MARCH | 2025

Arete

Annual Crimeware Report

2024 Trends and Highlights

Table of Contents

Overview

Arete's elite team of experts provides unparalleled capabilities to address the entire cyber threat lifecycle. From incident response and restoration to threat actor communications and managed security services, this comprehensive visibility informs our understanding and analysis of the threat landscape. Leveraging frontline data collected during incident response engagements, Arete identified and analyzed notable trends and shifts throughout 2024, including the evolution of the threat landscape, the most commonly observed ransomware and extortion groups, trends in ransom demands and industries targeted, and what may be coming next.

Across the ransomware and extortion incidents Arete responded to in 2024, several notable trends emerged:

- Law enforcement actions created a volatile operating environment for threat groups in the first half of 2024. By the second half of the year, LockBit and ALPHV/BlackCat—the two largest Ransomware-as-a-Service (RaaS) threats in 2023—were largely removed from the ransomware ecosystem.
- Threat actors adapted to the increase in law enforcement pressure, with new threat groups rapidly emerging, partnerships forming between groups, and an air of distrust enveloping the threat landscape.
- Most ransomware and extortion activity in 2024 was opportunistic in nature, with threat actors targeting certain technologies or exploiting vulnerabilities as opposed to focusing on a specific industry.
- Victim organizations continued to demonstrate an improved capability to recover from attacks without paying ransom demands.
- In 2024, cybercriminals leveraged many of the same malware variants and legitimate tools observed in 2023. However, an emerging trend was an increased development of endpoint detection and response (EDR) evasion tools.
- In the Asia-Pacific (APAC) region, ransomware threats became more sophisticated and impactful, targeting critical industries like healthcare, finance, government, and infrastructure.

2024 Trends from Arete's Incident Response Engagements

Total Named Threat Actors	Total Unnamed Threat Actors
74	47

Arete's Threat Intelligence team continuously analyzes data and insights to accurately identify and attribute unique unnamed threat actors when possible. In 2024, Arete was able to retroactively identify and name 16 distinct threat groups over the course of the year.

TOP 10 THREAT GROUPS IN 2024

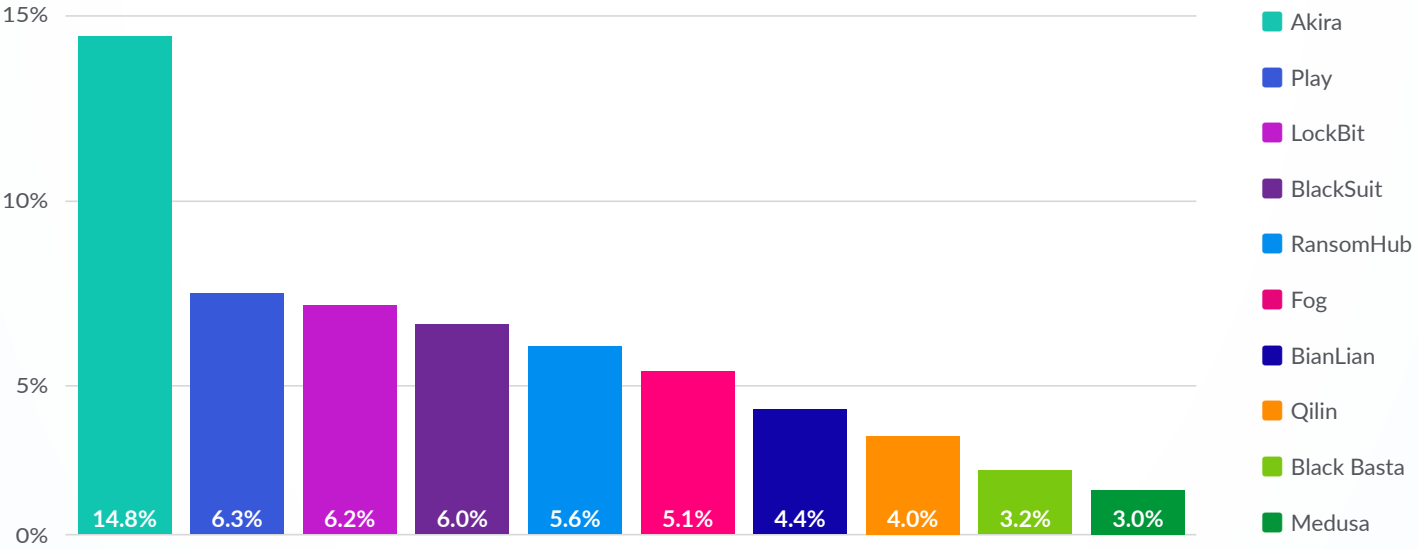


Figure 1

TOP 5 THREAT GROUPS IN 2024 BY QUARTER

Figure 2

Notable Threat Groups in 2024

Akira

In 2024, Akira benefited from law enforcement actions that disrupted LockBit and ALPHV's operations and was the most active threat group throughout the year. Akira was consistently one of the top groups observed by Arete each month and accounted for almost 15% of all ransomware and extortion activity in 2024. Throughout the year, Akira exploited multiple vulnerabilities to gain initial access, including a critical SonicWall VPN access control flaw (CVE-2024-40766) in Q4. Given Akira's consistent activity levels and adaptability, the group will likely remain a dominant ransomware threat in 2025. For more details and an in-depth technical analysis of Akira's ransomware, read Arete's Malware Spotlight on Akira.

Play

With the decline of LockBit and the shuttering of ALPHV this year, Play remained an active ransomware threat in 2024, particularly in the first half of the year. While Play is not consistently among the most active ransomware groups each month, its median ransom demand of $1.59 million demonstrates the scale of potential financial losses associated with this threat actor. On a positive note, Play is the threat actor most frequently identified in pre-ransomware incidents, in which security staff or defenses identify and stop the threat actor before they can successfully encrypt and/or exfiltrate data.

Arete currently tracks Fog and Akira as two closely related threat actors with multiple overlaps but slight differences in their operations. We will continue to closely monitor how these two groups work together.

BlackSuit

BlackSuit is believed to be a continuation of Royal ransomware and significantly increased its activity in 2024, most notably in the first quarter of the year. BlackSuit targets both Windows and Linux users, and although the group typically operates using a double extortion method of encryption and data exfiltration, Arete has observed instances where the group does not encrypt and instead demands ransom payments for data suppression. Arete also observed BlackSuit use aggressive pressure tactics, including calling victims to pressure them into making a ransom payment.

RansomHub

Of the new RaaS groups formed in 2024, RansomHub was one of the most successful, rapidly developing into one of the top threats observed by Arete in the second half of the year. The group has targeted a wide range of high-profile victims in its short tenure thus far, including telecom giant Frontier and British auction house Christie's. RansomHub also demonstrates a willingness to allow individual affiliates and existing threat groups like Scattered Spider to use its RaaS. Arete published a Malware Spotlight on RansomHub, with detailed insights on the group's observed behavior and a technical analysis of its ransomware executable.

Fog

Fog emerged as a new ransomware group in 2024. Initially, it primarily targeted organizations in the education sector using compromised VPN credentials but later expanded its attacks to target other industries. In doing so, Fog became one of the most active groups in the second half of 2024 and, in Q4, was the second-most active threat group behind Akira. Fog also recently exploited the same SonicWall VPN vulnerability (CVE-2024-40766) as Akira, contributing to its consistent activity levels.

BianLian

Like in 2023, BianLian remained a data extortion-only threat group throughout 2024, typically gaining initial access via Remote Desktop Protocol (RDP) credentials or third-party remote access tools. Although it was rarely among the most active groups month-to-month, BianLian remained a consistent threat throughout the year. The group maintained its highly aggressive pressure tactics and is known to repeatedly call and message employees of victim organizations in an attempt to coerce ransom payments.

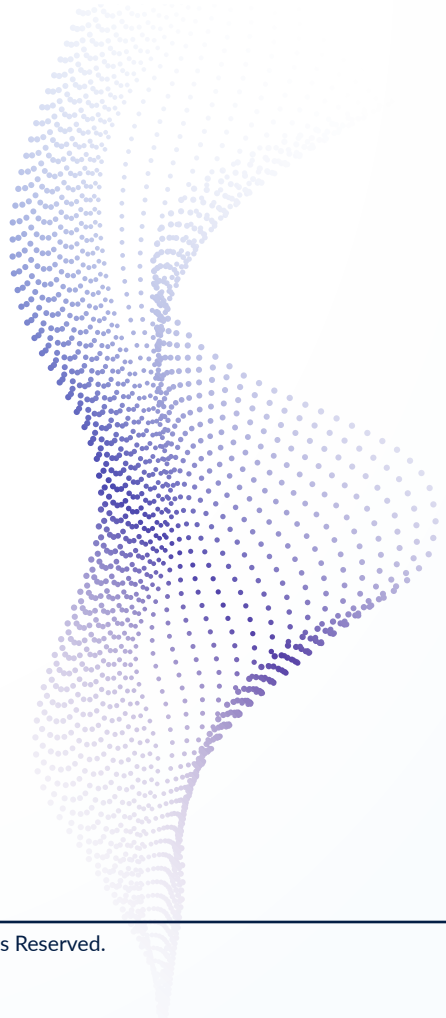
Qilin

In 2024, Qilin became noticeably more active, likely capitalizing on the law enforcement disruptions to LockBit and ALPHV. The group also gained media visibility in June 2024 when it was linked to the ransomware attack on pathology service provider Synnovis, which impacted several major National Health Service (NHS) hospitals in the UK.

Lynx

Lynx is yet another RaaS that emerged in the wake of law enforcement operations against ALPHV and LockBit in 2024. Arete first observed Lynx ransomware in July 2024, and the group demonstrates multiple similarities with INC's ransomware executable, infrastructure, and tooling. Regardless of potential connections to INC, Lynx established a clear identity for its RaaS, posting a steady stream of victims on its data leak site (DLS) since July 2024. It will likely remain a persistent threat going into 2025.

Akira ultimately dominated the ransomware landscape for the majority of 2024. The group maintained consistent, high activity levels throughout the year and was the most active group from Q2 through Q4. In the void left by LockBit and ALPHV, RansomHub and Fog quickly established themselves and emerged as top threats in the second half of the year. The threat landscape became more stable and predictable at the end of 2024. In the absence of major law enforcement operations against the remaining RaaS brands, these groups will likely remain the most prolific ransomware threats into 2025.



MARKET SHARE OF TOTAL ENGAGEMENTS BY TOP 2 THREAT GROUPS

Looking at the share of activity by the top two most active groups each quarter illustrates the fractured but more evenly distributed ransomware landscape that occurred as a result of law enforcement actions. At the end of 2023, LockBit and ALPHV were responsible for over a quarter of all ransomware and extortion engagements. In Q1 2024, LockBit and Akira were responsible for roughly the same percentage of total engagements. However, when ALPHV shut down and LockBit continued to decline, that percentage dropped to 20% for the top two threat groups in Q2.

In the absence of continued pressure from law enforcement against the larger RaaS organizations in the second half of 2024, threat group activity returned to a more predictable pattern in Q3 and Q4. As some of the emerging groups became more established, fewer groups were again responsible for larger percentages of ransomware activity. By Q3, the two most active groups—Akira and RansomHub—conducted almost a third of all ransomware attacks for the quarter. In Q4, Akira and Fog were the top two and conducted the same percentage of attacks for the quarter as LockBit and Akira did in Q1.

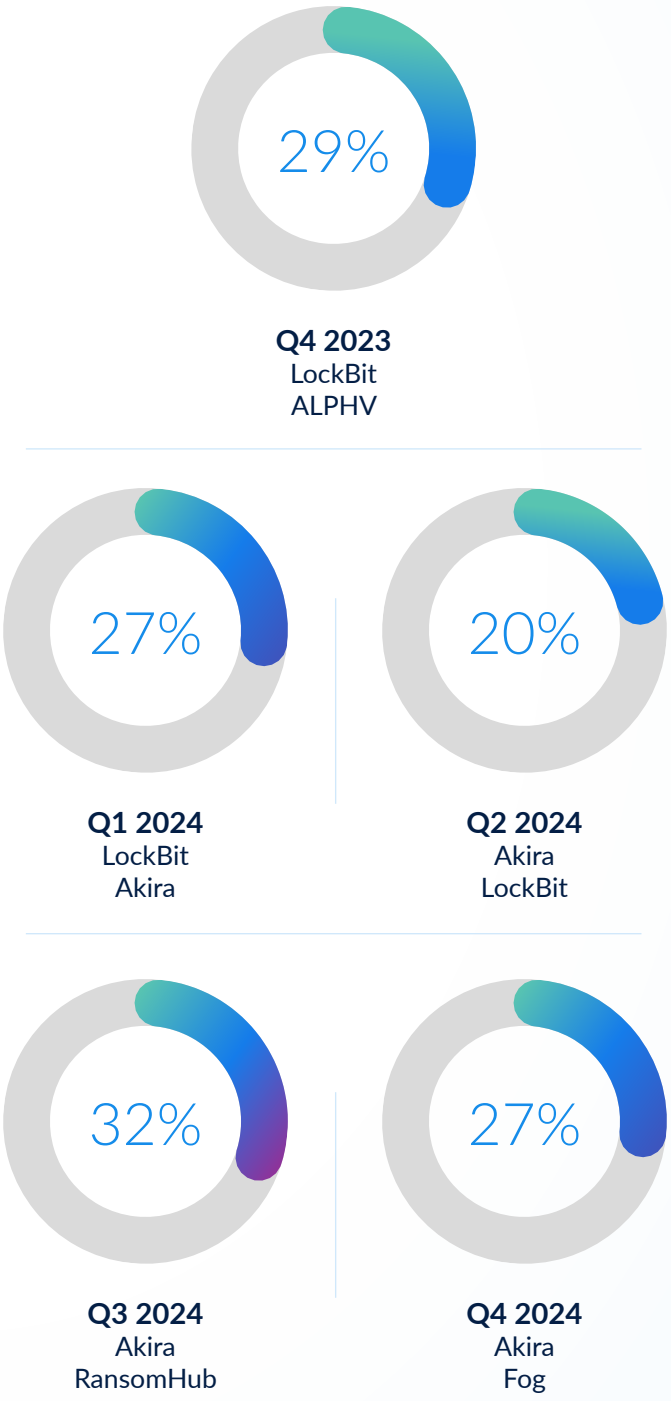


Figure 3

Disruptions to ALPHV and LockBit Changed the Threat Landscape in 2024

LockBit and ALPHV were two of the most prolific RaaS organizations in 2023. However, in late 2023 and early 2024, international law enforcement targeted the two RaaS groups, significantly disrupting their operations. ALPHV eventually shuttered its RaaS in March 2024, and while LockBit continued to operate throughout 2024, its activity levels increasingly declined as a result of law enforcement's actions. Initially, this led to a fractured and largely unpredictable threat landscape. However, without sustained pressure from law enforcement in the second half of 2024, new groups emerged and leveraged the disruptions to LockBit and ALPHV as recruiting tools to poach ex-affiliates.

With ALPHV and LockBit no longer positioned as the dominant RaaS groups in the ransomware ecosystem, Arete observed a more even distribution of activity month-to-month. Other established groups like Akira and Play maintained steady rates of activity, and newer and lesser-known threat groups such as BlackSuit, RansomHub, and Fog emerged to fill the void.

ALPHV shuttered its RaaS in March 2024, and while LockBit continued to operate throughout 2024, its activity levels declined.

LAW ENFORCEMENT ACTIONS AGAINST ALPHV AND LOCKBIT

DECEMBER 2023
The Federal Bureau of Investigation (FBI) seized ALPHV's DLS and obtained victim-specific decryption keys for over 500 victims. ALPHV eventually reestablished a new DLS and resumed operations.

FEBRUARY 2024
During Operation Cronos, a law enforcement disruption campaign targeting the LockBit RaaS, international law enforcement seized LockBit's DLS and numerous public-facing websites and servers used by LockBit administrators.

MARCH 2024
ALPHV's new DLS displayed a message stating that it had again been seized by law enforcement. This was ultimately an exit scam staged by the group after operators cheated an affiliate out of the $22M ransom payment from the Change Healthcare attack in February 2024.

MAY 2024
International law enforcement revealed Russian national Dmitry Yuryevich Khoroshev (also known as LockBitSupp) to be the leader of the LockBit RaaS organization. Khoroshev was subsequently sanctioned by the US Department of the Treasury's Office of Foreign Assets Control (OFAC), the UK's Foreign Commonwealth & Development Office (FCDO), and the Australian Department of Foreign Affairs.

MAY 2024
The UK's National Crime Agency (NCA) revealed that Aleksandr Ryzhenkov, one of the members of Evil Corp cybercriminal group sanctioned by the US Department of Treasury, had also operated as an affiliate of LockBit. The NCA also revealed that Operation Cronos had resulted in several international arrests of individuals with connections to LockBit.

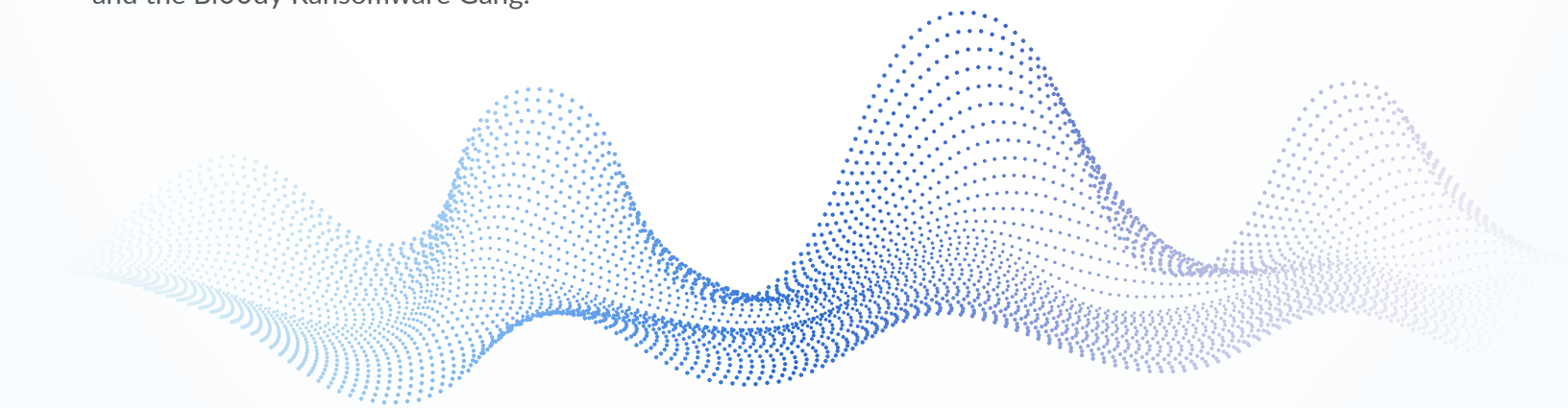
LockBit ALPHV/BlackCat

LockBit Will Linger in 2025, One Way or Another

Despite the successes of Operation Cronos and sanctions imposed against Dmitry Khoroshev, the LockBit RaaS organization did not completely shut down its operations or attempt to rebrand under another name. Arete continued to observe incidents attributed to LockBit RaaS affiliates in the second half of 2024; however, their activity levels significantly declined. In the first half of 2024, LockBit was responsible for about 13% of all Arete ransomware engagements, but in the second half of the year, that percentage dropped to just 1%. In late December 2024, LockBit announced it would release a new version of its malware dubbed LockBit 4.0, suggesting the group fully intends to continue operating under the LockBit brand in 2025.

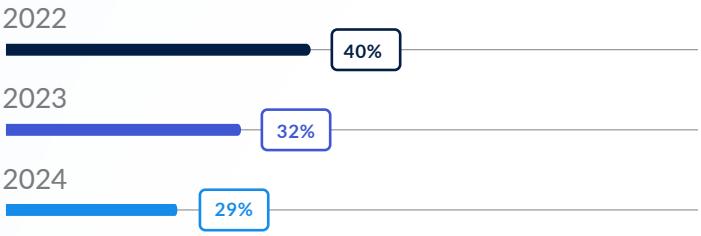
Arete continued to observe incidents attributed to LockBit RaaS affiliates in the second half of 2024; however, their activity levels significantly declined.

To complicate matters, threat actors not affiliated with the LockBit RaaS continued to conduct attacks throughout 2024 using the publicly available LockBit 3.0/LockBit Black builder that was leaked in September 2022. Unaffiliated threat groups using the builder add a layer of complexity in determining attribution and whether any sanction exposures exist. During 2024, groups observed or reported to be using the leaked LockBit builder but not believed to be associated with the RaaS included Monti, TRONL1, Brain Cipher, RADAR/Dispossessor, DragonForce, Cloak, FSTeam, and the Bl00dy Ransomware Gang.

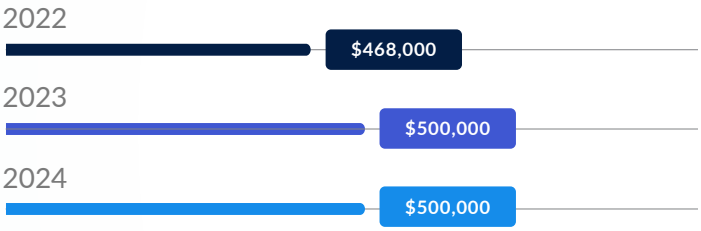


Trends in Ransom Demands and Payments

PERCENTAGE OF TIME A RANSOM IS PAID



MEDIAN RANSOM DEMAND



MEDIAN RANSOM PAYMENT

Figure 4

In 2024, the percentage of companies and organizations making ransom payments to cybercriminals continued to decline. Only 29% of ransomware and extortion victims made a payment to the threat actor in 2024, down from 32% in 2023. As organizations continue to improve their cybersecurity posture and recovery capabilities, threat actors come away empty-handed more often than not.

However, the decrease in ransom payment percentage was not as sharp from 2023 to 2024 as it had been from 2022 to 2023, suggesting that while businesses and organizations are increasingly paying fewer ransoms for recovery or data suppression, the percentage of time a ransom is paid may eventually plateau.

Interestingly, Arete also observed that median demands and payments have remained largely stable year over year. Although median ransom demands fluctuated from quarter to quarter in 2024, the median was $500,000 over the course of the entire year, which was the same amount observed for the entirety of 2023. Likewise, the median payment amount remained consistent over the past three years.

Despite this trend, attacks against higher-profile targets yielded higher demands and payments. In August 2024, an undisclosed company reportedly paid a $75 million ransom to the Dark Angels ransomware group, which was the largest recorded ransom payment made to a cybercriminal group. In 2025, ransomware groups may become more disruptive with their attacks in an effort to increase payment amounts as the percentage of payments declines.

Sector Impacts and Threat Actor Targeting

Manufacturing was the most impacted sector in 2024, closely followed by Professional, Scientific, and Technical Services. Collectively, these two sectors accounted for more than 40% of the ransomware and extortion victims observed by Arete throughout the year. The Construction, Finance & Insurance, and Healthcare & Social Services industries rounded out the top five most impacted sectors for the year. This data is influenced by cyber insurance trends, Arete's typical client profile, and threat actors' interest in these particular sectors. Most ransomware and extortion activity Arete observed in 2024 was opportunistic in nature, meaning threat actors were not targeting one specific industry.

Many instances of apparent targeting actually arose from the reuse of technology and service providers within specific industries and geographies.

- In the fall of 2024, threat actor Mimic attacked many Construction firms by leveraging a vulnerability in Foundation Software, an accounting software primarily used in the construction industry.

- In the summer of 2024, Arete observed a cluster of activity in one state, which arose from initial access through a service provider that largely serviced a single geographic area.

However, a limited number of threat actors are known to conduct intentionally targeted operations. The BianLian extortion group, the Luna Moth extortion group, and the Hunters International ransomware group continued to target Professional, Technical, and Scientific Services organizations. BianLian and Luna Moth are both extortion-only groups, which results in the Professional, Technical, and Scientific Services sector having one of the lowest median ransom payments of any industry.

The Construction sector had the highest median ransom demand. However, the potential impact was countered by the Construction industry also having one of the highest rates of backups sufficient for full recovery.

Healthcare & Social Services was the sector ranked first in maintaining complete backups to enable full recovery. Consequently, the sector emerged as one of the least likely to pay a ransom demand. This was a significant shift from prior years, in which Healthcare was one of the more vulnerable sectors.

Manufacturing once again established itself as one of the most resilient industries and maintained its status as the industry most likely to recover without paying the ransom, despite having the third-highest median ransom demand.

SECTORS	MEDIAN DEMAND
Construction	$742,000
Healthcare & Social Assistance	$600,000
Manufacturing	$500,000
Professional, Scientific, & Technical Services	$490,000
Finance & Insurance	$400,000

Figure 5

Sector Impacts and Threat Actor Targeting

In 2024, threat actors remained largely opportunistic in attacks. The primary shift is that year over year, organizations are increasingly adopting EDR and multi-factor authentication (MFA) to strengthen cyber resilience and prevent attacks.

NAICS SECTOR NAME	PERCENTAGE OF ENGAGEMENTS
Manufacturing	20.46%
Professional, Scientific, & Technical Services	19.57%
Uncategorized	12.81%
Construction	6.58%
Finance & Insurance	6.41%
Healthcare & Social Assistance	5.52%
Public Administration	4.80%
Information	4.27%
Wholesale Trade	3.74%
Administrative & Support & Waste Management & Remediation Services	3.02%
Educational Services	2.85%
Other Services (except Public Administration)	2.14%
Real Estate & Rental & Leasing	1.78%
Arts, Entertainment, & Recreation	1.42%
Transportation & Warehousing	1.25%
Retail Trade	1.25%
Accommodation & Food Services	1.07%
Agriculture, Forestry, Fishing & Hunting	0.53%
Utilities	0.36%
Mining, Quarrying & Oil & Gas Extraction	0.18%

Figure 6
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.

Threat Actor Targeting Based on Organizational Characteristics

Similar to targeting specific sectors, very few threat actors demonstrated targeting based on organizational characteristics like revenue, number of employees, or geography. However, there are select groups that consistently demonstrate targeting. The Play ransomware group continued showing some targeted behaviors, with an average victim annual revenue exceeding $500 million. Black Basta showed similar victimology.

THREAT ACTORS TARGETING HIGH-REVENUE ORGANIZATIONS

The other three threat actors with the highest average victim revenue attacked a much smaller number of victims. Two of these groups, Mr. Anazon and TRON L1, are relatively unsophisticated groups uniquely tracked by Arete. This lack of sophistication is reflected in tactics and an inability to capitalize on this victim demographic, with both groups having some of the lowest average demands. The fifth group, Daixin Team, is another very small threat actor with a much greater depth of experience. Daixin Team appears to intentionally determine ransom demands based on the revenue of each victim.

Although organizational characteristics are not often driving cyberattacks, several threat actors do consider victim revenue, employee count, and geography when determining the initial ransom demand. Arete has observed multiple RaaS groups set thresholds for demands based on the victim's revenue. More prolific ransomware groups like Akira, RansomHub, Play, Qilin, and Lynx have stated that they determine initial demands based on net income, financial documents, cyber liability limits, or other data exfiltrated during an attack that gives them insight into what amount a victim may be able to pay.

High-Profile Ransomware and Extortion Events in 2024

There were several high-profile cyberattacks in 2024 that caused considerable financial damage and impacted a large number of people, many of which involved healthcare organizations. With fewer victims making ransom payments, Arete anticipates that there will likely be more high-loss ransomware and extortion events in 2025.

HIGH-PROFILE CYBERATTACKS IN 2024

Figure 7

FEBRUARY 2024
Change Healthcare (ALPHV/BlackCat)

Change Healthcare is a leading healthcare technology solutions provider, and its platform processes over 15 billion healthcare transactions annually. In February 2024, ALPHV exploited compromised credentials to access Change Healthcare's Citrix portal and deploy its ransomware, encrypting the organization's systems and compromising sensitive protected health information (PHI) and personally identifiable information (PII). After a ransom was paid, ALPHV reportedly scammed its affiliate out of the $22M payment. The affiliate then worked with a separate group, RansomHub, threatening to leak the stolen data and attempting further extortion. This attack had a significant impact on the healthcare industry and exposed the data of more than 190 million individuals.

MAY 2024
Ascension Healthcare (Black Basta)

Ascension, one of the largest private U.S. healthcare systems, experienced a cyberattack linked to the Black Basta ransomware operation in May, which compromised personal and health data of nearly 5.6 million patients and employees. The stolen files contained various sensitive information, including medical records, payment details, insurance information, government IDs, and other personal data. The attack affected Ascension's MyChart electronic health records system, phone systems, and tools for ordering tests, procedures, and medications.

JUNE 2024

Synnovis UK (Qilin)

In June 2024, the Qilin ransomware group attacked Synnovis, a pathology services provider for the UK's NHS. The attack, which targeted critical systems, resulted in the cancellation of over 3,000 medical appointments and procedures within the first two weeks, causing significant disruption across multiple NHS trusts, particularly in London. Following the expiration of the ransom demand deadline, Qilin uploaded the stolen data to its dark web site, which included sensitive patient information such as names, dates of birth, NHS numbers, and details of blood tests.

JUNE 2024

CDK Global (BlackSuit)

Also in June 2024, the BlackSuit ransomware group was responsible for a significant IT outage at CDK Global, disrupting car dealerships across North America. CDK Global, a Software-as-a-Service (SaaS) provider, offers platforms that manage dealership operations, including sales, financing, inventory, and service. The attack interrupted critical services, including dealer management systems and CRM tools, forcing dealerships to rely on manual processes.

NOVEMBER 2024

Ahold Delhaize (Unknown)

In November 2024, an unknown threat group attacked Ahold Delhaize USA and severely disrupted operations at over 2,000 stores, including Hannaford, Food Lion, and Stop & Shop. The attack led to Hannaford's e-commerce portal being unavailable due to server problems, while the websites of other chains, including Food Lion and Stop & Shop, displayed an incident notice. The breach caused significant operational disruptions, including the inability of some stores to process credit and debit card payments and the suspension of online ordering services.

Commonly Observed Tools and Malware Used by Threat Actors in 2024

Although the threat landscape changed throughout the year, cybercriminals leveraged many of the same malware and tools they used in 2023. In particular, legitimate software applications commonly used by corporate IT departments continue to allow threat actors to evade security measures and stay undetected in the victim's environment. Additionally, cybercriminals continued to use much of the same malware throughout 2024.

However, as organizations become increasingly aware of the risk of cyberattacks and work to improve their security measures, threat actors also continue to adapt and evolve their encryption methods and evasion strategies. One notable trend that emerged in 2024 was the increased use of specific tools designed to evade or terminate EDR solutions.

Threat Actors Target EDR

Throughout 2024, threat actors increasingly used various tools to disable EDR software solutions and evade detection. First observed being used by RansomHub, EDRKillShifter is a tool that employs a technique known as Bring Your Own Vulnerable Driver (BYOVD), in which a legitimate driver—such as the Zemana Anti-Malware kernel driver or the Avast Anti-Rootkit driver—with known vulnerabilities is installed and exploited to gain kernel-level privileges. With EDRKillShifter, these privileges are ultimately used to disable EDR protection on the victim's systems.

Other EDR evasion tools observed in 2024 include TDSSKiller, a legitimate tool designed to remove rootkits that can disable antivirus and EDR software via a command-line script or batch file. Additionally, in October, cybercriminals were observed using the red-team tool EDRSilencer to conduct attacks. EDRSilencer leverages Windows Filtering Platform (WFP) APIs to block sending telemetry data between EDR agents on endpoints and the main EDR console, which allows threat actors to prevent EDR products from sending alerts to cybersecurity teams when malware is installed.

Arete has also observed threat actors abusing the QEMU machine emulator to silently load virtual drives and access network share drives to encrypt host files inside the virtual machine. Threat actors also leveraged VirtualBox and other virtual machine solutions to import tools and launch operations undetected. This technique allows ransomware to evade EDR solutions, as they do not capture execution logs from within the virtual machine.

With multiple EDR killers for sale on dark web forums, the use of these malicious tools will likely continue to rise in 2025. Implementing behavioral protection rules and blocking the download of system-level drivers within EDRs can help mitigate these threats. It is also crucial 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.

Top Tools Leveraged by Threat Actors in 2024

Remote Monitoring and Management (RMM) tools remained commonplace in threat actor toolkits in 2024. Since RMM software is commonly used by IT departments and managed service providers, threat actors often leverage RMM tools that already exist in the victim environment or install their own. Additionally, because RMM software has legitimate uses, it often goes undetected by security defenses. In 2024, the AnyDesk remote desktop application was the most commonly used RMM tool, leveraged by over 30 separate threat actor groups observed by Arete. Other RMM platforms commonly used by threat actors in 2024 included Atera, Splashtop, ScreenConnect, and TeamViewer.

As with any software, RMM tools are prone to flaws and vulnerabilities that threat actors can exploit to gain unauthorized access. For example, in February 2024, more than 14 threat groups exploited two vulnerabilities in the ScreenConnect RMM software to gain access and deploy malware, detailed in the "Major Vulnerabilities and Campaigns in 2024" section on page 22.

Mimikatz remained one of the most widely used tools in 2024 for accessing and extracting victim credentials. Although the tool has been around since 2007, it remains effective and has been used by multiple threat actors throughout the year, including RansomHub, Qilin, Lynx, and Rhysida. Arete also observed Mimikatz in more engagements during the second half of 2024 than in the first half of the year, suggesting that it will remain a popular tool for cybercriminals in 2025.

Threat actors use discovery tools to gather information about the devices or remote systems within a victim's network and identify potential vulnerabilities. Advanced IP Scanner was the most observed network discovery tool in 2024, used by multiple ransomware and extortion groups. Advanced Port Scanner, Angry IP Scanner, and Netscan were also commonly used by threat actors throughout the year.

Data exfiltration tools also remained largely unchanged from 2023. The top file transfer tools in 2024 were FileZilla, Rclone, and WinSCP. WinRAR and 7zip continued to be commonly used for file compression. As the threat of leaking sensitive data remains a powerful pressure tactic for ransomware and extortion groups, these tools will likely continue to be widely used by cybercriminals in 2025.

Ultimately, the most effective way to defend against cybercriminals abusing legitimate tools is to identify which applications are allowed in an environment and identify which users are authorized to use these tools. Many of the tools mentioned above are intended for use by IT administrators, so regular users deploying them should raise red flags in an environment. Endpoint detection and response solutions can also help detect suspicious activity, such as when threat actors use legitimate tools in the environment.

Top Malware Families in 2024

SocGholish

SocGholish is a type of malware that relies on deception to infect systems, often disguising itself as a legitimate software update. It is typically distributed through drive-by downloads, where users unknowingly download a harmful file while visiting compromised websites. Using social engineering tactics, SocGholish convinces victims to run a malicious JavaScript payload, allowing the malware to take control of their systems.

Active since at least 2018, SocGholish is a significant threat to security and privacy. It profiles infected systems and has been observed downloading ransomware onto targeted devices. Often functioning as an "initial access broker," it creates entry points for additional exploitation, frequently deploying secondary tools like Cobalt Strike to enable lateral movement and privilege escalation within networks. SocGholish has been observed in incident response engagements involving multiple threat actor groups in 2024, including Akira, Play, RansomHub, INC Ransom, BianLian, LockBit, Hunters International, Black Basta, and others.

Arete has observed SocGholish using homoglyph characters to evade detection. Homoglyphs are characters that look very similar but have different meanings. For example, “Apple.js" vs. “Apple.js”, where the second filename substitutes Cyrillic Small Letter Er (р, UTF-8 0xD180) for the English “p”, making it appear the same but function differently. Malware can exploit homoglyphs where filenames or domains appear legitimate but contain deceptive characters. The image below shows how the string will be displayed to a SOC analyst looking at the filename in an EDR tool and below is the hexadecimal representation of each character. Depending on the EDR tool, writing a threat detection rule for the ASCII string Apple.js will fail to detect the example on the right that has a Cyrillic character “р”. As a countermeasure, Arete created a custom threat detection mechanism to detect this malware, which is automatically deployed in endpoint detection and response tools for our clients.

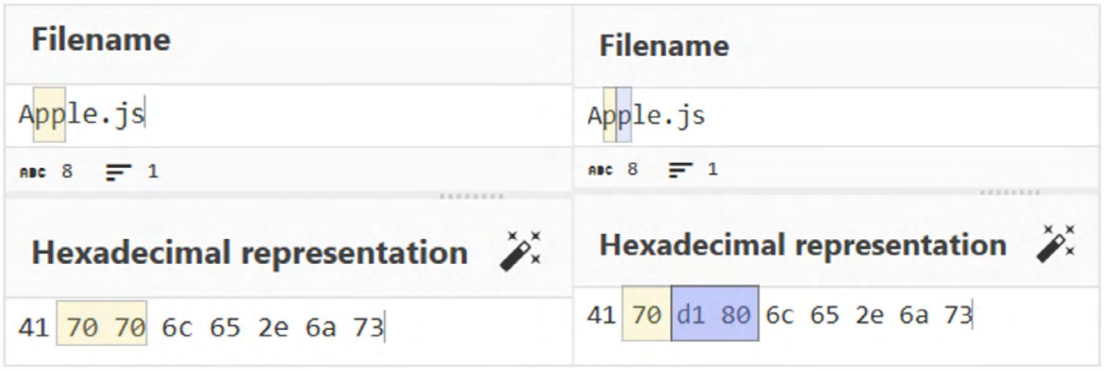


Figure 8: Hexadecimal representation of deceptive homoglyphs (Source: Arete)

Cobalt Strike

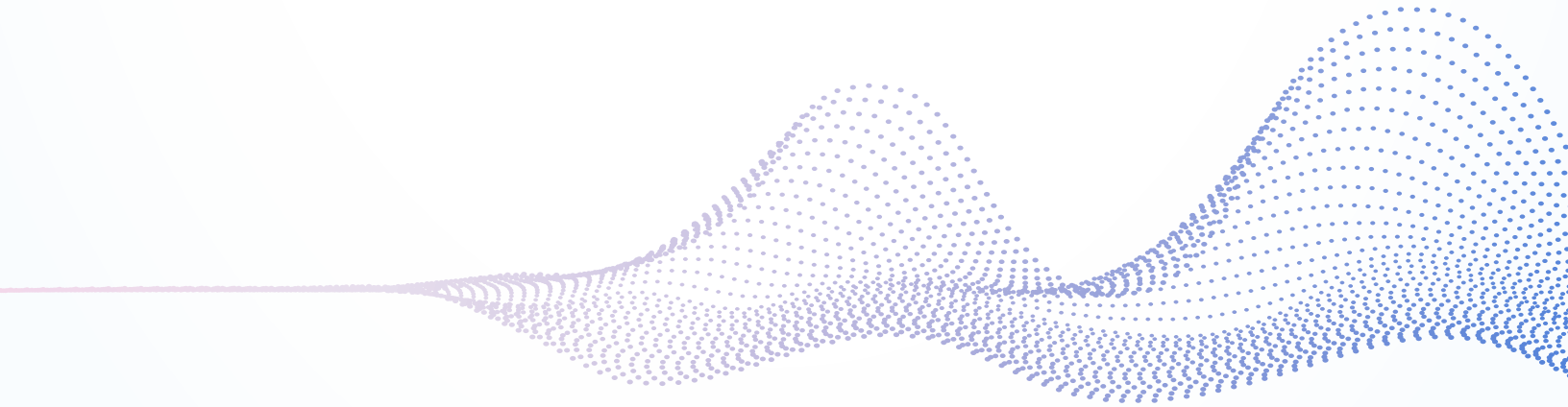
Cobalt Strike was initially created as a legitimate tool for red team security assessments but has since been widely used by cybercriminals. It offers various functions, including command-and-control (C2) communication, reconnaissance, and malware distribution, making it a crucial tool in the arsenal of many threat actors. Its advanced features create difficulties for defenders who are unfamiliar with its operation.

Due to its versatility and effectiveness, Cobalt Strike is commonly utilized in cyber-espionage and criminal activities, particularly by ransomware groups. In 2024, organizations like Europol and the UK's National Crime Agency (NCA) worked to curb its misuse by targeting outdated and unlicensed versions to limit its exploitation by cybercriminals. The most notable of these efforts was Operation MORPHEUS, during which international law enforcement took down nearly 600 IP addresses hosting maliciously used Cobalt Strike infrastructure in June 2024. Despite these efforts, cybercriminals continue to leverage Cobalt Strike. During 2024, Arete observed the use of Cobalt Strike in incident response engagements involving various threat groups, including RansomHub, Play, HsHarada, and Cl0p.

SystemBC

SystemBC is a multifunctional malware that operates as both a network proxy and a remote access trojan (RAT). It enables attackers to conceal malicious traffic by routing it through infected devices while also providing remote access for executing commands and deploying additional malware. Since its discovery, SystemBC has undergone significant evolution, incorporating modular functionality and employing advanced obfuscation techniques to bypass security defenses.

SystemBC is frequently associated with ransomware operations, where cybercriminals use it to gain an initial foothold in targeted systems through phishing campaigns and malware loaders. Its proxy capabilities help disguise attacker activity, making detection more difficult. Threat actors rely on encrypted command-and-control (C2) communications, reinforcing the role of SystemBC in stealthy payload delivery and persistent network infiltration. Its continued development underscores the growing sophistication of modern cyber threats. In 2024, Arete observed SystemBC in incident response engagements involving the threat groups Play, Rhysida, BlackSuit, and Qilin.



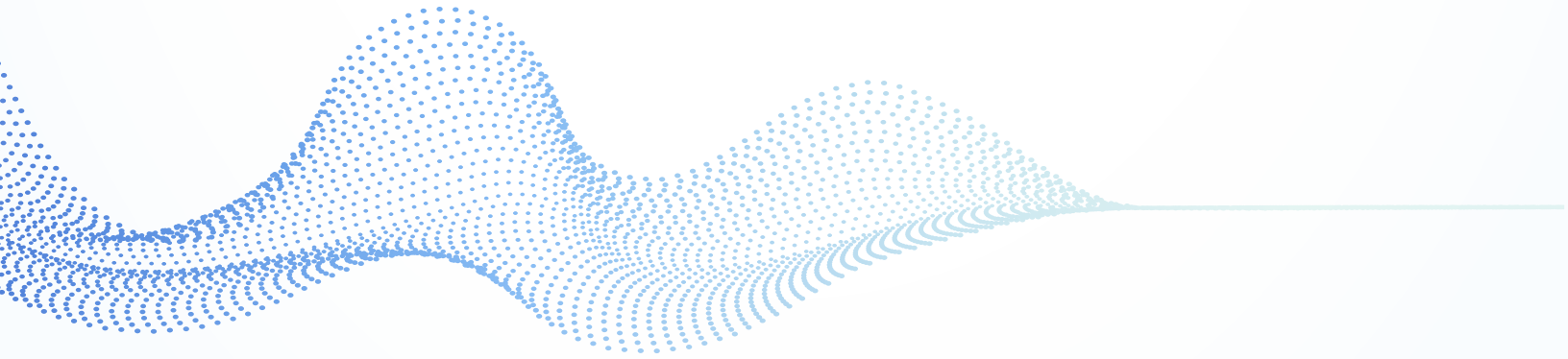
Lumma Stealer

Lumma Stealer is a highly active information-stealing malware that has been active since at least 2022 and operates in a Malware-as-a-Service (MaaS) model. It can compromise cryptocurrency wallets, browser extensions, passwords, and two-factor authentication (2FA) mechanisms. Since its discovery, it has been marketed on dark web forums and Telegram channels, making it widely accessible to cybercriminals. Its rapid adoption displays its effectiveness in gathering sensitive user data.

In 2024, Lumma Stealer not only increased in activity but also evolved its distribution and evasion techniques. One method involved fake CAPTCHA verification pages. These fraudulent CAPTCHAs appeared legitimate, tricking victims into interacting with them. However, in the background, the CAPTCHA execution triggered a concealed PowerShell command, which silently downloaded and deployed the Lumma Stealer malware. Arete has detected this threat activity using a custom threat detection mechanism created by our Threat Research Team. Arete has observed Lumma Stealer in incident response engagements involving the threat actor groups Qilin and Akira.

Neshta

Neshta remains a persistent threat due to its ability to infect executable files and spread through various vectors, including malicious downloads, spam emails, and deceptive software updates. It injects malicious code into executables, often disguising itself as legitimate Windows processes like svchost.com to evade detection. Once installed, Neshta modifies the Windows registry to ensure it runs at startup and continues to spread by infecting other executable files on the system. Neshta is particularly challenging to remove manually due to its persistence mechanisms, such as altering system files and registry keys to ensure continued execution upon system startup. Arete has observed Nestha in incident response engagements involving the threat actor groups RansomHub, BianLian, Qilin, and Rhysida.



Major Vulnerabilities and Campaigns in 2024

The availability of exploitable vulnerabilities contributed to the growth of cybercrime in 2024. The most targeted vulnerabilities were those affecting VPNs, firewalls, RMM tools, and a variety of third-party software solutions. Throughout the year, there was a growing concern over organizations' use of third-party software and their associated risks. Third-party software solutions frequently offer an increased level of privilege compared to other initial access methods, allowing threat actors to more easily traverse victim environments and accomplish their objectives.

In 2024, Arete observed several notable campaigns leveraging a variety of vulnerabilities:

ScreenConnect "SlashAndGrab" CVE-2024-1708 and CVE-2024-1709

14 ransomware groups

2024 started off with the exploitation of the SlashAndGrab vulnerabilities in the popular RMM tool ScreenConnect in February. When exploited together, the vulnerabilities allowed authentication bypass and path traversal, which resulted in the mass exploitation of ConnectWise customers running the ScreenConnect software. At least fourteen threat actors were identified as exploiting the vulnerabilities in conjunction with ransomware and cyber extortion campaigns.

Snowflake Compromises

UNC5537

First identified in April 2024, a threat actor named UNC5537 captured credentials relating to Snowflake users using information-stealing malware. The coordinated campaign against at least 165 organizations led to data exfiltration and subsequent extortion. The effect of this campaign was magnified by Snowflake's lack of MFA, leaving the door open for the credential-armed threat actors. The campaign led to the extortion of several large organizations, including Ticketmaster, AT&T, and Advanced Auto Parts.

Foundation Software Exploit

Mimic

Starting in mid-September, the threat actor Mimic began exploiting a vulnerability in Foundation accounting software, leading to highly privileged unauthorized access. The software is largely used by construction firms for invoicing, accounting, and other financial services. Foundation software servers often contain two high-privilege accounts that are frequently left with unchanged default credentials. These default credentials allow attackers to execute operating system commands directly from the SQL environment if the vulnerabilities are exploited, resulting in unauthorized access to sensitive data, manipulation of system files, and potential compromise of the entire system.

SonicWall CVE-2024-40766

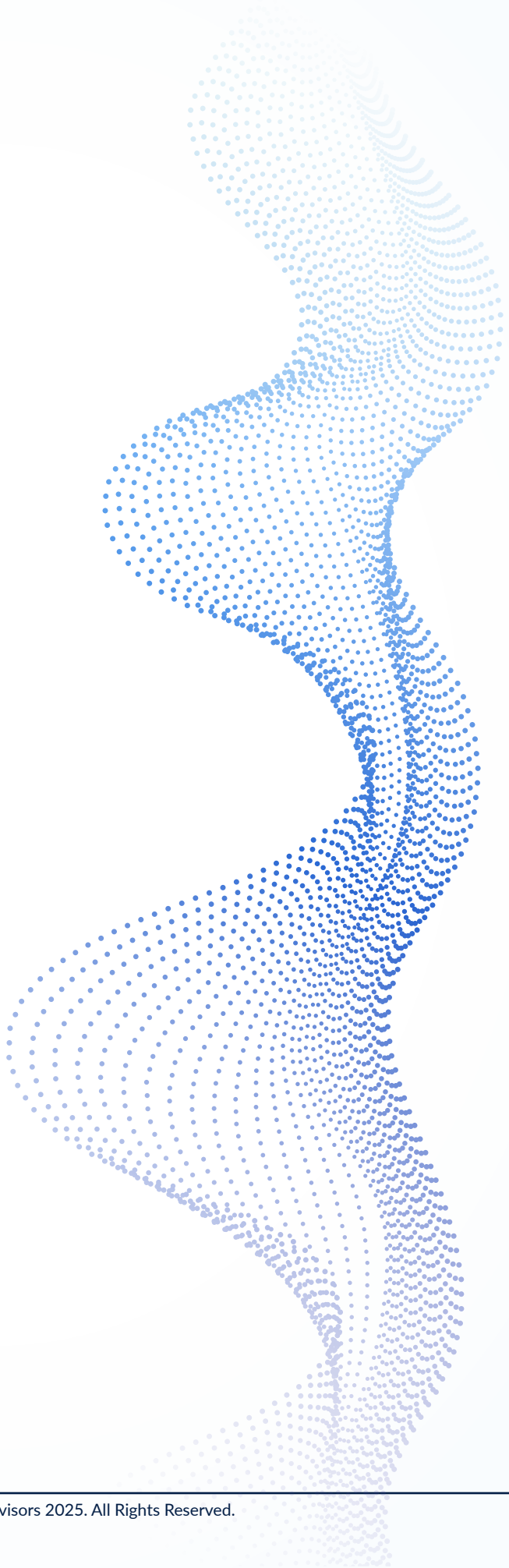
Akira, Fog, and Black Basta

With over 430,000 SonicWall firewalls exposed to the internet, vulnerabilities in the software tend to be a big hit with threat actors. A vulnerability initially believed to be restricted to the firewall's management access interface was later determined to also affect the firewall's SSLVPN feature. This led to the mass exploitation of SonicWall VPN appliances by well-known threat actors, including Akira, Fog, and Black Basta. The trend of actors abusing vulnerabilities in VPN appliances, specifically SonicWall, is an evolving threat that will likely continue in 2025.

Cleo CVE-2024-50623

Cl0p, Termite

Primarily perpetrated by the Cl0p threat group, a vulnerability in the Cleo file transfer product permitted unrestricted file uploads and downloads, resulting in remote code execution on unsuspecting victims. The first known exploitation was in early December 2024, with a notable increase in attack volume noted on December 8th. This is primarily believed to be due to the vulnerability originally being exploited by the newly emerged Termite ransomware group before the notorious Cl0p cybercrime group began exploitation. Shortly thereafter, Cl0p posted over 60 obfuscated victims to its DLS before starting to leak victim data in January 2025. The mass exploitation and exfiltration of data through file transfer vulnerabilities became commonplace for Cl0p, originating with the MOVEit vulnerabilities in 2023 and now continuing with Cleo.



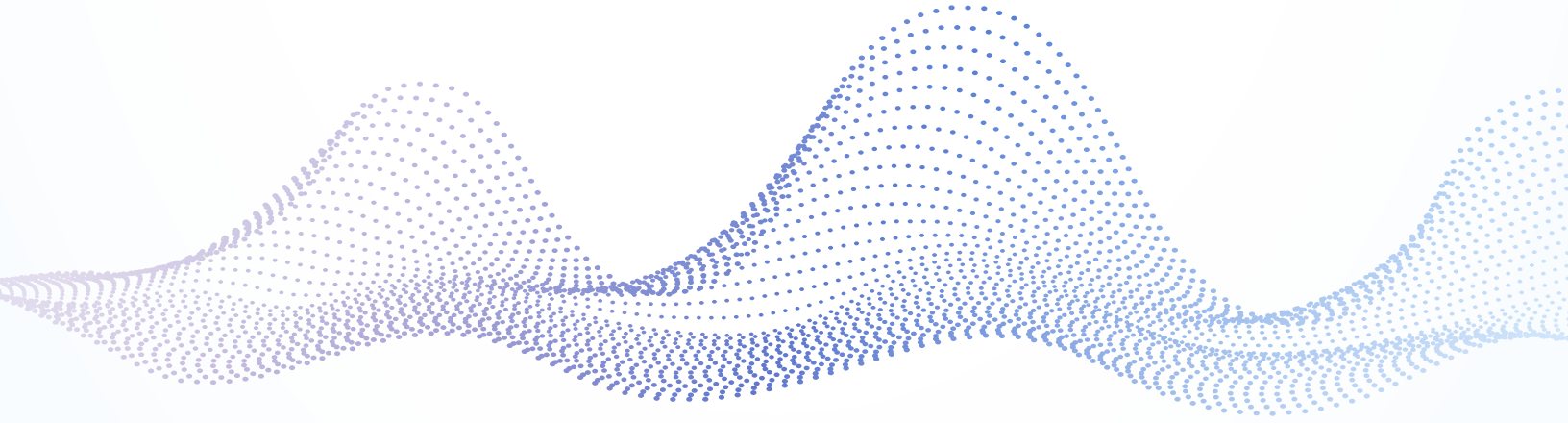
Defending Against Ransomware and Extortion Groups

Arete leverages MITRE ATT&CK® to help capture the complete picture of threat actor operations. ATT&CK is a globally accessible knowledge base of threat actor tactics and techniques that enables translation across various cybersecurity functions. Examining the most observed ATT&CK techniques from executable-enabled components of threat actor operations reveals the associated mitigations that would have been the most impactful for prevention.

Diving into the top ten ATT&CK techniques observed by Arete, Discovery tactics dominate. Discovery is used by threat actors looking to gain initial access to an environment or searching for weak points. **System Information Discovery (T1082), File and Directory Discovery (T1083),** and **Software Discovery: Security Software Discovery (T1518.001)** are all techniques threat actors use to gain information about a company's systems. These techniques tell a threat actor what the system's configurations look like, what files (and potential data to exfiltrate) exist on the system, and what security software they need to poke holes in.

Once inside a system, a threat actor needs to evade detection and execute their objectives. Some common techniques from the top ten include **Hijack Execution Flow: DLL Side-Loading (T1574.002), Process Injection (T1055),** and **Virtualization/Sandbox Evasion (T1497).** These strategies may involve the threat actor adapting once inside an organization's systems to avoid detection, like switching strategies if they detect a virtual machine environment (VME).

Closing out the top ten ATT&CK techniques are **Encrypted Channel (T1573), Obfuscated Files or Information (T1027), Archive Collected Data (T1560),** and **Masquerading (T1036).** These are all ways to disguise illegitimate activities under a legitimate cover. Archiving collected data or encrypting exfiltrated data is very common among ransomware incidents, since this may include not only evading detection but also demanding a ransom to regain access to the stolen and encrypted data.



MITRE ATT&CK TECHNIQUES MOST FREQUENTLY OBSERVED IN ARETE INCIDENT RESPONSE ENGAGEMENTS

ATT&CK TECHNIQUE	PERCENT OF TOTAL
System Information Discovery (T1082)	8.89%
Hijack Execution Flow: DLL Side-Loading (T1574.002)	8.70%
Process Injection (T1055)	7.82%
Software Discovery: Security Software Discovery (T1518.001)	7.47%
Encrypted Channel (T1573)	6.17%
Obfuscated Files or Information (T1027)	5.93%
Virtualization/Sandbox Evasion (T1497)	5.69%
File and Directory Discovery (T1083)	5.54%
Archive Collected Data (T1560)	5.32%
Masquerading (T1036)	4.85%
Process Discovery (T1057)	4.68%
Input Capture (T1056)	3.76%
Remote System Discovery (T1018)	3.67%
Application Window Discovery (T1010)	3.61%
System Time Discovery (T1124)	3.33%
Application Layer Protocol (T1071)	3.17%
Deobfuscate/Decode Files or Information (T1140)	3.00%
Impair Defenses: Disable or Modify Tools (T1562.001)	2.97%
Command and Scripting Interpreter (T1059)	2.73%
Non-Application Layer Protocol (T1095)	2.68%

Figure 9

Based on the top twenty ATT&CK techniques observed by Arete, we can infer the ATT&CK mitigations that organizations could potentially have used to defend against these common threat actor techniques.

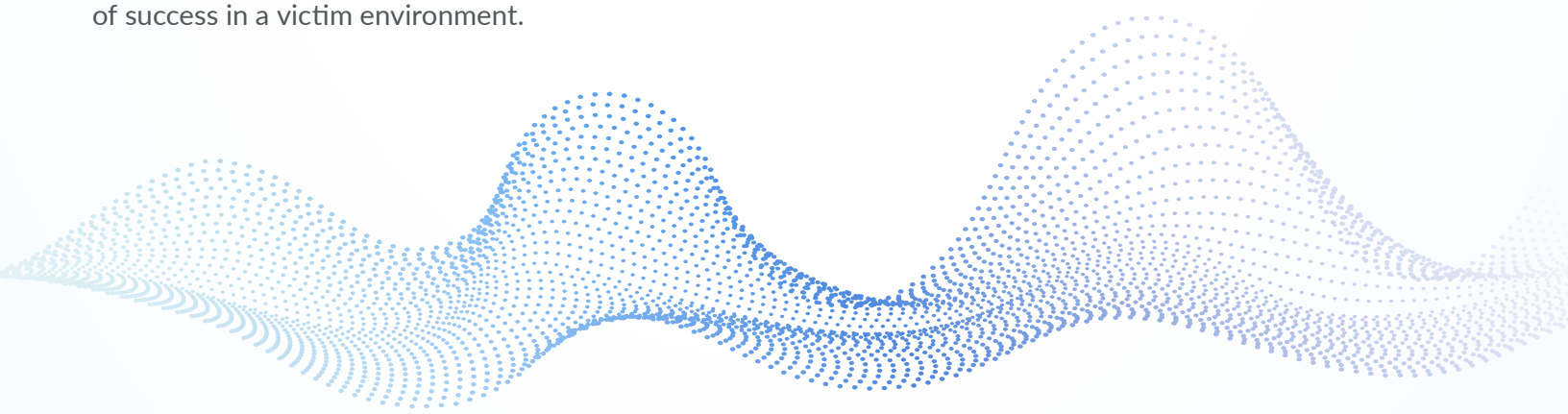
The resulting number one mitigation is **Behavior Prevention on Endpoint (M1040)**, which is often referred to in the industry as Endpoint Detection and Response (EDR). Over the last five years, Arete has seen increasing adoption of EDR technology among ransomware and extortion victims, which is a critical first line of defense. However, organizations should consider if they are using these tools effectively.

Among the approximately 60% of ransomware and extortion victims who come to Arete with EDR already in place, there is a steady increase in missed alerts preceding the encryption event. This highlights that EDR must be properly managed and tuned to be fully effective. EDR is only effective if the volume of alerts is reduced through tuning and relevant alerts are prioritized and responded to.

The emerging trend of threat actors evading EDR technology also highlights important considerations in configuration. Critical steps like turning on anti-tamper and restricting the download of system-level drivers can significantly impair threat actors' chances of success in a victim environment.

Audit (M1047) and **SSL/TLS Inspection (M1020)** are two other proactive mitigations companies can leverage to consistently check that their systems are secure. These practices include security assessments, red teaming, tabletop exercises, periodically reviewing a security checklist, and consistent implementation, which is crucial to defending against cyberattacks. Some technical strategies that audits and inspections should monitor include **Execution Prevention (M1038), Antivirus/Antimalware (M1049), Filter Network Traffic (M1037), and Network Intrusion Prevention (M1031).** All in the top ten ATT&CK mitigations, these techniques enable organizations to detect threat actors before they cause harm.

On the human side, **User Training (M1017)** is almost always at the top of the charts for recommended techniques. But human error often plays a role, so it is important to implement complementary protections as well. **Privileged Account Management (M1026) and Code Signing (M1045)** are two techniques that work on zero-trust principles: in other words, granting only necessary permissions to even privileged accounts and checking each script for a digital signature before allowing it to run.



MITRE ATT&CK MITIGATIONS THAT COULD POTENTIALLY HAVE PREVENTED INCIDENTS

MITIGATION TECHNIQUE	PERCENT OF TOTAL
Behavior Prevention on Endpoint (M1040)	15.82%
Audit (M1047)	13.98%
Antivirus/Antimalware (M1049)	10.02%
Network Intrusion Prevention (M1031)	8.92%
User Training (M1017)	8.00%
Privileged Account Management (M1026)	7.83%
Code Signing (M1045)	5.62%
Execution Prevention (M1038)	5.62%
SSL/TLS Inspection (M1020)	4.58%
Filter Network Traffic (M1037)	4.34%
Restrict File and Directory Permissions (M1022)	3.60%
User Account Management (M1018)	3.60%
Disable or Remove Feature or Program (M1042)	2.03%
Limit Software Installation (M1033)	2.03%
Restrict Web-Based Content (M1021)	2.03%
Network Segmentation (M1030)	1.99%

Figure 10

The most effective mitigations remain stable year over year. Just as ransomware and extortion groups continually evolve, security fundamentals, when carefully applied and managed, are the most effective strategies for preventing threat actor success.

2024 Cyber Threat Landscape in the APAC Region

Ransomware and extortion threats continue to pose significant challenges across the APAC region. Throughout 2024, these attacks evolved significantly, utilizing advanced tactics such as real-time targeting to identify vulnerabilities and tailor exploits to specific organizations. Threat groups employ sophisticated encryption to lock critical data and incorporate dual extortion by threatening to leak stolen information, maximizing pressure on victims to pay ransoms.

Additionally, the rise of RaaS operations made ransomware attacks more accessible, leading to a surge in high-profile incidents across the region. The use of cryptocurrencies for ransom payments adds additional complexity to tracing and mitigating the financial impact of these attacks. Emerging trends indicate a shift towards supply chain attacks and targeting of cloud services, amplifying the risk for interconnected systems.

Influence of Major Geopolitical Issues on Ransomware and Extortion

India

Financially motivated threat actors, state-sponsored threat actors, and other threat actors interested in data leaks are drawn to India's expanding economy, particularly industrial sectors like manufacturing, information and communication technology, financial services, e-commerce, and pharmaceuticals. One noteworthy tendency that evolved in the post-pandemic age is the rise in eCommerce and digital payments. Threat actors from North Korea, China, Pakistan, and Russia actively attack Indian organizations, and India's biggest international competitors are still China and Pakistan, both of which support cybercriminals who may take advantage of gaps in India's quickly digitizing economy.

Malaysia

Financially motivated threat actors, state-sponsored threat actors, and other threat actors interested in data leaks are drawn to Malaysia due to the country's growing economic activity, particularly in the industrial sectors of manufacturing, information and communication technology, financial services, oil and gas, and mining. The South China Sea disputes are significant sources of geopolitical conflict, which involve territory claims and marine rights. Threat actors from North Korea, China, and Russia frequently attack Malaysian organizations.

Japan

The size and diversification of Japan's economy give it enormous global significance. It is a major center for financial, manufacturing, automotive, and technology services. State-sponsored adversaries find Japanese firms' intellectual property (IP) very intriguing due to its quality. From a geopolitical perspective, North Korea, China, and Russia pose serious threats to Japan. Ongoing issues include territorial disputes, strategic partnerships with NATO and QUAD, and regional supremacy.

Notable Cyber Event: Niconico, a video-sharing website owned by Kadokawa Corporation, was shut down for a month due to a ransomware attack. Hundreds of thousands of users' personal information were compromised, negatively impacting the company's operations, stock value, and consumer trust.

Indonesia

The expansion of Indonesia's economy, particularly in several industrial sectors, including manufacturing, eCommerce, travel and tourism, infrastructure, construction, mining, and aviation, attracts threat actors with financial motivation, state-sponsored threat actors, and other threat actors interested in data leaks. Threat actors from China, North Korea, and Russia frequently attack Indonesian organizations. A major source of geopolitical conflict is the South China Sea disputes, which involve territory claims and marine rights.

Notable Cyber Event: Immigration and airport operations were among the more than 280 vital functions interrupted by a ransomware attack on the National Data Center. The ransom demand from the attackers was $8 million.

Australia, Singapore, and Other APAC Regions

Cyberattacks in the region have become more sophisticated, with threat actors using cutting-edge methods to breach networks and systems. Risks are higher in critical infrastructure sectors, and threat actors are becoming more interested in attacking key sectors, including telecommunications, energy, and finance. The frequency and intensity of ransomware attacks have increased, presenting serious difficulties for both government and commercial organizations. To disclose the compromised data, the attackers frequently demand cryptocurrency payments. Information warfare and cyber espionage are two examples of nation-sponsored cyber operations that appear to be on the rise. This presents serious security and geopolitical issues for the area.

Extortion Tactics Targeting the APAC Region

Leveraging Local Context

Attackers are increasingly tailoring extortion messages to specific regions or sectors. For example, ransomware groups may include regional language or culturally relevant references in ransom notes to enhance their credibility and increase the likelihood of payment.

High-Profile Targets

Publicly targeting high-profile organizations, like government entities or large corporations, is often a deliberate tactic to instill fear and prompt quick payment, as these organizations are under intense pressure to restore operations.

Cryptocurrency and Anonymity

Ransom payments are usually demanded in crypto-currencies, such as Bitcoin or Monero, which offer a degree of anonymity and make it more difficult for law enforcement to trace the funds.

Reputational Damage

In some cases, attackers also threaten to damage an organization’s reputation by releasing sensitive or embarrassing information, adding additional pressure for companies to comply with ransom demands.

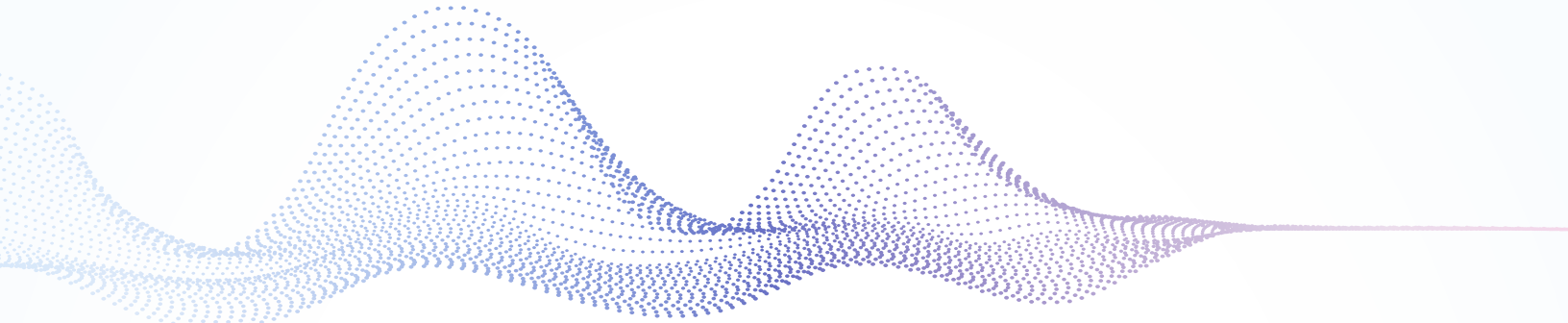
2025 Outlook

Although the top ransomware and extortion groups have changed, in many ways the threat landscape at the end of 2024 is similar to the end of 2023. Barring future law enforcement disruptions to the top RaaS groups in 2025, the ransomware ecosystem will likely remain relatively stable, with a few large groups like Akira, RansomHub, and Fog conducting the majority of cyberattacks. So long as they remain effective, threat actors will continue to leverage the same legitimate tools and software in 2025 to evade detection and facilitate attacks.

That is not to say that everything will remain the same in 2025. The percentage of organizations able to recover without paying a ransom continues to increase. As a result, threat groups may conduct more disruptive attacks or demand larger ransoms to compensate for the decreasing number of payments. As organizations work to improve their defenses, threat actors will continue to evolve and respond. EDR evasion tools will likely become more sophisticated and effective, and the exploitation of vulnerabilities will continue to rise moving into 2025.

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 Acknowledgment

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

The NCA announces the disruption of LockBit with Operation Cronos

Justice Department Disrupts Prolific ALPHV/Blackcat Ransomware Variant

U.S. and U.K. Disrupt LockBit Ransomware Variant

'Exit scam' - hackers that hit UnitedHealth pull disappearing act

United States Sanctions Senior Leader of the LockBit Ransomware Group

Further Evil Corp cyber criminals exposed, one unmasked as LockBit affiliate

Europol coordinates global action against criminal abuse of Cobalt Strike

THE RETURN OF LOCKBIT!

Arctic Wolf Labs Observes Increased Fog and Akira Ransomware Activity Linked to SonicWall SSL VPN

#StopRansomware: BianLian Ransomware Group

$75 Million Record-Breaking Ransom Paid To Cybercriminals, Say Researchers

Change Healthcare discloses $22M ransomware payment

Ascension: Health data of 5.6 million stolen in ransomware attack

Judge Sets Deadline for Motions to Dismiss Claims in Change Healthcare Data Breach Lawsuits

NHS confirms patient data stolen in cyber attack

Ransomware hits CDK Global, public sector targets in June

Ahold Delhaize Cybersecurity Incident Impacts Giant Food, Hannaford

ConnectWise ScreenConnect 23.9.8 security fix

A Catastrophe For Control: Understanding the ScreenConnect Authentication Bypass (CVE-2024-1709 & CVE-2024-1708)

Ransomware attackers introduce new EDR killer to their arsenal

SlashAndGrab: ScreenConnect Post-Exploitation in the Wild (CVE-2024-1709 & CVE-2024-1708)

Snowflake Breach: Everything We Know So Far

UNC5537 Targets Snowflake Customer Instances for Data Theft and Extortion

Flash Report: Cl0p Publishes Data of Cleo Compromise Victims

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

New Engagements
arete911@areteir.com

General Inquiries
marketing@areteir.com

www.areteir.com