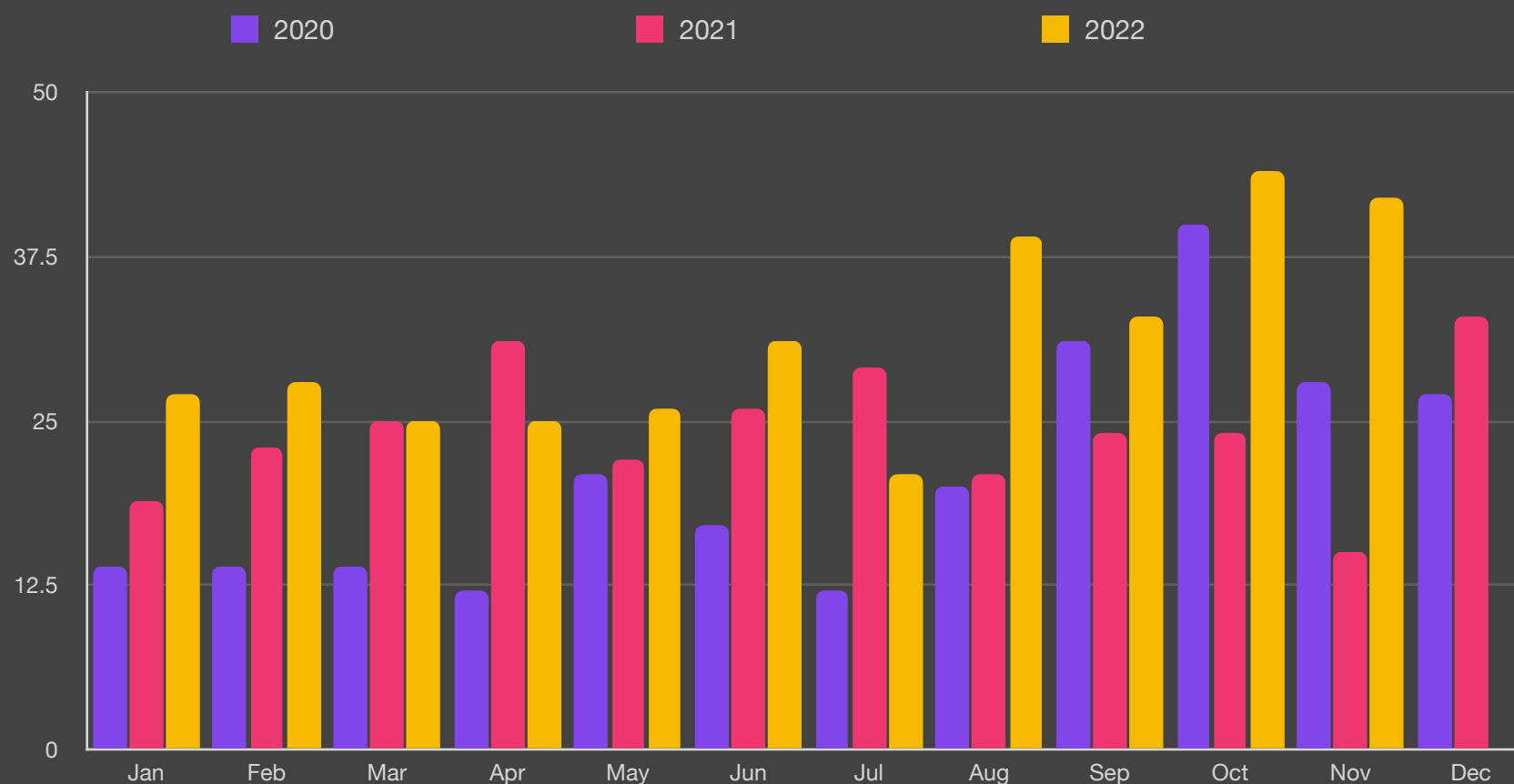


November 2022

November was the second busiest month of 2022 with 42 publicly disclosed attacks making the list. LockBit claimed attacks on defense giant Thales and German multinational company Continental. While the food industry in Canada took a hit when grocery chain Sobey's and major meat provider Maple Leaf Foods both reported attacks.



Ransomware Trend by Month



Key Trends



86% of all attacks use PowerShell



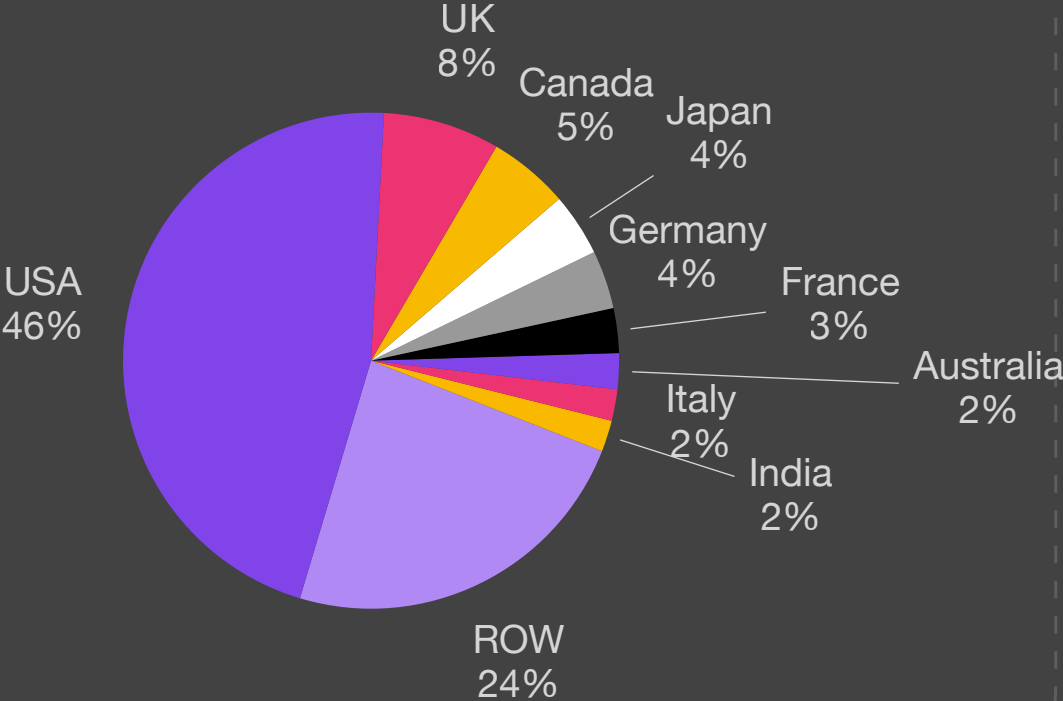
89% of attacks exfiltrate data



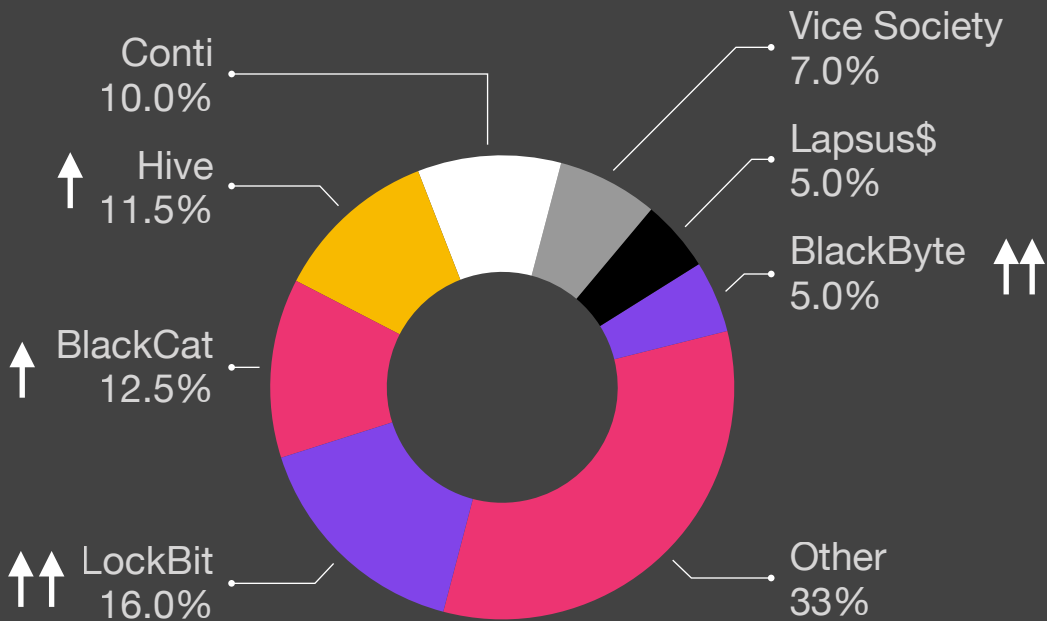
Average payout
US \$258,143k
+13.2% from Q2/22



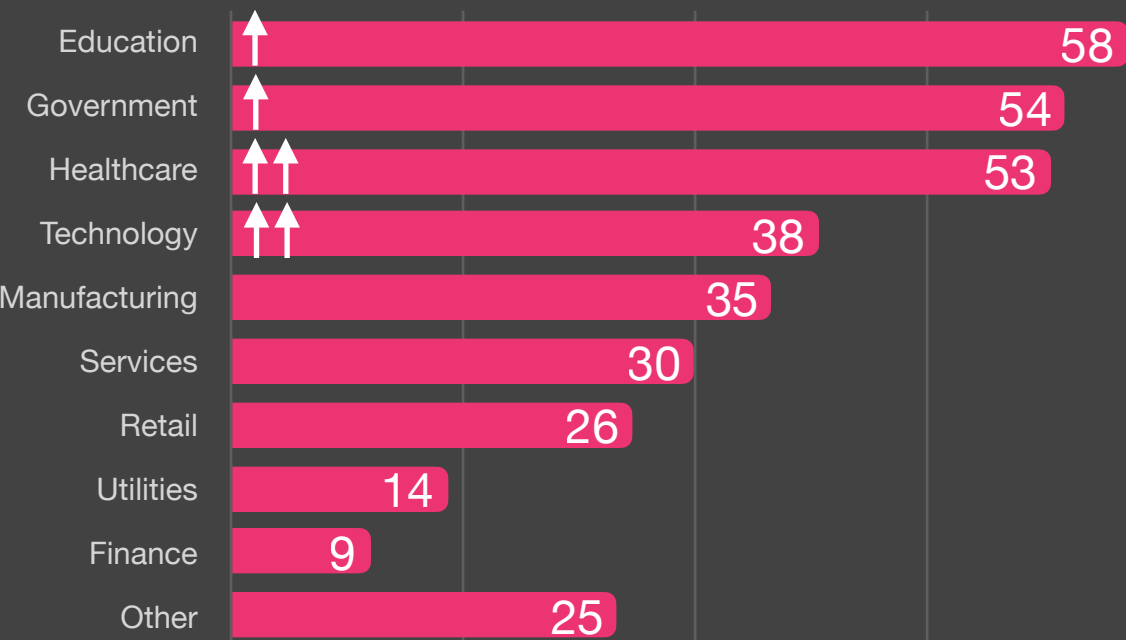
Ransomware by Country



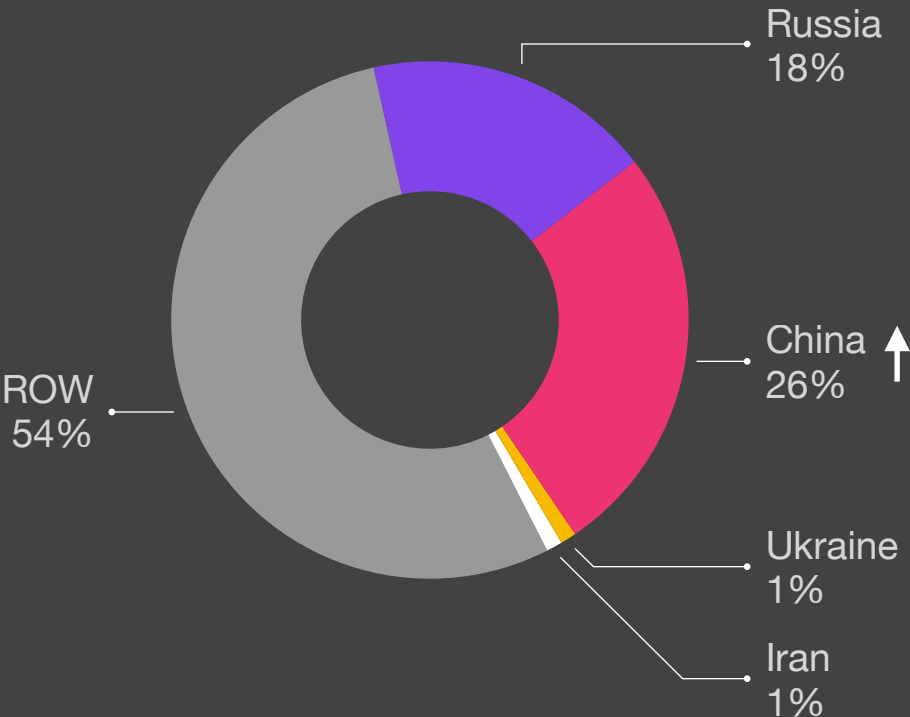
Ransomware by Variant



Ransomware by Industry

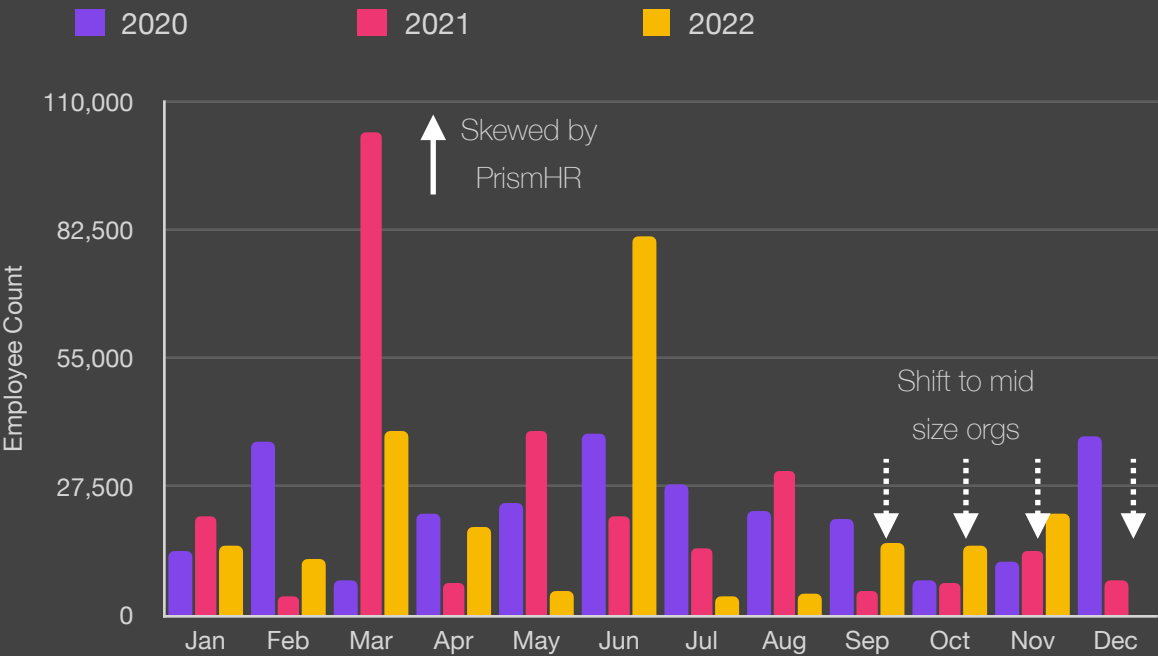


Ransomware Exfiltration Country

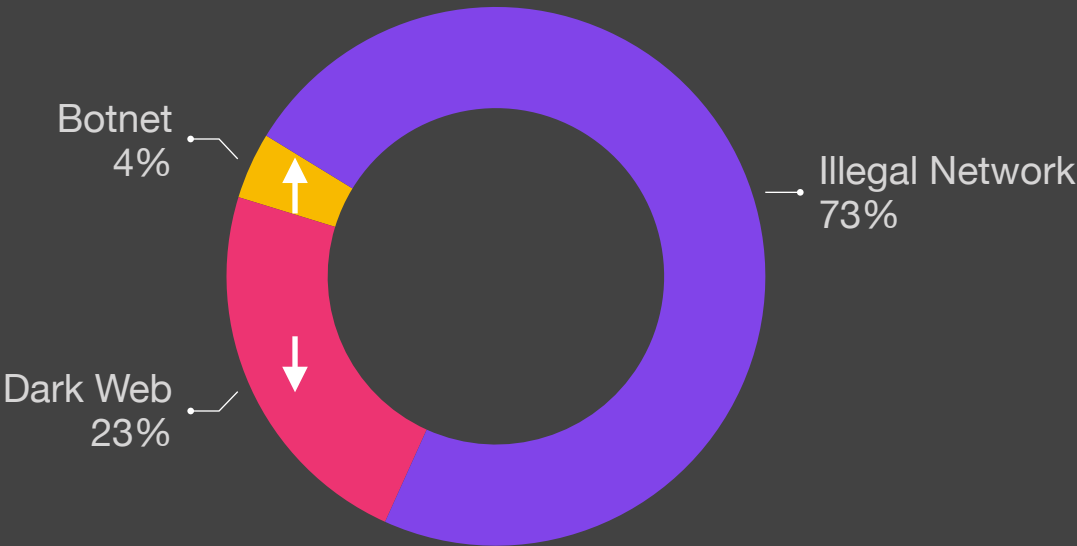




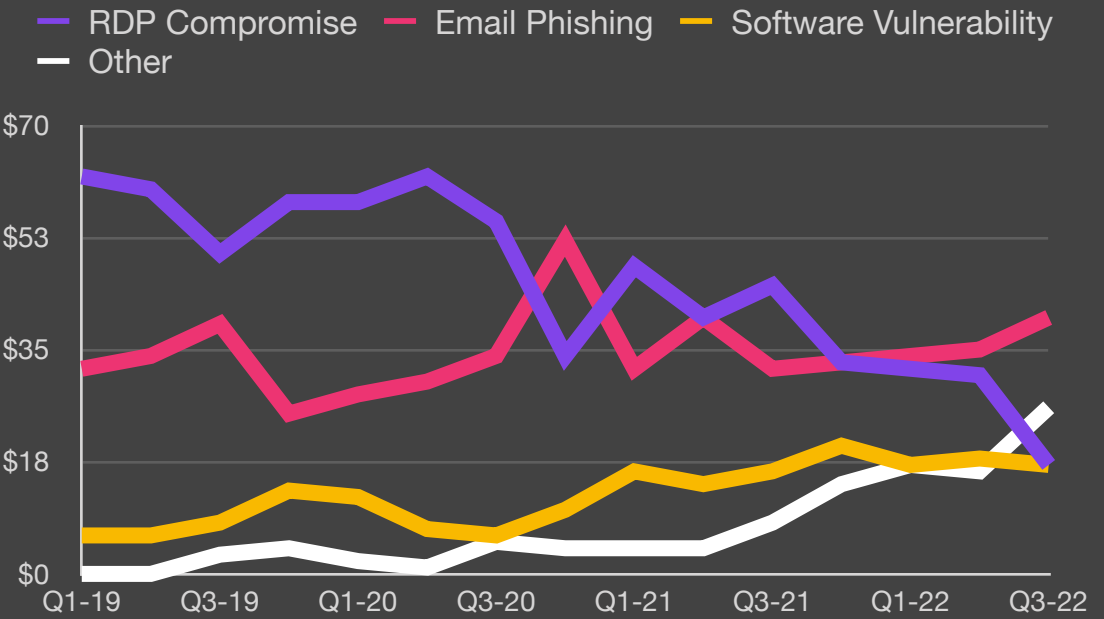
Size of Organization



Exfiltration Techniques



Attack Vectors²



²Courtesy Coveware

Roundup

Unusually, November saw the second highest number of ransomware attacks this year, a 180% increase year over year with a total of 42 attacks. There seems to be no end in sight, with recent insurance statistics demonstrating a general lack of preparedness. In fact, providers are now mandating more serious levels of protection before underwriting any new cybersecurity policy.

The biggest changes this month saw the persistent use of data exfiltration at 89% and a further increase in the use of PowerShell, now utilized in 86% of all attacks.

The greatest increases by industry involved Healthcare and Manufacturing with increases of 26% and 25% respectively. Smaller increases were observed in Education and Government, with 14% and 13% respectively, but continue to be the most targeted industries. Typically, these organizations struggle due to financial and skill shortages (please refer to BlackFog's latest research article).

LockBit easily took the lead this month in terms of variants with a 33% increase in successful attacks followed by BlackByte and BlackCat with increases of 25% and 14% respectively.



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.