NOVEMBER | 2024

Arete

Crimeware Report

Trends and Highlights from Q3 2024

Table of Contents

Overview

Arete's global teams gather data and insights from every aspect of the threat lifecycle. From incident response and restoration to threat actor communications and managed services, this comprehensive visibility informs our understanding and analysis of the threat landscape. Leveraging data collected during incident response engagements, we 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. This report details the trends observed during Arete's response to ransomware and extortion attacks from July 1 through September 30, 2024.

International law enforcement's disruption of the two most prolific Ransomware-as-a-Service (RaaS) groups at the beginning of the year led to the development of a fractured and unpredictable threat landscape by the end of Q2 2024. In Q3, the ransomware ecosystem remained diverse, with roughly the same number of known and unique unnamed threat actors observed by Arete during the quarter as observed in Q1 and Q2. However, the evenly distributed ransomware and extortion activity observed throughout Q2 began to consolidate, as a few select RaaS groups appeared increasingly frequently and were responsible for a greater percentage of the overall activity in August and September.

Across the ransomware and extortion incidents Arete responded to in Q3, several notable trends emerged:

- Akira and RansomHub dominated the ransomware landscape in Q3. Together, the two groups were responsible for 40% of all engagements in August and 35% of all engagements in September. RansomHub, in particular, has grown rapidly as a RaaS since appearing in February of this year and will likely remain one of the top threats for the rest of 2024.
- New ransomware groups continued to emerge throughout Q3, with newcomers like Lynx and Cicada3301 bearing similarities to RaaS organizations that previously shut down their operations or reportedly sold their source code.
- The percentage of companies and organizations paying ransoms remained low in Q3, but there was an increase in both initial demands and median payments made.
- In Q3, threat actors did not appear to intentionally target specific industries, unlike in Q2 when the Fog ransomware group regularly targeted organizations in the education sector.
- Cybercriminals continued to leverage most of the same malware variants and legitimate tools observed in the first half of 2024, except Cobalt Strike, which was observed notably less in Q3.

The shifts that Arete observed in the threat landscape during Q3 demonstrate that threat actors are increasingly adaptive and continue to evolve their tactics and operations.

Q3 2024 Highlights from Arete's Incident Response Cases

Total Named Threat Actors		
32	36	37
Q3 2024	**Q2 2024**	**Q1 2024**

Total Unnamed Threat Actors		
17	12	11
Q3 2024	**Q2 2024**	**Q1 2024**

MOST OBSERVED THREAT GROUPS IN Q3

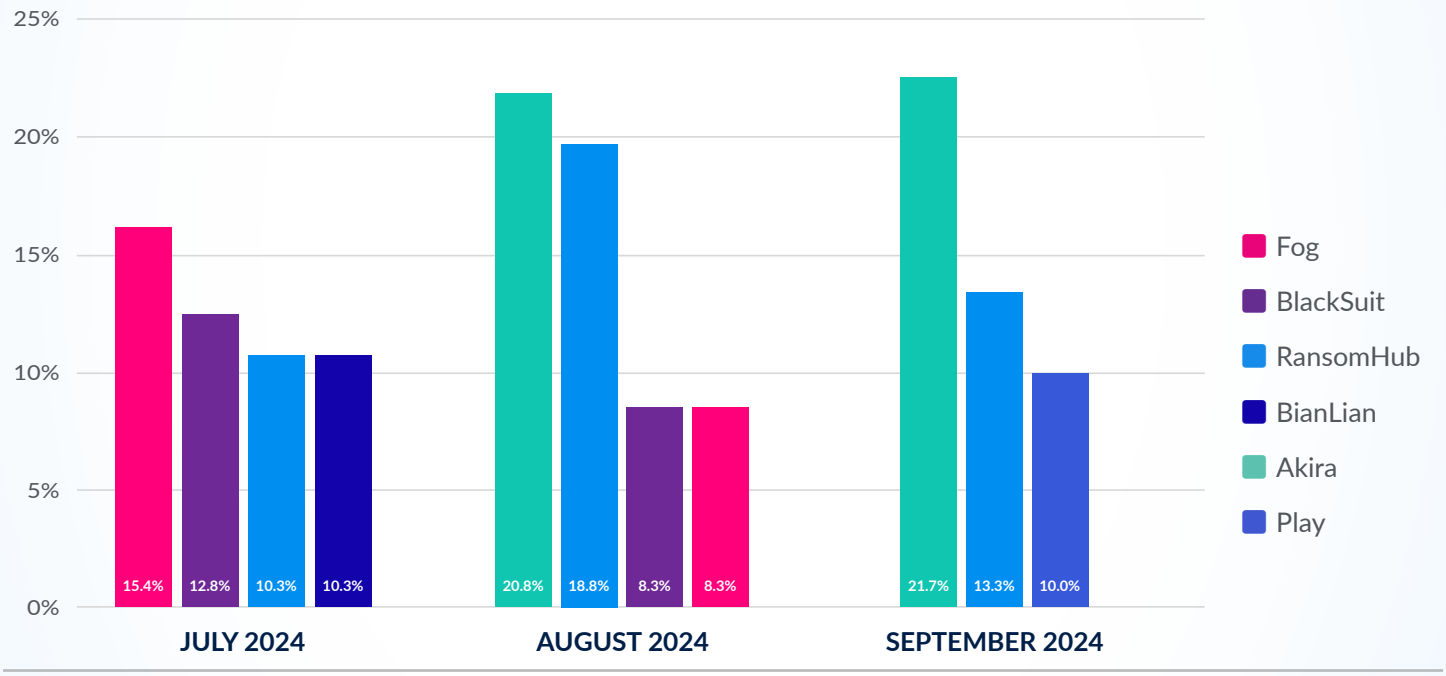


Figure 1

Law enforcement's disruptions of LockBit and ALPHV/BlackCat's operations at the beginning of 2024 created an unpredictable cyber threat landscape. Several newer and lesser-known threat groups from the first half of the year have since become formidable and active threats in Q3. The most notable is RansomHub, one of the top three most active groups during every month of Q3, trailing behind only Akira in August and September.

Another newer group that became a persistent threat in the second half of the year was Fog, which Arete reported on in detail in our Malware Spotlight in August. BlackSuit also remained one of the top ransomware threats in Q3 and was among the top three most active groups in July and August.

Alongside these new and emerging groups, more established groups like Akira, Play, and BianLian remained consistently active throughout the quarter.

Akira was the third most observed ransomware group in the second half of 2023 behind LockBit and ALPHV, so it comes as no surprise that it became the top threat actor in 2024, now that ALPHV shut down its operation and LockBit struggles to maintain relevance in the current ransomware landscape.

In Q3, Arete observed 32 separate named threat groups, slightly lower than the numbers identified in Q1 and Q2. Conversely, Q3 had a higher number of unnamed threat groups that operated distinctly from one another, with 17 unique unnamed groups in Q3, compared to 12 in Q2 and 11 in Q1. Arete assesses this uptick in Q3 to be attributed to our continually evolving analysis and attribution of unknown threat groups over time, as opposed to an increase in threat actors operating independently. Our Threat Intelligence team applies data and insights to past and present incident response cases to accurately attribute threat groups when possible. For example, in our Q1 2024 Crimeware Report, Arete noted 18 unnamed threat groups, which has since decreased to 11. Some of the threat actors Arete retroactively identified from earlier in the year include Nitrogen, Mimic, TRON L1, Red Ransomware, Radar/Dispossessor, and NDA Leaks.

Arete's Threat Intelligence team applies data and insights to past and present incident response cases to accurately attribute threat groups when possible.

An Unpredictable Ransomware Landscape Becoming Predictable Again

With ALPHV's halt in operations and LockBit's struggle to maintain a steady pace, the threat landscape remained unpredictable but became more evenly distributed by the end of Q2. The majority of ransomware and extortion activity was no longer dominated by a small number of threat actors. Activity from the top three threat groups comprised just over 28% of all engagements observed by Arete in Q2, a decrease of over 10% from what had been observed in Q1.

However, this trend shifted in Q3. By the end of the quarter, Akira and RansomHub emerged as the most consistently active threat groups. They were particularly active in August; combined, they were responsible for 40% of all ransomware engagements during the month. Akira has remained active since it emerged in 2023, and Arete assessed in our Q1 2024 Crimeware Report that it would likely become one of the top threat groups with ALPHV and LockBit no longer dominating.

RansomHub is the more surprising of the two, as the group was only first seen in February of this year. However, RansomHub has become one of the most significant threats in the cyber landscape, demonstrating rapid growth and increased operational sophistication during Q3 2024. Part of this growth can likely be attributed to the active recruitment RansomHub operators conducted on dark web forums earlier in the year, which was aimed specifically towards ex-affiliates of ALPHV and LockBit. The group offered a generous 90/10 split, with affiliates responsible for providing their crypto wallet to the victim and paying RansomHub its 10% cut after payment is received. RansomHub's RaaS also appears to be open to existing groups rather than just individual affiliates, with threat groups like NoName and Scattered Spider reported to be working with RansomHub as affiliates.

RansomHub was not the only RaaS group working with Scattered Spider in Q3. In July, Scattered Spider was reportedly using Qilin ransomware in its attacks. Notably, Scattered Spider was also an affiliate of ALPHV prior to its shutdown, illustrating that while law enforcement disruptions have been a positive trend in 2024, threat groups continue to quickly adapt afterward, aligning themselves with other RaaS brands or starting new ransomware operations.

RansomHub has become one of the most significant threats in the cyber landscape, demonstrating rapid growth and increased operational sophistication during Q3 2024.

MARKET SHARE OF TOTAL ENGAGEMENTS BY TOP 3 THREAT GROUPS

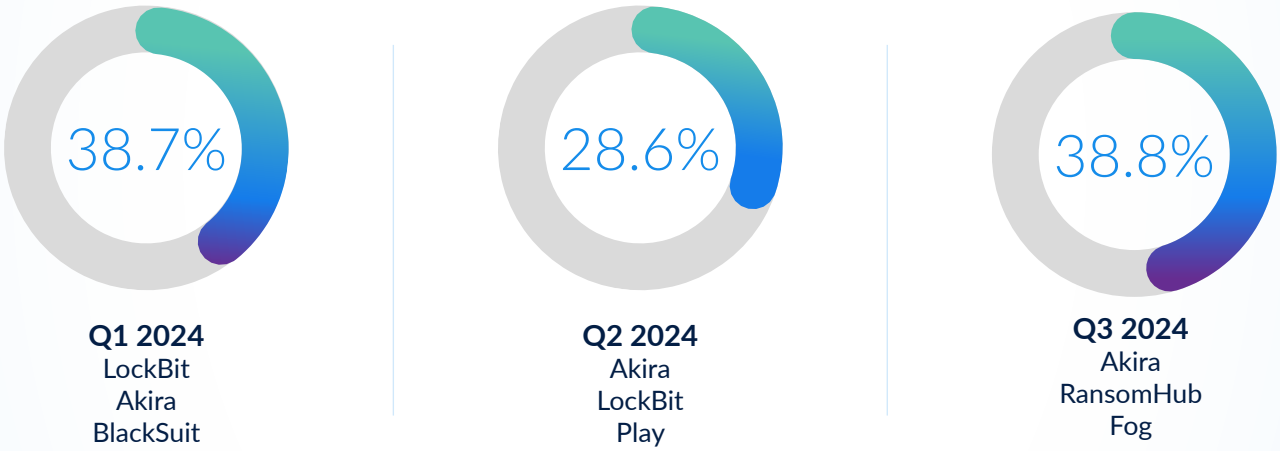
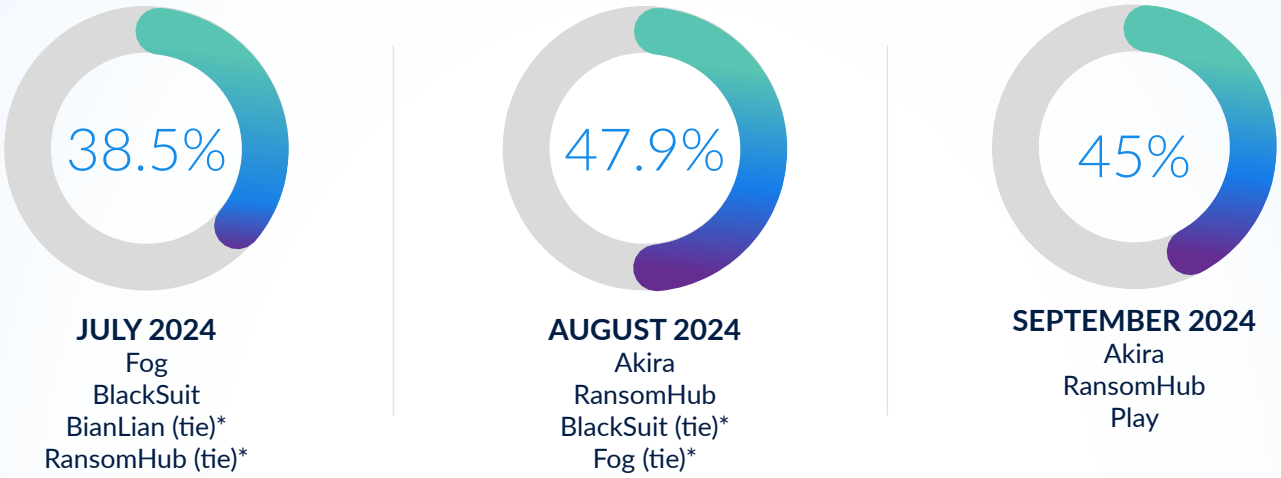


Figure 2

MARKET SHARE OF TOTAL ENGAGEMENTS BY TOP 3 THREAT GROUPS IN Q3 BY MONTH



*Percentage includes only one of the threat groups tied for the top three.

Figure 3

Threat Actor Spotlight: RansomHub

RansomHub operates as a RaaS operation and is known for its effective cybercrime operations and rapid development. Arete first observed RansomHub in May 2024, although the group was active since the beginning of the year, recruiting in dark web forums and posting victims to its data leak site since February. The group encrypts both Windows and Linux operating systems to broaden its scope and potential impact on various environments and impacts organizations across multiple sectors, including healthcare, government, and technology. The group and its affiliates typically operate with a double extortion model, exfiltrating data while encrypting victims' systems to coerce ransom payments.

RansomHub exploits known vulnerabilities for initial access in software and devices, including Apache ActiveMQ, Atlassian Confluence, Citrix ADC, F5 BIG-IP, and Fortinet FortiOS. After gaining access to victim environments, RansomHub recently integrated a new tool—EDRKillShifter—into its attack chain. EDRKillShifter uses vulnerable drivers to terminate endpoint detection and response software.

The sophisticated tactics and rapid evolution of RansomHub highlight the capability of high-volume groups to turn their profits into more advanced capabilities.

For persistence, RansomHub creates user accounts with admin privileges, re-enables disabled accounts, and uses Mimikatz to gather credentials. For lateral movement, the group often uses Remote Desktop Protocol (RDP), PsExec, and Cobalt Strike. Additionally, its ransomware employs intermittent encryption to expedite the attack process, with data exfiltration carried out using tools like PuTTY and AWS S3 buckets. The sophisticated tactics and rapid evolution of RansomHub highlight the capability of high-volume groups to turn their profits into more advanced capabilities.

Under New Management: New (Old) Threat Groups Emerge in Q3

Although Akira and RansomHub could likely remain the top ransomware groups for the remainder of the year, new threat groups continued to emerge in Q3. Two new RaaS groups, Lynx and Cicada3301, demonstrate overlaps with previous RaaS organizations.

Lynx

In late July, Arete observed a new RaaS group calling itself Lynx. Multiple open-source reports outline similarities between Lynx and INC ransomware, suggesting that Lynx is a possible rebranding of INC. In mid-May 2024, Arete reported that INC announced on dark web forums that it was selling its source code. Arete also noted that the clearnet data leak site domains for both INC ransomware and Lynx share the same registrar and servers, as well as similarities in registrant contact information.

Cicada3301

A new RaaS calling itself Cicada3301 emerged in late Q2, with Arete observing activity from the group starting in August. Open-source reports note several significant code overlaps between Cicada3301's ransomware and the ransomware previously used by ALPHV—the once prolific threat group that shut down its RaaS operations earlier this year following law enforcement actions. In addition to the code overlaps, Arete observed stylistic similarities in the format and design of the Tor chats Cicada3301 uses to communicate with and extort its victims and the Tor chats ALPHV used.

At this time, it is too early to assess whether the similarities between these groups are coincidental, a rebranding in the wake of law enforcement disruptions, or if these new groups are working with former developers from the previous RaaS groups or purchasing the ransomware code. Following law enforcement disruptions to ALPHV and LockBit earlier this year, Arete expected that affiliates would rebrand or re-affiliate with other threat groups or that other RaaS operations may rebrand to avoid law enforcement scrutiny, so any of these connections are plausible.

Trends in Q3 Ransom Demands and Payments

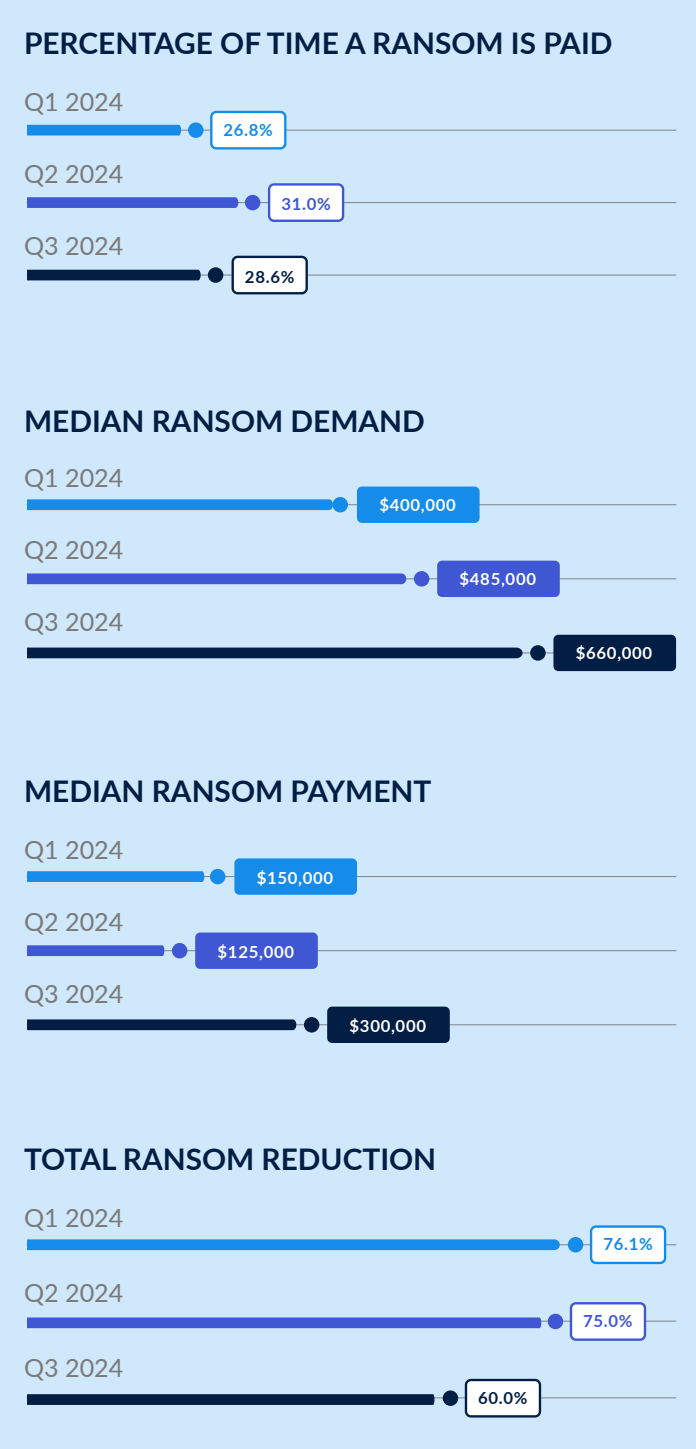


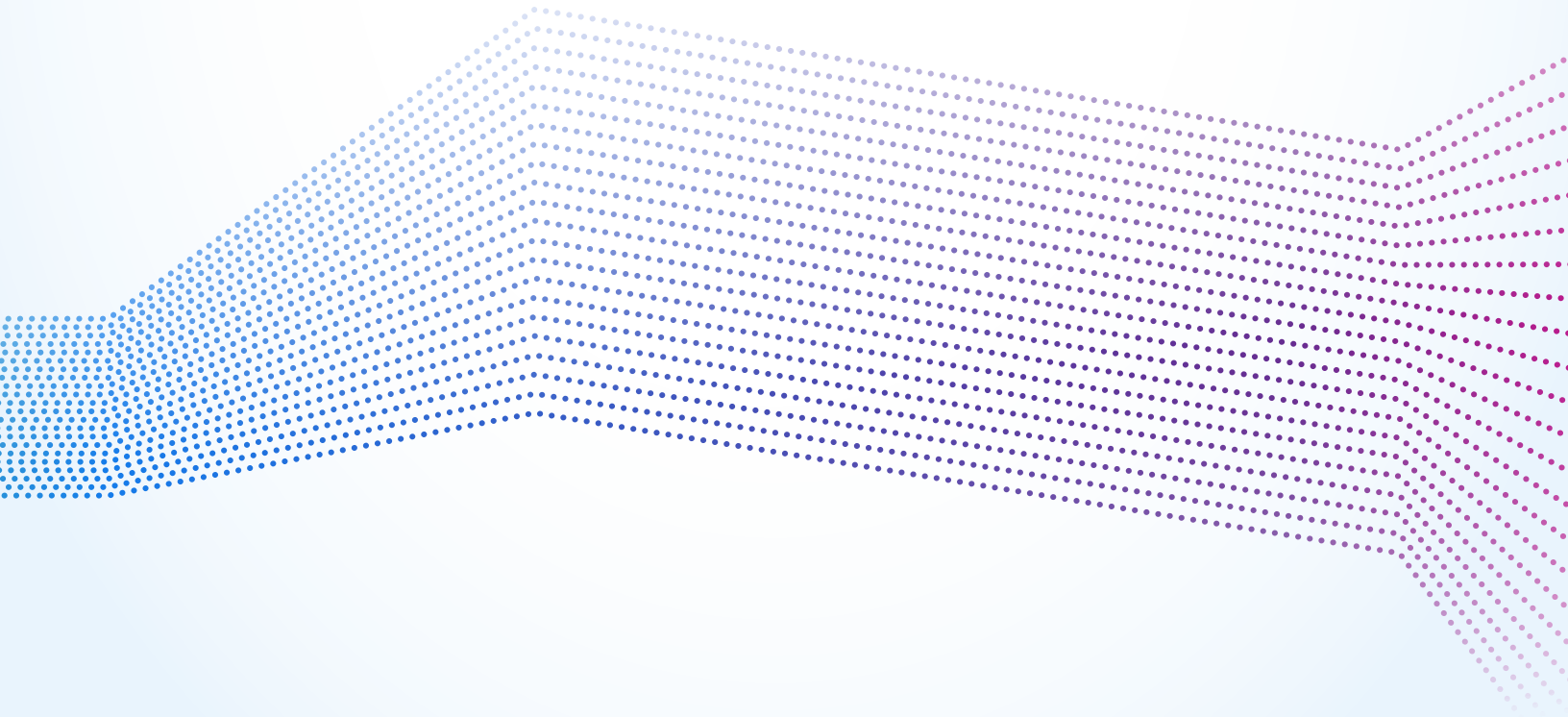
Figure 4

The percentage of companies and organizations paying ransoms demanded by threat actors remained low in Q3, consistent with the first half of 2024. This percentage sharply declined throughout 2023 and appears to have plateaued in 2024, with ransom payments being made on average in only 29% of all ransomware and extortion engagements throughout this year.

There was a sharp increase in the initial ransom amounts demanded by threat actors during Q3. Along with higher demands, the total ransom reduction for the quarter also declined, resulting in an increase in median ransom payments made during the quarter. Multiple factors appear to have contributed to this shift. RansomHub and Fog, two newer ransomware groups that became significantly more active in Q3, received over a third of all ransoms paid during the quarter, and a majority of their initial demands were at or above $1 million. August, in particular, was an outlier, with a median ransom payment of $500,000, compared to just $225,000 in July and $157,500 in September. Additionally, established groups like Akira have increased their initial demands over the year. Akira's median initial demand was $400,000 in Q1 and $500,000 in Q2. In Q3, their median initial demand increased to $700,000.

Given the multitude of variables surrounding each individual ransom payment, it is difficult to predict whether this trend will continue for the remainder of the year. With the splintering of threat groups in 2024, newer groups can be unpredictable in their willingness to negotiate ransom demands as they attempt to establish themselves in the threat landscape. Additionally, with fewer companies paying ransoms, threat groups could be increasing their demands to account for the number of victims who refuse to pay. The lower percentage of organizations making ransom payments remains a positive trend for the quarter, suggesting that companies are better prepared to respond to ransomware or extortion attacks. However, if ransomware demands continue to rise, it is increasingly important for organizations to take proactive steps to protect themselves and mitigate cyber risk.

The lower percentage of organizations making ransom payments remains a positive trend for the quarter, suggesting that companies are better prepared to respond to ransomware or extortion attacks.



Sector Impacts and Threat Actor Targeting

The North American Industry Classification System (NAICS) is the standard used by federal agencies to classify U.S. business organizations. The Cybersecurity and Infrastructure Security Agency (CISA) uses its own classification system of critical infrastructure sectors based on the role of those sectors in national security. Arete uses both classifications to better understand the impact of ransomware and extortion activity and identify trends in threat actor behavior indicative of targeting. Arete focuses on NAICS Industry Sector identification for the analysis in this report. The view of data from a CISA sector perspective is available upon request.

After a slight decrease in Q2 2024, the Manufacturing industry returned as the most impacted sector but remained in the top five industries most capable of recovering without a ransom payment. After being the most victimized sector in Q2 2024, the Professional, Scientific, & Technical Services industry returned to second place in Q3, accounting for about 16% of total engagements. Construction, Information Technology, and a fifth-place tie between Healthcare & Social Assistance and Public Administration rounded out the most impacted sectors.

Few threat actors demonstrated overt signs of intentionally targeting specific industries in Q3, contrary to Q2 when the Fog ransomware group demonstrated intentional targeting of the Educational Services sector. Rather, Manufacturing's status as the most impacted sector arose from many of the top threat groups showing a slight skew towards Manufacturing. Manufacturing organizations accounted for approximately 50% of Play victims, 25% of Akira victims, and nearly 20% of both Fog and RansomHub's victims. There was not a notable trend in initial access mechanisms used to target this sector.

Professional, Scientific, & Technical Services was the only sector that appeared to be intentionally targeted in Q3, accounting for 60% of the BianLian extortion group's attacks. This was also the only sector that saw more extortion than ransomware attacks, indicating there was no encryption associated with most incidents. This trend likely resulted in lower ransom demands and ransom payments for this sector, whose median ransom payment was less than half the next closest sector.[1] While BianLian uses a variety of initial access methods, its success in victimizing this industry may be related to the group's tendency to compromise email tenants. This tactic allows BianLian to learn about potential connections that may be instructive for future targeting.

The Rhysida ransomware group was the only group that showed a tendency to impact Healthcare & Social Assistance organizations within our data, with nearly half of Rhysida victims being in that sector. In broader industry reporting, the RansomHub and Qilin RaaS groups have launched highly disruptive attacks against the Healthcare & Social Assistance industry. While RansomHub and Qilin both rely on a variety of initial access techniques, Arete tracked a Rhysida campaign during Q3 in which threat actors leveraged fake Microsoft Teams applications to deliver the CleanUp loader malware into victim environments.

Beyond sector, Arete saw the Play ransomware group demonstrate the most notable trend towards impacting organizations with higher revenue. The average annual revenue of Play ransomware victims was $250 million. Combined with the group's propensity to rapidly post victims to data leak sites, victim revenue may be the key driver behind the group's relatively high median initial ransom demand of $1.5 million in 2024 and correspondingly high median ransom payment. This trend may indicate a targeting preference, making the Play ransomware group one of the few threat actors to intentionally seek out profitable targets.

[1]Arete intentionally does not release specific payment trends per industry in order to avoid advising threat actors. These numbers are available on request.

Sector Impacts and Threat Actor Targeting

NAICS Sector Name	Percentage of Engagements
Manufacturing	19.15%
Uncategorized	16.31%
Professional, Scientific, & Technical Services	15.60%
Construction	7.09%
Information	7.09%
Public Administration	4.96%
Healthcare & Social Assistance	4.96%
Wholesale Trade	4.26%
Finance & Insurance	4.26%
Other Services (except Public Administration)	3.55%
Educational Services	2.84%
Retail Trade	2.13%
Administrative & Support & Waste Management & Remediation Services	2.13%
Transportation & Warehousing	1.42%
Real Estate & Rental & Leasing	1.42%
Agriculture, Forestry, Fishing & Hunting	0.71%
Management of Companies & Enterprises	0.71%
Arts, Entertainment, & Recreation	0.71%
Mining, Quarrying & Oil & Gas Extraction	0.71%

Figure 5: Percentage of engagements in Q3 2024 by NAICS sector

Looking at threat actors for which there is sufficient data, BlackSuit and Akira came in second and third place for the average annual revenue profile of their victims: $60 million for BlackSuit and $40 million for Akira. When Arete further examined how the revenue profile and associated threat actor factored into decisions to pay the ransom, there was no statistically significant finding indicating that revenue or threat actor influenced whether victims paid a ransom. Factors around the availability of backups, internal attitudes towards payment, and timeline for recovery continue to play a far greater role than industry, revenue, or perpetrating threat actor when it comes to making a payment. Threat actor behaviors indicate they are aware of this, as we see little evolution in industry or revenue targeting but consistent iteration on pressure tactics to encourage payment.

Trends in Stolen Data: BianLian Imposes Highest Secondary Cost

As part of our end-to-end solutions to address the entire threat lifecycle, Arete's Data Mining and Document Review services are powered by cutting-edge technology to help organizations reduce risk. Utilizing advanced algorithms, our team quickly processes large volumes of data to accurately detect patterns and identify PII and other sensitive information. The steps of this process are shown below.

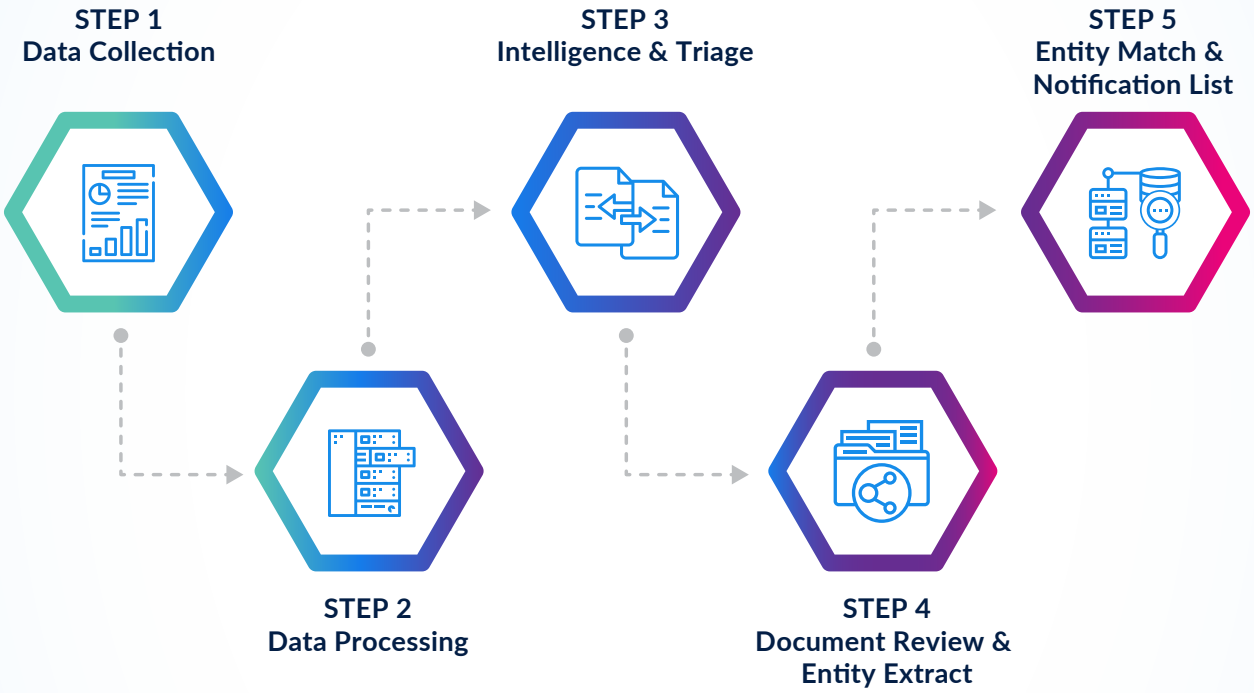


Figure 6: Arete's Data Mining and Document Review Process

This unique visibility gives Arete insight into which threat actors impose the highest secondary costs associated with data breaches. To protect and serve our clients, we will not share specific numbers but rather a high-level analysis of threat groups. Unlike most of the data in this report, this section analyzes engagements that concluded in Q3 versus started. Therefore, much of this data applies to engagements that started in Q2. This difference is caused by the length of time it takes to conclude an accurate, comprehensive analysis of the data.

Analysis of data breach incidents with identified threat actors demonstrates that attacks attributed to the BianLian extortion group by far impacted the greatest number of individuals on average. Attacks attributed to MedusaLocker and Hunters International ransomware groups impacted the second and third highest number of individuals, respectively. The Fog ransomware group and Luna Moth extortion group rounded out the top five threat groups in terms of impacted individuals.

Trends in Stolen Data: BianLian Imposes Highest Secondary Cost

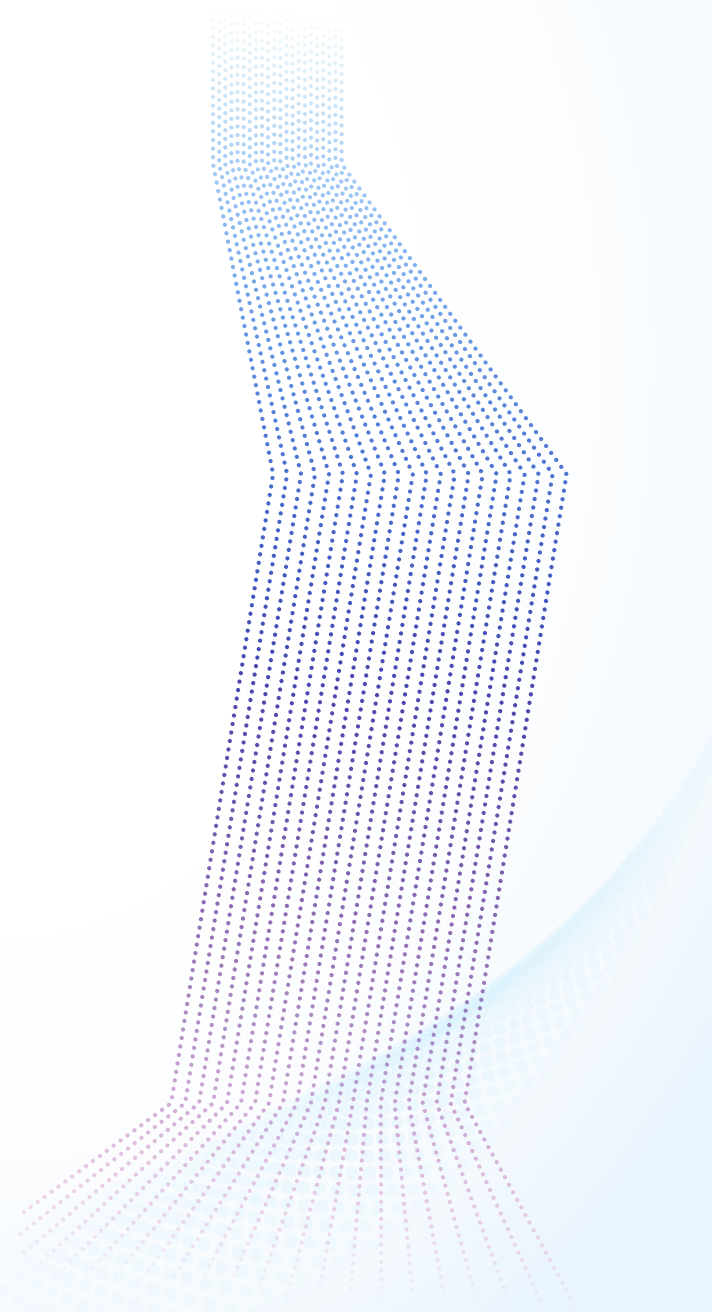
It is not surprising that BianLian's data theft exposed the most individuals, as they are a data extortion-only threat actor. More than any other threat group observed by Arete, BianLian appears to specialize in the theft of data impacting individuals, as opposed to impacting just the victim organizations.

Looking solely at the average amount of data believed to have been accessed or potentially exfiltrated by the threat actor, Abyss, LockBit, Hunters International, BlackSuit, and Luna Moth are the top five threat groups. The lack of overlap between the groups that impact the highest number of individuals and the groups that access the highest data quantity suggests that BianLian, MedusaLocker, and Fog may have greater precision when stealing data. This may be in part due to their selection of victims. For example, for much of this year, Fog specifically targeted organizations in the Education industry, which is more likely to store data on individuals than many other industries. In the case of BianLian, the average employee count for victimized businesses is 70 employees, meaning much of the exposure comes from non-employees.

This analysis is based on a limited data set, and the lack of more detailed analysis is intentional due to the sensitivity of this data. However, at a high level, this data indicates that BianLian may impose the highest secondary cost arising from individuals impacted in an attack.

The Fog ransomware group warrants mention due to its targeting of victims in the data-heavy Education sector, a focus that may be shifting as it began expanding its victim pool to include other sectors in Q3.

As part of our end-to-end solutions to address the entire threat lifecycle, Arete's Data Mining and Document Review services are powered by cutting-edge technology to help organizations reduce risk.



International Law Enforcement Efforts in Q3

After the significant disruption of ALPHV's infrastructure at the end of 2023, which eventually led to the brand's demise, international law enforcement maintained pressure against ransomware groups in early 2024, targeting LockBit's operations in February. This ultimately led to the reveal of LockBit's leader, Dmitry Khoroshev, who was subsequently sanctioned by the US, the UK, and Australian governments in May. As Arete reported in our H1 2024 Crimeware Report, law enforcement operations against these two ransomware organizations—the most prolific RaaS groups of 2023—significantly fractured the ransomware landscape in the first half of the year. Law enforcement applied additional pressure in Q2, with Operation Endgame targeting Malware-as-a-Service models in May and Operation MORPHEUS disrupting maliciously used Cobalt Strike infrastructure in June. Although law enforcement efforts against cybercriminals were comparatively quieter in Q3 than in the first half of 2024, there were some notable operations.

Operation Final Exchange: Sanctions Against Crypto Exchanges

On September 19, German law enforcement targeted 47 crypto exchanges that did not follow Know Your Customer (KYC) guidelines in what came to be known as Operation Final Exchange. The exchanges did not collect information that could be used to identify customers prior to transactions. This data collection is designed to protect banks and financial institutions from fraudulent activity.

In choosing not to follow these guidelines, the exchanges—all hosted in Germany—became a harbor for illicit financial activity, whether inadvertently or not. The exchanges aided in obfuscating cybercriminals' ransomed funds by allowing them to swap one currency for another, connect bank accounts, and instantly transfer government-issued currencies to crypto. Before the takedown, at least seventeen of these exchanges had a month with over 50% of direct inflows from illicit sources. These inflows were eventually traced back to sanctioned entities, ransomware actors, and breached data/dark web escrow brokers.

German police obtained extensive data on the users of the exchanges through the seizure of associated servers. The information obtained through these seizures, including transaction data, registration data, and IP addresses, will become an additional tool for law enforcement agents in the continuous effort to identify cybercriminals. Operation Final Exchange showcases the continued shift in law enforcement efforts to disrupt cybercrime. Thus far in 2024, law enforcement has targeted ransomware groups and illicit infrastructure, making it more difficult for cybercriminals to conduct operations. In this case, Operation Final Exchange temporarily degraded cybercriminals' ability to launder illicit funds.

Law Enforcement Takedown of Radar/Dispossessor in Q3

On August 12, the FBI seized servers associated with the Radar/Dispossessor ransomware group. The Dispossessor ransomware group was established in August 2023, and in February 2024, announced the addition of an actor known as Radar to its ransomware team. In the wake of coordinated law enforcement actions against LockBit in early 2024, Radar/Dispossessor was one of several threat groups who attempted to exploit LockBit's weakened position by utilizing the leaked LockBit builder and modeling their DLS into an almost carbon copy of LockBit's DLS. However, given the group's limited activity in the short time it operated, the impact of this disruption to the overall threat landscape was minimal.

Figure 7: Former Radar/Dispossessor DLS seized by law enforcement in August 2024 (Source: Arete)

Commonly Observed Tools and Malware Used by Threat Actors in Q3

Despite the many changes in the ransomware ecosystem throughout 2024, one constant is the tools and malware used by threat actors. In Q3, cybercriminals continued to leverage most of the same malware variants and legitimate tools that were observed in the first half of 2024.

If It Ain't Broke: Legitimate Tools Continue to be Effective

Arete monitors over 200 tools with legitimate uses that are abused by ransomware and extortion groups to enable their operations. Throughout 2024, several consistent tools were observed in ransomware and extortion engagements. These tools range in function, including remote monitoring and management (RMM), credential access, network discovery, and exfiltration, and many remain effective since they are also used legitimately by IT professionals and go undetected by security defenses.

Remote Monitoring and Management (RMM)

RMM tools continued to be some of the most commonly used by threat actors in Q3. Many of these tools are already used by IT departments for remote access and network management, and threat actors exploit existing RMM tools to gain initial access or install additional RMM tools, allowing them to maintain persistence and remain undetected in a victim's environment. AnyDesk is one of the most commonly observed RMM tools, and in Q3, it was abused by most of the top threat groups, including Akira, RansomHub, Fog, BianLian, and BlackSuit. Other RMM tools observed in Q3 included Atera, Bomgar, LogMeIn, Splashtop, ScreenConnect, and TeamViewer.

Credential Access

Threat actors leverage credential access tools to secure unauthorized entry into victim systems, allowing them to navigate laterally across a network or elevate user privileges. In Q3, Mimikatz continued to be the tool used to extract credentials from victim systems by most threat groups, including BlackSuit, RansomHub, BianLian, and Qilin. LaZagne and ProcDump were also observed during the quarter, primarily in engagements involving RansomHub.

Discovery

Discovery tools allow threat actors to gather information about victim networks and identify potential vulnerabilities. In Q3, threat actors continued to use the same network discovery tools observed in the first half of the year, with Advanced IP Scanner, Advanced Port Scanner, Angry IP Scanner, and Netscan being the four most commonly used.

Exfiltration

Data exfiltration has become a standard practice in cyberattacks, with some threat actors focusing solely on data extortion while others use it as additional leverage for double-extortion ransomware attacks involving encryption. Again, threat actors in Q3 continued to use many of the same tools from the first half of the year to facilitate data theft. These include WinRAR and 7zip for file compression and FileZilla, Rclone, MEGAsync, PuTTY, and WinSCP for file transfer.

Cobalt Strike: Trending Down in Q3

Throughout 2024, Arete has observed a decrease in the use of Cobalt Strike by cybercriminals, with the lowest use in Q3. Cobalt Strike is a legitimate commercial software used by red teams in cybersecurity operations, making it a popular tool for threat actors who have used unlicensed copies for malicious attacks for years. This decline is likely a result of Operation MORPHEUS, the international law enforcement operation that took down nearly 600 maliciously used Cobalt Strike servers in June 2024. Although threat actors will likely pivot to other means of initial access, the disruption of Cobalt Strike demonstrates the effectiveness of law enforcement operations against cybercrime.

Threat Actors Targeting Endpoint Detection and Response (EDR)

In Q3, Arete and open-source reporting observed the ransomware group RansomHub using the tools TDSSKiller and EDRKillShifter to disable EDR software to evade detection. TDSSKiller is a legitimate tool designed to remove rootkits, but it also has the ability to disable antivirus and EDR software via a command line script or batch file. RansomHub is not the first group to leverage this tool, as LockBit also used it back in 2023.

EDRKillShifter is a newer tool that uses a technique known as Bring Your Own Vulnerable Driver (BYOVD), in which a legitimate driver with known vulnerabilities is installed and then exploited to gain privileges. With EDRKillShifter, these privileges are ultimately used to disable the EDR protection on the victim's systems. Although RansomHub has been observed using EDRKillShifter, it is possible that other threat groups are developing their own versions of the tool, and BYOVD is a common technique Arete has observed being used by multiple threat groups.

Q3 also saw open-source reports of the EDRSilencer tool, which leveraged Windows Filtering Platform (WFP) APIs to block telemetry between EDR agents on endpoints and the main EDR console. While not broadly adopted, it has been observed to be used by ransomware groups in the wild.

As more organizations incorporate EDR solutions to better protect themselves against cybercriminals, threat actors will likely continue to develop tools to counter these protections. Behavioral protection rules and blocking downloads of system-level drivers within the EDRs can help counter these tools, and it is important for organizations to keep their systems updated and maintain adequate separation between user and admin privileges to limit threat actors' ability to install vulnerable drivers.

As more organizations incorporate EDR solutions to better protect themselves against cybercriminals, threat actors will likely continue to develop tools to counter these protections.

Top Malware Tools in Q3

Along with legitimate tools, many of the malware threats in Q3 remained the same as observed in the first half of 2024. Three of the four malware listed in Arete's H1 2024 Crimeware Report were again among the top malware observed during the quarter, highlighting their continued effectiveness to cybercriminals.

SocGholish

SocGholish remained a major malware threat in Q3, leveraging drive-by downloads often disguised as fake software updates or software installers to trick users into executing malicious code. Recent attacks have utilized PowerShell scripts to evade detection and deliver payloads, with the malware targeting specific environments by checking for virtualized systems. During the quarter, Arete observed multiple threat groups leveraging SocGholish in their attacks, including Akira, RansomHub, Play, and BlackSuit.

Neshta

The file-infecting virus Neshta was another malware used by multiple groups in Q3. Neshta continues to be a persistent threat due to its method of spreading by infecting executable files, and it attaches its malicious code to the beginning of these files, ensuring that it runs whenever the file is opened. RansomHub, BianLian, Qilin, and Rhysida were all observed using Neshta during the quarter.

SystemBC

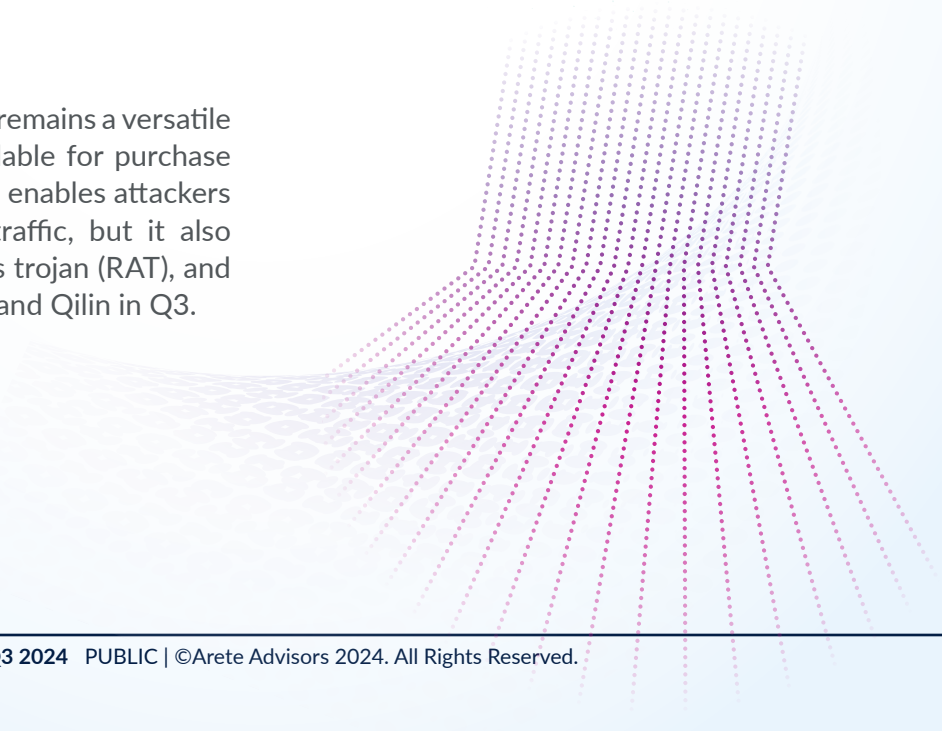
SystemBC first emerged in 2019 but remains a versatile and persistent malware that is available for purchase on underground markets. SystemBC enables attackers to mask their malicious network traffic, but it also acts as a downloader, remote access trojan (RAT), and backdoor, and was used by Rhysida and Qilin in Q3.

Lumma Stealer

Lumma Stealer targets cryptocurrency wallets, browser add-ons, and two-factor authentication codes, using evasion techniques like Base64 encoding and modular malware components to avoid detection, aiming to collect sensitive data from infected devices.

FlawedAmmyy

FlawedAmmyy is a type of RAT that cybercriminals use to take unauthorized control of infected Windows systems. It typically spreads through phishing emails or malicious downloads, masquerading as legitimate software, and allows attackers to steal sensitive data, manipulate files, or gain full control of the victim's machine. FlawedAmmyy is especially challenging to detect because attackers often execute it directly in memory, leaving minimal traces on the hard drive. It also has capabilities to move laterally within networks, increasing the risk for larger organizations.



Conclusion

Although law enforcement continued to combat cybercrime in the third quarter of 2024, the absence of any significant disruptions to the active threat groups operating in Q3 allowed established and emerging threat actors to fill the void left by ALPHV and LockBit. Over the course of the quarter, the ransomware landscape returned to a more predictable pattern, with Akira and RansomHub establishing themselves as the dominant ransomware groups going into Q4. Unfortunately, this highlights one of the greatest challenges in the fight against cybercrime: Threat actors remain resilient and adaptive to law enforcement pressure, and the positive effects of forcing the shutdown of larger ransomware gangs can ultimately be short-lived if the individuals within the group retain the ability to regroup and continue conducting attacks.

Despite these challenges, some positive trends continued in Q3. The increasing regularity of cyberattacks has caused many organizations to improve their cybersecurity posture and ability to recover. Even when attacks occur, payments to threat actors remain low, leaving cybercriminals empty-handed more often than not. Looking toward the last quarter of 2024, Arete anticipates this trend of fewer ransom payments to continue for the remainder of the year and perhaps decrease even more as organizations become better prepared to respond to a data breach or ransomware attack.

Although the threat landscape began trending in a more predictable pattern in Q3, this isn't necessarily an indication of how Q4 will play out. Threat actors are opportunistic, and individual threat groups come and go. Future law enforcement efforts will also play a significant role in how the ransomware ecosystem shapes up by the end of the year. Regardless of what Q4 may bring, Arete will continue to work relentlessly to serve those impacted by cyberattacks, helping companies around the world take back control of their systems and restore normal business operations.

Appendix & Sources

Data Collection and Analysis Methodology

Arete provides comprehensive incident response services, and the insights shared in this report are derived from incident response, digital forensics, restoration, managed detection and response, endpoint protection, threat hunting, threat intelligence, threat actor communications, dark web monitoring, and advisory and consulting services. While not every client opts to use all the cyber solutions Arete offers, Arete gathers data points from thousands of unique ransomware engagements going back to 2018. By collecting and validating data from diverse sources, Arete builds a comprehensive threat intelligence repository, analyzes raw data, identifies patterns, and provides context to enable informed decision-making.

All data pertaining to threat actors is collected and analyzed to ensure victims are anonymized and there is no chance of threat actors or readers identifying any victim. Only data from incidents where victims were extorted by the threat actor, with or without encryption, are included in this report. While we share some insights from pre-ransomware attacks in which threat actors were disrupted prior to encrypting and/or stealing data, those incidents are not included in any statistics. Finally, any information that Arete assesses could be used by threat actors to improve their operations (e.g., negotiated discounts per threat actor) is excluded from public reports but available to trusted partners upon request.

Bias Acknowledgement

There are thousands of ransomware attacks claimed by threat actors worldwide each year, while many more likely go unreported or remain unknown to the victims. Arete conducts analysis based on the data collected during our incident response engagements. These incident response engagements primarily represent organizations who have cyber insurance. As our data represents just a sample of the overall number of global ransomware attacks, it creates a sampling bias. The analysis contained in this report reflects the trends Arete observes first-hand during our engagements with cybercriminals and may differ from trends observed by the greater cyber community.

Appendix & Sources

- Arete Internal Data
- Ransomware Groups Demystified: Lynx Ransomware
- T-O-X-I-N-B-I-O – Ransomware Recruitment Efforts Following Law Enforcement Disruption
- NoName ransomware gang deploying RansomHub malware in recent attacks
- Worldwide Web: An Analysis of Tactics and Techniques Attributed to Scattered Spider
- Microsoft links Scattered Spider hackers to Qilin ransomware attacks
- #StopRansomware: RansomHub Ransomware
- Ransomware attackers introduce new EDR killer to their arsenal
- Lynx Ransomware: A Rebranding of INC Ransomware
- Dissecting the Cicada
- Operation Endgame: Coordinated Worldwide Law Enforcement Action Against Network of Cybercriminals
- Europol coordinates global action against criminal abuse of Cobalt Strike
- German Law Enforcement Seizes Russian No KYC Exchanges - Chainalysis
- German Police Shutter 47 Criminal Crypto Exchanges - Infosecurity Magazine
- The BKA
- Know Your Client (KYC): What It Means and Compliance Requirements
- Dispossessor ransomware group shut down by US, European authorities | Reuters
- New RansomHub attack uses TDSSKiller and LaZagne, disables EDR - ThreatDown by Malwarebytes
- Ransomware Attackers Introduce New EDR Killer to Their Arsenal
- LockBit 3.0 Ransomware Silently Disables EDR Using TDSSKiller

Cyber Emergency Helpline 866-210-0955
Phone 646-907-9767

New Engagements
arete911@areteir.com

General Inquiries
marketing@areteir.com

www.areteir.com