February 2023

A total of 40 ransomware attacks were publicly reported in February, a 21% increase on January. Government was the most heavily targeted sector, closely follow by healthcare. Several large organizations made headlines including, ION, Five Guys and Dole Foods, while we closed out the month with an attack on the US Marshals.

Roundup

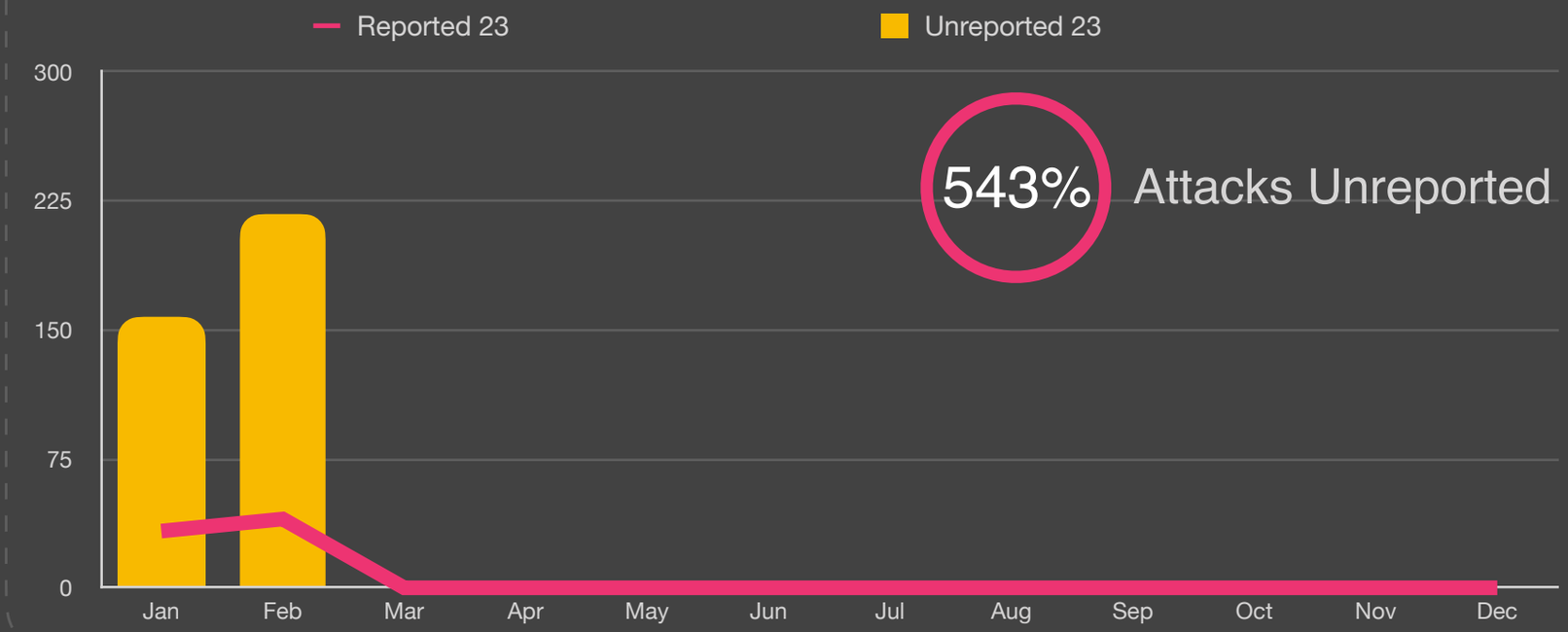
For the second month of 2023 we have seen new records broken, with February seeing a new high of 40 victims, a 43% increase from 2022. This month we continue to collect unreported data, and this month we see 543% of attacks remain unreported, a 65% increase over January.

Sector wise we saw education continue to dominate with 17 victims, and healthcare and government closely behind with 15 each. Government attacks saw the biggest increase in February, with a 150% increase since January, while Healthcare and Education saw 88% and 70% increases respectively.

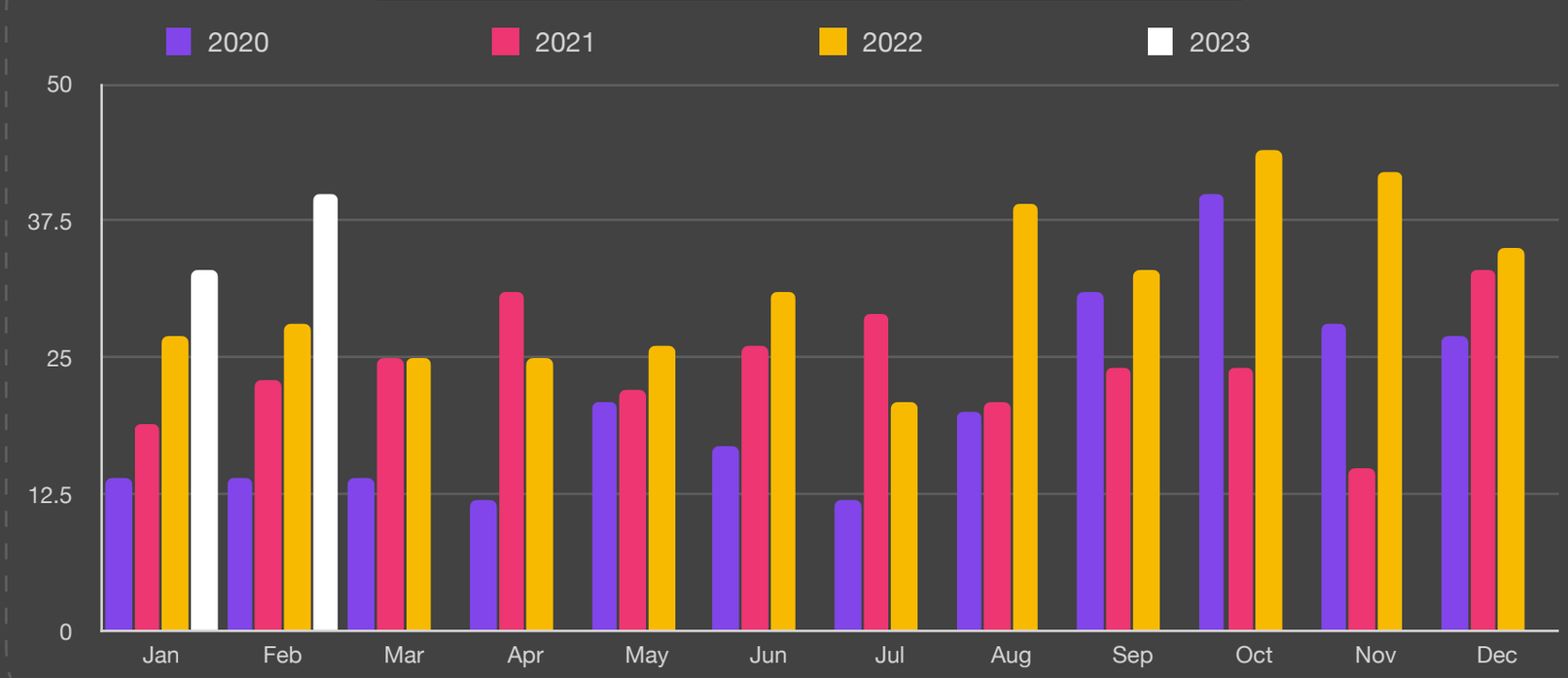
Data exfiltration continues as the main weapon of choice for ransomware and is used in 88% of all attacks. This month we also saw an increased number of attacks originating from China, which now represents 38% of all attacks, up from 36% in January. Russia remains stable at 9%.

Finally, in terms of variants, as we predicted in January we saw a dramatic increase in attacks from LockBit, as victims from previous months begin to disclose attacks. We expect this pattern to continue as unreported attacks continue to be dominated by LockBit, which is at 48%, while disclosed is at 24.3%. BlackCat also increased to 24.3%, although the growth in unreported remains significantly lower.

Unreported Ransom Attacks



Reported Ransomware by Month



Key Trends

543% Attacks Unreported

Feb Highest Feb in 4 years

+43% Over 2022

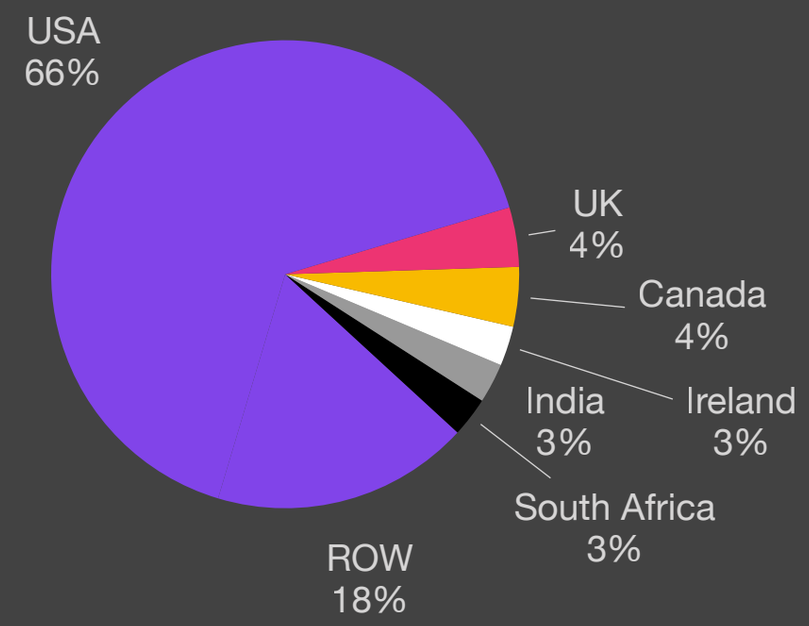
84% of all attacks use PowerShell

88% of attacks exfiltrate data

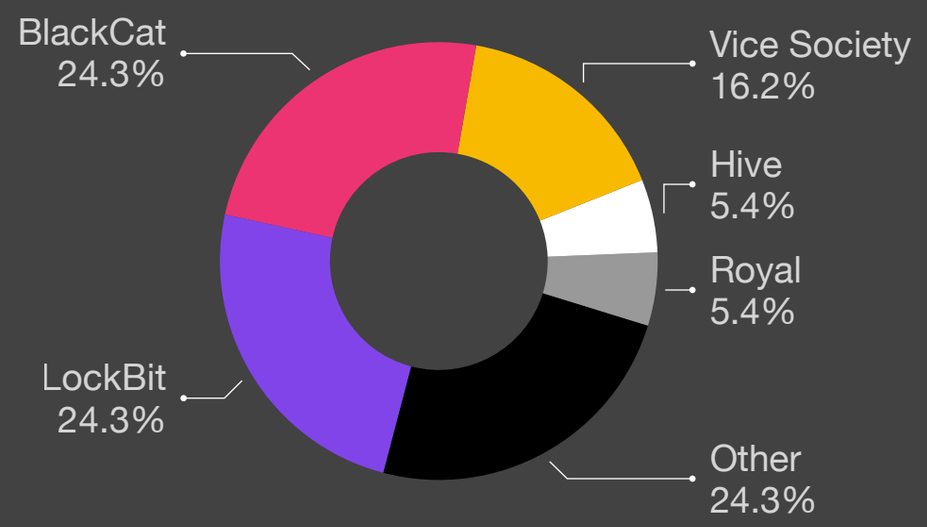
Average payout US $408,644k

+58% from Q3/22

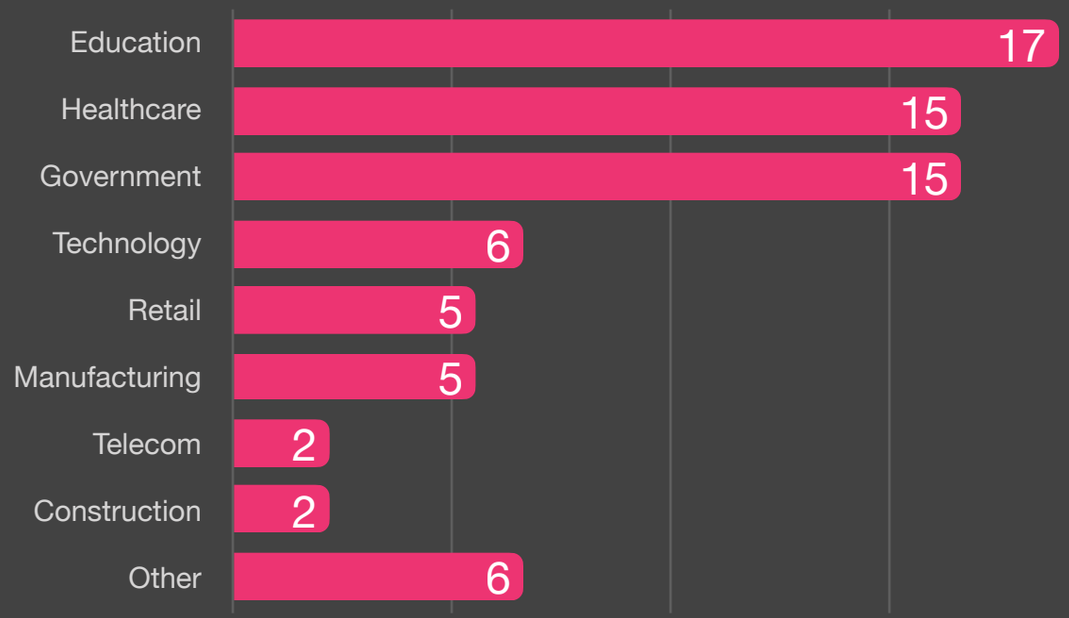
Ransomware by Country



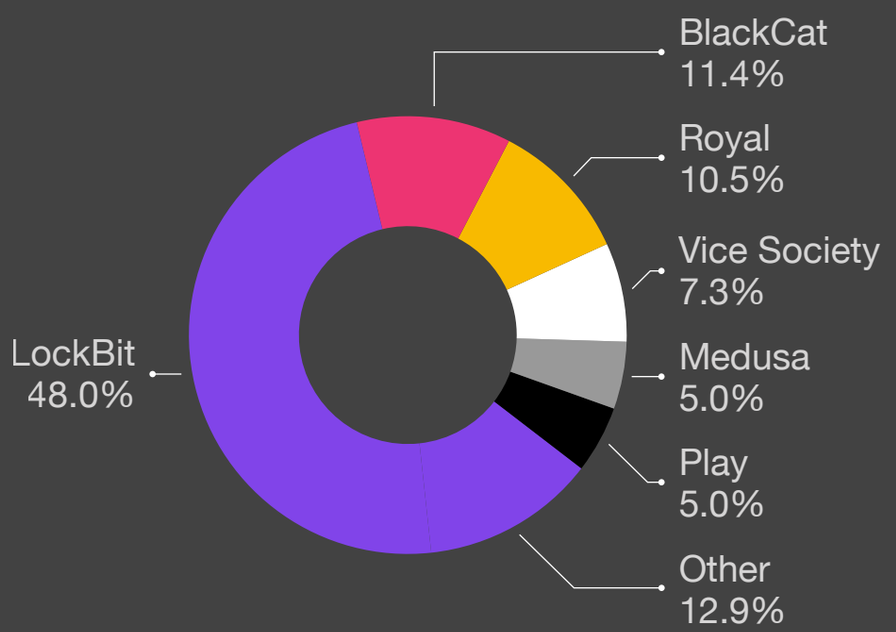
Reported Ransomware Variant



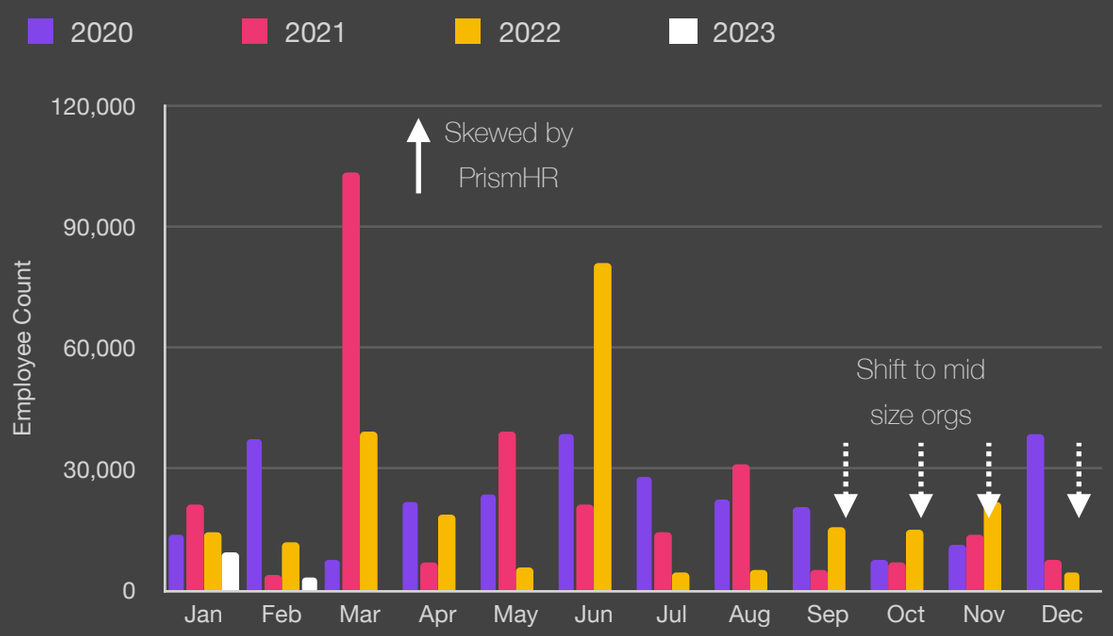
Ransomware by Industry



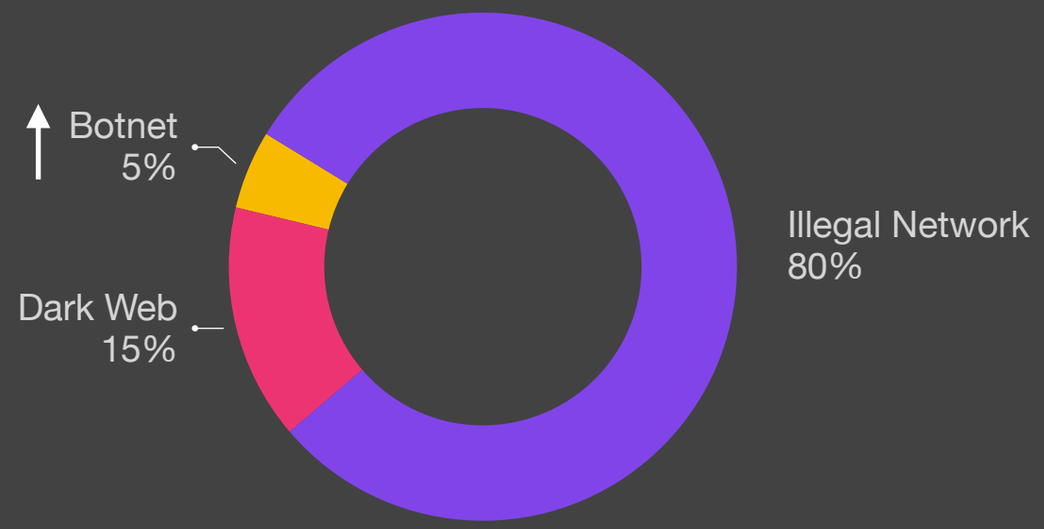
Unreported Ransomware Variant



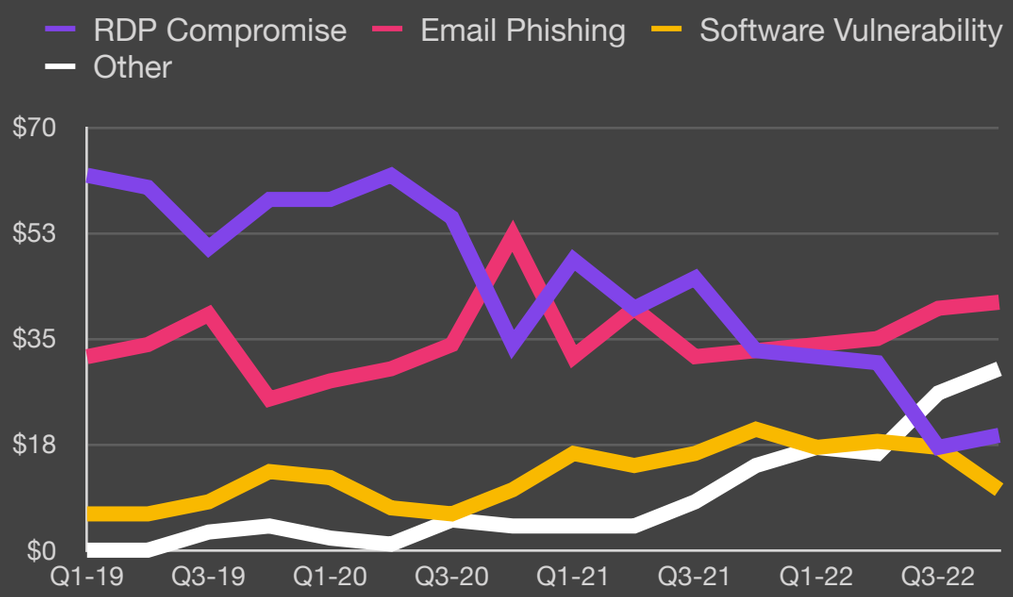
Size of Organization



Exfiltration Techniques

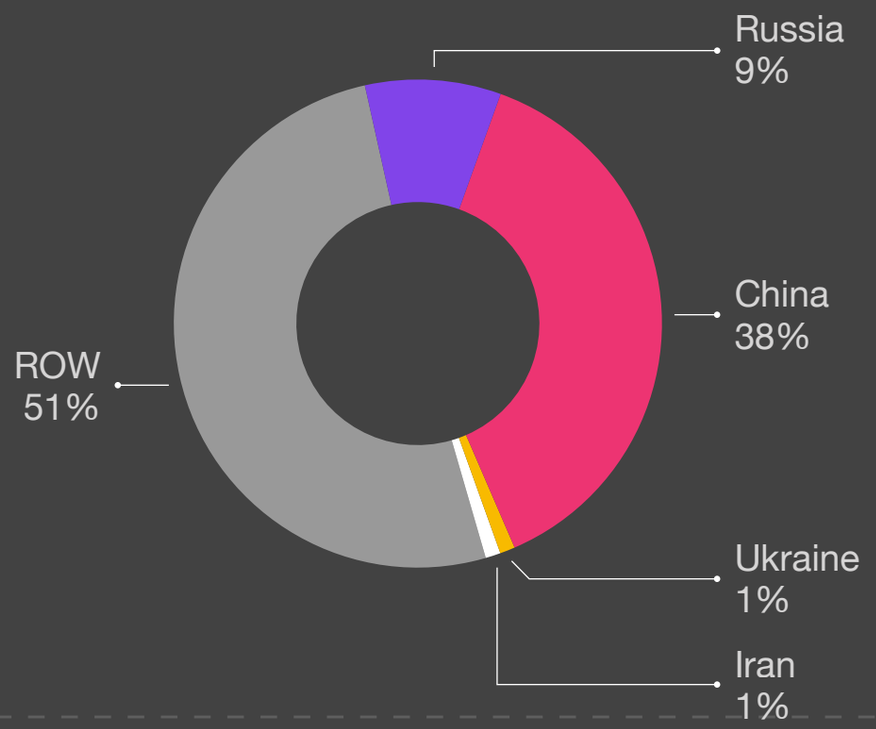


Attack Vectors[2]



[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.