DECEMBER | 2025

Arete

CRIMEWARE REPORT

TRENDS AND HIGHLIGHTS FROM Q3 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 from July 1 to September 30, 2025—the third quarter (Q3) of 2025— including the most active threat groups, shifts in ransom demands and industries targeted, and commonly used malware and initial access methods.

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

The most notable shift during this period was an unprecedented surge in engagements attributed to Akira starting in mid-July. In August, the group was responsible for over half of all Arete engagements.

The Qilin and PLAY ransomware groups remained active throughout Q3, and Arete also observed an uptick in attacks from extortion-only groups, such as World Leaks and the Pure Extraction And Ransom (PEAR) Team, toward the end of the quarter.

Vulnerability exploitation was the most common attack vector in Q3, particularly the widespread exploitation of vulnerable SonicWall devices by groups such as Akira and Qilin, which significantly contributed to the surge in Akira activity. Threat actors also continued to evolve social engineering techniques, including SEO poisoning and malvertising campaigns that weaponized legitimate administrative utilities to gain initial access to enterprise environments.

Although threat actors remained largely opportunistic and did not target specific industries, the uptick in Akira engagements led to a shift in which sectors were most impacted by cyberattacks. Additionally, trends in ransom payments suggest that Akira's activity surge may have led the group to rush negotiations, ultimately resulting in fewer payments.

Statistics and Trends from Arete's Incident Response Engagements

Q1 2025

32

Total Named Threat Actors

6

Total Unnamed Threat Actors

Q2 2025

35

Total Named Threat Actors

9

Total Unnamed Threat Actors

Q3 2025

35

Total Named Threat Actors

16

Total Unnamed Threat Actors

TOP THREAT GROUPS BY QUARTER

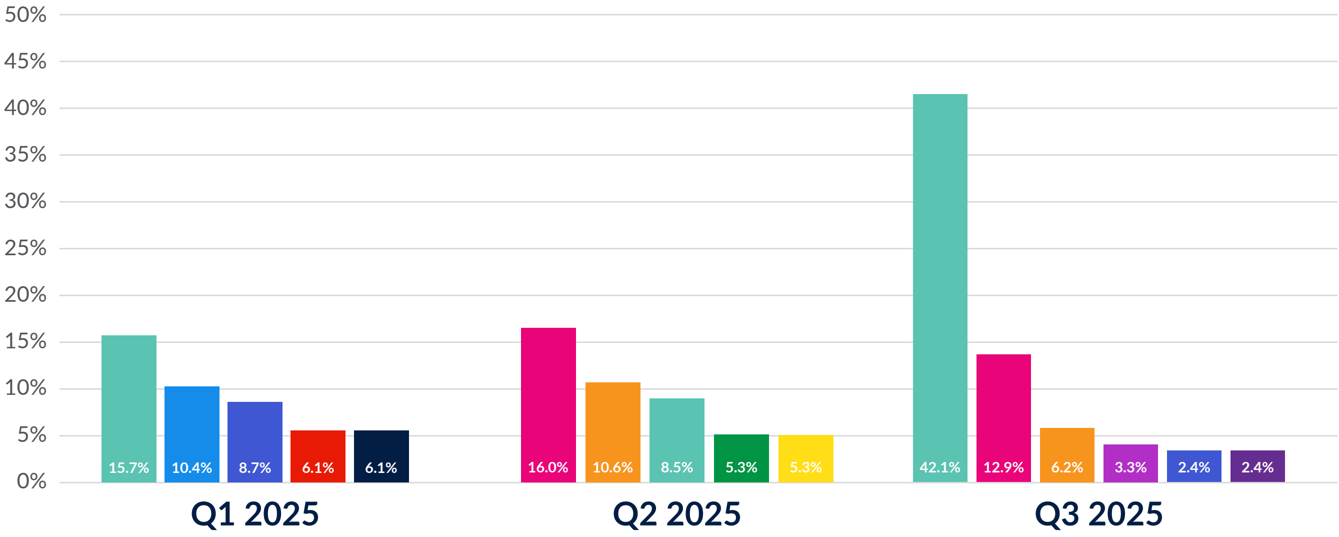


Figure 1

TOP THREAT GROUPS BY MONTH

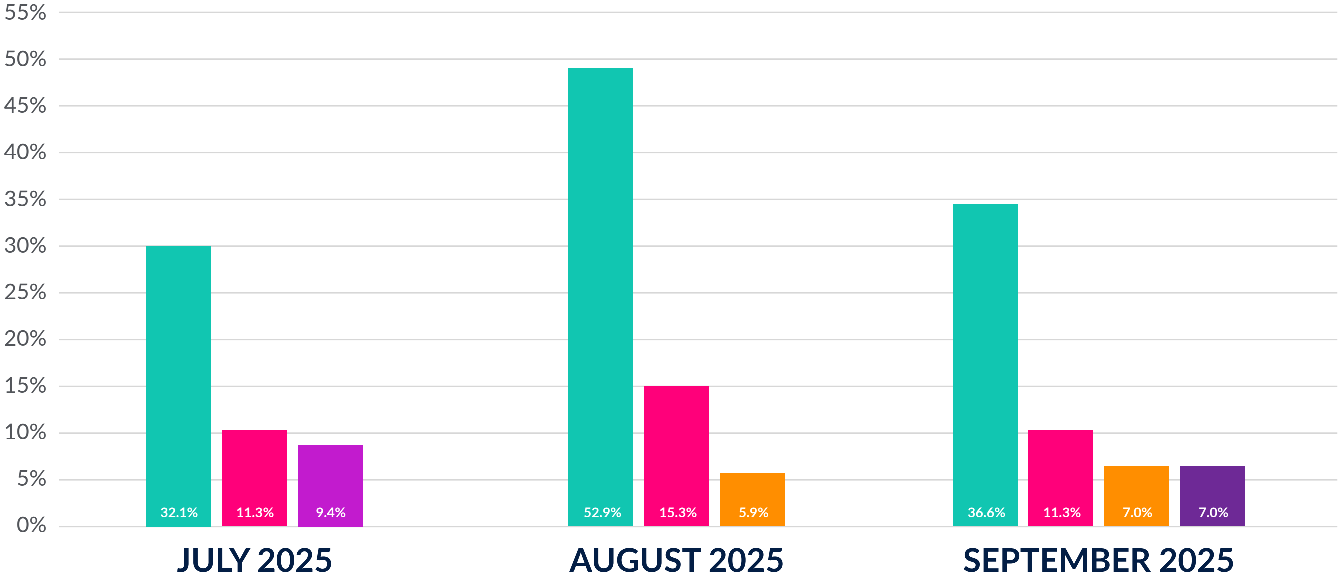


Figure 2

🟩 Akira	■ Luna Moth	🟦 RansomHub	🟦 INC Ransom
🟥 Cactus	■ Qilin	🟪 Sinobi Group	🟩 Interlock
🟪 World Leaks	🟧 PLAY	🟨 Lynx	

Arete observed an unprecedented spike in engagements attributed to Akira during the third quarter of 2025.

Arete observed an unprecedented spike in engagements attributed to Akira during the third quarter of 2025. The group has maintained consistent activity since it first appeared in 2023 and was the top ransomware group observed by Arete in 2024. However, in Q3, over 40% of all ransomware engagements were attributed to Akira, peaking in August with over 52% of incidents for that month. For comparison, Akira's previous peak was in Q4 2024, when it accounted for 18% of ransomware attacks. At the time, that was the highest quarterly activity from a single threat group observed by Arete since at least 2022. This recent spike was largely driven by the group exploiting vulnerable SonicWall devices, which will be covered in greater detail later in this report.

Qilin and PLAY also remained steadily active throughout the quarter, albeit at levels significantly lower than those of Akira. Since Q2 of this year, these three established groups have consistently remained the top threats. Qilin was the second most active threat group each month during Q3 and, like Akira, frequently exploited VPN vulnerabilities in both SonicWall and Fortinet devices.

Two emerging groups highlighted in our **H1 2025 Crimeware Report** were also among the top threat groups in Q3: the Sinobi Group and World Leaks. In July, the Sinobi Group was responsible for almost 10% of ransomware activity. Sinobi emerged this year and has multiple code and infrastructure overlaps with the Lynx ransomware group; however, Lynx continued to operate independently throughout Q3, and at this time, Sinobi does not appear to be an attempted rebrand. World Leaks, on the other hand, is a rebrand of the Hunters International ransomware group and was tied as the third most active threat group in September. Unlike Hunters International, World Leaks no longer deploys ransomware and now focuses solely on data exfiltration to extort its victims.

Scan QR code to access the
2025 H1 Crimeware Report

Highlights from the Threat Landscape

The Summer of Akira

Akira's surge in activity was primarily driven by the widespread exploitation of vulnerable SonicWall appliances, including activity tied to CVE-2024-40766, as well as brute-force attempts against exposed services, and the abuse of legacy service accounts whose credentials were left unchanged after firewall upgrades. These initial access vectors provided Akira operators with efficient and repeatable footholds, enabling them to compromise multiple organizations.

Hello SonicWall, My Old Friend

Beginning in mid-July 2025, security researchers observed a significant increase in incidents involving SonicWall SSL VPN endpoints, primarily affecting organizations with Gen 7 or recently migrated Gen 6 appliances. The key vulnerability exploited was CVE-2024-40766, an improper access control flaw in SonicWall SSL VPNs spanning multiple generations. Although it was patched in 2024, Akira continued to exploit the vulnerability in 2025, often in environments that appeared patched but retained latent weaknesses. Some reports also mentioned potential exploitation of SMA100-series vulnerabilities CVE-2025-40596 through CVE-2025-40599. Several affected organizations had fully updated their firmware, suggesting that the intrusions stemmed from credential reuse, misconfiguration, or migrated legacy accounts rather than unpatched code.

In early August 2025, SonicWall confirmed that the surge was not the result of a new zero-day vulnerability, but rather a re-exploitation of CVE-2024-40766, primarily affecting systems where legacy credentials remained after migration. During the Gen 6 to Gen 7 upgrade process, administrators who failed to reset or delete old service and privileged accounts inadvertently carried those credentials forward in configuration exports. These dormant accounts, some of which predated the 2024 fix, remained exploitable and were leveraged by Akira operators to authenticate through the VPN interface. Multiple organizations subsequently reported intrusions, configuration exfiltration, and ransomware deployment, with SonicWall's investigation confirming that attackers accessed customer backup files in some cases. Arete also tracked related client notifications of cloud backup compromise tied to the same campaign.

Akira Tools and Techniques

During Q3, Arete observed Akira repeatedly exploiting two Windows drivers in its recent campaign against SonicWall VPN users. The drivers, rwdrv.sys and hlpdrv.sys, were utilized as components of the Bring Your Own Vulnerable Driver (BYOVD) technique, in which Akira operators combined legitimate and malicious kernel-level drivers to disable Microsoft Defender and blunt endpoint detection and response (EDR) visibility. Akira further relied on legitimate remote administration utilities, including AnyDesk and TeamViewer, among others, to maintain access and stage exfiltration, demonstrating a consistent double-extortion model.

Akira's Q3 campaigns reflect a highly opportunistic yet technically capable operation, combining appliance-level exploitation, credential abuse, kernel-level evasion, and legitimate administrative tools to maximize impact. It is difficult to assess how long Akira will sustain this high volume of attacks. Although the group's activity started to decline since its peak in August, Akira remains the dominant threat group in Q4 thus far and will likely remain a top ransomware threat for the remainder of the year.

Extortion-Only Groups Emerge

Toward the end of Q3, there was a notable increase in activity from emerging extortion-only threat groups. Two relatively new extortion groups, World Leaks and the PEAR Team, were among the top five threat groups in September and collectively responsible for nearly 10% of the activity for the month.

Notably, the PEAR Team claimed exfiltration of several TB of data in each engagement, which is significantly more than what is typically observed. The group describes itself as a "community of highly responsible and strictly disciplined members... and have nothing common with any other threat actors."[1] Despite this claim, there are reportedly possible blockchain overlaps between the PEAR Team and the BianLian extortion group, the latter of which quietly ceased operations earlier this year. Although Arete has not observed any additional overlaps in infrastructure, the PEAR Team has been observed using similar pressure tactics, such as making repeated phone calls to their victims to pressure them into making payments.

A new threat actor known as the Genesis Group emerged in late September, also focusing on data theft rather than encryption. In Q4, Arete has already observed multiple incidents involving the Genesis Group, as well as activity from Luna Moth, which has been relatively quiet since Q1, suggesting a potential increase in extortion-only activity for the remainder of the year.

Two relatively new extortion groups, World Leaks and the PEAR Team, were among the top five threat groups in September and collectively responsible for nearly 10% of the activity for the month.

[1] https://www.ransomlook.io/group/pear

Notable Campaigns

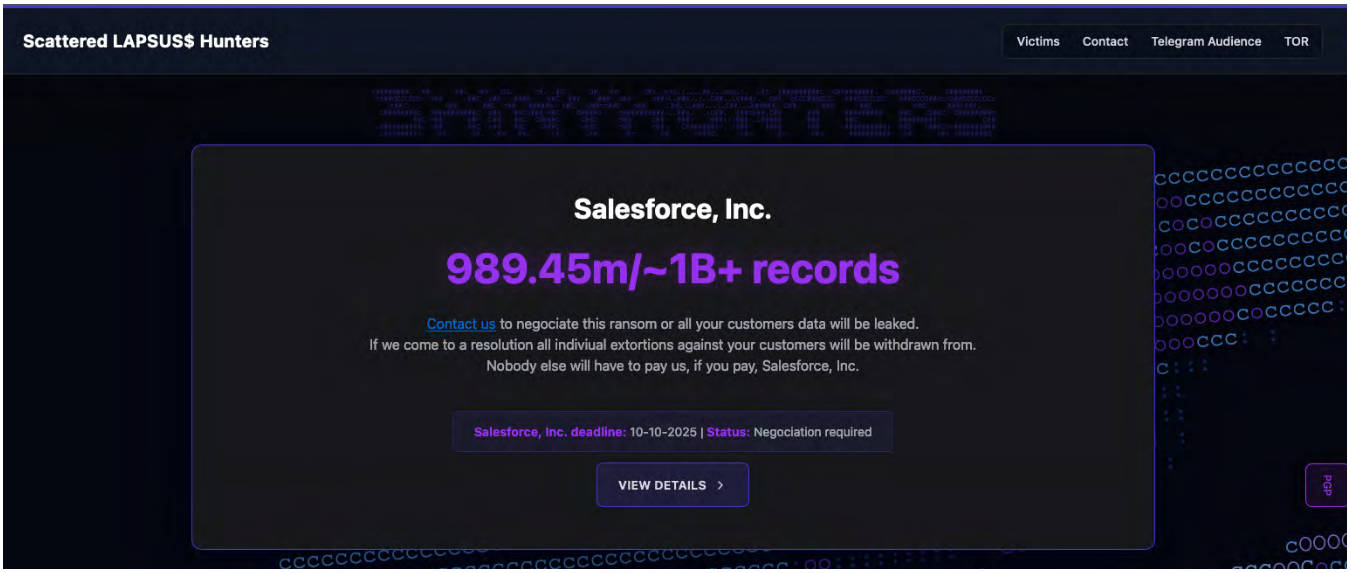
Salesforce Salesloft Drift

A widespread data theft campaign in August 2025 targeted SaaS platform Salesloft through its integration with the Drift AI chat agent. Threat actors stole OAuth and refresh tokens issued to Drift, granting persistent, MFA-bypassing access to connected customer Salesforce environments without generating authentication alerts, making the intrusion both scalable and difficult to detect.

Once authenticated via the Drift-issued tokens, threat actors pivoted through Salesloft into numerous Salesforce instances and performed broad API-level data extractions. The stolen data included customer records as well as sensitive cloud credentials such as AWS access keys, stored passwords, and Snowflake tokens. This activity aligns with that of Scattered Lapsus$ Hunters, a coalition of financially motivated actors known for exploiting SaaS trust relationships, over-permissioned OAuth integrations, and identity-centric techniques.

On August 20, 2025, Salesloft confirmed the Drift-related security issue and proactively revoked all Salesforce–Drift connections to contain the incident. However, stolen CRM data surfaced on the Scattered Lapsus$ Hunters extortion portal in early October, indicating that the stolen data is being weaponized for ongoing phishing, cloud compromise, and credential-based attacks.

This campaign highlights how linked SaaS platforms can amplify the impact of a single compromised integration, with abused OAuth tokens and broad API permissions enabling covert movement across platforms. It underscores the need for continuous monitoring of OAuth scopes, stricter third-party access controls, and better visibility into cross-SaaS data flows to limit the potential scope of compromise and minimize identity-based risk.



Salesforce, Inc.

989.45m/~1B+ records

Contact us to negociate this ransom or all your customers data will be leaked.
If we come to a resolution all indivual extortions against your customers will be withdrawn from.
Nobody else will have to pay us, if you pay, Salesforce, Inc.

Salesforce, Inc. deadline: 10-10-2025 | Status: Negociation required

Figure 3. Scattered Lapsus$ Hunters data leak site (Source: UpGuard)

Oracle E-Business Suite and the Return of Cl0p

The Cl0p ransomware group was relatively quiet this summer, with just one post per month to its data leak site (DLS) in June and July. However, those familiar with Cl0p's tactics and operational tempo likely took no solace in this lull, as they knew it meant Cl0p was hard at work laying the groundwork for its next campaign. After months of cultivating its operational environment and sowing access, it was time for the group to begin the age-old tradition of harvesting in autumn.

Cl0p began its harvest on September 29, 2025, when the group initiated a massive extortion email campaign targeting the executives of organizations it had infiltrated. The emails originated from a slew of compromised third-party accounts and claimed that a threat actor had breached their Oracle E-Business Suite (EBS) environment and exfiltrated sensitive data. Two weeks after Cl0p's barrage of emails, Arete observed the first update to the Cl0p DLS in months with the addition of Harvard University. Since then, dozens of victim organizations have been added to the DLS, including American Airlines, Schneider Electric, Louis Vuitton, and The Washington Post.

Oracle EBS is an integrated suite of business applications designed to manage core business processes, including finance, supply chain, manufacturing, human resources, and customer relationship management. Cl0p perpetuated the attack through a rather sophisticated chain of exploits targeting multiple vulnerabilities in EBS. Security researchers have noted that Cl0p leveraged at least five separate bugs to achieve its objective. This level of planning and technical acumen is what Arete has come to expect from Cl0p, as it remains one of the most successful ransomware groups operating today. At the time of this report, the activity is ongoing, and we expect to see many more postings to the Cl0p DLS related to these attacks.

Oracle released a patch for the vulnerability, tracked as CVE-2025-61882, on October 4, 2025, in a Security Alert Advisory. Enterprises using Oracle EBS versions 12.2.3-12.2.14 should follow patching guidelines immediately.

Initial Access Trends and Vulnerabilities Exploited

Emergence of FileFix as a Successor to ClickFix

During Q3, cybersecurity researchers identified FileFix as a sophisticated evolution of the previously observed ClickFix social engineering tactic. First observed in June 2025, FileFix introduced a more seamless and convincing method of user manipulation, relying on familiar Windows interactions to deliver malware. While ClickFix exploits the Windows Run dialog, FileFix targets the File Explorer address bar and browser file-input mechanisms, tricking victims into copying and pasting malicious clipboard content that executes locally. This shift made the technique more deceptive and compatible with modern browsers and OS environments, increasing its success rate across diverse user populations.

FileFix attacks combine cache smuggling and clipboard manipulation to covertly deliver malicious files. Using crafted web pages, attackers initiate a hidden file-input action that prompts Windows File Explorer to open. Simultaneously, JavaScript code places a preloaded PowerShell or CMD command on the clipboard, which the victim unknowingly pastes into the File Explorer address bar. Once executed, the script triggers a cached malicious payload, bypassing traditional security mechanisms. Observed payloads in these attacks include Interlock-style Remote Access Trojans (RATs), StealC information stealer, and other obfuscated loaders implemented through PowerShell, PHP, or Python.

FileFix introduced a more seamless and convincing method of user manipulation, relying on familiar Windows interactions to deliver malware.

By leveraging trusted OS features and user familiarity, attackers can execute malicious code without relying on traditional exploit chains or obvious phishing indicators. Throughout Q3 2025, security analysts observed FileFix's adoption among threat actors seeking stealthy initial access methods and enhanced evasion capabilities. This trend underscores the crucial need for security awareness training and defensive controls that focus on detecting anomalous user actions within local interfaces, as social engineering continues to evolve into a potent entry point for advanced malware campaigns.

SEO Hijacking and Malicious Ads for Legitimate Tools

Throughout Q3, cybersecurity researchers continued to observe a surge in SEO-poisoning and malvertising campaigns that weaponized legitimate administrative utilities to gain initial access into enterprise environments. Threat actors refined their techniques by manipulating search engine rankings and purchasing malicious advertisements to position trojanized installers of trusted tools, including PuTTY, WinSCP, FileZilla, and RV-Tools, at the top of search results. These lures were primarily aimed at IT administrators and system operators, a high-value demographic with privileged access to corporate infrastructure. When unsuspecting users downloaded and executed these fake installers, persistent backdoors and loaders such as Nitrogen or SMOKEDHAM were installed, often alongside the legitimate utility to avoid suspicion and maintain operational continuity.

Reported incidents revealed that threat actors distributed weaponized versions of legitimate administrative tools to gain initial access and deploy malware. In one case, a domain administrator downloaded a trojanized RV-Tools installer, which delivered the SMOKEDHAM PowerShell backdoor for remote access. The attacker then installed the Kickidler tool to record keystrokes and capture screenshots, enabling credential theft and lateral movement. Other campaigns used malicious domains such as puuty[.]org and file-zilla-projectt[.]org to host fake utilities containing the Nitrogen loader. Further analysis by security researchers connected these techniques to Rhysida ransomware operators and related intrusion sets that routinely abused legitimate remote-access and administrative tools, including PsExec, WinSCP, AnyDesk, and ProcDump, to evade detection and maintain persistence after compromise. This approach allowed adversaries to blend into normal administrative operations, evading detection and endpoint security controls.

Threat actors refined their techniques by manipulating search engine rankings and purchasing malicious advertisements to position trojanized installers of trusted tools at the top of search results.

MFA Bypass Methods

Multi-Factor Authentication (MFA) has long been a primary defense against account takeover. It incorporates at least two of the three pillars of identity verification (something you know, something you have, something you are) and substantially reduces the risk of unauthorized access. While MFA should be implemented wherever possible, it is not foolproof. Throughout Q3, cybercriminals continued to find ways to bypass MFA and accomplish account takeover. Three of the most common methods are:

MFA Fatigue / Prompt Bombing

One of the most common implementations of MFA involves sending a push notification to a user's smartphone to approve a login. MFA fatigue attacks seek to overwhelm the user to the point that they either approve the prompt to end the notifications or simply click approve by accident. Organizations can mitigate this threat by implementing a more complex approval system, such as requiring number matching instead of simply clicking "approve," or by limiting the number of login attempts allowed within a specified period.

Adversary-in-the-Middle (AiTM)

Similar to common phishing activity, cybercriminals conducting AiTM attacks seek to trick users into directing their traffic to adversary-controlled infrastructure. Unlike traditional phishing, where the user's final destination is the malicious site, the malicious infrastructure in AiTM acts as a conduit between the user and the legitimate site. The user authenticates to the legitimate site with both factors, and the adversary collects the resulting authentication cookie, then passes it back to the user to avoid suspicion. The adversary can now act as the user. As one unique session will now have two users in different locations, using different devices, this attack can be detected by monitoring for anomalous "impossible travel" activity.

Session Hijacking

In session hijacking, the threat actor bypasses the MFA process altogether by taking over an existing authenticated session. There are several variations of this tactic, but the attacker either employs infostealer malware, exploits a vulnerability, or otherwise leverages a weakness in implementation to obtain the unique session ID or authentication token. Because there are many ways an attacker can carry out session hijacking, there is no singular way to detect it. However, detections can be added for suspicious activity such as unusual login locations, several failed login attempts, sessions ending faster or remaining active for longer than normal, or sessions involving unrecognized browsers, OS versions, or hardware profiles to mitigate this attack vector.

Sector Impacts and Threat Actor Targeting

Continuing the trend that Arete has observed since at least 2024, Manufacturing and Professional, Scientific, & Technical Services remained the two most impacted sectors in Q3. While Manufacturing previously occupied the number two spot during the first half of the year, it was the most impacted sector during Q3. Akira and Qilin attacks were more equally distributed across sectors, but PLAY targeted Manufacturing organizations more than any other sector in Q3. Additionally, Luna Moth—one of the few active threat groups that tends to focus primarily on victims in the Professional, Scientific, & Technical Services sector—was quiet in Q3, resulting in fewer attacks in that sector compared to the first half of 2025.

Akira's impact was most noticeable in the Wholesale Trade sector, which saw an increase in percentage of engagements in Q3, of which Akira accounted for 72%. This is not to say that Akira was specifically targeting companies in the Wholesale Trade sector, but rather that the uncharacteristically high volume of Akira attacks in Q3 likely inflated the number of attacks for that sector during the quarter. This also appeared to be the case with the Administrative and Support and Waste Management and Remediation Services sector, which is not typically among the top five impacted sectors. However, Akira and Qilin, which combined were responsible for over half of all ransomware incidents for the quarter, perpetuated more attacks against organizations in this sector than they had in the first half of 2025.

MOST IMPACTED SECTORS

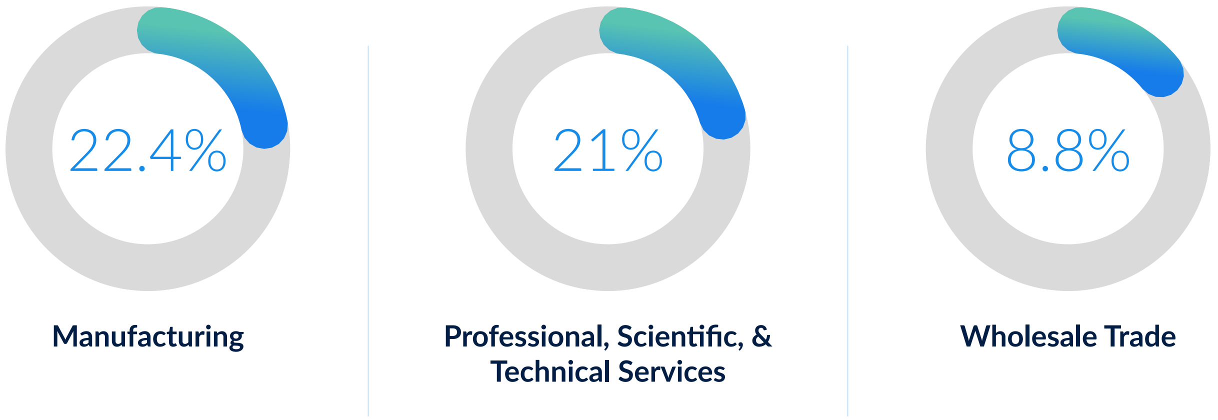


Figure 4. Top NAICS Sectors Impacted in Arete Engagements During Q3 2025

NAICS SECTOR NAME	PERCENTAGE OF ENGAGEMENTS
Manufacturing	22.4%
Professional, Scientific, & Technical Services	21.0%
Wholesale Trade	8.8%
Construction	6.8%
Administrative & Support & Waste Management & Remediation Services	6.3%
Healthcare & Social Assistance	6.3%
Finance & Insurance	4.4%
Information	3.4%
Real Estate, Rental & Leasing	3.4%
Retail Trade	3.4%
Transportation & Warehousing	3.4%
Public Administration	2.9%
Educational Services	2.0%
Management of Companies & Enterprises	1.5%
Other Services (except Public Administration)	1.5%
Uncategorized	1.5%
Accommodation & Food Services	0.5%
Arts, Entertainment, & Recreation	0.5%

Figure 5. Most impacted NAICS sectors in Q3 2025 (Source: Arete)

* *The North American Industry Classification System (NAICS) is the standard used by Federal agencies to classify US business organizations. The Cybersecurity and Infrastructure Security Agency (CISA) has their own separate classifications of critical infrastructure sectors.*

Trends in Ransom Demands and Payments

Throughout 2025, both the median ransom demand and median payment have steadily increased each quarter. However, the percentage of time a ransom is paid decreased each quarter. Only 29.8% of organizations paid a threat actor for restoration or data suppression in Q3.

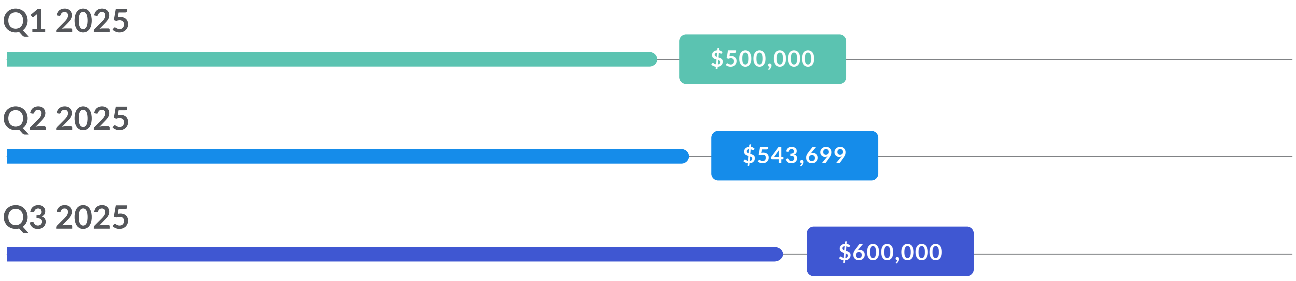
The increase in ransom demands in Q3 can partly be attributed to the surge in engagement attributed to Akira, whose median ransom demand was $750,000 for the quarter. Conversely, Akira was less successful in actually collecting ransom payments compared to other threat actors. In Q3, Akira collected ransom payments from less than 24% of its victims, compared to over 38% in the first half of 2025. During Q3, Arete observed behavioral changes in communications with Akira, as the group pushed for expedited negotiations, shortened deadlines, and demonstrated a reluctance to lower demands compared to prior negotiations, all of which indicated that the group may have targeted more victims than it could manage.

SECTORS	MEDIAN DEMAND	PERCENT OF TIME A RANSOM IS PAID
Manufacturing	$625,000	28.3%
Professional, Scientific, & Technical Services	$495,207	32.6%
Wholesale Trade	$750,000	27.8%

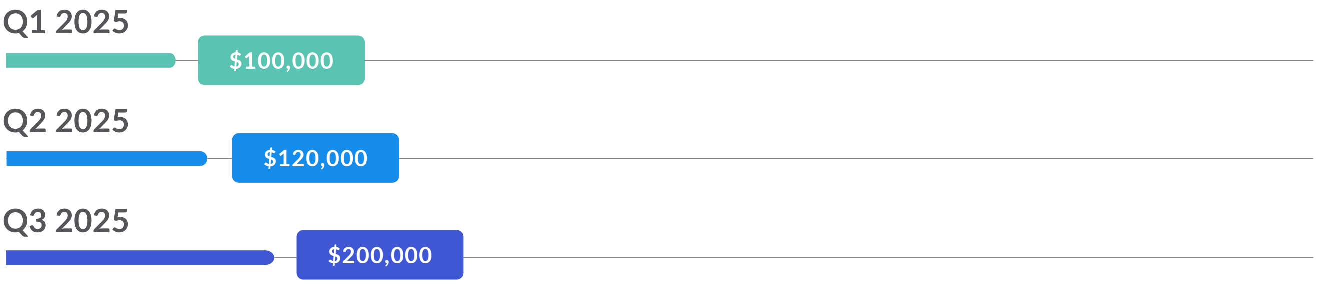
Figure 6. Ransom demands and payment percentages for top three sectors in Q3 (Source: Arete)

Examining the top three impacted sectors revealed no significant variation in median ransom demands or the percentage of time a ransom payment was made. As was the case in previous quarters, Manufacturing and Wholesale Trade organizations made payments less frequently than the average for all sectors; however, both sectors made payments more often in Q3 compared to the first half of the year. Notably, Akira was the only threat group that received ransom payments from Wholesale Trade organization in Arete engagements during Q3, suggesting that while Akira was less successful than other threat groups in extorting payments from victims overall, the group found more success with victims in this sector.

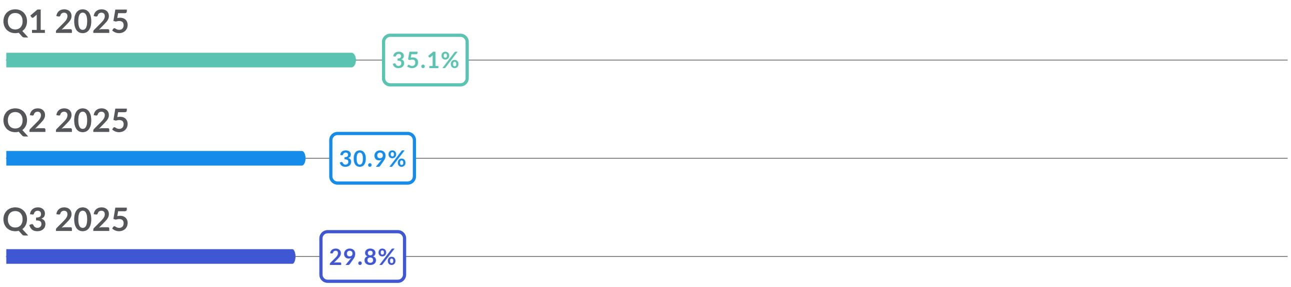
MEDIAN RANSOM DEMAND



MEDIAN RANSOM PAYMENT



PERCENTAGE OF TIME A RANSOM IS PAID



Only

29.8%

of organizations paid a threat actor for restoration or data suppression in Q3.

Outlook for the Remainder of 2025

Heading into Q4, it remains to be seen how long Akira can sustain the attack volume that Arete observed in Q3. Although the number of attacks attributed to Akira has decreased since its peak in August, the group was responsible for almost as many incidents in October as it was in September, and it is likely that Akira will remain the top ransomware threat for at least the remainder of 2025. As such, vulnerability exploits will also remain a prominent attack vector in Q4.

While a few established groups, such as Qilin and PLAY, will likely remain consistently active month-to-month, other previously active threat groups appear to be exercising more caution, either through rebranding, standing up affiliated subgroups, or simply going dark entirely. Social engineering attacks have also continued to evolve in sophistication and creativity and will remain a persistent threat for the remainder of the year.

On a positive note, after an increase in the percentage of organizations making ransom payments for recovery or data suppression in the first quarter of 2025, that number decreased in both Q2 and Q3. As observed in Q3, increased activity from groups like Akira was not correlated with successful extortion from victim organizations.

Arete continues to serve those impacted by cyberattacks, combining threat intelligence, end-to-end data, and compliance expertise to help organizations transform their response to cyber threats.

It is likely that Akira will remain the top ransomware threat for at least the remainder of 2025.

Vulnerability exploits will also remain a prominent attack vector in Q4.

Social engineering attacks have also continued to evolve in sophistication and creativity and will remain a persistent threat for the remainder of the year.

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 firsthand during our engagements with cybercriminals and may differ from trends observed by the greater cyber community.

Arete Internal Data

Arctic Wolf. (2025, July 31). Arctic Wolf observes July 2025 uptick in Akira ransomware activity targeting SonicWall SSL VPN. [Blog post]. Retrieved from *https://arcticwolf.com/resources/blog/arctic-wolf-observes-july-2025-uptick-in-akira-ransomware-activity-targeting-sonicwall-ssl-vpn/*

CrowdStrike. (n.d.). CrowdStrike identifies campaign targeting Oracle E-Business Suite zero-day CVE-2025-61882. [Blog post]. Retrieved from *https://www.crowdstrike.com/en-us/blog/crowdstrike-identifies-campaign-targeting-oracle-e-business-suite-zero-day-CVE-2025-61882/*

Cyberscoop. (2025, February 21). Oracle customers attacked using zero-day flaw linked to Clop ransomware gang, Google Mandiant finds. Retrieved from *https://cyberscoop.com/oracle-customers-attacks-clop-google-mandiant/*

Fortinet. (n.d.). Rhysida ransomware intrusion. [PDF Report]. Retrieved from *https://www.fortinet.com/content/dam/fortinet/assets/threat-reports/rhysida-ransomware-intrusion.pdf*

Google Cloud. (2025, February 21). Data theft targeting Salesforce instances via Salesloft and Drift. [Blog post]. Retrieved from *https://cloud.google.com/blog/topics/threat-intelligence/data-theft-salesforce-instances-via-salesloft-drift*

Google Cloud. (2025, March 18). Oracle E-Business Suite zero-day exploitation. [Blog post]. Retrieved from *https://cloud.google.com/blog/topics/threat-intelligence/oracle-ebusiness-suite-zero-day-exploitation*

GuidePoint Security. (2025, May 14). GRITRep: Akira Targeting SonicWall SSL VPNs. [Blog post]. Retrieved from *https://www.guidepointsecurity.com/blog/gritrep-akira-sonicwall*

NetManage IT. (2024, April). Report: Active Nitrogen campaign delivered via malicious ads for PuTTY & FileZilla. [PDF Report]. Retrieved from *https://blog.netmanageit.com/content/files/2024/04/Report-Active-Nitrogen-campaign-delivered-via-malicious-ads-for-PuTTY--FileZilla.pdf*

Talos Intelligence. (2024, November 7). State-of-the-Art Phishing: MFA Bypass. [Blog post]. Retrieved from *https://blog.talosintelligence.com/state-of-the-art-phishing-mfa-bypass/*

UpGuard. (2024, October 30). Salesforce Leak Extortion: Scattered Lapsus Hunters Targeting Salesforce Customers. [Blog post]. Retrieved from *https://www.upguard.com/blog/salesforce-leak-extortion-scatterered-lapsus-hunters*

Varonis. (n.d.). SEO poisoning: How to avoid falling victim. [Blog post]. Retrieved from *https://www.varonis.com/blog/seo-poisoning*

Vectra AI. (n.d.). MFA Bypass Attack: 3 Ways Attackers Beat Multi-Factor Authentication. [Webpage]. Retrieved from *https://www.vectra.ai/resources/mfa-bypass-attack*

RansomLook. (n.d.). Pear details. Retrieved from *https://www.ransomlook.io/group/pear*

USA & Canada

New Engagements arete911@areteir.com

Phone 646-907-9767

Cyber Emergency Helpline 866-210-0955

India

New Engagements arete112@areteir.com

Cyber Emergency Helpline 1800-890-7383

UK

New Engagements arete999@areteir.com

Cyber Emergency Helpline +44-800-208-8084

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.