August 2023

We recorded 59 publicly disclosed ransomware attacks in August, a 51% increase over the same period last year and the second busiest month for disclosed attacks in 2023. LockBit and Medusa were the most active ransomware groups, while education and healthcare were the highest targeted sectors, closely followed by government.

A number of organizations made headlines with attacks and breaches causing huge consequences, including Prospect Medical Holdings who were forced to revert back to pen and paper after a system-wide outage, while almost 1.5 million patients were impacted by a data breach on Alberta Dental Service Corporation.

Roundup

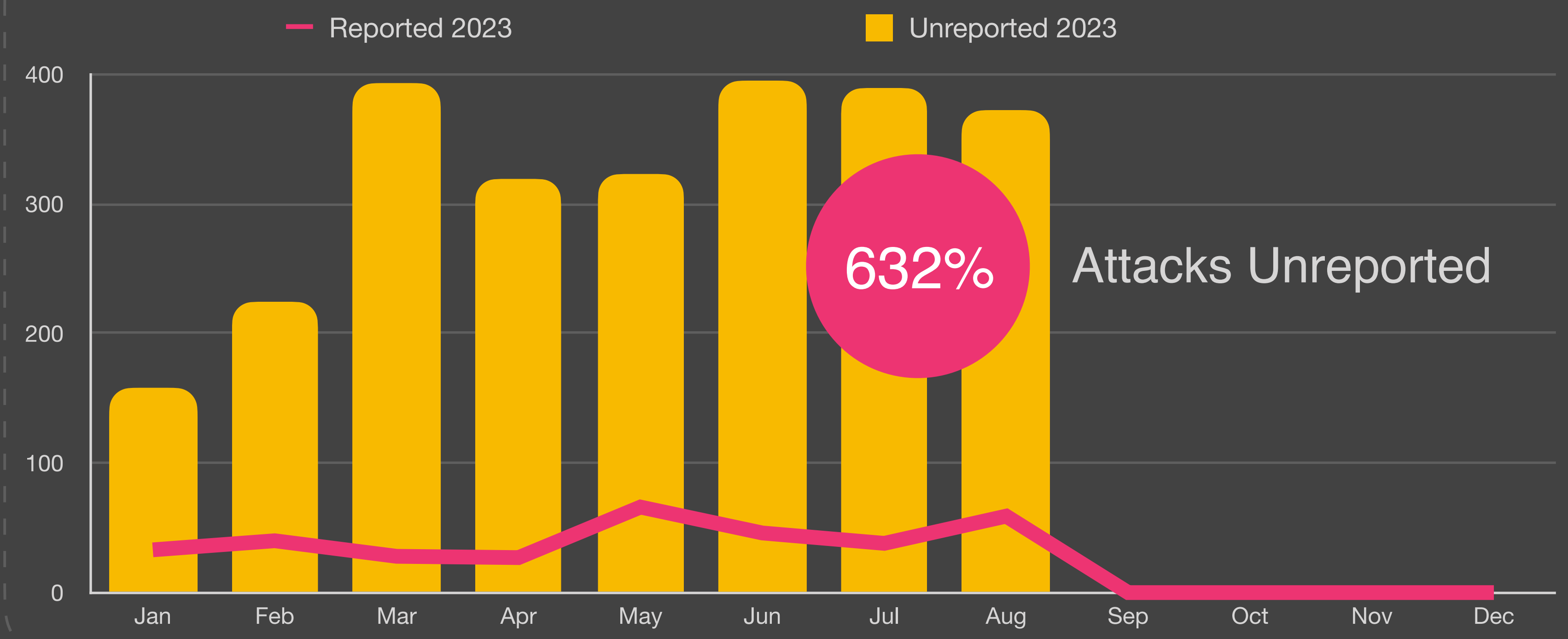
Traditionally a slower month, August this year broke new records and recorded the 2nd highest number of attacks on record with 59 publicly disclosed and 373 non disclosed attacks. This represents a ratio of 632% between unreported and reported. As with last month the MOVEit exploit continues to generate victims, now totaling 365.

This month also saw some big moves in both the manufacturing and service sectors, with increases of 36% and 31% respectively. While technology, government and education continue to grow with increases of 26%, 23% and 21% respectively.

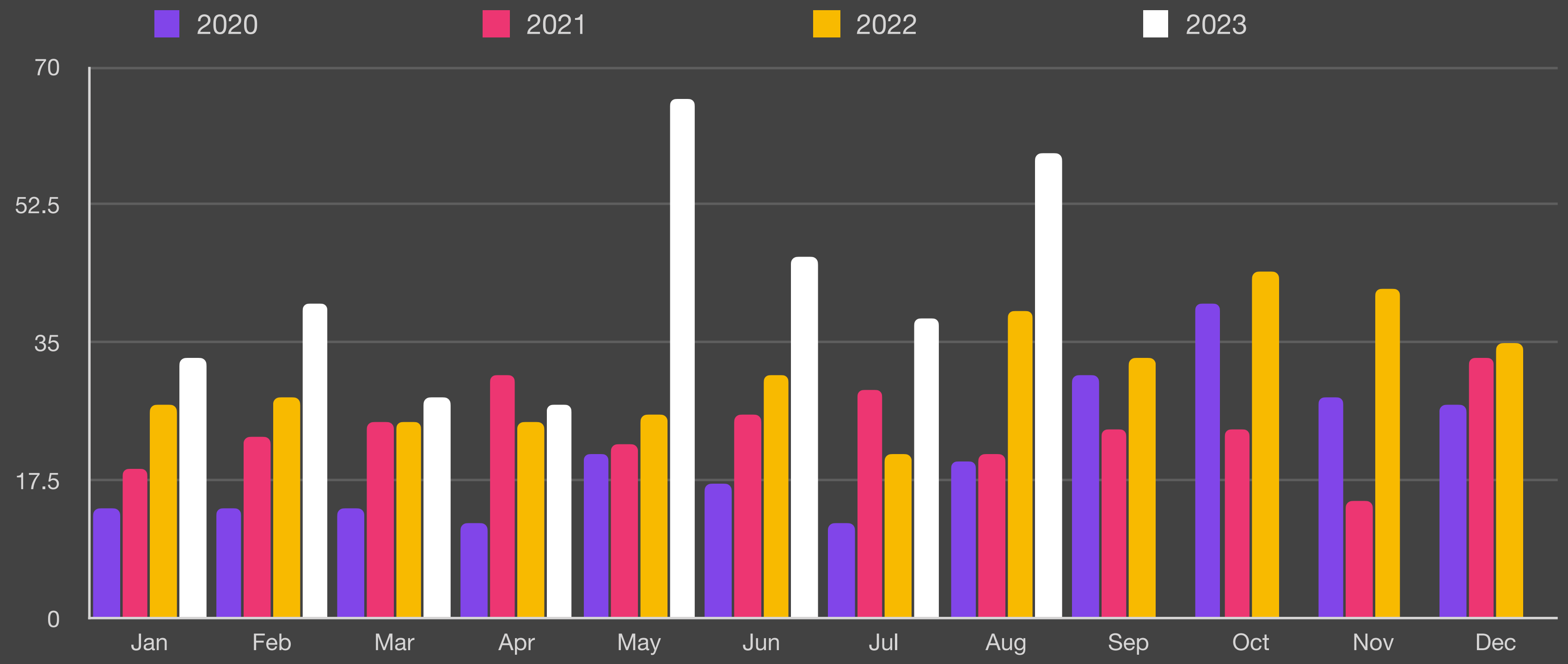
From a variant perspective, BlackCat and LockBit remain the two dominant variants, each accounting for 17.4% of victims, with Medusa and Play at 5.9% a piece. LockBit dominated in the number of unreported attacks at 35.4%, followed by CLOP at 14.1%.

Data exfiltration affected more than 90% of victims this month and continues to dominate as the primary mechanism for extorting organizations and individuals. China continues to dominate as the main destination for data exfiltration with 39%, with Russia at 9%.

Unreported Ransom Attacks



Reported Ransomware by Month



Key Trends

632% Unreported

2nd Highest in 4 years

1st Highest Ransom Payouts

52% of all attacks use PowerShell

90% of attacks exfiltrate data

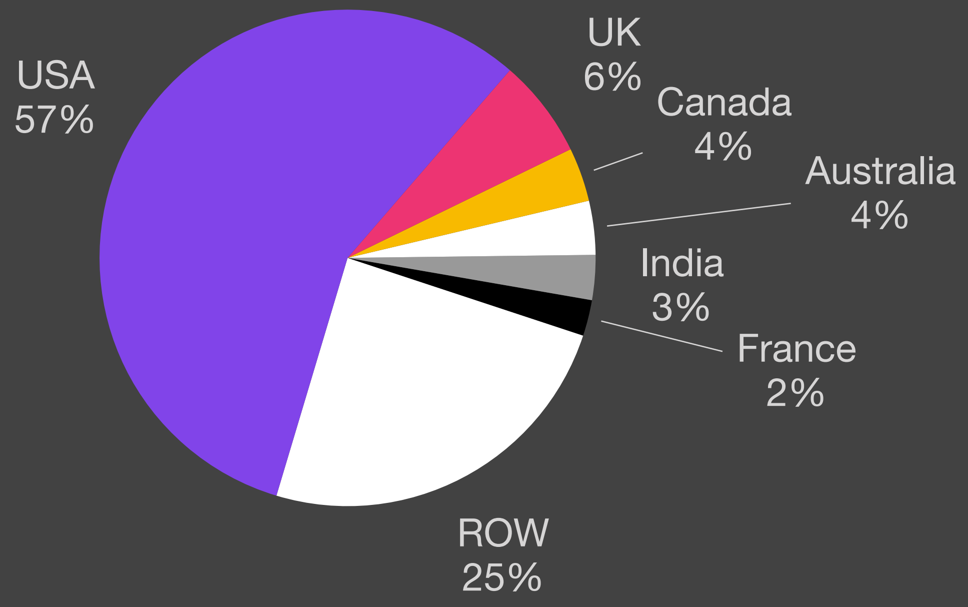
Average payout US $740,144

+126% from Q1/23

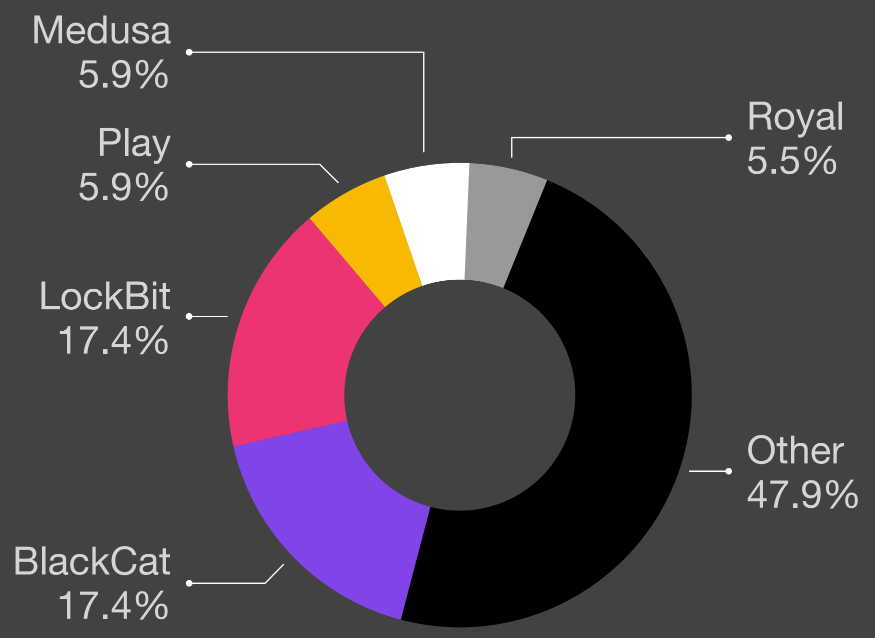
BlackFog State of Ransomware Report

August 2023

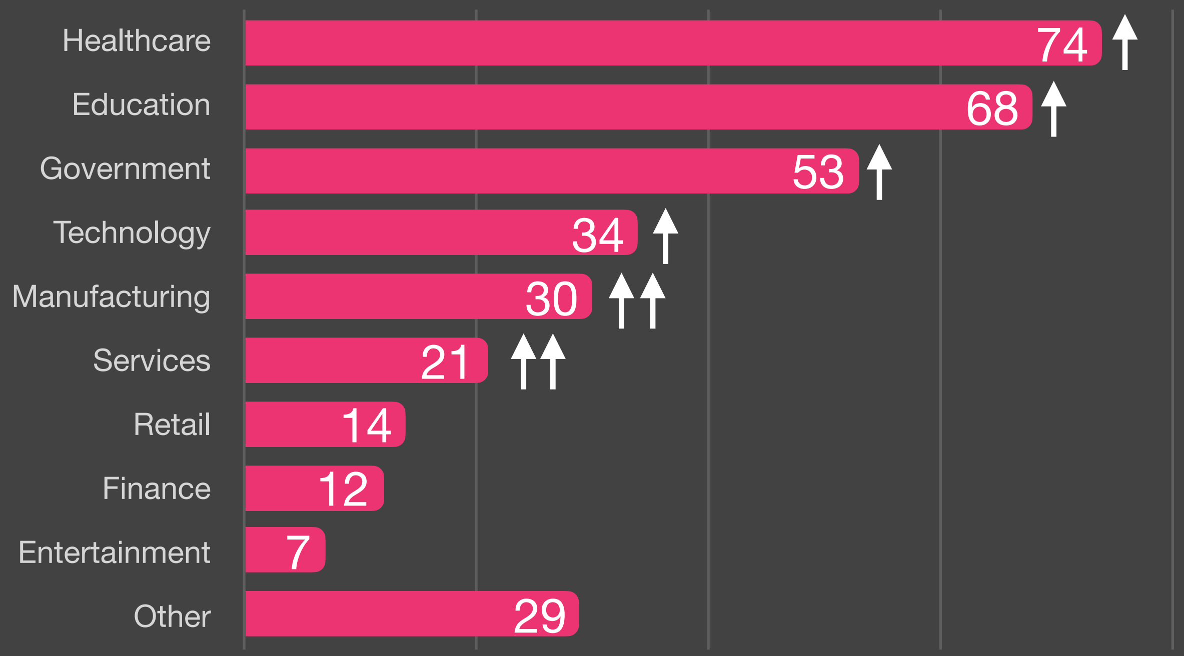
Ransomware by Country



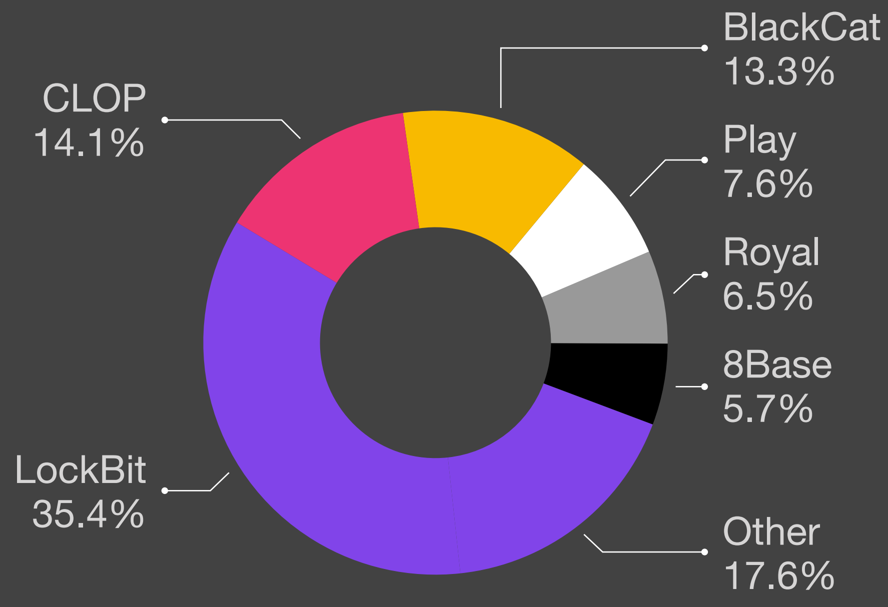
Reported Ransomware Variant



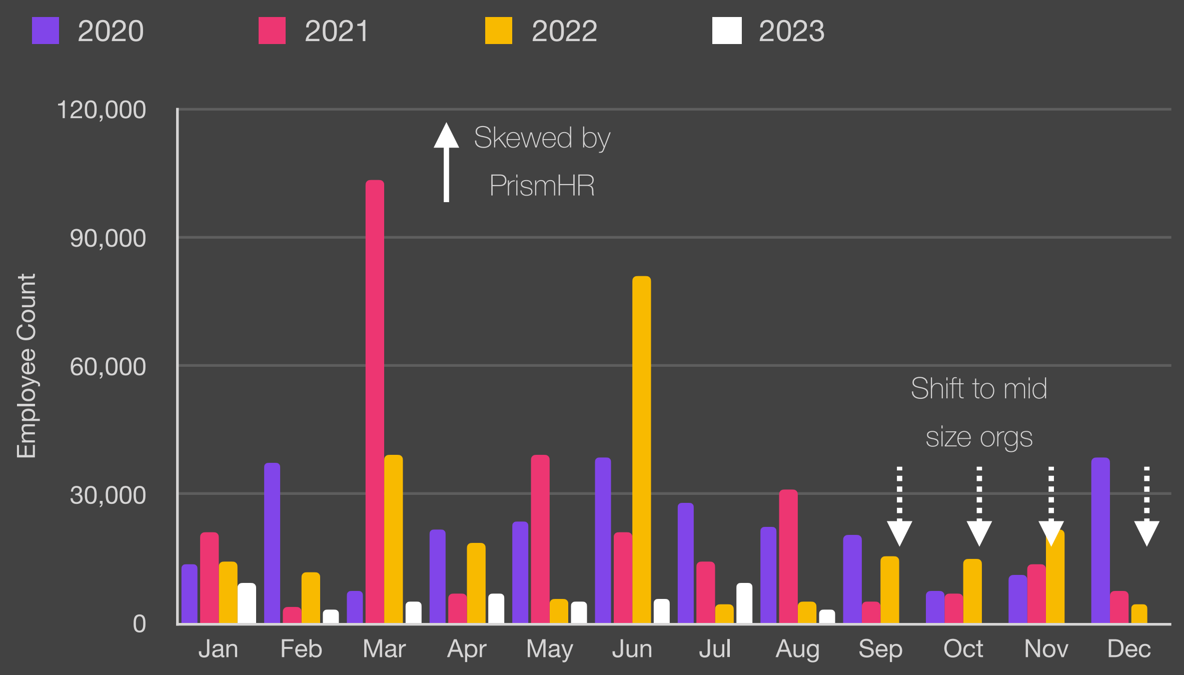
Ransomware by Industry



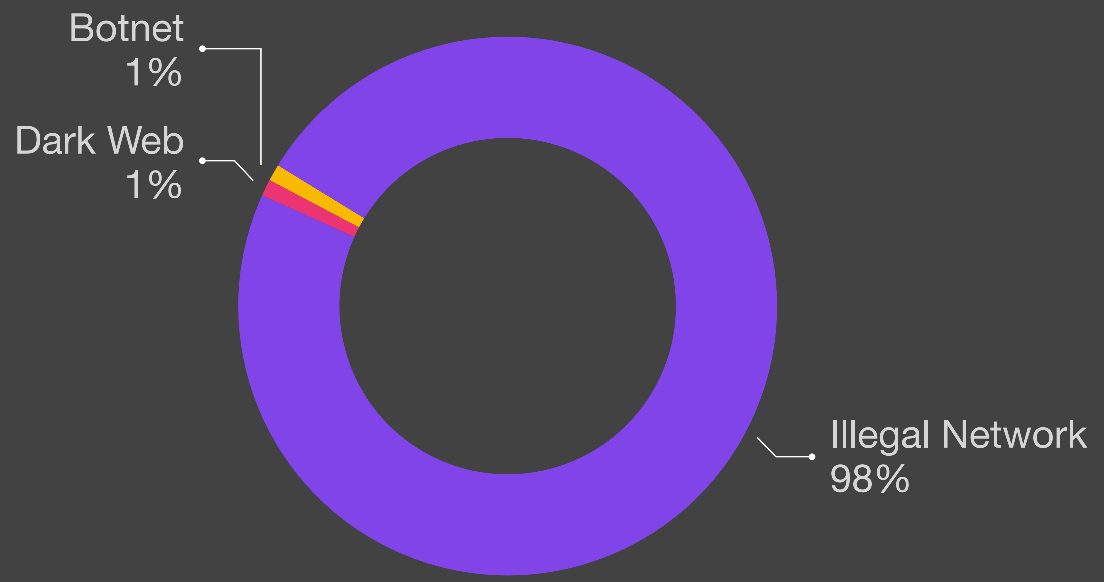
Unreported Ransomware Variant



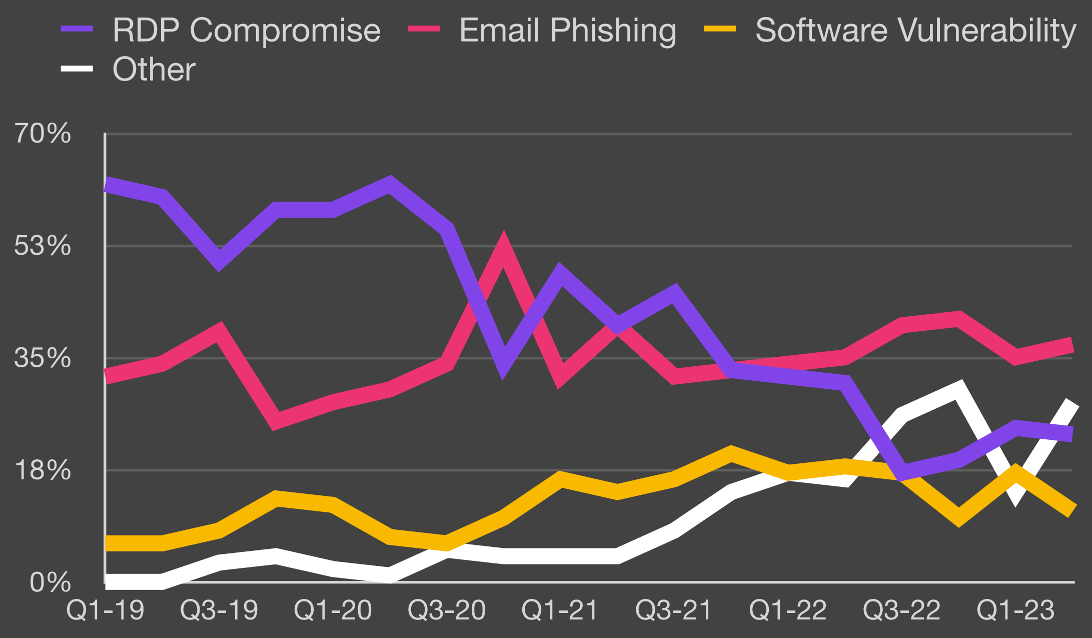
Size of Organization



Exfiltration Techniques

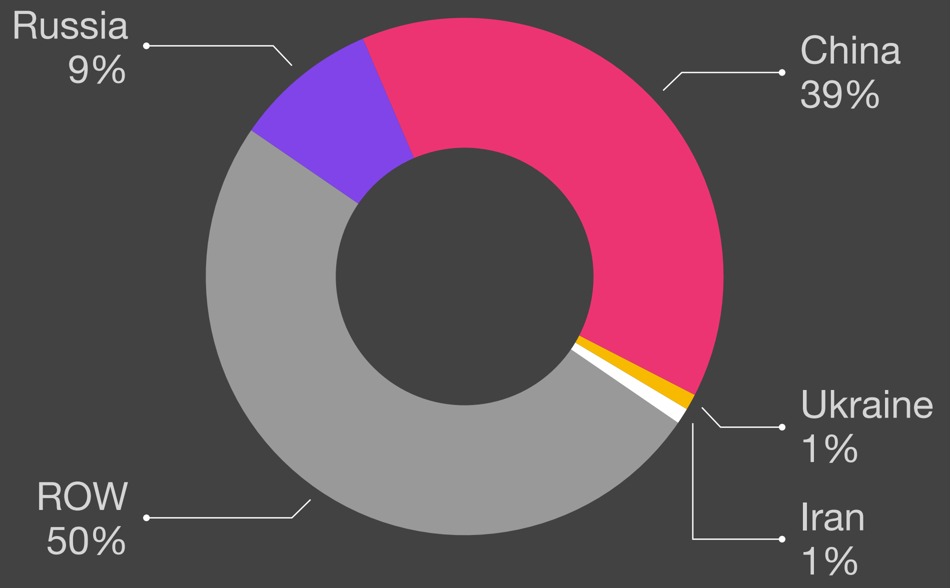


Attack Vectors[2]



[2]Courtesy Coveware

Ransomware Exfiltration 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.