Introduction

April saw 59 ransomware attacks make global news headlines, with healthcare and government leading the way with 13 attacks each, followed by the services industry in third place. Notable attacks included Norwegian aluminium producer Norsk Hydro who disclosed financial losses exceeding $40 million following an attack, as well as the the Hoya Corporation who found themselves faced with a $10 million ransom demand after Hunters International exfiltrated 2TB of data.

Roundup

April maintained the high attack rates we have come to expect this year with 59 reported attacks, representing the highest April on record, with 119% year-over-year growth. Similarly, the number of unreported attacks remained high at 342, representing a ratio of 580%, or nearly 6 times more unreported than reported attacks.

The biggest changes by sector, saw healthcare lead the way with 14 new attacks, a massive 47% increase over last month. This was followed by the government and retail sectors with increases of 40% and 38% respectively. Both manufacturing and technology saw modest increases of 25% each.

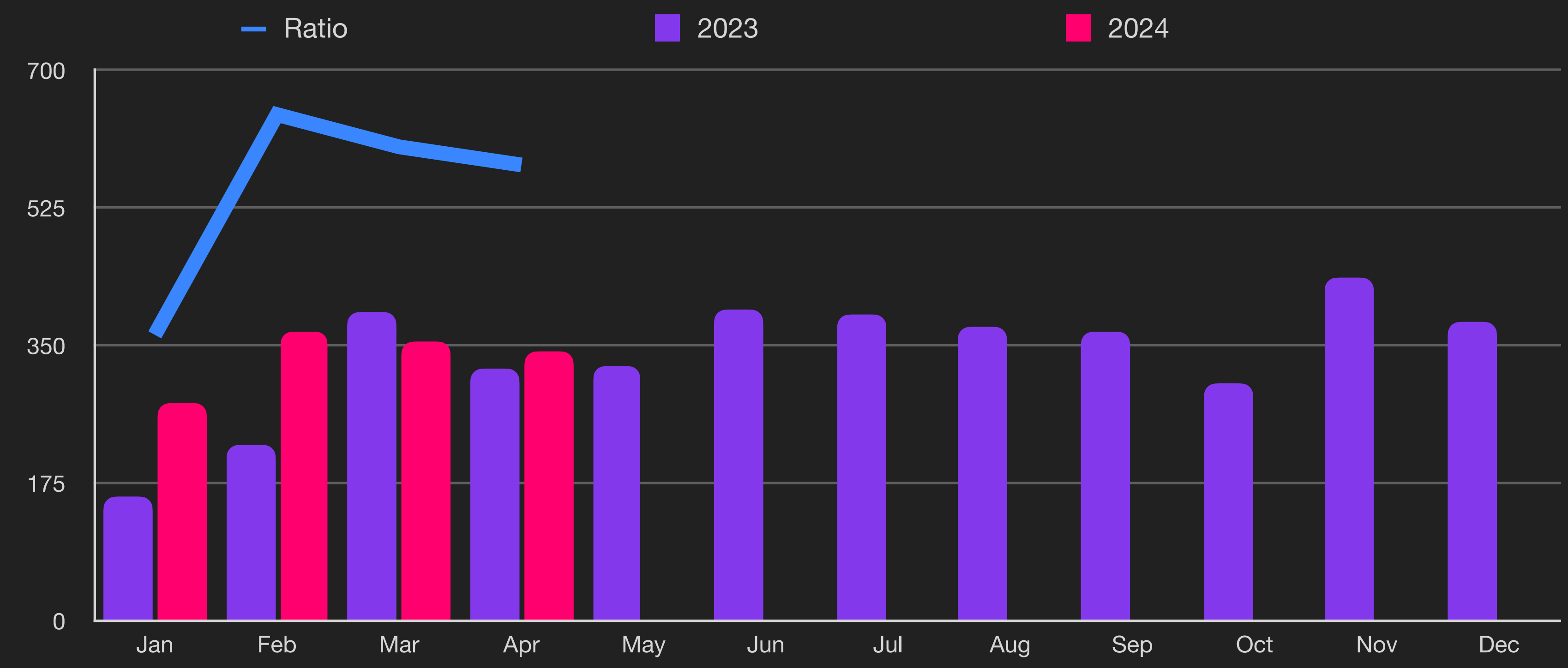
From a variant perspective, we saw the biggest changes in Medusa, moving to 3rd place with a 75% increase in attacks, followed by Rhysida and Lockbit with 43% and 19% respectively. Lockbit is still the dominant variant by more than 100% over its neareast competitor, BlackCat. This is also mirrored in the unreported attacks, although we did see a large increase in attacks from the Play variant with a 44% increase this month. This is typically a leading indicator of reported attacks in subsequent months.

Lastly, we saw China an Russia as the leading destinations of data exfiltration with 17% and 7% respectively. With extortion the primary goal of virtually all attacks, 92% of all ransomware attacks now involve some form of data exfiltration.

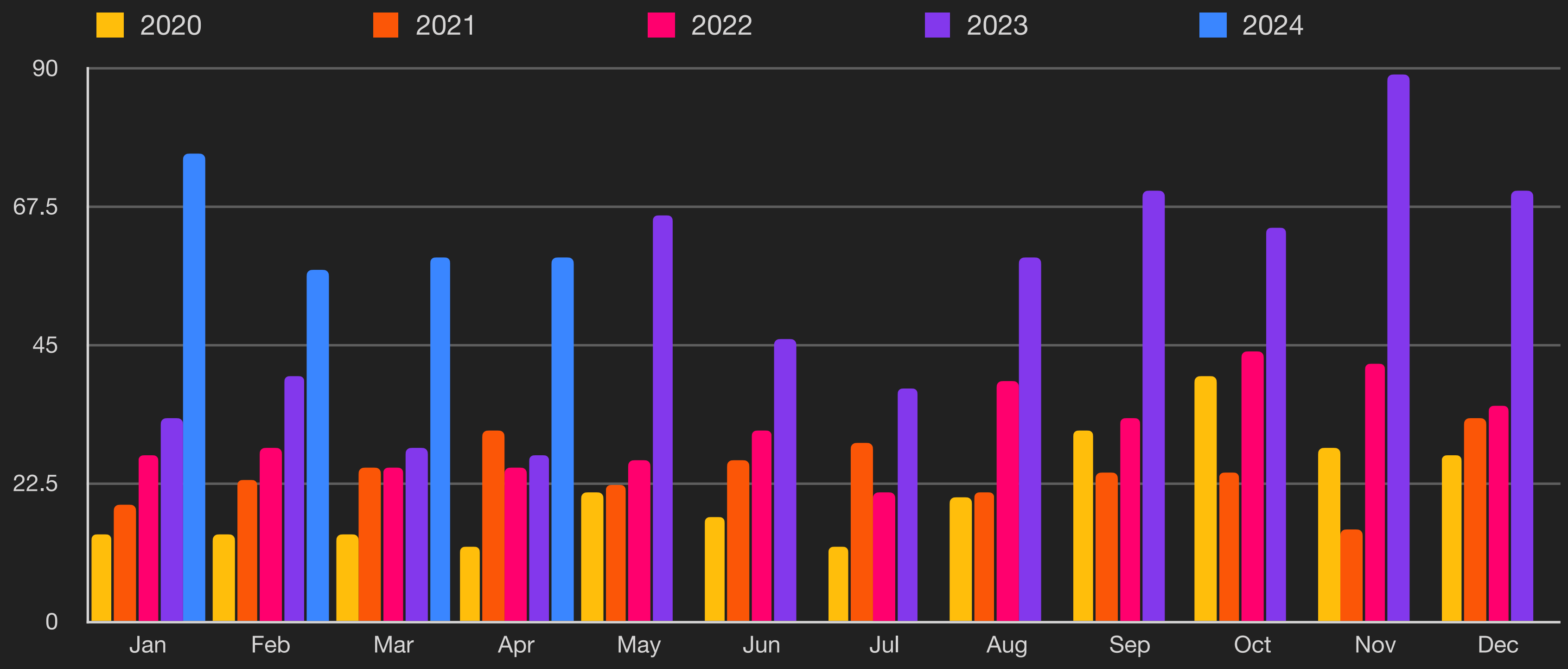
BlackFog State of Ransomware Report

April 2024

Unreported Ransomware Attacks



Reported Ransomware by Month



Key Trends

580% Unreported

1st Highest April

45% of all attacks use PowerShell

92% of attacks exfiltrate data

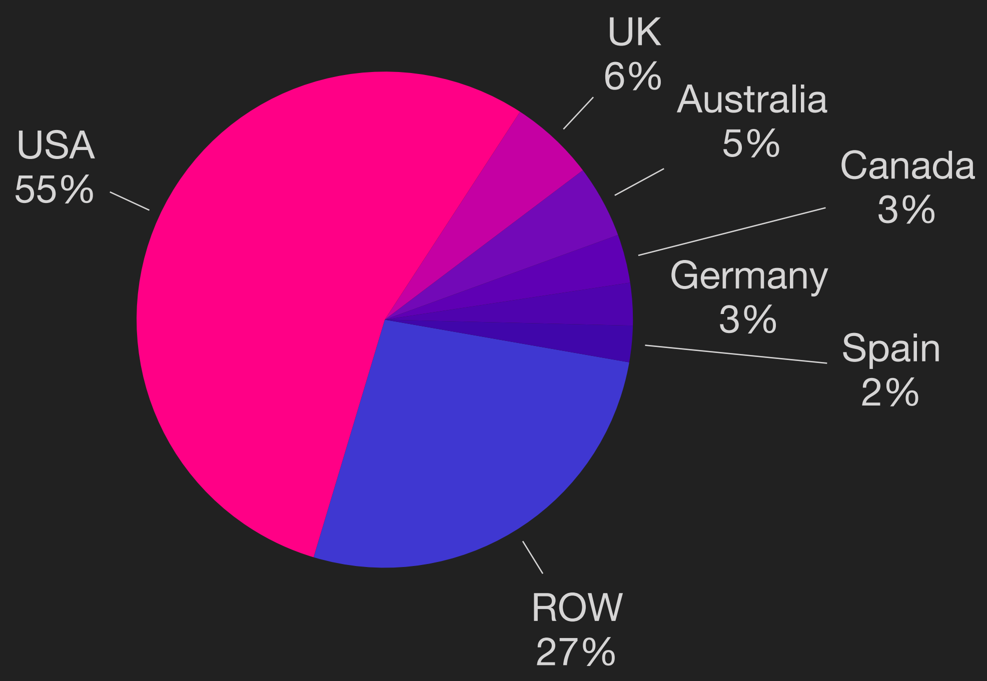
Average payout US $381,980

-32% from Q4/23

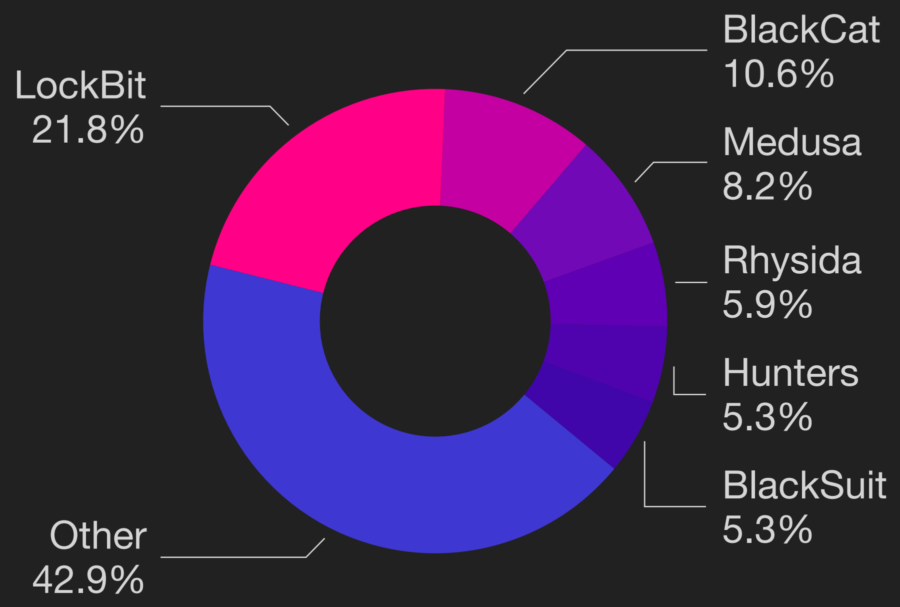
BlackFog State of Ransomware Report

April 2024

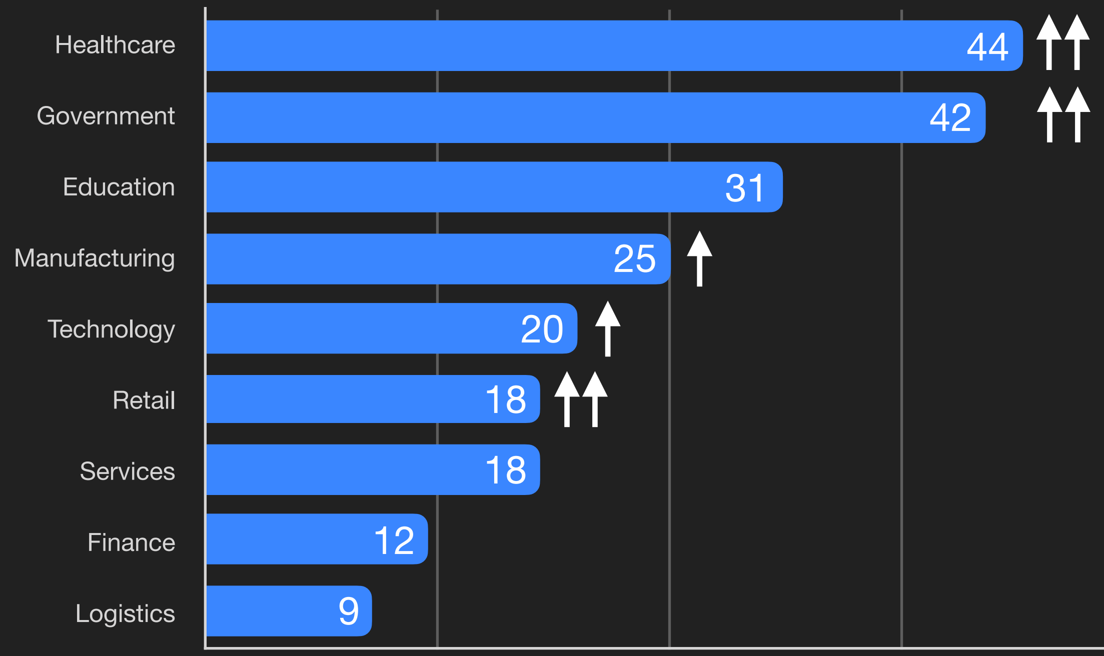
Ransomware by Country



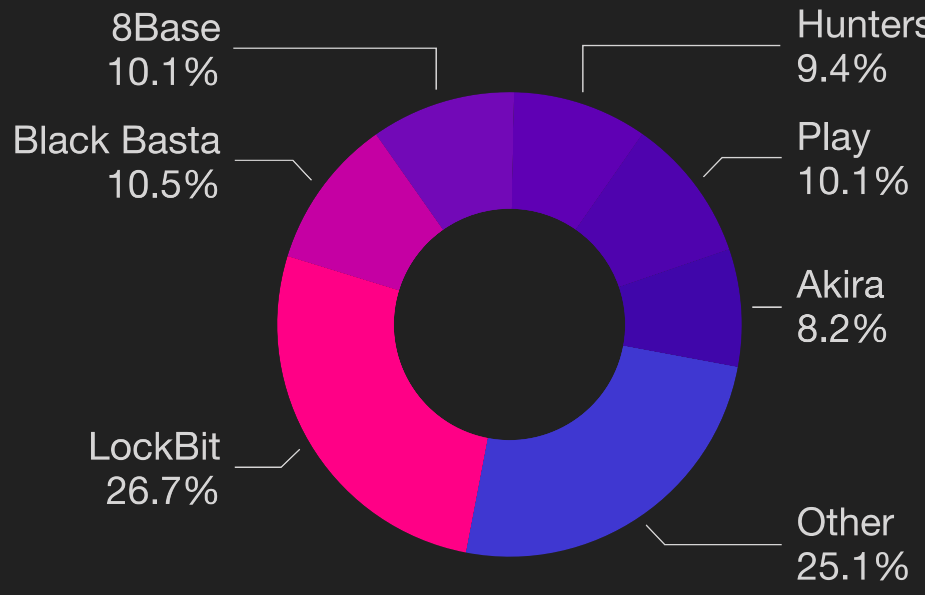
Ransomware Variant (Reported)



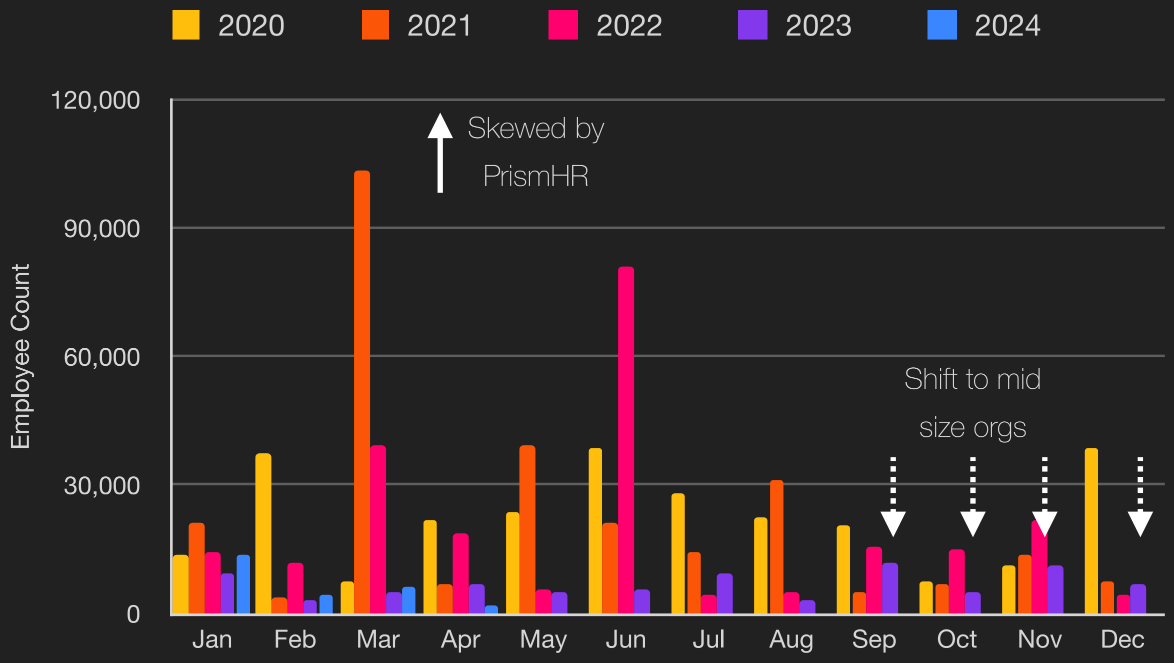
Ransomware by Industry



Ransomware Variant (Unreported)



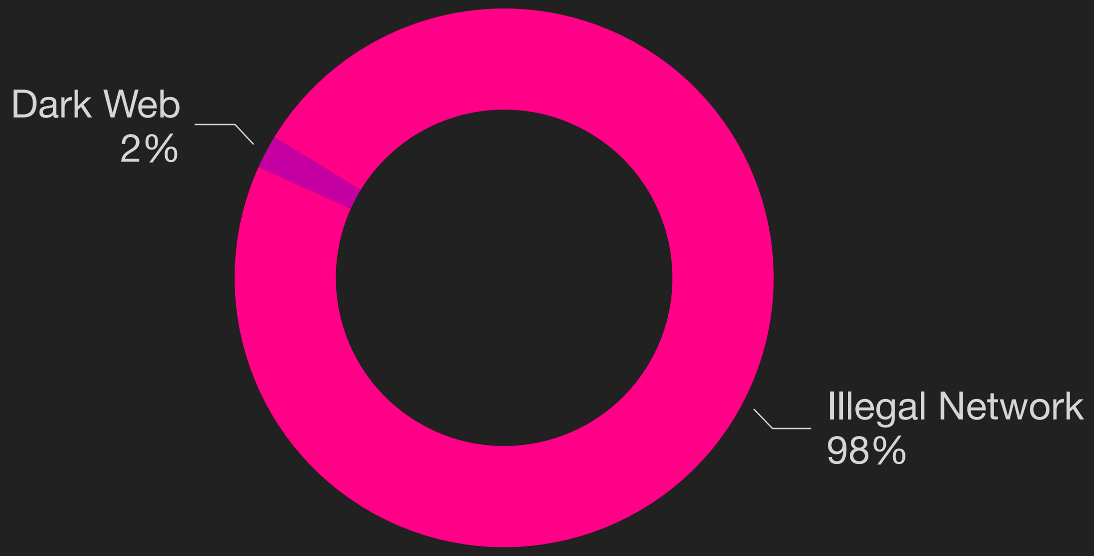
Size of Organization



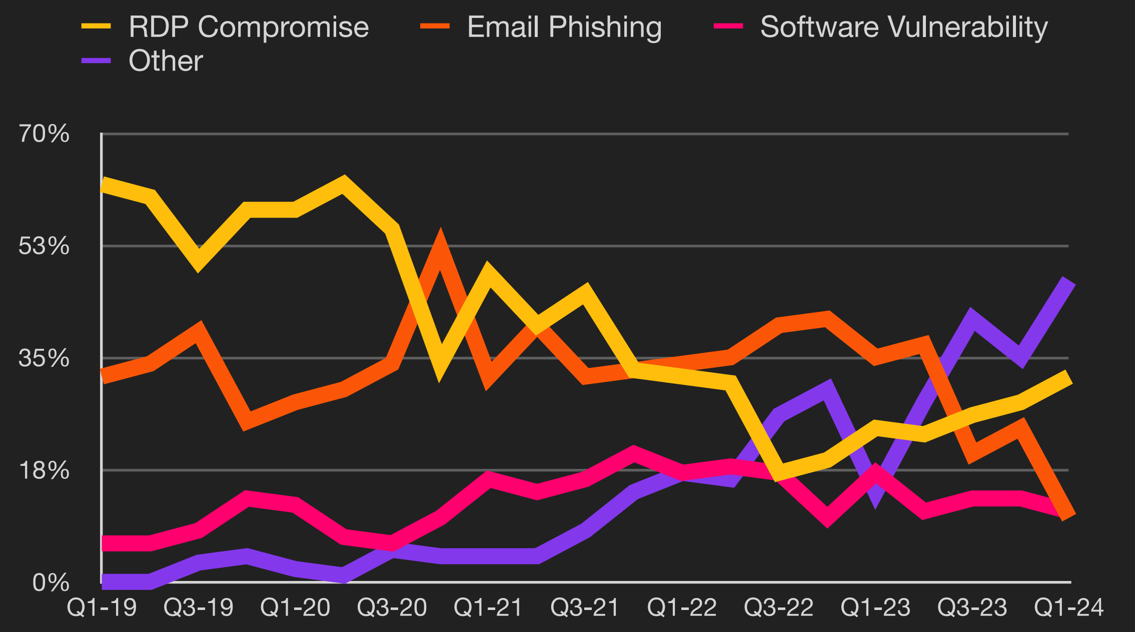
Skewed by PrismHR

Shift to mid size orgs

Exfiltration Techniques

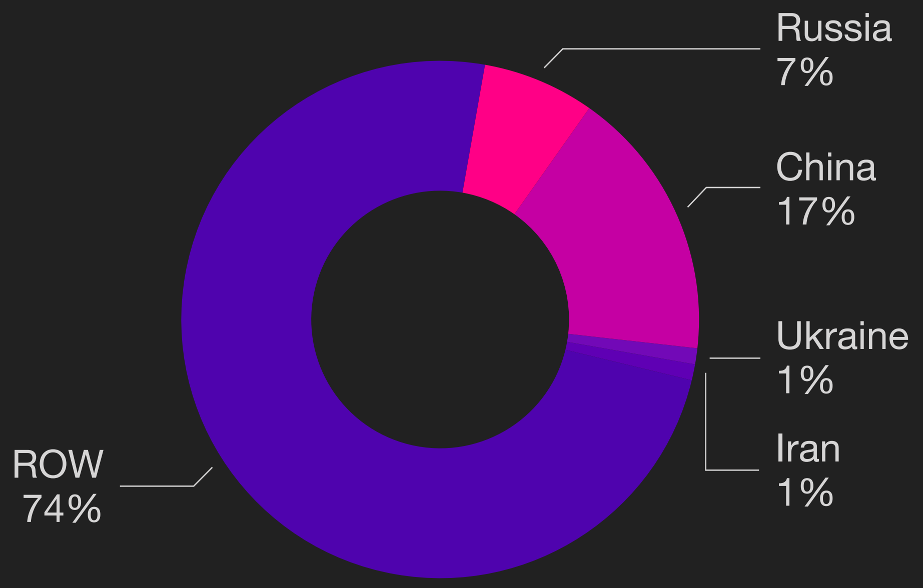


Attack Vectors[2]



[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.