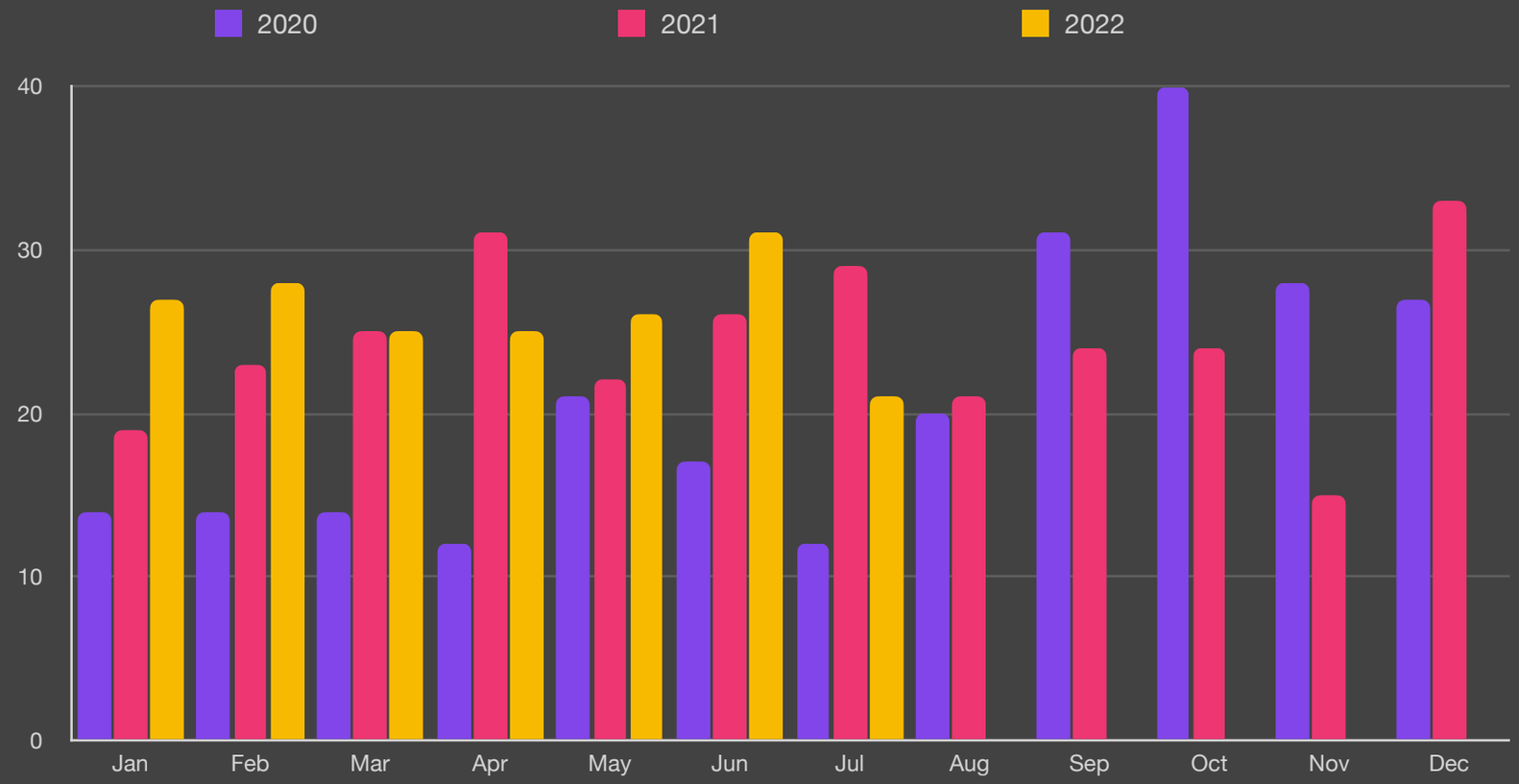
July 2022

In July we spotted 21 ransomware attacks in the press including one on an Australian prison when bad actors managed to take control of the computer systems. The LockBit gang was busy this month claiming attacks on Italy's tax agency, a small Canadian town, a town in Colorado and French telecoms firm, La Poste Mobile.

Ransomware Trend by Month



Key Trends

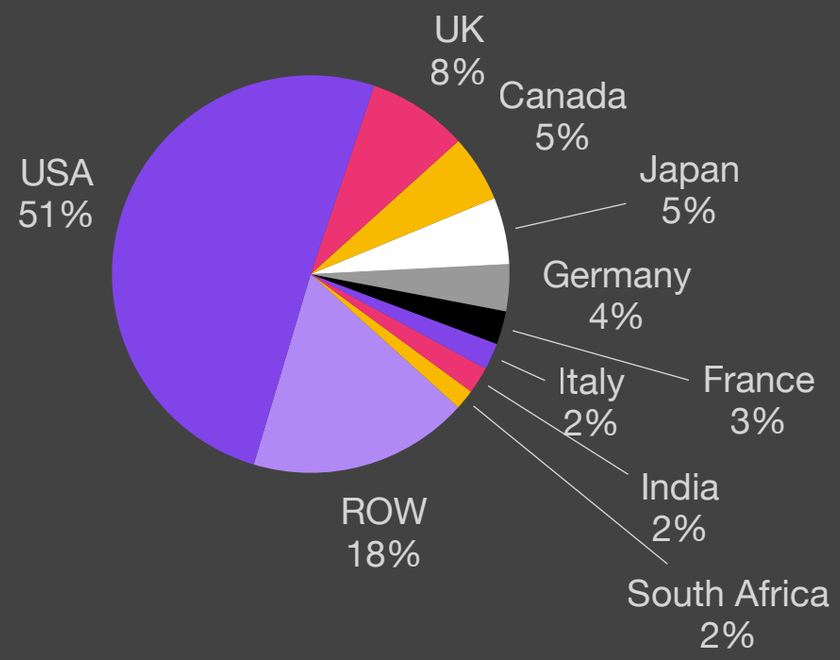
77% of all attacks use PowerShell

88% of attacks exfiltrate data

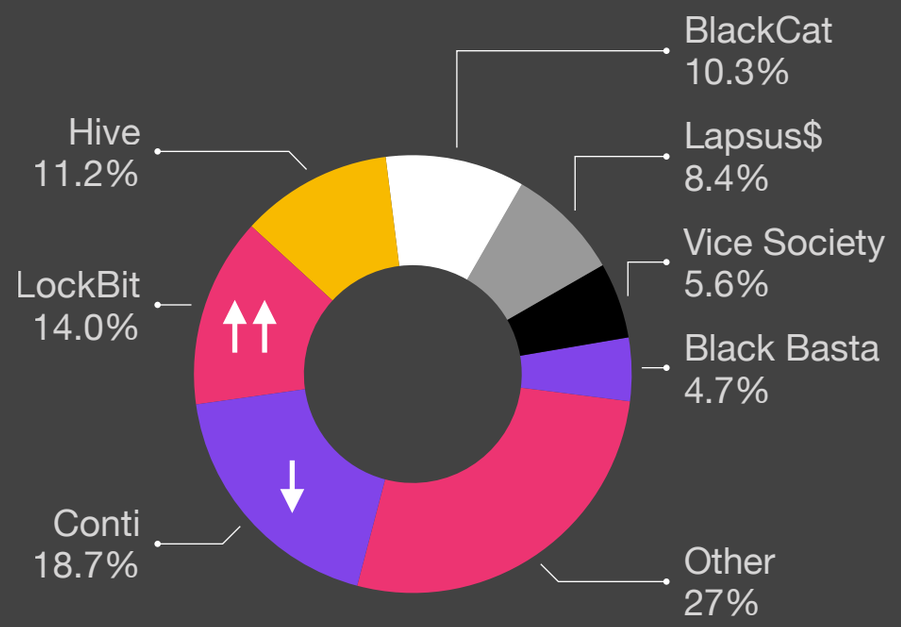
Average payout US $228,125k

+8% from Q1/22

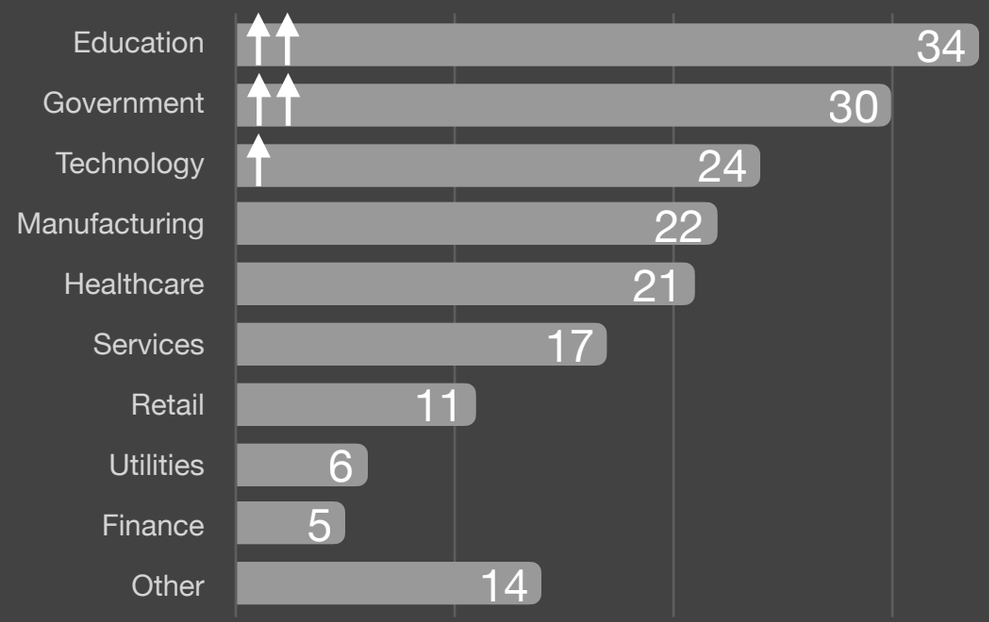
Ransomware by Country



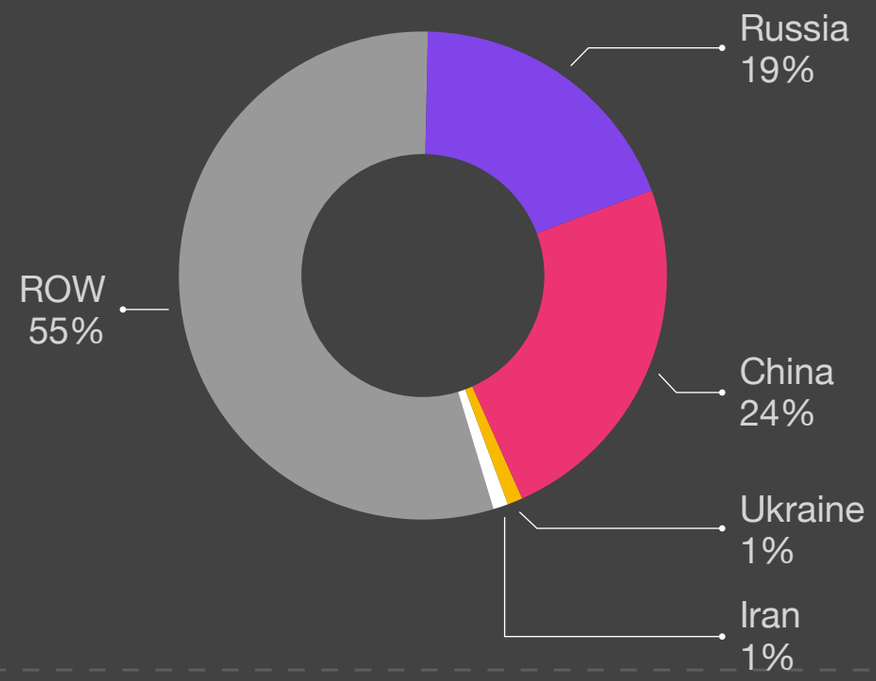
Ransomware by Variant



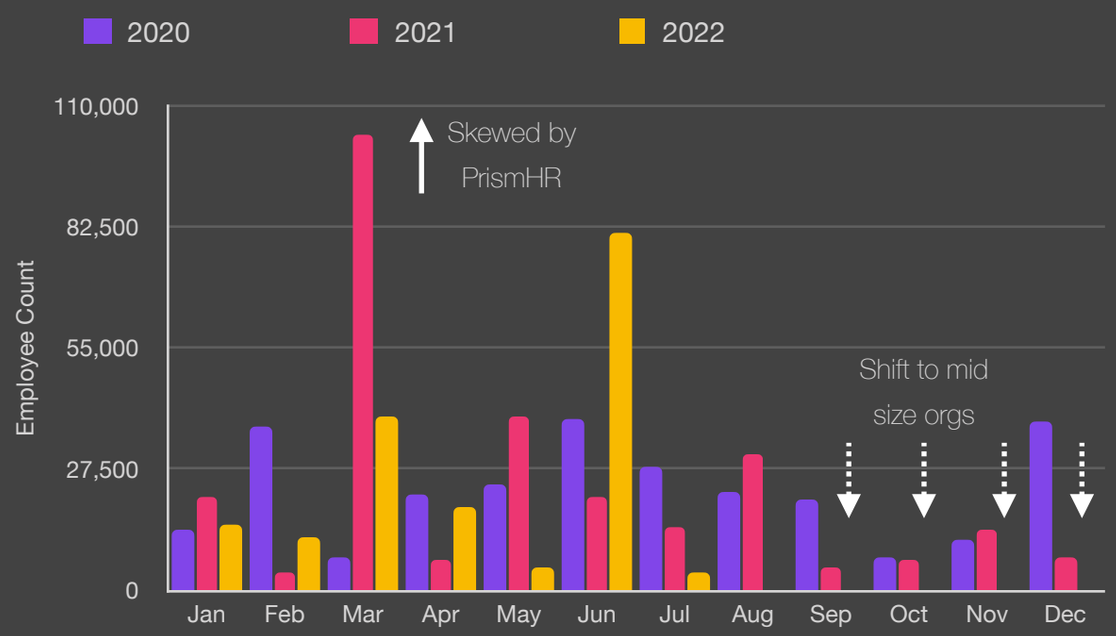
Ransomware by Industry



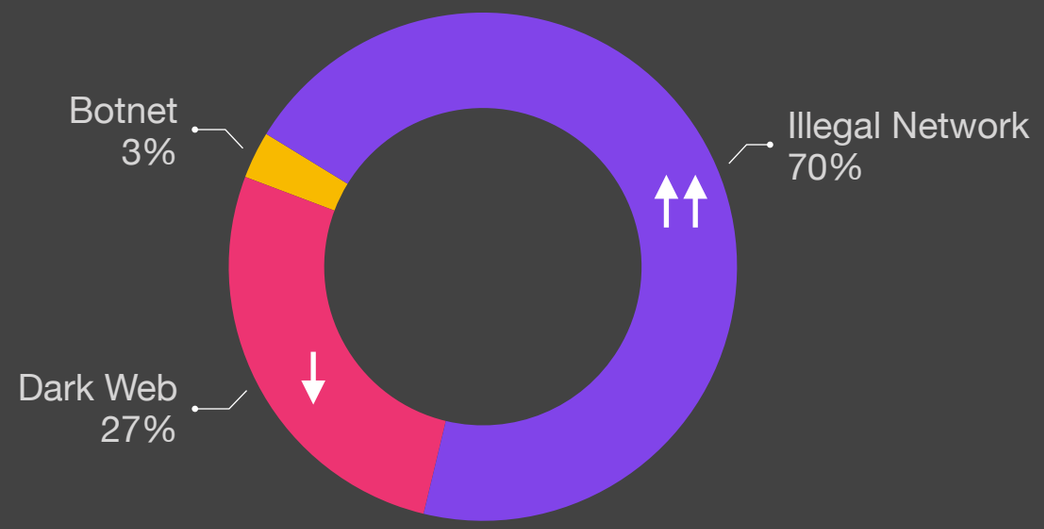
Ransomware Exfiltration Country



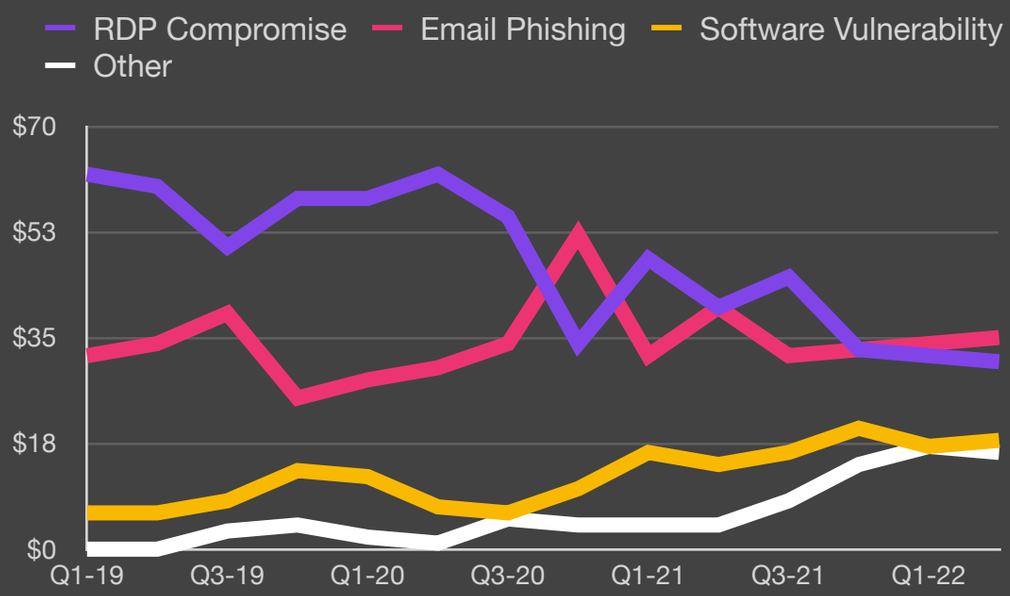
Size of Organization



Exfiltration Techniques



Attack Vectors[2]



[2]Courtesy Coveware

Roundup

Significantly this month, while we have seen a decrease in public notifications of attacks we have seen an increase in actual non public attacks suggesting that there are many incidents that remain unreported so far. We continue to track these numbers moving forward.

Lockbit continues to be the dominant player right now and jumped from 11.6% to 14% in only a month.

While education and government continue to be highly targeted with 21% and 20% increases respectively, we also saw attacks on the technology sector increase by 14% and for the first time this year overtake the manufacturing sector. Attackers are still focused on sectors with the weakest protection and lowest investments in cybersecurity and aging infrastructure.

Lastly we saw a continued increase in the total number of attacks that exfiltrated data, now at 88% of all attacks, as more cybergangs focus on extortion than encryption.

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.