SEPTEMBER | 2025

Arete

CRIMEWARE REPORT

TRENDS AND HIGHLIGHTS FROM H1 2025

Table of Contents

Overview

Ransomware and extortion activity in the first half (H1) of 2025 followed a relatively predictable pattern, with the majority of activity attributed to the same established threat groups that were the most active in the second half of 2024. Activity levels noticeably decreased in April and May, stemming from the RansomHub ransomware group going offline as well as various law enforcement activities against tools and infrastructure used by cybercriminals. However, ransomware activity picked back up again in June, largely driven by attacks from Qilin and Akira.

This report details the trends observed during Arete's response to ransomware and extortion attacks across industries from January 1 to June 30, 2025. Our unique dataset highlights key threat groups, tactics, and campaigns impacting insurance carriers, brokers, law firms, and insured organizations. Across the cyber incidents Arete responded to in the first half of this year, several notable trends emerged:

Shift in Key Threat Groups

RansomHub, the second-most active threat group in both the second half of 2024 and Q1 2025, unexpectedly went dark in early April. The Qilin ransomware group appeared to benefit the most from RansomHub's shutdown, emerging as the top threat group in the second quarter of the year.

Rebrands and Subgroups

Several threat groups were observed rebranding or forming subgroups, resulting in emerging groups like World Leaks, Sinobi Group, and Crux. Additionally, the DragonForce Ransomware-as-a-Service (RaaS) organization introduced a new decentralized "cartel" model, allowing affiliates to operate as their own brand while leveraging DragonForce's tools and infrastructure.

Compliance and Risk Alignment

Despite higher median ransom demands, median ransom payments decreased. This decline reflects rising regulatory pressures, improved recovery pathways without paying threat actors, and the importance of compliance-focused solutions.

Targeted Law Enforcement Efforts

Law enforcement activity in H1 focused on dismantling cybercriminal enablers and infrastructure, disrupting cybercriminals' ability to gather compromised credentials, share information on the dark web, and launder illicitly obtained funds.

Evolving Attack Methods

Vulnerability exploits, compromised credentials, and social engineering attacks were the most prominent attack vectors in H1. There was a notable increase in the sophistication of social engineering attacks, with the emergence of new techniques like ClickFix.

Arete's compliance-focused security solutions ensure that our partners and clients can not only understand the threat landscape, but also act decisively to mitigate cost and downtime, enhance compliance, and strengthen resilience.

Statistics and Trends from Arete's Incident Response Engagements

H1 2024

53
Total Named Threat Actors

24
Total Unnamed Threat Actors

H2 2024

50
Total Named Threat Actors

24
Total Unnamed Threat Actors

H1 2025

49
Total Named Threat Actors

15
Total Unnamed Threat Actors

Top Threat Groups by Half

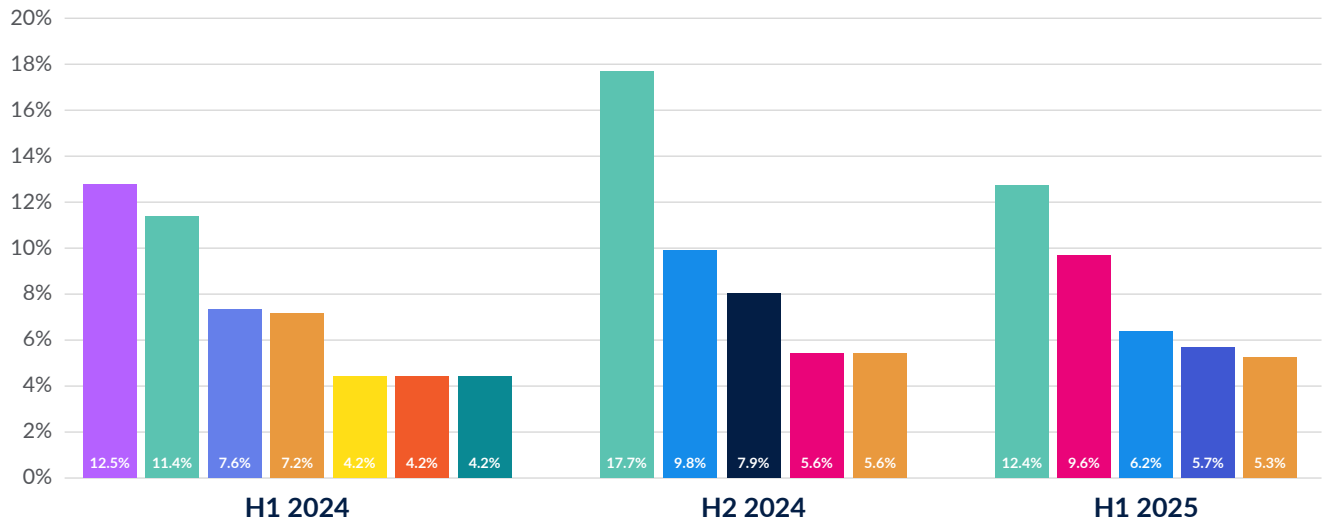


Figure 1

Top Threat Groups by Quarter

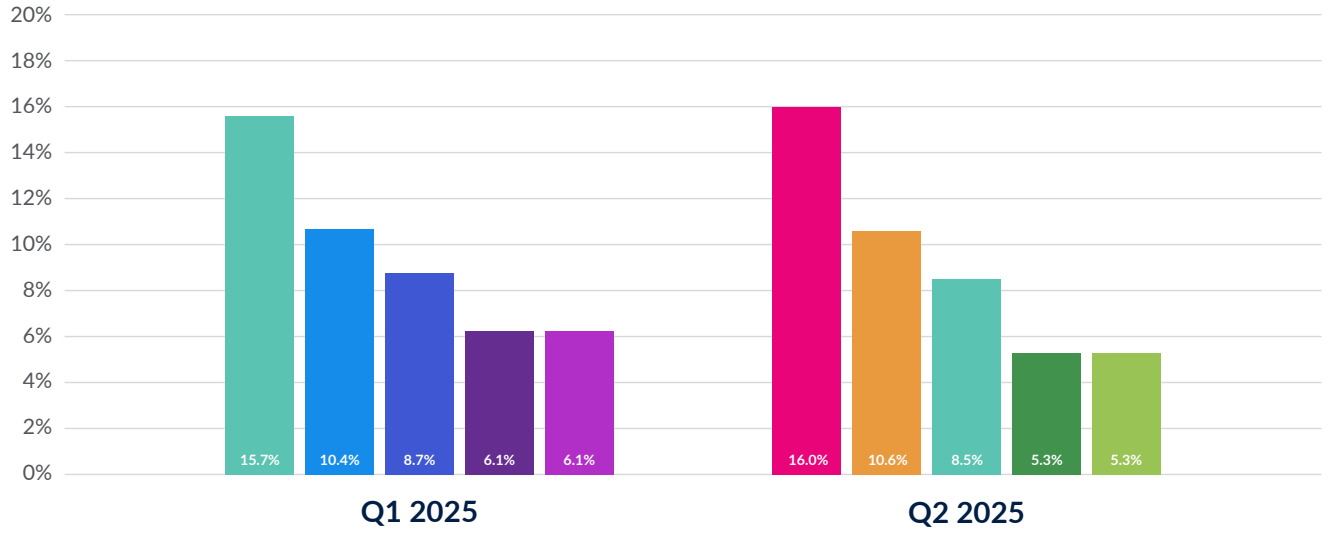


Figure 2

- Akira
- BlackSuit
- BianLian
- Cactus
- Fog
- Hunters International
- INC Ransom
- Interlock
- LockBit
- Luna Moth
- Lynx
- Medusa
- PLAY
- Qilin
- RansomHub

The first quarter of 2025 followed a relatively predictable pattern, similar to the end of 2024, with groups like Akira and RansomHub remaining among the most active threat groups. However, there was a distinct shift in the second quarter, as Akira had a lull in activity, particularly in May, when the group was responsible for less than 4% of all ransomware and extortion activity observed by Arete.

Akira wasn't the only group whose activity slowed in Q2. Arete observed a decrease in ransomware and extortion activity after March, and May saw the lowest number of engagements of any month thus far in 2025. Part of this decrease can be attributed to the absence of several established groups, the most notable of which was RansomHub, whose entire infrastructure, including its client chat portals and data leak site (DLS), abruptly went offline at the beginning of April. Additionally, BianLian—a previously active extortion group operating since 2022—was not observed in any engagements in Q2 and has not posted any new victims to its DLS since the end of March.

RansomHub Goes Offline

RansomHub launched in February 2024 and quickly emerged as a leading RaaS operation, attracting numerous threat actors by offering a cross-platform encryptor compatible with Windows, Linux, ESXi, FreeBSD, and ARM/Intel systems. Its affiliates adopted a variety of advanced tools and techniques in their campaigns, notably using Betruger malware and the Bring Your Own Vulnerable Driver (BYOVD) technique to disable endpoint security solutions.

However, on April 1, 2025, RansomHub's infrastructure abruptly went offline. Reports suggest that internal disagreements between RansomHub administrators and affiliates may have contributed to the shutdown, prompting affiliates to migrate to other RaaS platforms. Qilin, in particular, saw a significant surge in activity, nearly doubling its data leak volume after April. The group was only responsible for about 2% of ransomware activity in Q1 but emerged as the top threat group in Q2. Notably, most of its activity came in June, as the group exploited vulnerabilities in Fortinet's FortiGate appliances and reportedly attempted to recruit ex-RansomHub affiliates.

DragonForce also claimed that RansomHub would be migrating to its infrastructure. However, despite DragonForce's claims, there is no conclusive evidence to confirm that RansomHub merged or resumed operations under any other banner.

As of now, RansomHub remains offline with no signs of revival. Its future remains uncertain, with possibilities ranging from a rebranding or reintegration under another ransomware group to a complete shutdown of the brand. The abrupt halt of RansomHub underscores the volatility of the broader ransomware ecosystem, where internal conflicts, affiliate migrations, and rivalries can rapidly dismantle even highly successful operations.

Reports suggest that internal disagreements between RansomHub administrators and affiliates may have contributed to the shutdown, prompting affiliates to migrate to other RaaS platforms.

Threat Actor Insights

Top Threat Groups

Qilin

In 2025, Qilin emerged as one of the most prevalent and advanced ransomware operations in the current threat landscape. Throughout 2024, Qilin was linked to numerous high-impact intrusions, often leveraging known vulnerabilities to achieve initial access by bypassing authentication and executing remote code on unpatched systems. The group's operations proved highly lucrative, reportedly extorting over $50 million in ransom payments during 2024. Qilin's affiliate-driven RaaS model further distinguishes itself by offering "client-oriented" services, such as legal assistance through its "Call Lawyer" feature and enhanced extortion tactics, including a Distributed Denial-of-Service (DDoS) attack capability introduced in its April 2025 ransomware version. Qilin became noticeably more active in the second quarter of 2025, during which it was the most active threat group observed by Arete. This uptick can be attributed to several factors, including the exploitation of several vulnerabilities and the potential recruitment of ex-RansomHub affiliates.

Akira

Akira was the most active threat group observed by Arete in 2024 and started 2025 as the top threat in January and February after successfully targeting a critical SonicWall VPN access control flaw (CVE-2024-40766). Following a short hiatus in mid-2025, possibly due to staging for new attacks, Akira returned to its typical high activity levels in July and will likely remain a dominant threat in the second half of the year.

Play

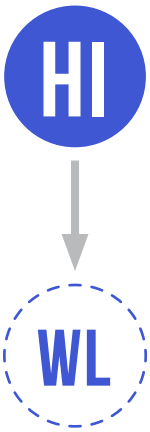
The Play ransomware group has been a persistent and active cybercriminal organization since at least 2022. While Play is not consistently the most active ransomware group each month, it was among the top five threat groups in the first half of 2025 and was the second-most active group in Q2, behind only Qilin. In 2025, Play continues to leverage SystemBC, a malware tool that functions as a proxy and a remote access trojan (RAT). This tool, as well as its ransomware payload, are often deployed in the Music directory of a victim's system. Play also continues to use harassing pressure tactics, including calls to the victim employees, and is quick to post the victim’s organization name and stolen data to its DLS.

INC Ransom

Reports from 2024 indicated that INC was considering selling its source code, and several similarities have since been observed between INC Ransom and the Lynx ransomware group. However, INC Ransom continues to operate in 2025 and had an uptick in activity in the first quarter of 2025. During that time, Arete observed INC Ransom exploiting vulnerabilities in the SimpleHelp Remote Monitoring and Management (RMM) software, and the group was responsible for almost as many incidents in Q1 2025 as in the entirety of 2024. In Q2, the group returned to lower activity levels and was observed in less than 2% of all engagements.

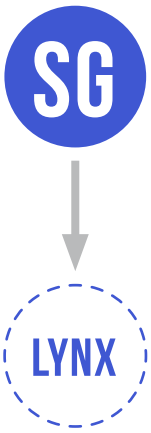
Rebrands & Subgroups Emerge in H1

Although established threat groups were responsible for much of the activity in H1, Arete also observed several possible rebrands and subgroups, including Hunters International rebranding as World Leaks, the emergence of the Sinobi Group, DragonForce's new "cartel" model, and a possible BlackByte subgroup calling itself Crux.



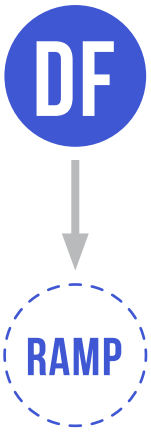
Hunters International Transitions to World Leaks

The Hunters International ransomware operation reportedly launched in October 2023. However, by late 2024, the group publicly announced its intent to cease ransomware operations and rebrand as World Leaks, citing increased risks and declining profitability driven by government crackdowns, global law enforcement actions, and heightened geopolitical pressures. Unlike its predecessor, World Leaks does not deploy ransomware and instead focuses solely on data exfiltration and blackmail. Affiliates are equipped with a custom-built exfiltration tool designed to automate large-scale data theft from victim networks, streamlining operations and eliminating reliance on encryption payloads. This shift underscores a shift within the cybercriminal ecosystem toward extortion-only attacks, reflecting an evolution in tactics aimed at reducing operational risk and evading heightened law enforcement scrutiny.



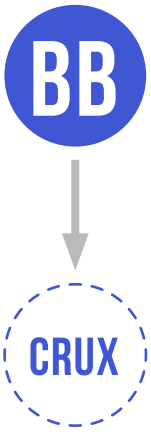
Sinobi Group & Lynx

The Sinobi Group emerged in 2025 and demonstrates multiple similarities with the Lynx ransomware group, including overlapping code, infrastructure, and an almost identical Tor chat and DLS. However, as Lynx continues to operate under its original name, it remains unclear whether Sinobi is a rebrand or a subgroup spawned from a sale or sharing of the Lynx encryptor or infrastructure. The group has also attempted to use a malicious driver file to bypass endpoint detection and response (EDR) tools, indicating the use of the Bring Your Own Vulnerable Driver (BYOVD) technique, a method used by multiple ransomware groups, including Lynx.



DragonForce Introduces a “Partners Program” and Co-Brands with RAMP

DragonForce—a RaaS operation that first surfaced in August 2023—announced a rebranding as the DragonForce Ransomware Cartel in March 2025, transitioning from a centralized RaaS structure to a decentralized partnership model. Under this new model, affiliates get access to DragonForce's tools and infrastructure but can operate under their own brands. In June, Arete observed a co-branded DragonForce and RAMP logo on a dark web forum, suggesting a close collaboration. RAMP, a prominent forum supporting cybercriminal activity, frequently hosts data leaks and discussions on exploits, further amplifying DragonForce's reach within the cybercrime ecosystem. These developments highlight DragonForce's growing influence and an innovative shift towards a partnership-like model built to attract affiliates seeking more autonomy from the traditional RaaS models.



Crux – A Possible BlackByte Subgroup

Crux ransomware emerged at the end of H1, claiming to be a subgroup of the BlackByte ransomware group. Crux's ransom notes follow a structured format consistent with previous BlackByte engagements, including incident details, assurances from the threat actor, and instructions for contact. The ransom notes also include a DLS link displaying the name 'BlackByte,' suggesting the possible reuse of legacy branding. Despite this claim, Arete notes that the last known BlackByte activity occurred in 2023, and it is currently unknown whether this new group is actually linked to the original BlackByte operation or is just using their name recognition.

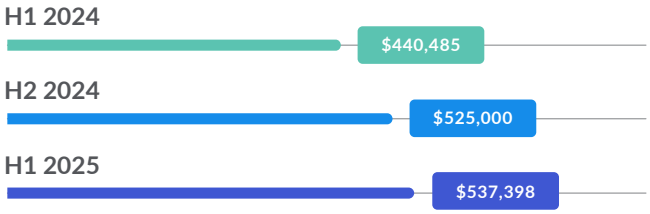
Trends in Ransom Demands and Payments

Although median ransom demands increased in the first half of 2025 compared to 2024, median payments decreased. This decrease can be partially attributed to the uptick in INC Ransom engagements in Q1 of this year, when it was the third-most active threat group. Organizations chose to make a payment in almost half of INC Ransom engagements, but the median payment was only $42,500.

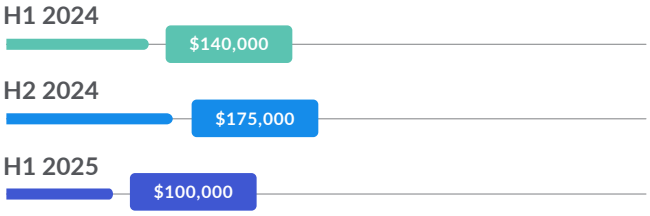
Additionally, the percentage of time a ransom was paid increased slightly in H1 of 2025 to 32.7%. This is consistent with the payment trends observed in Q1 of this year, as lower negotiated payment amounts could contribute to this increase in payment percentages

Despite the marginal increase in the percentage of time a ransom was paid, this figure remains relatively low, which is a positive indication of organizations' ability to recover from cyberattacks without needing to pay threat actors. Cybercriminals continue to come away empty-handed from ransomware and extortion attacks more than two-thirds of the time.

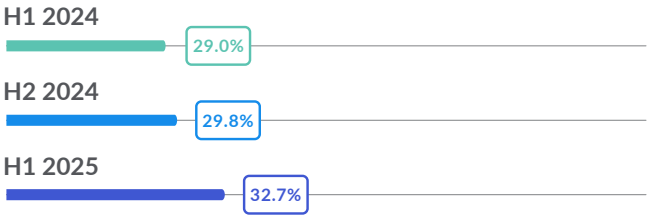
MEDIAN RANSOM DEMAND



MEDIAN RANSOM PAYMENT



PERCENTAGE OF TIME A RANSOM IS PAID



Although median ransom demands increased in the first half of 2025 compared to 2024, median payments decreased.

Sector Impacts and Threat Actor Targeting

NAICS SECTOR NAME	PERCENTAGE OF ENGAGEMENTS
Professional, Scientific, & Technical Services	20.2%
Manufacturing	14.4%
Healthcare & Social Assistance	8.7%
Construction	7.2%
Wholesale Trade	6.3%
Administrative & Support & Waste Management & Remediation Services	5.3%
Finance & Insurance	5.3%
Transportation & Warehousing	5.3%
Information	4.8%
Educational Services	3.8%
Retail Trade	3.8%
Other Services (except Public Administration)	3.4%
Public Administration	2.9%
Uncategorized	2.4%
Accommodation & Food Services	1.4%
Real Estate, Rental & Leasing	1.4%
Arts, Entertainment, & Recreation	1.0%
Management of Companies & Enterprises	1.0%
Agriculture, Forestry, Fishing & Hunting	0.5%
Mining, Quarrying, and Oil and Gas Extraction	0.5%
Utilities	0.5%

Figure 3. Most impacted NAICS sectors in H1 2025 (Source: Arete)

In 2025, threat actors remain largely opportunistic in which organizations they target, as opposed to focusing on specific industries. Professional, Scientific, & Technical Services and Manufacturing were the top two sectors impacted by ransomware and extortion attacks in the first half of 2025, consistent with the first quarter of the year. These were also the top two impacted sectors observed by Arete in 2024. The remaining top five sectors also remained unchanged from **Arete's Q1 2025 Crimeware Report.**

Arete has identified a few threat groups that typically conduct more targeted operations. The Luna Moth extortion group continues to primarily attack organizations in the Professional, Scientific, & Technical Services sector in 2025, specifically law firms, consistent with what Arete observed in previous years. Additionally, the Scattered Spider collective gained media visibility in the first half of 2025 for targeting well-known retail organizations in the UK and the US, before appearing to shift focus towards US insurance carriers.

In H1, Professional, Scientific, & Technical Services organizations saw the second-highest median ransom demand and made payments more frequently than the other four top sectors. This can be partially attributed to the sensitive nature of the data managed by these organizations as well as the risk of reputational damage. These organizations made a ransom payment in 38% of engagements in H1 2025, and half of these payments were for data suppression only.

Conversely, while Manufacturing was the second-most impacted sector, it remains the industry most often able to recover from cyberattacks without paying a ransom. In the first half of the year, only one in five Manufacturing organizations made a payment after a ransomware or extortion attack, which is almost 13% lower than all other sectors combined.

SECTORS	MEDIAN DEMAND	PERCENT OF TIME A RANSOM IS PAID
Professional, Scientific, & Technical Services	$700,000	38.1%
Manufacturing	$797,167	20.0%
Healthcare & Social Assistance	$443,355	27.8%
Construction	$282,500	26.7%
Wholesale Trade	$500,000	23.1%

Figure 4. Ransom demands and payment percentages for top five sectors (Source: Arete)

* *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) has its own separate classifications of critical infrastructure sectors.*

Law Enforcement Activity

Global law enforcement primarily targeted cybercriminal tools and infrastructure through coordinated actions in the first half of 2025. With the exception of international law enforcement's takedown of the 8Base ransomware group and the arrests of several of its members in February, there were no other high-profile takedowns of large RaaS organizations in H1. Instead, law enforcement agencies focused on dismantling cybercriminals' ability to steal data, share information, and launder illicit funds by targeting infrastructure and tools, significantly disrupting operations. As threat actors migrate to new tools, forums, and money laundering techniques, there are also increased opportunities for intelligence gathering and attribution as cybercriminals transfer their operations to new infrastructure.

Cracked and Nulled Marketplace Disruptions

In late January, the US Justice Department announced an international operation that led to the takedown of dark web marketplaces Cracked and Nulled. These forums were previously havens for cybercriminals seeking illicit information, including compromised passwords and stolen databases. Unfortunately, the disruption was largely temporary, as cybercriminals eventually migrated to new or existing dark web forums following the takedown.

Garantex Takedown

In early March 2025, the US Secret Service announced that it had seized web domains associated with the Russian crypto exchange Garantex, along with over $26 million in cryptocurrency assets, as a result of a coordinated effort with international law enforcement agencies. On the same day, the exchange announced on Telegram that it would be suspending its operations due to law enforcement's actions. According to TRM Labs, Garantex was responsible for 82% of all crypto volumes associated with sanctioned entities worldwide before the takedown, and the US Secret Service reported that Garantex has processed over $96 billion in cryptocurrency transactions since 2019.

Operation ENDGAME "Season 2"

In May, international law enforcement released an update on the latest phase of Operation ENDGAME, which resulted in the takedown of over 300 servers and 650 domains of new malware variants and groups that reemerged after law enforcement actions in 2024. These malware variants included Bumblebee, Lactrodectus, Qakbot, Hijackloader, DanaBot, Trickbot, and Warmcookie. In addition to the infrastructure takedowns, Europol reported that the latest phase of the operation resulted in arrest warrants against 20 individuals and the seizure of €3.5 million in cryptocurrency.

LummaStealer Takedown and Operation Secure

Also in May, the US Justice Department, in coordination with Microsoft, seized domains associated with the LummaC2 information stealer (LummaStealer), effectively disrupting the operation. LummaStealer previously made a name for itself as the most prominent information stealer available and was observed in numerous Arete engagements. This takedown significantly disrupted cybercriminals' abilities to obtain compromised credentials for initial access to victim environments. Following this action, law enforcement doubled down on disrupting information-stealing capabilities with Operation Secure. Led by Interpol from January to April 2025 and announced in June, this operation resulted in 32 arrests, data and server seizures, and the takedown of over 20,000 IPs and domains linked to malicious information stealers, including Lumma, RisePro, and MetaStealer. With participating agencies from 26 countries, Operation Secure was one of the largest coordinated law enforcement actions against cybercrime to date.

Law enforcement agencies focused on dismantling cybercriminals' ability to steal data, share information, and launder illicit funds by targeting infrastructure and tools, significantly disrupting operations.

Initial Access and Malware Trends

Vulnerability exploits, compromised credentials, and social engineering attacks were the most prominent attack vectors in H1 2025. As in previous years, software vulnerabilities remained a primary target for cybercriminals, with a focus on perimeter devices, including VPNs and firewalls.

Notable vulnerability exploits observed in H1 2025 include:

SimpleHelp

Several vulnerabilities in SimpleHelp remote support software versions 5.5.7 and earlier (CVE-2024-57726, CVE-2024-57727, and CVE-2024-57728) allowed for unauthenticated path traversal, remote code execution, and privilege escalation. Multiple threat groups exploited these vulnerabilities, including INC Ransom, whose uptick in activity during Q1 was partly attributed to this exploit.

SonicWall

Threat actors frequently exploited a SonicWall VPN access control flaw (CVE-2024-40766) first detected in Q4 2024. Although this vulnerability was primarily exploited in January and February, a recent Akira campaign in Q3 2025 attacking SonicWall devices is being attributed to this same vulnerability, according to statements from SonicWall.

Fortinet

In June 2025, threat actors—most notably the Qilin ransomware group—actively exploited two Fortinet vulnerabilities (CVE-2024-55591 and CVE-2024-21762) to bypass authentication and execute remote code on vulnerable FortiGate devices. This likely contributed to the uptick in Qilin attacks in June, when the group was responsible for over 26% of all ransomware and extortion attacks observed by Arete.

Social engineering attacks were also prevalent in the first half of 2025, with several campaigns demonstrating increased sophistication. One of the more prolific tactics observed involved threat actors using Microsoft Teams to gain initial access by flooding a victim's inbox with thousands of non-malicious emails and then posing as the victim organization's IT help desk on Microsoft Teams to convince the user to install a remote desktop support tool.

Another new social engineering technique known as ClickFix emerged in 2025. In this technique, a threat actor mimics a legitimate IT tool or process—such as pushing out a fake software security update prompt—that features a fake CAPTCHA challenge.

Once a user clicks the fake CAPTCHA, a malicious PowerShell script is automatically copied to their clipboard, along with additional instructions that trick the user into pasting the script and executing the malware, eventually granting the attacker unauthorized access to the network.

Multiple threat groups, including Interlock, Qilin, and Akira, were observed using this technique in the first quarter of the year. Since then, variations of ClickFix have emerged. Interlock has been observed using a variation dubbed FileFix to deploy a RAT. FileFix works much like ClickFix, except threat actors use Windows tools like File Explorer to trick users into executing the malicious PowerShell scripts. Another recent variation called PromptFix uses hidden text to prompt AI agents to trick users into running malicious scripts.

These initial access methods underscore the need for heightened user awareness and stronger endpoint defenses. Despite ongoing exploitation by ransomware groups, many organizations do not regularly update or patch their VPN devices and software, leaving them vulnerable to known flaws. A centralized patch management system can help ensure timely and consistent software updates, and periodic vulnerability scans are another way to proactively identify security vulnerabilities before they can be exploited by cybercriminals. On the human side, the primary way to minimize the risk of social engineering attacks is through employee awareness and training. Threat actors are continuously trying to find ways to make their social engineering attacks appear credible and legitimate and will likely continue to evolve and refine these tactics in the second half of the year.

Common Tools and Persistent Malware Strains Observed in H1 2025

Throughout 2025, Arete has analyzed malware families that combine persistence, stealth, and modular functionality to evade defenses. Threat actors are not only leveraging well-established tools but also adapting their delivery methods and expanding platform support to maximize impact. In the first half of 2025, PureLog Stealer, NetSupport RAT, AsyncRAT, and SystemBC stood out as the most persistent malware strains.

PureLog Stealer

PureLog Stealer is a .NET-based information-stealing tool and part of the Pure family of malware. In early 2025, security researchers observed a fourfold increase in phishing campaigns deploying PureLog as part of the attack chain, highlighting the tool's continued role in large-scale infostealer operations.

NetSupport RAT

The NetSupport RAT is an abuse of the legitimate NetSupport Manager remote administration tool, which allows it to blend into enterprise environments and evade suspicion. Once installed, it gives attackers complete remote control of a compromised system, including screen viewing, file transfers, remote execution, registry edits, and command execution. In early 2025, attackers increasingly used the ClickFix social engineering technique to deliver the NetSupport RAT through phishing and compromised websites. In mid-2025, new campaigns used fake GitCode and DocuSign pages, combining clipboard poisoning with multi-stage PowerShell payloads to install the RAT.

AsyncRAT

AsyncRAT is a free, open-source remote access trojan widely abused by threat actors for command and control. In 2025, phishing campaigns began using Cloudflare quick tunnels and layered payload chains, including Dropbox links, internet shortcuts, and script-based loaders to deliver AsyncRAT while avoiding detection. By mid-2025, more than 30 active AsyncRAT variants were observed in circulation, including forks like DcRat and VenomRAT, demonstrating continued evolution and widespread use.

SystemBC

SystemBC is a multifunctional malware that can connect to command-and-control servers and download and execute malicious payloads. This year, analysts observed a new SystemBC variant targeting Linux systems, expanding its reach beyond Windows environments. This variant remains stealthy, using encrypted channels for command-and-control communication and enabling attackers to span Windows and Linux systems within a network. Its role in facilitating lateral movement and blending malicious traffic across different platforms underscores its growing threat to enterprise environments.

Cybercriminals also frequently leverage legitimate software used by corporate IT departments to evade security measures and stay undetected in victim environments. During the first half of 2025, Arete observed threat actors abusing many of the same tools and applications as in previous years to gain remote access, conduct network discovery, navigate laterally through compromised networks, and exfiltrate sensitive data from victim systems.

Threat actors continued to leverage remote monitoring and management (RMM) tools extensively in 2025, most frequently AnyDesk, Atera, MeshAgent, ScreenConnect, SimpleHelp, Splashtop, and TeamViewer. RMM software also remains susceptible to vulnerabilities that can be exploited by threat actors, such as the SimpleHelp vulnerability discussed earlier in this report.

Other legitimate tools commonly abused by threat actors in cyberattacks included Advanced IP Scanner for network reconnaissance and discovery, command-line tools like PowerShell and PsExec to execute processes and commands, and programs like FileZilla, WinSCP, and MegaSync to transfer and store stolen data.

The most effective way to defend against cybercriminals' abuse of legitimate tools is to identify which applications are allowed in an environment and 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.

Defending Against the Most Observed Threat Groups

Arete integrates MITRE ATT&CK® as a core element of its threat detection, analysis, and response processes. By aligning identified adversary behaviors to ATT&CK techniques, Arete delivers a structured, intelligence-led approach to understanding attacker methodologies and prioritizing defense measures.

In H1 2025, Arete observed a marked increase in file-based techniques leveraging reconnaissance, evasion, and persistence to advance attacks while remaining undetected. Techniques such as **System Information Discovery (T1082)** and **Security Software Discovery (T1518.001)** were frequently used to profile victim environments and assess security controls, followed by **Process Injection (T1055)** and **DLL Side-Loading (T1574.001)** to stealthily execute malicious code within legitimate processes.

Defensive bypass was a recurring theme, with adversaries employing **Obfuscated Files or Information (T1027)**, **Software Packing (T1027.002),** and **Virtualization/Sandbox Evasion (T1497)** to circumvent detection and automated analysis. Data theft campaigns commonly utilized **Archive Collected Data (T1560)** and **Encrypted Channels (T1573)** to compress and securely transmit stolen information.

Reconnaissance activity was also prevalent, with techniques like **File and Directory Discovery (T1083), Process Discovery (T1057),** and **Remote System Discovery (T1018)** supporting lateral movement and targeted data collection. Concurrently, adversaries deployed **Masquerading (T1036), Input Capture (T1056),** and **Application Window Discovery (T1010)** in credential theft efforts, while attempts to **Impair Defenses (T1562.001)** and leverage **Command and Scripting Interpreter (T1059)** further highlighted a focus on persistence and automation.

These observed behaviors, coupled with stealth-driven tactics like **Deobfuscate/Decode Files or Information (T1140)** and **System Time Discovery (T1124),** underscore the evolving sophistication of adversaries in H1 2025. This evolution reinforces the necessity of a layered security approach to proactively disrupt malicious activity and strengthen organizational resilience.

Arete emphasizes a layered defense strategy aligned with the MITRE ATT&CK mitigations to counter the adversary behaviors observed in H1 2025. **Behavior Prevention on Endpoints (M1040)** remains a critical control, leveraging advanced EDR solutions to detect and block malicious actions in real time. Complementing this, **Audit-Focused Monitoring (M1047)** enabled detailed visibility into system and network activities, aiding early detection of anomalous behaviors.

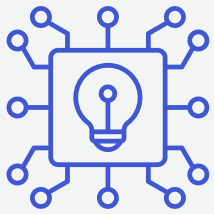
Traditional protections like **Antivirus and Antimalware (M1049)** continued to play a vital role, particularly when integrated with behavioral analytics to counter modern malware strains. Strengthening identity protections through **Privileged Account Management (M1026)** and **User Account Management (M1018)** proved

effective in reducing lateral movement opportunities and credential abuse, while **User Training (M1017)** addressed the persistent risk of social engineering and phishing-driven initial access.

On the network front, **Intrusion Prevention Systems (M1031)**, coupled with **SSL/TLS Inspection (M1020)** and **Network Traffic Filtering (M1037)**, were key in disrupting encrypted C2 channels and unauthorized exfiltration attempts. Additionally, enforcing **Execution Prevention (M1038)** and **Code Signing (M1045)** policies helped block unauthorized scripts and ensure the integrity of executable files.

Mitigations focused on access controls, such as **Restricting File and Directory Permissions (M1022)** and **Limiting Software Installation (M1033)**, further reduced attack surfaces, while **Disabling Unnecessary Features or Programs (M1042)** curtailed exploitable functionalities. Similarly, **Restricting Web-Based Content (M1021)** limited exposure to malicious domains and drive-by downloads.

Collectively, these controls reinforce Arete's defense-in-depth approach, combining proactive endpoint measures, rigorous network security, identity management, and user awareness to counter evolving adversary tradecraft observed in H1 2025.



By mapping observed techniques from H1 2025 to the MITRE ATT&CK framework, Arete aligns the evolving tactics of ransomware groups with targeted defensive strategies, operationalizing this intelligence into actionable mitigations that help organizations strengthen their security posture against real-world threats.

Outlook for H2 2025

Arete's 2025 Q1 Crimeware Report predicted that the threat landscape was likely to change in Q2, and it did. Ransomware and extortion activity levels dropped off in April and May, RansomHub appears to have permanently shut down its operation, and several rebrands and subgroups emerged in the latter half of H1.

Continued pressure from international law enforcement against cybercriminal infrastructure and tools had a disruptive effect on the cyber threat ecosystem. The trends observed in ransom demands and payments remained positive, and although payments have been made slightly more often than in 2024, the median payment decreased despite higher median initial ransom demands compared to 2024.

Trends in initial access and the tools and malware used by threat actors remained consistent throughout H1, and Arete anticipates vulnerability exploits will remain the top initial access vector in the second half of the year. With regards to the broader threat landscape, Arete's observations suggest that the second half of 2025 will see a marked increase in ransomware and extortion events after the lull in Q2, particularly from Akira and Qilin. This trend is appearing in Q3, with Akira aggressively targeting organizations using SonicWall products.

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.

The second half of 2025 will see an increase in ransomware and extortion events, particularly from Akira and Qilin.

Arete anticipates vulnerability exploits will remain the top initial access vector in the second half of the year.

Although payments have been made slightly more often than in 2024, the median payment decreased despite higher median initial ransom demands compared to 2024.

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 that 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.

Scan QR code to access the
2024 Annual Crimeware Report

Arete Internal Data

Check Point Research. (2025, July 31). **The state of ransomware – Q2 2025.**
https://research.checkpoint.com/2025/the-state-of-ransomware-q2-2025/

Group profiles
https://www.ransomlook.io/groups

Group-IB. (2025, April 30). **Ransomware debris: An analysis of the RansomHub operation.**
https://www.group-ib.com/blog/ransomware-debris/

Shread, P. (2025, April 2). **DragonForce claims to be taking over RansomHub.** The Cyber Express.
https://thecyberexpress.com/dragonforce-claims-to-be-taking-over-ransomhub/

Trend Micro. (2024, August 22). **How Trend Micro managed detection and response pressed pause on a Play ransomware attack.**
https://www.trendmicro.com/en_us/research/24/h/pressing-pause-on-play-ransomware.html

Cluley, G. (2025, June 20). **Qilin offers "Call a lawyer" button for affiliates attempting to extort ransoms from victims who won't pay.** Forta.
https://www.tripwire.com/state-of-security/qilin-offers-call-lawyer-button-affiliates-attempting-extort-ransoms-victims

Tactics, A. (n.d.). **Getting to the crux (Ransomware) of the matter.** Huntress.
https://www.huntress.com/blog/crux-ransomware

Group-IB. (2025, April 2). **The beginning of the end: The story of Hunters International.**
https://www.group-ib.com/blog/hunters-international-ransomware-group/

Ilascu, I. (2025, June 17). **Hackers switch to targeting U.S. insurance companies.** BleepingComputer.
https://www.bleepingcomputer.com/news/security/google-warns-scattered-spider-hackers-now-target-us-insurance-companies/

INTERPOL. (n.d.). **20,000 malicious IPs and domains taken down in INTERPOL infostealer crackdown.**
https://www.interpol.int/en/News-and-Events/News/2025/20-000-malicious-IPs-and-domains-taken-down-in-INTERPOL-infostealer-crackdown

U.S. Department of Justice. (2025, April 25). **Cracked and nulled marketplaces disrupted in international cyber operation.**
https://www.justice.gov/opa/pr/cracked-and-nulled-marketplaces-disrupted-international-cyber-operation

Arghire, I. (2025, February 11). **Authorities disrupt 8Base ransomware, arrest four Russian operators.** SecurityWeek.
https://www.securityweek.com/authorities-disrupt-8base-ransomware-arrest-four-russian-operators/

Owda, A. (2025, January 30). **Operation Talent: FBI takes down Cracked.io and Nulled.to in global cybercrime crackdown.** SOCRadar® Cyber Intelligence Inc.
https://socradar.io/operation-talent-fbi-takes-down-cracked-io-nulled-to/

U.S. Department of Justice. (2025, June 23). **Justice Department seizes domains behind major information-stealing malware operation.**
https://www.justice.gov/opa/pr/justice-department-seizes-domains-behind-major-information-stealing-malware-operation

TRM Labs. (2025, April 28). **Grinex emerges as likely Garantex rebrand.**
https://www.trmlabs.com/resources/blog/grinex-emerges-as-likely-garantex-rebrand

U.S. Secret Service Media Relations. (2025, April 7). **U.S. Secret Service seizes Russian cryptocurrency exchange websites.**
https://www.secretservice.gov/newsroom/releases/2025/03/us-secret-service-seizes-russian-cryptocurrency-exchange-websites

Operation Endgame. (n.d.). **Operation Endgame.**
https://www.operation-endgame.com/

Lumen Technologies. (2025, June 26). **Inside DanaBot's infrastructure: In support of Operation Endgame II.** Lumen Blog.
https://blog.centurylink.com/inside-danabots-infrastructure-in-support-of-operation-endgame-ii/?utm_source=rss&utm_medium=rss&utm_campaign=inside-danabots-infrastructure-in-support-of-operation-endgame-ii

The DFIR Report. (2025, July 14). **KongTuke FileFix leads to new Interlock RAT variant.**
https://thedfirreport.com/2025/07/14/kongtuke-filefix-leads-to-new-interlock-rat-variant/

Muncaster, P. (2025, September 15). **"PromptFix" attacks could supercharge Agentic AI threats.** Infosecurity Magazine.
https://www.infosecurity-magazine.com/news/promptfix-attacks-supercharge/

Arete

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

New Engagements
arete911@areteir.com

General Inquiries
marketing@areteir.com

www.areteir.com