

Introduction

This month we uncovered 63 publicly disclosed ransomware attacks, making it the highest August we've ever recorded, and the third highest month of the year so far. Unsurprisingly healthcare was the worst hit sector with 19 attacks, representing 30% of all reported incidents. In a month where RansomHub took credit for almost a third of attacks, a number of new variants such as Lynx and Helldown also caused chaos for their victims.

Roundup

August witnessed the 3rd highest number of attacks for the year with 63 publicly disclosed attacks, already surpassing the total number of attacks in 2020, 2021 and 2022. It also represents the the second highest number of undisclosed attacks of the year with 464, with a ratio of 737% undisclosed to disclosed attacks.

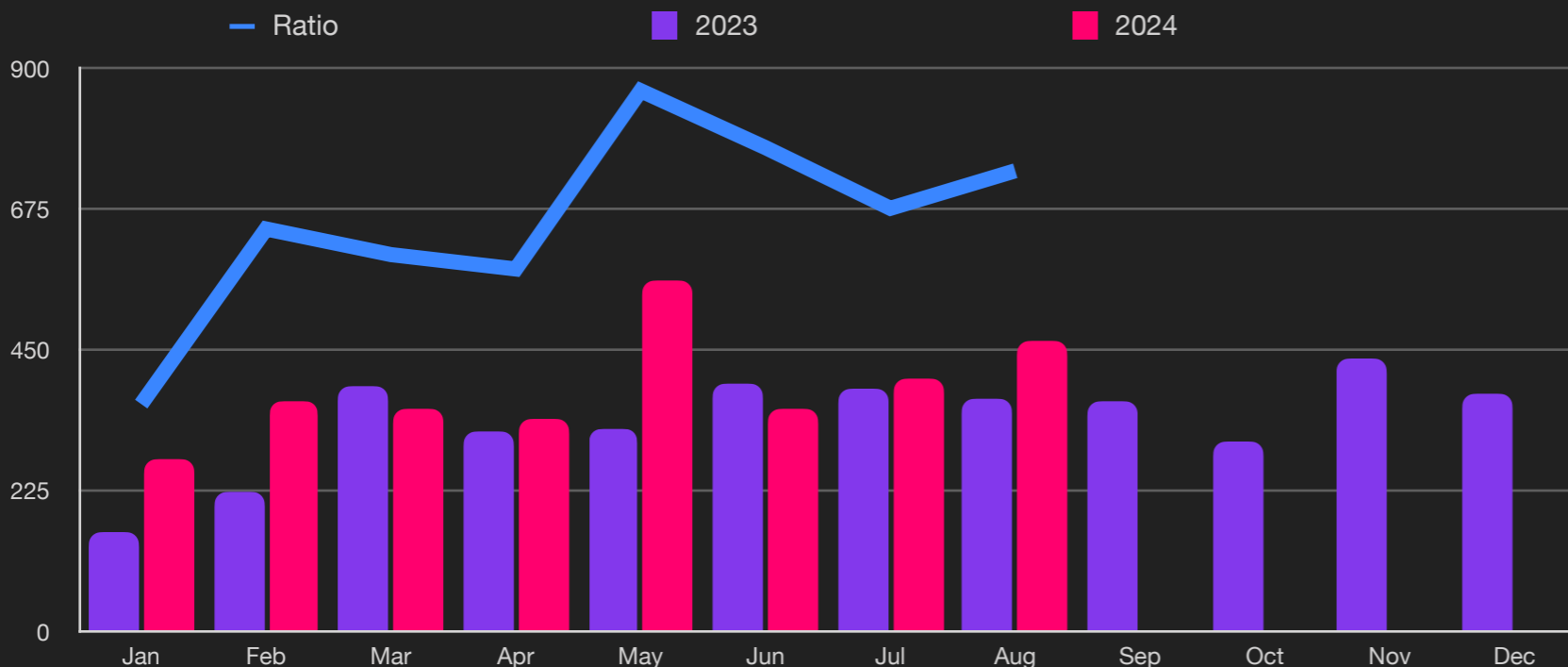
From a sector perspective Healthcare had the biggest increase this month with 20%, or 16 verified attacks. This makes Healthcare the most targeted sector by a significant margin, followed by Government and Education, which saw only modest increases of 10% and 12% respectively.

In terms of variants, this month we saw RansomHub, a new entrant rocket to 7.9% of all attacks, followed by Medusa and Rhysida at 7.6% and 6.0% respectively. While LockBit still maintains its lead with 18.4% of all attacks, we only saw one confirmed attack this month. A similar trend was observed in unreported attacks with RansomHub commanding 8.4% of attacks.

Lastly, we saw data exfiltration rates to China increase significantly to 20% this month (an increase of 4%) and Russia stable at 6%, with 93% of all attacks involving data exfiltration.



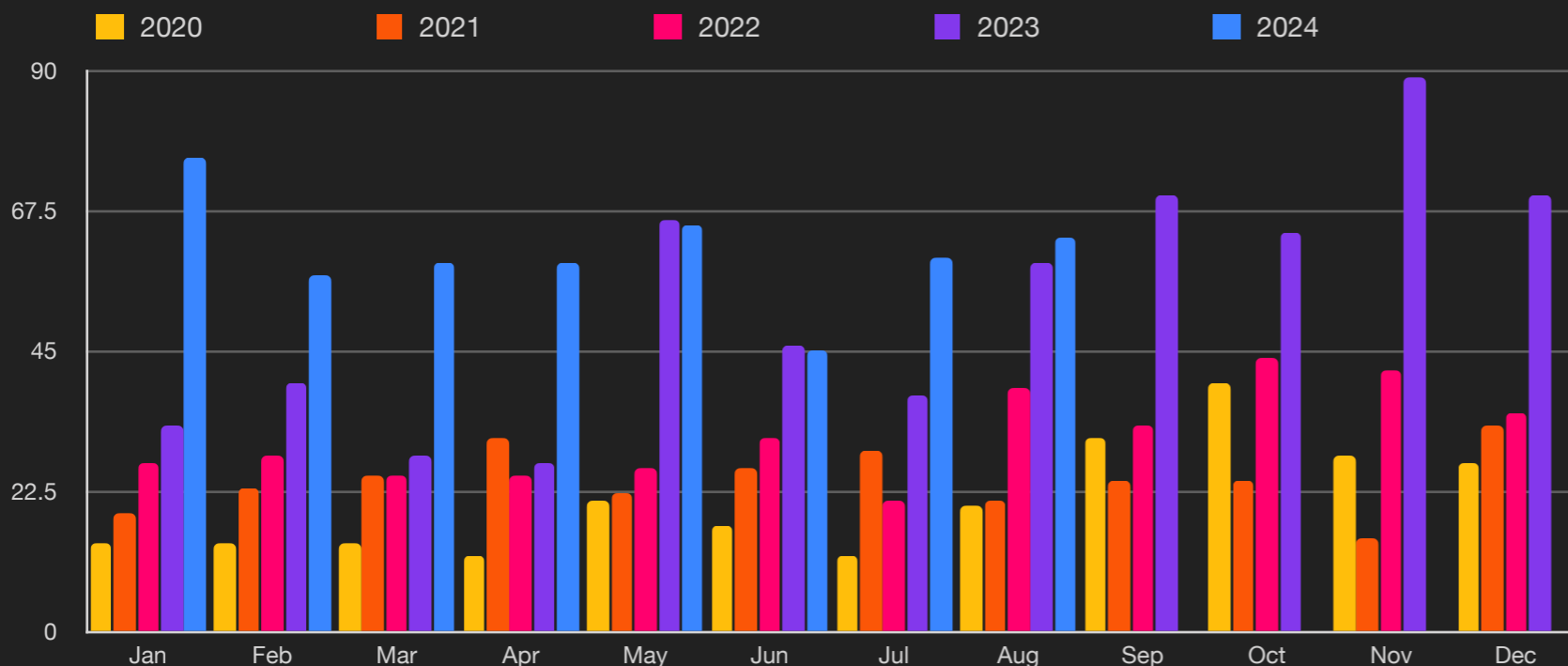
Unreported Ransomware Attacks



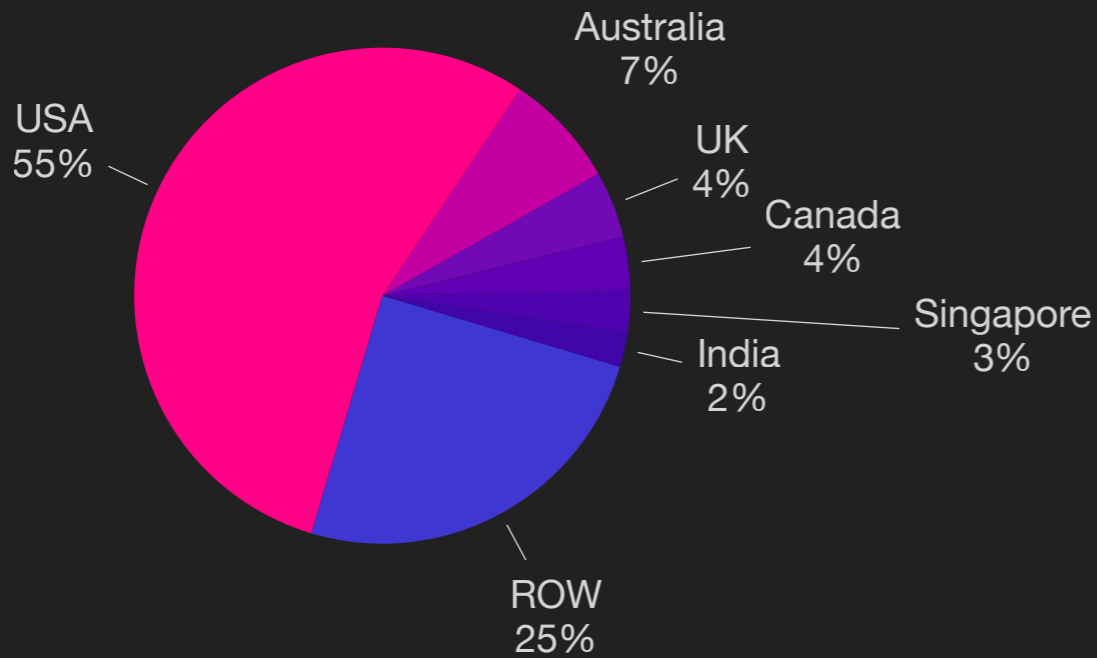
Key Trends

- 737% Unreported
- 3rd Highest of Year
- 60% of all attacks use PowerShell
- 93% of attacks exfiltrate data
- 43% of exfiltration victims pay vs 36% +20% from Q1/24
- Average payout US \$391,015 +2.4% from Q1/24

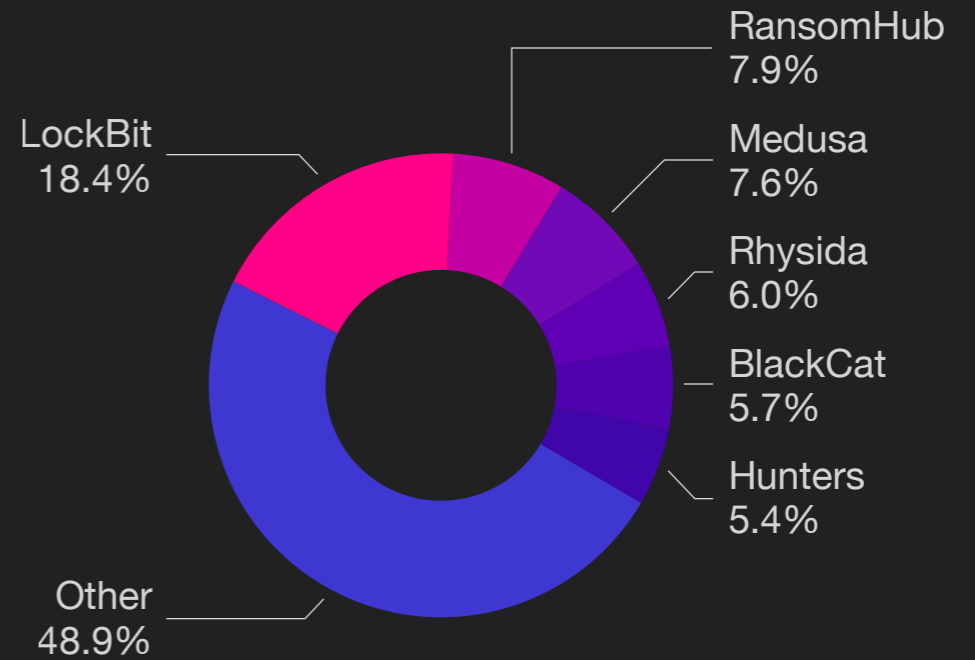
Reported Ransomware by Month



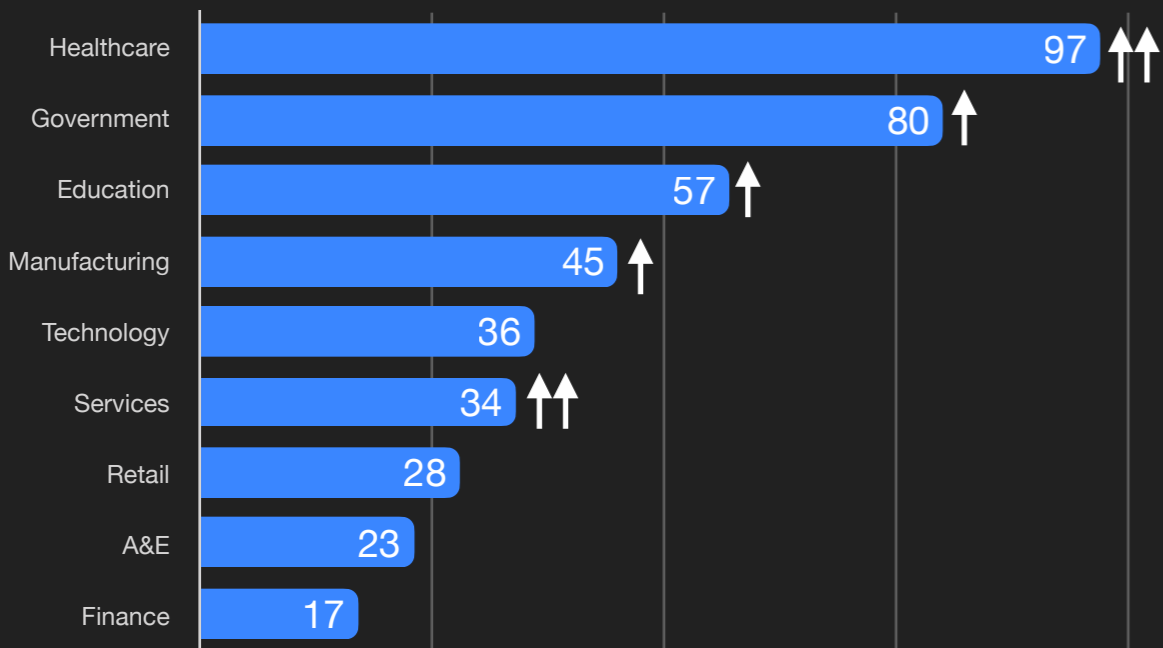
Ransomware by Country



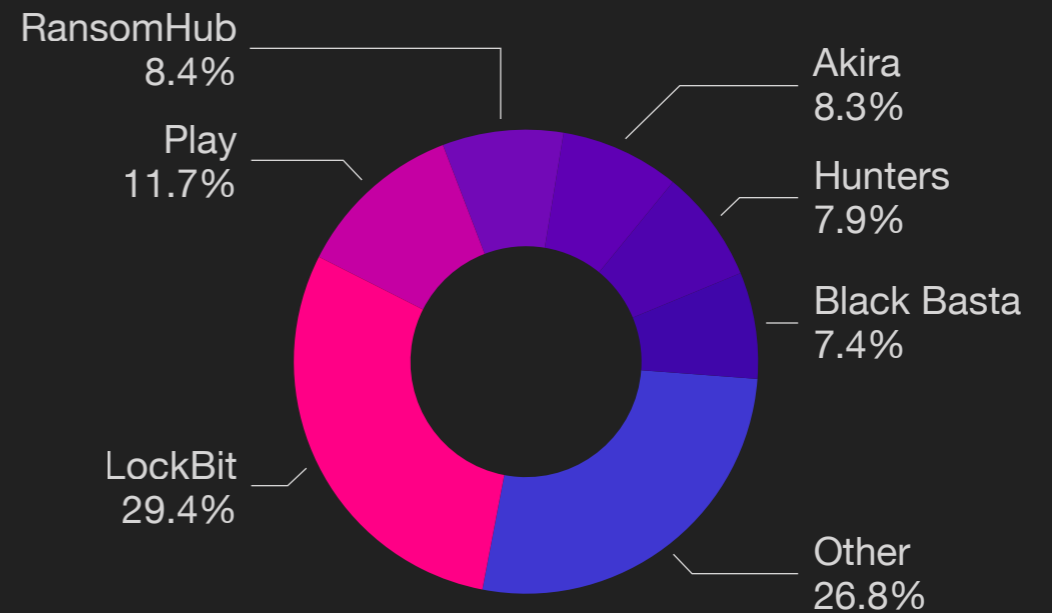
Ransomware Variant (Reported)



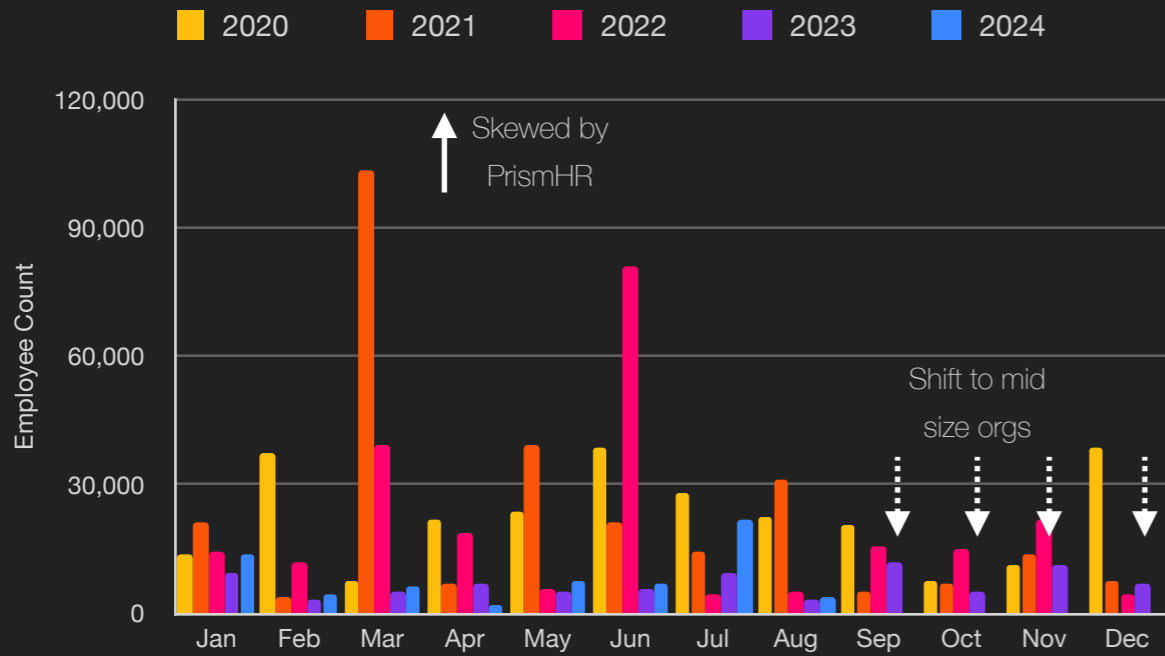
Ransomware by Industry



Ransomware Variant (Unreported)



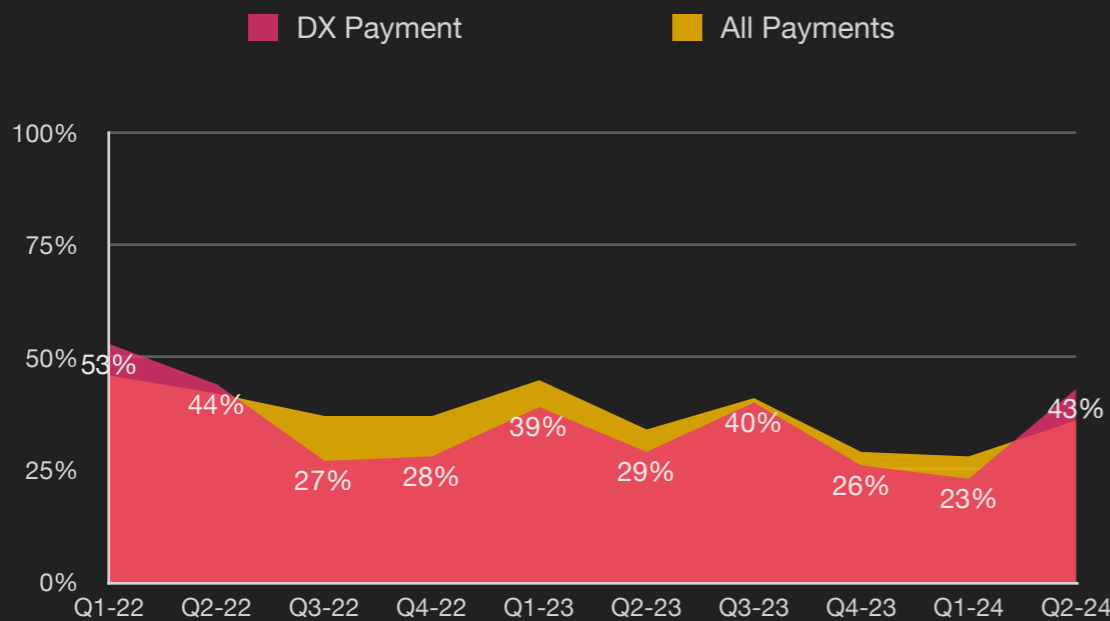
Size of Organization



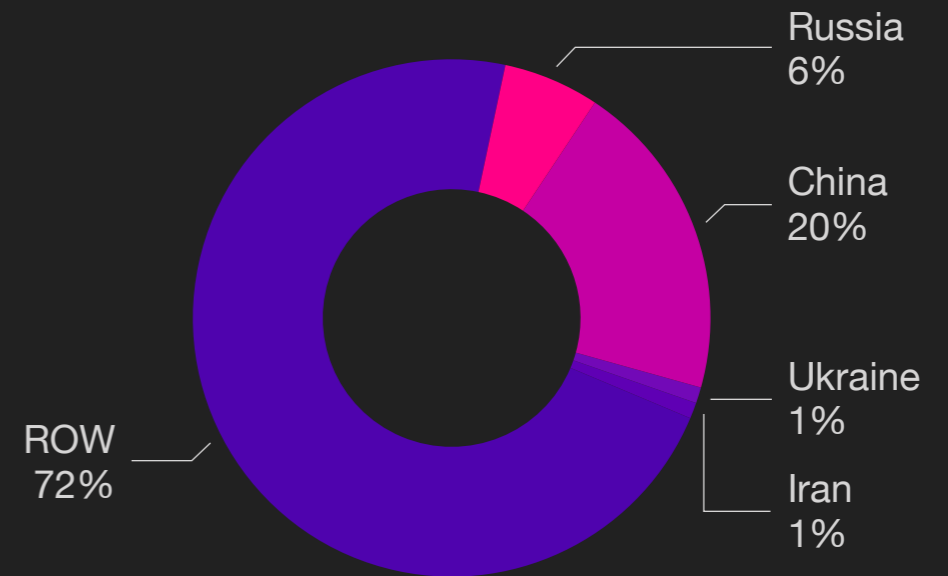
Exfiltration Techniques



Exfiltration Payment Rates²



Exfiltration by Country



²Courtesy Coveware



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.

