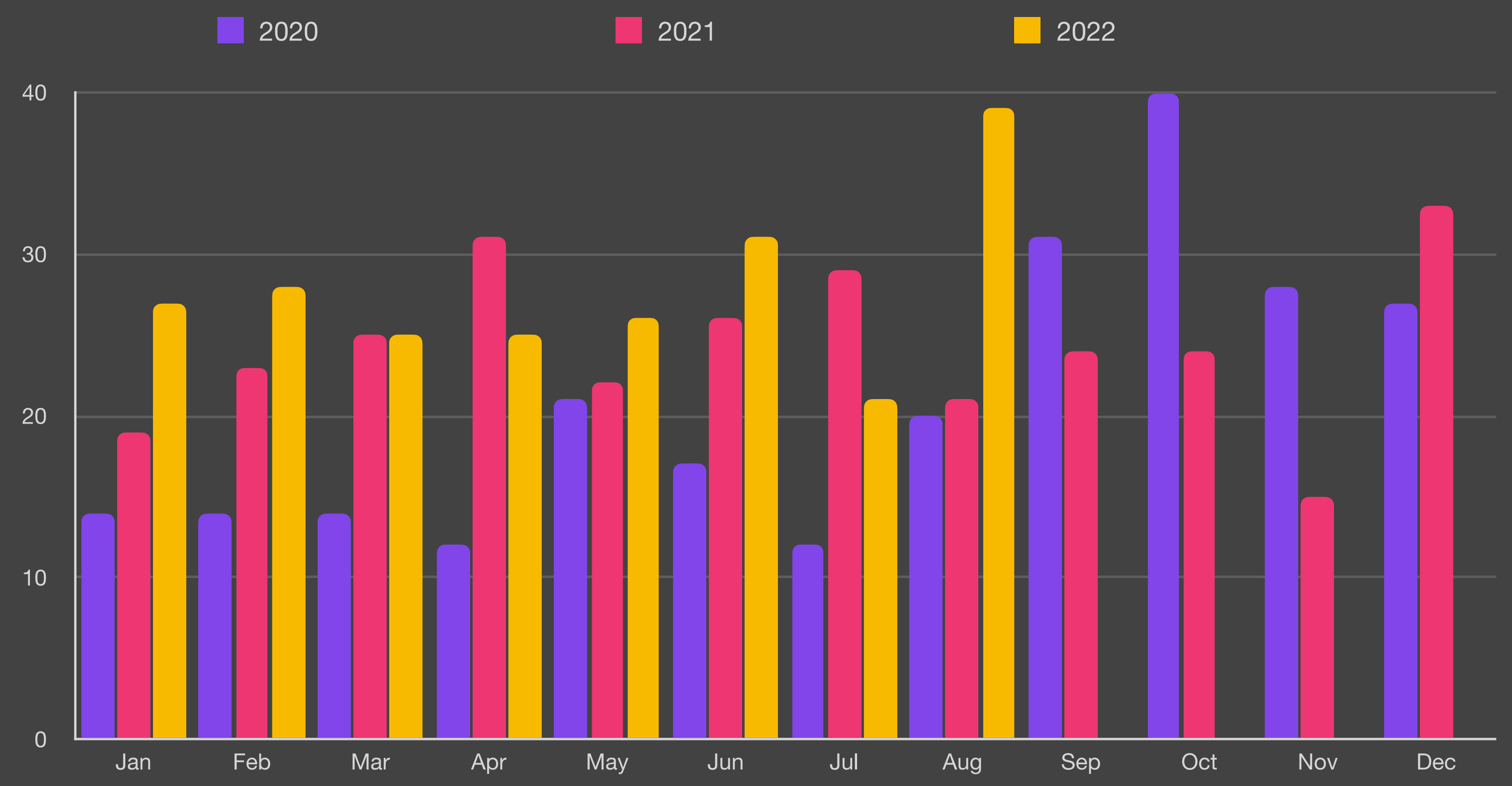
August 2022

In August we recorded 39 ransomware attacks, the second highest month we've ever recorded. Healthcare organizations were hit hard this month with 10 different incidents recorded, including an attack on the UK's NHS as well as an attack on a French hospital which resulted in a massive $10,000,000 ransom demand. Education, government and utilities also seemed to be high on the target list for cybercriminals. South Staffordshire Water's ransomware incident gained a lot of news coverage when Clop misidentified their organization for another larger water supplier. Yanluowang Group (part of Lapsus$) made headlines when it infiltrated Cisco's corporate network, publishing 3,100 files of data on the dark web.

Ransomware Trend by Month



Key Trends

80% of all attacks use PowerShell

87% of attacks exfiltrate data

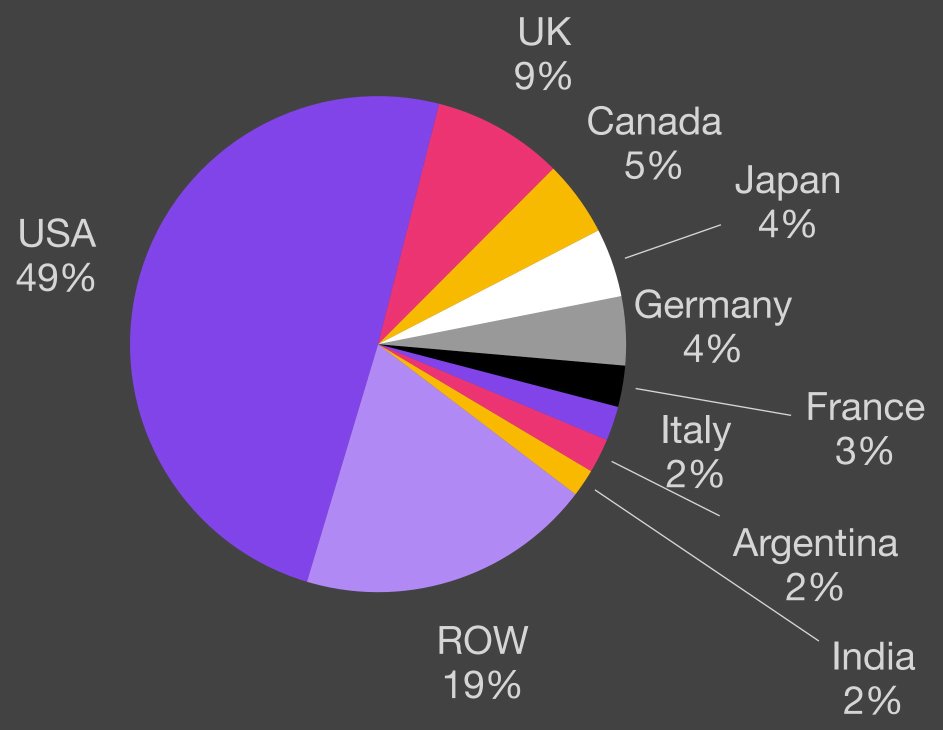
Average payout US $228,125k

+8% from Q1/22

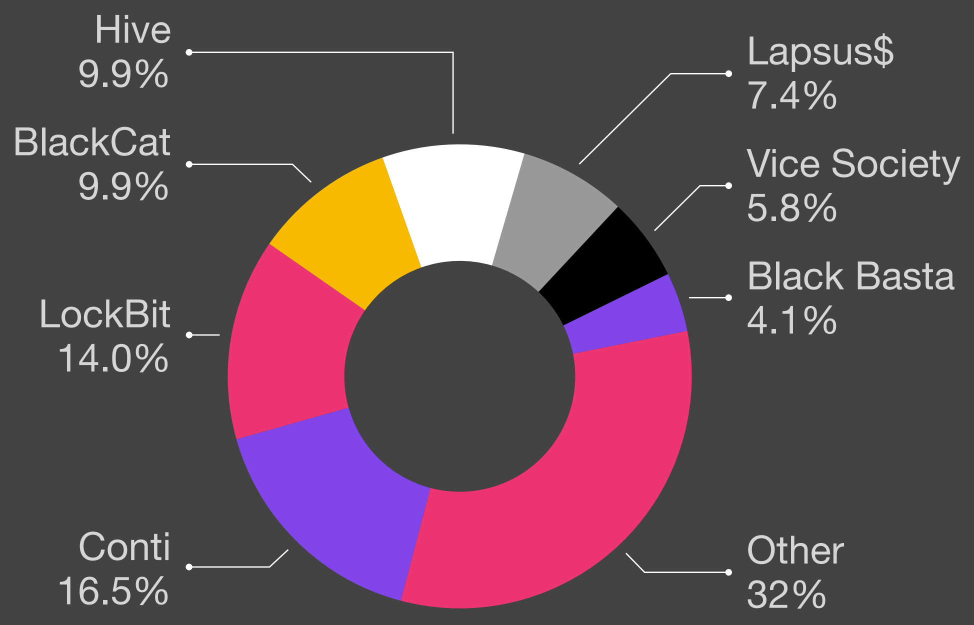
BlackFog Global Ransomware Report

August 2022

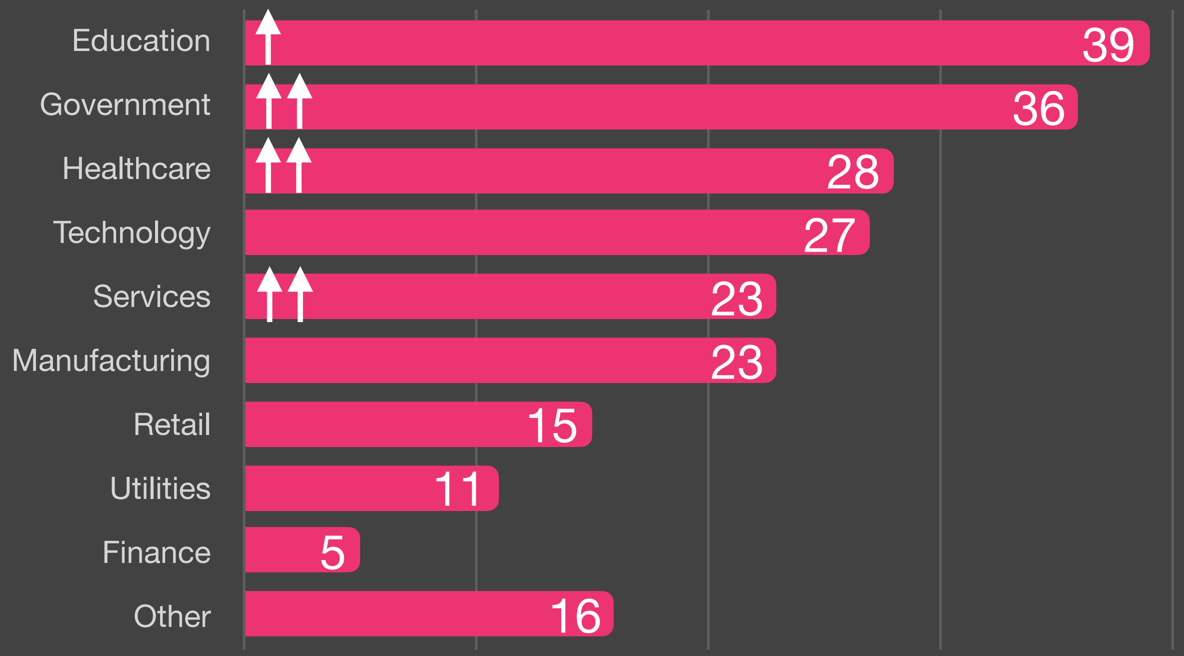
Ransomware by Country



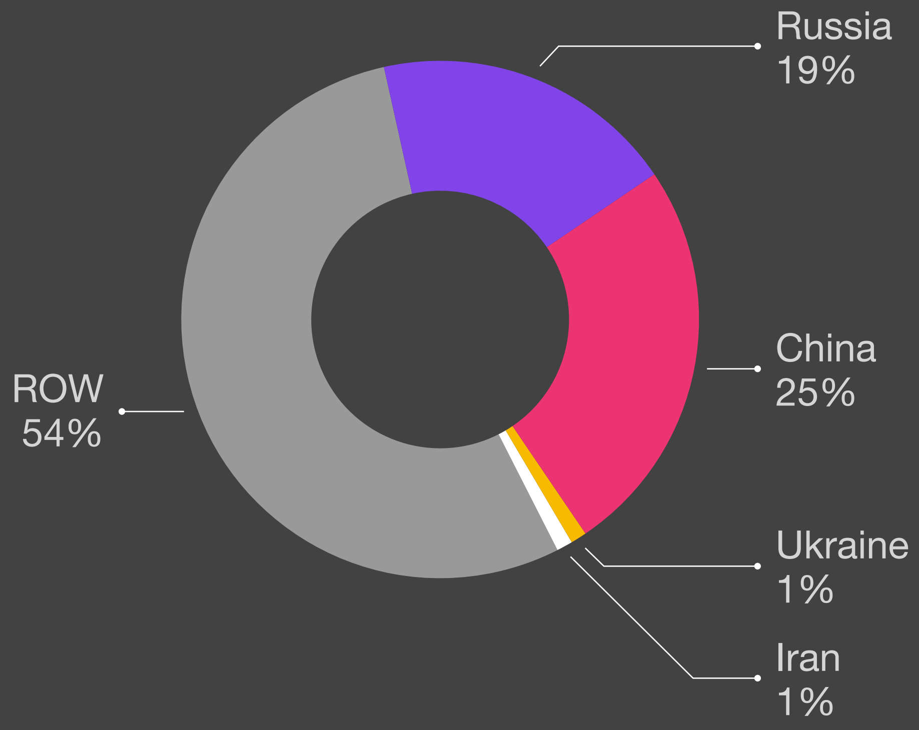
Ransomware by Variant



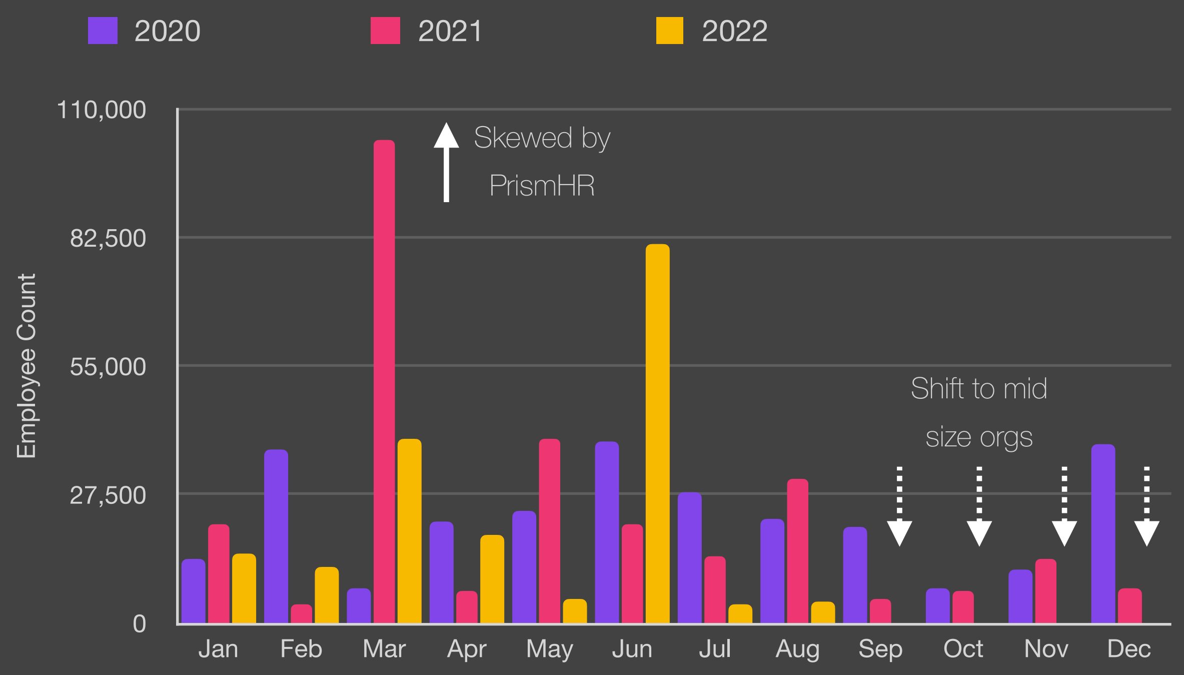
Ransomware by Industry



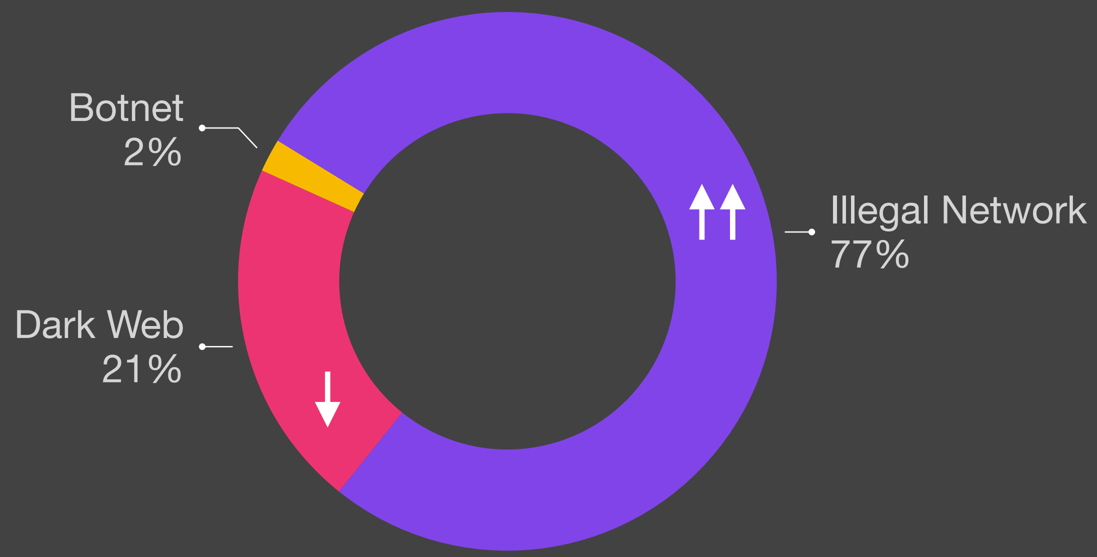
Ransomware Exfiltration Country



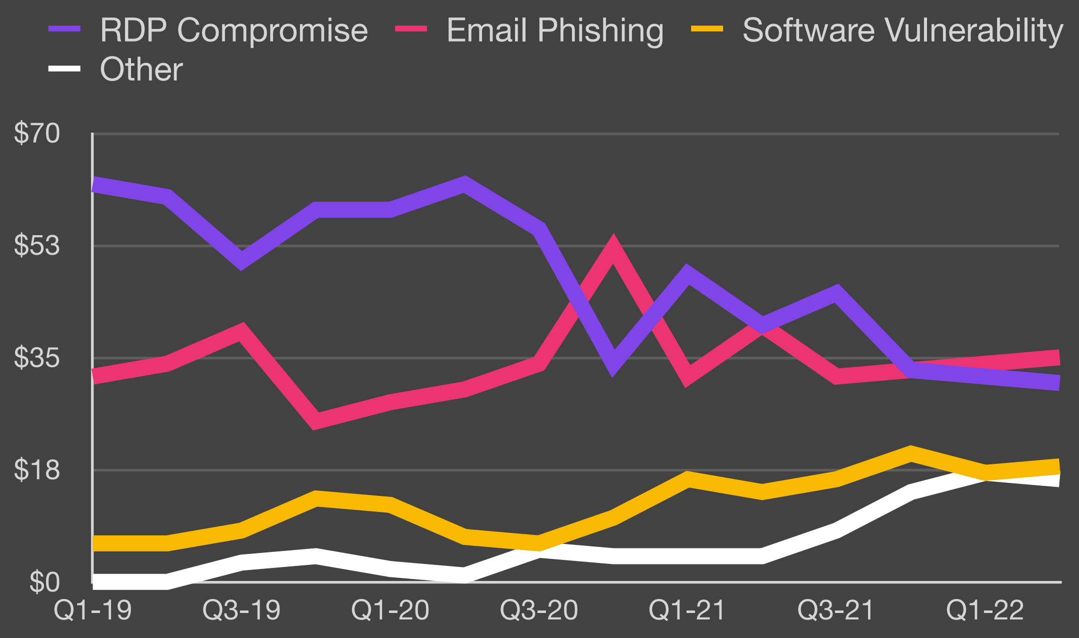
Size of Organization



Exfiltration Techniques



Attack Vectors[2]



[2]Courtesy Coveware

Roundup

August represents the second biggest month of ransomware attacks since we began recording ransomware attacks back in 2020.

We continue to see increased attack rates in sectors with low levels of protection and aging infrastructure such Education and Government, with increases of 15% and 20% respectively. This month we also saw dramatic increases in Healthcare and Services sectors of 33% and 35% respectively as attackers look to broaden their targets.

Lockbit continued its dominance along with Conti at 14% and 16.5% respectively. The top 4 variants now contribute to 50% of all new attacks.

Lastly, this month we also saw that attacks leveraging the PowerShell for the first time hit 80%, a new record.

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.