July 2023

We tracked 38 publicly disclosed ransomware attacks in July, representing an 81% increase on 2022, the busiest July we've recorded over the past 4 years. Healthcare was heavily targeted with 14 attacks targeting that sector alone. Many large organizations made news headlines during the month including the Japanese Port of Nagoya who were forced to deal with massive disruption due to a ransomware attack, while 11 million patients were impacted by the incident on HCA healthcare, and cosmetics giant Estee Lauder fell victim to an attack from not one, but two ransomware groups.

Roundup

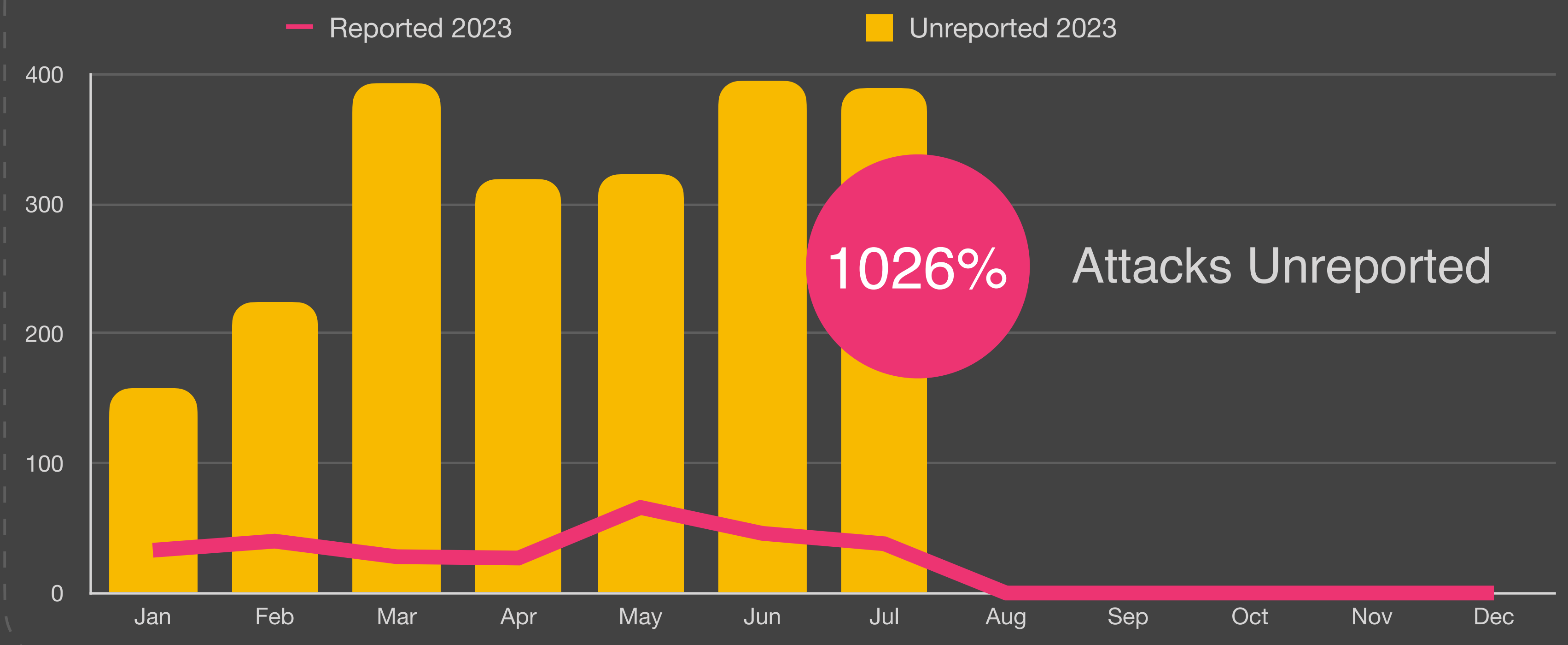
This month we continue to see a large volume of attacks, culminating in the highest July in 4 years, with 38 publicly disclosed and 390 undisclosed attacks. This represents a 10 fold difference between unreported versus reported attacks, as we continue to see the effects of the MOVEit exploit.

The most notable change saw healthcare overtake education as the most targeted sector, with a 29% increase in attacks. Education came a close second with 56 reported attacks, while the Government saw a 19% increase from last month. Other sectors remained largely unchanged.

BlackCat and LockBit remain the two dominant variants with 18.4% and 16.8% respectively. As we predicted last month, we saw CLOP overtake BlackCat in the number of unreported attacks due to the MOVEit exploit. We expect this to continue in the coming months as the full extent of this exploit is realized.

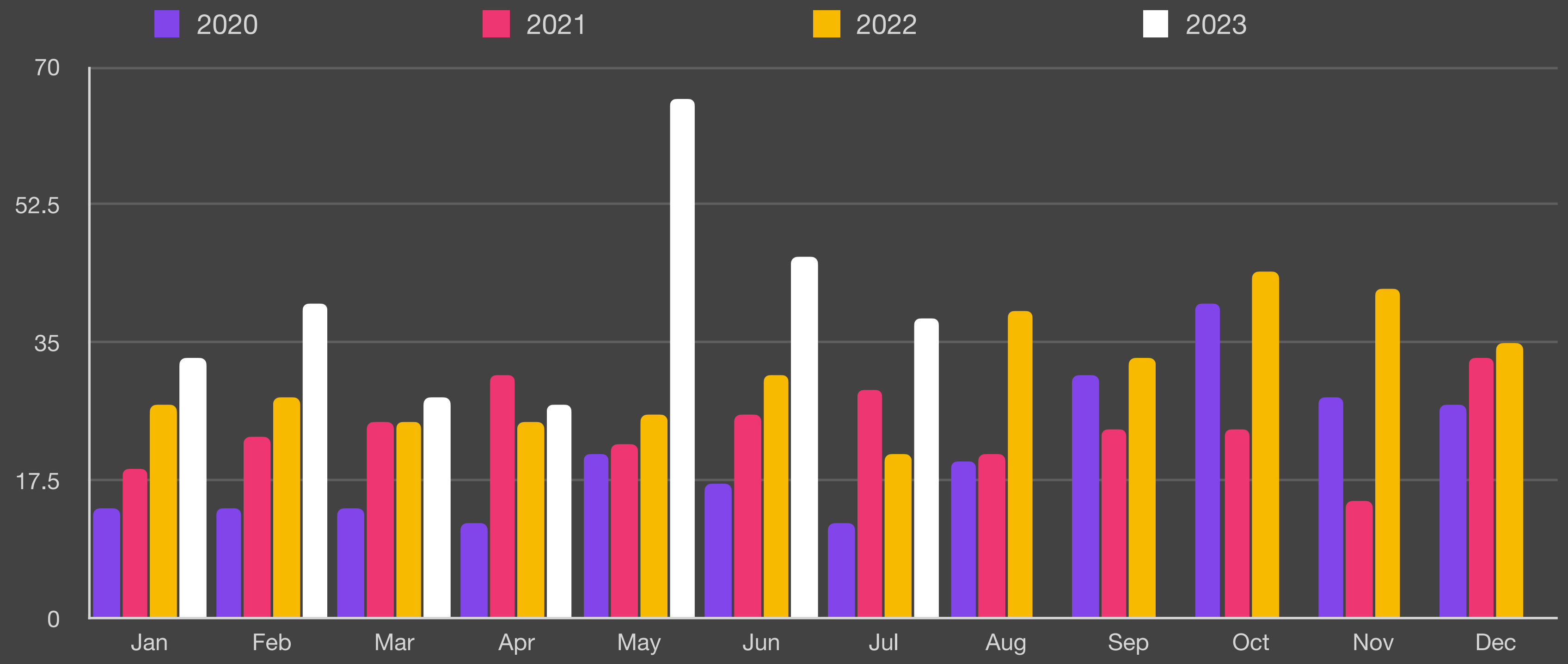
Lastly, exfiltration continues to be the primary weapon of choice for attacks. Leveraging data for extortion contributes to this quarters all time record, with an average payout of US$740,144. China continues to be the main destination for data loss at 41% with Russia at 9%.

Unreported Ransom Attacks



1026% Attacks Unreported

Reported Ransomware by Month



Key Trends

1026% Unreported

Jul Highest July in 4 years

1st Highest Ransom Payouts

61% of all attacks use PowerShell

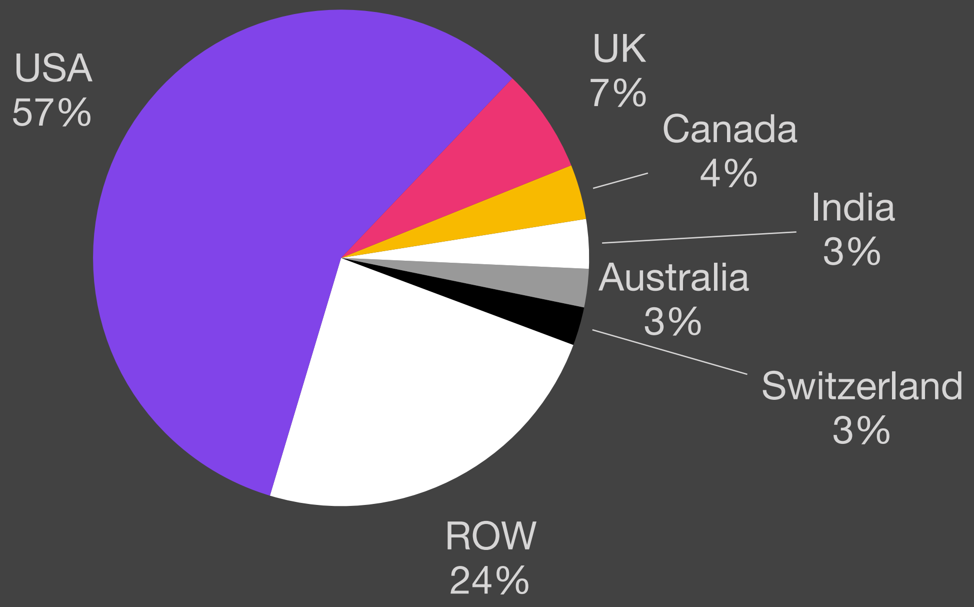
89% of attacks exfiltrate data

Average payout US $740,144 +126% from Q1/23

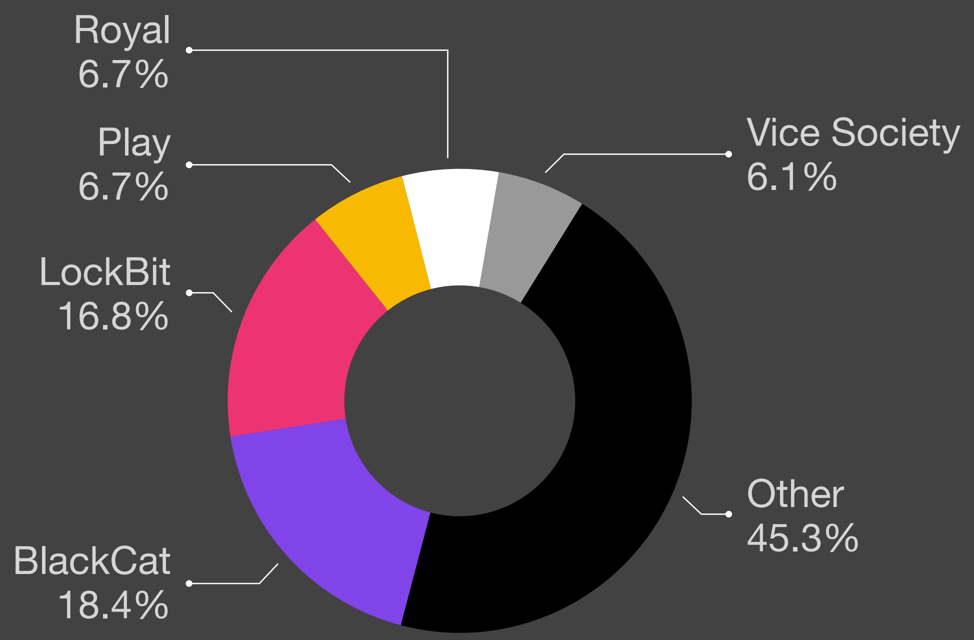
BlackFog State of Ransomware Report

July 2023

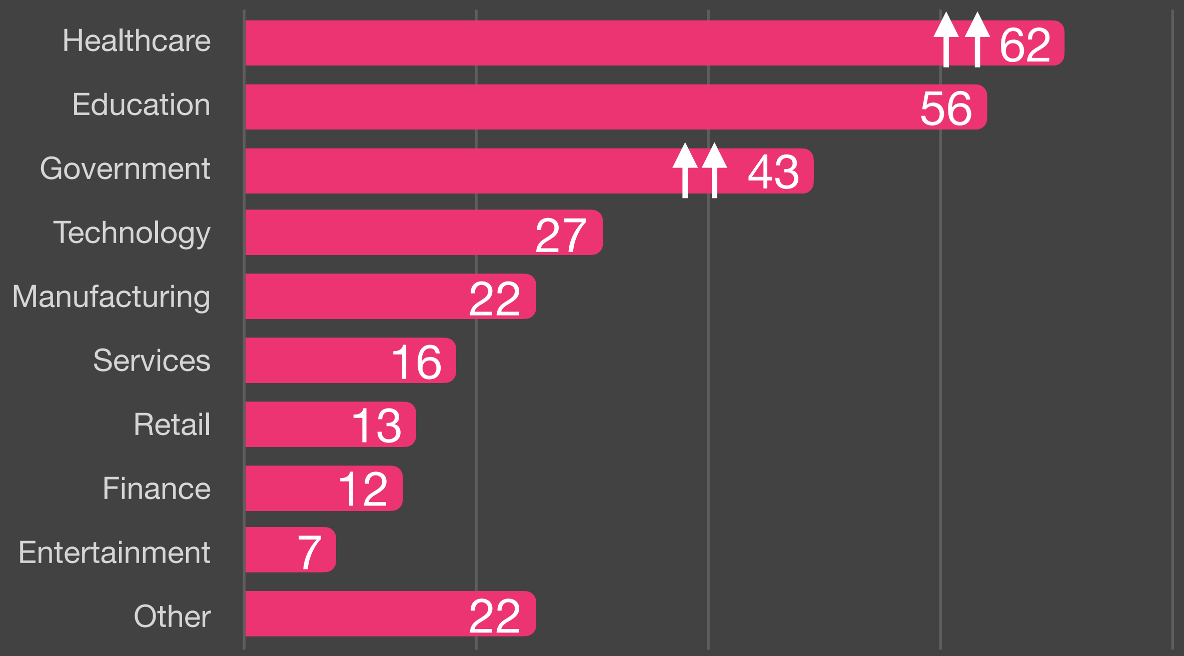
Ransomware by Country



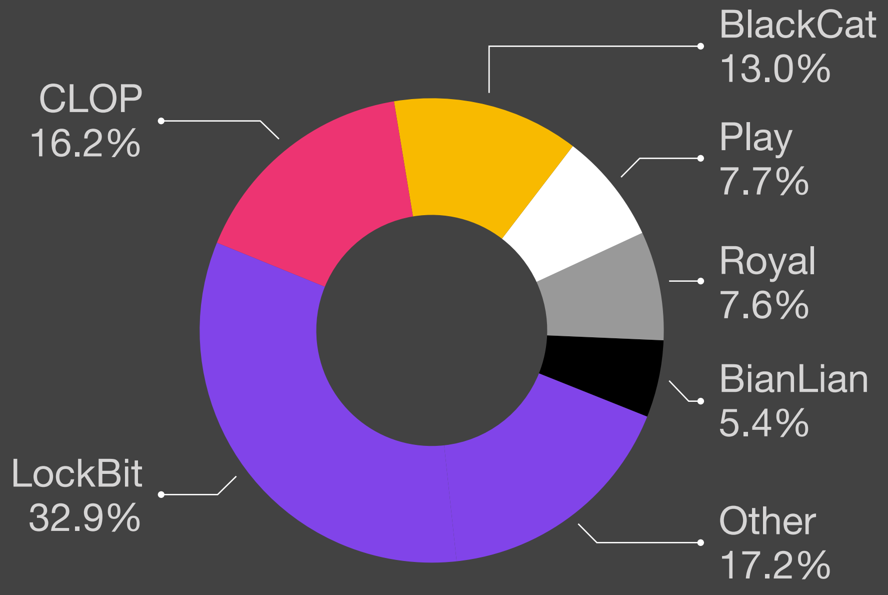
Reported Ransomware Variant



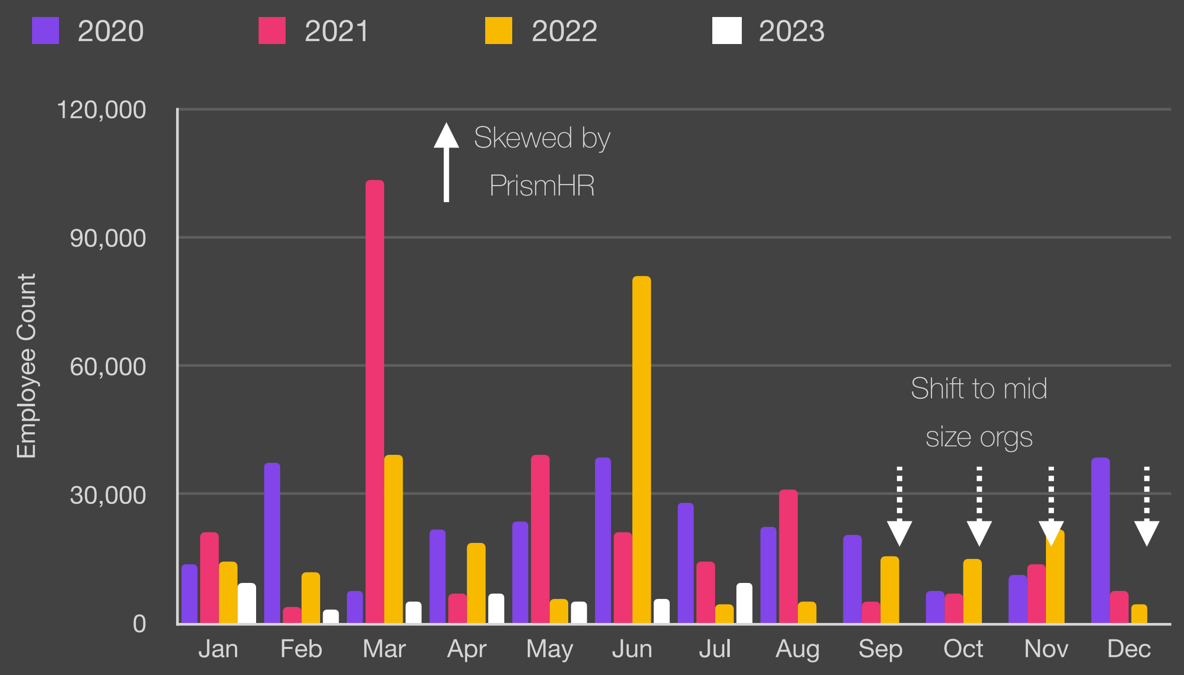
Ransomware by Industry



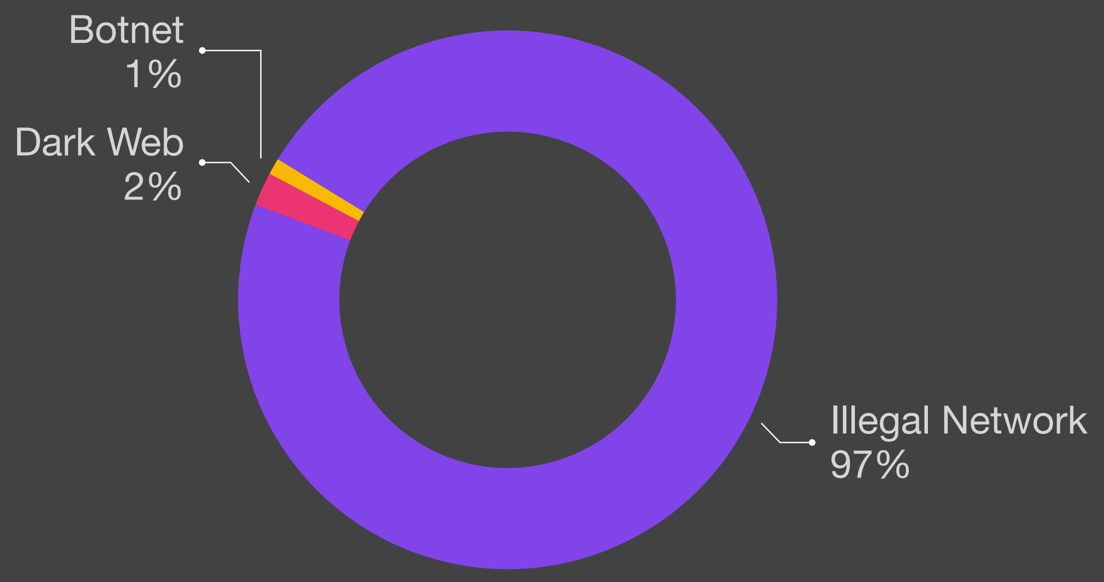
Unreported Ransomware Variant



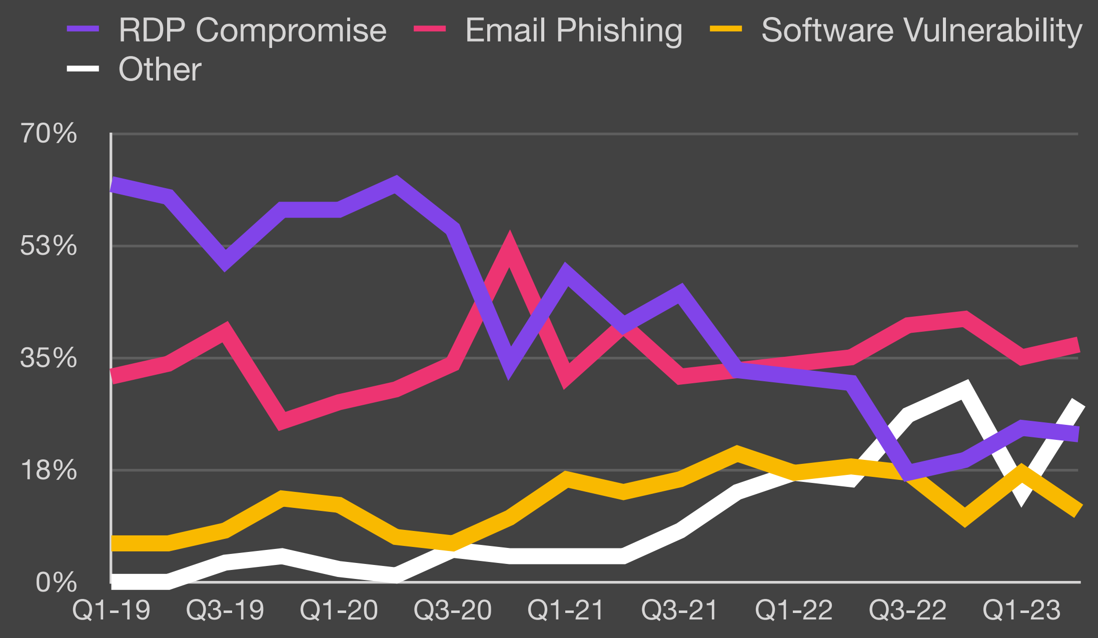
Size of Organization



Exfiltration Techniques

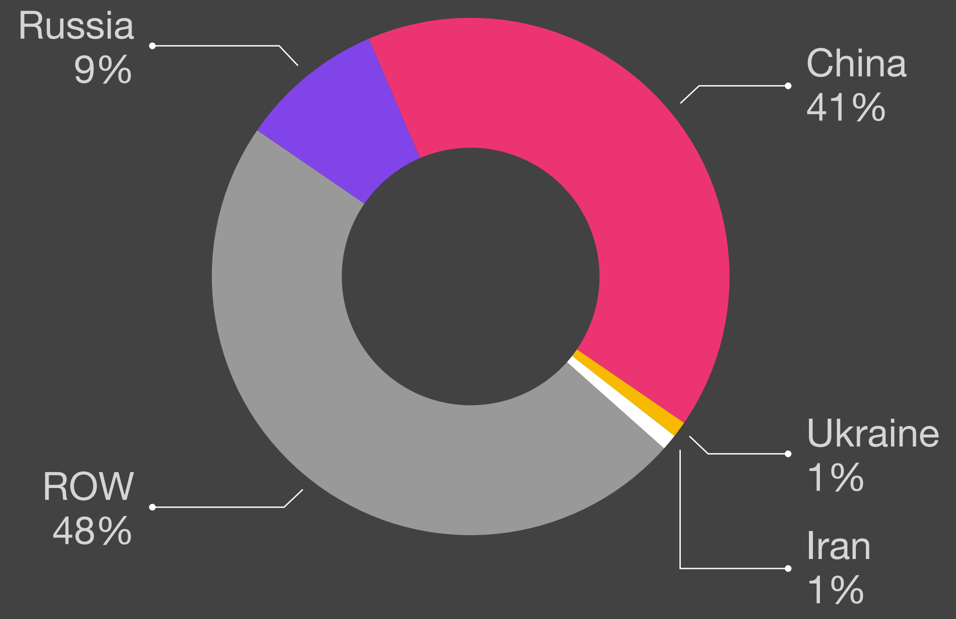


Attack Vectors[2]



[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.