October 2023

We recorded sixty-four publicly disclosed ransomware attacks in this month, the busiest October we have seen since we started this blog in 2020 and a 45% increase on last year's figures.

Government and healthcare were the most impacted sectors, with sixteen and fourteen attacks respectively. Notorious gangs BlackCat and LockBit topped the lists of variants in a month were we also seen a number of new gangs emerge, including a possible rebrand of the disbanded Hive ransomware group.

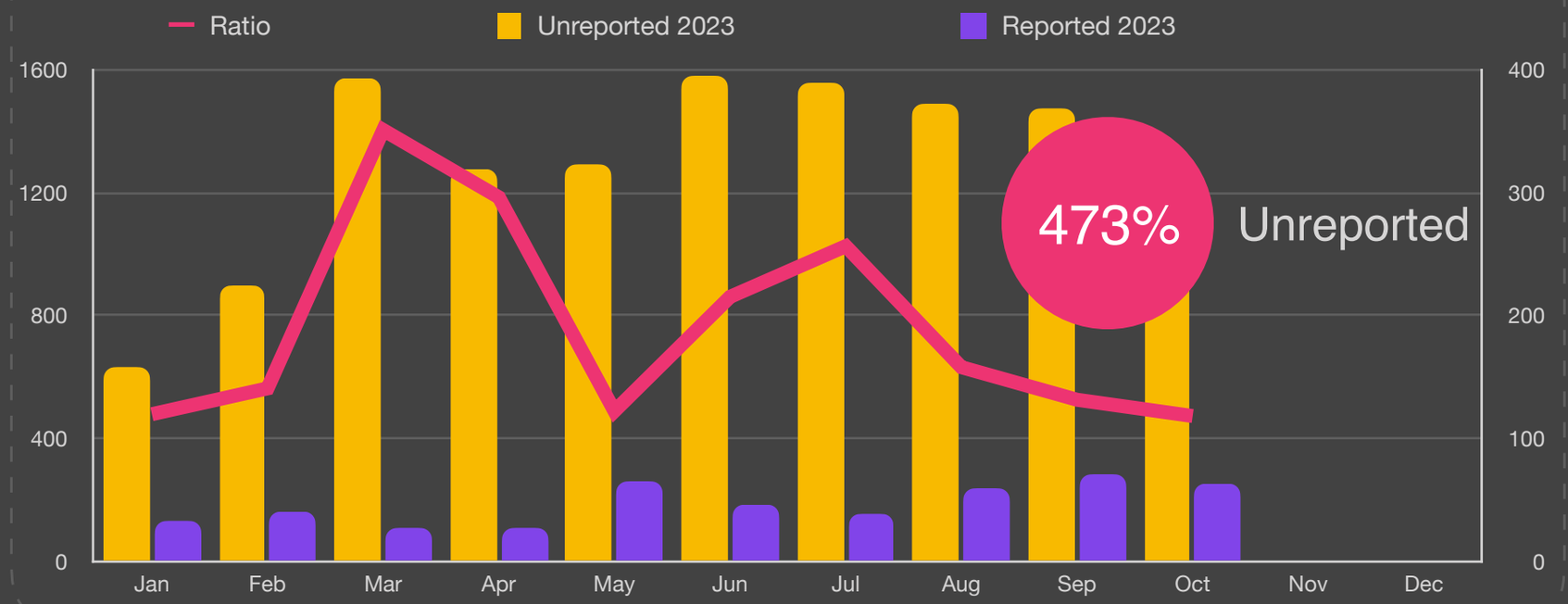
Roundup

October was the 3rd largest month for ransomware this year with a total of 64 disclosed and 303 undisclosed attacks with a ratio of 473% unreported to reported. This ratio is now one of the lowest we have seen in the last year and a good sign that companies are starting to report breaches rather than hide them. We expect this trend to continue with the recent charges against the SolarWinds CISO by the SEC.

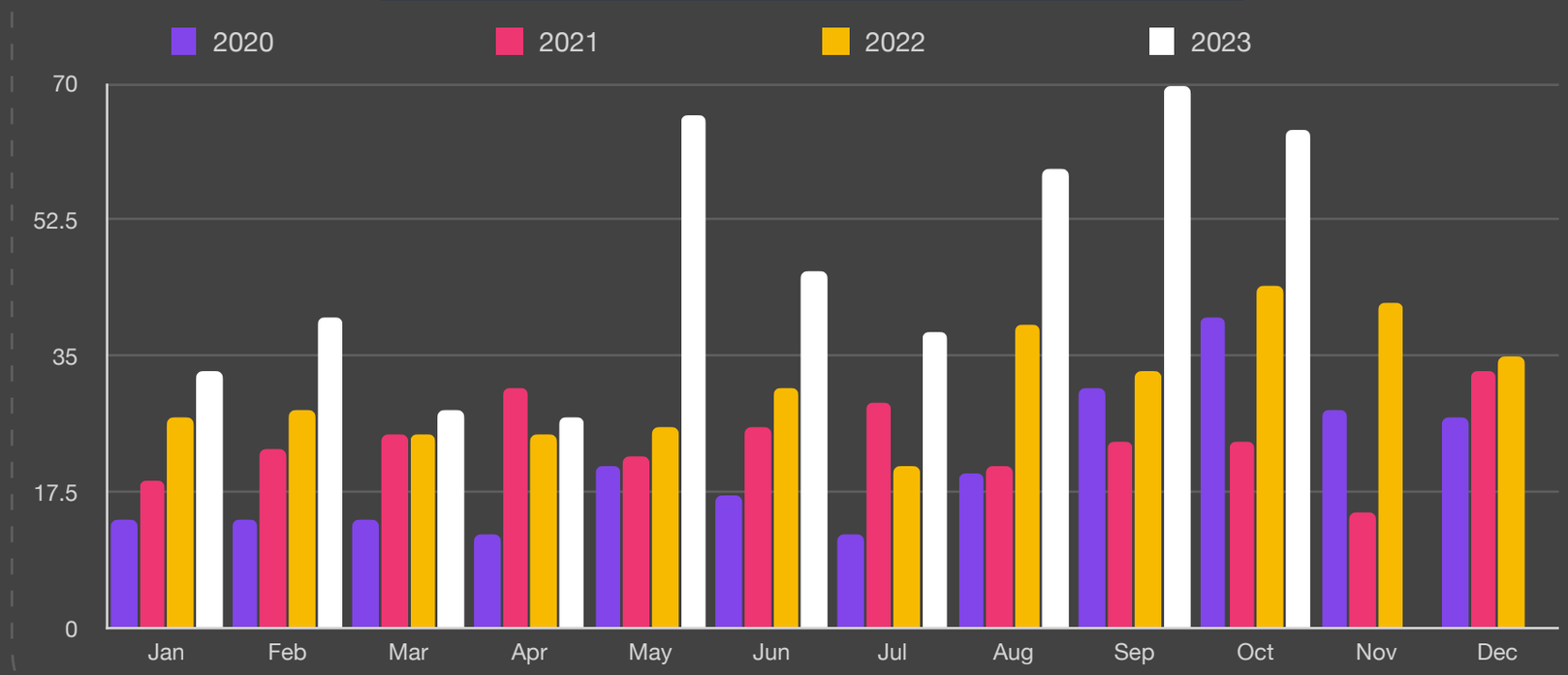
Other notable changes this month saw the biggest changes in the Services and Government sectors with 33% and 25% increases respectively. Smaller increases were seen in both Healthcare and Manufacturing of 16% and 13% respectively.

BlackCat and Lockbit continue to dominate the unreported attacks with 18.8% and 16.9% respectively and also correlate with the top trends in unreported variants. 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

473% Unreported

3rd Highest of Year

1st Highest Ransom Payouts

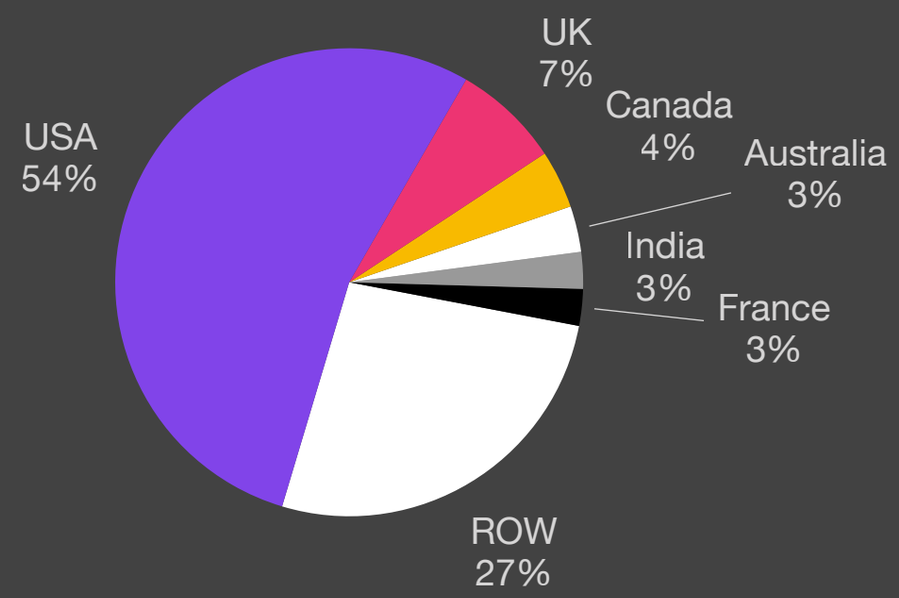
48% of all attacks use PowerShell

90% of attacks exfiltrate data

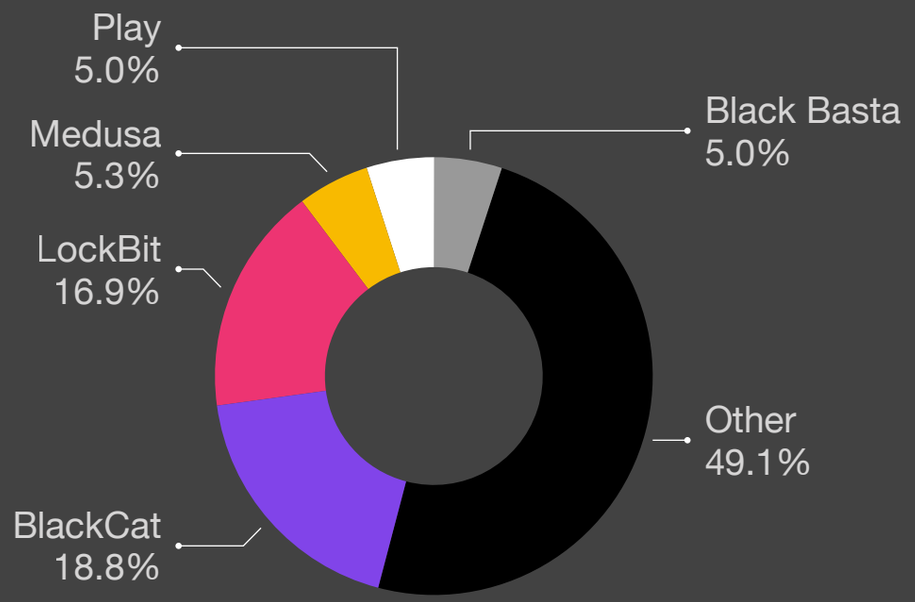
Average payout US $850,700

+15% from Q2/23

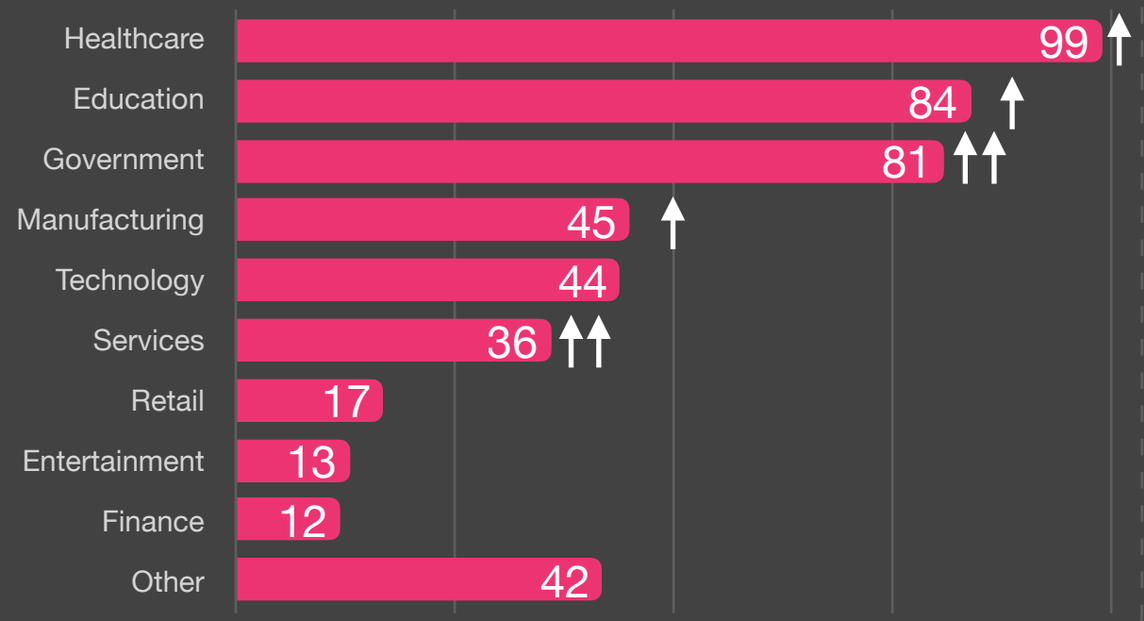
Ransomware by Country



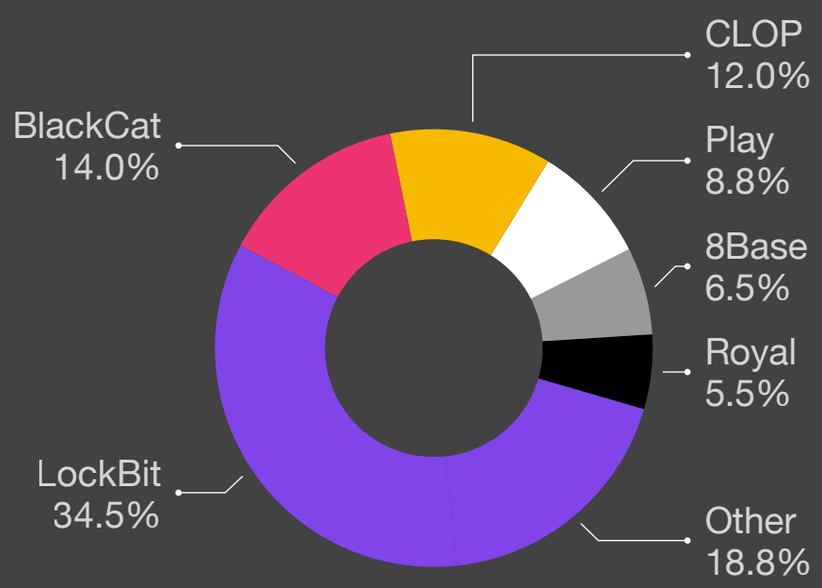
Reported Ransomware Variant



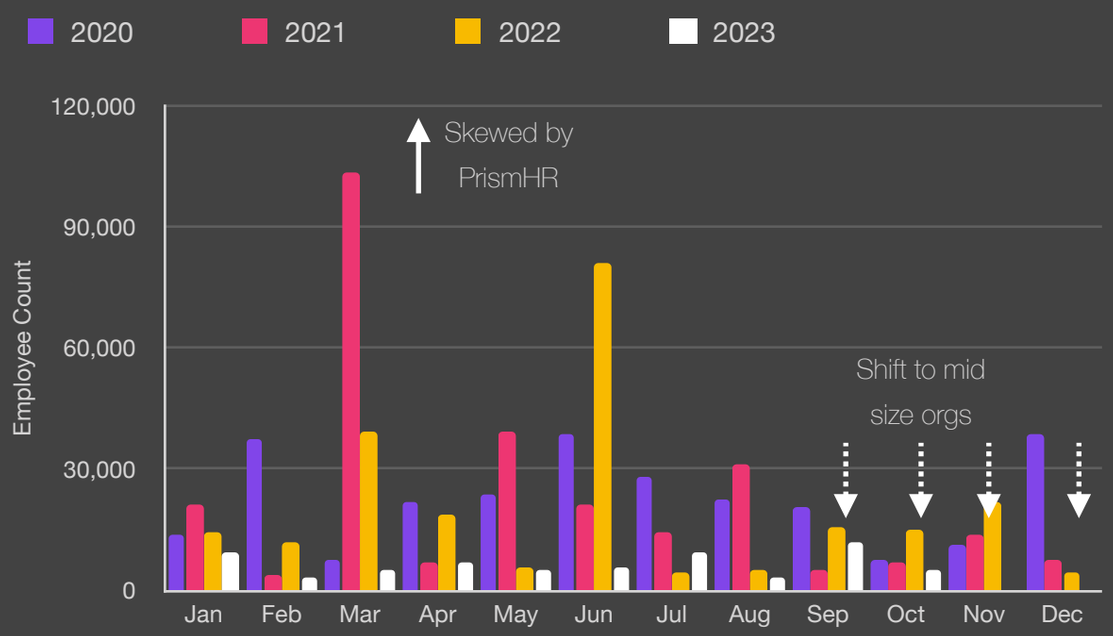
Ransomware by Industry



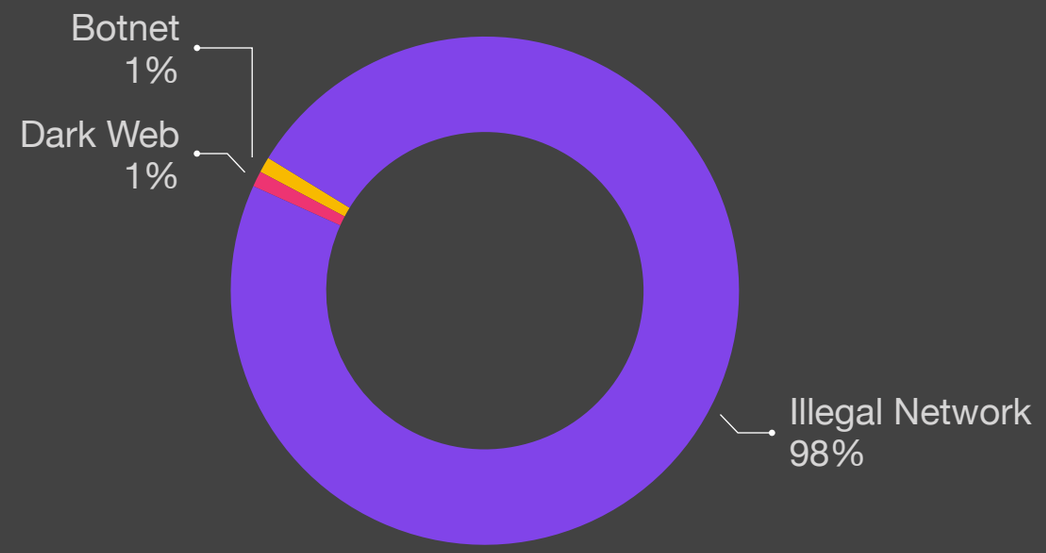
Unreported Ransomware Variant



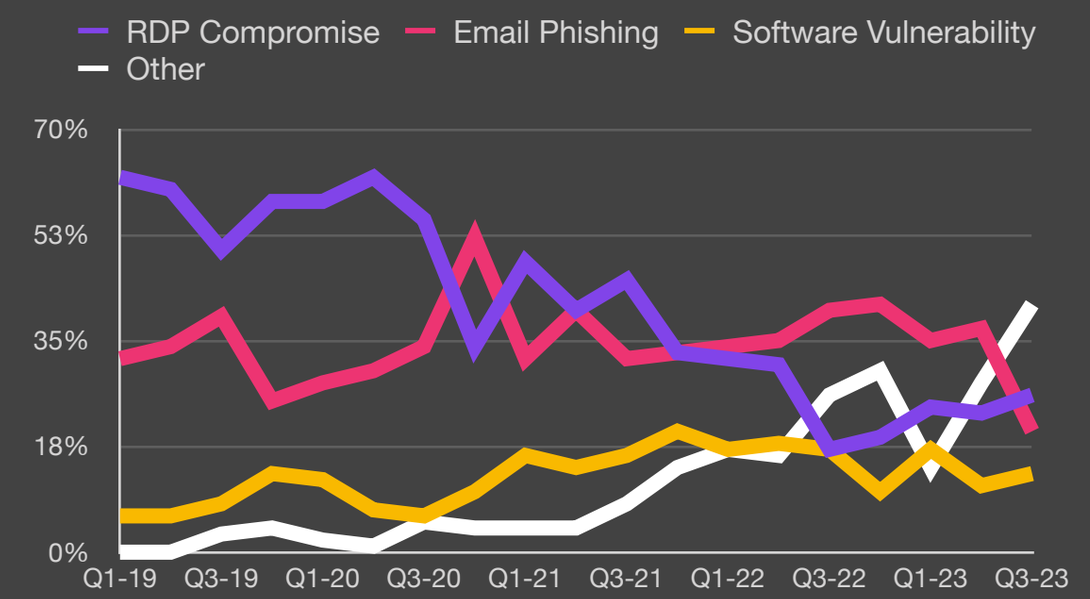
Size of Organization



Exfiltration Techniques

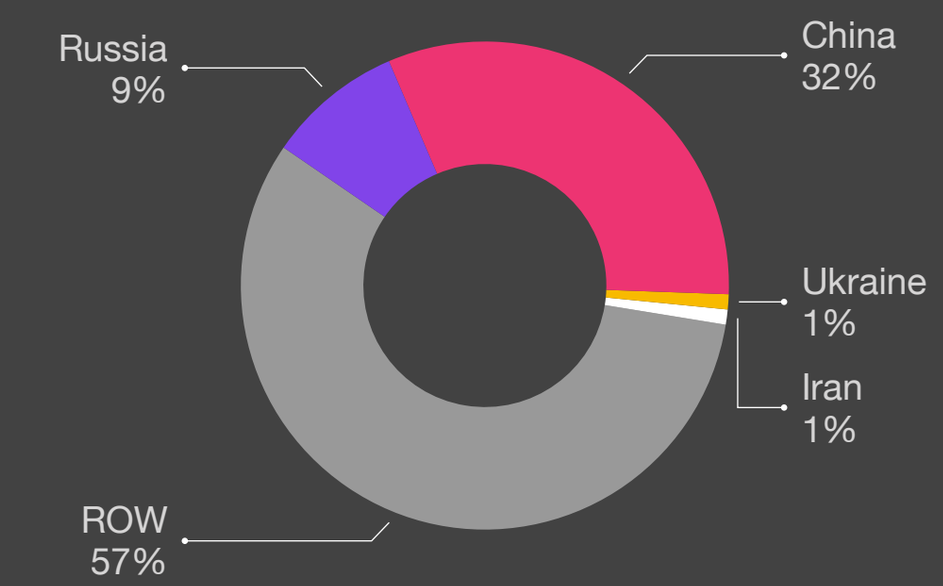


Attack Vectors[2]



[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.