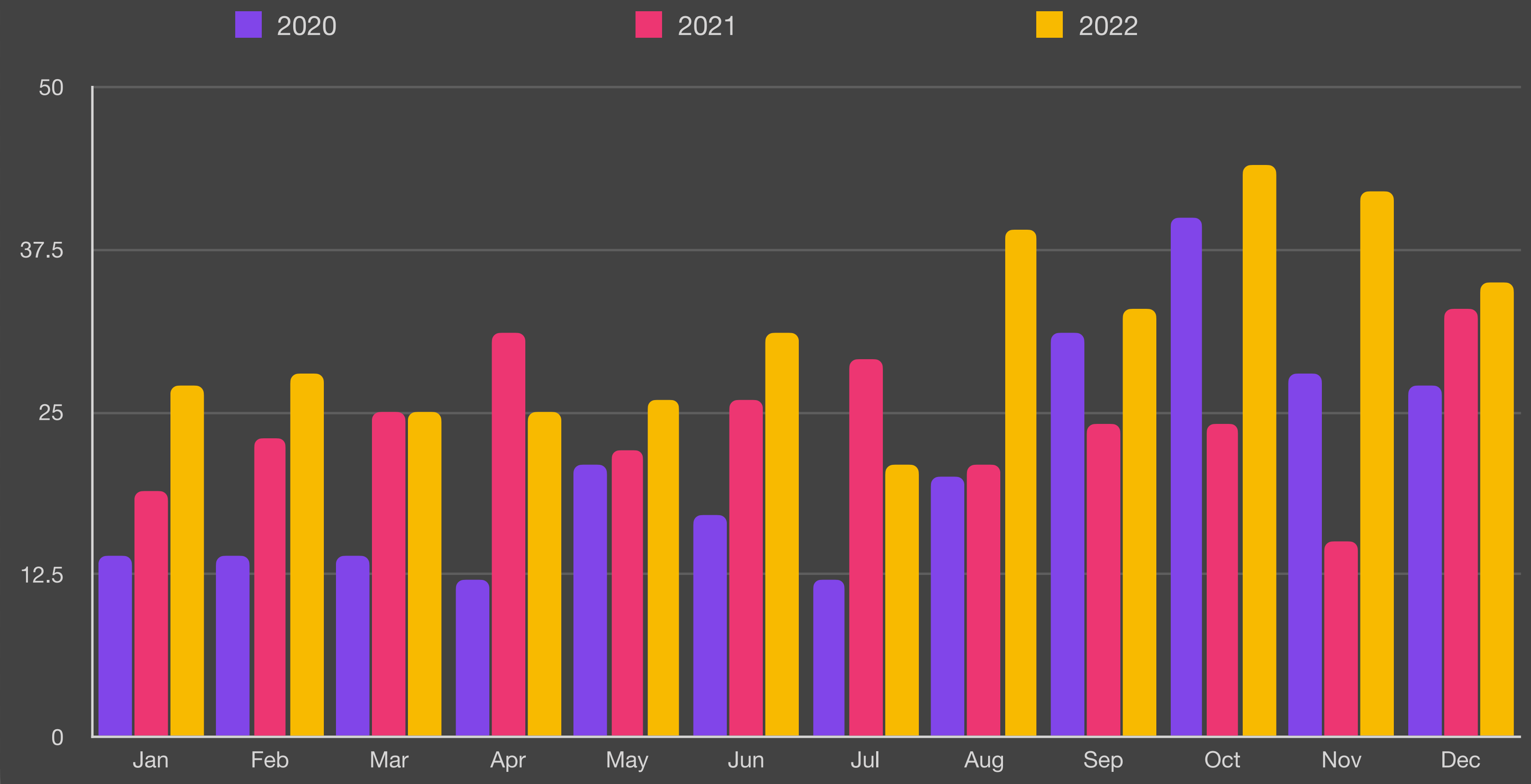
December 2022

We finish the year with 35 reported ransomware attacks, the busiest December recorded in three years. December saw some interesting twists, including an apology and a free decryptor from the LockBit criminal gang after a ‘partner’ launched an attack on the the Toronto Hospital for Sick Children. In another interesting twist, California based toy manufacturer Jakks had their data locked by Hive and BlackCat/ALPHV on the same day. The two groups agreed on a ransom of $5million to prevent either group from leaking data. UK based newspaper publisher The Guardian also made its own headlines when they were the first to report an attack on themselves over the Christmas period.

Ransomware Trend by Month



Key Trends

87% of all attacks use PowerShell

89% of attacks exfiltrate data

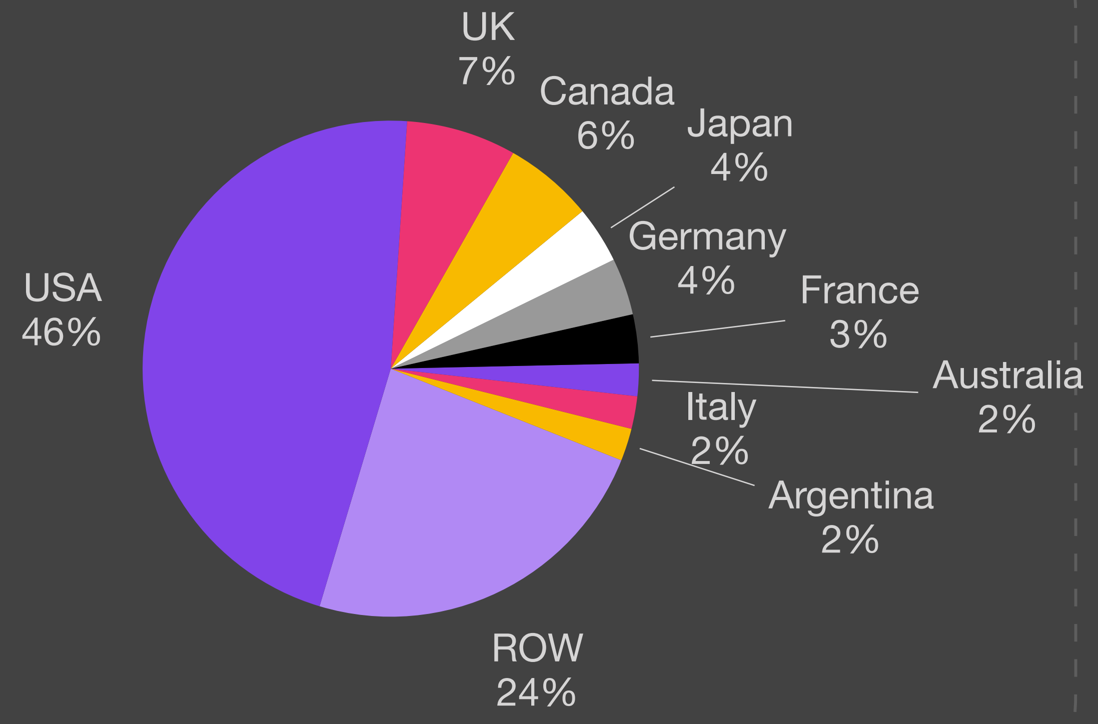
Average payout US $258,143k

+13.2% from Q2/22

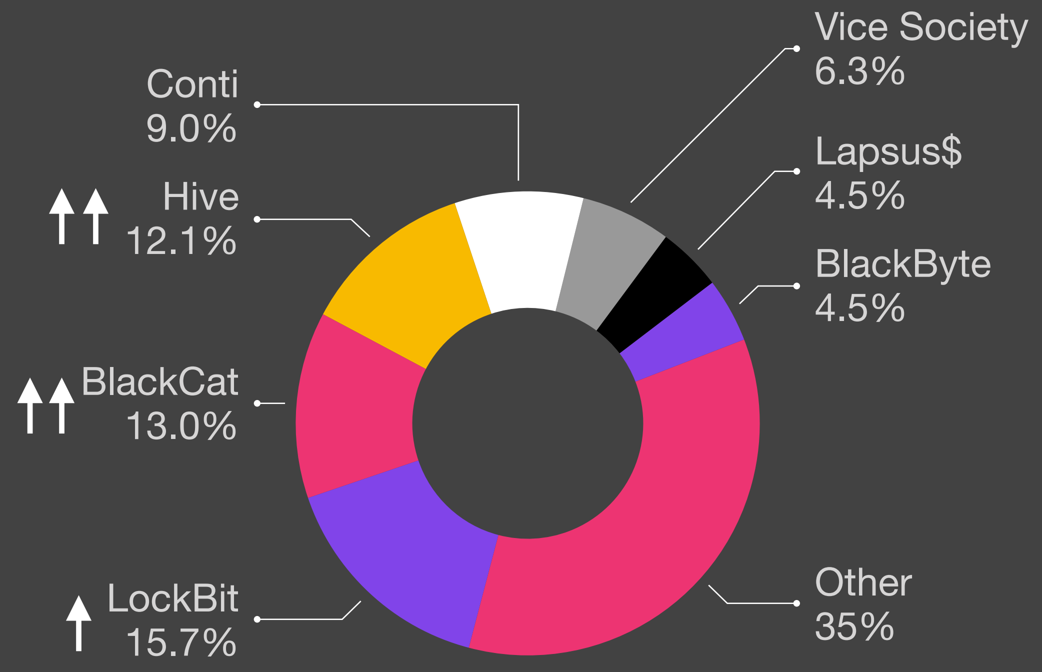
BlackFog Global Ransomware Report

December 2022

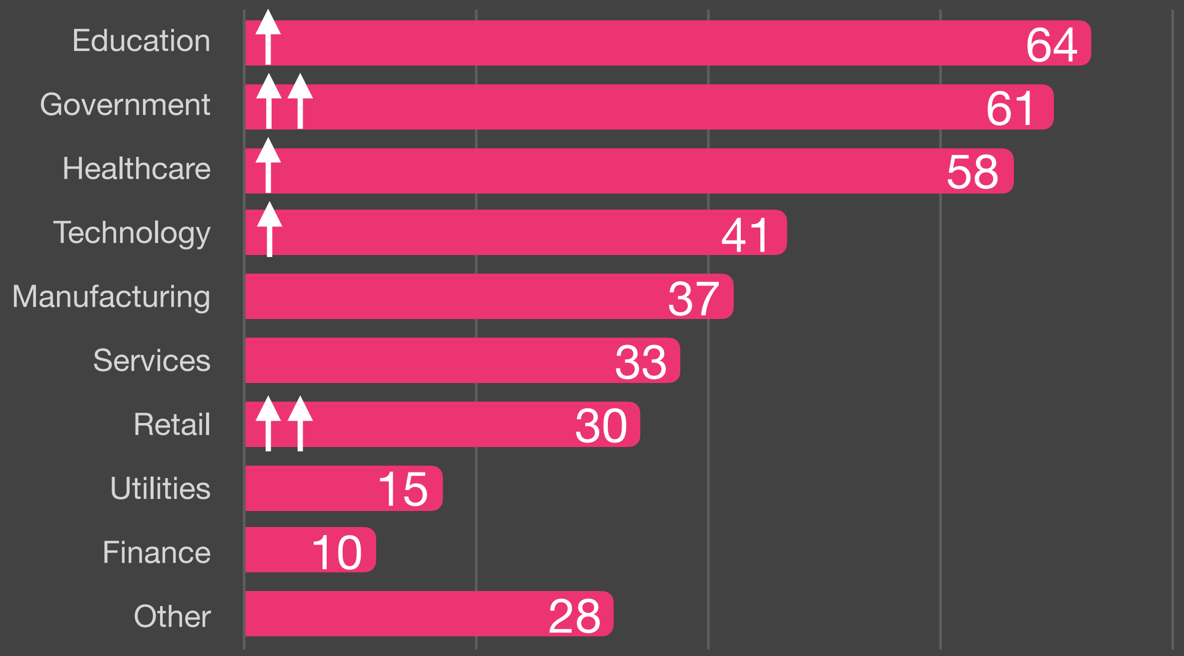
Ransomware by Country



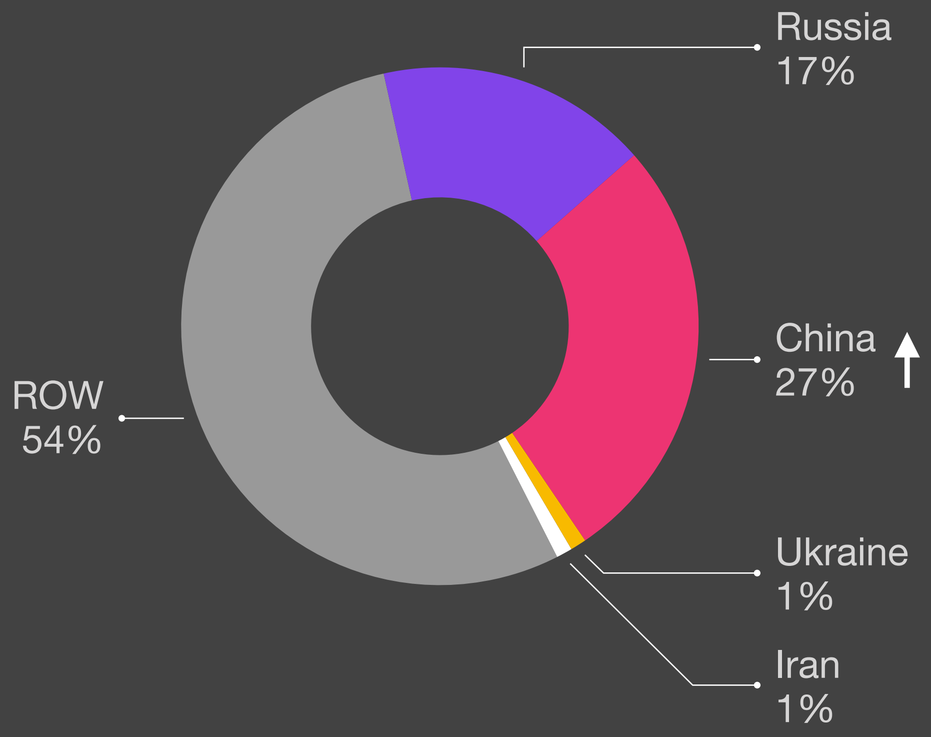
Ransomware by Variant



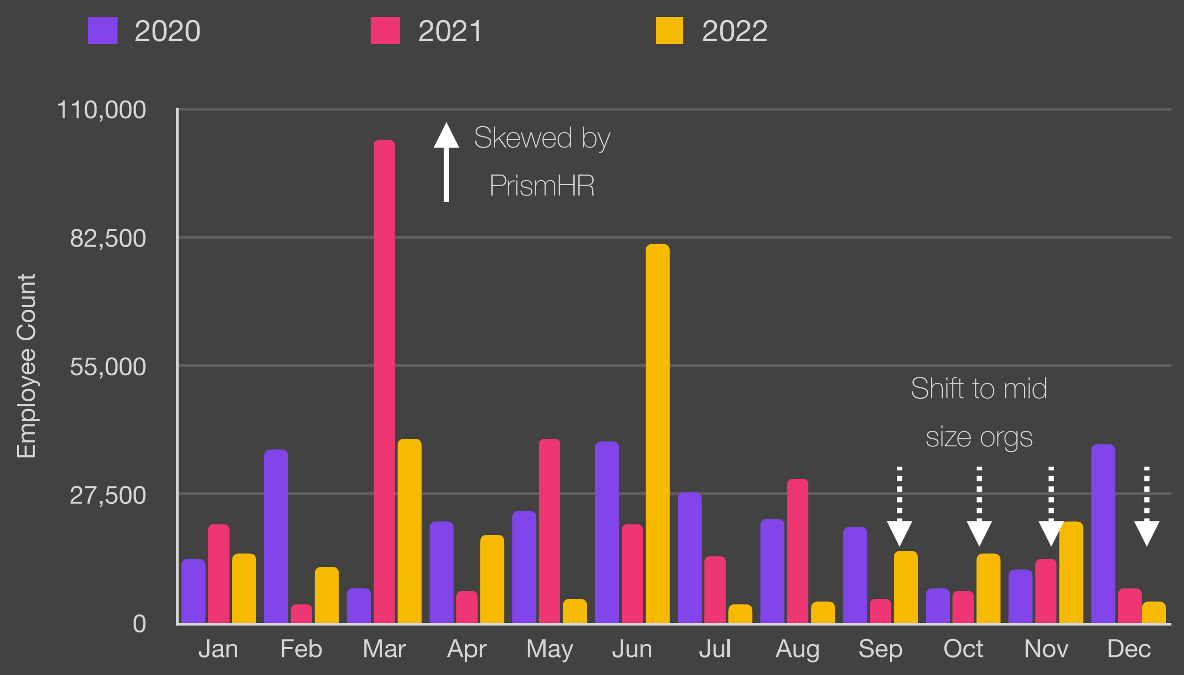
Ransomware by Industry



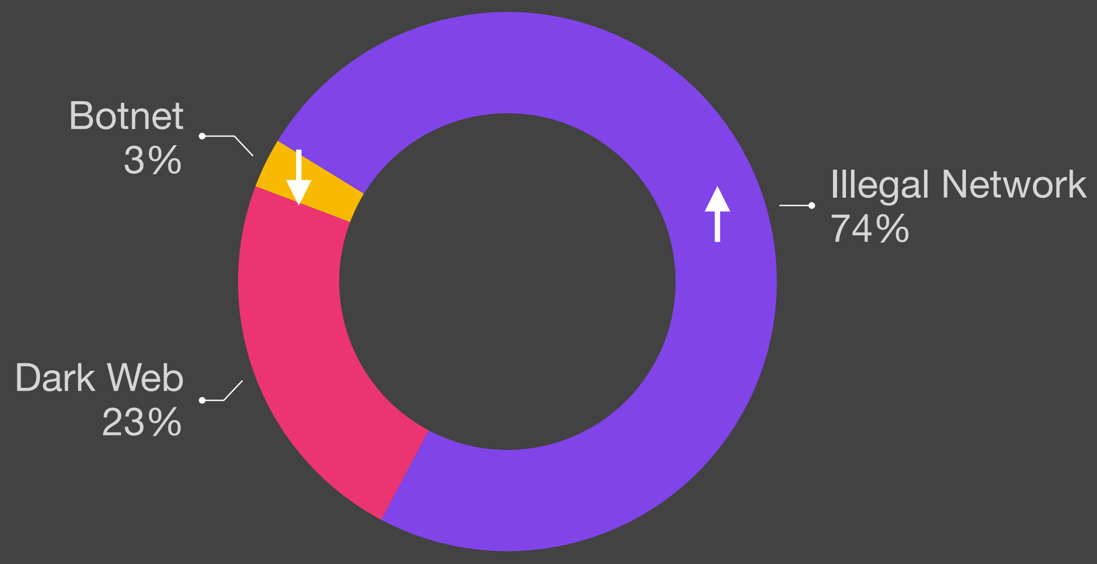
Ransomware Exfiltration Country



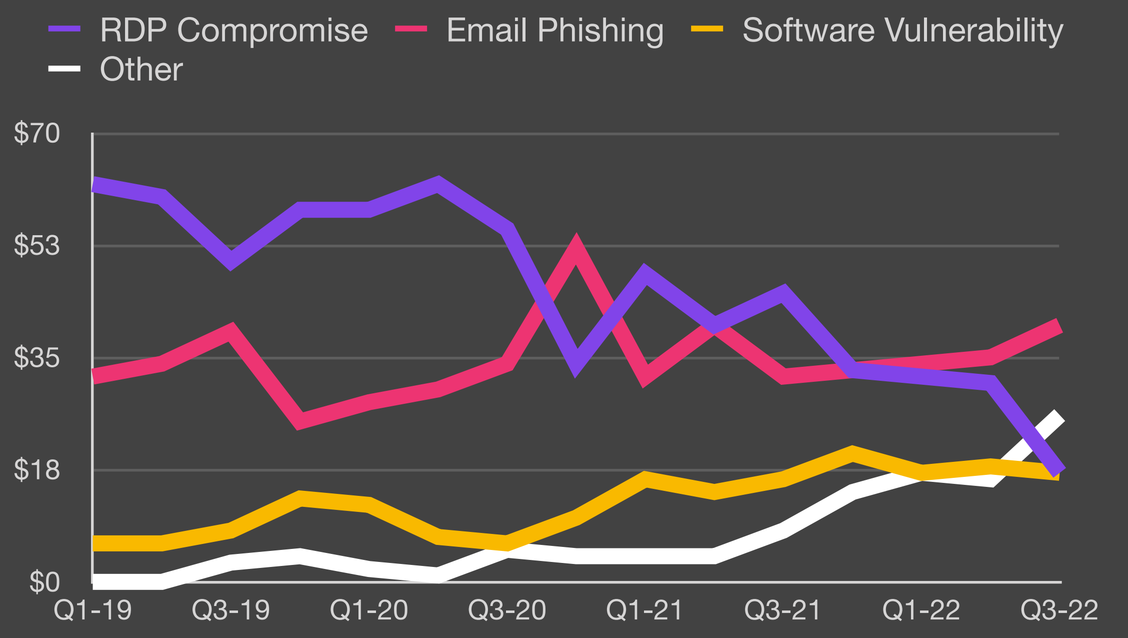
Size of Organization



Exfiltration Techniques



Attack Vectors[2]



[2] Courtesy Coveware

Roundup

As we say goodbye to 2022 ransomware continued its assault in December with 35 new attacks, the highest in 3 years, and the 4th highest from a record breaking year.

From an industry perspective Retail and Government saw the biggest increases of 15% and 13% respectively. The government together with education and healthcare were the top targets throughout year, easily outstripping the closest, technology by more than 30%. This reinforces the trend focusing on industries with the lowest levels of protection and skill shortages.

This month we also saw a large increase in attacks using Hive and BlackCat variants with 17% and 16% increases respectively. LockBit, which ended the year as the most effective variant of 2022 ended at 15.7% of all successful attacks.

Finally, we ended the year with 87% of all attacks leveraging PowerShell and 89% involving some form of data exfiltration, no surprise given the dramatic shift in attacks focusing almost entirely on data extortion.

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.