September 2023

With seventy publicly disclosed attacks, September set a new record since starting our State of Ransomware blog back in January 2020. Healthcare and government were the highest targeted sectors, with twelve attacks each, closely followed by education with eleven. A large number of ransomware groups launched attacks this month, with BlackCat leading the charge claiming fifteen attacks, we also notes a number of new variants emerging. BlackCat's attacks on **Caesars Entertainment** and **MGM Resorts** dominated the headlines for most of this month, alongside incidents with other big organizations such as **SONY**, **Johnson Controls** and **PhilHealth**.

Roundup

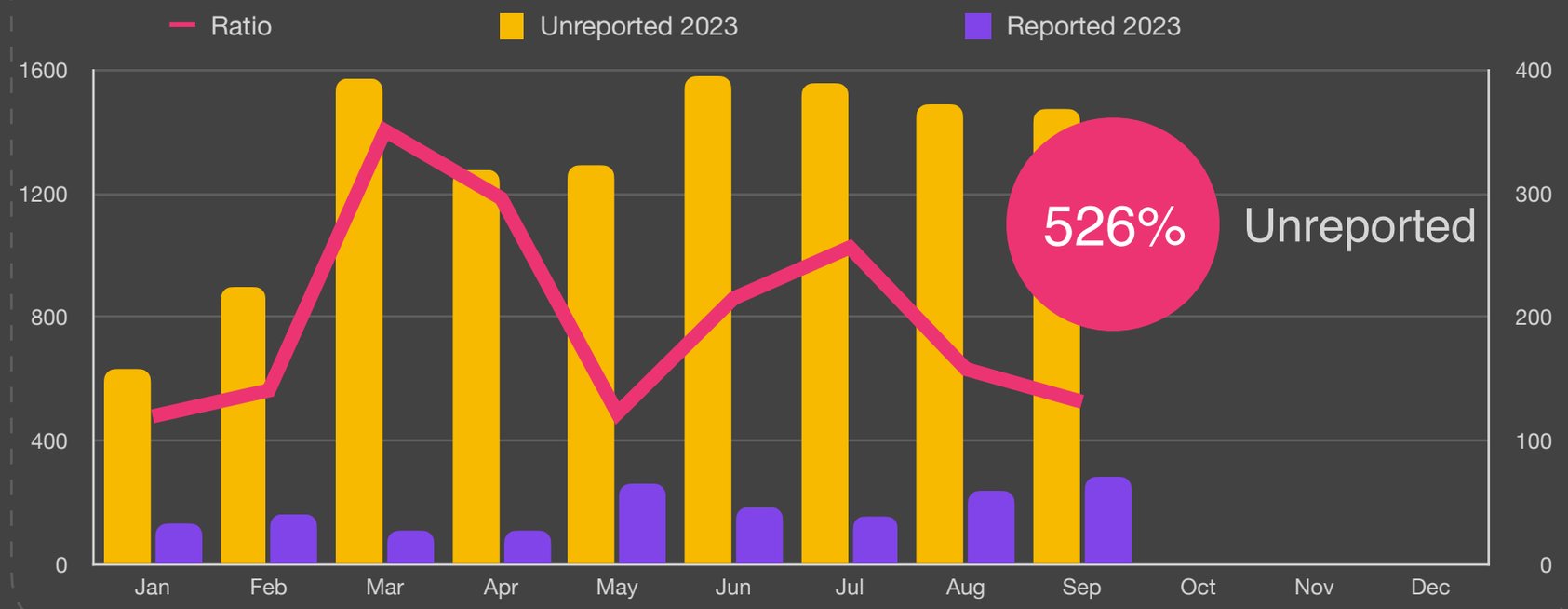
Historically, the last few months of the year witness higher attack rates. This year, we have seen even more dramatic increases, with September boasting over double the attack rate compared to the same time last year. In fact, with more than 3 months to go in the year we have already exceeded last years tally by 20%, with 407 attacks versus 341 for the entire 2022 year.

The undisclosed attack rates remain relatively unchanged this month with a 526% ratio of unreported to reported attacks.

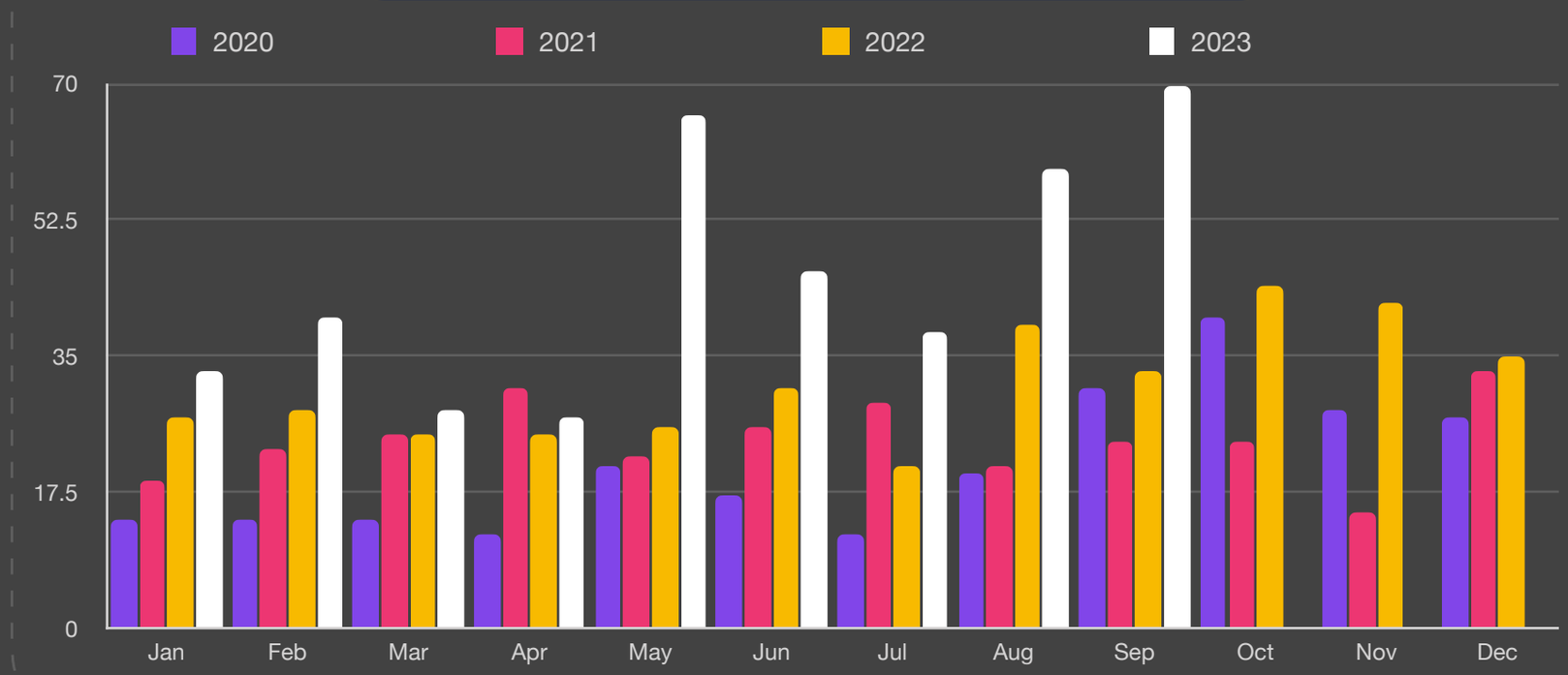
This month saw some other notable changes, specifically in the sectors of Manufacturing, Technology and Government with 33%, 24% and 23% increases respectively. While, Healthcare and Education continue to lead the way, both with increases of 14% over the previous month.

September also saw BlackCat increase its lead as the primary attack vector with 19.3% of all victims, followed by LockBit at 17.5%. LockBit dominated the number of unreported attacks at 35.2%, followed by BlackCat at 14.1%. As in previous months, data exfiltration continues to dominate as the primary mechanism for extortion at 90% with traffic flowing to China at 32% and Russia 9% of the time.

Unreported Ransom Attacks



Reported Ransomware by Month



Key Trends

526% Unreported

1st Highest in 4 years

1st Highest Ransom Payouts

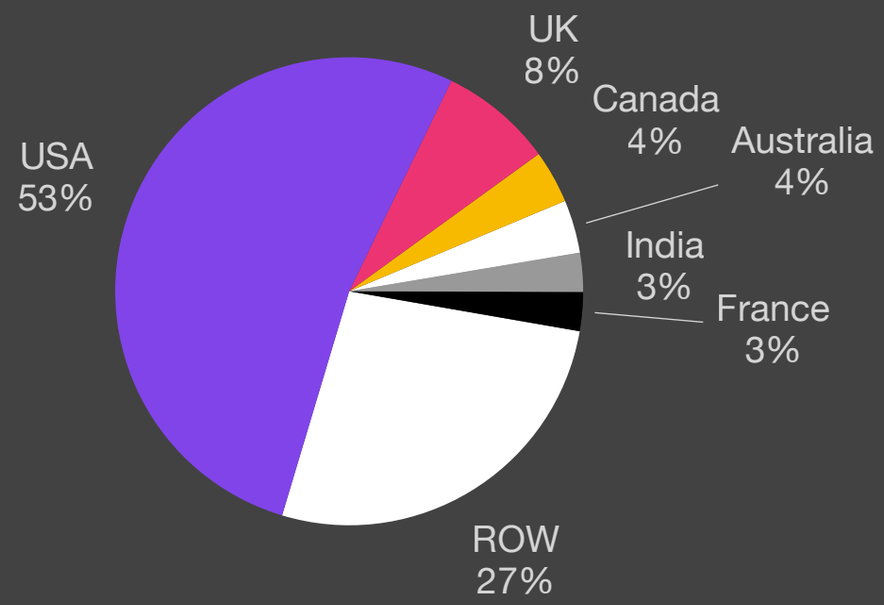
50% of all attacks use PowerShell

90% of attacks exfiltrate data

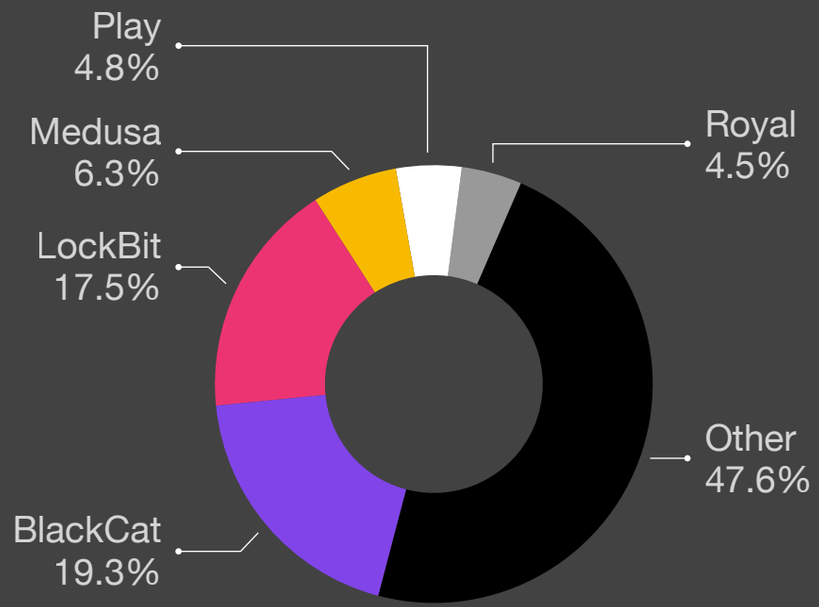
Average payout US $740,144

+126% from Q1/23

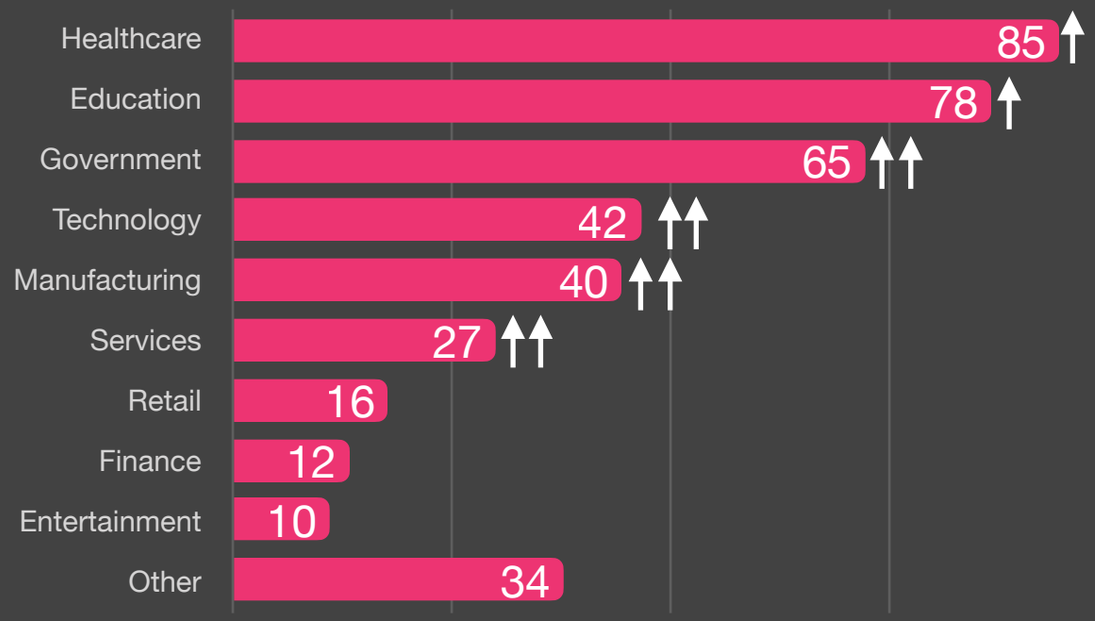
Ransomware by Country



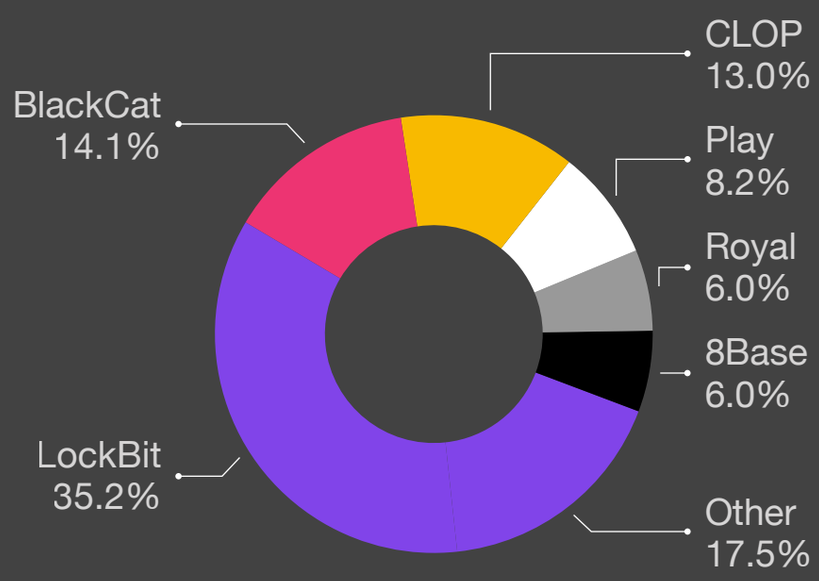
Reported Ransomware Variant



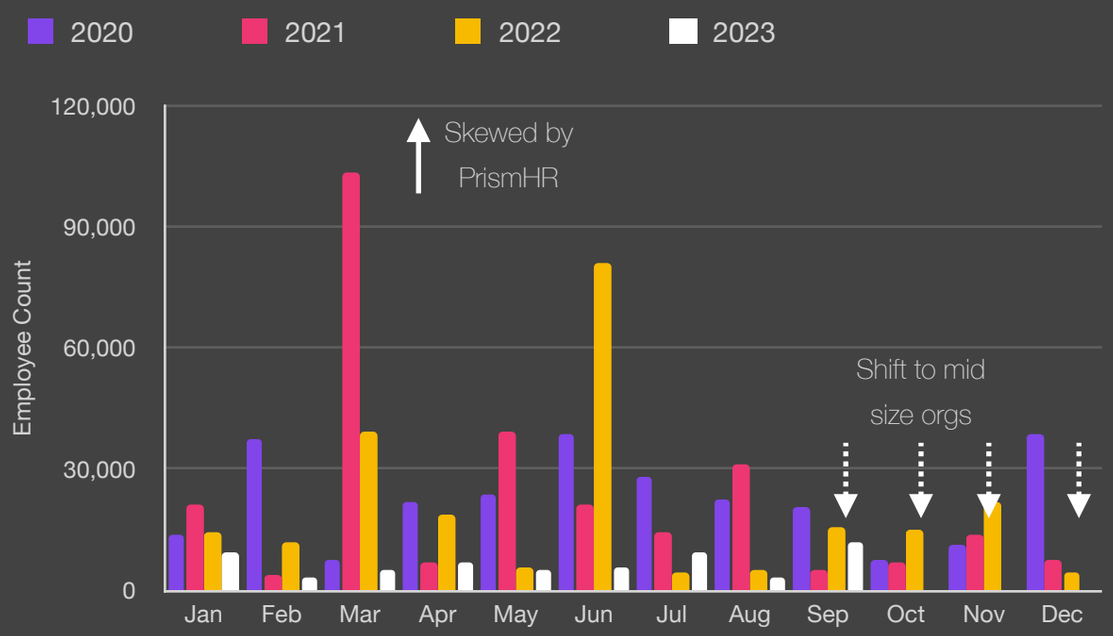
Ransomware by Industry



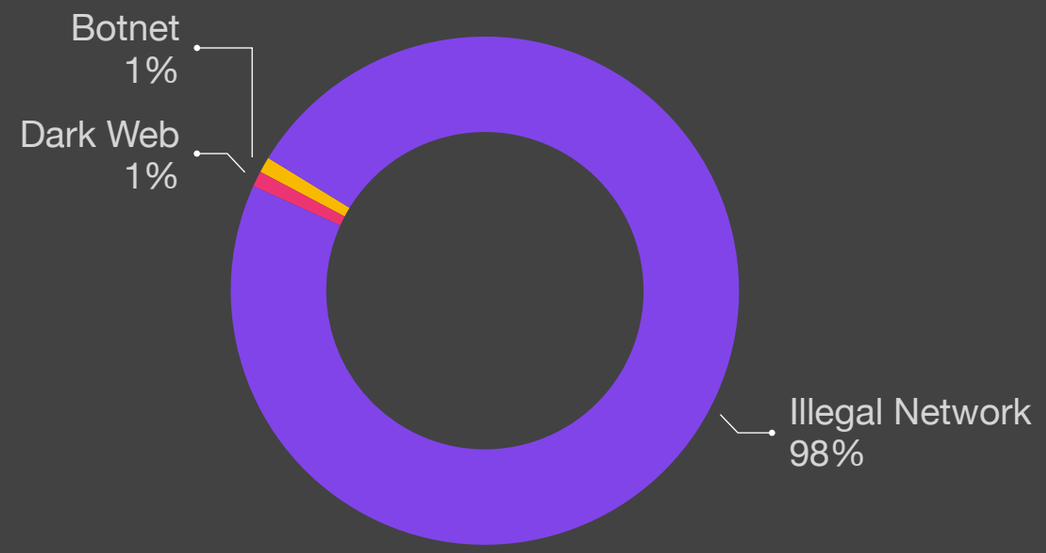
Unreported Ransomware Variant



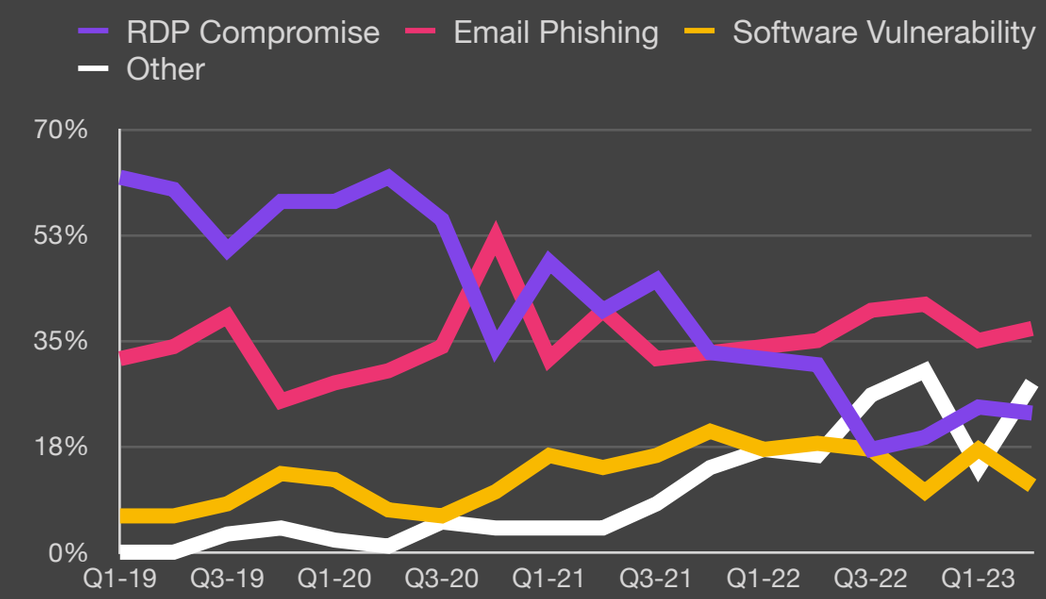
Size of Organization



Exfiltration Techniques

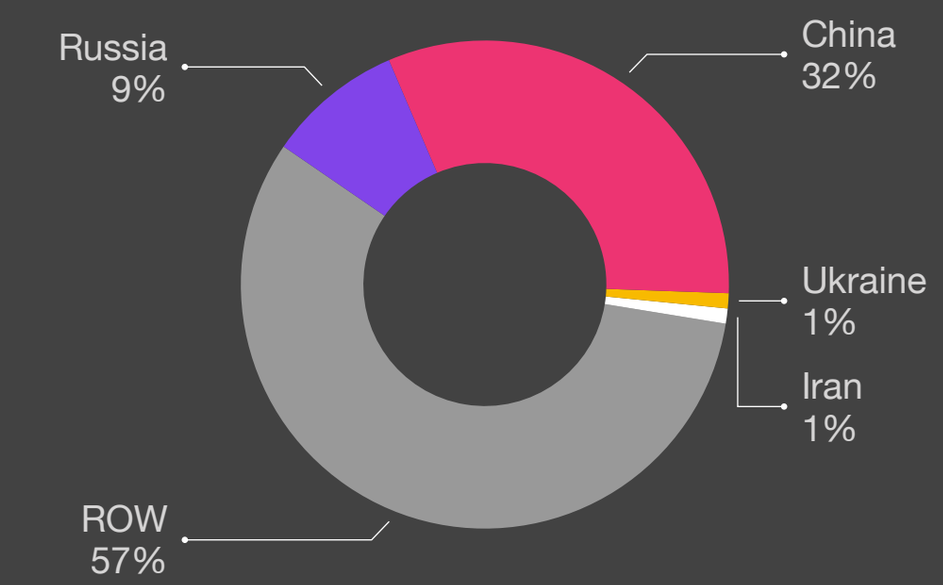


Attack Vectors[2]



[2]Courtesy Coveware

Ransomware Exfiltration Country



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.