December 2023

December is historically one of the quieter months of the year for ransomware, but this was not the case in 2023, with seventy publicly disclosed ransomware attacks recorded. This figure sees a massive 97% increase on December last year. LockBit and BlackCat remained the two most active variants, while we also saw new variants such as DragonForce make its mark on the ransomware landscape. Healthcare was the most impacted industry with high profile attacks on **Integris Health** and **Fred Hutchinson Cancer Center** making headlines during the month.

Roundup

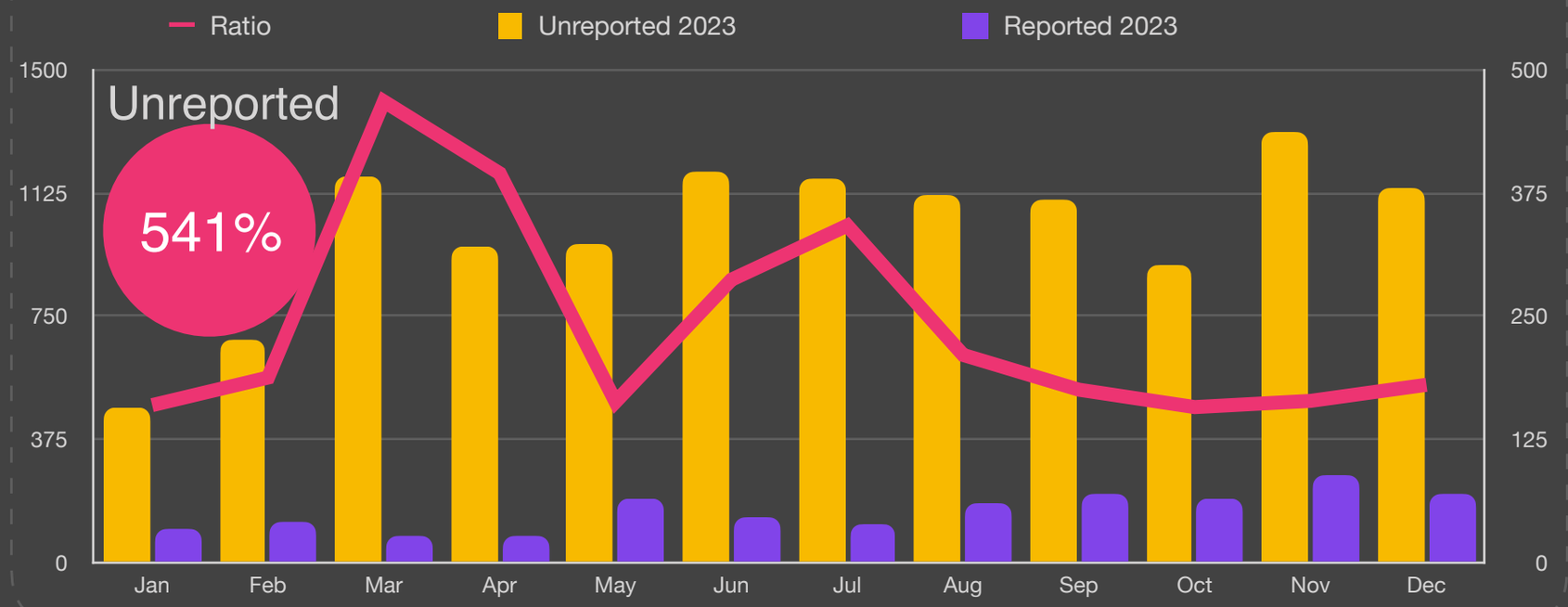
In December we continued to see new records, finishing with the second highest number of attacks on record with a total of 70. The latter half of 2023 saw twice the number of attacks as 2022 and shows no signs of slowing down. The unreported attack ratio was 541%, meaning companies were only reporting 1 in 5 attacks globally. While this is off its peak of 10 to 1 earlier in the year, it is still significantly higher than we would like to see.

We are hoping the new SEC reporting requirement should have some impact in January as this is now in full effect.

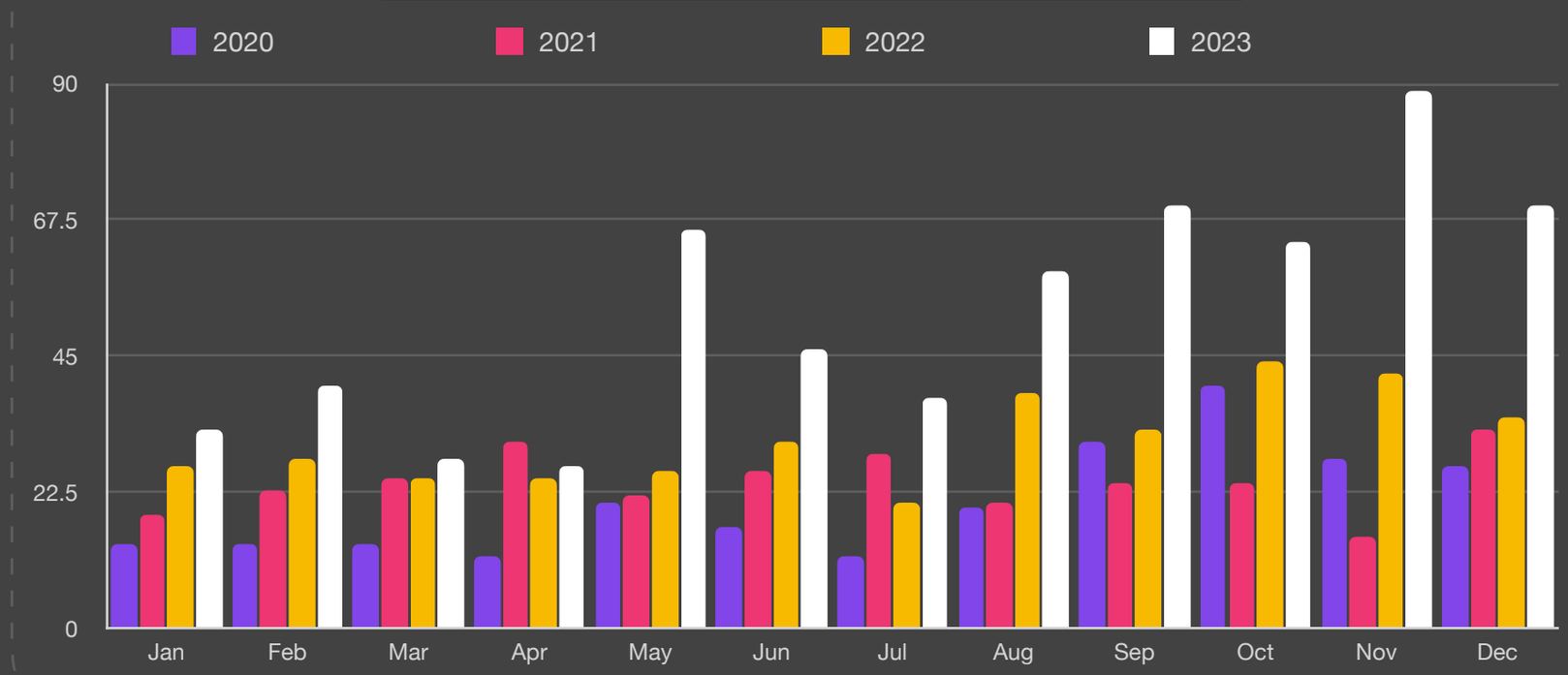
Healthcare finished the year as the most targeted sector with 138 attacks, and increase of 15% over the previous month. As expected, the holiday season saw increased pressure on both the retail and finance sectors with 23% and 18% increases respectively. This month also witnessed significant increases in manufacturing, education, technology and services of 20%.

In terms of variants we saw LockBit and BlackCat continue to dominate reported attacks with 19.2% and 18.4% respectively. LockBit also dominated the unreported attacks at 35.3% and BlackCat at 14.1%. Data exfiltration continues to dominate as the primary mechanism for extortion, now at 91% with traffic exfiltration to China at 29% and Russia 9%.

Unreported Ransom Attacks



Reported Ransomware by Month



Key Trends

541% Unreported

2nd Highest of Year

1st Highest December Ever

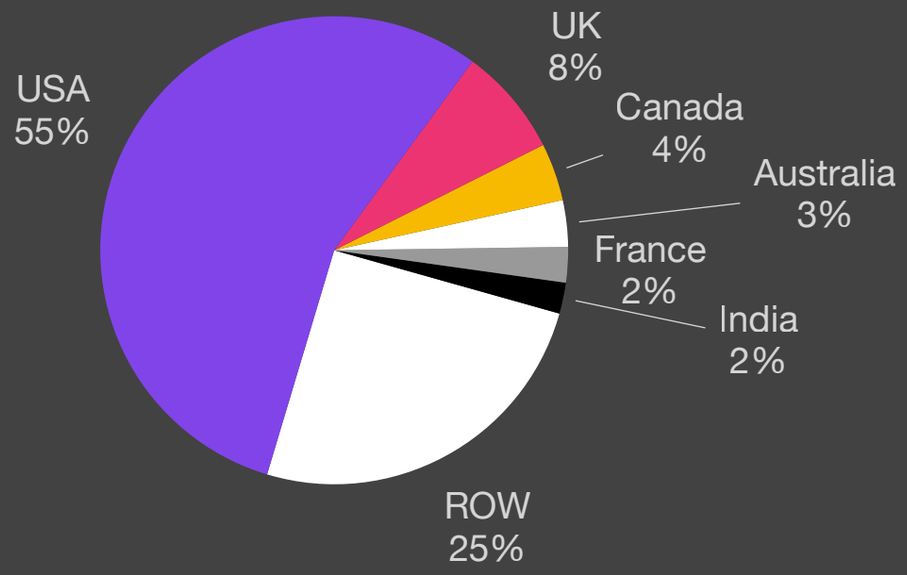
43% of all attacks use PowerShell

91% of attacks exfiltrate data

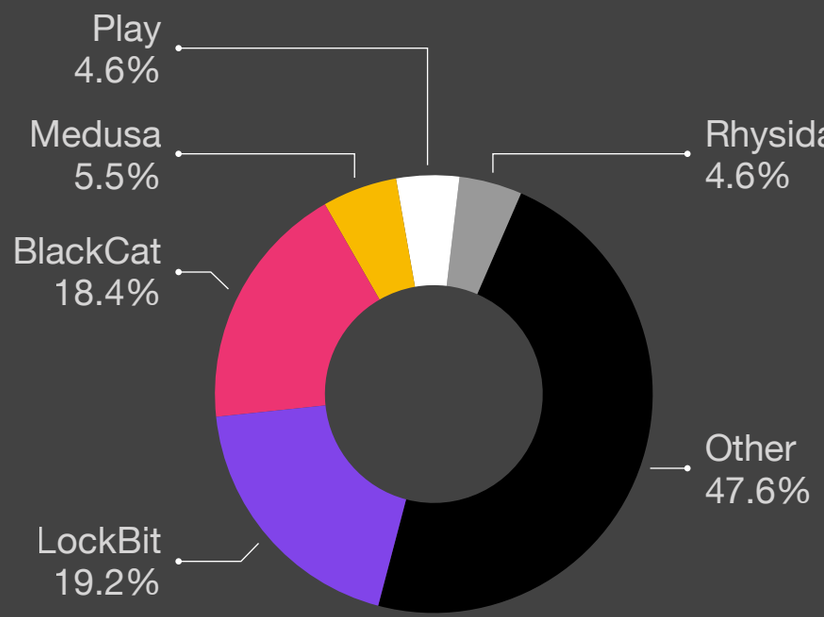
Average payout US $850,700

+15% from Q2/23

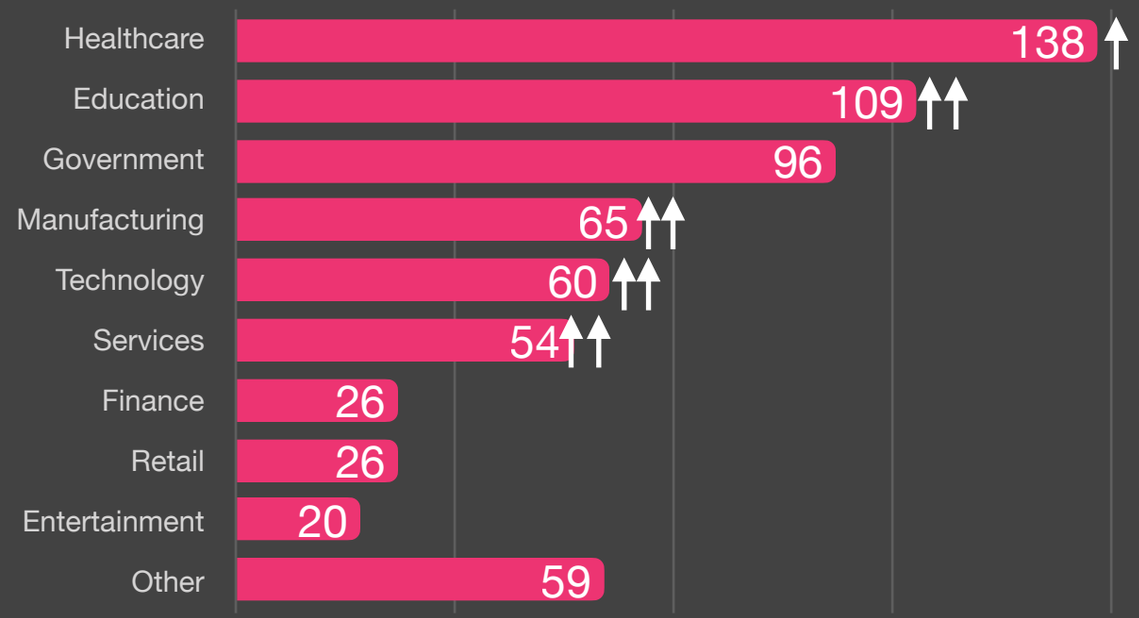
Ransomware by Country



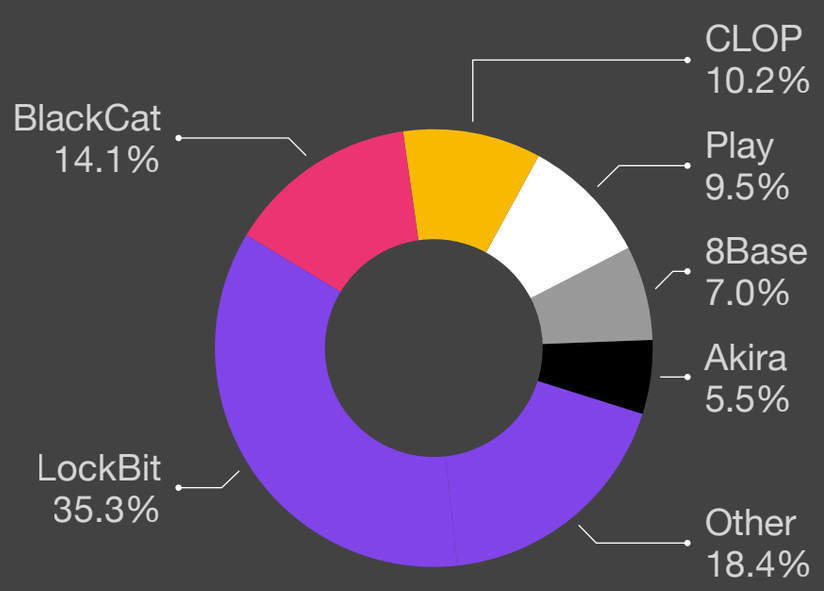
Reported Ransomware Variant



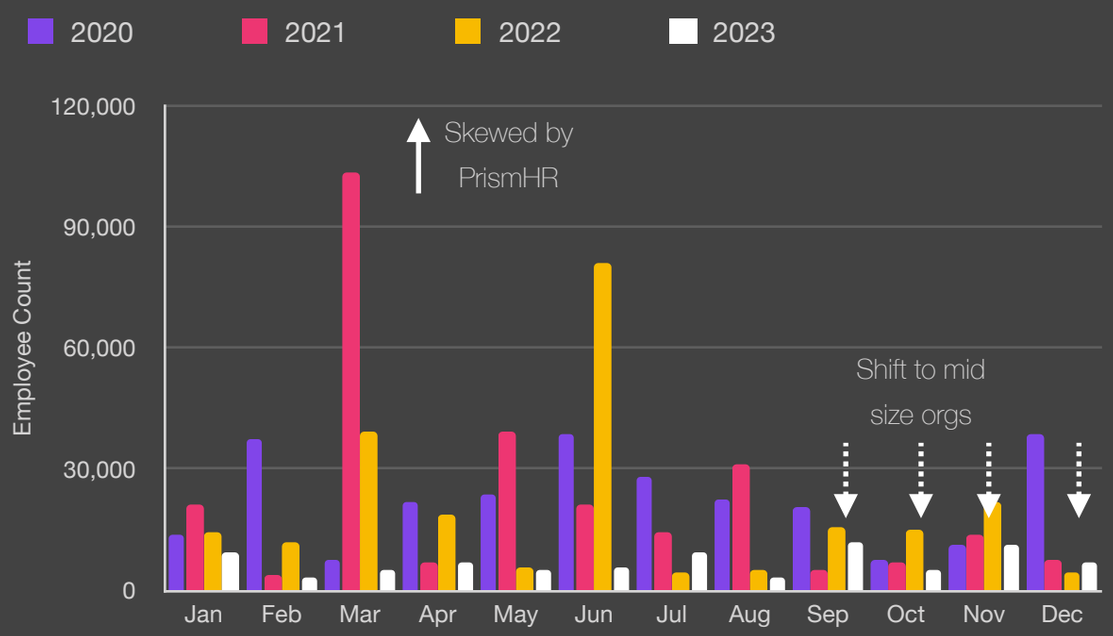
Ransomware by Industry



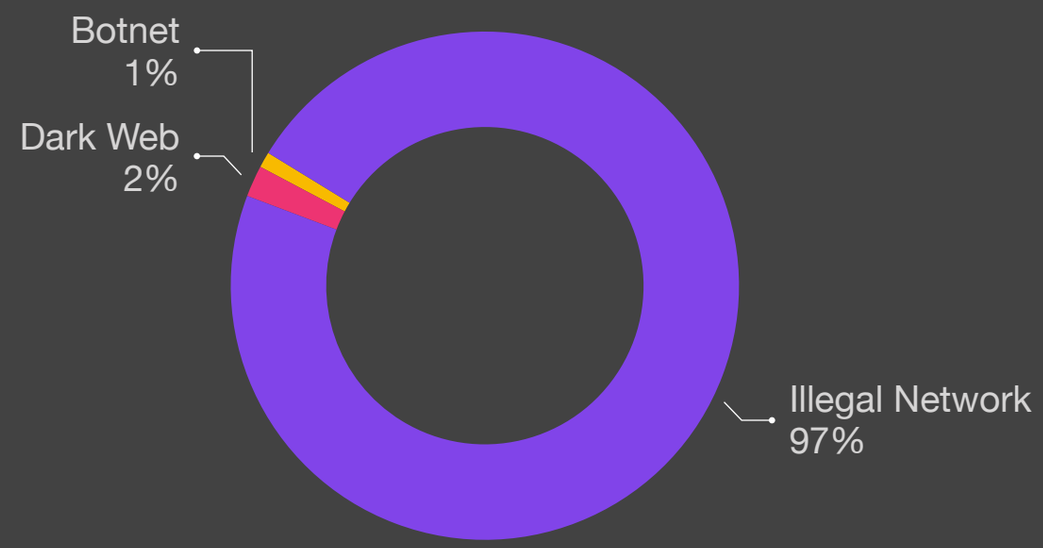
Unreported Ransomware Variant



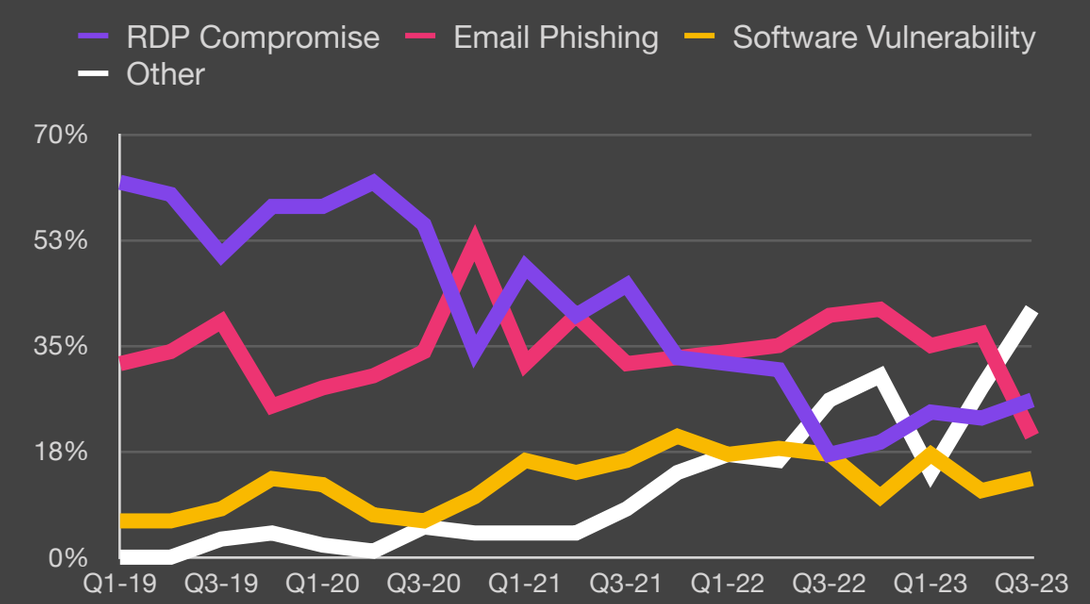
Size of Organization



Exfiltration Techniques

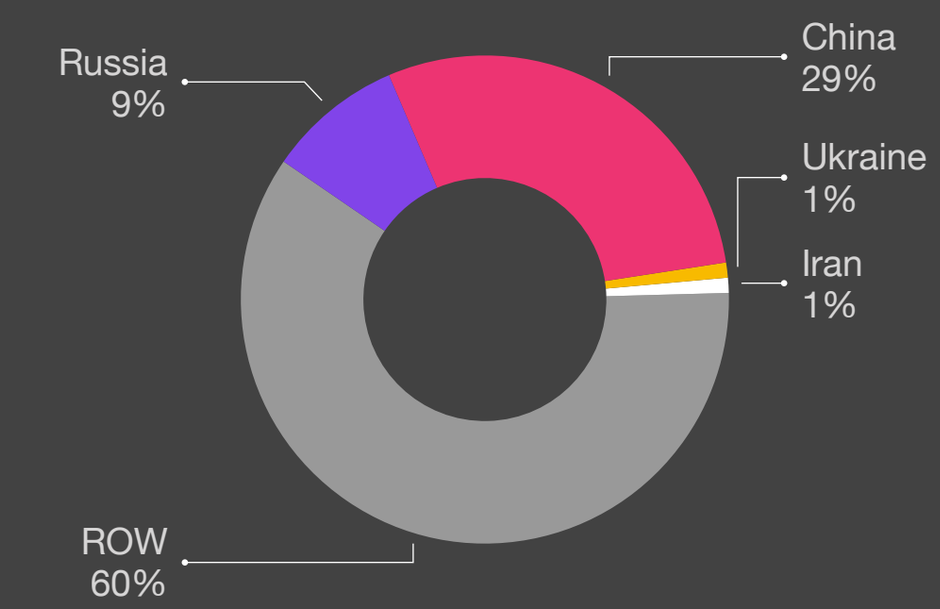


Attack Vectors[2]



[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.