Introduction

2024 has started out with the highest number of January attacks we've ever recorded, with 76 attacks representing a 130% increase compared to 2022's figures. Education topped the list of targeted industries, followed by healthcare and manufacturing. LockBit was the most active ransomware group this month, with Akira knocking BlackCat off the second-place spot for the first time. Notably 91% of disclosed attacks involved data exfiltration.

Roundup

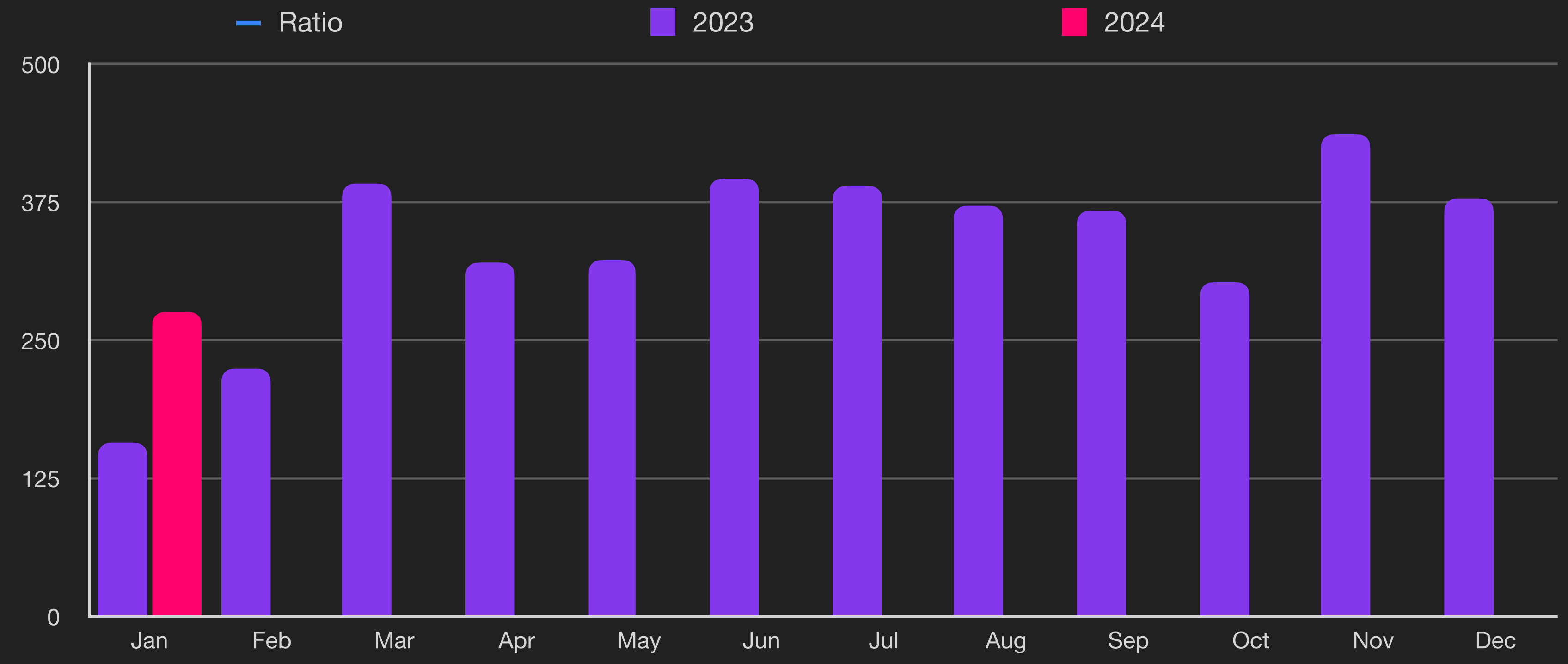
We begin 2024 with a record January and second highest number of attacks ever, in fact, 130% more than in 2023. Similarly, unreported attacks increased 75% over the previous year. On a more positive note, the ratio of unreported to reported attacks fell to a new low of 364%, suggesting that the new regulations introduced by the SEC in December are having a significant effect on ransomware reporting.

From an industry perspective we saw education under siege with 14 attacks, more than 75% greater than last years clear favorite, the healthcare sector. Rounding out the top 4 sectors we saw healthcare at 8, manufacturing 7 and government at 6. Even at this early stage we are seeing a similar breakdown by country as we saw throughout 2023 with USA at 57% and UK at 8% and Singapore in 3rd place with 4% of attacks.

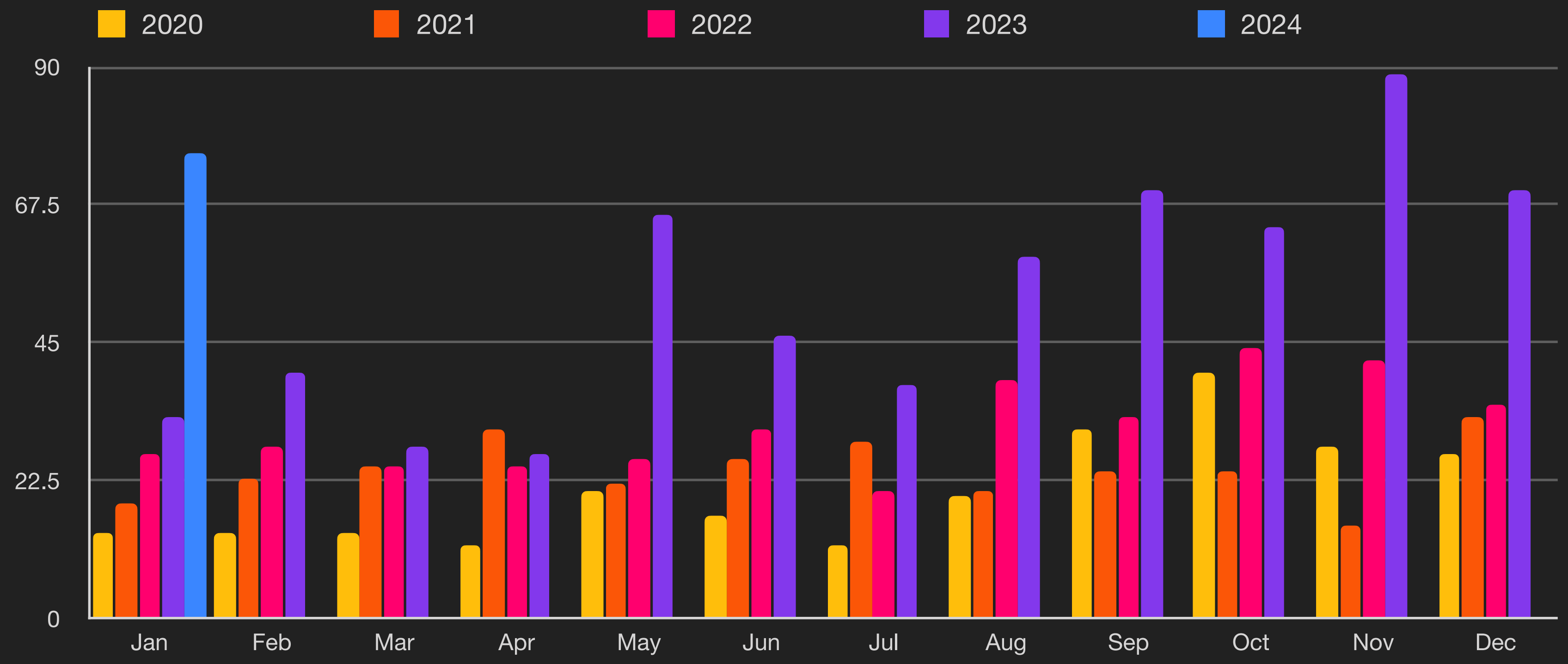
LockBit continues to dominate as the main ransomware variant with 29.4%, which is also reflected in the number of unreported attacks at 30.9%. This month we also saw Akira move into second place with 11.8%, followed by BlackCat at 9.8%.

Finally, data exfiltration continues to dominate the news and is now the primary goal of all attackers, at 91% of all ransomware. We are now seeing extortion continue for years after the initial attack, even if the victim paid the initial ransom. There are so many ways to leverage data once it has been exfiltrated. Lastly, we see that China and Russia continue to dominate as the leading destinations for exfiltrated data with 18% and 8% respectively.

Unreported Ransomware Attacks



Reported Ransomware by Month



Key Trends

364% Unreported

1st Highest January

2nd Highest Month on Record

35% of all attacks use PowerShell

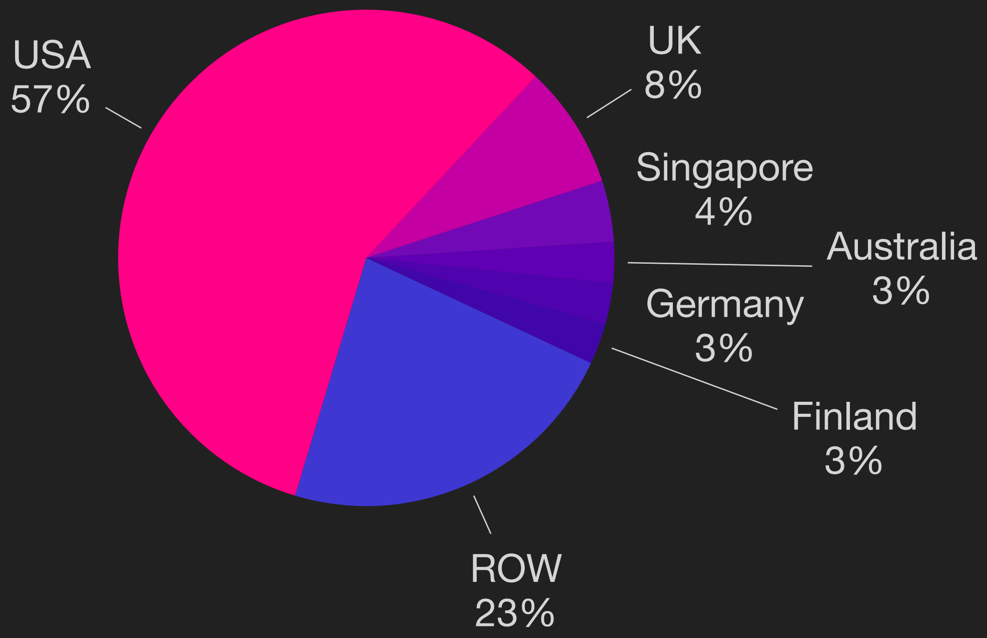
91% of attacks exfiltrate data

Average payout US $568,705
-33% from Q3/23

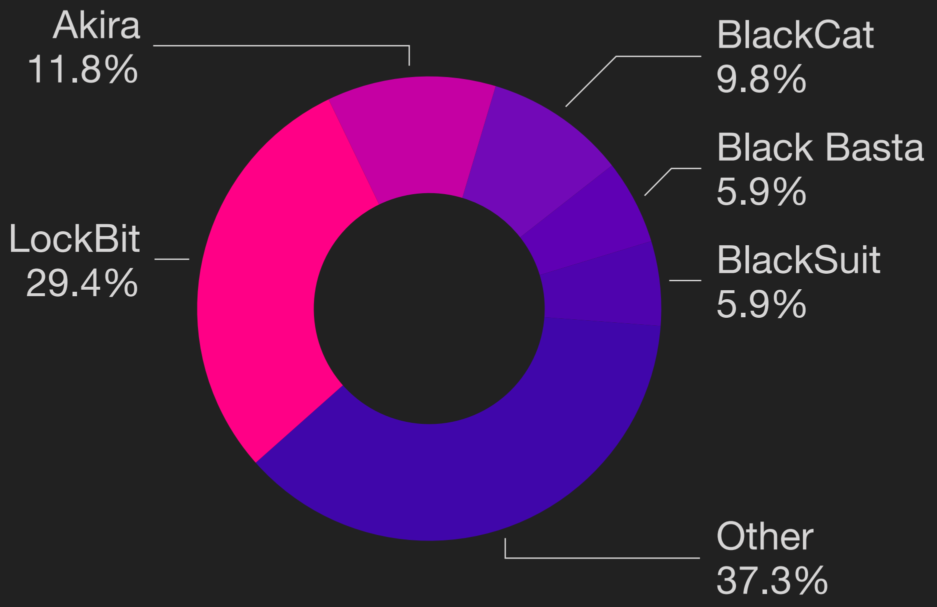
BlackFog State of Ransomware Report

January 2024

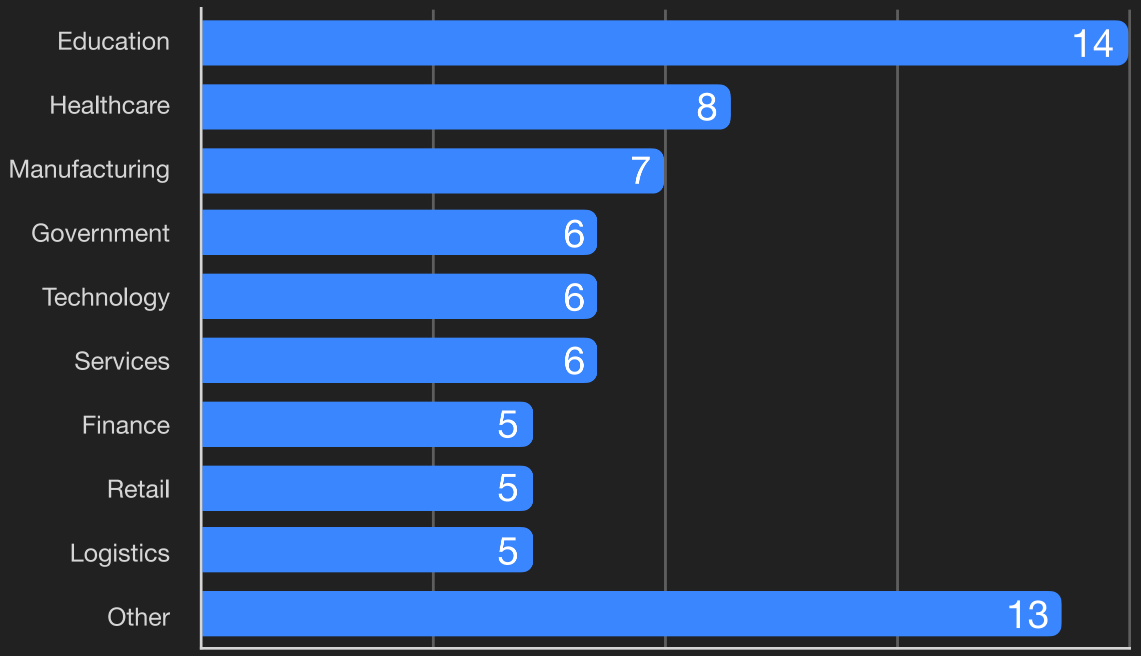
Ransomware by Country



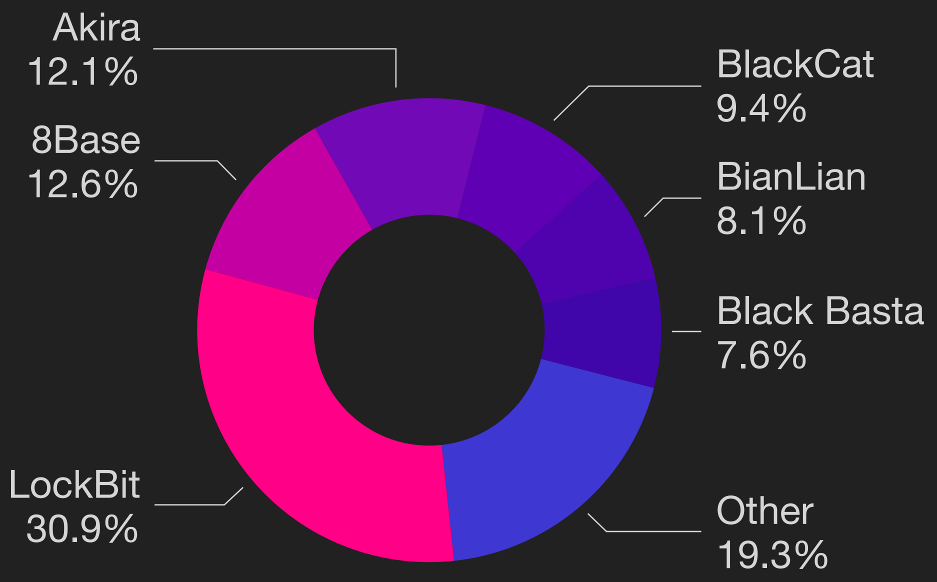
Ransomware Variant (Reported)



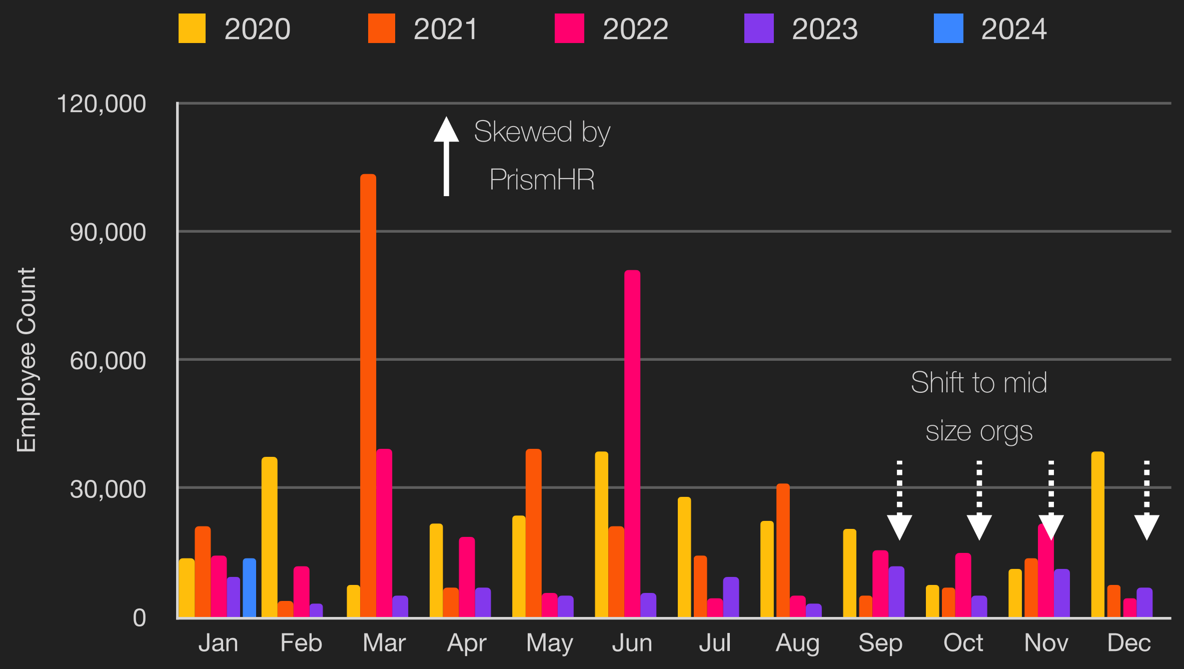
Ransomware by Industry



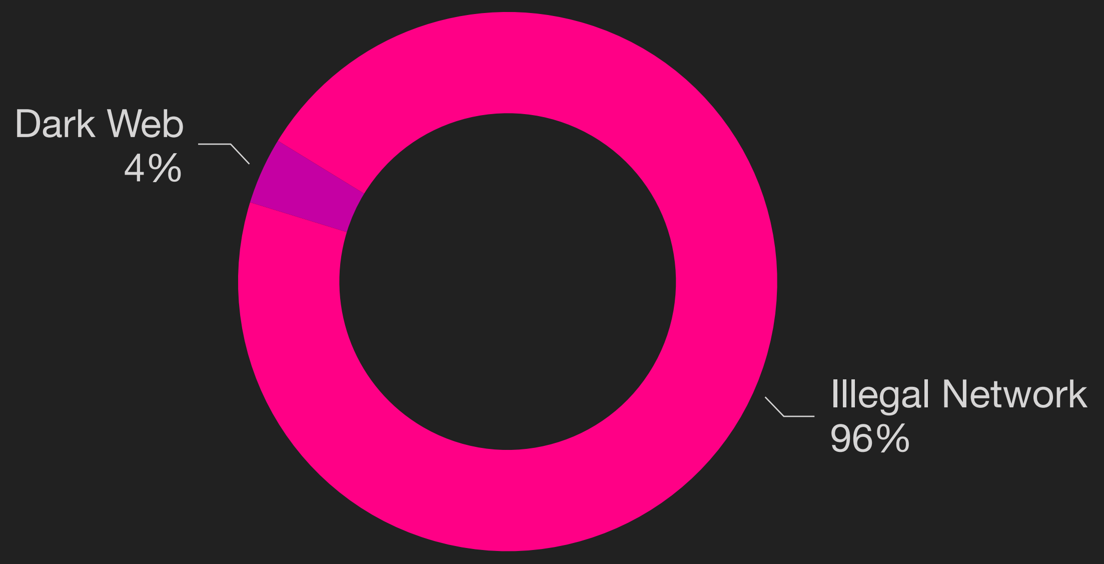
Ransomware Variant (Unreported)



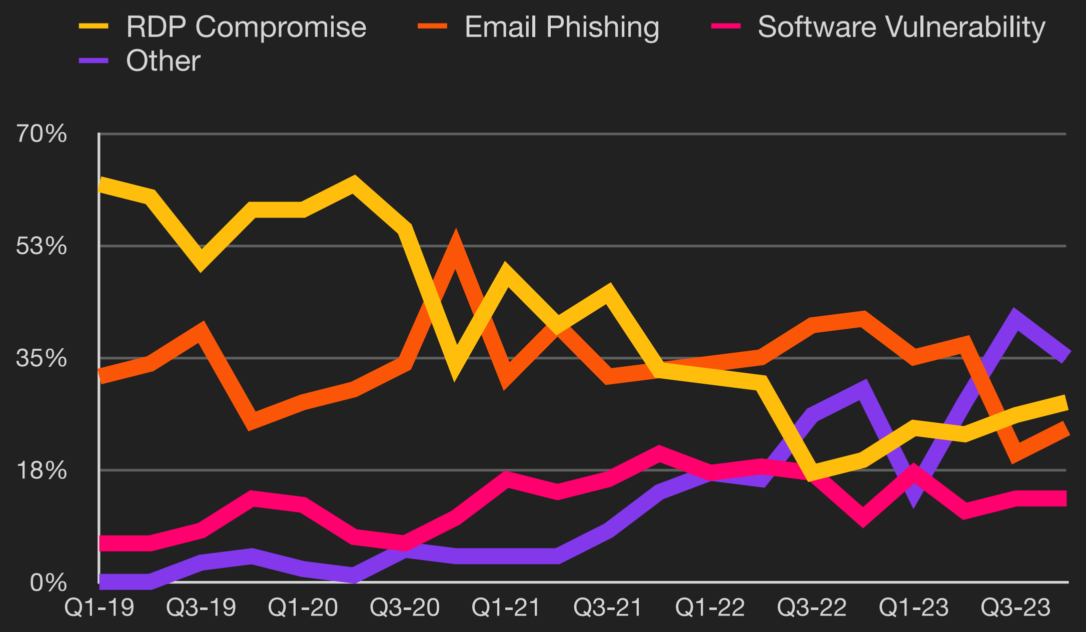
Size of Organization



Exfiltration Techniques

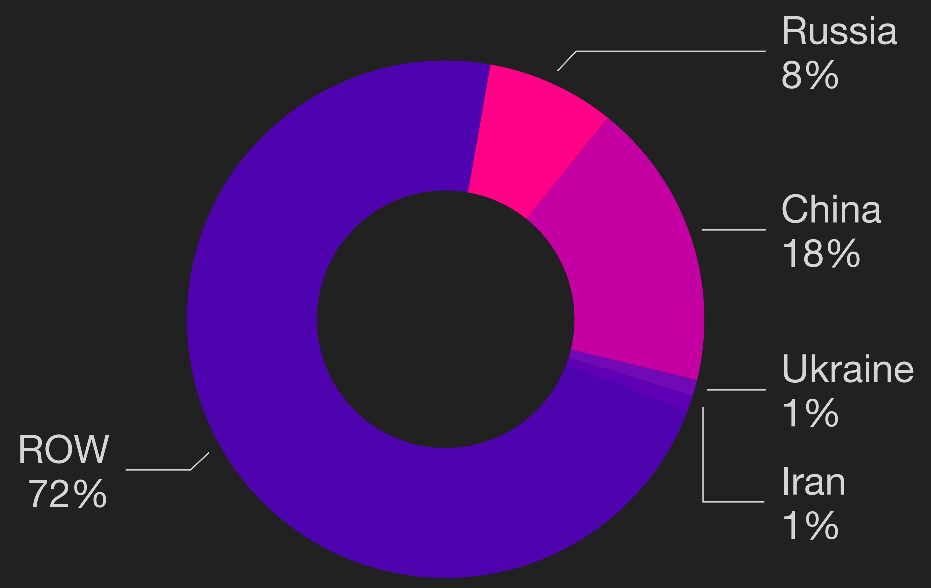


Attack Vectors[2]



[2]Courtesy Coveware

Exfiltration by Country



Methodology

- This report was generated in part from data collected by BlackFog Enterprise over the specified report period. It highlights significant events that prevented or reduced the risk of ransomware or a data breach and provides insights into global trends for benchmarking purposes. This report contains anonymized information about data movement across hundreds of organizations and should be used to assess risk associated with cybercrime.
- Industry classifications are based upon the ICB classification for Supersector used by the New York Stock Exchange (NYSE).
- All recorded events are based upon data exfiltration from the device endpoint across all major platforms.

GLOBEE® AWARDS

CYBERSECURITY BREAKTHROUGH AWARD 2023

CYBER SECURITY EXCELLENCE AWARDS ★ WINNER ★ 2022

CYBER SECURITY EXCELLENCE AWARDS ★ WINNER ★ 2023