Introduction

Unlike recent years where July has been a quiet month for ransomware, this year we have recorded 60 publicly disclosed attacks, a 58% increase from last year. Although the US was the highest targeted location, there was a surge of attacks in Australia this month, with 7 recorded. Government topped the targeted industries with 15 attacks, followed by education and healthcare with 9 attacks each. LockBit and Ransomhub were both as equally dominant, clocking up 5 claimed victims. Some of the big news stories this month included attacks on Los Angeles County Superior Court, OneBlood and Southern California's 911 services.

Roundup

As the 3rd highest month of the year, July was unusually busy, and represents the largest July on record with 60 publicly disclosed attacks. Similarly, it represents the second highest number of undisclosed attacks of the year with a total of 406, and a ratio of 677% undisclosed to disclosed attacks.

Interestingly, the biggest increase in attacks this month was the arts and entertainment sector with 31%. This was closely followed by the government sector with a 24% increase, while education and healthcare had modest increases of 19% and 14% respectively.

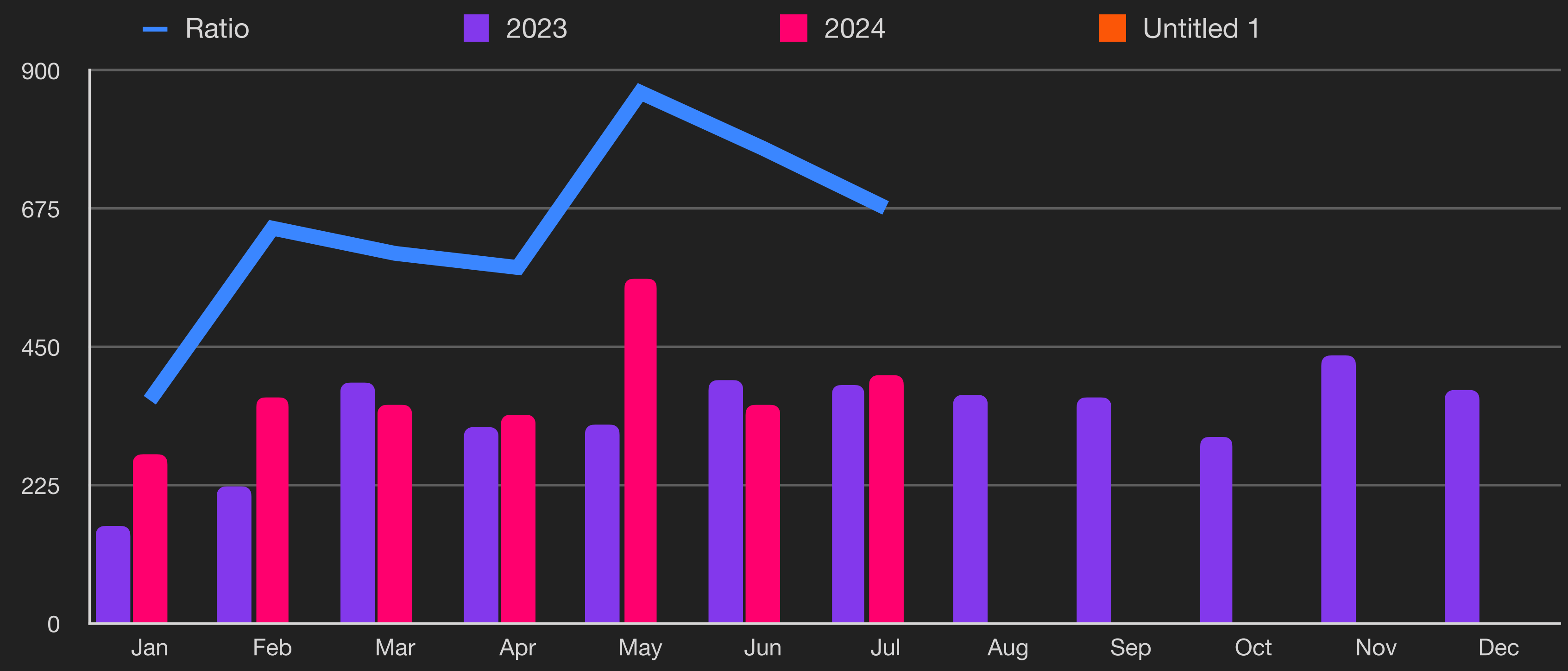
Continuing from last month, Medusa saw a 19% increase in reported and 14% unreported attacks, with LockBit still maintaining a 200% lead over its nearest rival.

This month we have also started monitoring ransomware payment rates courtesy of our friends at CoveWare. As most ransomware now focuses on data exfiltration we note that 43% of victims involving data exfiltration choose to pay the ransom versus 36% overall. This highlights the increasing importance that organizations place on intellectual property and customer data. Over 93% of attacks now involve data exfiltration with China and Russia the leading destinations with 16% and 6% respectively.

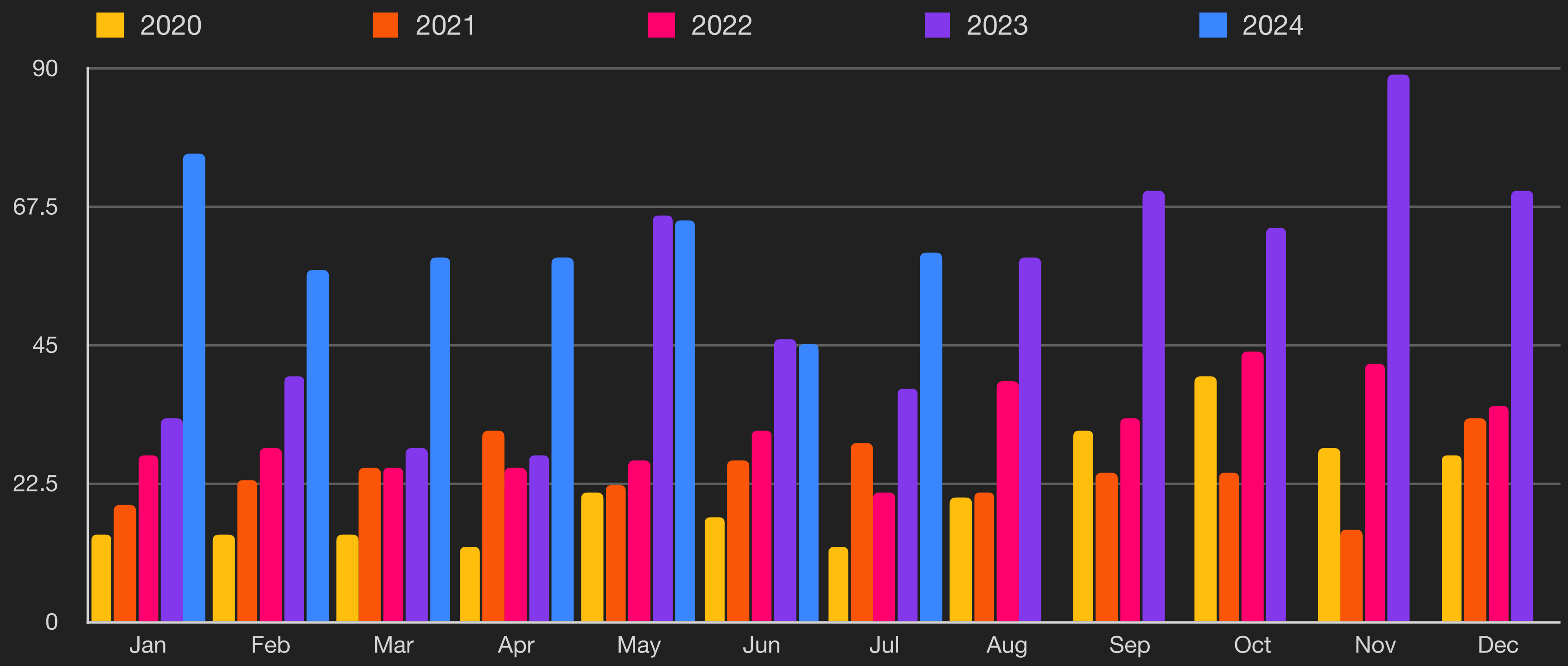
BlackFog State of Ransomware Report

July 2024

Unreported Ransomware Attacks



Reported Ransomware by Month



Key Trends

677% Unreported

1st Highest July

61% of all attacks use PowerShell

93% of attacks exfiltrate data

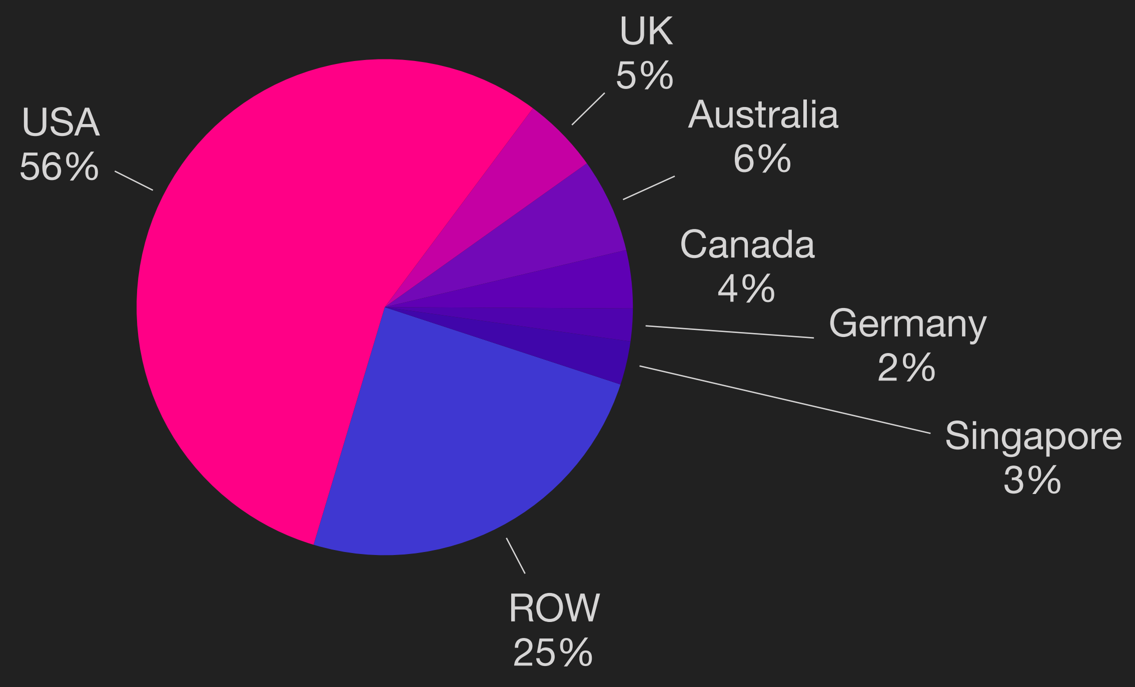
43% of exfiltration victims pay vs 36%
+20% from Q1/24

Average payout US $391,015
+2.4% from Q1/24

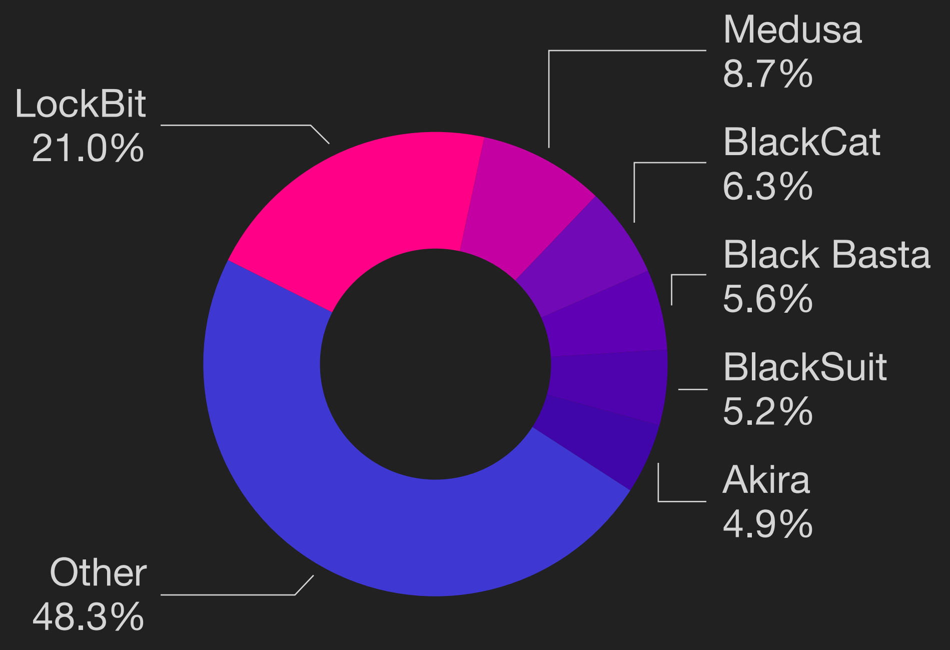
BlackFog State of Ransomware Report

July 2024

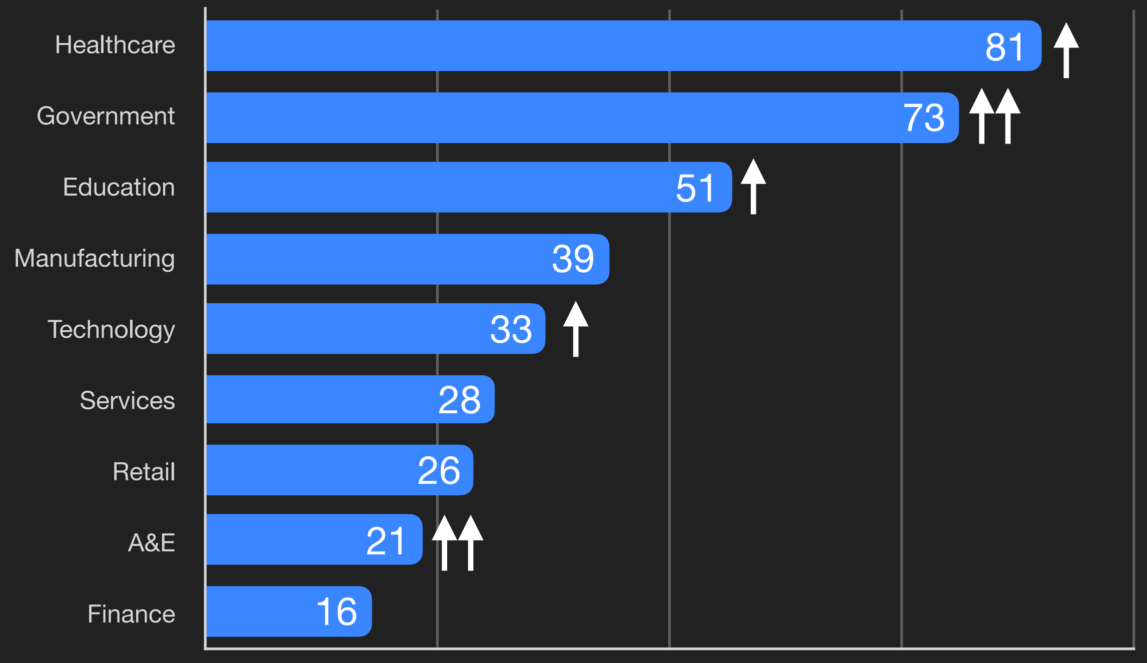
Ransomware by Country



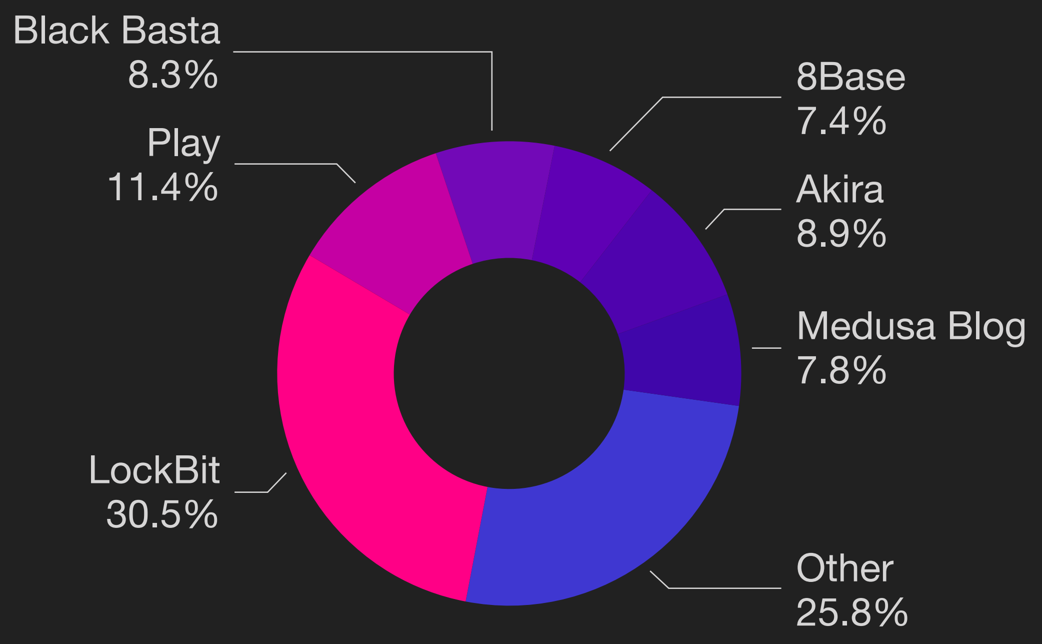
Ransomware Variant (Reported)



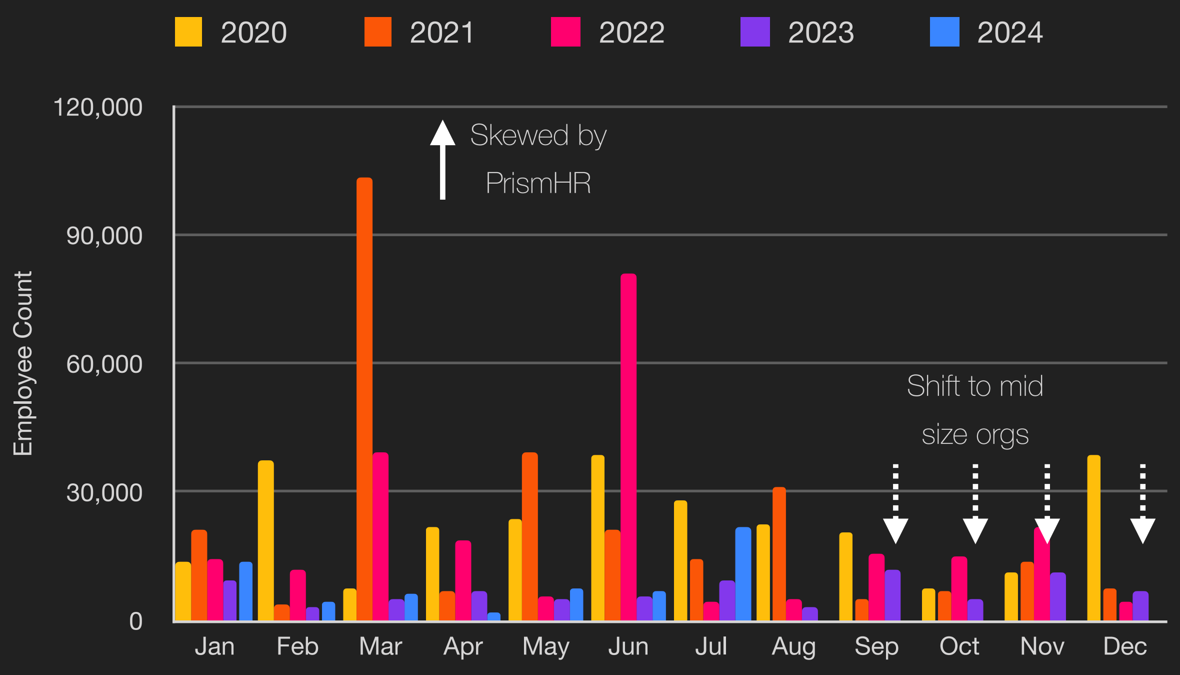
Ransomware by Industry



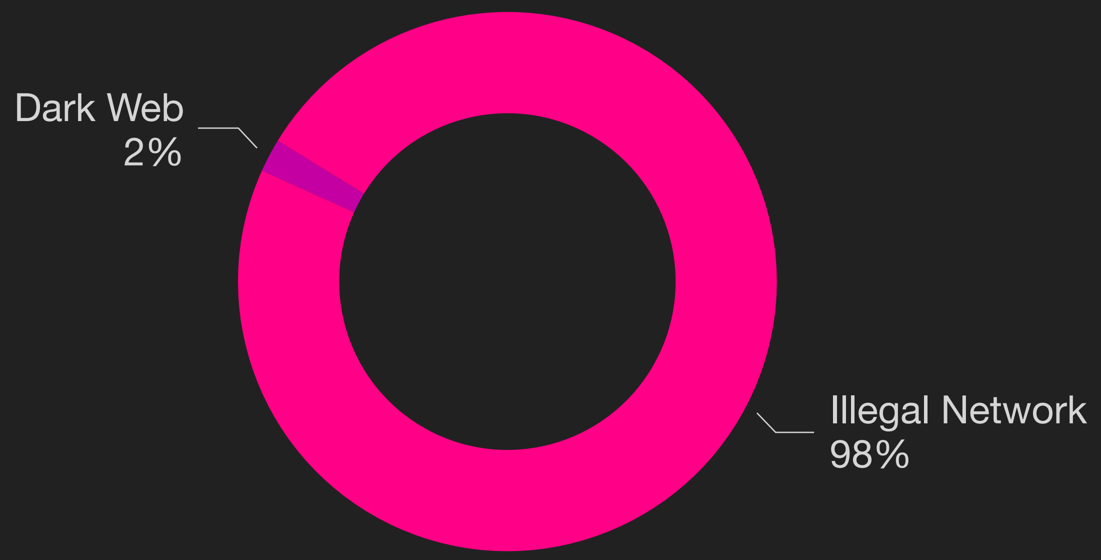
Ransomware Variant (Unreported)



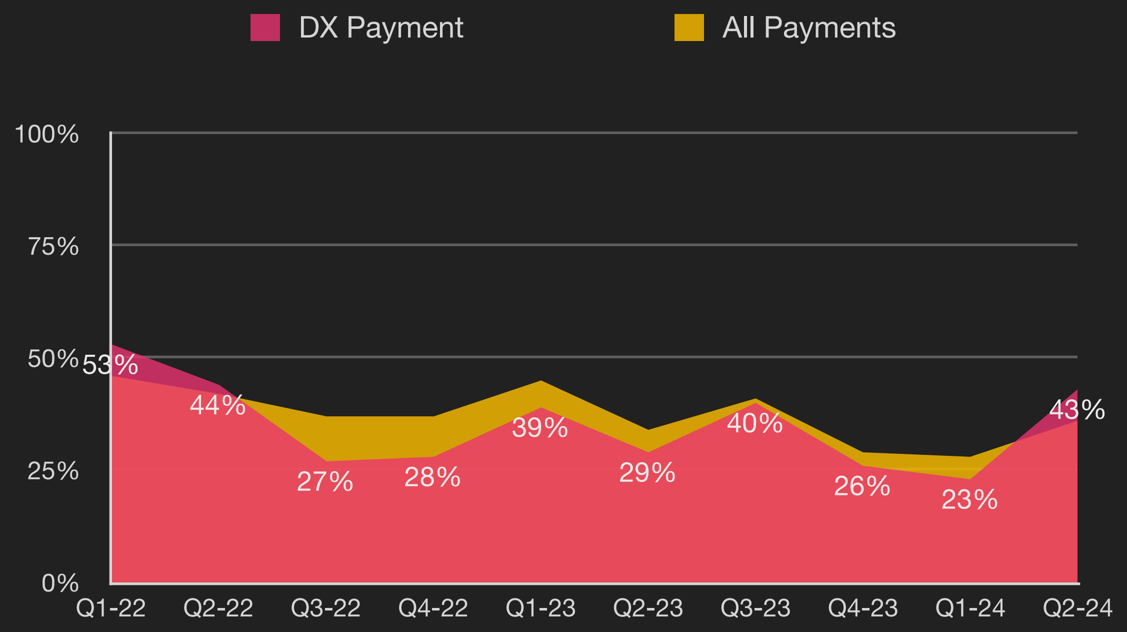
Size of Organization



Exfiltration Techniques

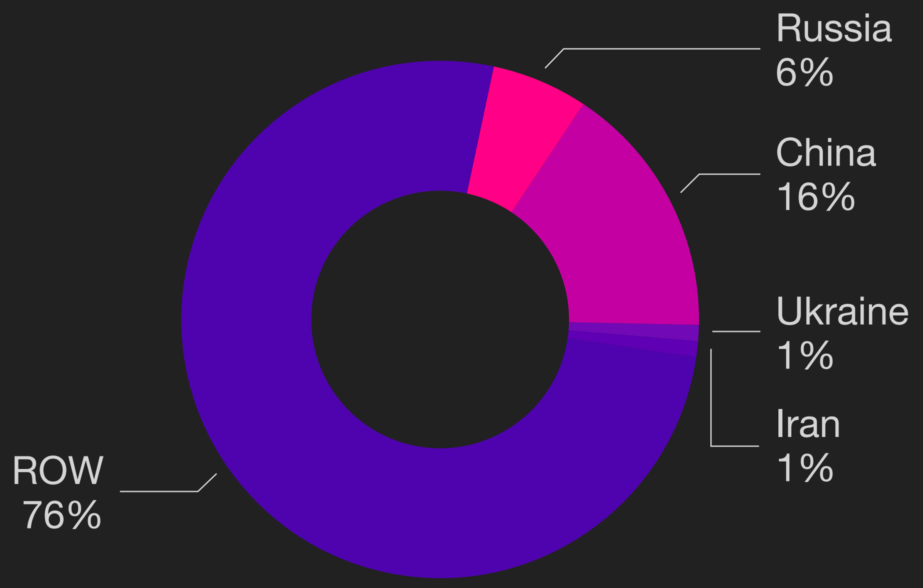


Exfiltration Payment Rates[2]



[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.