JUNE | 2025

Arete

CRIMEWARE REPORT

TRENDS AND HIGHLIGHTS FROM Q1 2025

Table of Contents

Overview

Arete provides cyber risk solutions to address the entire threat lifecycle, from incident response and restoration to threat actor communications and managed security services. Leveraging data and intelligence collected during ransomware and extortion incident response engagements, Arete identified and analyzed notable trends and shifts during the first quarter (Q1) of 2025, including the most active threat groups, shifts in ransom demands and industries targeted, and commonly used malware and initial access methods.

Activity in Q1 2025 was relatively predictable, with the majority of ransomware and extortion attacks conducted by established groups that have operated for at least a year. Akira and RansomHub were the two most active threat groups, but RansomHub is reportedly struggling with internal issues, and the group's future may be questionable. Regardless of RansomHub's future, a number of established groups, including Qilin, BianLian, and Cactus, were active throughout the quarter and will likely remain persistent threats in the near term.

Across the ransomware and extortion incidents that Arete responded to in Q1, several notable trends emerged:

Akira remained the most active threat group in Q1 and was responsible for over 15% of all ransomware and extortion engagements, continuing its upward trend from 2024. INC Ransom, which was relatively quiet in 2024, was the third-most active group of the quarter, enabled partly by a critical vulnerability in SimpleHelp software, which the group exploited during Q1.

In February, internal chat logs from the Black Basta ransomware group were publicly leaked, exposing the inner workings of the group and revealing tactics its members use to target and gain access to victim environments. Arete has not observed any activity from the group so far in 2025, and it is likely that its members will attempt to rebrand or move to other ransomware groups in the wake of the leaked chats.

Social engineering attacks involving Microsoft Teams remained a persistent threat. Originally used by Black Basta in Q4 2024, this tactic was observed in incidents involving the Cactus threat group and a separate unnamed threat actor in Q1 2025. Additionally, multiple groups, including Akira, Qilin, and Interlock, were observed using "ClickFix" techniques, which trick users into executing malicious PowerShell scripts via deceptive CAPTCHA challenges to gain unauthorized access to victim networks.

Statistics and Trends from Incident Response Engagements

31
Total Named Threat Actors

8
Total Unnamed Threat Actors

Top Threat Groups By Quarter

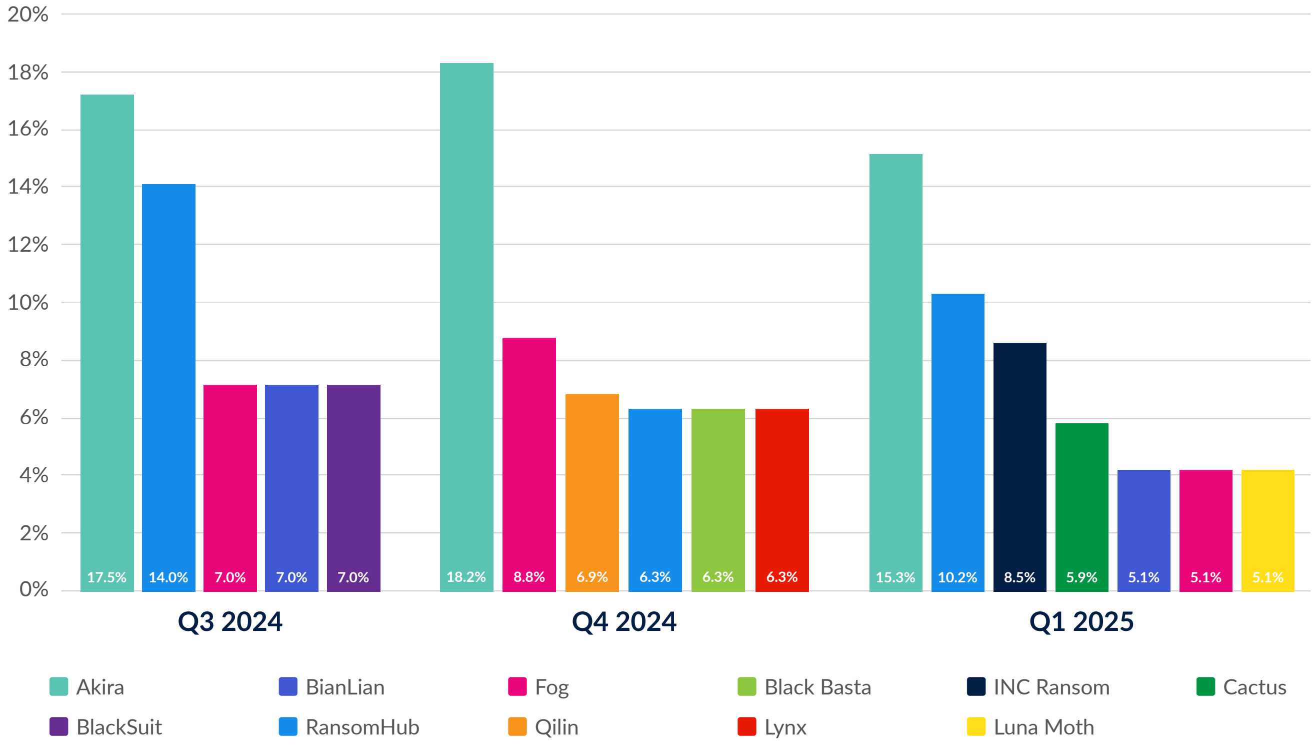


Figure 1

Top Threat Groups by Month in Q1

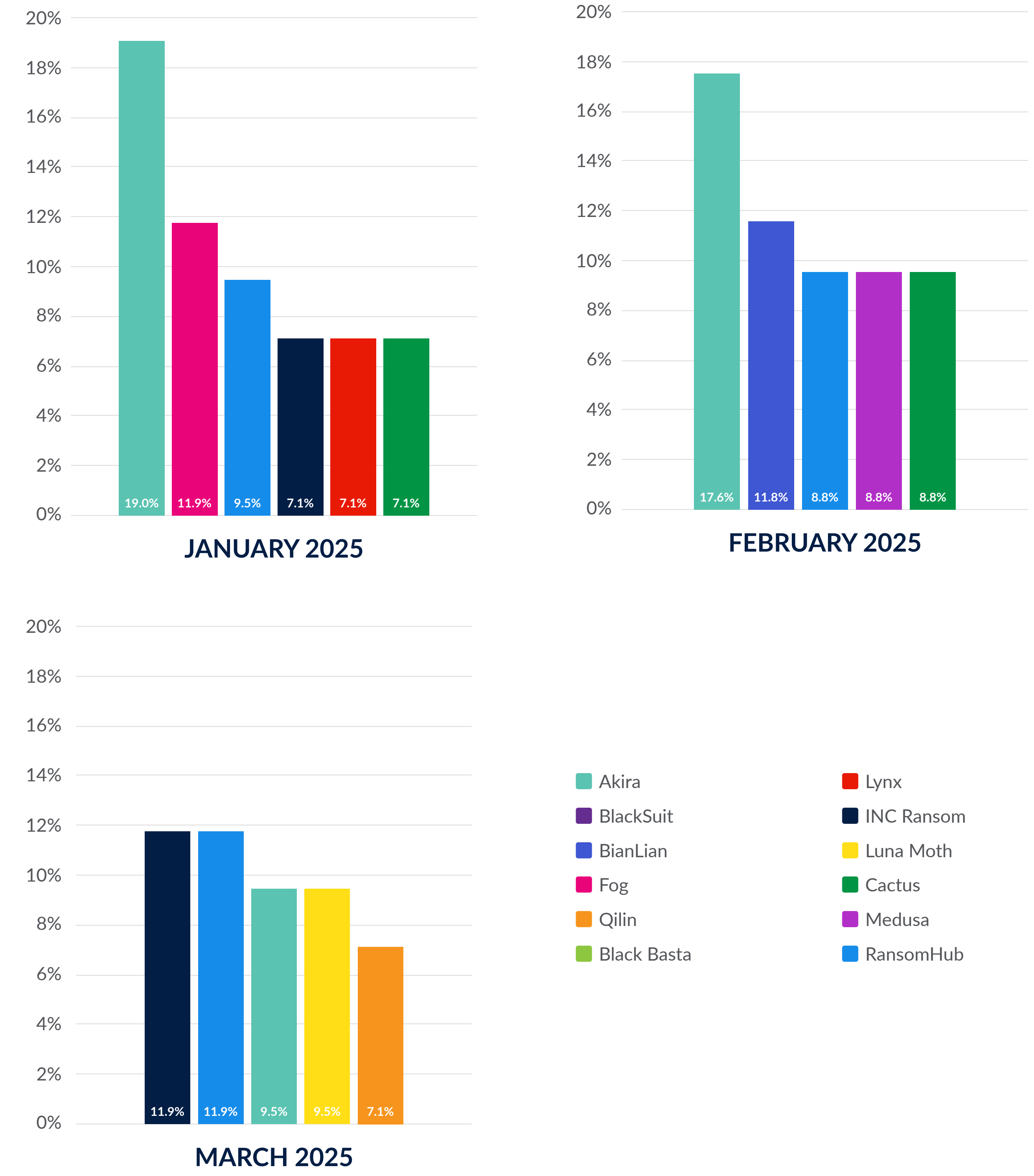


Figure 2

As was the case at the end of 2024, Akira remained the dominant ransomware group in the first quarter of 2025, accounting for 15.3% of ransomware and extortion incidents. RansomHub also remained among the top three most active threat groups each month throughout the quarter. Given their high activity levels in the second half of 2024, Arete predicted that these two groups would remain among the most active going into 2025 in our 2024 Annual Crimeware Report.

Despite its high activity in Q1, RansomHub's presence in the threat landscape may significantly diminish in Q2. RansomHub's infrastructure, including its data leak site (DLS), has been down since March 31, 2025, and remained inaccessible as of June 11, 2025. Open-source reports and dark web conversations among affiliates suggest that the outage is the result of an internal conflict between some of the group's affiliates, but no specific details or causes for the outage have been confirmed. It is not currently known when or if the group will come back online.

Apart from these two groups, the Q1 threat landscape was relatively diverse, with various established threat groups like BianLian, Cactus, Medusa, Qilin, and Luna Moth alternating in their activity levels from month to month. Although the top threat actors during this period were established groups that have operated since at least 2024, Arete also observed several new groups enter the scene, including AidLocker, HSWW, Krypt, and Weyhro.

The outlier among the top threat groups in Q1 was INC Ransom, the third most active threat group for the quarter and tied with RansomHub as the most active group in March. INC's uptick in activity was somewhat unexpected. Although the group has operated since 2023, Arete observed it in only about 2% of all ransomware and extortion engagements in 2024, and there were reports in July 2024 that the group was selling its source code. However, during Q1, INC was observed exploiting known vulnerabilities in the SimpleHelp Remote Monitoring and Management (RMM) software (CVE-2024-57726, CVE-2024-57727, and CVE-2024-57728), which could account for the higher-than-usual activity in the first quarter of 2025. While INC will likely remain a threat going into Q2, it seems unlikely that the group will sustain the volume of attacks observed in Q1, based on data from previous years.

Scan QR code to access the
2024 Annual Crimeware Report

Highlights from the Threat Landscape

Black Basta Chat Logs Leaked

On February 11, 2025, Telegram user ExploitWhisper leaked 200,000 chat logs from the ransomware group Black Basta. These chats spanned from September 2023 to September 2024 and provided an important look into the group's inner workings, connections to other threat groups, and related incidents. The chat logs reveal a polished, sophisticated organization that often conducts extremely in-depth research on potential victims and prioritizes high-revenue companies when selecting targets. An analysis of the days and times of message activity also revealed that Black Basta affiliates are most active during a relatively standard Monday to Friday schedule.

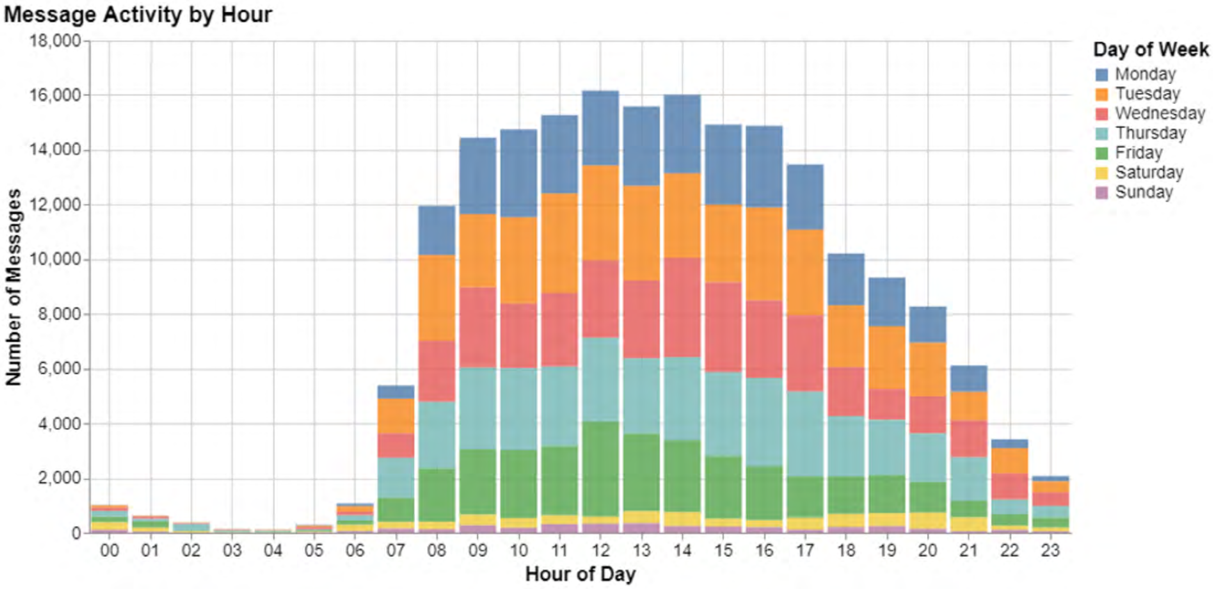


Figure 3. Chart depicting the days and times that Black Basta affiliates were most active, highlighting that even cybercriminals often adhere to a standard work schedule. *(Source: Arete)*

Black Basta closely monitors common vulnerabilities and exposures (CVEs), with chat logs revealing references to 62 unique vulnerabilities, 53 of which are known to have been exploited. In many cases, these CVEs appeared in conversations just hours after public disclosure, indicating the group's rapid response and interest in purchasing zero-days. Additionally, the chats showed that Black Basta has developed custom exploits for some CVEs. Analysts also noted that group members frequently discussed vulnerabilities without explicitly naming CVEs.

According to the logs, the most common initial access methods leveraged by the group were Remote Desktop Protocol (RDP), virtual private networks (VPNs), and security protocols. Black Basta used infostealer malware to obtain compromised credentials and conduct credential-stuffing attacks. In one instance, a tech support employee's account was infected with infostealer malware, resulting in 50 compromised credentials. The group also commonly uses phishing campaigns targeting Microsoft services like Office 365 and Azure to gain credentials and bypass multifactor authentication (MFA). Other techniques noted included Address Resolution Protocol (ARP) poisoning, traffic interception, and Active Directory attacks.

A tool developed by Black Basta called BRUTED was revealed to be automating brute-force VPN attacks in the following services: SonicWall NetExtender, Palo Alto GlobalProtect, Cisco AnyConnect, Fortinet SSL VPN, Citrix NetScaler (Citrix Gateway), Microsoft RDWeb (Remote Desktop Web Access), and WatchGuard SSL VPN. The framework was designed to acquire credentials on edge network devices and allowed the group to gain initial access to victim environments, move laterally, and deploy its ransomware. VPN and remote access tools were among the top intrusion methods Arete observed in 2024, and the exposure of a tool like BRUTED reflects that ransomware groups are continuously evolving their techniques to find new ways to gain initial access and deploy ransomware. Black Basta also commonly used Shodan, Zoomeye, and Cobalt Strike, according to the chat logs.

Black Basta is suspected of having included some former members of Conti, an older ransomware group that also disbanded after its chat logs were leaked. Although Black Basta was active in late 2024, Arete has not responded to an incident involving the group in 2025, and its DLS has been down since January. While it is unknown whether Black Basta will reappear this year, it is possible that the group may attempt to rebrand again in the wake of these chat leaks. Members have also reportedly moved over to the Cactus ransomware group, and Arete observed Cactus using social engineering tactics this year similar to those Black Basta used in Q4 2024.

Return to Sender:

Threat Actors Send Physical Letters Posing as BianLian

The lines between cybercrime and mail fraud blurred in late February 2025, when Arete observed several incidents involving ransom letters sent via the postal service claiming to be from the BianLian extortion group. The letters, signed from the "BIANLIAN GROUP," were addressed to specific individuals at target companies and claimed that the sender had gained access to the target's network and stolen sensitive files. The letters demanded a ransom payment, typically ranging from $200,000 to $500,000, and contained a QR code linking to a Bitcoin wallet for payment. Although the letters contained links to BianLian's known DLS, they were ultimately assessed to be a scam from a threat actor posing as BianLian.

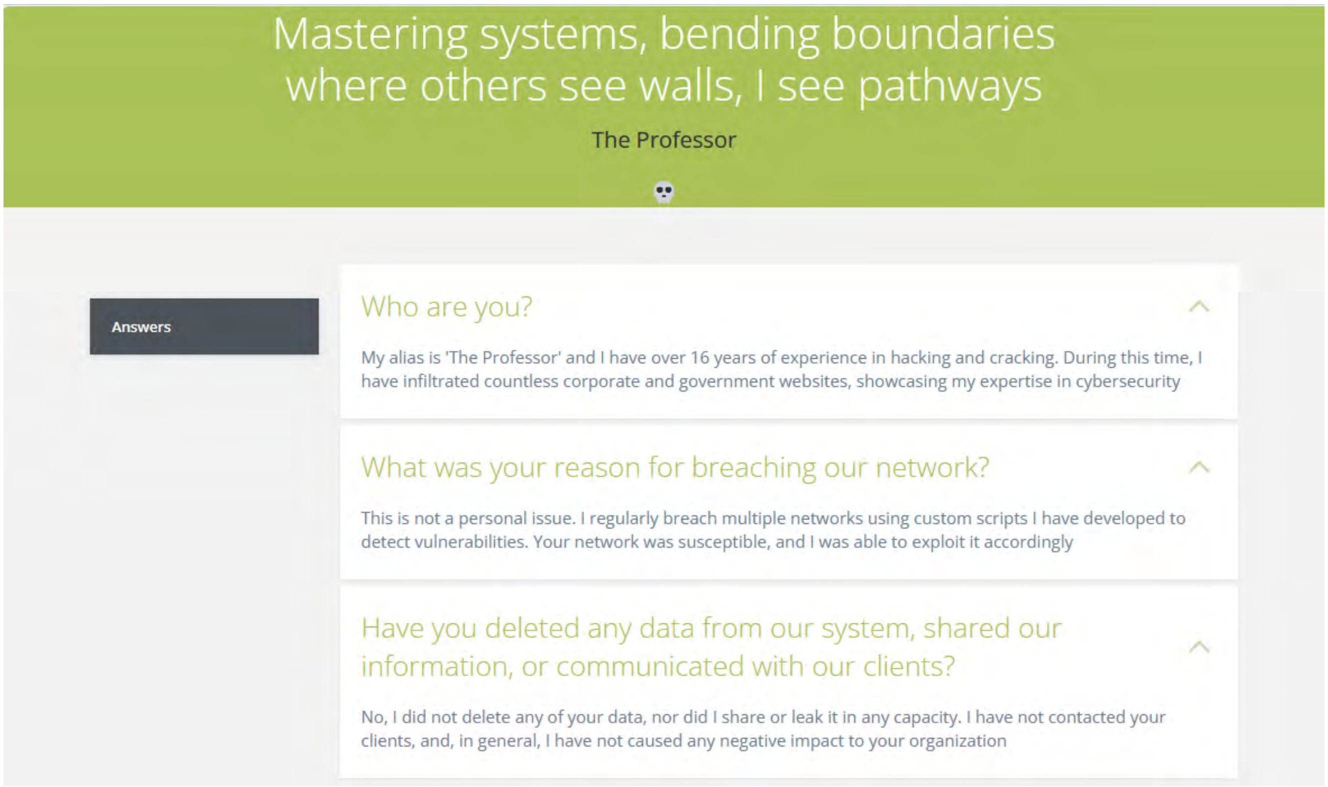
Arete did not discover indications of data exfiltration during investigations for clients who received a letter, and the FBI issued a public announcement warning of the scam in early March. While it is not uncommon for less established threat actors to impersonate larger, more well-known Ransomware-as-a-Service (RaaS) or extortion groups, these campaigns increase the complexity of accurately attributing cyber threats. This campaign also illustrates that creative cybercriminal scams aren't always highly technical or sophisticated and may require only some paper and a postage stamp.

Threat Actor Spotlight:

Mr. Anazon Changes Alias to “The Professor”

Arete first observed the self-identified extortionist called Mr. Anazon in 2023. They are presumed to be operating alone and are likely a native English speaker. Although not as prolific as the larger ransomware and extortion groups, Mr. Anazon remained periodically active in 2024 and increased their activity from 2023. The threat actor exploits vulnerabilities in software applications and operates multiple domains, typically ending with “proxy[.]com”, pre-staging them for up to two months prior to using them to communicate with victims. In 2024, Mr. Anazon primarily targeted unsecured Amazon Web Services (AWS) Simple Storage Service (S3) buckets and claimed to use automated scanning tools and crawlers to index sensitive data for exfiltration.

In Q1 2025, Arete observed Mr. Anazon using the alias “The Professor” during communications with their victims. The ransom email subject line and content have stayed consistent over time, with the primary difference being the new alias and an updated number of years of experience in the signature block of the email. Additionally, the domain used to communicate with the victim now leads to an FAQ page, a change from the website displayed in previous years.



Mastering systems, bending boundaries where others see walls, I see pathways

The Professor

Who are you?

My alias is 'The Professor' and I have over 16 years of experience in hacking and cracking. During this time, I have infiltrated countless corporate and government websites, showcasing my expertise in cybersecurity

What was your reason for breaching our network?

This is not a personal issue. I regularly breach multiple networks using custom scripts I have developed to detect vulnerabilities. Your network was susceptible, and I was able to exploit it accordingly

Have you deleted any data from our system, shared our information, or communicated with our clients?

No, I did not delete any of your data, nor did I share or leak it in any capacity. I have not contacted your clients, and, in general, I have not caused any negative impact to your organization

Figure 4. FAQ page for "The Professor" (Source: Arete)

Mr. Anazon/The Professor exemplifies the smaller portion of threat actors who choose to operate independently rather than aligning themselves with larger ransomware or extortion groups. Some will appear briefly before moving on or changing personas, while others, like Mr. Anazon, operate with relative consistency for years.

Law Enforcement Activity in Q1

Although law enforcement operations in Q1 were not as high-profile and impactful as those against LockBit and ALPHV/BlackCat in early 2024, there were still several notable actions, as law enforcement continues to pursue and pressure cybercriminals.

In early February, a joint effort by the US Federal Bureau of Investigation (FBI), the UK National Crime Agency (NCA), Europol, and law enforcement agencies from 12 other countries led to the takedown of 27 servers used by the 8Base/Phobos ransomware group and the arrests of four of its members.

8Base, which uses a variant of Phobos ransomware and has been operating since 2023, was responsible for extorting approximately $16 million in ransom payments from more than 1,000 victims worldwide, according to the US Department of Justice. Although 8base wasn't among the top threat groups Arete observed in 2024, the volume of victims highlights the global impact the group achieved in a relatively short timeframe.

Separately, on February 11, the US, UK, and Australian governments sanctioned the bulletproof hosting provider (BHP) Zservers, its registered company name XHOST Internet Solutions LP, and six of its administrators for providing support to ransomware groups, including LockBit affiliates. BHP providers are hosting services that offer anonymity from law enforcement and function as a part of the cybercrime-as-a-service ecosystem by selling access to servers and infrastructure. Despite its widespread use, however, XHOST infrastructure is not often the primary infrastructure leveraged by threat actors and was observed in only 2% of Arete ransomware and extortion engagements to date.

An international law enforcement effort led to the takedown of

27

servers used by the 8Base/Phobos ransomware group

8Base is responsible for extorting approximately

$16M

in ransom payments

from more than

1,000

victims worldwide

Sector Impacts and Threat Actor Targeting

NAICS SECTOR NAME	PERCENTAGE OF ENGAGEMENTS
Professional, Scientific, & Technical Services	18.8%
Manufacturing	14.5%
Healthcare & Social Assistance	12.0%
Construction	9.4%
Wholesale Trade	7.7%
Other Services (except Public Administration)	5.1%
Administrative & Support & Waste Management & Remediation Services	4.3%
Educational Services	4.3%
Transportation & Warehousing	4.3%
Finance & Insurance	3.4%
Information	3.4%
Retail Trade	3.4%
Accommodation & Food Services	2.6%
Arts, Entertainment, & Recreation	1.7%
Management of Companies and Enterprises	1.7%
Public Administration	1.7%
Uncategorized	1.7%

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.*

Professional, Scientific, and Technical Services was the most impacted sector in Q1, followed by Manufacturing, which aligns with the trend observed in 2024, when these two sectors were also the most targeted. Professional, Scientific, and Technical Services accounted for almost 19% of the ransomware and extortion victims observed by Arete in the first quarter, just slightly lower than the 19.57% observed in 2024. This trend can partially be attributed to targeted operations by the Luna Moth extortion group. Although Luna Moth was only responsible for just over 5% of ransomware and extortion incidents in Q1, the group solely targeted victims in the Professional, Scientific, and Technical Services sector, namely law firms, consistent with the group's previous operations.

Other than Luna Moth, the threat actors observed in Q1 appeared to remain opportunistic in nature, targeting technologies or vulnerabilities rather than specific industries. For example, INC Ransom and RansomHub exploited a specific vulnerability in SimpleHelp RMM software (CVE-2024-57727), while Akira continued to target SonicWall vulnerabilities.

Publicly available financial information also affects which organizations some threat groups target. Multiple threat groups, including Hunters International and Lynx, use revenue data found on ZoomInfo to target companies and set initial ransom demands, regardless of whether the information is accurate. During one engagement in Q1, the threat actor explicitly mentioned that if an organization's annual revenue exceeds $5 million on the ZoomInfo website, it becomes a potential target for cybercriminal groups. Furthermore, Arete observed members of Black Basta mention ZoomInfo over 900 times in their leaked chat logs, demonstrating the site's role as a popular reconnaissance and targeting tool for threat actors.

SECTORS	MEDIAN DEMAND	PERCENT OF TIME A RANSOM IS PAID
Manufacturing	$1,200,000	23.5%
Professional, Scientific, and Technical Services	$700,000	40.9%
Wholesale Trade	$500,000	11.1%
Healthcare & Social Assistance	$443,355	28.6%
Construction	$200,000	27.3%

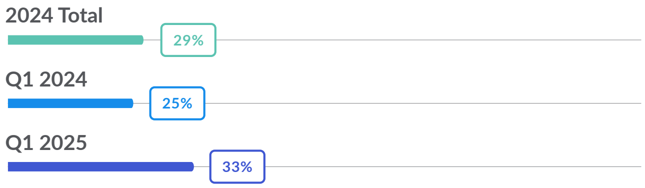
Figure 7

Of the top five sectors impacted in Q1, Manufacturing had the highest median ransom demand. However, as was the case in 2024, organizations in this sector remained resilient in their ability to recover without paying a ransom, making a payment only 23.5% of the time, almost 10% less often than the overall average for all sectors.

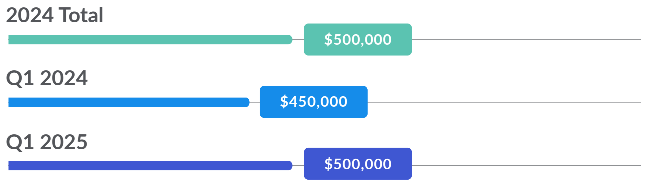
Conversely, Professional, Scientific, and Technical Services had a higher-than-average median ransom demand and made a payment more often than the other four top sectors, in part due to the frequent need for these organizations to pay to prevent sensitive stolen data from being leaked. The Luna Moth extortion group, which solely targeted victims in the Professional, Scientific, and Technical Services sector in Q1, did not utilize encryption but received payments from two-thirds of its victims in exchange for data suppression. Although the absence of encryption typically leads to a lower median demand, several demands over $1 million in Q1 from other groups like Akira and Cactus drove up the median demand for this quarter.

Trends in Ransom Demands and Payments

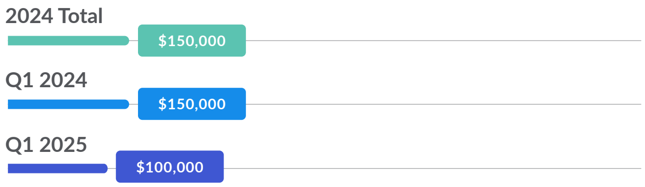
PERCENTAGE OF TIME A RANSOM IS PAID



MEDIAN RANSOM DEMAND



MEDIAN RANSOM PAYMENT



Although the percentage of organizations making ransom payments to cybercriminals declined from 2023 to 2024, that number increased slightly to 33% in Q1 2025. From month to month, however, the percentage of time a ransom was paid has trended downward since the start of the year.

In January, a payment was made in about 37% of all ransomware and extortion engagements. However, that figure was a little over 32% in February, and it decreased again to 31% in March.

Additionally, although more organizations opted to pay a ransom in Q1, the median payments decreased compared to 2024, while the median initial ransom demand stayed the same. These lower negotiated amounts could also have resulted in the slightly higher number of organizations making ransom payments in Q1.

Arete has noted in previous Crimeware Reports that while the frequency of ransom payments to cybercriminals has been trending down over the past few years, eventually that percentage was likely to plateau.

How Often Do Threat Actors Actually Leak Data?

The threat of data exposure is one of the primary pressure tactics that cybercriminals use to coerce their victims into making ransom payments, with most established threat groups operating a dedicated DLS. While the tactic has proven effective, not all ransomware and extortion groups ultimately leak data on their DLS. Based on the victims posted during Q1 2025, Arete observed the following trends among the three most active ransomware groups of the quarter when a ransom payment was not made for data suppression:

Akira

Of the total engagements where a ransom payment was not made to the threat actor, Akira posted the victim to its DLS 55% of the time. The percentage of victims not posted to the DLS (45%) closely matches the percentage that did not have evidence of data exfiltration during forensic analysis.

INC Ransom

In Q1, INC Ransom posted victims to its DLS just 40% of the time. In previous years, Arete observed INC Ransom reach out to the victims' employees as an added pressure tactic to elicit ransom payments, but Arete has not observed this tactic thus far in 2025.

RansomHub

Arete observed RansomHub posting victims to its DLS 50% of the time, based on the engagements in Q1 where a ransom was not paid. However, as noted earlier in this report, RansomHub's DLS has been down since late March 2025.

Initial Access Trends and Commonly Observed Tools and Malware

In Q1 2025, Arete observed that ransomware groups continued to refine their initial access methods, with vulnerability exploits, compromised credentials, social engineering, and ClickFix attacks emerging as the most prominent attack vectors. These techniques, often used in combination, enable threat actors to breach environments quickly and with minimal detection, posing significant risk to organizations worldwide.

Vulnerability Exploits

Vulnerability exploits continue to be a common method ransomware and extortion groups use to target known vulnerabilities in exposed systems and gain unauthorized access into victim environments. In Q1, threat actors continued to focus on perimeter devices such as VPNs, firewalls, and network management systems. Arete observed Akira ransomware exploiting a server-side request forgery (SSRF) vulnerability in SonicOS SSH (CVE-2024-53705), allowing the threat actors to manipulate server requests internally.

Meanwhile, Qilin ransomware targeted Fortinet products, exploiting a VPN-related flaw in FortiManager (CVE-2024-55591) and a critical vulnerability in FortiOS 7.0.16 (CVE-2024-21762), which affects SSL VPNs and enables remote, unauthenticated code execution via specially crafted HTTP requests. These exploits reflect a broader trend of ransomware groups leveraging remote code execution and authentication bypass vulnerabilities in unpatched or misconfigured public-facing infrastructure.

Notable Vulnerabilities Exploited in Q1

SimpleHelp RMM

In early 2025, multiple threat groups, including INC Ransom and RansomHub, exploited critical vulnerabilities in SimpleHelp RMM software to gain unauthorized access to target networks. The vulnerabilities (CVE-2024-57726, CVE-2024-57727, and CVE-2024-57728) affect SimpleHelp versions 5.5.7 and earlier, allowing for unauthenticated path traversal, remote code execution, and privilege escalation.

CrushFTP

In late March, a critical vulnerability was discovered in the managed file transfer solution platform CrushFTP. The vulnerability (CVE-2025-31161) affects CrushFTP versions 10 and 11, allowing unauthenticated attackers to temporarily authenticate as any user, including administrators, leading to full server compromise. CVE-2025-31161 is simple to exploit, and public exploit code is readily available, increasing risk to organizations using the platform. While the KillSec threat group has publicly claimed responsibility for exploiting CVE-2025-31161, it is likely that multiple threat actors are actively targeting this vulnerability.

Compromised Credentials

In the first quarter of 2025, compromised credentials remained a prevalent method for initial access in cyberattacks, with several threat actors leveraging stolen or weak login information to infiltrate networks. Notably, ransomware groups such as Medusa were observed launching widespread phishing campaigns aimed at harvesting user credentials. Once access was gained, these actors used valid login details to move laterally across networks, escalate privileges, and establish persistence—all while bypassing many traditional security defenses.

Arete also notes the growing role of the dark web in facilitating this access. Threat actors increasingly relied on stealer logs, which are collections of credentials harvested through infostealer malware and later sold or traded on underground forums. These logs provide attackers with ready-made access to corporate accounts, VPNs, and cloud platforms, allowing them to bypass traditional access controls and operate covertly.

Social Engineering through Fake Invoices and Remote Support Tools

In Q1, Arete observed multiple threat groups using email bombing and social engineering tactics involving Microsoft Teams to gain initial access to victim environments. Email bombing involves flooding a victim's inbox with thousands of non-malicious emails, posing as the victim company's IT help desk, and messaging the victim on Microsoft Teams to convince them to install a remote desktop support tool, such as Microsoft Remote Assist, that provides the threat actor with remote access to their machine.

In other incidents, threat actors gained access through phishing links that led to fake OWA/OneDrive login pages and subsequent redirection to malicious URLs. Black Basta has been observed using this tactic since 2024, and in February 2025, Arete observed the Cactus threat group and a separate unnamed threat actor cluster using the same tactic. Follow-up actions in victim environments demonstrate an overlap between Cactus and Black Basta, which is assessed to be a result of members of Black Basta moving to the Cactus threat group in the aftermath of the Black Basta internal chat logs leak.

Additionally, in March 2025, the Luna Moth extortion group resumed using phishing emails with fake invoices from StarZ HD or Zinio to lure victims into contacting attackers. During staged support sessions, users are tricked into installing remote tools like Zoho Assist, allowing the deployment of utilities like WinSCP for further access.

Trend of ClickFix Attacks Emerges

In the first quarter of 2025, multiple threat groups, including Qilin, Akira, and Interlock, adopted a social engineering tactic known as “ClickFix.” This technique involves mimicking legitimate IT tools or processes, such as software updates or system verification prompts, to trick users into executing malicious PowerShell scripts via deceptive CAPTCHA challenges hosted on compromised websites. These commands enable the deployment of malware, allowing attackers to gain unauthorized access to corporate networks and initiate file-encrypting ransomware attacks.

Top Tools and Malware Observed

During Q1, threat actors largely used many of the same tools and malware as in 2024 and continued to leverage legitimate IT software tools in cyberattacks. That said, the landscape of malware and tools did evolve in Q1, with the use of advanced, off-the-shelf tools and continued use of tools designed to bypass or disable endpoint detection and response (EDR) software.

RMM Tools

Remote monitoring and management (RMM) tools have become a prevalent choice for threat actors seeking persistent access to compromised environments. These legitimate IT administration tools, including ScreenConnect, Atera, AnyDesk, and SimpleHelp, are increasingly exploited to facilitate unauthorized access, lateral movement, and data exfiltration. Their use is particularly concerning due to their legitimate nature, which allows attackers to blend in with normal network traffic and evade detection.

AnyDesk emerged as one of the most favored RMM tools by threat actors due to its ease of deployment, lightweight footprint, and ability to operate stealthily in compromised environments. RMM platforms are used not only for access, but also to conduct lateral movement and deploy additional malicious payloads, such as ransomware and information stealers to exfiltrate data.

Discovery Tools

Threat actors' use of discovery tools remained consistent compared to previous reporting periods, reinforcing their critical role in the reconnaissance and lateral movement attack stages. In Q1 2025, Arete identified continued use of Advanced IP Scanner and NetScan, widely available utilities favored for their simplicity and effectiveness in mapping network infrastructure, identifying live hosts, and discovering open shares. Additionally, Arete observed an increased use of specialized tools, including SharpShares, which Akira employed to identify accessible network shares and prioritize high-value data for exfiltration or encryption. Similarly, the DarkAngels ransomware group leveraged BloodHound, a powerful Active Directory mapping tool that enables attackers to uncover complex permission relationships, identify attack paths, and facilitate privilege escalation across domain environments.

Exfiltration Tools

In 2025, threat actors continue to rely on the same legitimate tools for data exfiltration that were observed in 2024, with a notable preference for cloud-based utilities. MEGAsync was frequently used to upload stolen data to MEGA Cloud, leveraging its synchronization features to automate the process. Similarly, tools like Rclone, WinSCP, and FileZilla were employed to transfer large volumes of data to external servers or cloud storage platforms.

Lateral Movement Tools

Lateral movement remained a critical tactic in ransomware campaigns, with threat actors relying on a combination of legitimate administrative tools and custom utilities to navigate and escalate privileges within compromised networks.

Notably, PSExec was frequently used to remotely execute system commands, allowing attackers to move laterally across the network by exploiting administrative privileges. PowerShell and Windows Management Instrumentation (WMI) were also leveraged extensively, enabling attackers to execute scripts and commands remotely while maintaining stealth. Mimikatz played a crucial role in credential dumping, allowing threat actors to extract passwords and escalate privileges, facilitating further lateral movement. Remote Desktop Protocol (RDP) was commonly exploited, often through stolen credentials or vulnerabilities, to access additional network systems. Additionally, NetSupport Manager, a legitimate remote access tool, was observed being used to maintain control over compromised systems and enable continued movement within the network. All these tools, while legitimate in nature, were used by cybercriminals to blend in with normal network activity, making detection more challenging.

Threat Actors Continue to Leverage EDR Evasion Tools

Threat actors continued to use tools to bypass or disable EDR software. In February, Arete observed the Medusa ransomware group utilizing the Poortry tool to evade EDR software when attacking victims. Poortry is a tool that uses a modified kernel driver to bypass or disable EDR software and has been a threat since 2022. It leverages three core capabilities to evade most built-in driver protection capabilities: abusing leaked certificates, forging signature timestamps, and bypassing Microsoft attestation signing. Some of the drivers observed in the Medusa engagements had expired or illegitimate certificates that were named to appear as legitimate EDR drivers. In particular, Arete observed the drivers masquerading as CrowdStrike Falcon and Palo Alto Cortex.

Additionally, Arete observed RansomHub continue to use EDRKillShifter to disable EDR software during an engagement in Q1. RansomHub was first observed using EDRKillShifter in the second half of 2024, and the tool employs a “bring your own vulnerable driver” (BYOVD) technique, which exploits legitimate but vulnerable drivers. Specifically, Arete has noted that EDRKillShifter is loaded from an executable named magic.exe, which deploys the vulnerable driver. This executable is believed to be a dedicated EDR-killing utility designed to disable security software, providing attackers with elevated privileges and stealth during post-exploitation phases.

Arete observed an increase in the use of EDR killers by multiple threat groups in 2024, and this trend will likely continue in 2025 as more organizations rely on EDR solutions to secure their environments. The continued use of these tools highlights the increasing sophistication of ransomware operators and the critical need for defenses capable of detecting such advanced tactics.

Top Malware Observed

In Q1 2025, threat actors continued to rely on a mix of credential stealers, RATs, and socially engineered loaders to compromise systems at scale. These malware families stood out for their use of evasion tactics, social engineering, and persistent infection methods across widespread campaigns.

Lumma Stealer

Lumma Stealer is credential-harvesting malware that specializes in targeting cryptocurrency wallets, browser-saved passwords, extensions, and two-factor authentication (2FA) tokens. Lumma Stealer remains popular among threat actors in 2025 due to its frequent updates, sophisticated evasion techniques, and user-friendly operation. Lumma now utilizes the ChaCha20 cipher to decrypt its configuration files, regularly rotates command-and-control (C2) servers to avoid detection, and leverages platforms such as GitHub to host payloads, complicating detection by traditional security tools. Security analysts also recently confirmed Lumma's ability to extract data from major browser extensions.

Neshta

Neshta is file-infecting malware that primarily targets Windows systems by embedding malicious code into executable (.exe) files. Once executed, Neshta ensures persistence by modifying Windows registry keys, often disguising itself as legitimate system files like “svchost.com.” It continually infects additional executables on compromised systems, complicating remediation efforts. Beyond its primary file-infection capability, Neshta can also serve as a backdoor, allowing attackers to steal sensitive data, deploy further malware, and conduct reconnaissance. Its advanced persistence tactics, including registry modification and embedding in crucial system files, frequently require specialized malware removal tools or, in severe cases, complete system reinstallation. Analysts verified that recent Neshta variants have adopted sophisticated obfuscation methods, significantly increasing their resilience against conventional antivirus solutions.

SocGholish

Commonly known as "FakeUpdates," SocGholish is JavaScript-based malware primarily leveraging social engineering by impersonating legitimate software updates to deceive users into downloading malicious payloads. In 2025, SocGholish continues evolving, incorporating sophisticated infection techniques involving JavaScript, PowerShell, and compressed file formats designed to bypass security defenses. SocGholish remains a significant threat, with confirmed evidence that recent campaigns extensively utilize multi-stage loaders to enhance infection effectiveness and obfuscation.

NetSupport RAT

NetSupport is a remote access trojan (RAT) derived from the legitimate NetSupport Manager remote administration software. Though initially intended for legitimate use, threat actors repurposed NetSupport Manager for malicious purposes, achieving unauthorized control of compromised systems. Once installed, NetSupport RAT enables attackers to manipulate data, deploy additional payloads, conduct real-time screen monitoring, and capture screenshots, audio, and video. In early 2025, threat actors notably increased NetSupport RAT infection success rates through social engineering tactics, prominently employing the ClickFix method discussed earlier in this report.

Defending Against the Most Observed Threat Groups

Arete leverages the MITRE ATT&CK® framework as a foundational component of its threat detection, analysis, and response strategies. By mapping observed techniques from Q1 2025 to ATT&CK, Arete not only tracks the evolving tactics of ransomware groups but also provides organizations with actionable insights and aligned mitigations to strengthen their security posture against real-world threats.

ATT&CK-Based Techniques Used by Threat Actors

In Q1 2025, Arete observed threat actors continuing to employ a wide range of techniques to navigate, escalate privileges, and evade detection within compromised networks. Techniques including **System Information Discovery (T1082)** and **File and Directory Discovery (T1083)** were frequently used to gather critical system and file information. Attackers also leveraged **Process Injection (T1055)** and **Hijack Execution Flow: DLL Side-Loading (T1574.001)** to inject malicious code into legitimate processes, further obscuring their presence.

Masquerading (T1036) and **Obfuscated Files or Information (T1027)** were used to disguise malicious activities and evade detection by security software, which was also targeted through **Software Discovery: Security Software Discovery (T1518.001)**. To evade security measures, attackers employed **Virtualization/Sandbox Evasion (T1497)** and **Encrypted Channels (T1573)**.

Additionally, techniques like **Impair Defenses: Disable or Modify Tools (T1562.001)** and **Input Capture (T1056)** were utilized to disable security tools and capture sensitive user input. These techniques highlight the evolving sophistication of ransomware operations, with threat actors utilizing diverse methods to evade defenses and persist within targeted environments.

Mitigation Techniques

Based on the top ATT&CK techniques observed by Arete during Q1, several high-impact ATT&CK mitigations emerge as the most effective defenses organizations can implement to counter the techniques used by threat actors. These include measures such as Behavior Prevention on the Endpoint (M1040), Execution Prevention (M1038), and Network Intrusion Prevention (M1031) to block malicious activity at various stages.

Enhancing identity and access management through **Privileged Account Management (M1026)** and **User Account Management (M1018)**, combined with **User Training (M1017)**, can significantly reduce the risk of initial access and lateral movement.

Additional mitigations like **Filter Network Traffic (M1037)**, **Limit Software Installation (M1033)**, and **Disable Unnecessary Programs (M1042)** help harden the environment and limit the opportunities for attackers to execute or persist. These ATT&CK-aligned mitigations reflect best practices tailored to the most prevalent techniques observed in ransomware operations.

Conclusion

In the first quarter of 2025, the ransomware ecosystem largely followed a predictable pattern from the end of 2024. Akira remained the most observed threat group, and the top groups month-to-month were mostly the same known and established threat groups active in the second half of 2024. While many of the same tools, malware, and access trends also remained consistent, threat actors increasingly leveraged social engineering tactics in Q1, which continue to evolve in sophistication.

There are indications that the threat landscape may undergo some changes in Q2. International law enforcement continues to pressure cybercriminal groups, as illustrated by efforts against 8Base in Q1. And unlike in 2024, when law enforcement was largely responsible for disrupting the large RaaS groups, 2025 has already seen disruptions to two established RaaS groups that appeared to stem from internal issues, first with public exposure of Black Basta's internal chat logs and again in late March with RansomHub's infrastructure suddenly going offline. To hedge against setbacks like these, threat groups may begin to rebrand more frequently or set up separate but closely affiliated brands, similar to Akira and Fog. Individual threat actors may also affiliate with more than one RaaS to mitigate risk and ensure continuity of operations, which was observed in Q1 with members of Black Basta moving to Cactus.

As the threat landscape evolves throughout 2025, Arete remains committed to leveraging our unparalleled data and experience to inform our clients and partners and work to combat cyber extortion.

Akira remained the most observed threat group in the first quarter of 2025.

International law enforcement continues to pressure cybercriminal groups.

Individual threat actors may affiliate with more than one RaaS to mitigate risk.

Appendix and 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.

Arete Internal Data

Mail scam targeting corporate executives claims ties to ransomware. (2025, March 6). Internet Crime Complaint Center. *https://www.ic3.gov/PSA/2025/PSA250306-2*

Abrams, L. (2024, October 25). **Black Basta ransomware poses as IT support on Microsoft Teams to breach networks**. BleepingComputer. *https://www.bleepingcomputer.com/news/security/black-basta-ransomware-poses-as-it-support-on-microsoft-teams-to-breach-networks/*

Timothy, J., Mouton, Jean-Pierre, & Silver, R. (2025, April 8). **RansomSnub: RansomHub's Affiliate Confusion. GuidePoint Security.** **https://www.guidepointsecurity.com/blog/ransomsnub-ransomhubs-affiliate-confusion/**

Blbkin, V. (2025, March 6). **Inside Black Basta ransomware Group's chat leak.** Eclypsium. *https://eclypsium.com/blog/inside-black-basta-ransomware-groups-chat-leak/*

Wright, R. (2025, February 27). **Leaked ransomware chat logs reveal Black Basta's targeted CVEs.** Cybersecurity Dive. *https://www.cybersecuritydive.com/news/leaked-ransomware-chat-logs-reveal-black-bastas-targeted-cves/741129/*

Black Basta exposed: A look at a cybercrime data leak. (2025, February 28). Intel 471. *https://intel471.com/blog/black-basta-exposed-a-look-at-a-cybercrime-data-leak*

Winder, D. (2025, March 2). **Ransomware gang leak shows stolen passwords and 2FA codes driving attacks.** Forbes. *https://www.forbes.com/sites/daveywinder/2025/03/02/ransomware-gang-leak-shows-stolen-passwords-2fa-codes-driving-attacks/*

Team, K. C., Edited: Kapon, B. (2025, March 7). **Black Basta leak: New findings reveal victim details.** KELA Cyber. *https://www.kelacyber.com/blog/black-basta-leak-victim-details/*

Townsend, K. (2025, March 3). **Black Basta Leak Offers Glimpse Into Group's Inner Workings.** Security Week. *https://www.securityweek.com/black-basta-leak-offers-glimpse-into-groups-inner-workings/*

Loveria, C., Carbery, S., Samaniego, J., O'Connor, A., Kenefick, I., Cardoso, G., Silva, L. (2025, March 3). **Black Basta and Cactus ransomware groups add BackConnect malware to their arsenal.** Trend Micro. *https://www.trendmicro.com/en_us/research/25/b/black-basta-cactus-ransomware-backconnect.html*

Key figures behind Phobos and 8Base ransomware arrested in international cybercrime crackdown. (2025, February 11). Europol. *https://www.europol.europa.eu/media-press/newsroom/news/key-figures-behind-phobos-and-8base-ransomware-arrested-in-international-cybercrime-crackdown*

Phobos ransomware affiliates arrested in Coordinated International. (2025, February 10). Department of Justice. **https://www.justice.gov/opa/pr/phobos-ransomware-affiliates-arrested-coordinated-international-disruption**

#StopRansomware: Medusa Ransomware. (2025, March 12). CISA. *https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-071a*

Toulas, B. (2025, April 18). **Interlock ransomware gang pushes fake IT tools in ClickFix attacks.** BleepingComputer. *https://www.bleepingcomputer.com/news/security/interlock-ransomware-gang-pushes-fake-it-tools-in-clickfix-attacks/*

Tactics, H. A. (2025, April 4). **CrushFTP CVE-2025-31161 AUTH Bypass and Post-Exploitation.** Huntress. *https://www.huntress.com/blog/crushftp-cve-2025-31161-auth-bypass-and-post-exploitation*

A vulnerability in CrushFTP could allow for unauthorized access. (2025, March 27). CIS. *https://www.cisecurity.org/advisory/a-vulnerability-in-crushftp-could-allow-for-unauthorized-access_2025-032*

Parsons, M., Cowie, C., Souter, D., Neal, H., Bradshaw, A., Gallagher, S. (2025, January 21). **Sophos MDR tracks two ransomware campaigns using "email bombing," Microsoft Teams "vishing."** Sophos News. *https://news.sophos.com/en-us/2025/01/21/sophos-mdr-tracks-two-ransomware-campaigns-using-email-bombing-microsoft-teams-vishing/*

Ramos, A. (2025, January 24). **Arctic Wolf observes campaign exploiting SimpleHelp RMM software for initial access.** Arctic Wolf. *https://arcticwolf.com/resources/blog/arctic-wolf-observes-campaign-exploiting-simplehelp-rmm-software-for-initial-access/*

Tancio, B., Cureg, F., & Samaniego, J. (2025a, January 30). **Lumma Stealer's GitHub-Based delivery explored via managed detection and response.** Trend Micro. *https://www.trendmicro.com/en_us/research/25/a/lumma-stealers-github-based-delivery-via-mdr.html*

Lakshmanan, R. (2025, February 11). **Threat actors exploit ClickFix to deploy NetSupport RAT in latest cyber attacks.** The Hacker News. *https://thehackernews.com/2025/02/threat-actors-exploit-clickfix-to.html*

Arete

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

New Engagements
arete911@areteir.com

General Inquiries
marketing@areteir.com

www.areteir.com

Arete Advisors, LLC makes no claims, promises or guarantees about the accuracy, completeness, or adequacy of the contents of this report and expressly disclaims liability for errors and omissions in the content. Neither Arete Advisors, LLC, nor its employees and contractors make any warranty, express or implied or statutory, including but not limited to the warranties of non-infringement of third-party rights, title, and the warranties of merchantability and fitness for a particular purpose, with respect to content available from this report. Arete Advisors, LLC assumes no liability for any direct, indirect, or any other loss or damage of any kind for the accuracy, completely, or usefulness of any information, product, or process disclosed herein, and does not represent that the use of such information, product, or process would not infringe on privately owned rights. Information contained in this report is provided for educational purposes only and should not be considered as legal advice.