Quorum Cyber

Global Cyber Risk Outlook Report

2025 Mid-Year Review

Leadership Foreword

At Quorum Cyber, we believe effective defence starts with deep, continuous visibility into the evolving threat landscape. In our role at the intersection of intelligence, incident response, and counter extortion, we are uniquely positioned to observe how threat actors operate, adapt, and increasingly collaborate to amplify their impact. This report, Relentless Threats: 2025 Mid-Year Global Cyber Risk Outlook, reflects the insight derived from our front-line engagements and strategic monitoring over the first half of the year.

What we've seen in H1 2025 is both striking and sobering. The sheer volume of new entrants, more than 70 new threat groups and Malware-as-a-Service offerings, highlights the unyielding pace of cybercriminal innovation. These aren't isolated developments. They reflect a broader trend of professionalisation in the cybercrime ecosystem, where affiliate models, franchising, and white-label services now mirror legitimate enterprise software operations.

Key developments covered in this report include the emergence of ransomware groups like Codefinger, which exploited legitimate AWS features to encrypt cloud storage — marking a concerning pivot toward targeting cloud-native infrastructure. We've also tracked the rise of Acreed, a new stealware variant that surged after law enforcement takedowns, underscoring the resilience of the underground marketplace. And perhaps most notably, we observed a convergence of state and criminal capabilities, with North Korea's Moonstone Sleet deploying a Russian-language Ransomware-as-a-Service platform in attacks against software firms.

Each of these stories reflects a broader truth: the threat landscape is no longer just a battleground of malware and exploits, but a dynamic ecosystem driven by service models, reputational economies, and competitive pressures. Groups like Qilin and DragonForce are pushing the boundaries of extortion — offering legal harassment services, AI negotiation bots, and call centres to maximise pressure on victims. We are witnessing the rise of 'quadruple extortion' as the next phase of ransomware operations.

As we move into the latter half of 2025, we anticipate further innovation in social engineering, extortion tactics, and cloud abuse. We also expect greater regulatory and legal entanglements as the lines between sanctioned actors and criminal affiliates blur. This report offers practical recommendations to build resilience in the face of those trends, grounded in what we are seeing right now across our incident response, intelligence, and counter extortion functions.

The threats are relentless — and so are we. Our mission is to help you anticipate, understand, and outpace the adversaries you face. We hope this report informs and empowers your defences in the months ahead.

Paul Caiazzo
Chief Threat Officer, Quorum Cyber

Table of Contents

Click # to jump to page

Executive Summary 05

January 08

- Monthly Summary 09
- Codefinger 10
  - Overview 10
  - Background and Identity 10
  - Operations 10
  - Assessment 11

February 12

- Monthly Summary 13
- Acreed 14
  - Overview 14
  - Background and Identity 14
  - Operations 15
  - Assessment 15

March 16

- Monthly Summary 17
- Qilin and Moonstone Sleet Cooperation 18
  - Overview 18
  - Background and Identity 18
  - Operations 19
  - Assessment 19
  - Sanctions and Complications 19

April 20

- Monthly Summary 21
- DragonForce/RansomHub 22
  - Overview 22
  - Background and Identity 23
  - Operations 23
  - Assessment 24

May 25

- Monthly Summary 26

RansomBay 27
Overview 27
Background and Identity 27
Operations 28
Assessment 28

June 30

Monthly Summary 31
GLOBAL Ransomware 32
Overview 32
Background and Identity 32
Operations 32
Assessment 33
Qilin Services Development 34
Overview 34
Background and Identity 34
Operations 35
Assessment 36

Financial Impact Trend 37

Sector Consideration 38

Quorum Cyber's Threat Intelligence 39

Reccomendations 40

Ransomware 40
Stealware 41

About Quorum Cyber 42

Global Cyber Risk Outlook Report 42

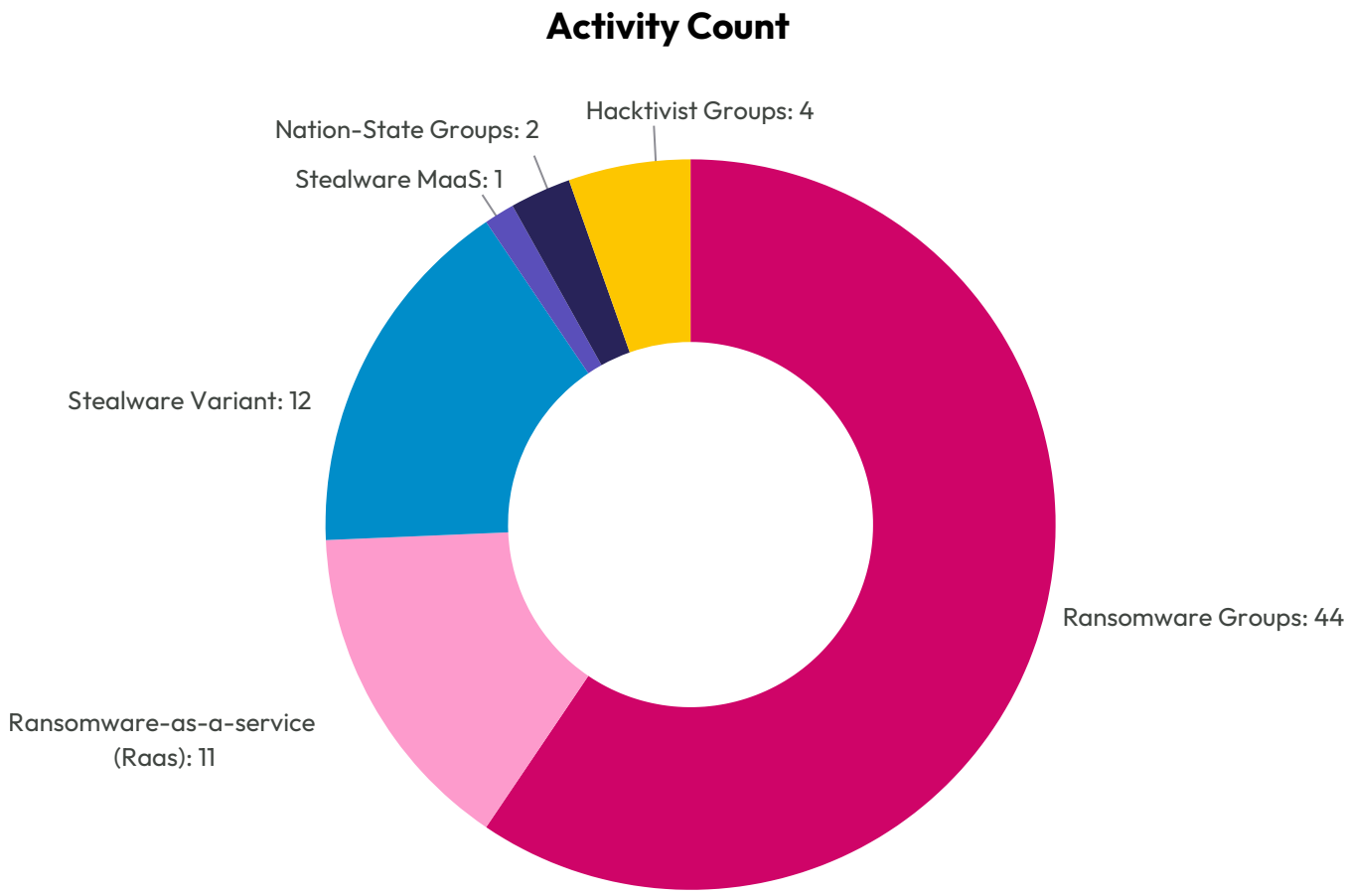
Appendix – Terminology Yardstick 43

Intelligence Terminology Yardstick 43

Executive Summary

In the first half of 2025, the Quorum Cyber Threat Intelligence (QCTI) team has identified and tracked over 70 new threat groups and Malware-as-a-Service (MaaS) offerings. During this period, the team noted a marked increase in the sophistication and innovation of threat actors. The continued emergence of new groups and services highlights the ever-evolving threat landscape and the persistent need for defenders to maintain currency with the latest attack vectors.

Broken down, our findings are:



Source: Quorum Cyber Threat Intelligence

Executive Summary

Key developments: January - June 2025

Codefinger: a new ransomware group exploited Amazon Web Services (AWS) Simple Storage Service's (S3) Server-Side Encryption with Customer-Provided Keys (SSE-C) to encrypt cloud data, rendering it unrecoverable without the ransom key. This marks a shift toward targeting cloud infrastructure using legitimate features.

Acreed Stealer: a novel infostealer gained traction on Russian cybercrime forums following the takedown of Lumma. Acreed rapidly became a leading source of stolen credentials, demonstrating the resilience of the cybercriminal marketplace to meet demand.

Moonstone Sleet & Qilin: North Korea's Moonstone Sleet deployed Qilin ransomware in a campaign targeting software and IT firms. This was the first known instance of a Democratic People's Republic of Korea (DPRK) actor using third-party Ransomware-as-a-Service (RaaS), signalling greater convergence between state and criminal capabilities.

DragonForce & RansomHub: conflict was seen between these two major RaaS operations, including infrastructure defacements, takeovers, and forum posts, pointing to significant restructuring and aggressive rivalry within the RaaS market.

RansomBay: a new RaaS platform associated with DragonForce offered a white-label model allowing affiliates to rebrand ransomware payloads and operate under customised identities, reflecting an increased maturity and scalability of the RaaS ecosystem.

Qilin Service Expansion / GLOBAL: the established ransomware group Qilin added legal intimidation and customer harassment to its extortion toolkit, offering affiliates call centres and legal complaints to pressure victims. This likely represents a new phase of 'quadruple extortion', targeting regulatory, reputational, and customer trust vectors. Meanwhile, a new RaaS offering, GLOBAL, introduced an AI-based negotiation chatbot, again showing innovation within the extortion phase of ransomware attacks.

Introduction

Quorum Cyber's Mid-Year Global Cyber Risk Outlook Report 2025 presents an overview of threat actor activities observed between January and June. It offers actionable guidance to help organisations enhance their resilience in an increasingly dynamic cyber threat landscape.

The report is structured as a month-by-month assessment, with each section spotlighting a notable group or activity. This format illustrates the significance of the evolving threat landscape and provides context for emerging risks and trends.

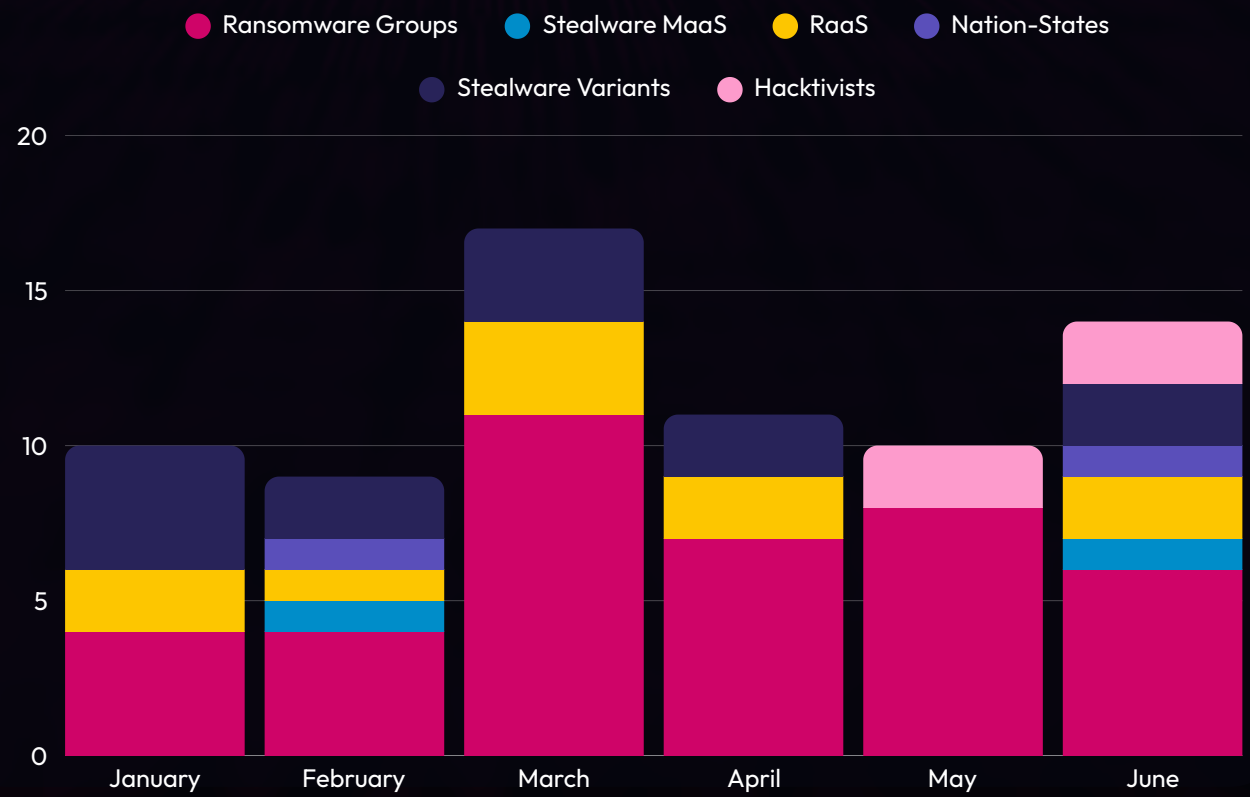


Figure 1: H1 2025 - Activity Tracker

Source: Quorum Cyber Threat Intelligence

January

- **10** new and evolving threat groups identified
- Focus areas: Ransomware & Information-Stealing Malware

Spotlight

January was defined by the emergence of **Codefinger**, a sophisticated ransomware group that exploited AWS S3's SSE-C. By abusing this legitimate cloud feature, Codefinger rendered cloud-stored data irrecoverable without the ransom key, signalling a novel and concerning evolution in cloud-targeted extortion tactics.

January

2025

In January, QCTI identified and tracked 10 counts of new and evolving threat group activity, encompassing both ransomware and information-stealing malware operations. The month saw a significant surge in stealware development, with new stealers emerging in rapid succession: FrigidStealer, SvcStealer, Astral Stealer, and Flesh Stealer. Notably, FrigidStealer specifically targeted macOS environments, reflecting an increasing diversification in platform targeting by criminal developers. The release of multiple infostealers within such a short window suggests both high developer turnover and sustained demand for credential-harvesting capabilities on criminal marketplaces.

Ransomware operations remained highly active. BlackLock, assessed as a likely strategic rebrand of Eldorado, entered the ecosystem as a confirmed RaaS operation, likely to evade detection, complicate attribution, and recruit new affiliates. Meanwhile, GD LockerSec appeared to be an amateur effort with unsubstantiated claims of AWS targeting, while a resurgence of the Babuk name was noted, this was likely a name hijacking attempt.

Outside the ransomware and stealer space, the newly surfaced ‘Belsen Group’ was linked to the leak of 15,000 FortiGate firewall configurations, reportedly exfiltrated using a zero-day vulnerability dating back to 2022. This points to a well-resourced adversary capable of long-term strategic compromise and storage of sensitive infrastructure data.

Most notably, the month was defined by the emergence of Codefinger, a sophisticated ransomware group that exploited AWS S3’s SSE-C. By abusing this legitimate cloud feature, Codefinger rendered cloud-stored data irrecoverable without the ransom key, signalling a novel and concerning evolution in cloud-targeted extortion tactics.

Codefinger

Overview

In January 2025, the ransomware threat group Codefinger conducted a novel ransomware campaign targeting AWS S3 buckets. By leveraging AWS's SSE-C, Codefinger encrypted data within S3 buckets using locally generated encryption keys, effectively rendering the data inaccessible to the victim organisation.

Codefinger offered the decryption keys in exchange for ransom payments. By exploiting legitimate cloud service features to achieve malicious objectives, the Codefinger campaign underscored an evolution in ransomware tactics towards the targeting of cloud storage systems.

Background and Identity

Codefinger was first identified in January 2025. There is no current attribution to any known advanced persistent threat (APT) or ransomware affiliate network for the group, and its modus operandi does not resemble other ransomware gangs. Unlike traditional ransomware groups that focus on encrypting endpoint devices, Codefinger demonstrates a sophisticated understanding of exploiting cloud-native features for malicious purposes.

Operations

For initial access, Codefinger leverages compromised AWS credentials with sufficient permissions (s3:GetObject and s3:PutObject) to access AWS S3 buckets. The group then utilises SSE-C for the encryption of S3 bucket contents. The AES-256 encryption key is locally generated and not retained by AWS, making conventional recovery methods ineffective without victim cooperation.[1] AWS processes the key during encryption but does not store it; only a hash-based message authentication code (HMAC) is logged, which cannot be used for decryption.

The group sets a seven-day deletion policy on encrypted data using the S3 Object Lifecycle Management application programming interface (API) and leaves a ransom note in each affected directory, providing payment details and a warning against tampering with permissions or files.

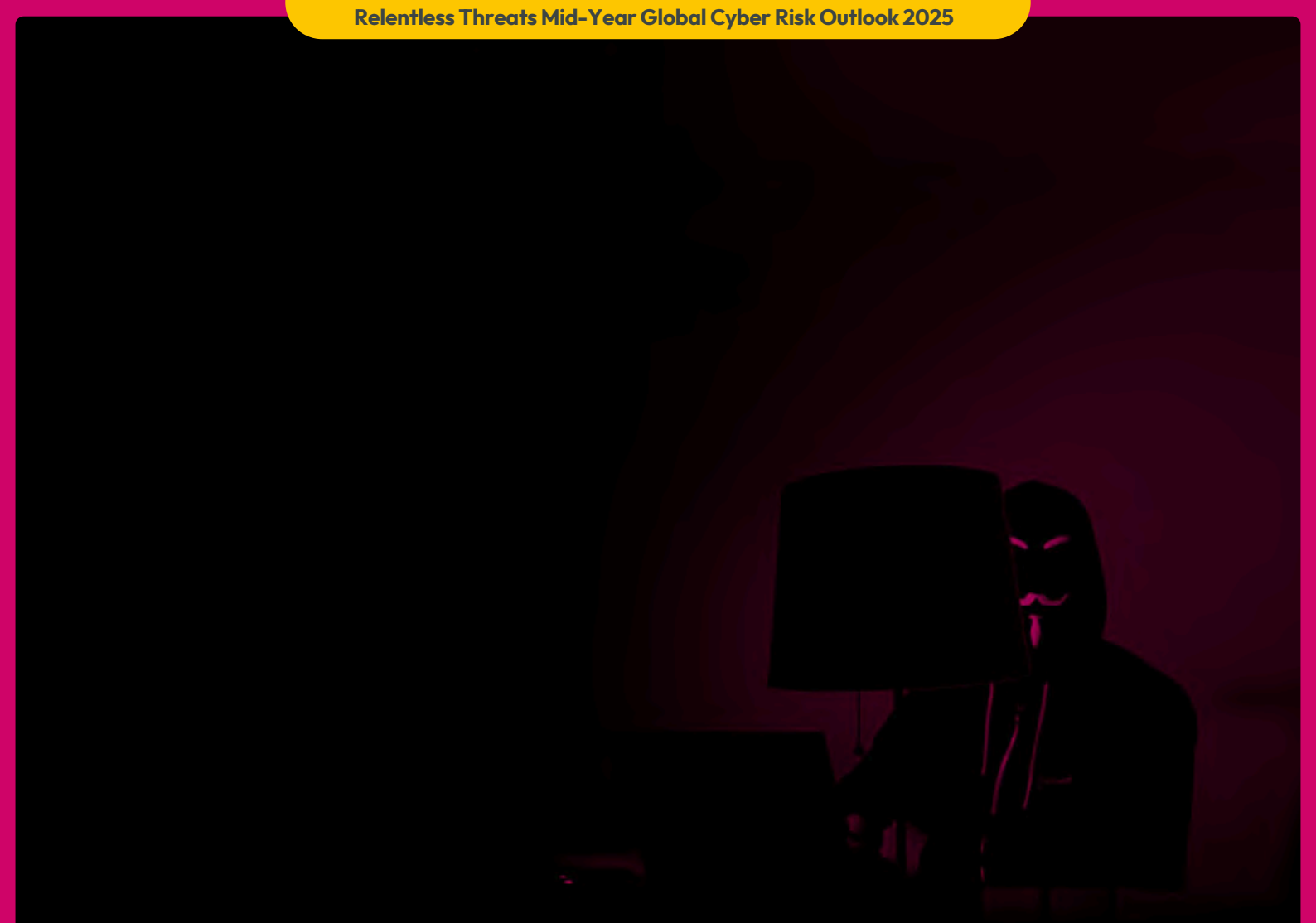
[1] Amazon S3

Assessment

The Codefinger campaign represents an evolution in ransomware tactics, moving from traditional endpoint encryption to direct targeting of cloud storage services. This can lead to irrecoverable data loss since AWS does not store customer-provided encryption keys. The further use of data deletion policies increases the pressure on ransom negotiations.

While the group's activity is presently low-volume, its attack path is novel and poses an elevated risk to organisations that rely on AWS S3 as a core part of their business operations. The absence of double-extortion techniques hints at limited maturity, but the technique may gain popularity among other threat actors.

Organisations using AWS are recommended to adopt strong cloud security key management practices, including, securing AWS keys or access tokens, restricting SSE-C usage, implementing advanced logging, and engaging AWS support.



February

- **8** new and notable threat groups identified
- Activity spanned: Ransomware, Infostealers, and Suspected Nation-State Operations

Spotlight

A new infostealer, **Acreed**, emerged, and subsequently filled a critical gap in the infostealer market after the takedown of Lumma stealer infrastructure by law enforcement in May. Its swift adoption and effective credential theft functionality demonstrate the cybercriminal ecosystem's resilience and its capacity to adapt quickly to enforcement actions.

February

2025

In February, QCTI identified and tracked eight instances of new and notable threat group activity, with developments spanning ransomware, infostealers, and suspected nation-state operations. Ransomware activity remained prominent, with several new actors emerging, including Team xxx, Anubis, and Run Some Wares. Unusually, Anubis combined file encryption with permanent file destruction, likely to sabotage recovery efforts post-encryption and increase pressure on victims. On the stealware front, GIFTEDCROOK expanded far beyond basic credential theft, introducing functionality to harvest documents selectively, indicating a move toward potentially intelligence-driven data theft.

February's most strategic development came with the exposure of Storm-2372, a suspected Russian state-linked APT engaged in targeted data collection. The group's tooling searches for a wide range of file formats, suggesting an interest in documents and configurations of operational value. This points to broad espionage motivations, likely focused on sensitive business or governmental environments. Most notably, a new info stealer, Acreed, emerged and subsequently filled a critical gap in the infostealer market after the takedown of Lumma stealer infrastructure by law enforcement in May. Its swift adoption and effective credential theft functionality demonstrate the cybercriminal ecosystem's resilience and its capacity to adapt quickly to enforcement actions.

Acreed

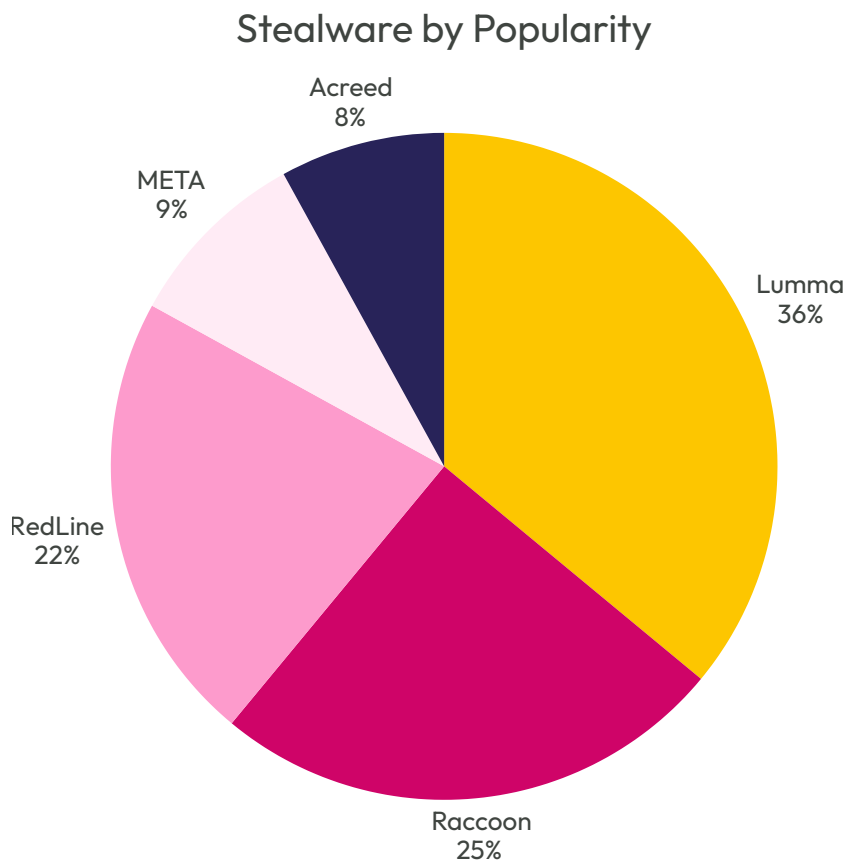
Overview

Acreed is a newly emerged infostealer malware (stealware) first seen on Russian-language cybercrime forums in February 2025. Acreed rapidly gained traction following the May 2025 takedown of Lumma stealer, with credentials compromised by Acreed increasing by 240 times on the Russian Market platform in May 2025.[2]

Despite recent takedowns of prominent infostealers like Lumma and coordinated efforts such as Interpol's Operation Secure,[3] the appearance of Acreed Stealer underscores the resilience of cybercriminals in developing, distributing, and adopting new malware strains.

Background and Identity

There is limited visibility of the developers behind Acreed. The stealware has surged in popularity, producing new credential theft logs on the Russian Market, a prominent dark web platform for selling stolen credentials.



Source: Quorum Cyber Threat Intelligence

Note: As of August, Acreed usage has jumped to 23.5% of the market"

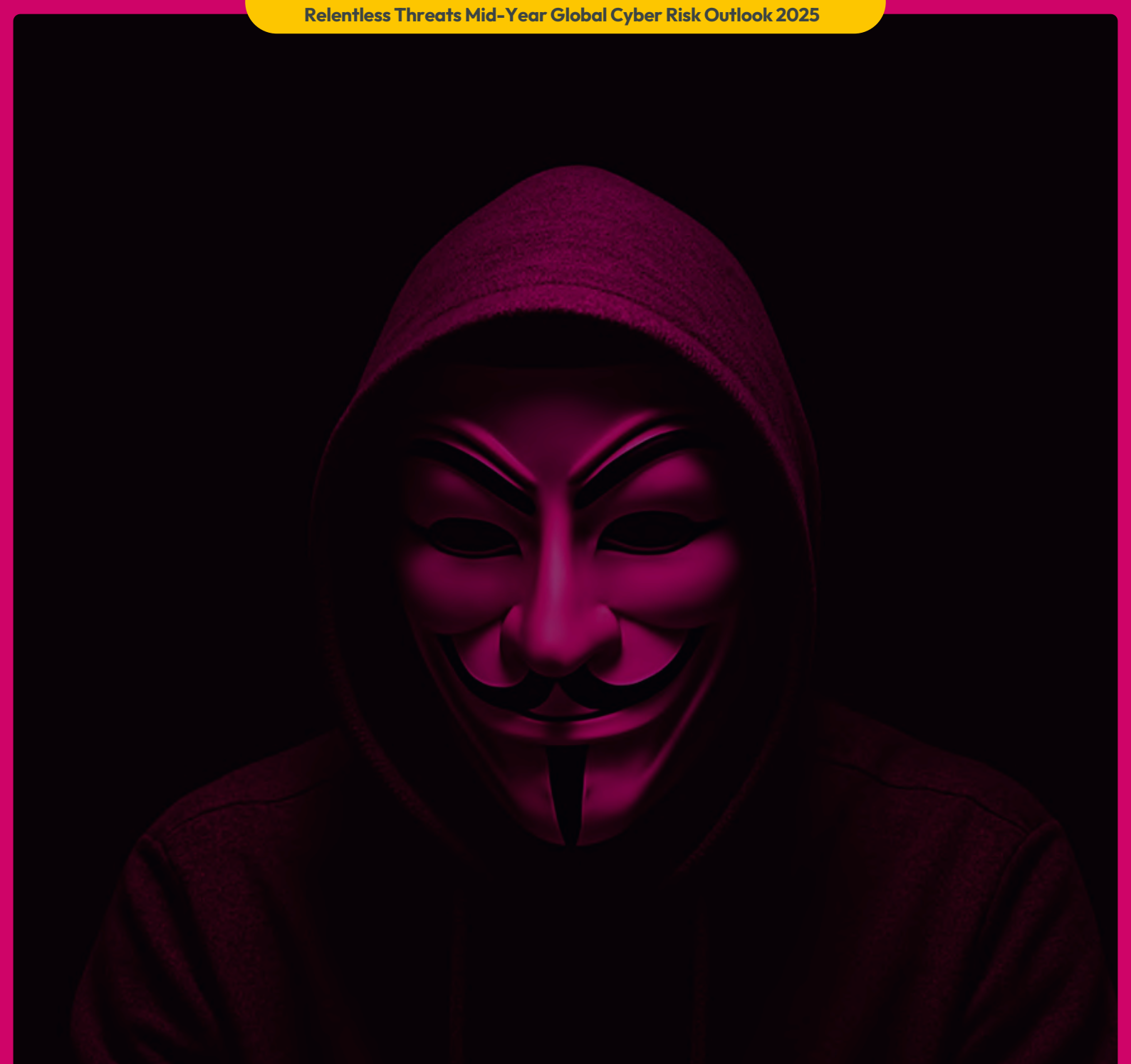
[2] Group-IB
[3] INTERPOL

Operations

Acreed targets data stored in Chrome, Firefox, and their derivatives, such as passwords, cookies, cryptocurrency wallets, and credit card information.

Assessment

The introduction of Acreed Stealer into the cyber threat landscape, particularly in the wake of significant law enforcement actions against other infostealers, underscores the resilience and adaptability of cybercriminal networks to cater to a persistent demand for infostealer capabilities. Despite a significant infrastructure takedown in May 2025, Lumma Stealer continues to maintain a dominant position within the stealware ecosystem. Even if a future takedown effort were to completely dismantle Lumma's operations, it is highly likely that alternative strains such as Acreed would rapidly emerge to fill the void and sustain the threat posed by infostealers.



March

- **17** new and evolving threat groups identified
- Dominated by **15** ransomware threats, plus stealware and nation-state activity

Spotlight

State-Criminal Convergence: North Korea's **Moonstone Sleet** deployed **Qilin** ransomware, blurring the lines between nation-state and criminal operations. This tactic complicates attribution and introduces sanctions risks for victims, as ransomware is used to mask espionage under criminal infrastructure.

March

2025

In March, QCTI identified and tracked 17 instances of new and evolving threat group activity, dominated by a surge in ransomware activity with 15 new threats observed. Among them were VanHelsing, Mamona, and QWCrypt, the latter deployed by the previously espionage-focused RedCurl. This marked a strategic pivot from traditional corporate espionage to financially motivated ransomware by RedCurl, potentially to obscure data theft or to escalate pressure on victims. QCTI also observed the emergence of a new RaaS under the name of RALord, which rebranded to Nova within weeks of operation, likely to improve evasion or reframe its affiliate appeal. The emergence of other groups such as The Skira Team, Secpo, Weyhro, and Arkana Security reflects the continued fragmentation of the ransomware landscape.

March's activity also highlighted the complexity of attribution in cybercriminal attacks. The appearance of Mora_001 raised potential sanctions considerations due to its ransom note infrastructure, which referenced a TOX ID previously associated with LockBit. While the extent of any operational overlap remains unclear, the reuse of communication channels linked to a sanctioned entity may expose victims and responders to legal and regulatory risks. Meanwhile, a new ransomware group, OX Thief, claimed to have involvement in a 2024 ransomware attack which was previously attributed to Medusa, a RaaS which has claimed over 300 victims since its emergence.

Stealware activity remained high, with new families including WRECKSTEEL, Hannibal, and Gremlin Stealer. WRECKSTEEL was reportedly used by Russian-linked group UAC-0219 against Ukrainian targets, adding to a trend of criminal stealer malware being leveraged in cyberespionage campaigns.

The most notable trend in March was the convergence of state and criminal activity with North Korea's Moonstone Sleet deploying Qilin ransomware. The move will likely complicate attribution, with ransomware deployment enabling nation-state cyber threats to blend with criminal infrastructure for plausible deniability, with implications for victims owing to North Korea's status as a sanctioned entity.

Qilin and Moonstone Sleet Cooperation

Overview

In March 2025, the North Korean state-aligned threat actor tracked as Moonstone Sleet was observed utilising Qilin ransomware in a limited number of attacks. The campaign represents the first publicly reported instance of this North Korean state-aligned actor deploying commercially available RaaS tooling.

The convergence of nation-state and cybercriminal tradecraft through shared tooling is likely to present challenges for attribution in future ransomware attacks. Due to North Korea's nuclear programme and history of human rights violations, the state remains under heavy financial sanctions. These restrictions make the generation of legitimate funds almost impossible, leading to a long history of illicit financial activity such as ransomware support, almost certainly for a cut of the profits and payment for initial access.

Background and Identity

Moonstone Sleet

The group tracked as Moonstone Sleet (formerly Storm-1789) is a nation-state activity group based out of the Democratic People's Republic of Korea, known for both financially motivated and espionage operations. The group is likely affiliated with Bureau 121 of the DPRK's Reconnaissance General Bureau (RGB), the military's cyber warfare division.

Moonstone Sleet primarily targets entities within the software development, IT, education, and defence industrial base sectors. These sectors are of interest to North Korea for both economic and military intelligence collection as the state seeks to close its military and technological gap, particularly with South Korea and the United States.

Qilin ransomware

Qilin (formerly known as Agenda) ransomware is a RaaS operation first observed in mid-2022. Likely operated by Russian-speaking actors, it supports both Windows and Linux environments and is customised by affiliates via a builder toolkit. Qilin's codebase includes functionality to terminate services, evade defences, and exfiltrate data, often preceding double-extortion attempts.

Operations

In late February 2025, Moonstone Sleet deployed Qilin ransomware in a targeted campaign against software and IT firms, marking a significant tactical shift in its operations, which had previously used its own custom ransomware. Initial access was often gained through fake job offers, a long-standing DPRK tactic designed to lure software engineers into interacting with malicious content.[4] In at least one case, the Qilin ransomware deployment was preceded by lateral movement or credential theft, indicating that reconnaissance and broader network access was a primary objective.

Assessment

Moonstone Sleet's deployment of Qilin ransomware likely indicates a strategic pivot aimed at reducing development overhead, accelerating deployment timelines, and further blurring attribution lines. The DPRK continues to rely on cybercrime to circumvent sanctions, and RaaS toolsets provide plausible deniability and integration into existing affiliate networks.

Sanctions Complications

Due to the reported usage of Qilin by Moonstone Sleet and the sanctions implications, organisations successfully targeted by the group will need to take additional precautionary steps if considering ransom payment. In most cases, these steps will be conducted by your negotiation or intelligence service providers, thereby providing businesses with actionable confidence to proceed with limited risk.

Note: Any ransomware case confirmed to be by a known sanctioned entity will immediately be ineligible for ransom payment due to the risk of violating international law.

Executive liability:

According to the UK government, a breach of financial sanctions may be a criminal offence with the potential repercussions.

Up to
7 years
in prison

Up to
£1.0M
in fines

and
50%
in total paid amount

[4] Microsoft Security

April

- **11** notable incidents of emerging threat group activity
- Continued activity across ransomware and stealware domains

Spotlight

Ransomware Turf War: April saw rising tensions between DragonForce and RansomHub, marked by infrastructure defacements and shared tooling. Evidence suggests both rivalry and potential strategic alignment. RansomHub's data leak site going offline points to a likely takeover by DragonForce, signalling a shift in power dynamics within the ransomware ecosystem.

April

2025

In April, QCTI identified and tracked 11 notable incidents of emerging threat group activity. Ransomware activity remained steady with the appearance of several new operators including Devman, SatanLock, Crypto24, Bert, Silent, and Gunra. Meanwhile, Hunters International formally rebranded as World Leaks, shifting its operating model from full RaaS operations to pure data theft and extortion. Ransomware attacks made global headlines, with attacks on the UK retail sector via social engineering calls to IT vendors, underlining social engineering as a persistent initial access vector in ransomware attacks.

In the stealware space, Salvador stealer targeted Android devices as a mobile banking trojan, while Chihuahua stealer appeared targeting browser data and crypto wallet information using .NET. The expansion to Android platforms shows ongoing efforts to diversify stealware across operating systems, while maintaining the core objective of large-scale credential and data theft.

Significantly, April was shaped by growing tensions between DragonForce and RansomHub. Infrastructure defacements, forum claims, and shared operational tooling suggested both competition and cooperation between the two groups, raising the possibility of strategic alignment that could bolster resilience and widen affiliate reach. At the time of writing, RansomHub's data leak site (DLS) remains down, indicating the activity was likely the outcome of an aggressive and successful takeover by DragonForce operators.

DragonForce / RansomHub

Overview

In April 2025, interactions between two major RaaS operations - RansomHub and DragonForce - showed indications of competition, conflict, and co-operation. RansomHub's DLS went offline on 31st March. Following this, a DragonForce-linked actor announced on a dark web forum that RansomHub would soon resume operations using DragonForce's infrastructure, indicating a possible merger or strategic alignment between the two groups. However, site defacements and public accusations of betrayal were seen between affiliates of the groups, and at the time of writing, RansomHub's DLS remains offline.

The interactions between RansomHub and DragonForce reflect broader volatility in the cybercrime ecosystem, elevating the risk to victim organisations as competition and rivalry between cybercrime affiliates and operators are likely to have spillovers on victims via repeat extortion. Instability within these groups can make attribution difficult, impeding incident response and threat hunting owing to unpredictable attack patterns, and presenting challenges to ransom negotiators.

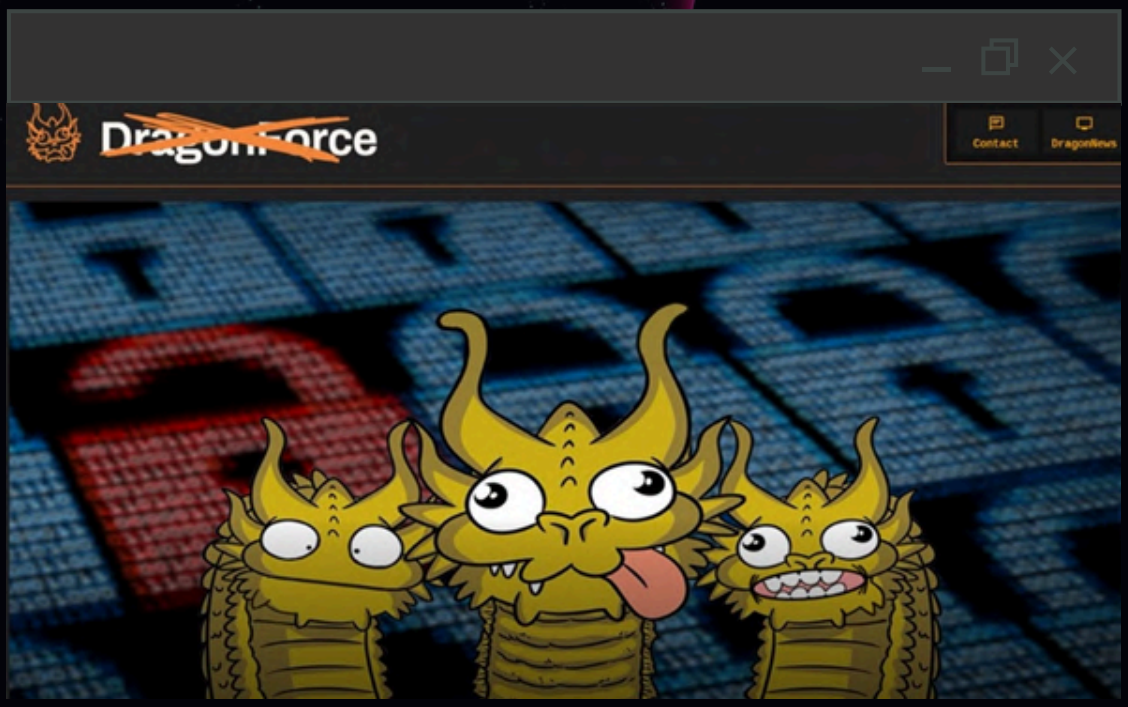


Figure 3: RansomHub defacement of DragonForce

Source: DragonForce DLS

Background and Identity

RansomHub

RansomHub is a RaaS operation that emerged in early 2024. It employs a double-extortion model and has targeted over 210 victims across various critical infrastructure sectors, including healthcare, government services, and financial services. The group is known for its favourable affiliate terms, attracting experienced affiliates from other prominent ransomware variants like LockBit and ALPHV.

In February 2025, RansomHub gained significant attention by publishing 4TB of sensitive data stolen from Change Healthcare. The initial breach was executed by an ALPHV affiliate who, after not receiving payment, collaborated with RansomHub to monetise the stolen data.

DragonForce

DragonForce emerged in August 2023 and was originally known for lower-tier pro-Palestine hacktivist operations. The group restructured in March 2025 into a RaaS 'cartel' and now functions more as an umbrella platform, allowing independent threat actors to operate semi-autonomously under the DragonForce 'brand', much like LockBit's previous model, while keeping up to 80% of ransom payments.

Operations

On 31st March 2025, RansomHub's DLS went offline, displaying a message 'RansomHub – R.I.P (03.03.2025)' prompting speculation of law enforcement disruption or internal instability. Around this time, DragonForce launched a defacement campaign against other rival ransomware groups, including BlackLock and Mamona, asserting itself as a dominant cartel within the underground ransomware ecosystem.[5]

Soon after, DragonForce banners and promotional messages appeared on RansomHub's former DLS, suggesting either a takeover or an offer of an infrastructural partnership. This was corroborated by a DragonForce-linked actor on a dark web forum, stating that RansomHub's operations would soon resume via DragonForce's tooling and infrastructure, and asking RansomHub to "consider our offer".

[5] Sophos

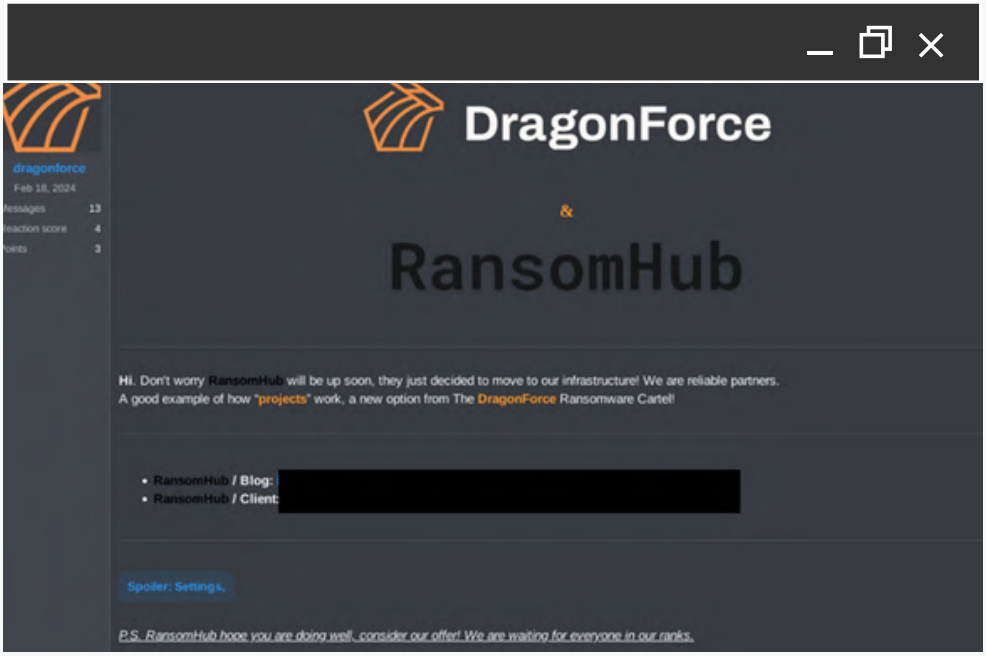


Figure 4: DragonForce forum post on RansomHub
Source: RansomHub DLS

Assessment

There is a realistic possibility that RansomHub and DragonForce have converged under the 'DragonForce cartel' brand, merging their infrastructure. However, it is more likely the activity was initiated by DragonForce operators attempting to consolidate influence over the ransomware ecosystem by defacing – and where possible, dissolving or taking over – competitors.

The strategic implications of either outcome are significant for potential victims:

- Cartelisation and mergers between rival groups are likely to increase operational tempo and reach by consolidating power and resources.
- The blending of tactics, techniques, and procedures (TTPs) from multiple groups is almost certain to make direct attribution more difficult, hindering incident response efforts.
- Operational instability between affiliates from rival groups is likely to increase the risk of targets experiencing multiple sequential or simultaneous attacks, as data is reused or sold by multiple groups, prolonging negotiations and increasing reputational and financial harm to victims.

May

- **11** new or evolving threat groups identified
- Ransomware remained dominant, with continued expansion of the RaaS ecosystem

Spotlight

RaaS Platform Maturity: The launch of RansomBay, tied to the DragonForce ecosystem, introduced a white-label model allowing affiliates to customise payloads under their own branding. This development represents a concerning shift towards more sophisticated, enterprise-style operations among cybercriminals in the Ransomware-as-a-Service (RaaS) market, increasing their scalability, operational resilience, and autonomy.

May

2025

In May, QCTI identified and tracked 11 new or evolving threat group activities, with ransomware operations maintaining a dominant presence. The month saw a broadening of the RaaS landscape, with groups such as J, IMN Crew, LeakedData (also known as Silent Ransom Group), World Leaks, Devman, Direwolf, and Datacarry either launching new operations or expanding their visibility. Silent Ransom Group was observed targeting the legal sector using 'call-back' phishing, where victims are socially engineering into installing attacker-controlled remote desktop software.

Stealware activity included the identification of TerrastealerV2, linked to the long-running Golden Chickens MaaS group. The stealer operates alongside TerraLogger, with the strains designed for credential theft and keylogging respectively.

The month was most notably defined by the emergence of RansomBay, a RaaS platform tied to the DragonForce ecosystem. Offering a white-label model that allows affiliates to customise DragonForce payloads under their own branding, RansomBay demonstrates a new level of maturity in the RaaS marketplace as RaaS offerings increasingly mirror enterprise platforms. This model provides affiliates with greater autonomy and branding flexibility while increasing the resilience and scalability of the parent operation.

RansomBay

Overview

RansomBay, a novel RaaS platform associated with the operators behind DragonForce, was discovered in late April 2025. RansomBay offers affiliates the opportunity to deploy DragonForce payloads under their own branding via a 'projects' system, where 'partners' can migrate to DragonForce infrastructure. This white-label approach almost certainly complicates attribution efforts and likely enhances the operational security of both the core DragonForce group and its affiliates.

Figure 5: RansomBay and DragonForce logos
Source: Ransomware.live

Background and Identity

DragonForce rebranded as a 'cartel' in March 2025 before initiating a wave of attacks against rival groups, likely including RansomHub. Following the changes to RansomHub's DLS a month earlier, in late April 2025, RansomBay displayed RansomHub as an example of the new 'projects' system in the DragonForce cartel (see Figure 7).

There is a remote chance that the platform's name and pirate-themed iconography are deliberate references to The Pirate Bay (TPB), the well-known torrent indexing site, and may be intended to position RansomBay as a similar hub for the distribution and monetisation of ransomware payloads.

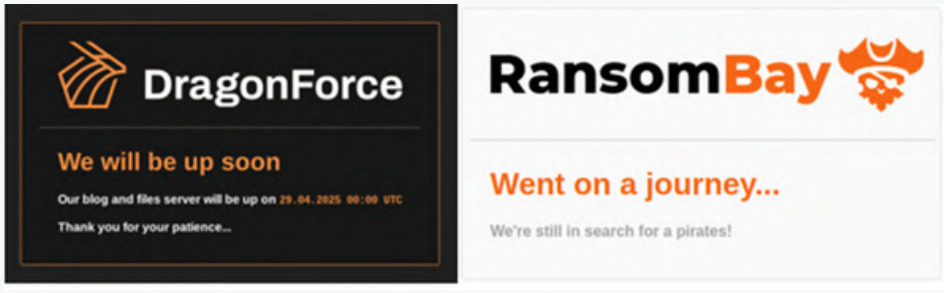


Figure 6: DragonForce and RansomBay update page
Source: RansomBay

Operations

White Label Model

RansomBay offers affiliates a white-label framework; this allows for affiliates to customise DragonForce ransomware payloads with distinct branding. This enables threat actors to tailor attacks to specific industries, regions, or victim profiles, enhancing both psychological impact and operational flexibility. Affiliates can run multiple brands simultaneously, benefitting from what is marketed as a stable and disruption-resistant ecosystem.

DragonForce claims a 20% share of ransom payments, leaving affiliates with 80%, and supports their operations with a suite of tools including payload builders, file servers, decryption utilities (NTLM and Kerberos), and fully featured admin/client panels. A dedicated “call-service” facilitates victim engagement, while Data Leak Site support double extortion tactics. The platform advertises itself as fully automated and highly resilient, underpinned by robust infrastructure featuring 24/7 monitoring via the so-called DragonForce Ransomware Cartel, proprietary Anti-DDoS protection, and unlimited PETABYTE-scale storage.

As of the time of writing, RansomBay’s Torsite displays the message, "We’re still in search for a pirates!" (sic), highlighting the groups desire for continued growth.

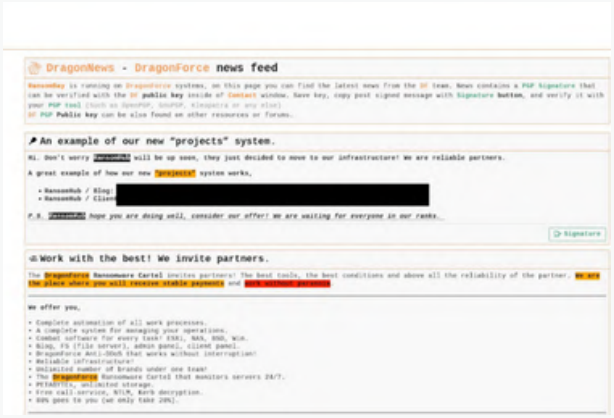


Figure 7: RansomBay Site
Source: RansomBay Site

Assessment

The emergence of RansomBay reflects an evolution of the RaaS economy, which is showing increasing decentralisation, greater brand abstraction, and a maturing service model. Quorum Cyber Threat Intelligence is tracking a broader trend of RaaS operators professionalising their offerings by creating scalable, franchise-like models that likely reduce operational risk, and are harder to disrupt through conventional law enforcement or intelligence-led takedowns.

Project Model

DragonForce's transition towards a 'cartel' model and RansomBay's 'projects' system shows a likely strategic shift towards a federated operational model. This mirrors similar developments observed in the 2023-2024 period with groups like ALPHV and LockBit, but RansomBay's more explicit franchise-style offering, with re-brandable tooling, integrated infrastructure support, and a stable revenue-sharing model, indicates a more mature and commercially aware evolution.

April 2025 UK Retail Sector Attacks

The recent confirmation by Marks & Spencer that DragonForce was associated with its April 2025 ransomware attack reinforces the operational scale and impact of this evolving cartel model. RaaS platforms like RansomBay can enable widespread, financially devastating operations through outsourced affiliates while obfuscating attribution. As the chairman of Marks & Spencer told the House of Commons Business and Trade Sub-Committee in July 2025: "when this happens, you don't know who the attacker is. (...) They never send you a letter signed 'Scattered Spider'."[6]

Branding

RansomBay likely reflects the importance of hacker culture within cybercrime communities, where branding, identity, and reputation matter. Allusions to The Pirate Bay and adoption of a 'cartel' public image likely indicate that threat actors are increasingly conscious of how their platforms are perceived within underground cybercrime communities. It is likely that cybercriminal marketplaces may further emulate the marketing and operational structures of legitimate enterprises, using branding for service differentiation to attract and retain talent and affiliate members.

New group enablement

The introduction of the RansomBay white-label service provides individuals that would traditionally lack the skills and resources to start their own named ransomware, thus lowering the barrier of entry

[6] House of Commons

June

- **12** emerging threat group activities identified
- Categories: Ransomware, Nation-State Operations, Stealware, and Hacktivism

Spotlight

AI-Enhanced Ransomware: The newly launched GLOBAL RaaS platform introduced an AI-driven chatbot to assist affiliates during extortion negotiations. This innovation aims to improve the persuasiveness and efficiency of attacker communications, marking a notable evolution in ransomware tactics.

June

2025

In June, QCTI identified and tracked 12 instances of emerging threat group activity across ransomware, nation-state operations, stealware deployment, and hacktivism. Ransomware remained the most active category, with nine new groups emerging or continuing operations, including Warlock, Walocker, KaWaLocker, and Kawa4096. Stealware developments included the appearance of Katz Stealer MaaS which employed multi-stage obfuscation and in-memory execution to harvest credentials and steal sensitive data at scale.

Nation-state activity included a China-linked threat group performing operations dubbed 'PurpleHaze', which targeted managed service providers and third-party IT infrastructure in a continuation of strategic supply chain compromise tactics likely for cyber espionage.

In the hacktivist space, keymous (also known as Keymous+ or KeymousTeam) expanded its operations across multiple sectors and regions, with attacks affecting targets in the United States, Denmark, and Israel. Separately, GhostSec signalled a shift from hacktivism to hacker-for-hire operations, likely monetising its prior influence and network access.

The most significant developments this month centred around the GLOBAL and Qilin ransomware groups. GLOBAL, a newly launched RaaS, introduced an AI-driven chatbot to assist affiliates during extortion negotiations. This feature is likely designed to enhance the persuasiveness and efficiency of attacker communications. Meanwhile, Qilin expanded its extortion toolkit beyond encryption and data theft, offering affiliates additional services such as harassment of victims, legal intimidation, and even outsourced call centres. These techniques represent a shift toward 'quadruple extortion', intensifying pressure through reputational, regulatory, and customer-facing vectors. Taken together, these developments represent a significant evolution in the extortion and negotiation phases of RaaS offerings, where operators are increasingly incorporating psychological and social engineering across all stages of their attacks.

GLOBAL Ransomware

Overview

GLOBAL surfaced as a RaaS in June 2025. Distinctively, it offers affiliates an AI-powered negotiation chatbot, a pioneering feature in the ransomware landscape. This innovation is almost certainly designed to improve the persuasiveness, scale, and efficiency of extortion communications with victims. If operational as described, this capability marks a significant and concerning evolution in cyber extortion, increasing both the pressure on victims and the strategic complexity of responding to ransomware incidents.

Background and Identity

GLOBAL was launched by a threat actor known as '$$$', first promoted on the Ramp4u cybercrime forum on 2nd June 2025. The actor is well-established in RaaS circles, having previously operated or promoted groups such as Eldorado, MamonaRIP, and BlackLock. There are strong technical and behavioural overlaps between GLOBAL and these previous projects. It is likely that GLOBAL is an evolution or rebrand of BlackLock, whose reputation was diminished in March 2025 following the exposure of its internal operations by security researchers via a vulnerability in its DLS.

This rebrand is a probable attempt by the operators to escape reputational damage and re-engage affiliates under a new and more sophisticated brand.

Operations

GLOBAL replicates the typical features of established RaaS platforms, including:

- Full encryption, customisation, and attack lifecycle control
- A web-based negotiation portal accessible via Tor
- High affiliate revenue share (85%)
- No entry or upfront fees. Payment structure is designed to prioritise affiliates.

Targeting patterns align with those of Russian-speaking ransomware groups, explicitly avoiding the Commonwealth of Independent States (CIS) countries, critical infrastructure, and non-profit organizations. As of 15th July 2025, GLOBAL had identified 18 victims across seven countries, with a significant proportion belonging to the healthcare sector.

Initial access is obtained primarily via Initial Access Brokers (IABs). There is evidence of collaboration between '$$$' and an IAB named HuanEbashes. Payloads are built in Golang, supporting VMware ESXi environments for rapid encryption across virtualised systems.

Assessment

The introduction of an AI-assisted negotiation chatbot by GLOBAL demonstrates a shift in RaaS focus from merely improving malware to enhancing social engineering and psychological manipulation during the extortion phase. By automating negotiation interactions, GLOBAL could potentially reduce response times, avoid human errors, sustain pressure on victims with consistent, tailored messaging, and free up affiliate time to conduct multiple attacks in parallel.

From a defensive perspective, this change reduces opportunities for intelligence collection. Ransom negotiators frequently rely on analysing language, timing, and tone to assess threat actor capability and intent.

AI-generated messages remove many of those cues, making it more difficult to manage negotiations, identify operators, or exploit negotiation fatigue.

Moreover, the capability to automate ransom chats introduces the potential for scaled extortion operations. There is a realistic possibility that a disparity in automation, with attackers using AI and defenders still relying on human-led response, will strain incident response and negotiation teams, especially for small-to-medium-sized enterprises.

If AI negotiators become more common, defenders may begin to reverse-engineer AI negotiation patterns, identifying chatbot responses and using that knowledge to script counter-tactics or predict future messaging. However, this will require cross-sector collaboration and rapid intelligence sharing.

GLOBAL's launch signals a trend of RaaS operators becoming more competitive and investor-focused, offering affiliate-centric features like upfront payments and multilingual promotion. As such, the ransomware ecosystem may become more accessible to novice cybercriminals, increasing the threat volume.

Qilin Services Development

Overview

Although Qilin is not a newly emerged group, it warrants renewed attention due to its pivot to legal and reputational harassment. This change likely emerges from the competitive pressures between RaaS offerings, which are likely resulting in tactical innovations between RaaS operations seeking to attract and retain affiliates. On 25th June 2025, Qilin revealed it is incorporating legal intimidation and customer harassment into its extortion toolkit.[7] These additions go beyond traditional double extortion (data encryption and exfiltration) and even triple extortion (adding distributed denial-of-service (DDoS) attacks), marking the emergence of what might be termed quadruple extortion. This pivot is both a competitive differentiator and an indication of the growing professionalisation of cyber extortion.

Background and Identity

Qilin is one of several RaaS groups innovating to remain competitive in a saturated ecosystem. The group's latest shift appears partially driven by competition with other ransomware collectives such as DragonForce. In such an environment, offering broader services at a lower cost attracts more affiliates and potentially leads to higher victim conversion rates.

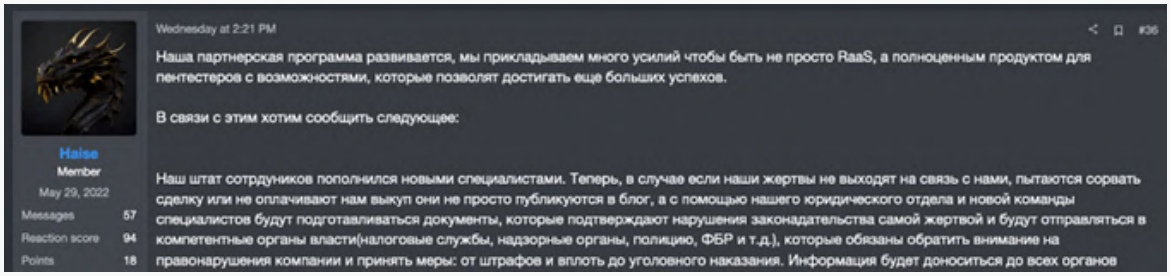


Figure 8: A Qilin representative forum post
Source: Group-IB

[7] Group-IB

Operations

Qilin's newly introduced tactics include:

Legal harassment: Qilin now claims to employ legal 'specialists' to prepare documents alleging misconduct by victims such as tax violations, breaches of data protection regulations, or other forms of non-compliance. These complaints are reportedly submitted to regulatory and law enforcement authorities such as tax agencies, police, or data protection commissioners.

Customer harassment: Qilin is establishing a call centre offering services in seven languages. Using stolen personally identifiable information (PII), operators will contact customers of victim organisations to urge legal action or apply direct psychological pressure. This may include threatening calls or attempts to distress customers to the point of initiating complaints or lawsuits against the compromised company.

Affiliate support: The group now offers affiliates additional options for negotiation support, including escalating cases via legal and reputational channels if a ransom is not paid or discussions stall.

Fraud and data weaponisation: If no payment is forthcoming, stolen PII will be sold or shared with other cybercriminal groups for use in fraud, phishing, or identity theft campaigns.

Assessment

This development aligns with a broader trend of ransomware groups innovating in the negotiation phase of their operations. Qilin's introduction of legal and customer harassment represents an escalation in its capability to apply pressure in ransom negotiations. By extending pressure to regulators, law enforcement, and affected customers, Qilin increases the victim's exposure to legal, reputational, and operational risks:

- **Increased regulatory exposure:** even if legal allegations are unfounded, the process of defending against complaints submitted to agencies or regulators can be costly and reputationally damaging
- **Customer trust degradation:** direct contact from a criminal group to clients, especially if accompanied by threats or fraudulent use of stolen PII, could irreparably harm customer relationships and brand trust
- **Prolonged incident timelines:** the harassment of clients and the filing of external complaints extend the duration and complexity of incident response and recovery efforts.

Qilin's strategy also reflects the broader trends of the blending of psychological operations with technical intrusions. Other groups are likely to follow Qilin's lead, especially if these tactics prove effective in increasing payment rates.

Financial Impact

Over the past four years, the QCTI team has tracked a 53% average increase in initial ransom demands between Q1 2022 – Q1 2025.

Average initial ransomware demand:

Q1 2025: £1,439,317 (US$1,926,166)	**Q1 2024:** £628,752 (US$841,428)	**Q1 2023:** £929,377 (US$1,243,738)	**Q1 2024:** £936,942 (US$1,253,862)

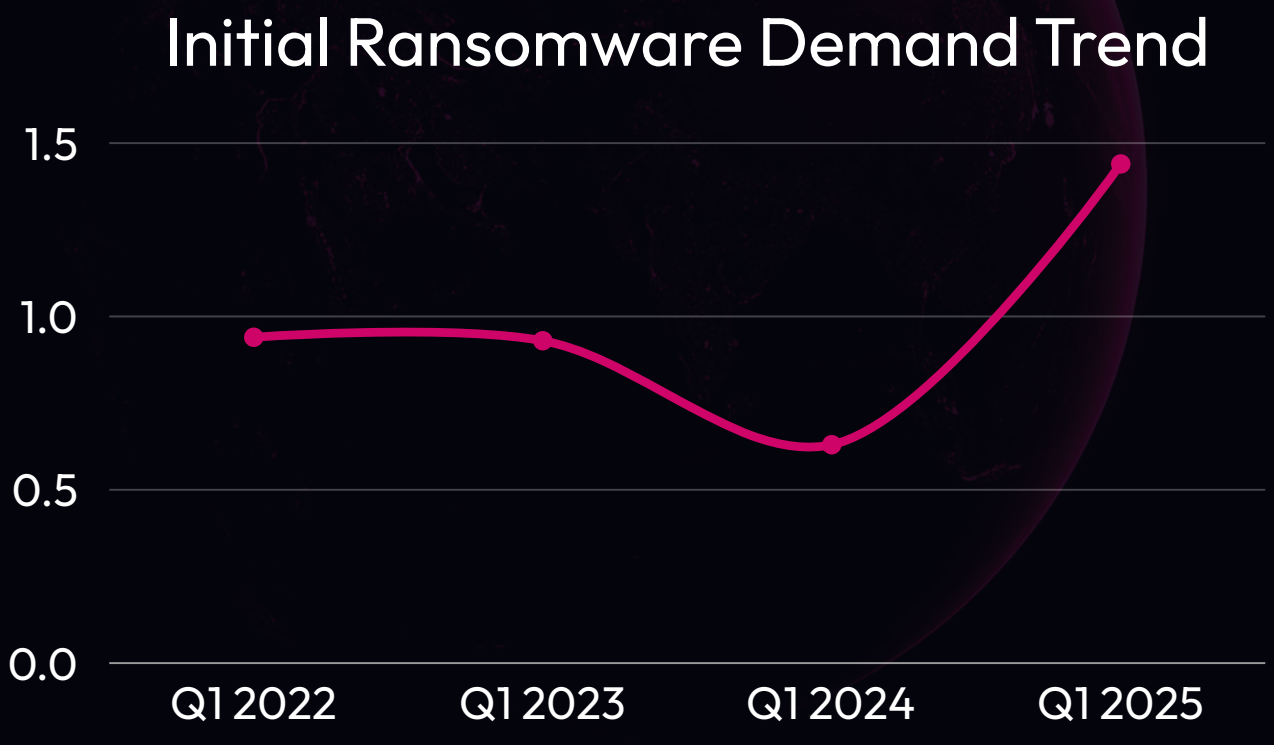


Figure 3: Initial Ransomware Demand Trend

Source: Quorum Cyber – Counter Extortion Threat Intelligence

Sector Consideration

Whilst QCTI has identified an average rise of 53% spread out across all sectors, not all sectors are afforded the same levels of initial demand. When broken down and investigated, initial demands can vary based on several factors, including the targeted sector, the financial size of the victim business, and the threat group itself.

Industries Experiencing Higher-Than-Average Ransomware Demands

Finance:
+179%

Manufacturing:
+97%

Industries Experiencing Lower-Than-Average Ransomware Demands

Retail:
-6%

Healthcare:
-24%

Initial Demand Assessment

Decrease in Ransom Payments: In 2024, QCTI tracked a 35% decline in ransom payments compared to 2023.

RaaS operating costs: as RaaS offerings become larger and increasingly more sophisticated, these illicit organisations' operating costs are also likely following an upwards trajectory. In the current RaaS landscape, groups must compete to remain relevant and ensure that customers seeking ransomware services choose their offering. The development and implementation of AI chatbots, white-label ransomware services, and offensive legal services almost certainly require background support staff and developers, just like in a legitimate business.

It is owing to these factors - high operating costs, the need for innovation, and the drop in previous years' payments - that we assess groups are demanding more in initial payments and are likely to continue to demand more in the coming years.

Quorum Cyber's Threat Intelligence

QCTI continues to see new threat actor groups being established and fresh, innovative services being offered in cybercrime marketplaces. New services are lowering the barrier for entry and making it easier than ever for low-skilled cybercriminals to artificially raise their capabilities above their level of skill. Furthermore, these trends highlight the ever-evolving threat landscape and the persistent need for defenders to keep up to date with the latest attack vectors. In this rapidly changing cyber threat environment, it's imperative for defences to be adaptable to strengthen organisational resilience.

Over the past four years, from Q1 2022 to Q1 2025, the QCTI team has assessed that initial ransom demands have risen by 53%, putting an extra financial burden on organisations across all sectors. However, the specific increase in the initial ransom demands varies considerably by sector and this depends on the financial size of the victim's business and the specific threat actor's behaviour.

One new evolution demonstrates how the RaaS ecosystem has grown in maturity and scalability. Copied from enterprise business models, the white-label model enables cybercriminal affiliates to rebrand ransomware payloads and operate under their own distinct identity. This enables threat actors, who would otherwise lack the skills and resources to start their own branded ransomware, to tailor attacks to specific industries, regions, or victim profiles, while increasing the parent operation's revenues, resilience, and scalability.

Recommendations

Given the recent developments in the threat actor landscape during the first half of 2025, including the weaponisation of cloud infrastructure, the evolution of RaaS, and the increased use of coercive extortion tactics, organisations are strongly advised to implement resilient security measures. The following high-level recommendations are relevant across all sectors and aim to support organisations in defending against these emerging cyber threats.

Ransomware

✓ Policies to counter social engineering

Requests for credential reset for users with admin privileges should require additional investigation by engaging with user line management before password resets are issued.

✓ Intelligence-led vulnerability management

Maintain a strong, intelligence-led patching policy that prioritises vulnerabilities that are under active exploitation or those that have a published proof of exploit.

✓ Harden cloud storage and key management

Disable customer-managed encryption features such as AWS SSE-C unless strictly required. Implement logging and alerting on changes to encryption policies, data lifecycle rules, and access permissions in cloud storage services like AWS S3 and Azure Blob.

✓ Critical systems resilience

Maintain offline, encrypted backups of critical data. The UK's National Cyber Security Centre (NCSC) recommends the rule of '3-2-1': three copies, on two devices, and one offsite.

✓ Enhance user awareness and engineering security culture

Educate staff, particularly developers and IT personnel, on social engineering threats such as job lures, fake recruiters, and infostealer-delivered malware. Encourage timely reporting of suspicious activity.

Recommendations

Stealware

✓ Dark web and credential theft visibility

Establish continuous monitoring for exposed corporate credentials and brand impersonation. Prompt credential rotation and assess potential access paths if exposures are identified.

✓ Policies to counter social engineering

Enforce conditional access across all cloud and Software-as-a-Service (SaaS) platforms, including Microsoft 365, AWS, and identity providers. Policies should dynamically assess user identity, device posture, location, and risk signals before granting access. This mitigates credential abuse and lateral movement following initial access. Conditional access policies should also enforce regular multi-factor authentication (MFA) refresh for all users. At a minimum, QCTI recommends MFA to be refreshed every 2-3 days for all users, and every 8 hours for users/accounts with admin privileges.

✓ Limit the use of multiple browsers

Limit browser usage across the business to one or two browsers maximum. By limiting how many different browsers are in use, a business can reduce the amount of exposure from browser-based vulnerabilities. Additionally, many stealware variants specifically target a chosen browser, so by limiting browser diversity a company can mitigate stealware opportunity.

✓ Deploy phishing-resistant MFA

Adopt phishing-resistant MFA methods such as FIDO2 security keys or device-bound passkeys, particularly for privileged and high-risk accounts. Legacy methods like short message service (SMS) or app-based one-time passwords (OTPs) are increasingly vulnerable to adversary-in-the-middle (AiTM) and MFA fatigue attacks.

By implementing these measures, organisations can substantially reduce their attack surface and improve resilience against both opportunistic and targeted threat actors exploiting the increasingly sophisticated cybercriminal ecosystem.

Global Cyber Risk Outlook Report

2025 Conclusion

As we progress through 2025, the cyber security landscape remains highly complex and rapidly evolving. The interplay of geopolitical tensions, technological advancements, and human ingenuity is reshaping the digital landscape at an unprecedented pace. This requires a fundamental shift towards adaptive defence strategies that leverage threat intelligence to anticipate and neutralise threats before they materialise.

About Quorum Cyber

Founded in Edinburgh in 2016, Quorum Cyber is one of the fastest-growing cyber security companies in the UK and North America with over 400 customers on four continents. Its mission is to help good people win and it does this by defending teams and organisations across the world and all industry sectors against the rising threat of cyber-attacks, enabling them to thrive in an increasingly hostile, unpredictable, and fast-changing digital landscape. Quorum Cyber is a Microsoft Solutions Partner for Security, a member of the Microsoft Intelligent Security Association (MISA), and the 2025 Microsoft Security MSSP of the Year.

Find Out More

Every organisation faces unique cyber security challenges. Our range of managed security services and incident response services are designed to defend and protect organisations wherever they are on their security journey.

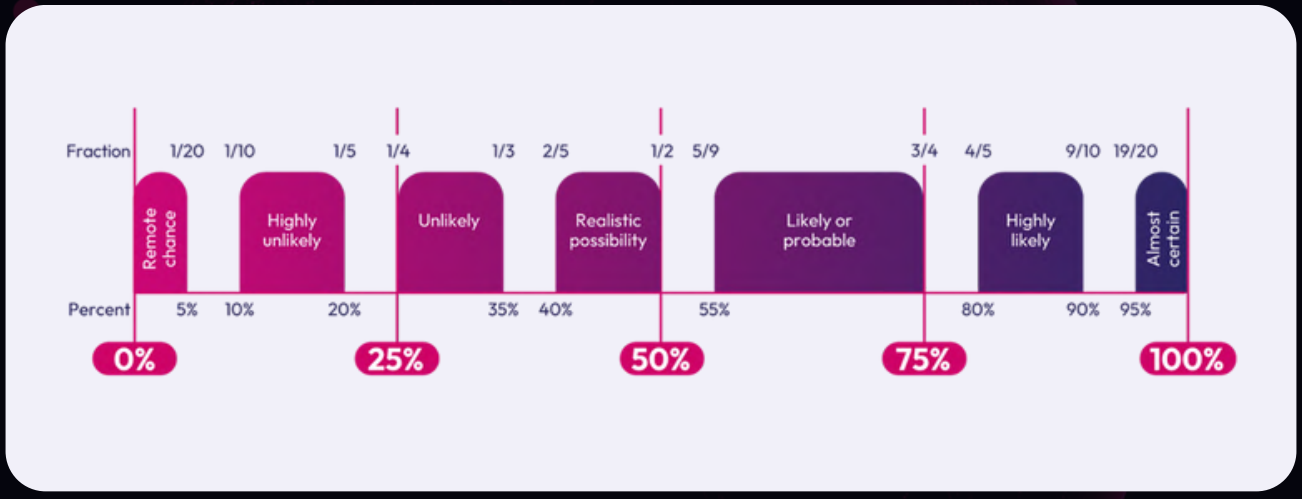
For further information or to discuss how Quorum Cyber can protect your organisation, please visit our website or get in touch with us via info@quorumcyber.com

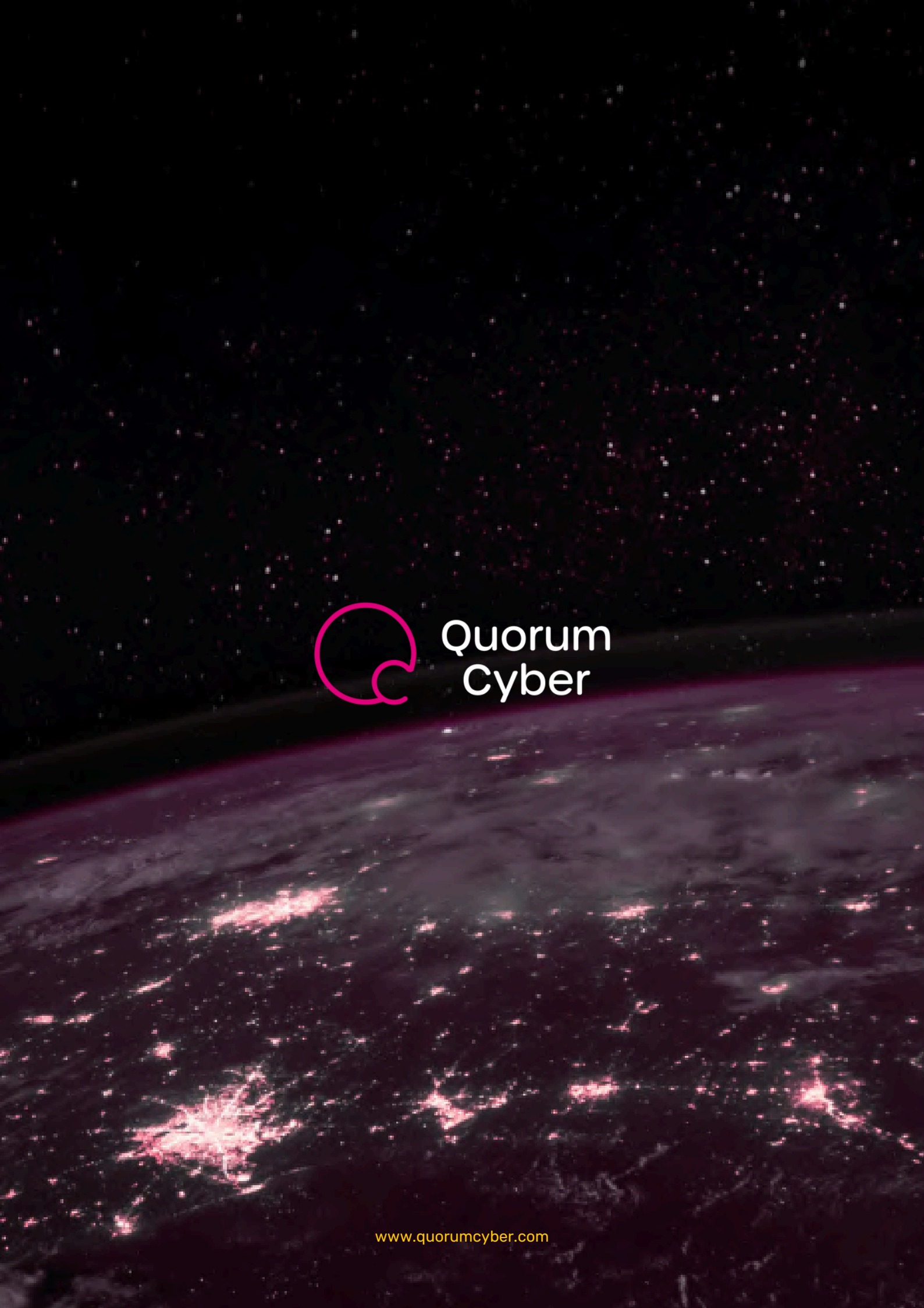
Appendix – Terminology Yardstick

Intelligence Terminology Yardstick

Key assessments within this report have been written using the Intelligence Terminology Yardstick. The assessed likelihood of events corresponds with pre-defined language to remove areas of uncertainty when ingesting Quorum Cyber Intelligence reports.

Intelligence Cut-off Date (ICoD): 16/07/2025 10:00 UTC





www.quorumcyber.com