



## | Brief |

# Ransomware Threat Landscape Continues to Diversify in 2024

F-2024-04-23a

Classification: TLP:CLEAR

Criticality: Medium

Intelligence Requirements: Ransomware, Deep & Dark Web

**April 23, 2024**

**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 12:00 PM (EDT) on April 22, 2024**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

## **Brief** | Ransomware Threat Landscape Continues to Diversify in 2024

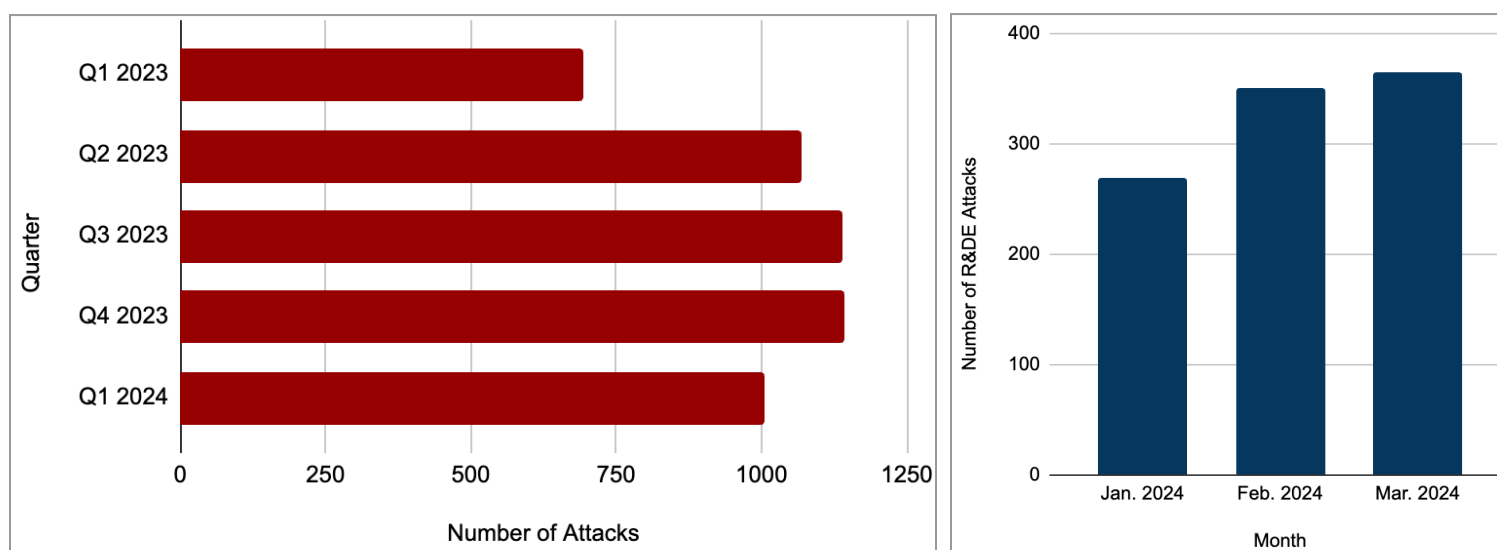
### ➤ Key Findings

- The frequency of ransomware and digital extortion (R&DE) attacks is on an upward trajectory, with the number of observed incidents during Q1 2024 only slightly less than that of the previous quarter—despite Q4 2023 constituting more attacks than any other quarter observed by ZeroFox.
- So far in 2024, the five most active collectives have been responsible for a continually decreasing proportion of total R&DE activity. This is indicative of a growing number of highly active threat groups, many of which are exhibiting an upward trajectory in their attack frequency.
- Several smaller threat groups, such as DarkVault, DragonForce, MyData, and Red, have displayed high attack tempos, which are historically atypical for newer collectives. It is very likely that such groups are benefitting from the acquisition of experienced affiliates from LockBit and ALPHV.
- It is likely that the R&DE threat landscape will continue to diversify during the coming months, with an increasing number of threat collectives conducting a growing proportion of total activity.

## Details

The frequency of R&DE attacks is on an upward trajectory, with the number of observed incidents during Q1 2024 only slightly less than that of Q4 2023. This is despite the first quarter of the year historically seeing significantly lessened activity and ZeroFox observing more attacks during Q4 2023 than in any other quarter on record. Given high levels of R&DE activity during the first part of April, there is a likely chance that Q2 2024 will surpass Q1.

- Reporting suggests that victim refusal to meet ransom demands fell to an all-time low in Q1 2024, indicating a very likely chance that the total number of R&DE attacks was much higher than that observed by ZeroFox.<sup>1</sup>



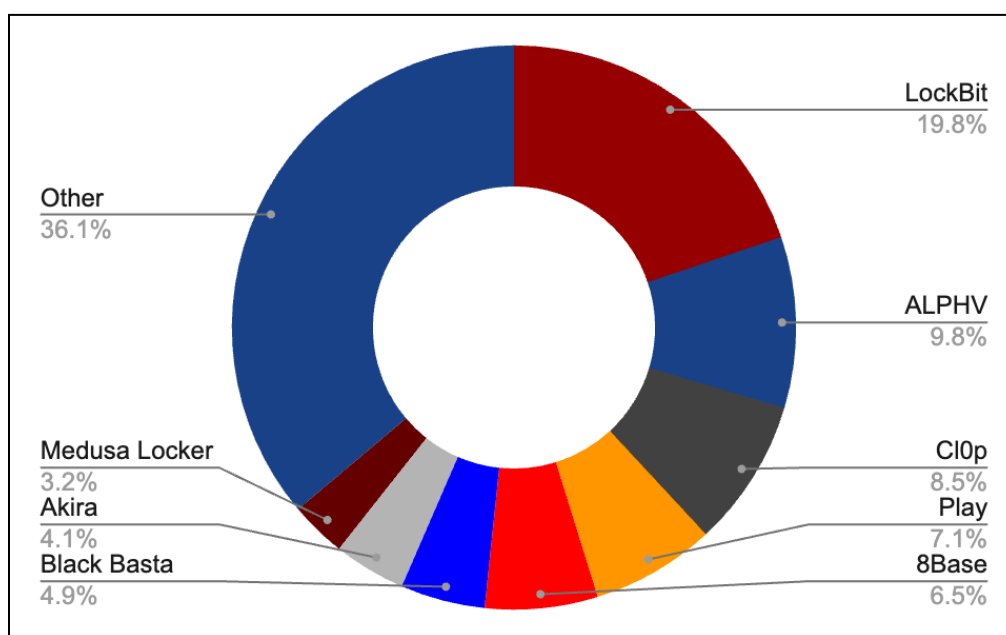
**Total R&DE incidents by quarter and by month**

Source: ZeroFox Intelligence

An increasingly diverse threat landscape is contributing to the high number of incidents, with a large, growing number of collectives responsible for attacks. This is being propelled in part by several smaller and newer collectives becoming significantly more active.

<sup>1</sup> [hXXps://www.coveware\[.\]com/blog/2024/4/17/raas-devs-hurt-their-credibility-by-cheating-affiliates-in-q1-2024](https://www.coveware[.]com/blog/2024/4/17/raas-devs-hurt-their-credibility-by-cheating-affiliates-in-q1-2024)

- Throughout 2023, the top five most active collectives (LockBit, ALPHV, CI0p, Play, and 8Base) together accumulated a total of at least 2,100 attacks—approximately 52 percent of total R&DE activity.
- So far in 2024, the five most active collectives have been responsible for a continually decreasing proportion of total R&DE activity. Throughout January and February, the most prominent threat groups were LockBit, 8Base, ALPHV, Hunters International, and Akira, which accounted for approximately 47 percent of total activity. This reduced to 41 percent in March and 35 percent so far in April, due primarily to the reduction of LockBit and ALPHV activity.



**Proportion of R&DE activity by threat group, 2023**

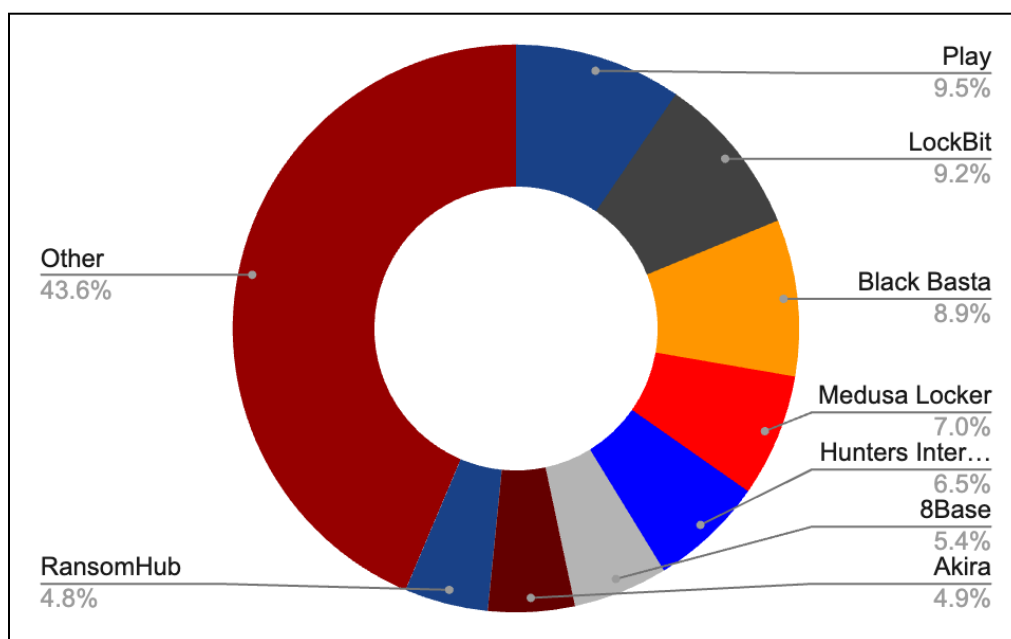
Source: ZeroFox Intelligence

While still conducting comparatively low numbers of attacks, several threat collectives have increased their operational tempo during 2024.

- The number of attacks conducted by BlackSuit have increased each month during 2024, from three in January (accounting for approximately 1 percent of global R&DE) to 13 so far in April (accounting for approximately 7 percent of global R&DE).
- Despite being first observed as recently as February 2024, RansomHub has already conducted at least 35 attacks, displaying a tempo that is atypical for a

newer collective. It is almost certain that RansomHub obtained affiliates from ALPHV following its disruption. This is supported by the addition of technology organization Change Healthcare to the RansomHub victim leak site on April 8, 2024; Change Healthcare had initially been extorted by ALPHV in February 2024.

- Black Basta conducted at least 41 attacks in March 2024—the highest observed in any previous month and significantly higher than its average of 16 monthly since they were first observed in approximately May 2022.
- Medusa Locker conducted at least 60 attacks during February, March, and April 2024, exhibiting an upward trajectory and its most active months on record.
- Hunters International conducted at least 30 attacks in February 2024, accounting for 9 percent of global R&DE activity, and it is likely that this will be surpassed in April 2024. Hunters International has also exhibited a significant operational tempo since it was first observed in Q3 2023.

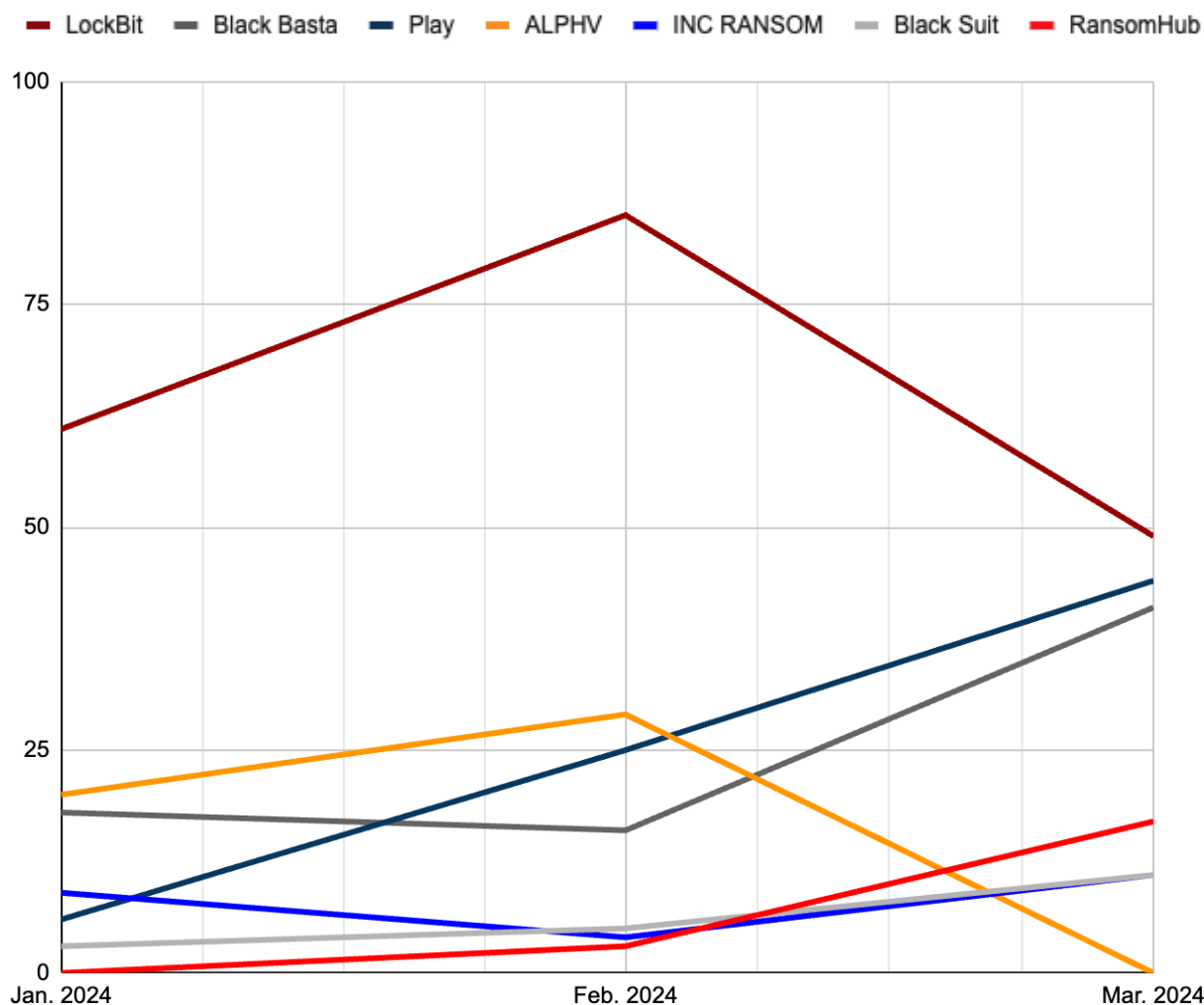


**Proportion of R&DE activity by threat group, March 1 to April 18, 2024**

*Source: ZeroFox Intelligence*

Several smaller R&DE collectives, such as DarkVault, DragonForce, MyData, and Red, have also exhibited notably high attack tempos for relatively new outfits. Like RansomHub, it is very likely that such groups are benefitting from the acquisition of experienced affiliates from LockBit and ALPHV.

Newer threat collectives are likely to continue exhibiting upward attack trajectories as their efficacy increases, their services and reputation become established in DDW forums, and they are able to garner new and experienced affiliates.



**Trajectory of attacks by R&DE threat group**

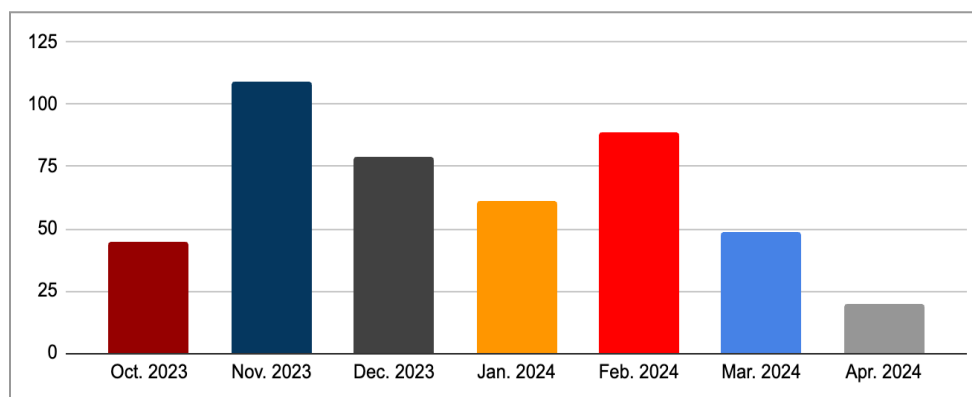
*Source: ZeroFox Intelligence*

The two most prominent threat groups of 2023, ALPHV and LockBit, have been conducting a smaller proportion of total R&DE activity each month following their disruption by law enforcement (LE) entities in December 2023 and February 2024, respectively.

In the weeks following LockBit's disruption, the group continued to upload significant numbers of victims to its leak site. It is almost certain that the majority of these were

associated with extortion operations that were ongoing at the time of the LE disruption of the collective's digital infrastructure.

- LockBit's proportion of monthly R&DE activity peaked in February 2023, at over 50 percent of observed attacks. This reduced to 22 percent in February 2024 and stands at just 3 percent so far in April 2024.



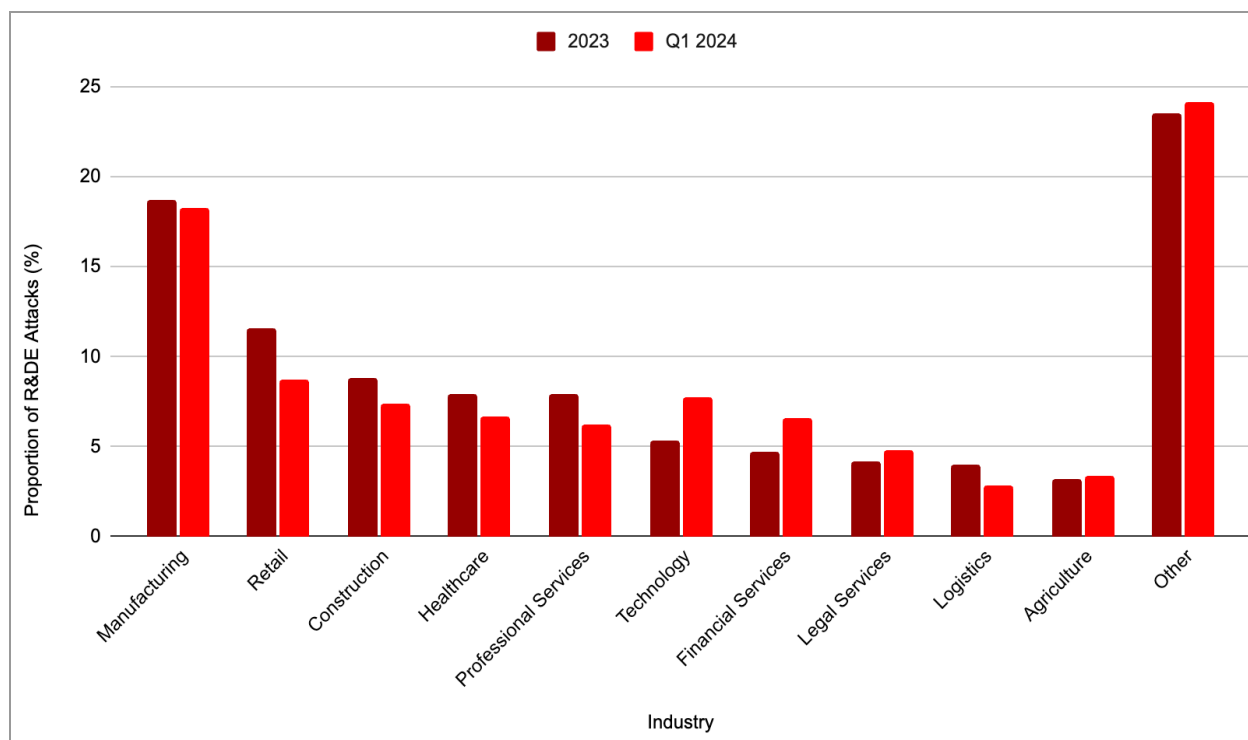
**LockBit attacks, October 2023 to April 18, 2024**

*Source: ZeroFox Intelligence*

There is a roughly even chance that LockBit's attack tempo will increase throughout 2024, as the collective attempts to recover digital infrastructure and attract new affiliates. However, the group is very unlikely to reach the heights observed during 2023 due to the damage inflicted upon its reputation in DDW forums, the release of a decryption tool, and the continued LE scrutiny that is likely deterring affiliates.

- LockBit's continued—albeit reduced—tempo is being enabled through its [.]onion "LockBit 3.0" leaksite, which continues to list both new victims and those from before LE disruption.

ALPHV was responsible for approximately 10 percent of all R&DE attacks from January 2023 up until its December LE disruption. This reduced to 4 percent during Q1 2024, with no incidents being observed so far in April. It is likely that the damage to ALPHV's digital infrastructure and the significant loss of affiliates will prevent the collective from resuming operations. There is a roughly even chance that senior figures will attempt a rebrand during 2024, though it is very unlikely that recovery will be sufficient to meet the activity levels of 2023.



## R&DE attacks by Industry

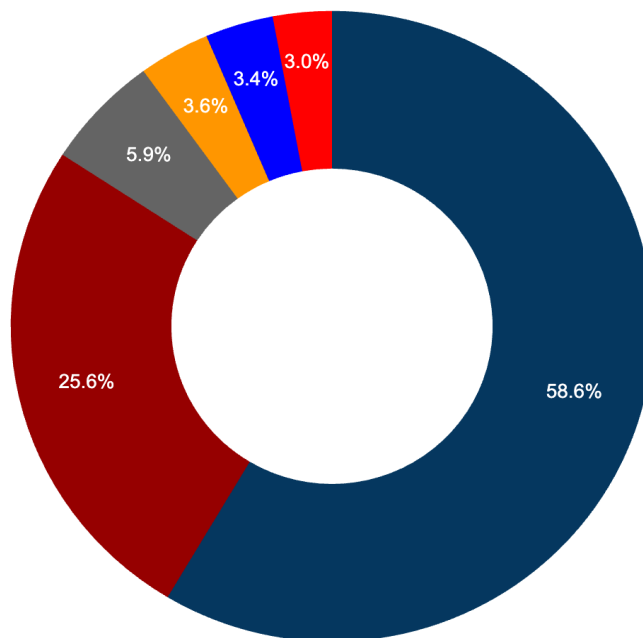
Source: ZeroFox Intelligence

ZeroFox observed very little change in the industries of targeted organizations during Q1 2024. Compared to 2023, small increases were noted in the manufacturing, retail, construction, healthcare, and professional services industries. It is very unlikely that these increases are indicative of new targeting patterns; rather, they are likely the result of expected threat landscape fluctuations.

Manufacturing will very likely remain the most targeted industry over the coming months, though variations will likely be observed as newer and smaller threat collectives establish and adapt their techniques, tactics, and procedures (TTPs).

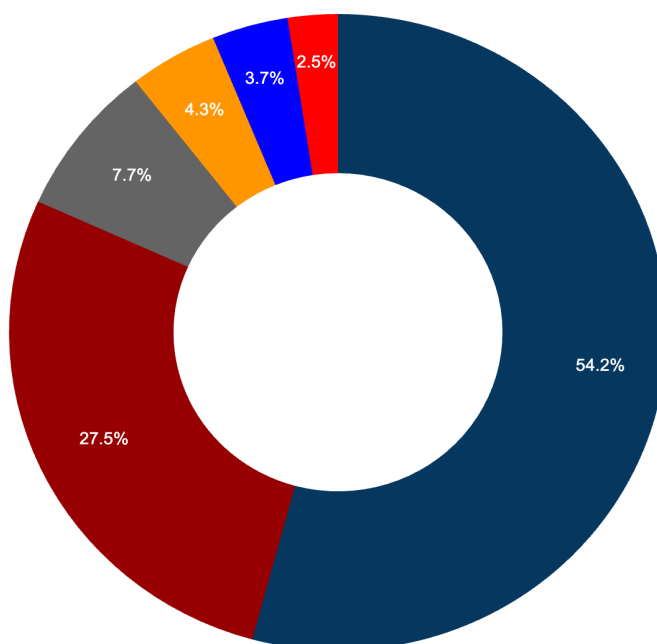
The region of victims also exhibited little variation between 2023 and Q1 2024. Slight increases in the targeting of North America-based organizations are very likely the result of natural fluctuations and not indicative of increased emphasis. North America will almost certainly remain the region most targeted by R&DE attacks over the coming months.

● North America ● Europe ● Asia-Pacific ● South America ● Middle East & Africa ● Australia & New Zealand



**R&DE attacks by region, Q1 2024**

Source: ZeroFox Intelligence



**R&DE attacks by region, 2023**

Source: ZeroFox Intelligence

## **Recommendations**

- Adopt a Zero-Trust cybersecurity posture based upon a principle of least privilege.
- Implement network segmentation to separate resources.
- Implement secure password policies with phishing-resistant multi-factor authentication (MFA), complex passwords, and unique credentials.
- Leverage cyber threat intelligence to inform detection of R&DE threats and their associated TTPs and Indicators of Compromise (IOCs).
- Ensure critical, proprietary, or sensitive data is always backed up to secure, off-site or cloud servers at least once per year—and ideally more frequently.
- Develop a comprehensive incident response strategy.
- Configure email servers to block emails with malicious indicators and deploy authentication protocols to prevent spoofed emails.
- Deploy a holistic patch management system and ensure all business IT assets are updated with the latest software as quickly as possible.
- Proactively monitor for compromised accounts being brokered in DDW forums.
- Configure ongoing monitoring for Compromised Account Credentials.

## Appendix A: Traffic Light Protocol for Information Dissemination

|                                |                                                                                                                                                                                                        |                                                                                                                                                                                                                                                                                                                              |
|--------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                | <b>Red</b>                                                                                                                                                                                             | <b>Amber</b>                                                                                                                                                                                                                                                                                                                 |
| <b>WHEN SHOULD IT BE USED?</b> | <b>Sources may use</b><br><b>TLP:RED</b> 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. | <b>Sources may use</b><br><b>TLP:AMBER</b> when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.                                                                                                           |
| <b>HOW MAY IT BE SHARED?</b>   | <b>Recipients may NOT share</b><br><b>TLP:RED</b> with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.                                     | <b>Recipients may ONLY share</b><br><b>TLP:AMBER</b> 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.<br><b>Note that</b><br><b>TLP:AMBER+STRICT</b> restricts sharing to the organization only. |
|                                | <b>Green</b>                                                                                                                                                                                           | <b>Clear</b>                                                                                                                                                                                                                                                                                                                 |
| <b>WHEN SHOULD IT BE USED?</b> | <b>Sources may use</b><br><b>TLP:GREEN</b> when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.              | <b>Sources may use</b><br><b>TLP:CLEAR</b> when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.                                                                                                                                                      |
| <b>HOW MAY IT BE SHARED?</b>   | <b>Recipients may share</b><br><b>TLP:GREEN</b> information with peers and partner organizations within their sector or community but not via publicly accessible channels.                            | <b>Recipients may share</b><br><b>TLP:CLEAR</b> 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%         |