benefit from ALPHV/BlackCat's law enforcement troubles in December 2023, potentially picking up ALPHV/BlackCat affiliates to increase the cadence of their operations at the close of the year.

Akira primarily relies on vulnerabilities in Cisco devices to achieve initial access before typically using AnyDesk to maintain persistence and launch various operations. Arete also noted Akira is utilizing SocGholish and Gootloader to enable its operations. SocGholish is a JavaScript-based framework that masquerades as an update and is used by a variety of threat actors. Gootloader is a piece of malware used by multiple threat actors to download additional payloads. Akira's diverse arsenal likely contributed to the group's success in 2023.

Black Basta

A consistent adversary in Q1 and Q2, Black Basta was less active in Q3. The group originally used the remote access trojan (RAT) Qakbot to gain access to victim environments. However, after Qakbot's operations were disrupted by law enforcement, Black Basta shifted to new initial access methods, which included vulnerability exploits and other RATs. Evolving its initial access methods allowed Black Basta to resume more frequent operations in Q4.

A security researcher discovered an error in Black Basta's encryption algorithm that allowed for partial decryption of some files. A decryptor was released in December 2023, but unfortunately, did not work for most victims. Black Basta resolved the flaw within weeks of the decryptor's release, and its operations were not significantly impacted.

Luna Moth

Luna Moth was the sole extortion-only operation among Arete's most observed threat actors. It was also one of the most regimented threat groups Arete encountered in 2023. The group follows a nearly identical attack path in many of their engagements and almost exclusively targets law firms. It operates a limited number of campaigns each year but compromises multiple victims in each campaign.

Luna Moth operates a limited number of campaigns each year but compromises multiple victims in each campaign.

Luna Moth gains initial access through a social engineering technique called callback phishing, in which the threat actor sends an email that prompts a user to call a phone number. This prompt email is typically an invoice for a high-value purchase. After users called the threat actor provided phone number, they were prompted to install legitimate remote monitoring and management tools like Atera or Splashtop, which granted the threat actor persistence and enabled them to install more tools and eventually exfiltrate data.

Luna Moth sometimes compromises so many organizations in a single campaign that it takes months for the group to extort victims. Arete observed at least one case in which Luna Moth stole data months before they threatened to release the data.

Play

Play's operations remained stable throughout the year, with a significant increase in Q4. This increase coincided with a deviation from the group's standard attack paths, and around the same time, researchers began claiming the group transitioned from a closed operation to a RaaS provider. However, these claims cannot be confirmed, and Arete noted that the group's highly structured operations correlate more with a closed ransomware group than a RaaS operation.

Play ransomware utilizes Cobalt Strike for post-compromise and SystemBC RAT to maintain persistence on a victim's network. The group exploits Microsoft Exchange vulnerabilities such as the ProxyNotShell (CVE-2022-41040, CVE-2022-41082). Play's infection chain includes using compromised accounts or unpatched Fortinet SSL VPN vulnerabilities to gain access to an organization's environment.

Royal

The Royal ransomware group was the second most active threat group in Q1 before its operations under the Royal name greatly decreased after May 2023. The group attacked a limited number of victims in June and July before ceasing public activity. CISA and the FBI reported that Royal is likely rebranding to Blacksuit ransomware. Arete first encountered Blacksuit in Q4 2023 and saw limited overlap in behaviors. Blacksuit ransomware began sharply increasing at the start of 2024, showing that although names may change, Blacksuit continues operations.

Royal likely began to re-brand its operations in Q2 after attracting significant law enforcement attention by attacking more than 300 organizations in less than a year and demanding more than $200 million in ransoms. After observing the January 2023 takedown of Hive ransomware, Royal likely shifted operations to evade disruption and potential arrest.

Phobos

Phobos' operations directly contrasted with Play's organized attacks. In fact, many Phobos engagements involved variants of Phobos potentially operated by different threat groups. Throughout 2023, Arete saw Phobos ransomware deployed under the names Faust, elbie, Devos, and 8base. 8base demonstrated such distinct negotiation tactics that Arete began tracking them as an entirely separate organization. 8base is the only Phobos affiliate to operate a DLS and consistently provide the same contact information.

Throughout 2023, Arete saw Phobos ransomware deployed under the names Faust, elbie, Devos, and 8base.

Phobos ransomware was built using Dharma/Crysis ransomware source code sold in 2020 and is distributed as part of a RaaS operation. The multiple variants of Phobos are capable of encrypting ESXi, Windows, and virtual servers. Phobos affiliates are known to encrypt backups and rely primarily on Remote Desktop Protocol (RDP) for initial access. The central Phobos operators do not appear to impose payment restrictions on the various affiliates, as Arete is often able to negotiate discounts exceeding 50%.

BianLian

BianLian is a hybrid ransomware and extortion operation that originally used custom encryptors to extort money but moved to a primarily data theft-based model after a security company released a decryptor for its ransomware executable. After moving to exfiltration-only attacks, BianLian became even more aggressive during ransom negotiations, often posting victims to their DLS and contacting employees and customers.

In over 50% of Arete's BianLian engagements, they gained initial access through open RDP. Once inside a victim environment, BianLian often relies on legitimate remote monitoring and management (RMM) tools like TeamViewer, AnyDesk, GoToAssist, and ScreenConnect. Arete also saw BianLian leverage Gootloader to download additional payloads. BianLian typically exfiltrates using MegaSync and rclone and then send ransom demands via email, often from a compromised employee account. In more than one case, Arete saw BianLian contact victim employees using internal chat applications like Slack.

Cl0p

Cl0p perpetrated one of the most impactful crimeware campaigns of the 2020s when it exploited a zero-day vulnerability[2] in Progress Software's MOVEIt file transfer application tracked as CVE-2023-34362. The attack started on May 27, 2023, and continued throughout the summer of 2023.

Cl0p perpetrated one of the most impactful crimeware campaigns of the 2020s when it exploited a zero-day vulnerability in Progress Software's MOVEIt file transfer application.

The vulnerability allowed Cl0p to inject code into the file transfer solution, which resulted in a web shell named LEMURLOOT being installed. This web shell allowed Cl0p to steal data from the underlying MOVEIt database. This was the group's second campaign in 2023 after it exploited a vulnerability in Fortra's GoAnywhere MFT servers at the start of the year.

Cl0p exploited and stole data from so many victims in the MOVEIt attack that it had to change its data leak strategy (as described on page 23) and extort victims in batches. Some victims' data was extorted months after the exfiltration occurred. While the actual number of victims is likely different, Cl0p published more than 100 organizations' names on their DLS associated with this campaign. A company name on the DLS is not confirmation that they were compromised or that the data stolen was sensitive; however, it is still telling of the massive scale of this campaign.

Effectiveness of Ransomware-as-a-Service Groups

Half of the most observed threat actors operate as Ransomware-as-a-Service (RaaS) organizations, in which the core operators sell access to encryptors and tools to other threat actors in return for a percentage of the attack profits. Across the most observed threat groups, RaaS groups were more effective at fully encrypting victims.

RaaS groups were responsible for 63% of victims that were fully encrypted, versus closed groups, which were responsible for 22% of fully encrypted victims. The remaining 15% of victims were attacked by threat actors who relied on either open-source ransomware executables or simple executable-for-sale models. RaaS groups also accounted for 54% of victims where data was confirmed to be exfiltrated, showing RaaS groups were also slightly more effective at exfiltrating data. Closed groups were responsible for only 35% of cases where data was exfiltrated. The remaining 11% of engagements here also arose from threat actors relying on operating models different than RaaS or closed groups.

Overall, RaaS groups were more effective at causing damage. This likely arises from the separation and specialization in criminal duties that RaaS operations afford crimeware actors. These specialized roles include initial access brokers who specialize in gaining access to victim environments and then selling that access; ransomware operators who develop the infrastructure and software; ransomware affiliates who purchase or develop their own access and deploy the operator's ransomware; and money managers who handle exchanges and moving the money underpinning these roles.

THREAT GROUPS WITH THE HIGHEST AVERAGE RANSOM DEMANDS

THREAT ACTOR	RAAS	AVERAGE DEMAND	DATA EXFILTERED
Cl0p	No	$7,937,500	89%
Play	No	$3,089,725	46%
ALPHV/BlackCat	Yes	$2,983,752	43%
Black Basta	Yes	$2,615,000	28%
RansomHouse	Yes	$1,785,100	83%
LockBit	Yes	$1,762,689	41%
Cactus	No	$1,470,000	14%
Royal	No	$1,277,118	43%

Figure 4: Threat groups with the highest average ransom demands

While specialization within RaaS groups drives higher effectiveness in how the encryptor functions, it does not correspond to greater success at data exfiltration. In fact, Arete's data demonstrates that closed groups were more successful at exfiltrating data. Additionally, closed groups were also responsible for the highest average ransom demands, as shown in Figure 4.

Among the groups with the highest average demands, Cactus and RansomHouse were the only two who did not make the list of Arete's most observed threat actors. Cactus Ransomware was first observed in March 2023 but attacked only a small number of victims until September 2023. From September 2023–January 2024, the group posts an average of 15 victims per month to their DLS, and they often repeat victims in their posts. RansomHouse specializes in data exfiltration and is generally viewed as a consortium of different groups that have multiple ransomware versions.

In summary, RaaS groups may be able to do more damage with their malware, but closed groups are slightly more successful at exfiltrating data and are slightly more likely to demand higher ransoms. Looking ahead to 2024, these numbers may shift as RaaS groups look to evade law enforcement and improve their capabilities across the board by working with higher-quality affiliates.

Closed groups are slightly more successful at exfiltrating data and are slightly more likely to demand higher ransoms.

2024 Outlook for RaaS Groups

While the ongoing competition between RaaS groups has led to innovative extortion methods, evolving tactics, and "one shop RaaS groups" for encryption capabilities, the growth of these operations also creates considerable risks to the groups' continued survival. The inability to vet and manage affiliates continues to be an issue for RaaS groups moving into 2024, as law enforcement capitalizes on opportunities to disrupt ransomware operations.

Our team predicts that well-known groups will continue to splinter into smaller, more insular ransomware groups. While closed ransomware groups may not become commonplace, it is likely that the developers and owners of ransomware operations will give increased attention to the vetting and management of their affiliates. Groups such as Scattered Spider, which bounces between data encryption using Blackcat's payload and extortion-only activities, will likely become more common.

In addition to a more thorough vetting of affiliates, it is likely that threat actors will employ additional mechanisms to manage their risk. The lines between initial access brokers, affiliates, and ransomware groups will likely blur as threat actors choose the crimeware ecosystem job description most profitable to them, given their current circumstances. In an effort to "let the heat die down," actors may choose quieter, less public measures of monetizing their skillsets before jumping back into ransomware operations that use public naming and shaming of victims. Quieter measures may include simply selling access to victims or demanding smaller ransom payments. Meanwhile, other groups may stand-up "quick hit" brandings that use very public means to extort money from victims before quickly rebranding to a new name. While the names, brands, and tactics may change, the faces behind cybercrime will largely remain the same, hidden behind the ones and zeros.

Trends in Ransom Demands and Payments

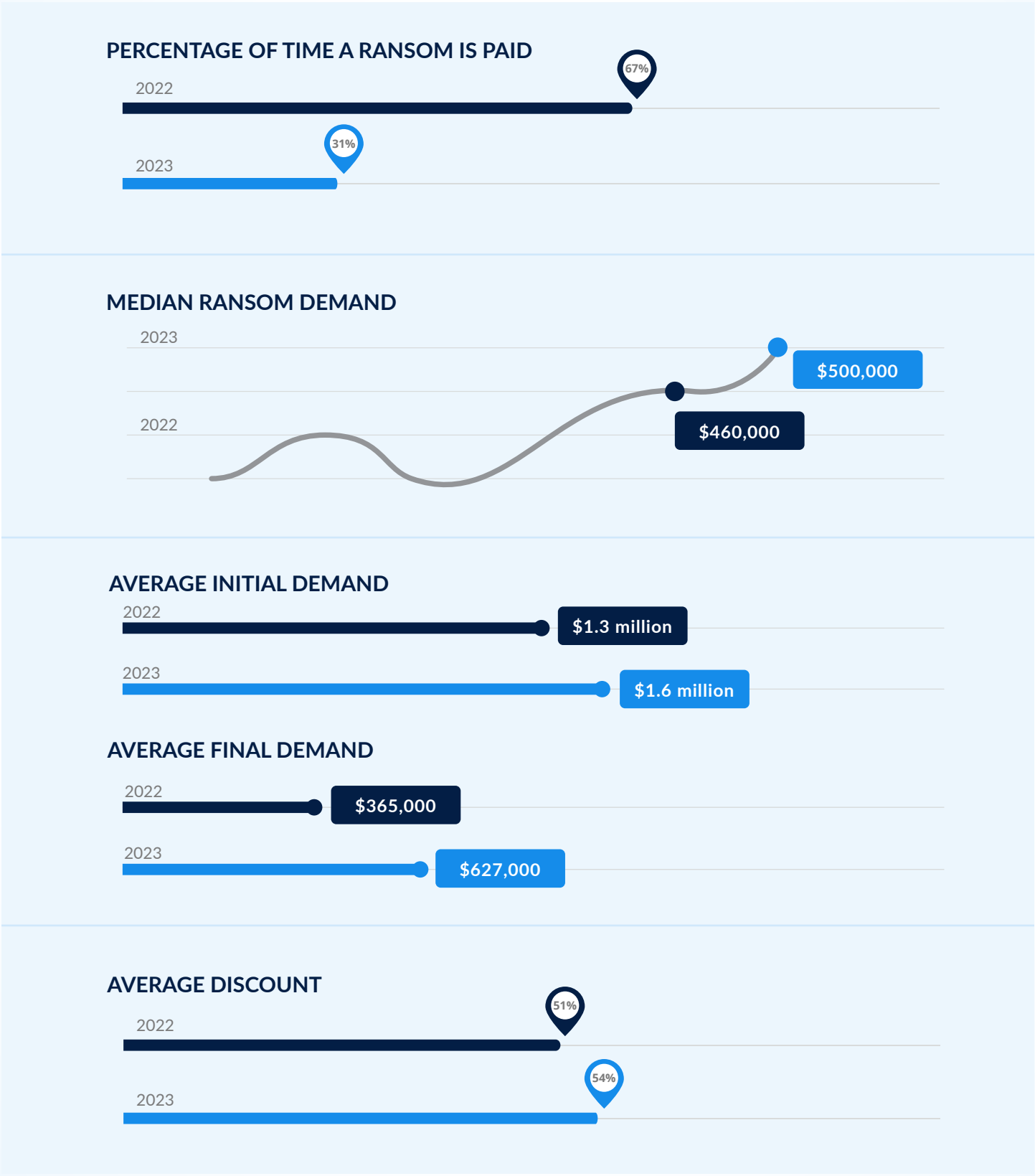

Figure 5: Trends in ransom demands and payments observed by Arete in 2022 and 2023

Arete works closely with organizations to assess backups and restore data and systems after ransomware and extortion cases. In some cases, organizations choose to pay ransom demands to receive decryption keys, proof of deletion, and stolen data. In those cases, Arete assesses relevant indicators associated with the engagement to identity the threat actor, where possible, and evaluate applicable risks associated with facilitating a payment.

In 2023, Arete witnessed a significant surge in ransom payment amounts, with a notable increase in both initial and final demands compared to the preceding year. The average initial demand in 2023 was $1.6 million, and the average final demand was $627K—in 2022, the average initial and final demand was $1.3 million and $365K, respectively. This increase was likely threat actors' response to fewer victims paying ransoms, compelling threat actors to demand more money to earn the same level of profits. These changes may also be driven by the price of bitcoin. In 2022, the price of bitcoin declined overall, whereas 2023 saw the price of bitcoin climb. Looking ahead to 2024, bitcoin prices are expected to increase once again, and a similar increase in ransom demands may occur.

Figure 6: The price of bitcoin from 2017 to 2024

Ransomware Groups Adopt More Aggressive Policies

In 2023, Arete saw several ransomware groups make changes to their internal policies or extortion tactics, instructing affiliates to take a more aggressive approach to pressure victims. With ransomware attacks increasing in 2023 but fewer victims paying, ransomware groups in 2024 will likely continue to evolve and adopt new tactics to stand out and coerce their victims into paying ransom demands.

LockBit

In September 2023, LockBit reportedly had internal discussions on changes to their ransom payment policies. This stemmed from frustration with the inconsistency and variability of ransom demands set by its affiliates, which ranged from offering substantial discounts to maintaining a firm stance during negotiations. At the time, LockBit proposed several options for regulating ransom demands, including setting a minimum payment based on the victim company's annual revenue or ransomware insurance policy, capping the discount percentage, or maintaining the status quo.

These reports were corroborated in late 2023 when Arete observed details of the new policy posted by an affiliate:

> *"From October 1, 2023, it is strictly forbidden to discount more than 50% of the originally requested amount in correspondence with the attacked company during the negotiation process. For those who have a steely character, know how to determine the ransom amount that a company will pay with a high probability and almost never make large discounts please keep this rule in mind and adjust the ransom amount with the size of the maximum allowable discount.*
>
> *The ransom amount is still set at your discretion in whatever amount seems fair to you.*
>
> *However, based on the study of many successful and profitable deals, when the pentester's work is done perfectly, a lot of valuable data is downloaded and all backups are destroyed, it is recommended to stick to the following figures:*
>
> - *Companies with revenue up to 100 million pay from 3% to 10%*
> - *Companies with revenue up to 1 billion pay from 0.5% to 5%*
> - *Companies with revenue more than 1 billion pay from 0.1% to 3%*
>
> *Please strictly follow the rules and try to adhere to the recommendations as much as possible."*

Since October 2023, Arete observed LockBit affiliates referencing this new policy during the negotiation process, and affiliates have been adhering to the new rules. Prior to October 1, 2023, Arete saw an average discount of 55% from initial ransom demand in payments to LockBit. After October 1, the average discount dropped to 45%.

BianLian

In reports from May 2023, the FBI shared observations of BianLian ceasing encryption of victims' files and shifting exclusively to data exfiltration. This change was likely a result of the free BianLian decryptor released by Avast in January 2023. Arete also observed this shift directly in engagements with BianLian. Without encryption to pressure victims into paying, BianLian became notably more aggressive during negotiations and in pressure tactics throughout 2023. After the group steals data and leaves a ransom note, they begin aggressively contacting employees of the victimized company. This harassment typically continues until a

payment is made to the group. In their own words, they will harass "every employee, relatives of employees, [and] clients" until a deal is closed. Other tactics observed by Arete include posting a public pre-release of victims' data to their DLS, threatening to post data on forums, social media, and magazines, contacting and harassing family members of employees, and referencing legal and regulatory issues their victims could face—even going so far as to reference specific subsections of laws and statutes.

ALPHV/BlackCat

In 2023, ALPHV/BlackCat adopted several unique and aggressive tactics to pressure victims to pay. The group is known to actively target organizations in the healthcare industry, and in early 2023, they started leaking sensitive patient data on their DLS, including data and photos of cancer and plastic surgery patients. Although ransomware groups leaking PII and PHI is common, the sensitive nature of the images drew attention from multiple media outlets. In November, it was also reported that BlackCat began reporting their victims to the U.S. Securities and Exchange Commission (SEC) as another new tactic to pressure victims to pay for data suppression.

Later in the year, following law enforcement actions against the group in December 2023, the group posted new rules, stating it would allow affiliates to target any organization, including hospitals and critical infrastructure, as long as it is outside of the Commonwealth of Independent States (CIS), a regional intergovernmental organization formed by Russia and 11 republics formerly part of the Soviet Union. The new rules also stated that discounts on ransom demands would no longer be given.

> *"Because of their actions, we are introducing new rules, or rather, we are removing ALL rules except one, you cannot touch the CIS, you can now block hospitals, nuclear power plants, anything, anywhere.*
>
> *The rate is now 90% for all advertisers.*
>
> *We do not give any discounts to companies, payment is strictly the amount that we indicated.*
>
> *VIP advertisers receive their own private affiliate program, which we raise only for them, on a separate DC, completely isolated from each other."*

Unlike the policy changes within LockBit, Arete has not observed BlackCat affiliates adhering to the new rules, as they continue engaging in standard ransom communications with victims, offering discounted prices, and showing a willingness to negotiate. Further, the group was already known for attacking the healthcare industry, and while it is unknown if the group will pursue critical infrastructure targets in 2024, there have not been any reports of affiliates doing so since the new rules were posted.

Ransomware Groups Add Threats of Violence to Pressure Tactics

Ransomware groups use a variety of harassment tactics to pressure their victims into paying ransom demands. These include threats of exposing stolen data on the dark web or social media, as well as more aggressive tactics such as direct phone calls and emails to victims, their employees, customers, clients, and in some cases, contacting relatives of the victim. However, in previous years, ransomware groups have typically stopped short of threats of physical harm to their victims. A concerning observation by Arete in 2023 was pressure tactics that involved threats of violence to victims.

- In early 2023, Arete observed an isolated case in which a ransomware group sent a detailed threat of physical violence against specific employees of a victim, as well as their parents and children. The threat actor also claimed they would send out letters and video evidence of their history of violence towards non-paying customers.
- In October 2023, it was reported that Octo Tempest, a collective of threat actors associated with Scattered Spider and an affiliate of ALPHV/BlackCat would, in rare instances, contact specific individuals and issue physical threats toward them and their relatives, including threatening to send a shooter to their house to obtain login credentials.
- After a ransomware attack against a medical facility in November 2023, the threat actors reportedly considered targeting patients with a tactic known as "swatting," where fake bomb threats or other false reports of violence are made to law enforcement to elicit authorities to show up to the victim's residence heavily armed.
- In late 2023, Arete also observed a threat actor calling their victim and threatening to blow up the victim's building if their demands were not met, resulting in the involvement of law enforcement and the evacuation of the building as a precaution due to the severity of the threat.

Based on both Arete's observations and open-source reporting, the use of these extreme tactics is still rare. While Arete first observed ransomware groups using threats of violence during 2023, other security researchers have seen this sort of behavior used in the past. In 2018, a collective of hackers called Apophis Squad conducted mass emailed bomb threats against individuals, businesses, and institutions in the U.S. and the United Kingdom until some of its members were arrested in early 2019. Similarly, in 2019, the ransomware group Ryuk made threats of violence to cybersecurity defenders.

The threats of violence observed and reported in 2023 seem to reflect individual personalities attempting last-ditch scare tactics to get information or money from victims, as opposed to any larger shift in tactics by ransomware groups. Threats of physical violence are more likely to attract attention from law enforcement, and Arete assesses that ransomware groups are unlikely to adopt violent threats as a regular part of their pressure methods. Although occasional incidents of violent threats may occur in 2024, a trend among cybercriminals is unlikely to emerge.

How Encryption Impacts Payment

Arete works closely with victims to avoid facilitating ransom payments whenever possible, and analyzing trends in encryption demonstrates that the number of systems encrypted has little impact on overall payment likelihood. The decision to pay a ransom is much more nuanced; rather than being based on the number of systems encrypted, the reason for payment is likely tied to how much the encryption prevents the victim from operating their business or generating revenue and if the cost of lost revenue is more than the cost of the ransom demand.

On a positive note, most victims, regardless of the percentage of systems encrypted, were much more likely to decline payment and instead choose to restore or rebuild their systems. This trend coincides with the general decline in the number of ransom payments Arete observed from 2022 to 2023.

Most victims, regardless of the percentage of systems encrypted, were much more likely to decline payment and instead choose to restore or rebuild their systems.

ENCRYPTION AND RANSOM PAYMENT IN THE TOP TEN THREAT ACTORS OBSERVED

THREAT ACTOR	RANSOMWARE OR EXTORTION	RAAS?	% OF VICTIMS FULLY ENCRYPTED	% OF VICTIMS WHO DID NOT PAY THE RANSOM
LockBit	Ransomware	Yes	11%	66%
ALPHV/BlackCat	Ransomware	Yes	6%	50%
Akira	Ransomware	Yes	16%	47%
Black Basta	Ransomware	Yes	17%	62%
Luna Moth	Extortion	No	NA	35%
Play	Ransomware	No	9%	86%
Phobos	Ransomware	Yes	10%	57%
Royal	Ransomware	No	14%	67%
BianLian	Hybrid	No	20%	50%
Cl0p	Hybrid	No	NA	83%

Figure 7: Encryption and ransom payments in the top ten threat actors observed by Arete in 2023

Trends in Data Exfiltration

While conducting root cause analysis, Arete identifies the specific data accessed by threat actors and determines whether the data was exfiltrated from the victim environment. Across all Arete engagements in which data exfiltration could be confirmed, employee data was the most frequently exfiltrated data, followed by client data. In instances of exfiltration, multiple data types were often compromised. Client data and employee data were exfiltrated in nearly half of all engagements where exfiltration occurred. This trend is likely due to the accessibility of this data in victim environments versus any deliberate targeting by the threat actor.

Most Common Tools Used to Exfiltrate Data		
rclone	MegaSync	WinSCP
FileZilla	FTP/SFTP	Microsoft SharePoint built-in folder sync capabilities

40% of Engagements

Confirmed Data Exfiltration

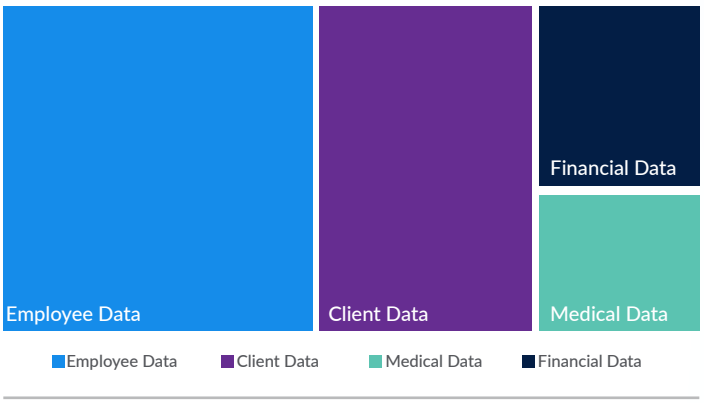

Figure 8: Types of data exfiltrated observed by Arete in 2023

Threat Actors Increasingly Use Dropbox to Exfiltrate Data

Throughout 2023, the Arete observed an increase in threat actors exfiltrating data via Dropbox, shifting from tools like MegaUpload or compromised Amazon Web Services (AWS) S3 buckets. Threat actors are likely using Dropbox due to a combination of three factors:

- Ability to use client deployments of Dropbox as living off the land (LOTL) techniques
- Low or limited cost @ $18 per month
- Large capacity with a minimum of 3TB of space

When using Dropbox, if the application is installed and configured on an endpoint, the Dropbox cache folder becomes a synchronization folder that can be used as a rudimentary or semi-automated method of exfiltration. This means the threat actor does not need to install additional tools to exfiltrate data, which may potentially expose the threat actor's operations. All file changes are synchronized within the dropbox. cache folder, and links/copies of the files are located within the cache folder.

Dropbox simplifies a threat actor's operations, but it also creates opportunities for forensic analysts to identify the specifics of what was stolen. If analysts can correlate Dropbox logins with the Dropbox activity in question, they can confirm the amount of data sent in conjunction with the Dropbox files/folder size obtained from the Dropbox logs.

Logs can be retrieved from Dropbox accounts to identify the activities that occurred during the period in question. Dropbox retains additional detailed logging beyond what is routinely available within the login account. The Dropbox log files record the actions performed at a specific point in time, including creation/uploading, downloading, renaming, deletion, moving, etc. The logs enable analysts to determine which users logged in to download files. The logs also contain more detailed information based on the logging settings, including login events, both successful and failed, and IP addresses for the login. One challenge for forensic analysts is that these logs may be encrypted as part of the configured security settings. This can make determining what information was stolen more challenging.

To help reduce the potential for Dropbox data being impacted during an incident, Arete advises organizations to consider the following:

1. Implement multi-factor or two-step authentication through a randomly generated token application such as Authenticator.
2. Password protect files within Dropbox as an added layer of security by requiring an additional password to be entered to view the files.
3. Limit the usage of the Dropbox application and synching capability on local PC's wherever possible to reduce the chance of local copies of Dropbox files being accessible from endpoints.
4. Limit third-party applications from connecting to Dropbox to reduce the chance of files being synchronized, shared, or accessible through other applications.

Dropbox simplifies a threat actor's operations, but it also creates opportunities for forensic analysts to identify the specifics of what was stolen.

FROM THE HEADLINES

Threat actors using their own or compromised Dropbox accounts also creates a potential data recovery opportunity through the courts. In November 2023, a healthcare network sued Wasabi Cloud Storage for access to and deletion of data the Lockbit ransomware group exfiltrated from the healthcare network's environment during a ransomware attack. The case is still being decided, but it presents a potential path forward for victims whose data is exfiltrated to legitimate cloud storage providers.

Source

https://trellis.law/doc/198318806/summons -complaint

Figure 9: Data exfiltration through legitimate cloud storage providers may create recovery opportunities through legal means.

Exfiltration remains a key tool for extortion. Looking ahead into 2024, threat actors will almost certainly continue to evolve their exfiltration methods to steal more data faster and without being detected.

Evolution of the Threat Landscape

Throughout 2023, threat actors faced many challenges, including internal issues, law enforcement actions, and the geopolitical landscape. In response to these challenges, the top cybercrime groups remained focused on evolving their tactics and investing in their operations to expand their share of the market. These groups attempt to find a balance between attracting top affiliates and avoiding the unwanted attention and risk that come with growth.

Affiliated Problems with RaaS

Insider Threats

While the affiliate model allows RaaS operations to expand their ability to attack victims, it also exposes their operations. The challenge of this model was first highlighted during Conti's demise. Amidst a tense geopolitical landscape at the onset of the Russia-Ukraine conflict, Conti issued a polarizing pro-Russian statement, angering a Ukrainian affiliate and inevitably leading to their proprietary information and source code being leaked in February 2022.

At the beginning of 2023, the risk of insider threats was highlighted when Hive ransomware was taken down in a coordinated law enforcement effort. The effectiveness of the takedown was largely attributed to sloppy Hive affiliates leaving a trail of information for agents to follow. The Federal Bureau of Investigation (FBI) infiltrated and maintained access to Hive's infrastructure for seven months prior to the disruption. While it is likely many affiliates migrated to other RaaS operations, Hive ransomware had not resumed operations under the same brand by the end of 2023.

Closing out 2023, law enforcement took collective action against ALPHV/BlackCat ransomware. Notably, law enforcement was able to persuade a confidential human source to gain access to ALPHV/BlackCat's internal operation, according to an affidavit. Of the many known issues with the affiliate structure, this is the first identified instance of law enforcement agents persuading an affiliate to inform on the ransomware group backing them.

No Honor Among Thieves

While the race to attract affiliates is increasingly competitive, that does not mean that affiliates remain loyal to the RaaS of their choosing. Affiliates have been known to jump back and forth between RaaS operations to utilize capabilities that best fit their targets. For example, this year, a LockBit affiliate pivoted to 3AM ransomware's encryptor after LockBit's encryptor failed to encrypt the victim's environment. Additionally, Arete saw the Scattered Spider threat group shift between using ALPHV/BlackCat's encryptor and conducting solo exfiltration-based extortion attacks. Scattered Spider is emblematic of dynamic groups that adapt their operations to victims and move between the affiliate structure and closed operations, depending on what best meets their needs at a given time. This dynamism is likely to be more common as affiliates seek to insulate themselves from the risk of working with a single RaaS operation.

Lower Barrier of Entry

As assessed in Arete's 2023 Semi-annual Report, the barrier to entry into cybercrime continued to edge lower throughout 2023. Arete saw an increase in the number of engagements believed to be operated by small-scale ransomware or extortion operations. Prospective threat actors are utilizing existing leaked source code, access from IABs, commodity malware, and even AI modules to develop convincing social engineering content and mitigate any technical shortcomings they may have.

A prime example of this is Arete's dealings with the extortionist self-identified as "Mr. Anazon," who registered all website infrastructure within the second half of 2023. Mr. Anazon relied entirely on off-the-shelf tools to gain access and achieve objectives in victim environments. Despite using relatively simple methods, the threat actor has managed to successfully extort multiple victims.

RaaS = Risk Analysis Assessment Service?

As RaaS groups attempt to attract top affiliates, threat actors increasingly must consider the risk associated with visible attacks. For many years, threat actors have enjoyed a level of anonymity and protection from law enforcement actions; however, displacement from global conflict has disrupted this. As RaaS groups target victims, they strive to balance large ransom payouts and capabilities that would attract top affiliates with the associated risk and attention from law enforcement that comes from high profile attacks. Furthermore, as RaaS groups continue to grow, managing affiliates becomes increasingly difficult.

LockBit operators struggled to manage affiliates throughout 2023. Several affiliates leaked encryptors, and the multitude of encryptor offerings made it difficult for the owners to distinguish legitimate affiliate operations from unknown threat actors utilizing previously leaked LockBit ransomware encryptors.

To avoid the risk associated with larger ransomware brands, Arete observed multiple threat actors decline to offer a name during ransom negotiations. These groups stated that they were not sanctioned and that no one needed their name. For these groups, clearly the risk of law enforcement attention overrode the desire to build a big name RaaS brand like Lockbit or ALPHV/BlackCat.

A Return to Vetting Practices

As the affiliate model continues to plague the RaaS ecosystem, it is likely that the model will be rethought. When ransomware groups first began transitioning to the affiliate model, they thoroughly vetted each affiliate and primarily functioned on an invite-only basis. Prominent ransomware groups such as REvil started out operating under this model but transitioned to a less stringent vetting process to drive profits before their downfall. It is likely that RaaS groups will begin slowly transitioning back to a process of stringently vetting their affiliates. However, it is unknown if this will happen under current brands or as existing groups rebrand their present operations.

Ransomware Groups Using Torrents in Data Leak Sites

In August 2023, the Cl0p threat group began leveraging torrents to leak stolen data more efficiently. In addition to the data leak site the group used as part of its extortion tactics, Cl0p created a second TOR site that uses torrents to distribute stolen data. This alternative torrent leak site became necessary primarily due to the large volume of data the group was able to steal following their exploitation of a zero-day vulnerability in the MOVEit secure file transfer platform in late May 2023, an attack that impacted over 2,700 organizations.

Torrenting is a means of distributing and downloading files using a protocol that leverages peer-to-peer (P2P) file sharing to distribute data in a decentralized manner. Data leak sites on TOR have much slower download speeds than other browsers, and Cl0p was one of the first groups to leverage P2P transfer for exposing leaked data, which allows them to distribute stolen data faster and makes it more difficult for law enforcement to take down the leaked data. However, one drawback to this method is that for someone to download the stolen data, it requires someone else with the data to seed the transfer, and Arete has observed occasions where it's taken several days or longer for someone available to seed the file transfer on Cl0P's torrent site.

LockBit also began adding a torrent download option on some of their victims' pages in 2023, likely for faster transfer of large sets of victim data and another means to pressure victims into paying not to release data. The use of these torrent options illustrates how ransomware groups continually find ways to improve their criminal operations. Arete expects other groups will start leveraging torrent sites in 2024 as an alternative to traditional TOR data leak sites. The faster download speeds offer broader accessibility to large sets of leaked data, allowing ransomware groups to threaten their victims with the potential cost and reputational damage that may result from the exposure of their stolen data.

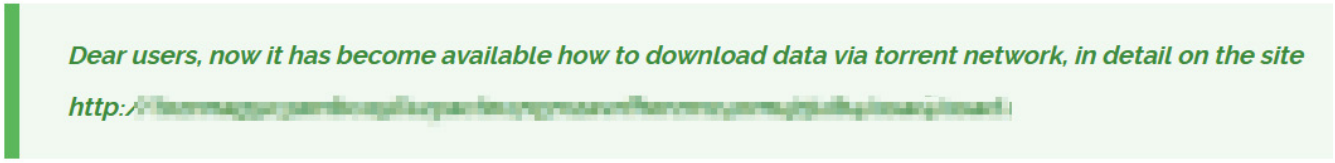

Figure 10: Cl0p announcement of their torrent site

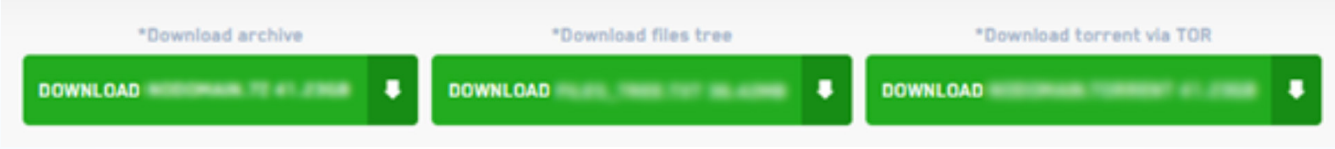

Figure 11: Image of torrent option on LockBit's DLS

Impacts on Critical Infrastructure

CRITICAL INFRASTRUCTURE RANSOMWARE AND EXTORTION IMPACTS

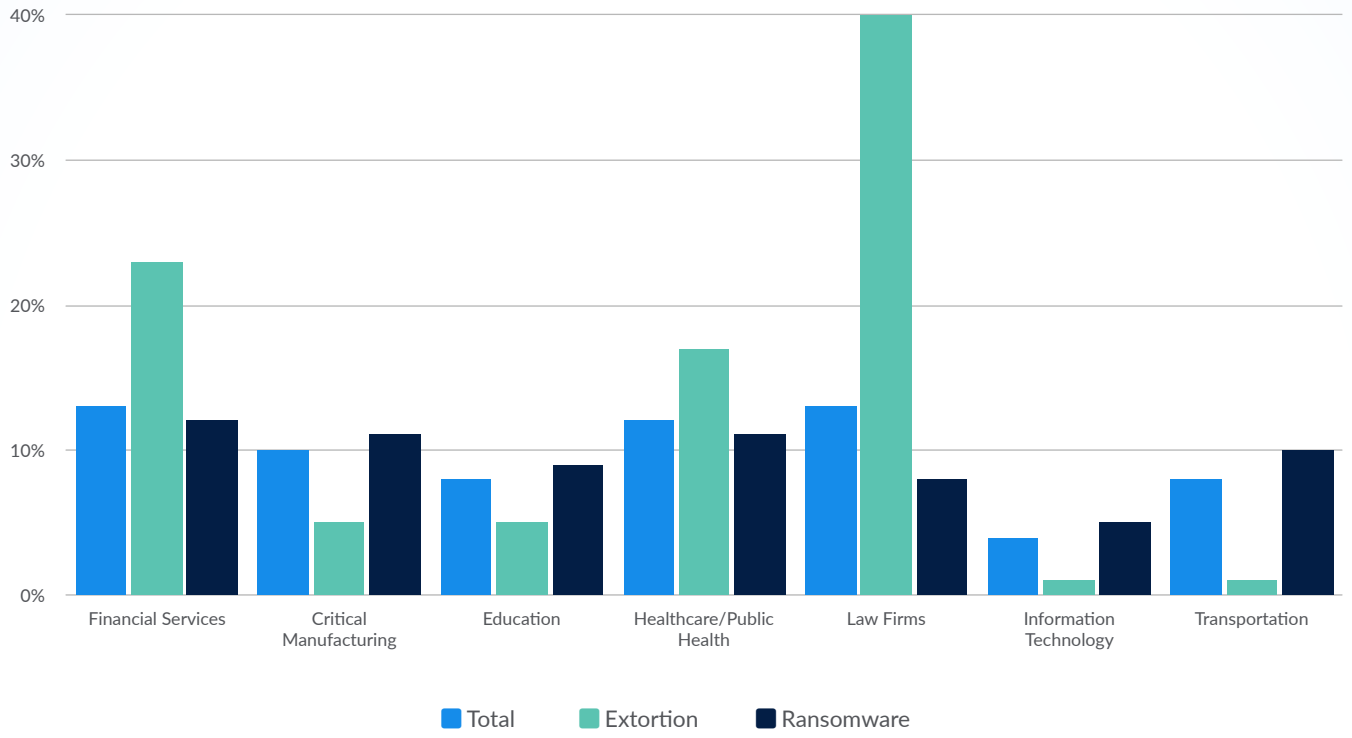

Figure 12: Ransomware and extortion events in critical infrastructure sectors observed by Arete in 2023

Financial services and law firms stood out as the most frequently attacked sectors in 2023, with healthcare/public health coming in at a close third. For deeper analysis, we distinguished between ransomware and extortion events, demonstrating that extortion accounted for a majority of events impacting the top three sectors. The primary differentiator between ransomware and extortion events is that ransomware events involve the use or intended use of encryption to hold data hostage as part of the extortion demand.

Looking solely at ransomware events, the financial services sector remains the most attacked sector, but healthcare/public health, critical manufacturing, and residential/shelter facilities, housing and real estate, and related services come in close second. This variety of impacted sectors indicates that threat actors are considering the value of data and the defenses of these organizations. Ransomware groups that attacked the financial services and healthcare/public health sectors appeared to target those organizations with the understanding they could demand higher ransoms due to the sensitivity of the data. However, residential/shelter facilities, housing and real estate, and related services were almost all impacted by opportunistic threat actors.

Financial services and law firms stood out as the most frequently attacked sectors in 2023, with healthcare/public health coming in at a close third.

When we consider why organizations decided whether to pay a ransom, no sector was significantly more or less likely to have backups or to accept the cost of recovery. Sector did not have a significant impact on whether a victim paid a ransom. Organizations across all sectors should implement controls, including robust backups, to increase cyber resilience in today's threat landscape.

Timing Is Everything – Real-World Events Impacting Sector Targeting

During Fall 2023, Arete anticipated a notable increase in activity against education and municipal governments, including entities like fire departments and police departments, after noting a similar pattern in 2022.

Surprisingly, there was no such increase in Fall 2023, and this absence led to the hypothesis that these institutions might have been targeted due to their role as polling locations during elections, making them more vulnerable. As we look forward to 2024, it is possible that this specific targeting of education and municipal governments will resurface in the fall months.

Top Malware and Tools Used by Threat Actors

Malware is software created specifically for malicious use, while tools are pieces of software that often also have legitimate use. Threat actors build malware to carry out specific actions like encryption, but they increasingly rely on tools with legitimate uses, as they may allow the threat actor's operations to go undetected for longer.

Ransomware Groups Consistently Innovate on Ransomware Payload

Throughout 2023, Arete observed threat actors increasingly leverage ransomware executables that both required command line arguments to execute and delete the ransomware after execution.

Some ransomware groups included the ability to self-delete within the executable itself, while groups like LockBit created a .tmp file containing separate instructions for the executable to delete itself. Arete also observed the D0nut threat group using separate utilities to self-delete, which is likely to enable its operations to be more modular.

INC ransomware demonstrated another relatively rare technique in 2023: downloading the ransomware executable as an image. While threat actors have used the capability to spread malware using images (called steganography), the technique is rarely employed to download a ransomware executable. After the threat actor's downloader was installed on the system, the threat actor downloaded the image, decrypted it, and then executed the ransomware payload. The image is likely intended to help the threat actor evade traditional anti-virus tools.

Arete observed threat actors increasingly leverage ransomware executables that both required command line arguments to execute and delete the ransomware after execution.

Leaked Source Code and Ransomware Builders

Throughout 2023, threat actors complicated identification by working with multiple ransomware brands, refusing to name themselves, and, perhaps most challengingly, by using leaked ransomware source code and builders to enable their operations.

Babuk source code

Arete observed more than a dozen threat groups in 2023 use ransomware encryptors based on the Babuk source code leaked in 2022. Some groups iterated on the code and only used portions of it, while other groups used nearly the exact code. The groups would modify the ransom note and update the threat actor's contact information, but otherwise operations remained the same.

Chaos ransomware builder

Across the one-off named ransomware variants Arete observed in 2023, several appeared to have been created using the Chaos ransomware builder. The builder was first observed in 2021 and has undergone multiple rounds of development. Ransom notes produced by this builder were all fairly similar, with slight customizations specific to each threat actor deploying it.

Other groups with source code leaked in 2023 included HelloKitty ransomware and Zeppelin ransomware. In 2022, Conti's and LockBit's source codes were both leaked, and Arete observed them being utilized by a limited number of threat actors in 2023.

Leaked source code and builders make attribution of threat actors very challenging. Determining who the threat actor is, and consequently, whether that threat actor is sanctioned, requires examining all facets of a threat actor's operations, including their techniques, infrastructure, and tools.

The Usual Suspects Enable Threat Actor Operations

Throughout 2023, Arete saw several threat actors use the same tools to enable their operations prior to deploying their own encryptor. The most frequently observed malware included CobaltStrike, Mimikatz, malicious PowerShell Scripts, and SocGholish. All four tools provide threat actors with different capabilities but have certain artifacts that enable defenders to detect and disrupt the activity. Therefore, these pieces of malware are often downloaded using legitimate remote monitoring and management (RMM) tools like SplashTop, Atera, ScreenConnect, or TeamViewer. RMM tools are often present in companies' environments for IT or vendors to perform critical functions. Therefore, when threat actors download their own version into a victim's environment or hijack an existing RMM, it may escape notice. This gives the threat actor regular, uninterrupted access to perform other actions, like disabling security tools that may detect Mimikatz or CobaltStrike.

Stopping threat actors before they deploy malware requires tracking and securing RMMs using MFA, allowlisting RMM IDs authorized to an environment, and blocking those not allowed.

Law Enforcement Actions and the Ransomware Ecosystem

In 2023, international law enforcement agencies markedly accelerated the pace and sophistication of their actions against various facets of the cybercriminal ecosystem. A notable development was the increased use of 'hack-back' techniques by law enforcement to infiltrate and disrupt criminal operations. These techniques successfully dismantled multiple encrypted communication platforms, dark web markets, hacker forums, illegal cryptocurrency exchanges, and ransomware/botnet infrastructures. Joint efforts led to the arrest of over 4,000 cybercriminals worldwide, including more than 20 core members of ransomware groups.

Notable Law Enforcement Operations in 2023

JANUARY 2023
The Justice Department announced a successful disruption campaign against Hive ransomware.

AUGUST 2023
The FBI announced the disruption of the Qakbot botnet through a multi-agency, global operation, including the U.S., France, Germany, the Netherlands, Romania, Latvia, and the United Kingdom.

OCTOBER 2023
The Ragnar Locker ransomware group was dismantled through a significant international law enforcement operation coordinated by Europol and Eurojust.

DECEMBER 2023
The Justice Department disrupted the ALPHV/BlackCat ransomware group.

Among the most significant law enforcement operations were those executed against Hive, Qakbot, Ragnar Locker, and ALPHV/BlackCat.

In January 2023, the Justice Department announced a successful disruption campaign against Hive ransomware. This notorious cybercriminal organization targeted over 1,500 victims across more than 80 countries, including key sectors such as healthcare, education, finance, and infrastructure. Starting in July 2022, the FBI covertly infiltrated Hive's networks, capturing and distributing decryption keys to global victims, thereby preventing ransom payments totaling $130 million. In total, the FBI provided over 300 decryption keys to recent victims and an additional 1,000 to former victims. Collaborating with German and Dutch law enforcement, the FBI also seized Hive's servers and websites, significantly crippling its operations.

In August 2023, the FBI announced the disruption of the Qakbot botnet through a multi-agency, global operation, including the U.S., France, Germany, the Netherlands, Romania, Latvia, and the United Kingdom. Qakbot was one of the most frequently observed tools enabling initial access for ransomware operations. The disruption of Qakbot forced ransomware groups to switch to new tools and vulnerability exploits.

In October 2023, the Ragnar Locker ransomware group was dismantled through a significant international law enforcement operation coordinated by Europol and Eurojust. Known for its high-profile attacks on

global critical infrastructure, the group was disrupted through coordinated actions in several countries. The pivotal arrest occurred in Paris on October 16, supplemented by searches and interviews in Czechia, Spain, and Latvia. The primary suspect, an alleged developer for the group, was presented to the Paris Judicial Court. The ransomware's infrastructure, including its data leak website on TOR, was seized and taken down in the Netherlands, Germany, and Sweden. This operation was a continuation of a complex investigation involving multiple countries, led by the French National Gendarmerie, and building on previous arrests in Ukraine in October 2021.

In December 2023, the Justice Department disrupted the ALPHV/BlackCat ransomware group. This group targeted over 1,000 networks globally, including U.S. critical infrastructure. This intervention aided over 500 victims worldwide and prevented approximately $68 million in ransom payments. The operation involved accessing BlackCat's network, seizing its websites, and leveraging international law enforcement cooperation. Despite this disruption to ALPHV/BlackCat's infrastructure, the group quickly resumed operations.

Looking back, 2023 showed optimistic trends in law enforcement efforts. The multi-pronged approach of law enforcement against the cybercriminal ecosystem yielded direct results, progressively disrupting criminal operations and enhancing global digital security.

2024 Outlook

Throughout 2023, Arete observed ransomware and extortion groups launching more frequent attacks, enhancing malware tools, expanding attack surface, and implementing sophisticated techniques to access data and evade detection. This continued evolution leads Arete to surmise that we will see a similar or even increased frequency of cyberattacks in 2024.

The threat landscape has recently seen both collaboration and competition between groups as they face sustained pressure from global law enforcement. These business-like mergers and competitions are likely to increase in 2024 as groups work to attract affiliates and expand their market share. Increasing specialization in the cybercrime ecosystem will make partnerships between groups more crucial for enabling operations.

Initial access to victim environments will likely continue to be primarily outsourced in 2024, with many threat actors relying on public exploit code as well as stolen credentials and commodity Trojans sold by initial access brokers. Arete expects to see some groups invest in vulnerability exploit development to enable large-scale compromises that impact many victims simultaneously. Attack speed may also factor into the scale of these campaigns, as groups seek to compromise as many victims as possible before effective defenses are implemented. This will likely create outsized impacts from a few targeted events.

As we saw in 2023, Arete expects some organizations to continue to avoid paying ransoms by employing robust backups. To counteract this lost revenue, threat actors will likely continue demanding higher ransom payments. However, other threat groups may maintain a pattern of smaller ransom demands, expecting that victims may be more willing to pay smaller ransoms. Regardless, some threat actors are likely to be frustrated by declining payments and resort to threats of physical violence.

We expect to see the cybercrime ecosystem continue to expand and attract new players, fueled by the sale of crimeware services and leaked ransomware source code and builders. These newcomers may stand up data leak sites and maintain an active social media presence to form their reputations, but more mature threat groups are likely to continue to avoid naming themselves, as operating under a single name attracts attention from law enforcement. This expansion will make attribution more complex and require in-depth, multi-layered tracking and analysis.

We expect to see the cybercrime ecosystem continue to expand and attract new players, fueled by the sale of crimeware services and leaked ransomware source code and builders.

Threat actors will likely continue developing faster and stealthier methods for data exfiltration, including relying more on Dropbox and cloud syncing tools that already exist in victim environments. Due to the utility of encryptors for enabling targeted law enforcement operations, some groups may also shift towards exfiltration-only attacks.

Preventing, detecting, and responding to cybercrime in 2024 will require an end-to-end, data-driven approach. Arete's teams will continue to address risk at every stage of the threat lifecycle and empower our global clients and partners with actionable data and insights.

Sources

[1] Notes ;-) (ransomlook.io)

[2] https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-158a

- Threat Actor Insights
- Arete Internal Data
- Ransomware Data Leak Sites
- https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-165a
- https://twitter.com/vxunderground/status/1618885718839001091/photo/2
- https://www.bleepingcomputer.com/news/security/lockbit-ransomware-goes-green-uses-new-conti-based-encryptor/
- https://blog.talosintelligence.com/understanding-the-phobos-affiliate-structure/
- https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-061a
- https://github.com/srlabs/black-basta-buster
- https://www.ic3.gov/Media/News/2023/231113.pdf
- https://krebsonsecurity.com/2022/06/ransomware-group-debuts-searchable-victim-data/
- https://www.bleepingcomputer.com/news/security/ransomware-gang-cloned-victim-s-website-to-leak-stolen-data
- https://securityscorecard.com/research/a-deep-dive-into-black-basta-ransomware/
- https://krebsonsecurity.com/2023/12/blackcat-ransomware-raises-ante-after-fbi-disruption/
- https://www.darkreading.com/cyberattacks-data-breaches/hunters-international-cyberattackers-take-over-hive-ransomware
- https://therecord.media/hive-ransomware-decryptors-fbi-bryan-smith-interview-click-here
- https://www.justice.gov/opa/pr/justice-department-disrupts-prolific-alphvblackcat-ransomware-variant
- https://www.virustotal.com/gui/file/cf43074cc3c077418b126a9f03cd23c1cf6a2364752fb19aa68a8b0b4461b818/behavior
- https://www.cyber.nj.gov/garden_state_cyber_threat_highlight/evolving-extortion-tactics-in-ransomware-attacks
- https://www.microsoft.com/en-us/security/blog/2023/10/25/octo-tempest-crosses-boundaries-to-facilitate-extortion-encryption-and-destruction/
- https://www.darkreading.com/cyberattacks-data-breaches/swatting-latest-extortion-tactic-ransomware-attacks
- https://www.theregister.com/2024/01/05/swatting_extorion_tactics/
- https://www.justice.gov/usao-cdca/pr/members-hacker-collective-face-federal-charges-attacking-computer-systems-emailing-mass
- https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-131a
- https://www.trendmicro.com/en_se/research/21/h/chaos-ransomware-a-dangerous-proof-of-concept.html
- https://www.bleepingcomputer.com/news/security/hellokitty-ransomware-source-code-leaked-on-hacking-forum/

Sources

- https://chuongdong.com/reverse%20engineering/2022/03/19/LockbitRansomware/
- https://github.com/gharty03/Conti-Ransomware
- https://www.bleepingcomputer.com/news/security/hellokitty-ransomware-source-code-leaked-on-hacking-forum/
- https://cybernews.com/news/putin-team-ransomware-emerges-from-leaked-contis-source-code/
- https://www.bleepingcomputer.com/news/security/clop-ransomware-now-uses-torrents-to-leak-data-and-evade-takedowns/
- https://socradar.io/the-torrent-landscape-understanding-security-risks-and-the-future/
- https://www.emsisoft.com/en/blog/44123/unpacking-the-moveit-breach-statistics-and-analysis/
- https://www.zdnet.com/article/what-is-torrenting-and-how-does-it-work/
- https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-158a
- https://twitter.com/vxunderground/status/1702925435443585286
- https://socradar.io/lockbits-new-regulations-sets-minimum-for-ransom-demands/
- https://cybersecuritynews.com/lockbit-demands-3-revenue-ransom/
- https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-136a
- https://www.bleepingcomputer.com/news/security/bianlian-ransomware-gang-shifts-focus-to-pure-data-extortion/
- https://www.hipaajournal.com/ransomware-gang-ups-the-ante-by-publishing-naked-images-of-patients/
- https://www.databreaches.net/two-california-plastic-surgery-practices-suffer-cyberattacks-and-embarrassing-patient-data-leaks/
- https://www.databreaches.net/alphv-files-an-sec-complaint-against-meridianlink-for-not-disclosing-a-breach-to-the-sec/
- https://www.bleepingcomputer.com/news/security/how-the-fbi-seized-blackcat-alphv-ransomwares-servers/
- https://krebsonsecurity.com/2023/12/blackcat-ransomware-raises-ante-after-fbi-disruption/
- https://www.justice.gov/opa/pr/us-department-justice-disrupts-hive-ransomware-variant
- https://www.fbi.gov/news/stories/fbi-partners-dismantle-qakbot-infrastructure-in-multinational-cyber-takedown
- https://www.europol.europa.eu/media-press/newsroom/news/ragnar-locker-ransomware-gang-taken-down-international-police-swoop
- https://www.justice.gov/opa/pr/justice-department-disrupts-prolific-alphvblackcat-ransomware-variant

Cyber Emergency Helpline 866 210 0955
Phone 646 907 9767

New Engagements
arete911@areteir.com

General Inquiries
marketing@areteir.com

www.areteir.com