January 2023

The first month of 2023 saw 33 publicly disclosed ransomware attacks, the highest number of attacks we have ever recorded for a January. The education sector topped the victim list with 11 attacks, over a third of all incidents recorded this month. Royal Mail, deemed as “critical national infrastructure” in the UK, was hit by a LockBit attack, causing severe disruption to all overseas deliveries. Clop targeted the New York City Bar, exfiltrating 1.8TB of data and posting some “unkind” words regarding their concern for data safety.

Roundup

After a record breaking 2022 we start January with yet another record, this time the highest January on record with 32 attacks, a 22% increase over 2022. We also start 2023 with new statistics and now include unreported attacks so we can see the scope of the problem. This month we see that 478% of attacks have gone unreported, a growing trend we have seen over the past year.

We also start 2023 with education leading the way with 10 attacks, 30% of the total for the month. This continues the trend we saw from 2022 followed closely by healthcare and government with 8 and 6 attacks respectively.

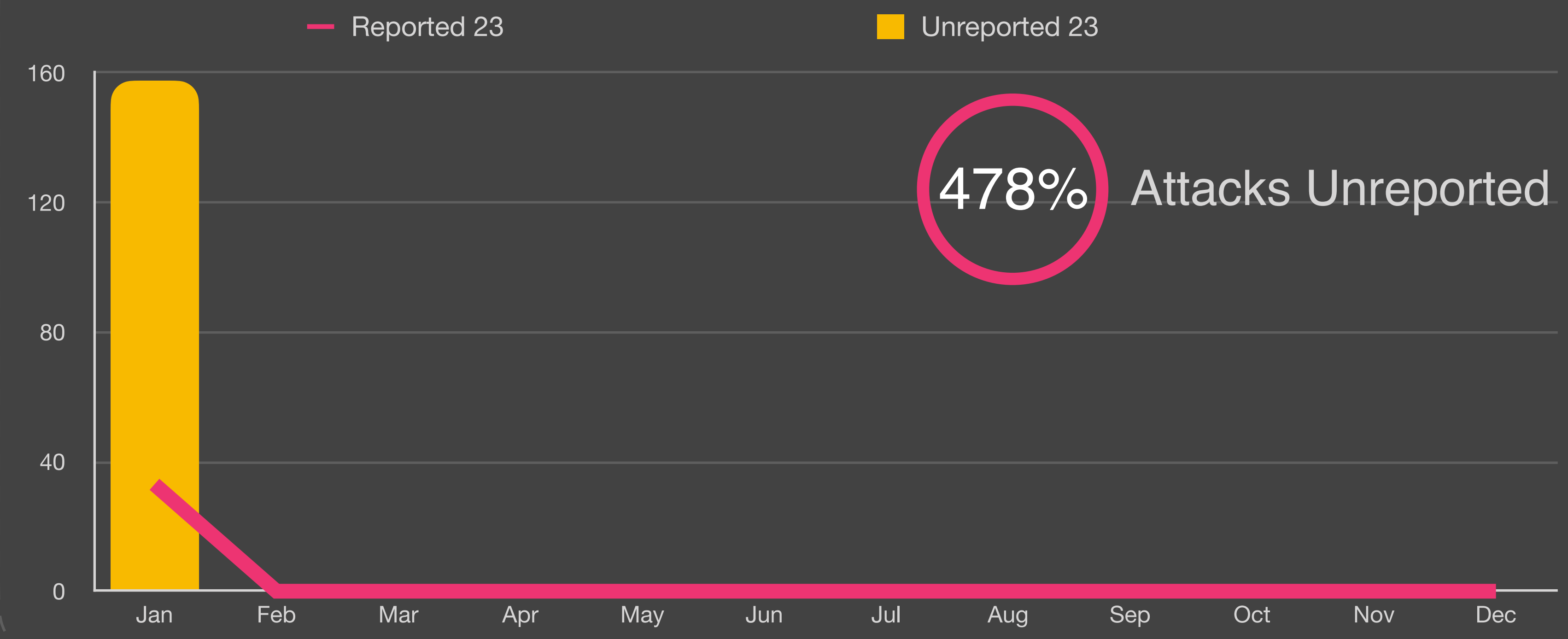
January also saw some big changes in data exfiltration, which is dominated by China, representing 36% compared to Russia at 9%. As in 2022 we see that exfiltration is now the dominant technique for ransomware and was involved in 88% of all attacks in January.

Lastly, we see that LockBit continues to be dominant variant, and expect this to increase further over the coming months and was involved in 18.8% of reported attacks, but crucially 32.6% of unreported attacks. We expect to see this reflected in next months statistics as we see some pull through from unreported to reported.

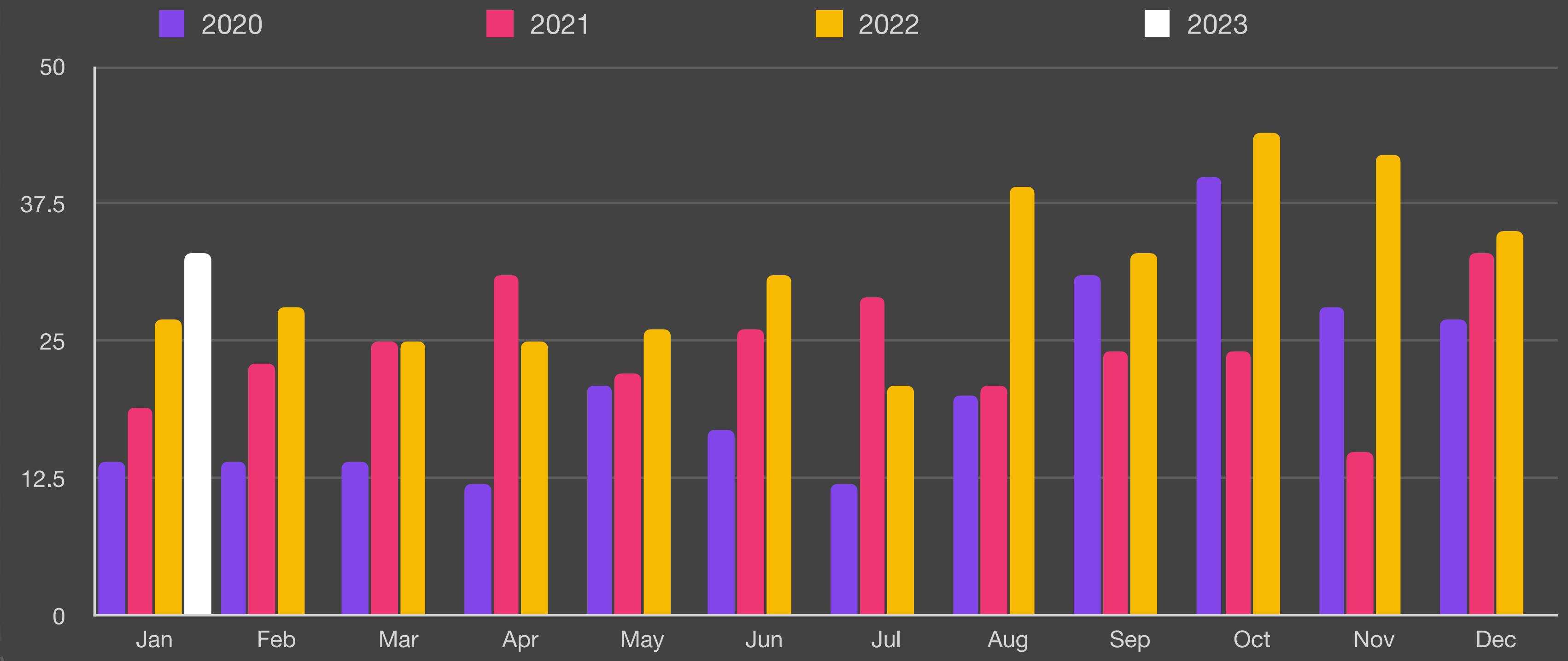
BlackFog Global Ransomware Report

January 2023

Unreported Ransom Attacks



Reported Ransomware by Month



Key Trends

478% Attacks Unreported

Jan Highest on Record

+22% Over 2022

87% of all attacks use PowerShell

88% of attacks exfiltrate data

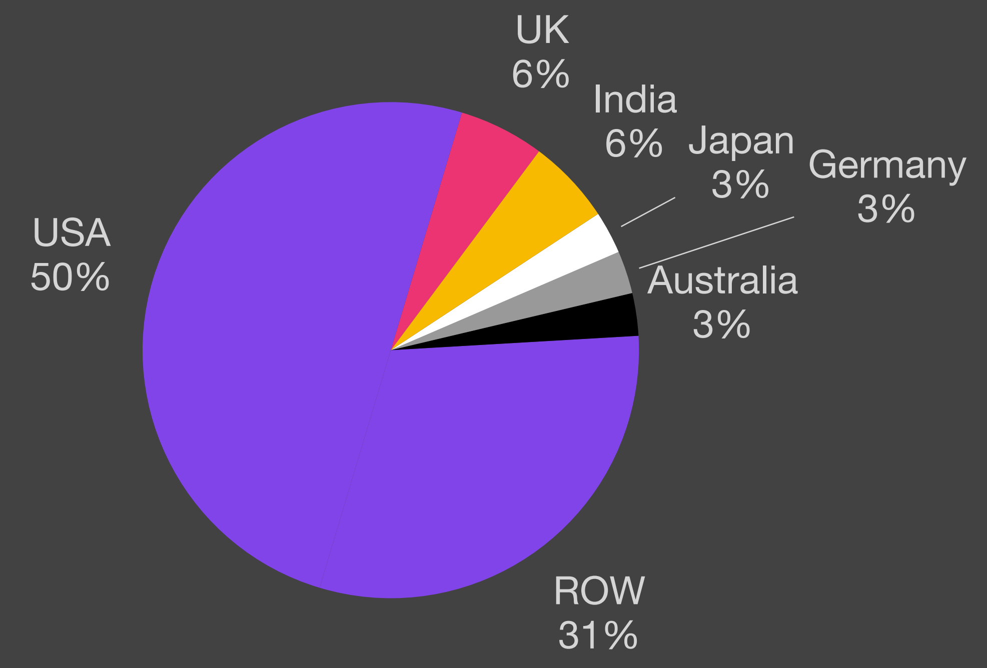
Average payout US $408,644k

+58% from Q3/22

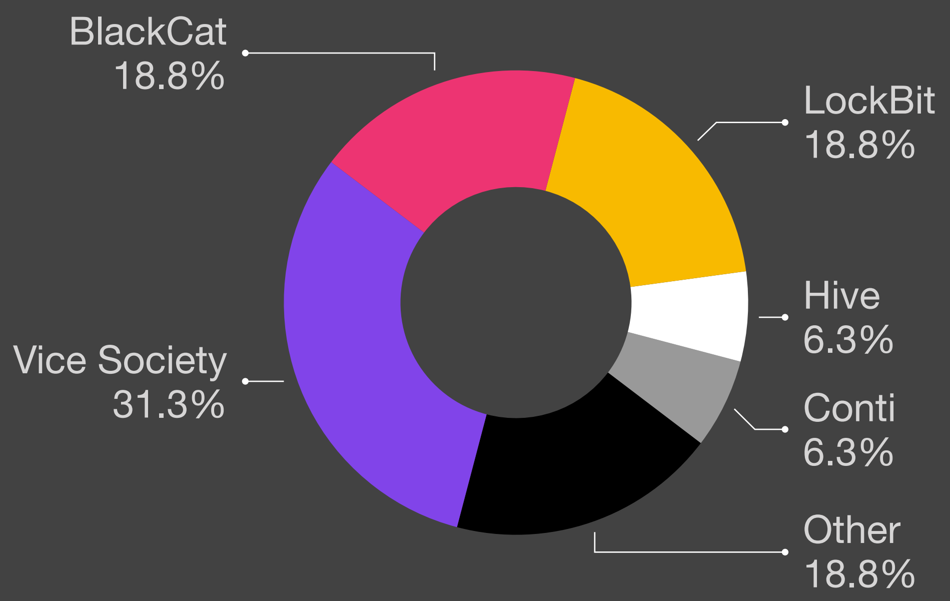
BlackFog Global Ransomware Report

January 2023

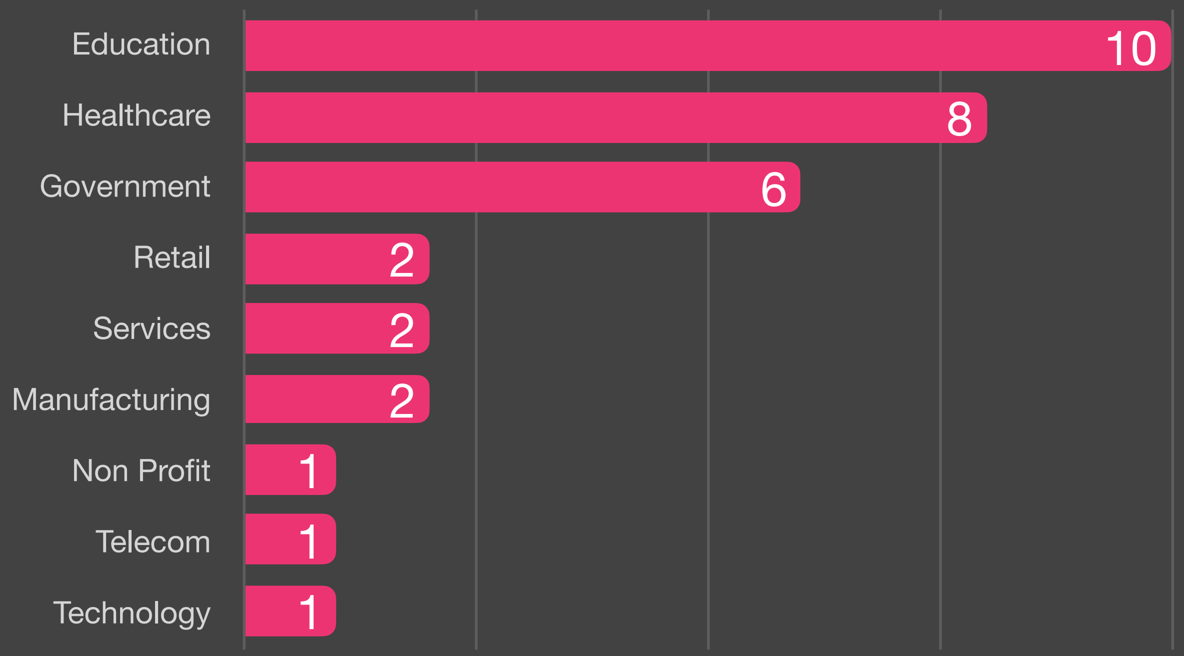
Ransomware by Country



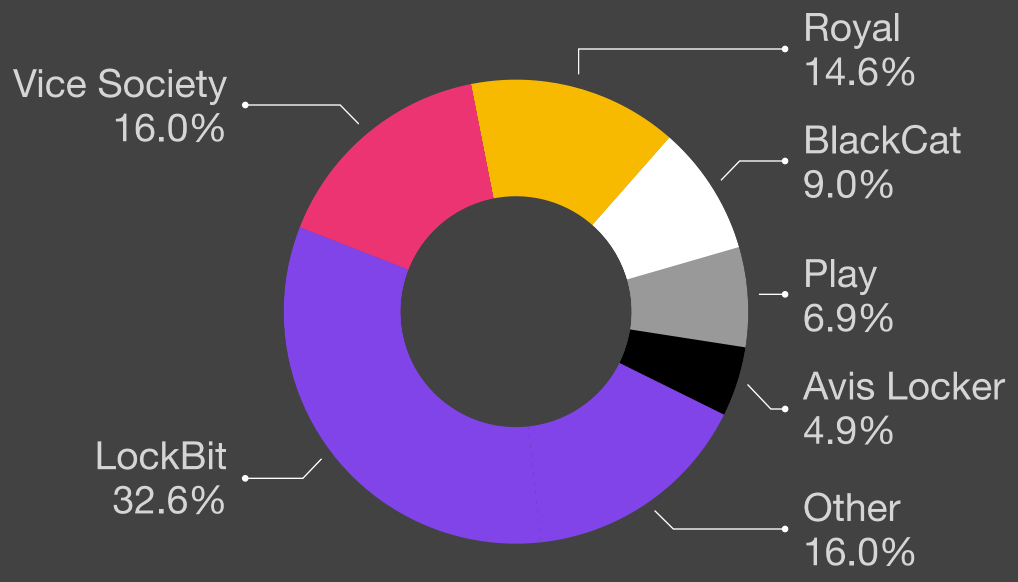
Reported Ransomware Variant



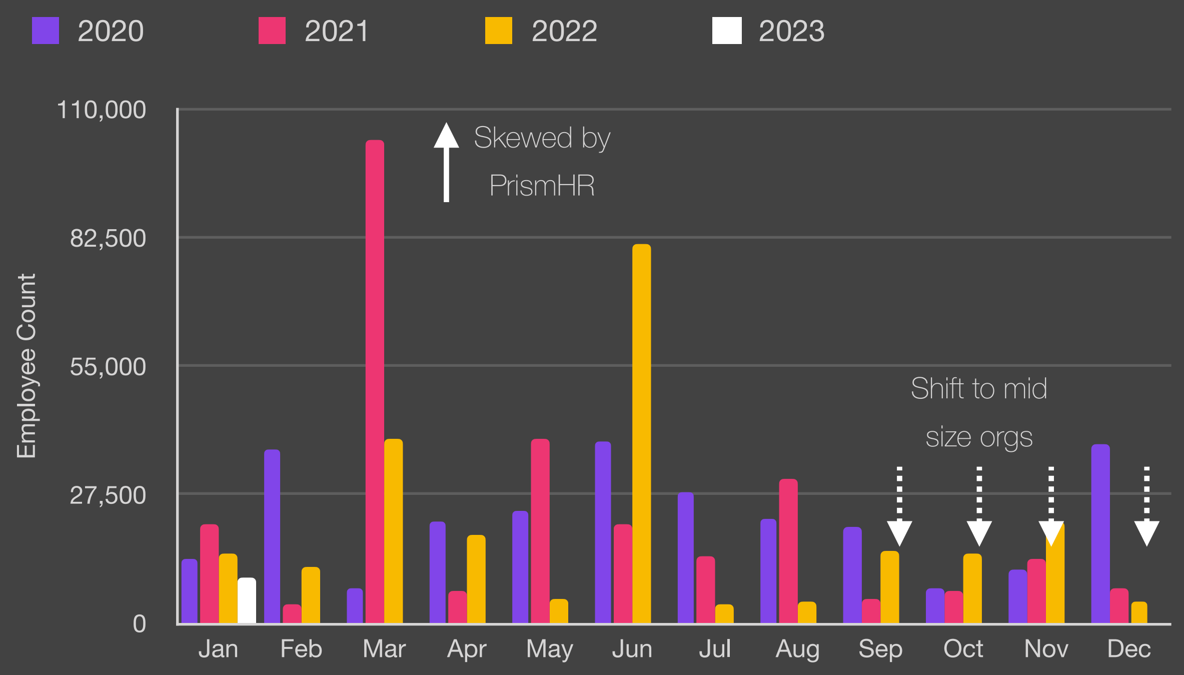
Ransomware by Industry



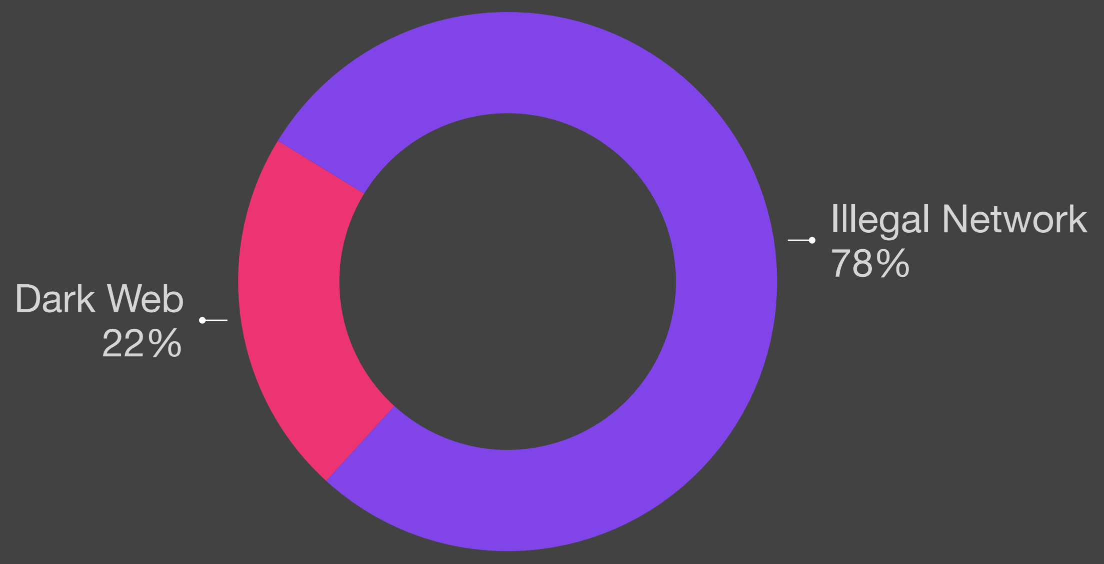
Unreported Ransomware Variant



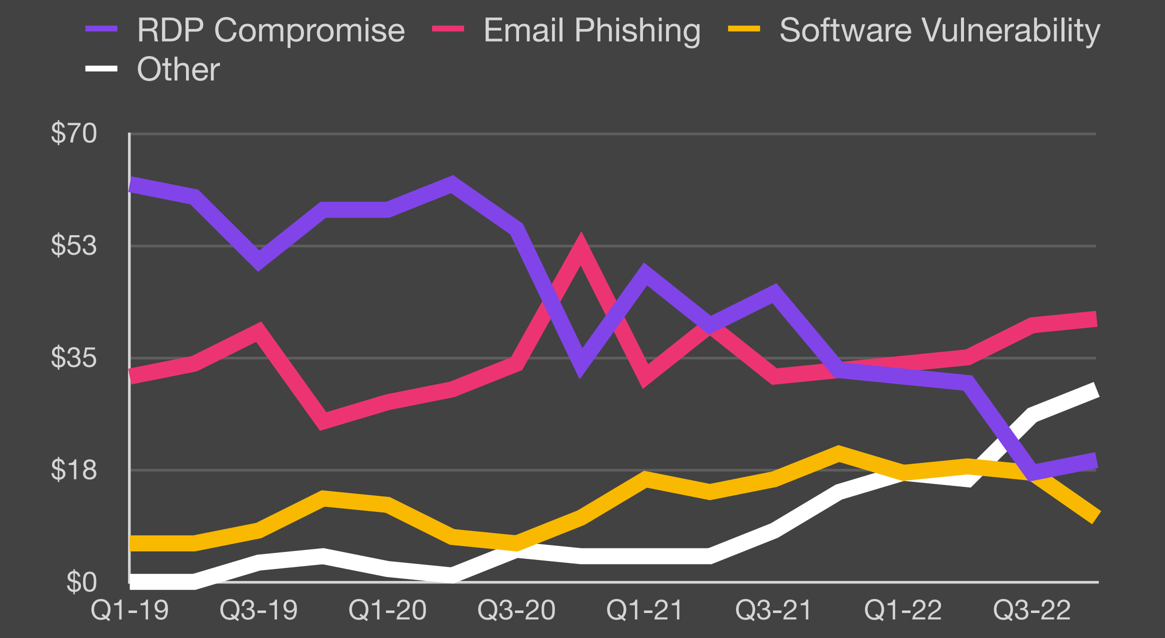
Size of Organization



Exfiltration Techniques

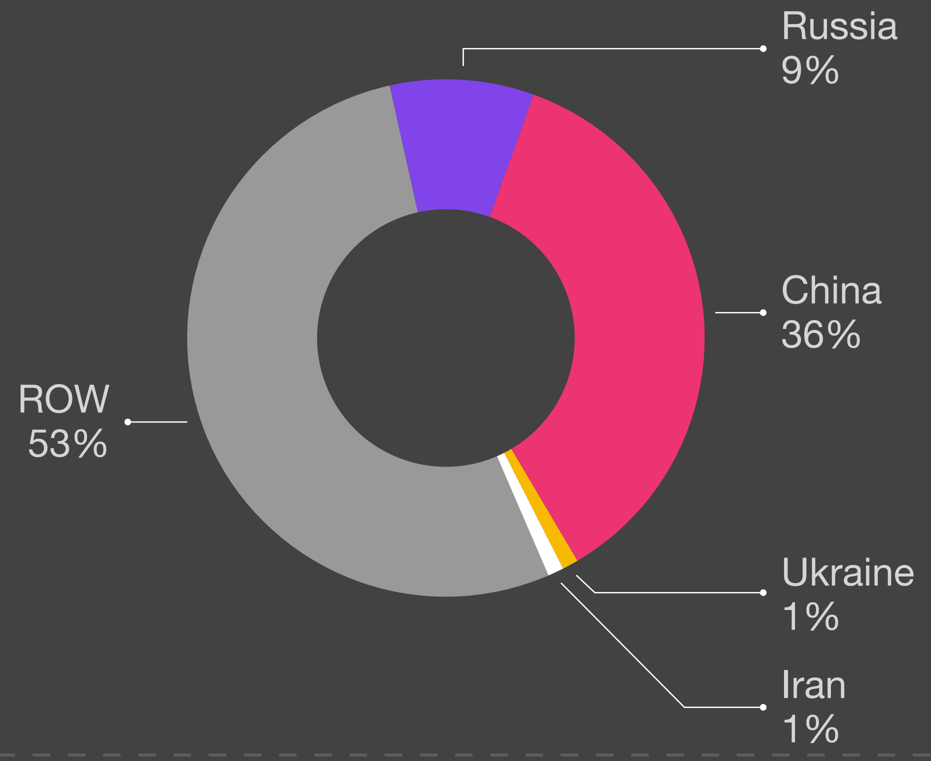


Attack Vectors[2]



[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.