ZEROFOX INTELLIGENCE

Assessment

Q2 2025 Ransomware Wrap-up

A-2025-07-29a

Classification: TLP:CLEAR

Criticality: Low

Intelligence Requirements: Ransomware, Digital Extortion, Threat Actor

July 29, 2025

Scope Note

ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot always be independently verified. As such, ZeroFox applies rigorous analytic standards and tradecraft in accordance with best practices and includes caveat language and source citations to clearly identify the veracity of our Intelligence reporting and substantiate our assessments and recommendations. All sources used in this particular Intelligence product were identified prior to 7:00 AM EDT on July 29, 2025; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

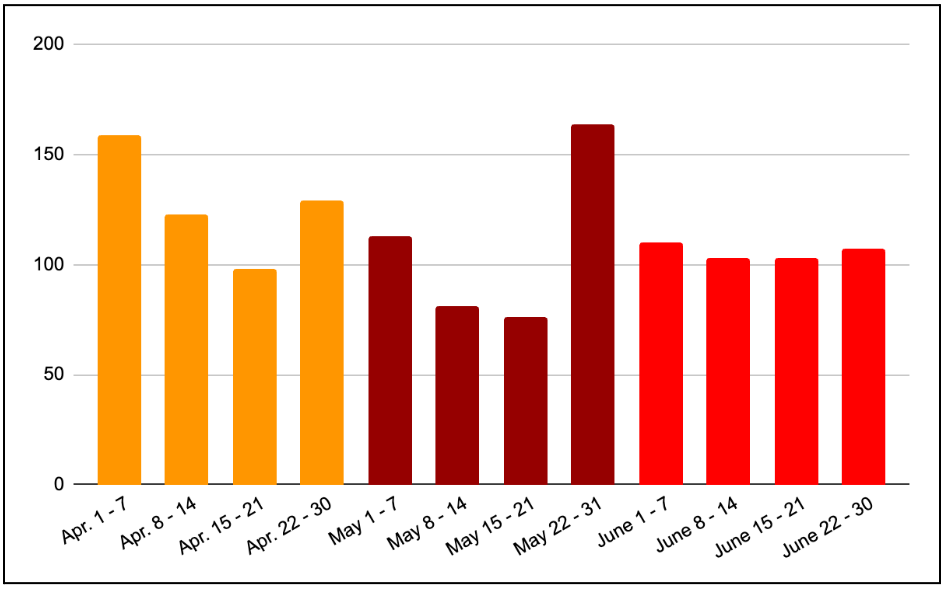
| Assessment | Q2 2025 Ransomware Wrap-up

| Key Findings

- ZeroFox observed at least 1,366 separate ransomware and digital extortion (R&DE) incidents during Q2 2025—a drop of approximately 30 percent from the record-breaking 1,961 incidents observed during the first quarter of the year.
- North America-based organizations were the most targeted by a substantial margin, accounting for approximately 57 percent of all incidents. This is consistent with the 58 percent average observed throughout 2024 and a slight decrease from the 66 percent observed in Q1 2025.
- During Q2 2025, organizations in the manufacturing industry were targeted by more R&DE incidents than those in other industries, experiencing a total of at least 33 attacks. Approximately 19 percent of all R&DE incidents targeted entities in the manufacturing industry during Q2 2025, a slight decrease from the approximately 21 percent observed during Q1 2025.
- The five most active R&DE collectives ZeroFox observed during Q2 2025 were almost certainly Qilin, Play, Akira, SafePay, and INC Ransom. This is a notably different picture from the first quarter of 2025; only two of those same five collectives appear on both lists (Qilin and Akira).

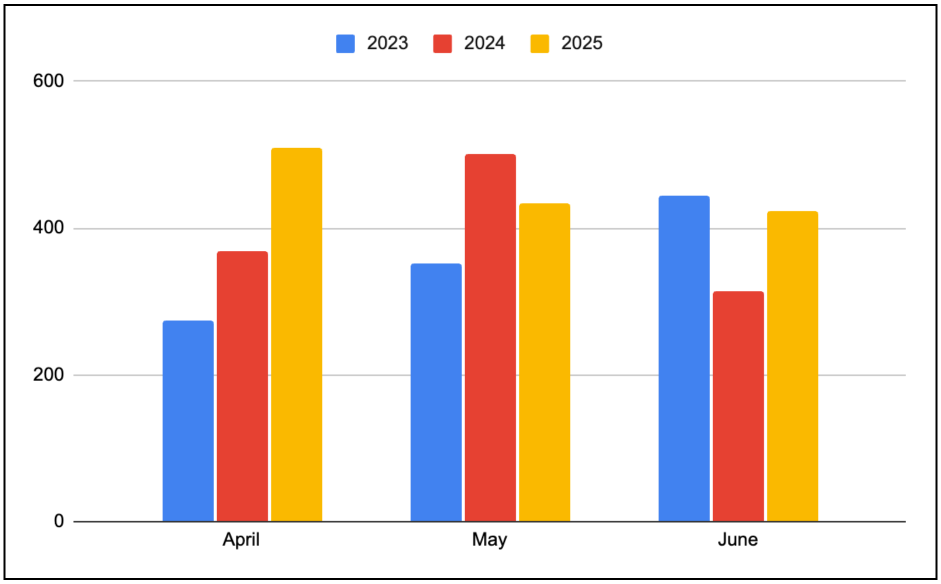
Q2 2025 Overview

ZeroFox observed at least 1,366 separate R&DE incidents during Q2 2025—a drop of approximately 30 percent from the record-breaking 1,961 incidents observed during the first quarter of the year. However, Q2 2025 marked an increase of incidents compared with the same time periods in 2024 and 2023, which accounted for at least 1,184, and 1,070 incidents, respectively. Both 2023 and 2024 saw Q1 comprising the lowest number of quarterly attacks and Q4 having the highest number.



Q2 2025 R&DE incidents by week

Source: ZeroFox Intelligence

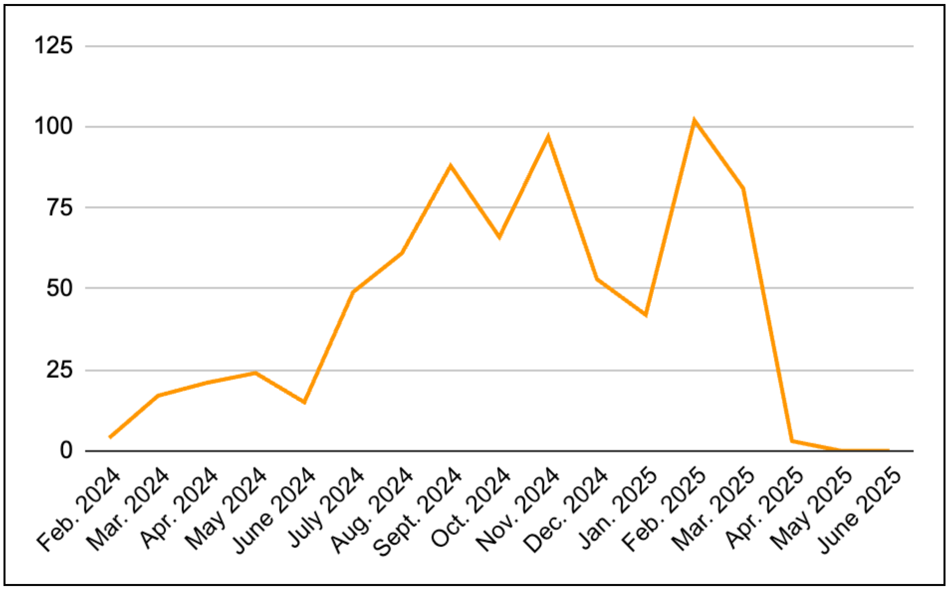


Q2 R&DE incidents 2023–2025

Source: ZeroFox Intelligence

The decrease in global R&DE incidents during Q2 2025 is very likely due in part to the cessation of the well-known ransomware-as-a-service (RaaS) collective RansomHub. In Q1 2025, RansomHub conducted at least 225 R&DE incidents, accounting for approximately 12 percent of all incidents. In Q2 2025, the collective accounted for approximately three attacks, representing 0.2 percent of global incidents. The collective's dark web victim leak site has been offline since April 1, 2025, and no new victims have since been observed.

- RansomHub had been conducting an average of approximately 19 attacks per week throughout Q1 2025, with February seeing more incidents than any other month (approximately 102).

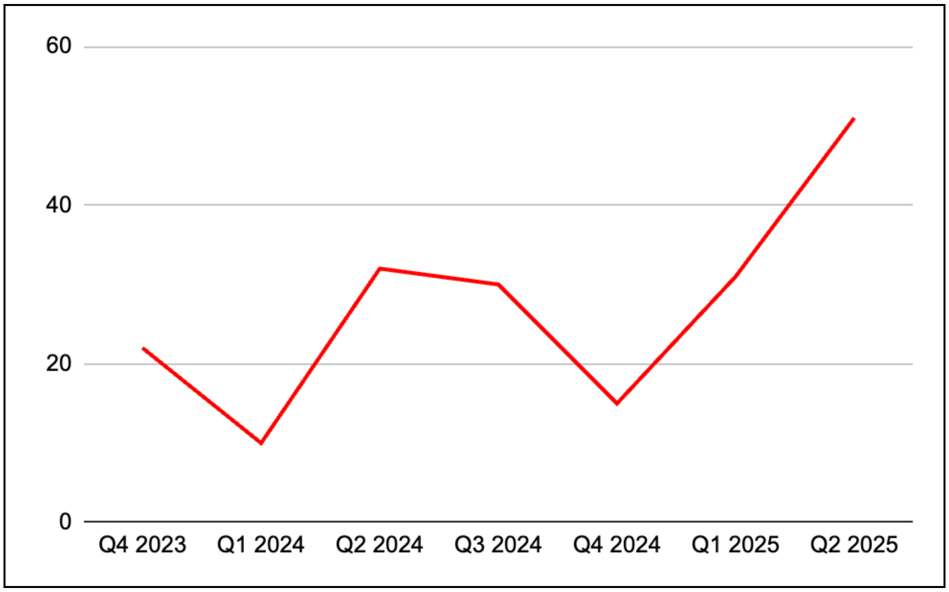


RansomHub attacks by month

Source: ZeroFox Intelligence

At the beginning of Q2 2025 (around April 4, 2025), an account associated with the R&DE collective DragonForce posted in the Russian-language dark web forum RAMP claiming that RansomHub "will be up soon" and that the collective had decided to move to DragonForce's infrastructure. This statement was also posted to the DragonForce[.]onion victim leak page. In a separate post, DragonForce urged RansomHub to "consider their offer" without providing any detail. It is currently unclear whether RansomHub has initiated a collaboration with DragonForce, the extent to which resources would be shared, and what this would mean for the future threat posed by both DragonForce and RansomHub.

- Since first observed in December 2023, DragonForce had maintained a relatively low attack tempo, averaging approximately nine incidents per month. However, ZeroFox observed a significant uptick in activity beginning in early April 2025—leading to the collective's most prominent month, in which the group conducted at least 25 separate attacks.
- In Q2 2025, ZeroFox observed at least 51 incidents attributed to DragonForce—a record high for any three-month period for the collective.



DragonForce attacks by quarter

Source: ZeroFox Intelligence

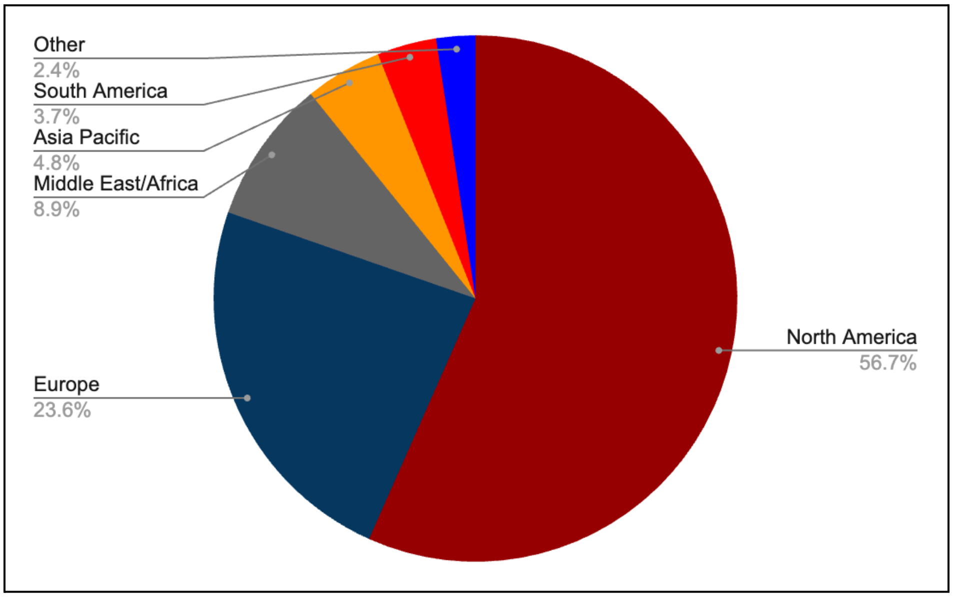
Regional R&DE targeting patterns in the second quarter of 2025 were largely consistent with those observed during previous months. North America-based organizations were the most targeted by a substantial margin, accounting for approximately 57 percent of all incidents. This is consistent with the 58 percent average observed throughout 2024 and a slight decrease from the 66 percent observed in Q1 2025.

- There were at least 1,309 R&DE attacks that targeted North-America based organizations in Q1 2025; the number dropped to 774 attacks in Q2 2025, representing an approximately 41 percent reduction. There was an approximately 30 percent reduction of global R&DE attacks from Q1 2025 to Q2 2025.
- RansomHub was responsible for at least 155 R&DE incidents targeting North America-based organizations in Q1 2025, whereas the group was responsible for just two in Q2 2025. The cessation of RansomHub likely accounts for the approximately 12 percent decline of attacks targeting North-America based organizations.

Europe-based organizations were the second-most targeted region in Q2 2025, accounting for approximately 24 percent of all incidents. This is a slight increase from the approximately 18 percent observed in Q1 2025 and the 19 percent observed in Q4 2024. Together, North-American and Europe-based organizations accounted for approximately 80 percent of all R&DE incidents observed during Q2 2025, which is largely consistent with other quarters.

R&DE collectives typically operate opportunistically, with targeting patterns largely influenced by the availability of network access sold or advertised across deep and dark web (DDW) forums. These patterns are further shaped by the technical capabilities and operational preferences of individual affiliate actors. Nevertheless, North America remains a consistently attractive region and is almost certainly viewed as a target-rich area for lucrative, high-pay-off potential targets.

- The disproportionate targeting of North America-based entities can be partly attributed to the geopolitical motivations and ideological beliefs of financially motivated threat collectives fueled by opposition to “Western” political and social narratives.
- North America hosts a wide variety of robust industries that comprise substantial and fast-growing digital attack surfaces. The widespread integration of technologies like cloud networking services and Internet of Things (IoT) devices contributes to the accessibility of North American assets.

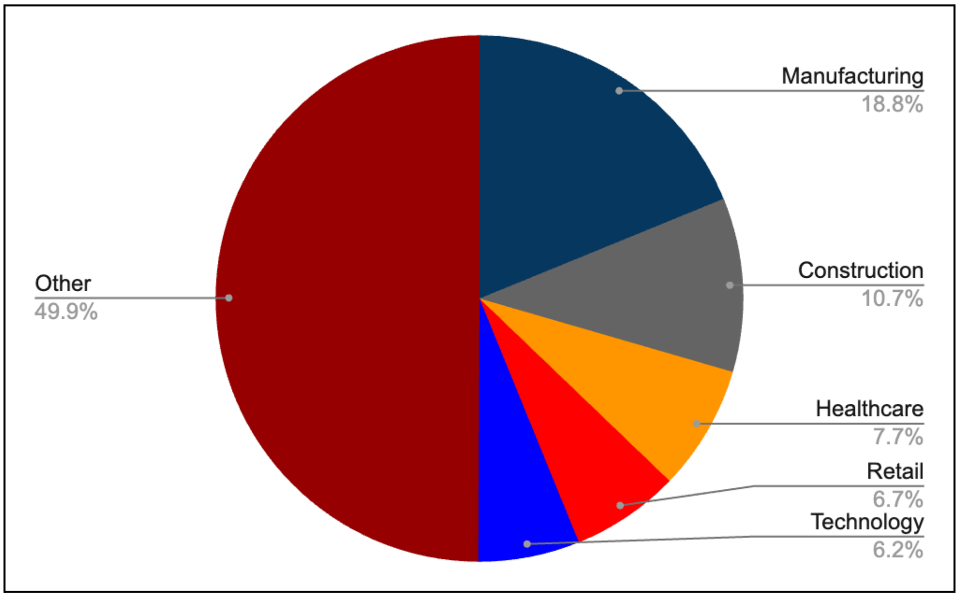


R&DE targeting by region, Q2 2025

Source: *ZeroFox Intelligence*

During Q2 2025, organizations in the manufacturing industry were targeted by more R&DE incidents than those in other industries (totaling at least 33 attacks). Approximately 19 percent of all incidents targeted entities in the manufacturing industry during Q2 2025, a slight decrease from the approximately 21 percent ZeroFox observed during Q1 2025. Manufacturing has consistently been the most targeted industry since at least 2021.

- During Q2 2025, organizations operating within the manufacturing industry continued to represent high-value targets for R&DE collectives. This sustained targeting is likely driven by factors such as low operational tolerance for downtime and the use of vulnerable operational technology (OT) infrastructure behind automation efforts.
- Other industries heavily targeted during Q2 2025 include construction, healthcare, retail, and technology; together with manufacturing, attacks on these industries accounted for approximately 50 percent of all incidents.

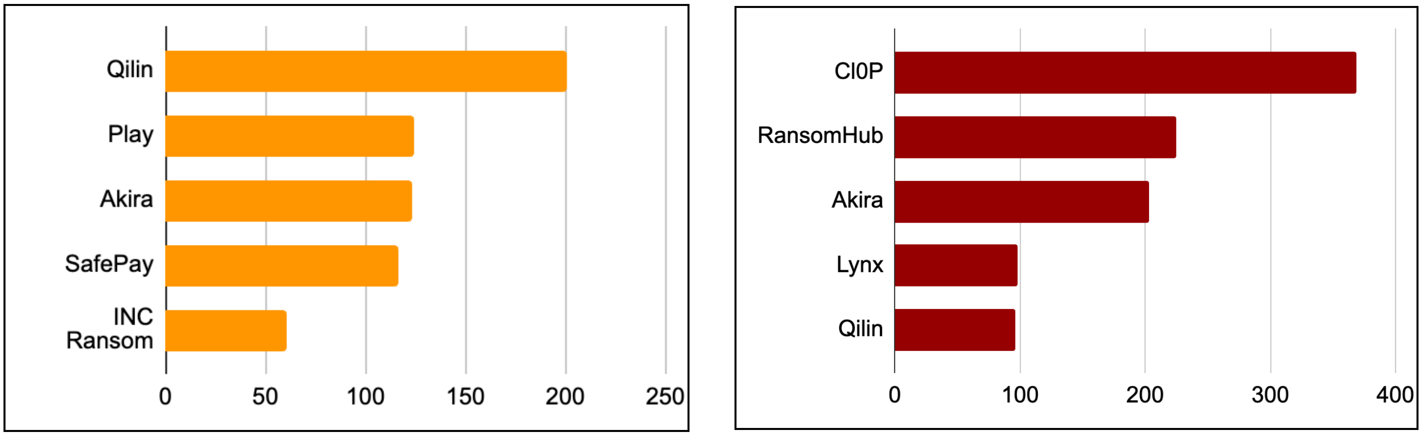


Top five most-targeted industries, Q2 2025

Source: ZeroFox Intelligence

Prominent Collectives

The five most active R&DE collectives ZeroFox observed during Q2 2025 were almost certainly Qilin, Play, Akira, SafePay, and INC Ransom. This is a notably different picture from the first quarter of 2025; only two of those same five collectives appear on both lists (Qilin and Akira). Together, these five collectives accounted for approximately 47 percent of all global R&DE attacks in Q2 2025. In comparison, the top five most prominent collectives for Q1 2025 accounted for approximately 50 percent of all global R&DE attacks. During Q2 2025, 18 collectives accounted for approximately 75 percent of all global R&DE attacks, which is slightly higher than the 13 collectives that accounted for the same percentage in Q1 2025 and equals the 18 observed in Q4 2024.



Top five most-prominent R&DE collectives during Q2 2025 (left) and Q1 2025 (right)

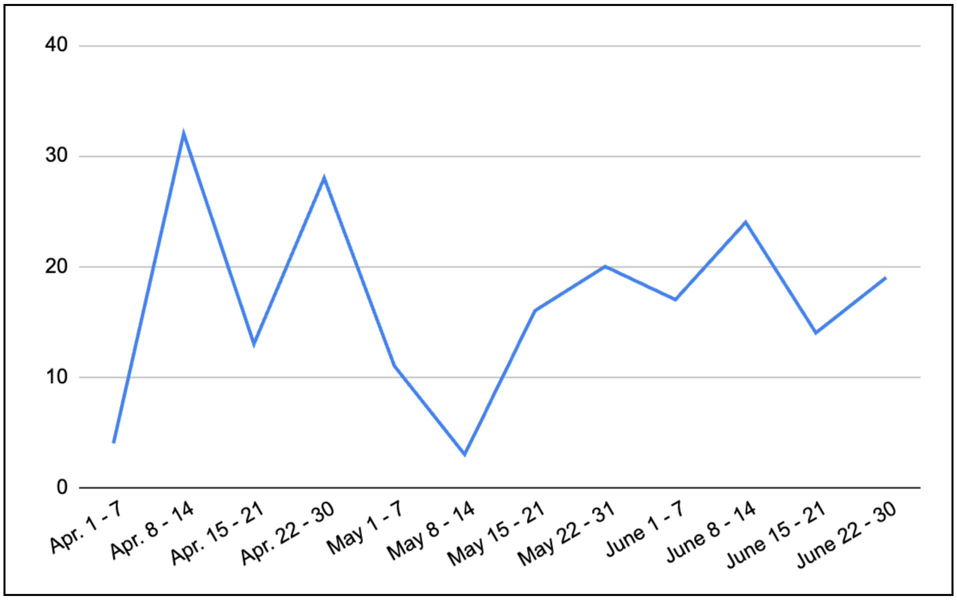
Source: ZeroFox Intelligence

Qilin

During Q2 2025, Qilin was responsible for at least 201 separate attacks, accounting for approximately 15 percent of all incidents—more than any other collective. Notably, Qilin was the fifth most prominent R&DE collective during Q1 2025, with approximately 106 incidents; the group demonstrated nearly twice as many incidents in Q2 2025, despite the overall global decrease of R&DE attacks.

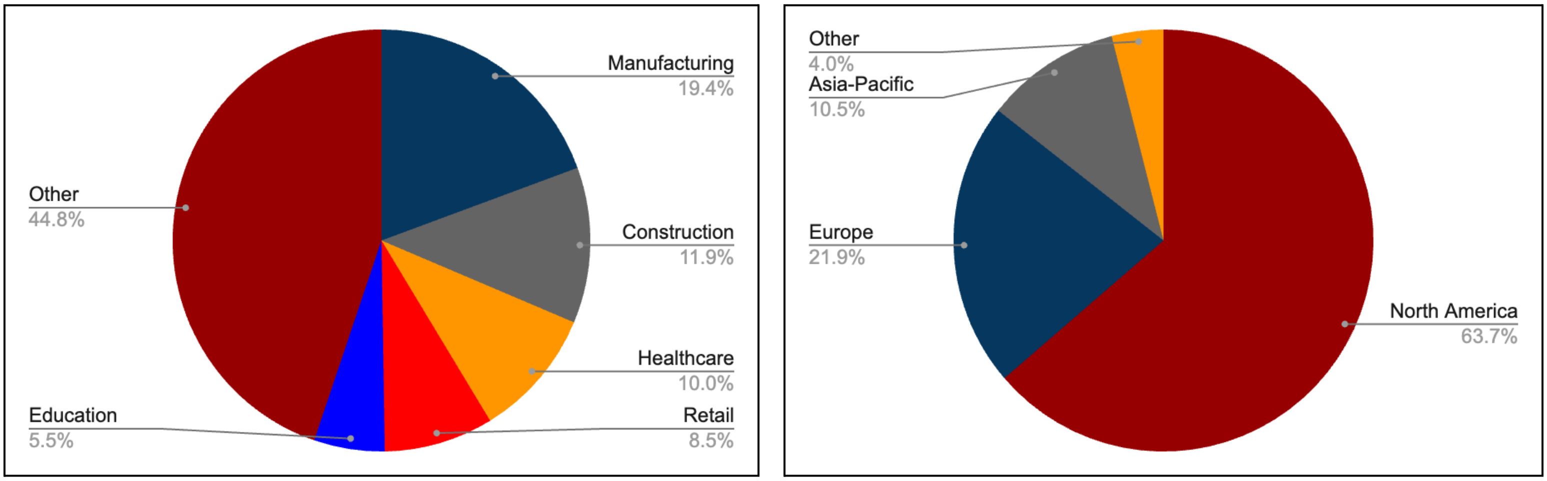
- During Q2 2025, Qilin disproportionately targeted North America-based organizations, which represented approximately 64 percent of the collective's victims and is slightly higher than the approximately 57 percent ZeroFox observed across the global R&DE landscape.

- Qilin's operational tempo began to increase significantly from Q4 2024, when the collective conducted at least 46 incidents. This continued through Q1 2025, which saw the group responsible for at least 106 incidents, and Q2 2025, when the collective accounted for a total of at least 201 incidents. It is likely that Qilin will remain one of the most prominent collectives in Q3 2025, maintaining its current attack tempo.



Qilin attacks by week, Q2 2025

Source: ZeroFox Intelligence



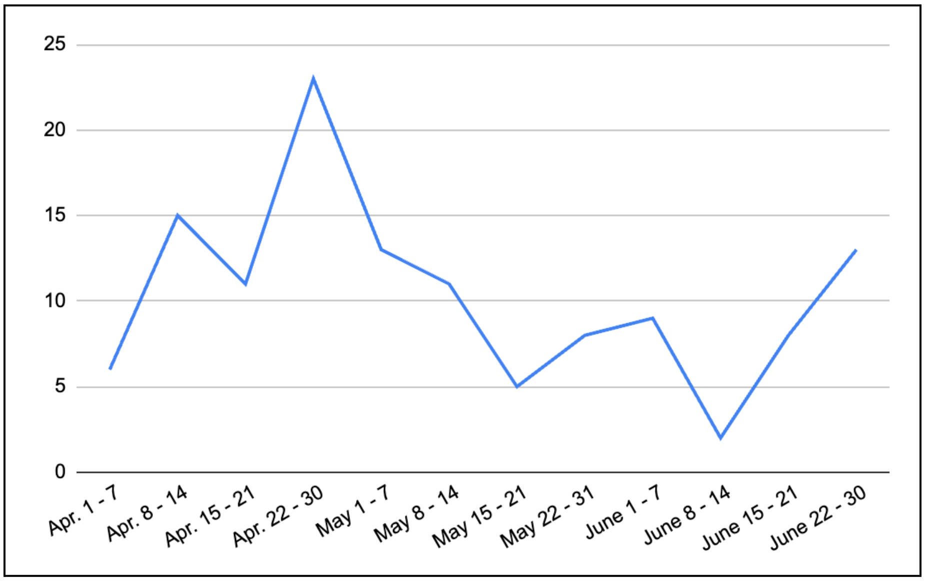
Qilin's most-targeted industries (left) and regions (right), Q2 2025

Source: ZeroFox Intelligence

Play

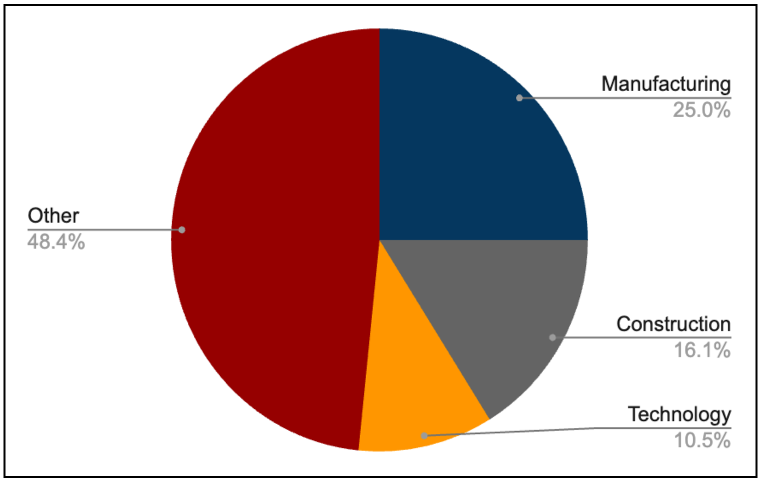
During Q2 2025, Play was the second most active collective and responsible for at least 124 attacks, accounting for approximately 9 percent of all global R&DE incidents; this is largely consistent with previous quarters ZeroFox has observed. Notably, Play's total number of incidents increased from 90 in Q1 2025 to 124 in Q2 2025, despite the overall global decrease of R&DE attacks.

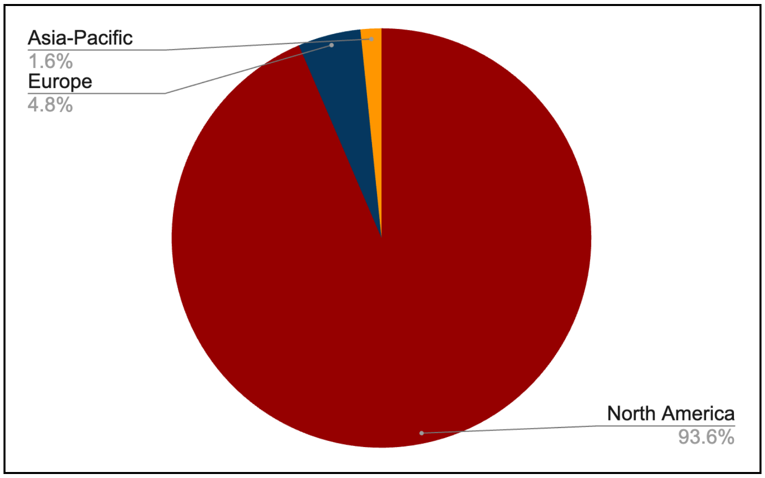
- Play has disproportionately targeted North America-based organizations in comparison to other collectives since at least Q3 2023; this reached a record high in Q2 2025, when the collective accounted for approximately 94 percent of the region's targeting. This is very likely reflective of its affiliates' tactics, techniques, and procedures (TTPs), which prioritize regions assessed as more likely to yield higher ransom payments. It is unlikely that the current proportion of high-value regional targeting will significantly increase, as this would require collectives to deliberately exclude potentially lucrative, opportunistic targets—unlikely for a financially motivated collective.
- The majority of Play's incidents targeted the manufacturing, construction, and technology industries, which accounted for approximately 25, 16, and 11 percent of its Q2 2025 attacks, respectively.



Play attacks by week, Q2 2025

Source: ZeroFox Intelligence





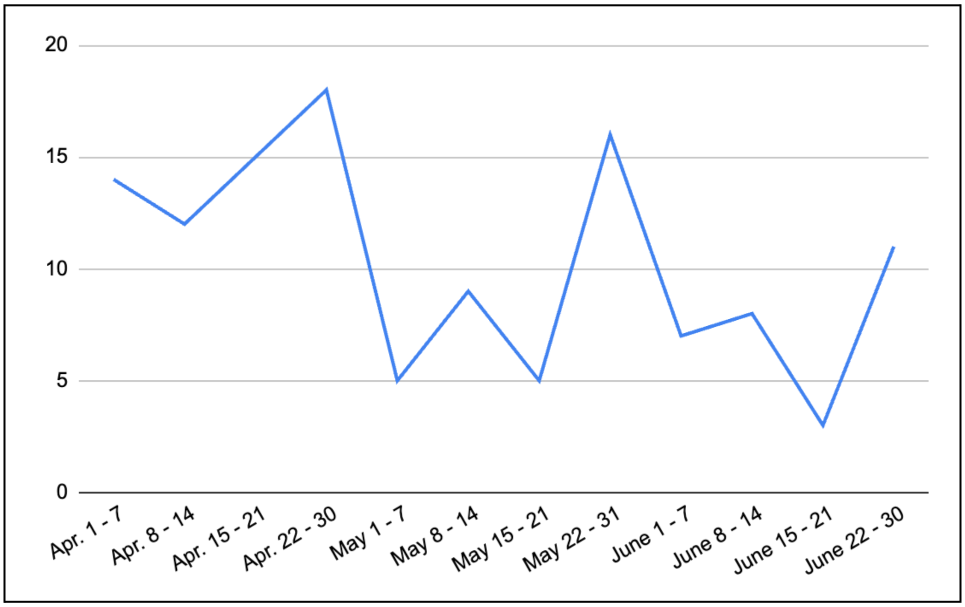
Play's most-targeted industries (left) and regions (right), Q2 2025

Source: ZeroFox Intelligence

Akira

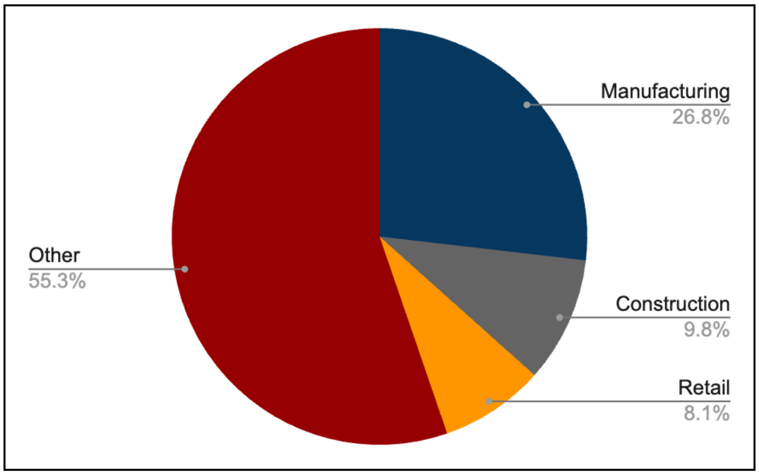
During Q2 2025, Akira was responsible for at least 123 separate attacks, accounting for approximately 9 percent of global R&DE incidents and making it the third most active collective for this period. Notably, Akira's total number of incidents decreased from 203 attacks in Q1 2025 to 123 attacks in Q2 2025; this is a 39 percent drop and above the overall 30 percent global decrease of R&DE attacks in this time frame.

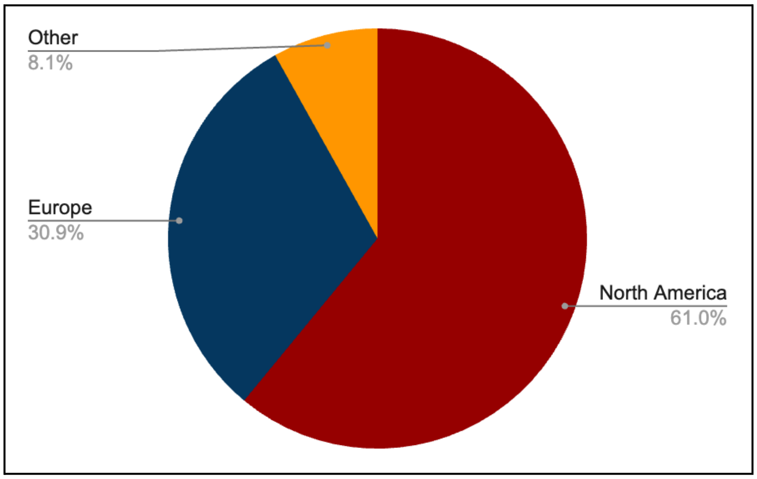
- Organizations in North America accounted for approximately 61 percent of all attacks attributed to Akira in Q2 2025, which is slightly above the approximately 57 percent average observed across the global R&DE landscape.
- Similarly, organizations in Europe accounted for approximately 31 percent of all attacks attributed to Akira during Q2 2025, slightly above the approximately 24 percent average of global R&DE attacks targeting the region.
- Manufacturing , construction, and retail were the most targeted industries during this period by Akira ransomware, accounting for approximately 27, 10, and 8 percent of the incidents, respectively. These have been consistently the industries most targeted by Akira in previous quarters.



Akira attacks by week, Q2 2025

Source: ZeroFox Intelligence





Akira's most-targeted industries (left) and regions (right), Q2 2025

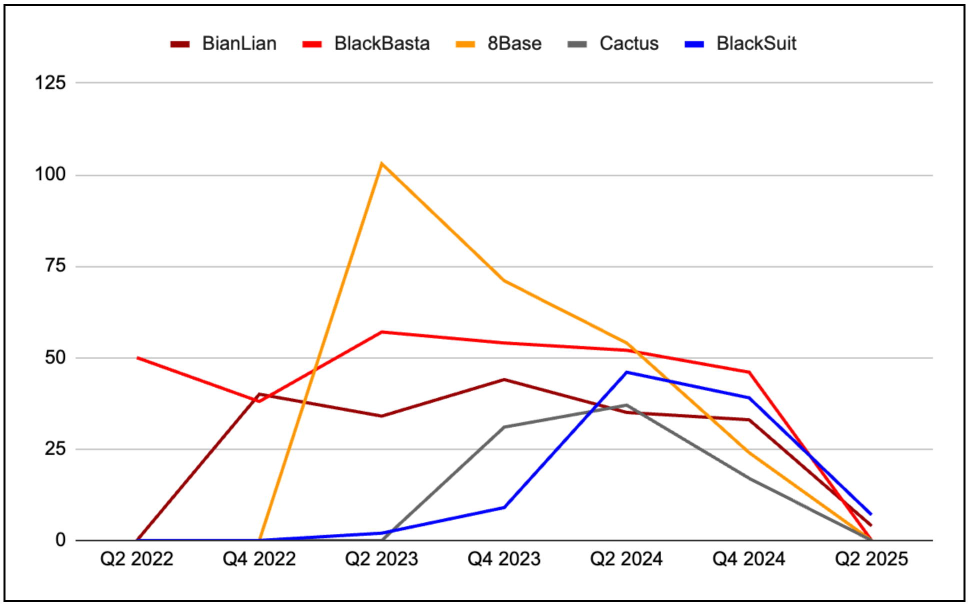
Source: ZeroFox Intelligence

Notable Declines

Following the cessation of RansomHub, ZeroFox has observed several collectives (BianLian, BlackBasta, 8Base, Cactus, and BlackSuit) demonstrate significantly less activity in Q2 2025 in comparison to previous quarters. While an array of factors have contributed to this, there is a likely chance that the reduction of activity is due to varying levels of operational security (OpSec) concerns within the collectives. It is not uncommon for RaaS collectives to take several months off and then resurface or rebrand themselves—both of which are likely efforts to quell pressure from law enforcement (LE).

- ZeroFox first observed BianLian in Q3 2022; the collective maintained a relatively consistent tempo, averaging approximately 30 attacks per quarter. However, this dropped significantly to just four attacks in Q2 2025. Both Q1 2023 and Q3 2023 saw similar significant drops in BianLian activity before the collective returned to normal levels of operational output.
- We first observed BlackBasta in Q2 2022; the group maintained a consistent tempo until Q4 2024, averaging approximately 47 attacks per quarter. However, this dropped significantly to just nine attacks in Q1 2025 and none in Q2 2025. ZeroFox assesses BlackBasta is unlikely to resurface using the same name.
- ZeroFox first observed 8Base in Q2 2023. The group has exhibited a decreasing tempo each quarter since then; it started with approximately 103 attacks, dropped down to zero in Q3 2024, and then reappeared with 24 and 22 attacks Q4 2024 and Q1 2025, respectively. However, 8Base accounted for zero attacks in Q2 2025.
- We first observed Cactus in Q3 2023; the collective has maintained a consistent tempo since, averaging approximately 33 attacks per quarter. Cactus accounted for the most attacks in Q1 2025 with 49; however, its activity dropped significantly to zero attacks in Q2 2025, and it is likely Cactus has now ceased as a RaaS collective.
- ZeroFox first observed BlackSuit in Q2 2023; the group exhibited varying levels of operational tempo since, averaging approximately 21 attacks per quarter until Q4 2024. However, this dropped significantly to just two attacks in Q1 2025 and seven attacks in Q2 2025. On July 24, 2025, the home page of BlackSuit's dark web data leak site displayed a message stating that "this site has been seized by U.S. Homeland Security Investigations as part of a coordinated international law enforcement investigation."[1] As of the writing of this report, there have been no public announcements of arrests related to BlackSuit, and it is likely that its members are already seeking to form a new collective.

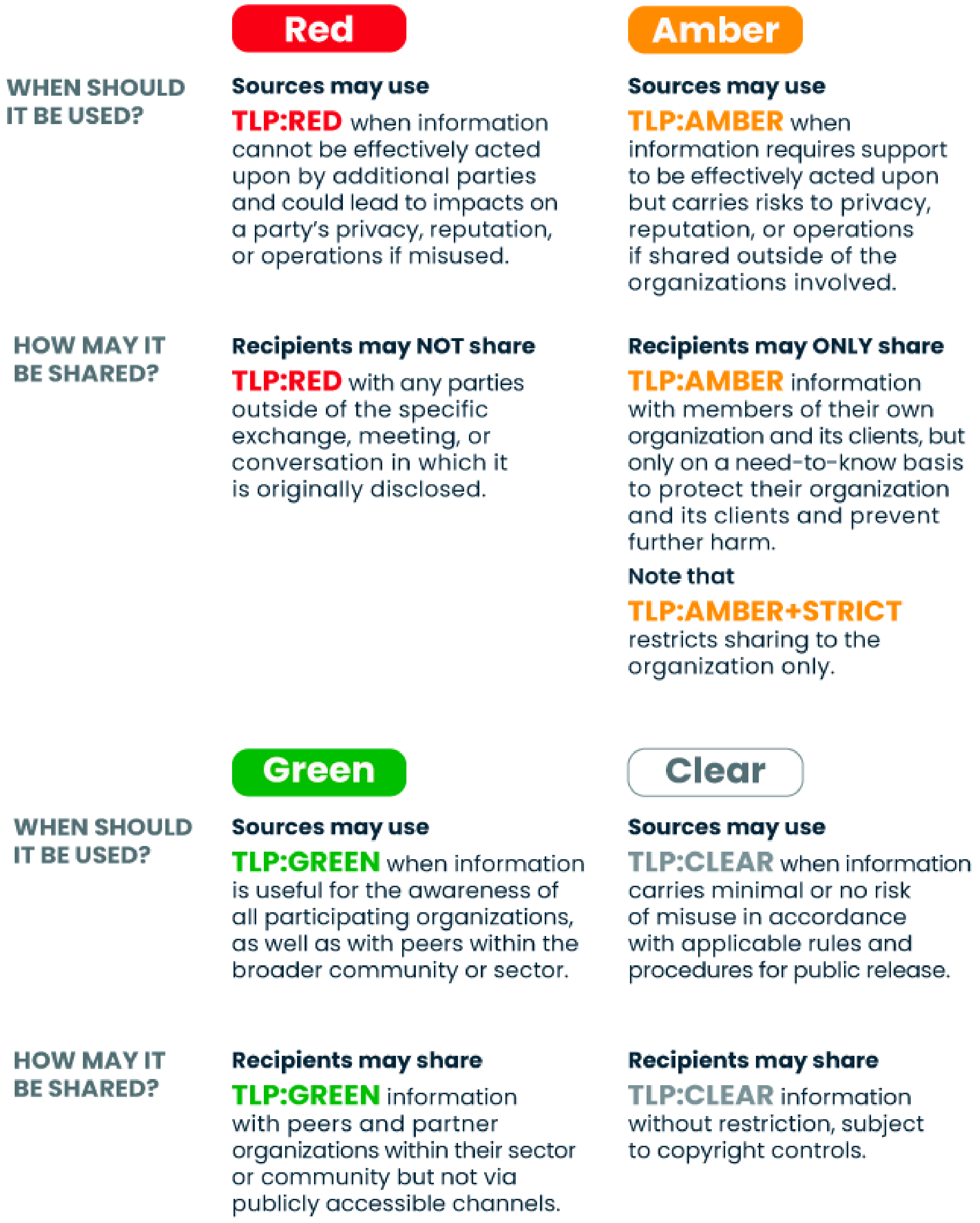
[1] hXXps://www.infosecurity-magazine[.]com/news/blacksuit-ransomware-sites-seized/



Threat collectives' overall decreased activity since Q2 2022

Source: ZeroFox Intelligence

Appendix A: Traffic Light Protocol for Information Dissemination

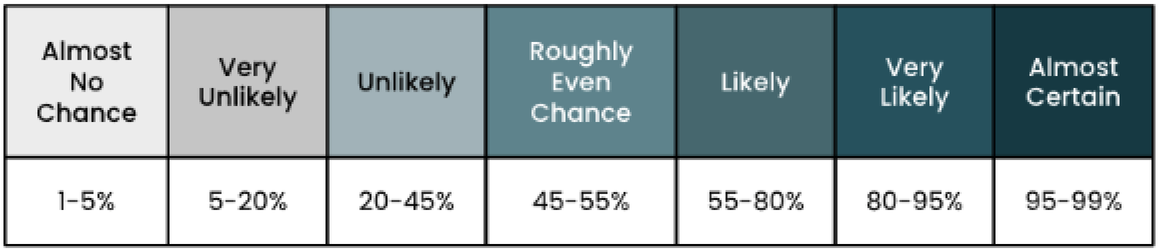


	Red	Amber
WHEN SHOULD IT BE USED?	**Sources may use** **TLP:RED** when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.	**Sources may use** **TLP:AMBER** when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.
HOW MAY IT BE SHARED?	**Recipients may NOT share** **TLP:RED** with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.	**Recipients may ONLY share** **TLP:AMBER** information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm. **Note that** **TLP:AMBER+STRICT** restricts sharing to the organization only.

	Green	Clear
WHEN SHOULD IT BE USED?	**Sources may use** **TLP:GREEN** when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.	**Sources may use** **TLP:CLEAR** when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.
HOW MAY IT BE SHARED?	**Recipients may share** **TLP:GREEN** information with peers and partner organizations within their sector or community but not via publicly accessible channels.	**Recipients may share** **TLP:CLEAR** information without restriction, subject to copyright controls.

Appendix B: ZeroFox Intelligence Probability Scale

All ZeroFox intelligence products leverage probabilistic assessment language in analytic judgments. Qualitative statements used in these judgments refer to associated probability ranges, which state the likelihood of occurrence of an event or development. Ranges are used to avoid a false impression of accuracy. This scale is a standard that aligns with how readers should interpret such terms.



Almost No Chance	Very Unlikely	Unlikely	Roughly Even Chance	Likely	Very Likely	Almost Certain
1-5%	5-20%	20-45%	45-55%	55-80%	80-95%	95-99%