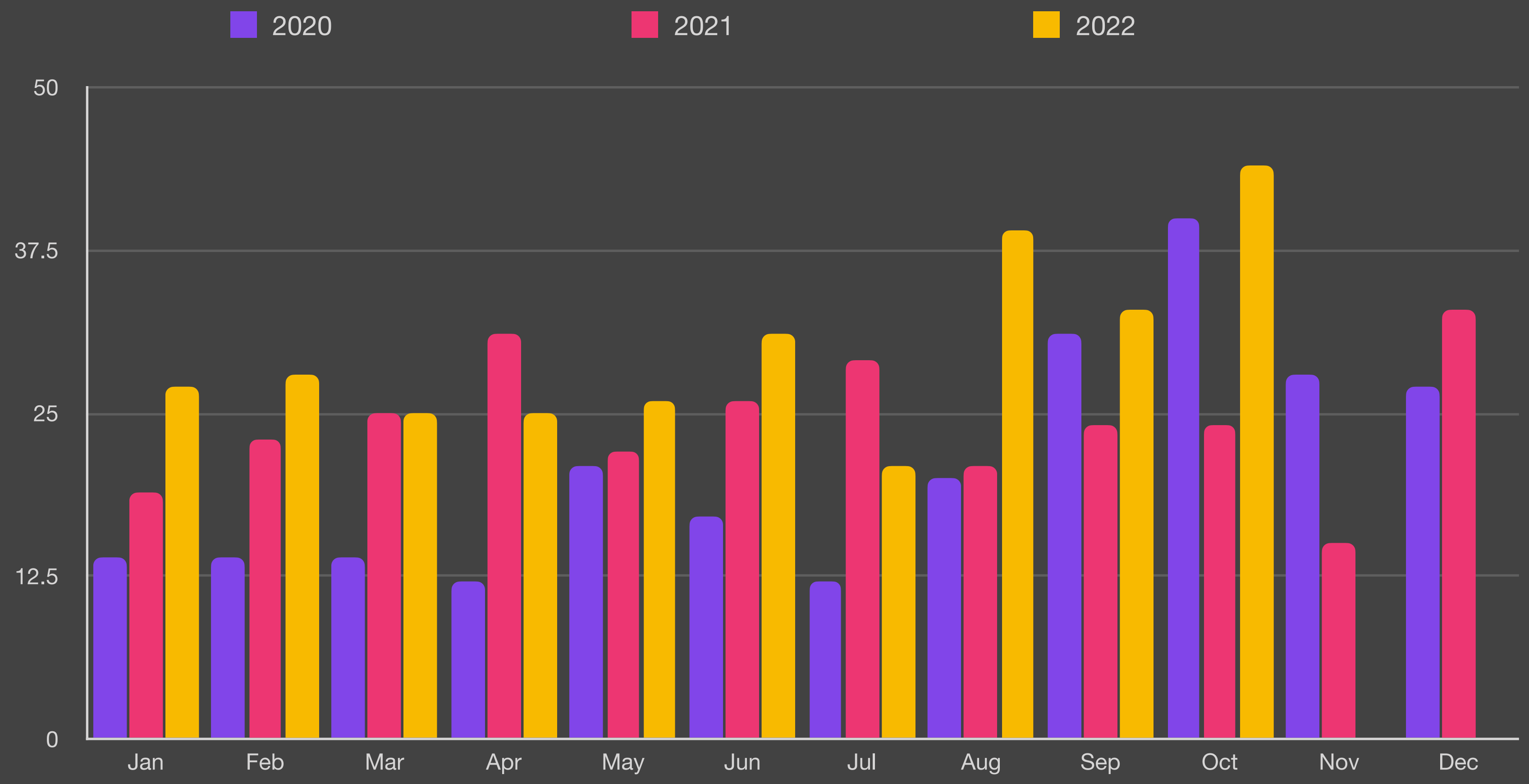
October 2022

A massive 44 incidents made ransomware news in October, setting a new record since we started collecting our data almost 3 years ago. The previous record was back in October 2020 when we uncovered 40 ransomware attacks in the news. Ferrari made headlines when RansomEXX posted some internal documents following an attack that the company strongly denies. A record breaking ransom of $60 million was demanded from UK car dealer Pendragon by the LockBit gang, while the month finished with an attack on hit ForceNet, the Australian defense communications platform used by military personnel and defense staff.

Ransomware Trend by Month



Key Trends

85% of all attacks use PowerShell

89% of attacks exfiltrate data

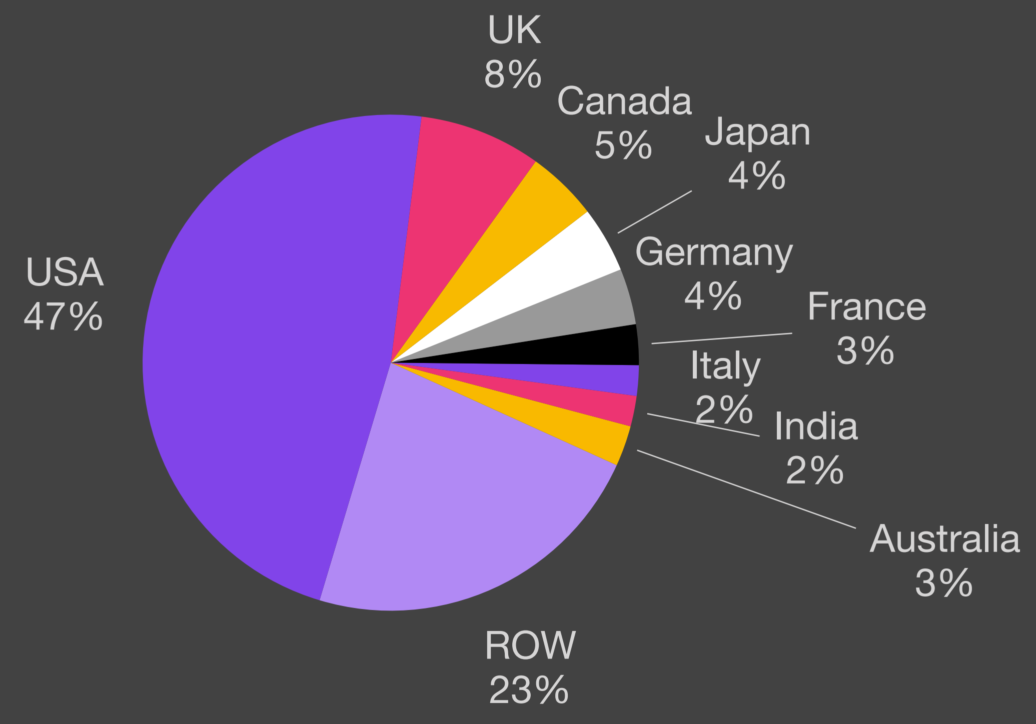
Average payout US $258,143k

+13.2% from Q2/22

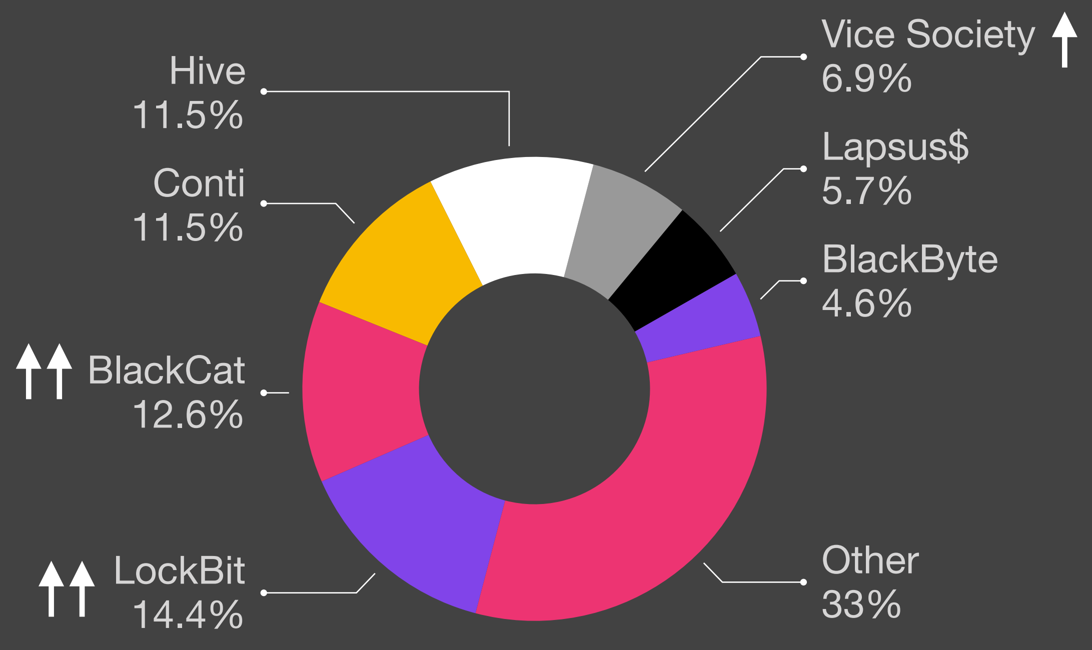
BlackFog Global Ransomware Report

October 2022

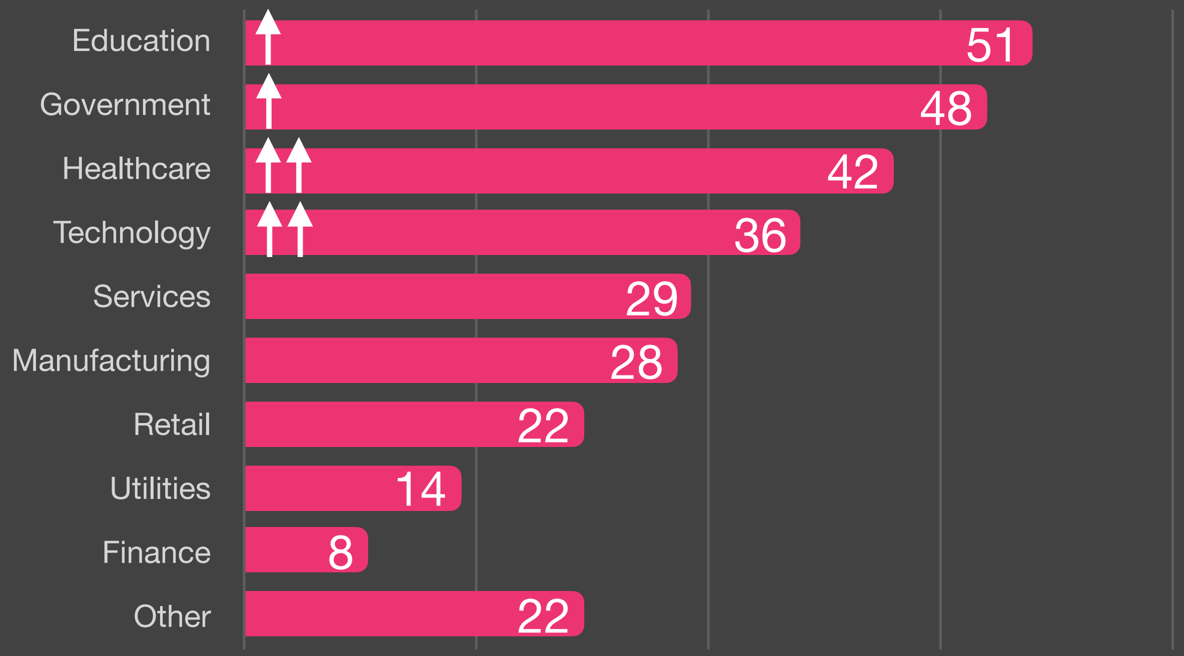
Ransomware by Country



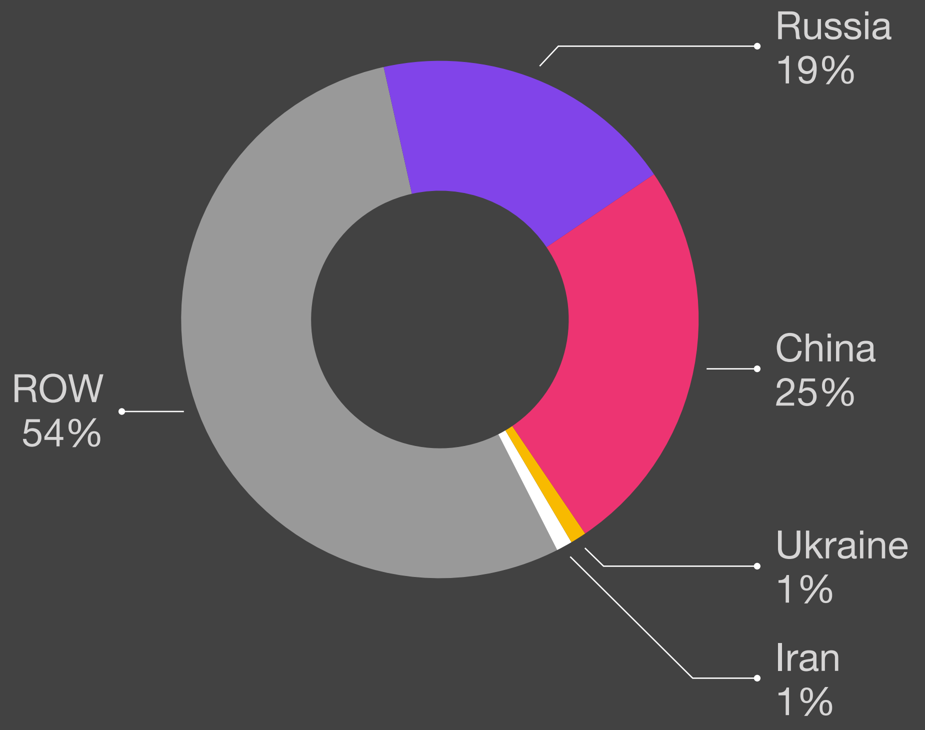
Ransomware by Variant



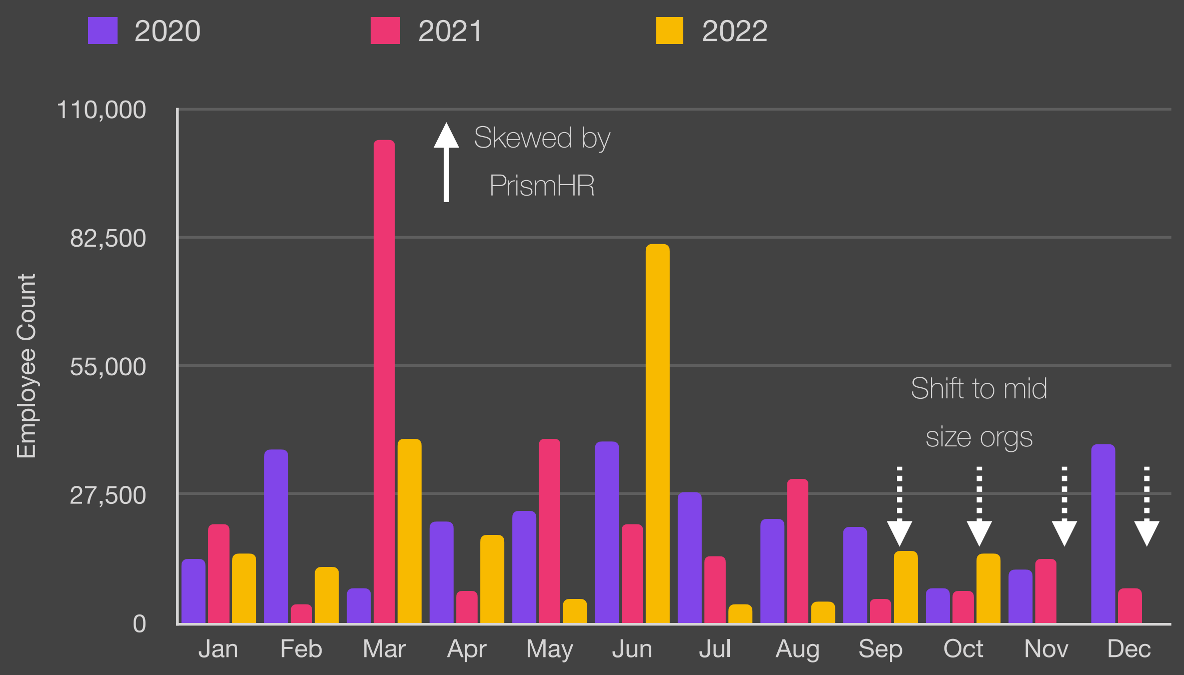
Ransomware by Industry



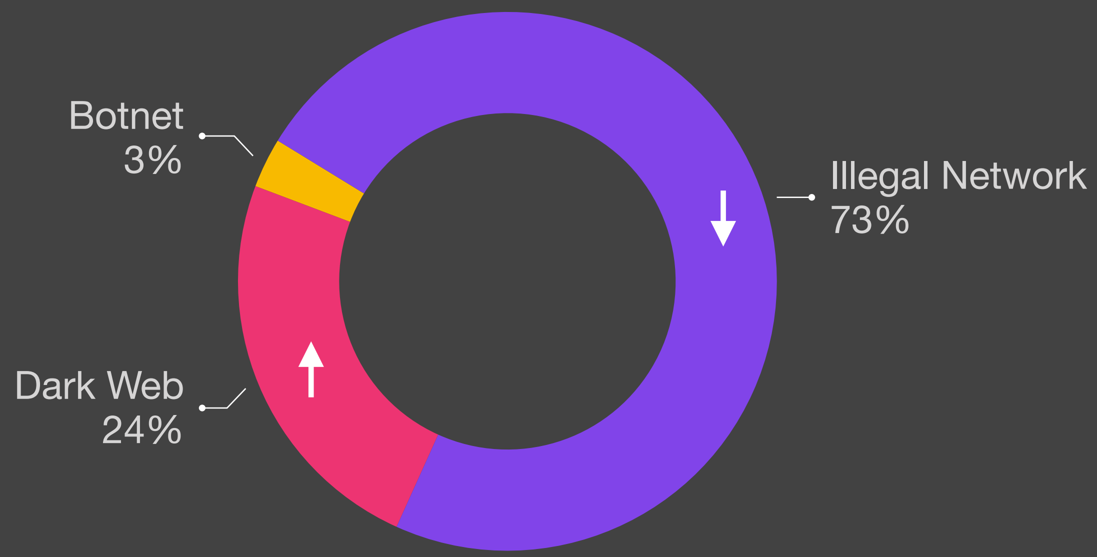
Ransomware Exfiltration Country



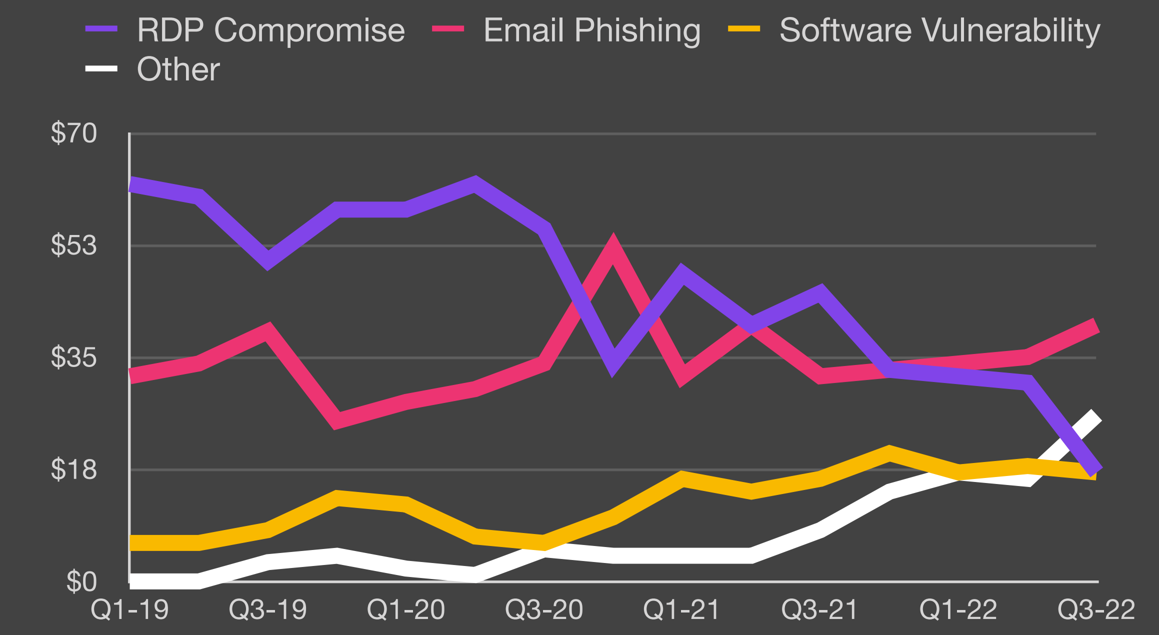
Size of Organization



Exfiltration Techniques



Attack Vectors[2]



[2]Courtesy Coveware

Roundup

October saw the highest number of confirmed ransomware attacks in the 3 years that BlackFog has been collecting data with a total of 44 publicized attacks. This highlights the limitations of existing traditional cybersecurity solutions and the general lack of preparedness by most organizations.

This month saw the largest increase in attacks on the Technology sector with an increase of over 29%. As in previous months we have also seen large increases in attacks on sectors with the lowest levels of protection in place, namely Healthcare, Education and Government with increases of 20%, 16% and 12% respectively.

The most dramatic changes in ransomware variants this month were BlackCat with an increase of 47% and Lockbit with an increase of 39%. This reflects the effectiveness of these variants and specifically the data destruction capabilities of BlackCat that we became aware of in September.

While we continue to see PowerShell increase utilization to 85% we note this month that data exfiltration is now involved in 89% of all successful attacks.

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.