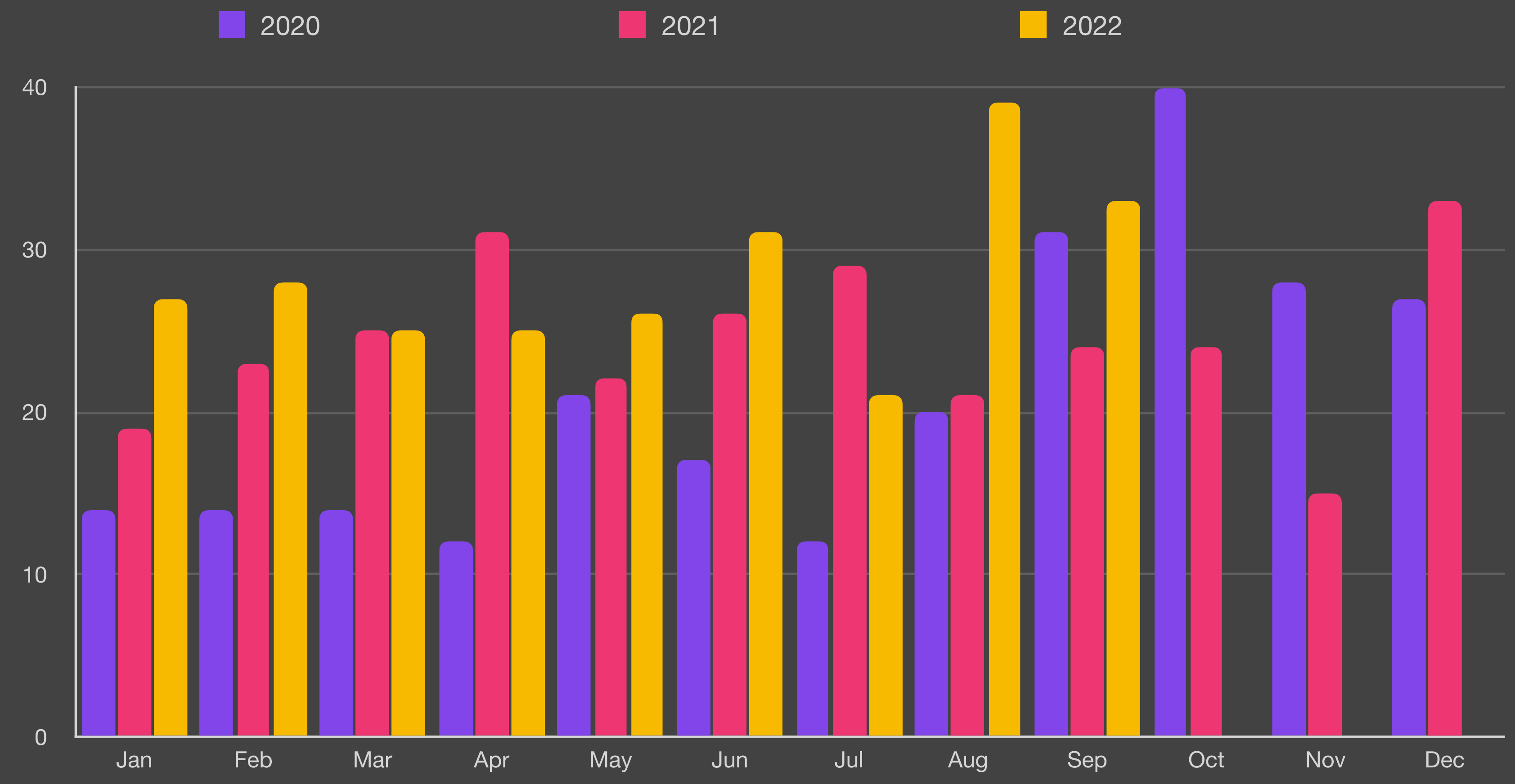
September 2022

In September we tracked 33 ransomware incidents, with government being the hardest hit vertical, followed closely by healthcare. LAUSD, the second largest school district in the US made news when an attack caused significant disruption, while a hacker managed to launch an attack on Uber using social engineering. Luxury UK farm shop Daylesford Organic hit the headlines when data belonging to high profile customers including the Duchess of York was compromised.

Ransomware Trend by Month



Key Trends

83% of all attacks use PowerShell

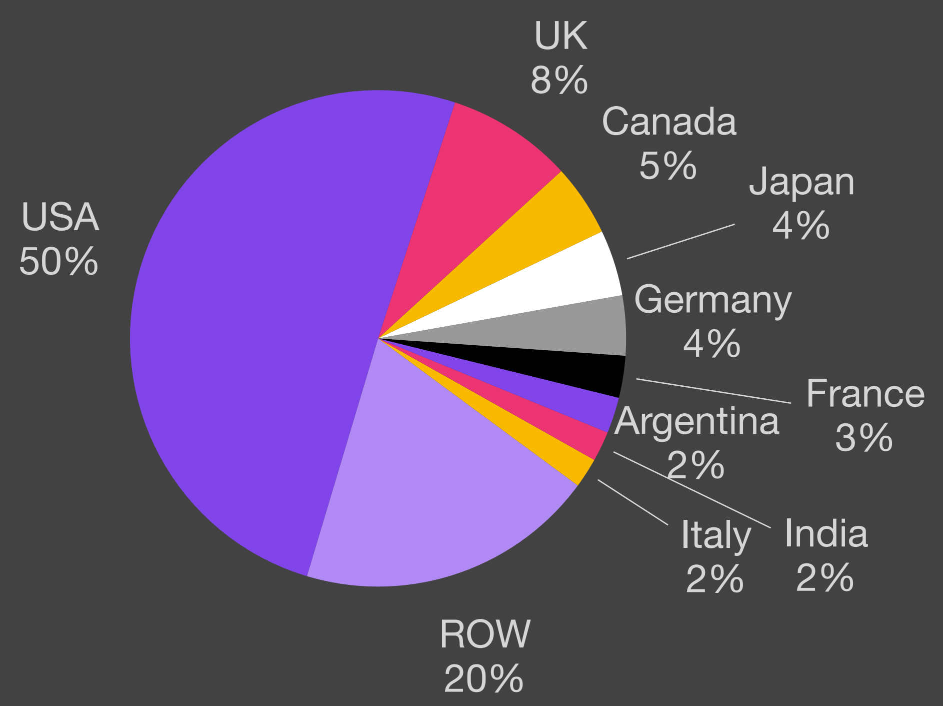
88% of attacks exfiltrate data

Average payout US $228,125k
+8% from Q1/22

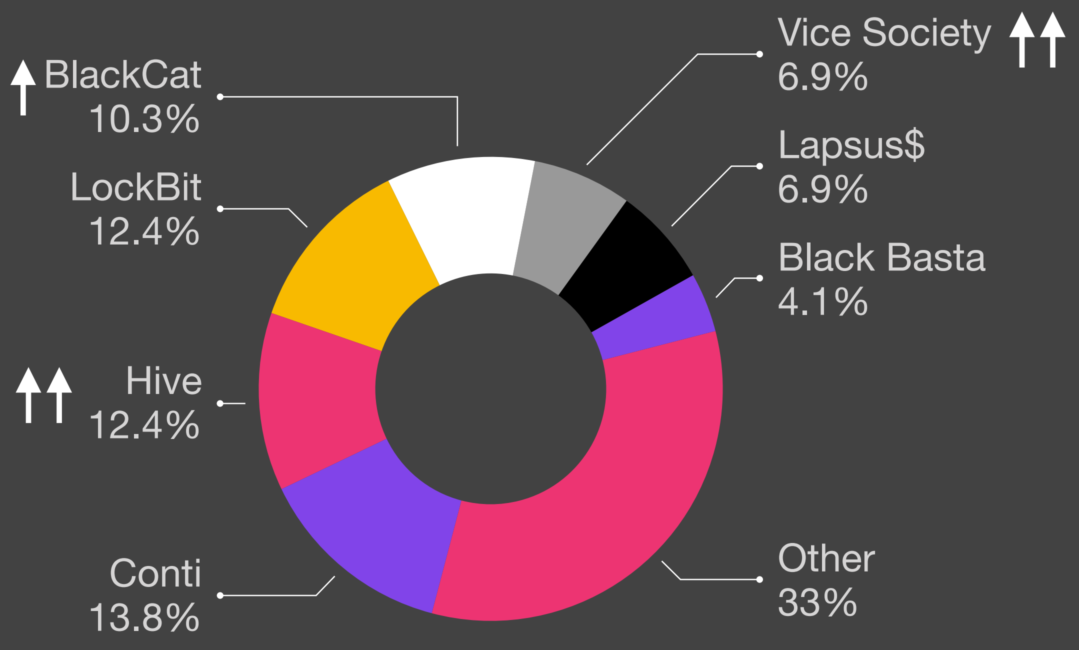
BlackFog Global Ransomware Report

September 2022

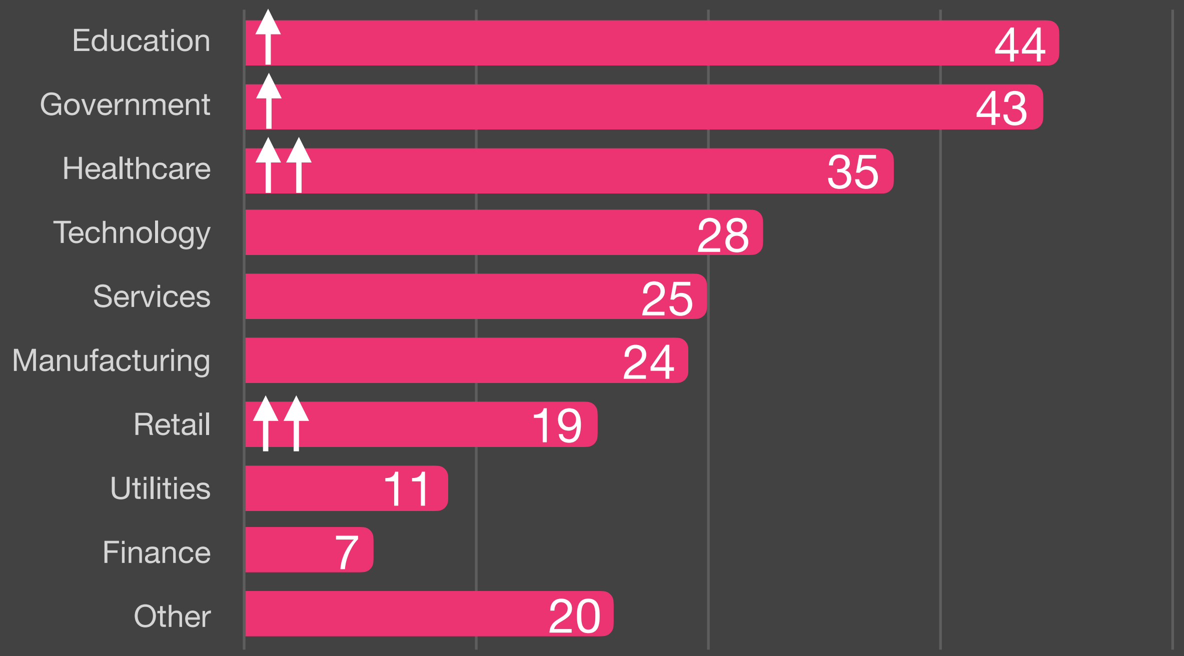
Ransomware by Country



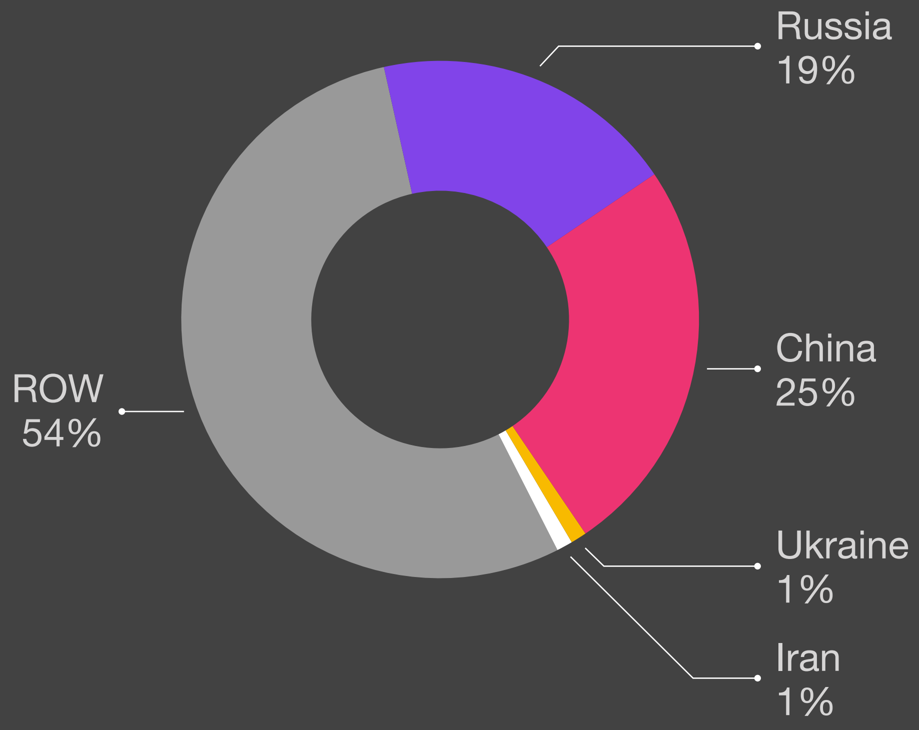
Ransomware by Variant



Ransomware by Industry



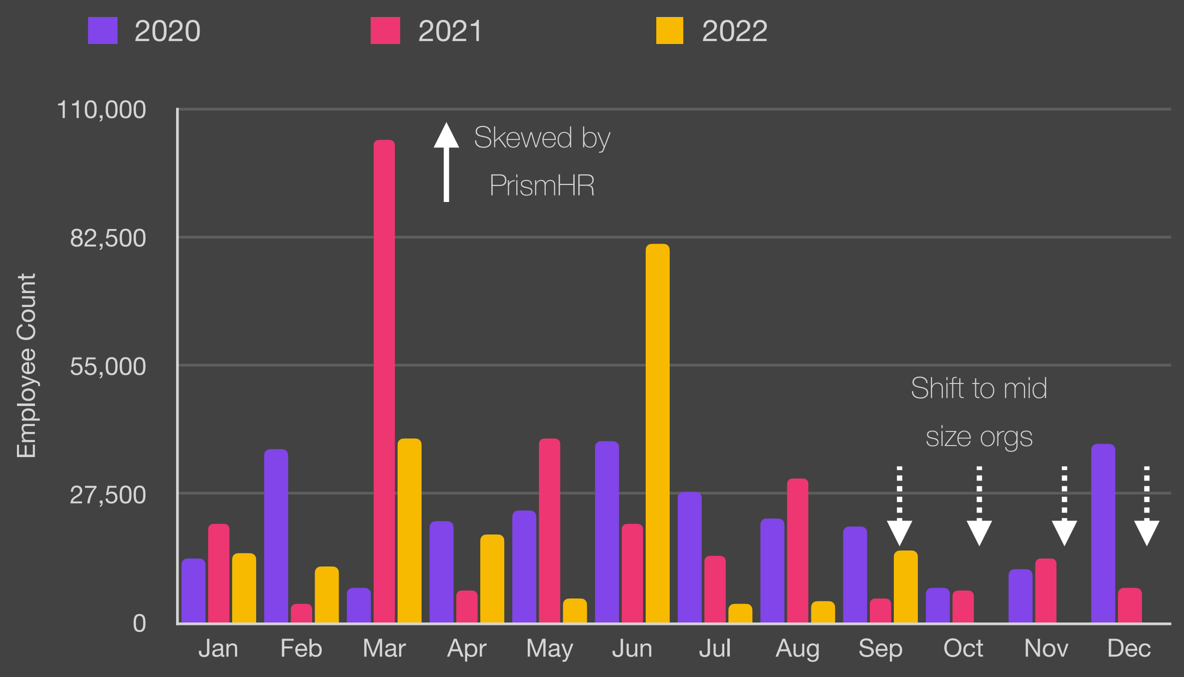
Ransomware Exfiltration Country



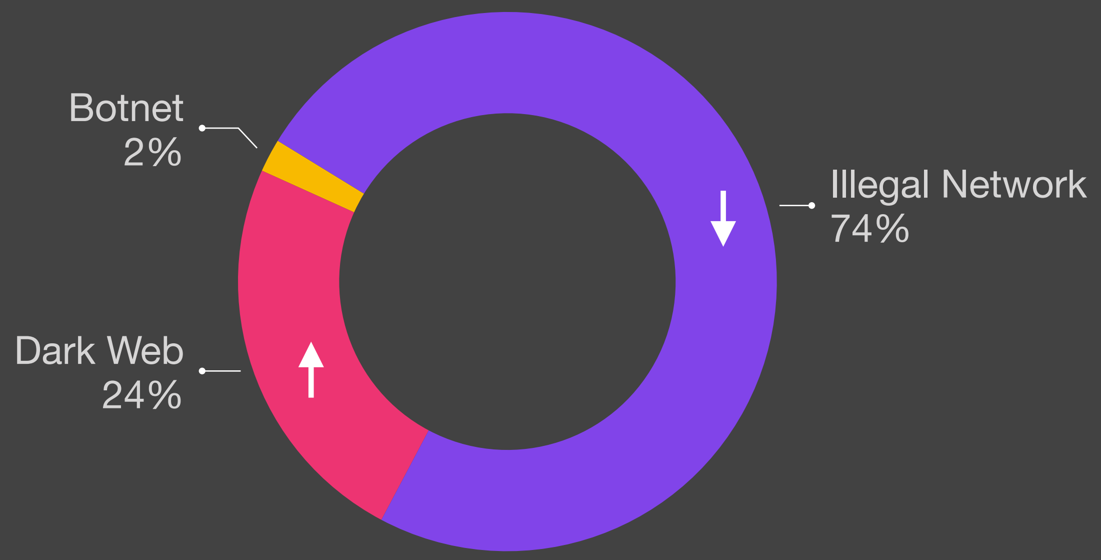
BlackFog Global Ransomware Report

September 2022

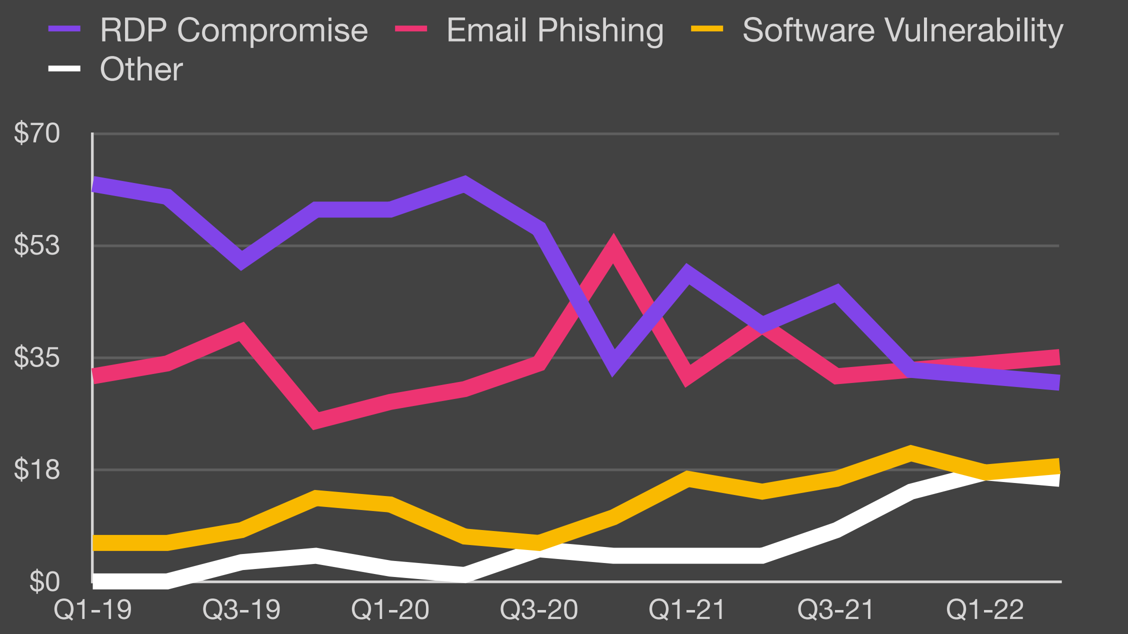
Size of Organization



Exfiltration Techniques



Attack Vectors[2]



[2]Courtesy Coveware

Roundup

September represents the second highest month of the year with 33 reported ransomware attacks. Ransomware shows no signs of abating with this month representing the third highest number of attacks over the past 3 years.

This month we have seen major increases in several ransomware variants. Hive attacks increased by over 50%, Vice Society by 43% and BlackCat 25%. These increases come at the same time that several variants have started experimenting with data destruction, most notably BlackCat.

As in previous months we continue to see a focus on the least protected sectors of Healthcare, Education and Government with increases of 25%, 13% and 19% respectively. This month however we saw the largest increase in the Retail sector of 27%, as cyber criminals explore new targets with low investments in cybersecurity.

PowerShell continues to to be highly leveraged as an attack vector and is now used in 83% of all 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.