Introduction

March saw 59 ransomware attacks make headlines with healthcare and government leading. The City of Hamilton and Town of Ponoka in Canada experienced attacks that caused widespread issues across government systems including online payments, while the City of Huntsville had their data held hostage following an attack. In other news Belgian beer producer Duvel halted production at all Belgian sites and its US site after the Stormous ransomware group claimed to have exfiltrated 8 GB of company data.

Roundup

2024 continues to break new records, with March being no exception with a total of 59 attacks, the highest in 4 years, and a 110% increase over 2023. Unreported attacks also remained strong with 356 attacks and a ratio of 603%, similar to last month. This indicates 6x as many attacks go unreported.

March also saw some big sector changes, with government attacks increasing by a massive 100%, and healthcare by 76%, now both leading the way with a total of 30 each. Our leading sector last month, education, increased by 35% and now sits in third place, while manufacturing increased 33% with a total of 27 attacks.

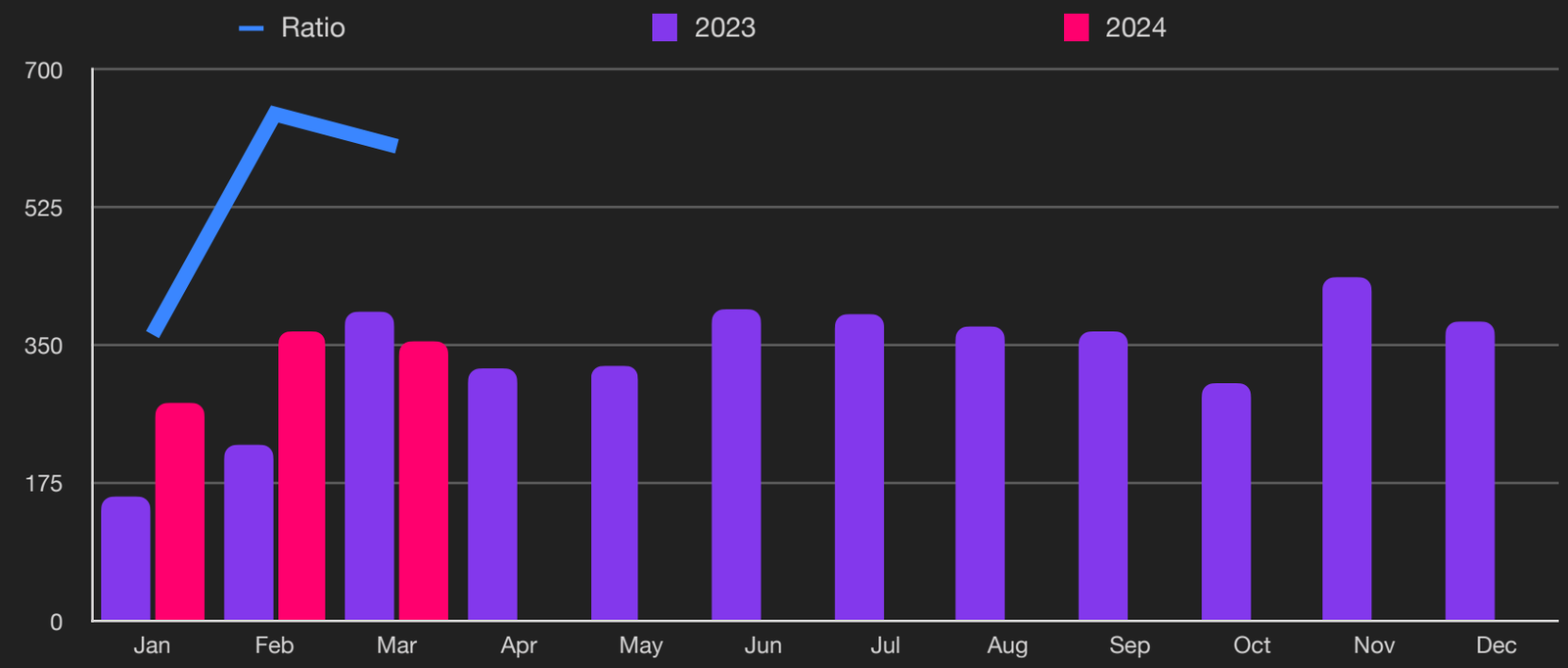
From a variant perspective LockBit continues as the dominant ransomware variant with 25.8%, followed by BlackCat with 14.2%, little change from the previous month. We do however see some large changes in unreported variants this month, which is typically a leading indicator for reported attacks in later months. This month we saw Black Basta and Hunters grow by 80% and 49% respectively, while 8Base grew by 39%.

Lastly, data exfiltration is now involved in 92% of all attacks. As the primary goal of all attacks, data exfiltration ensures that attackers can threaten and sell victims data for years to come, regardless of whether payments are made or not. This month we also see China and Russia dominate as the leading destinations for exfiltrated data with 18% and 8% respectively.

BlackFog State of Ransomware Report

March 2024

Unreported Ransomware Attacks

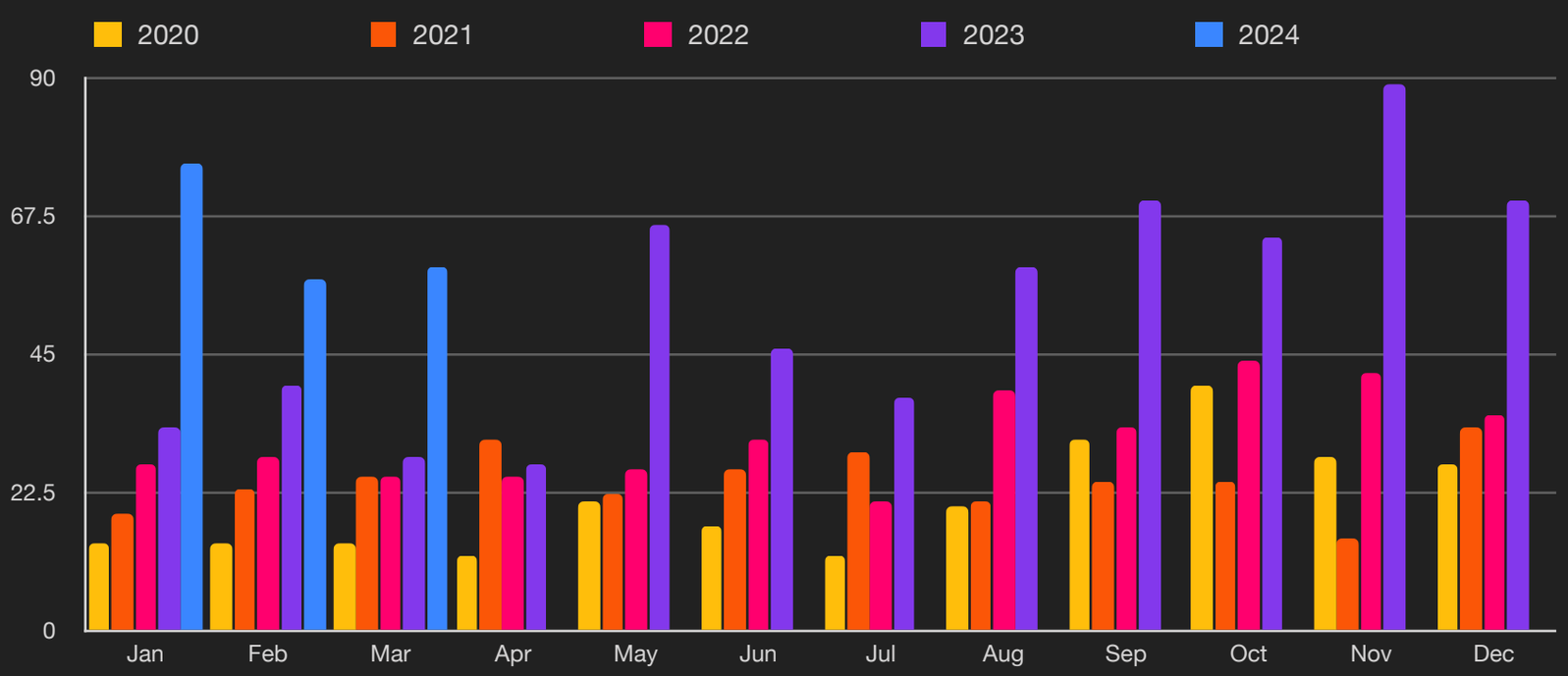


Key Trends

603% Unreported

1st Highest March

Reported Ransomware by Month



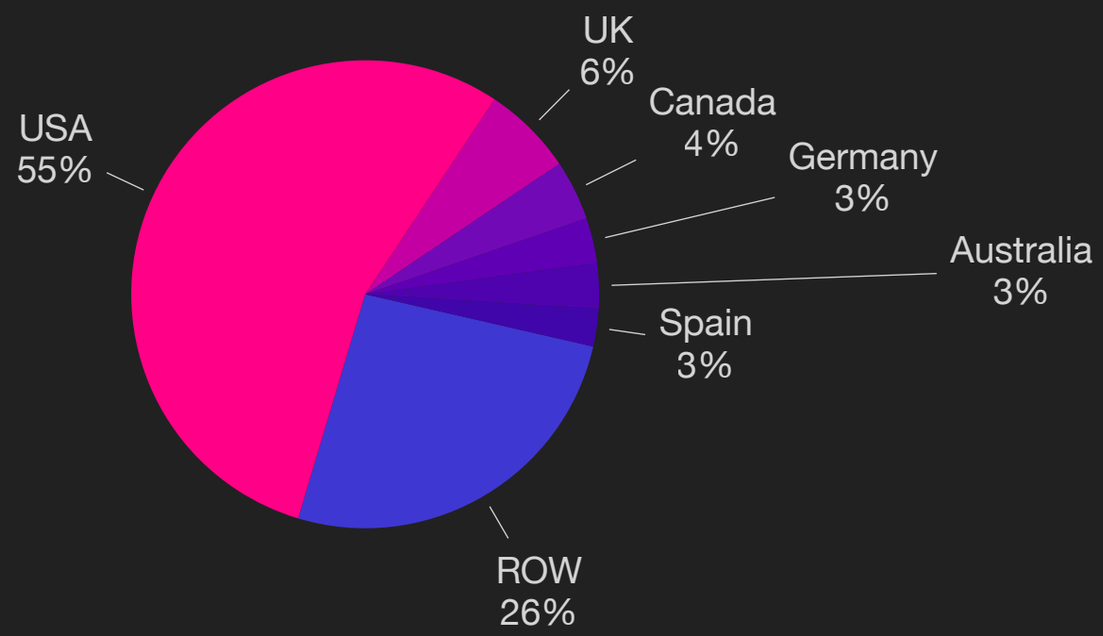
45% of all attacks use PowerShell

92% of attacks exfiltrate data

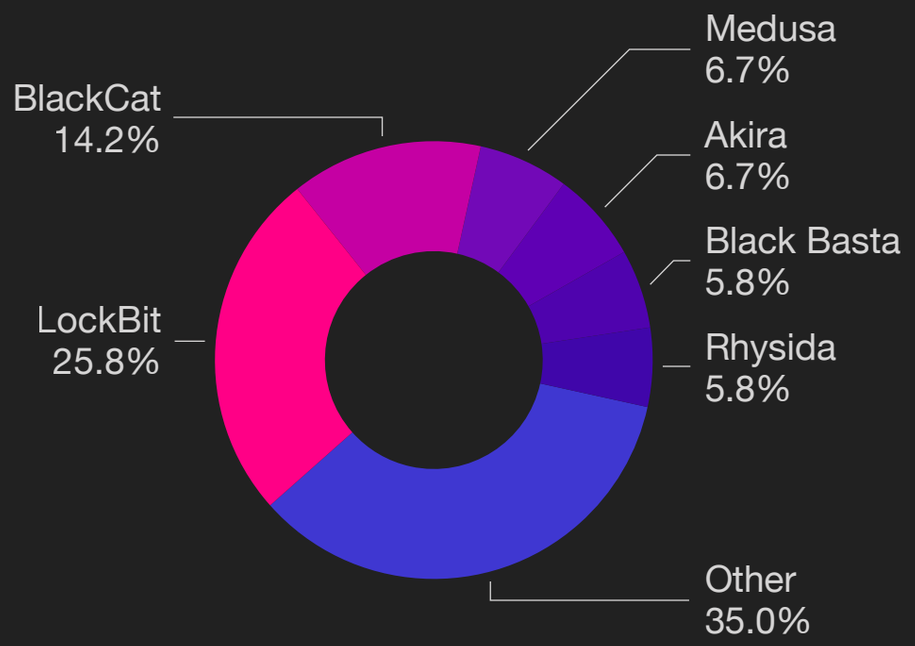
Average payout US $568,705

-33% from Q3/23

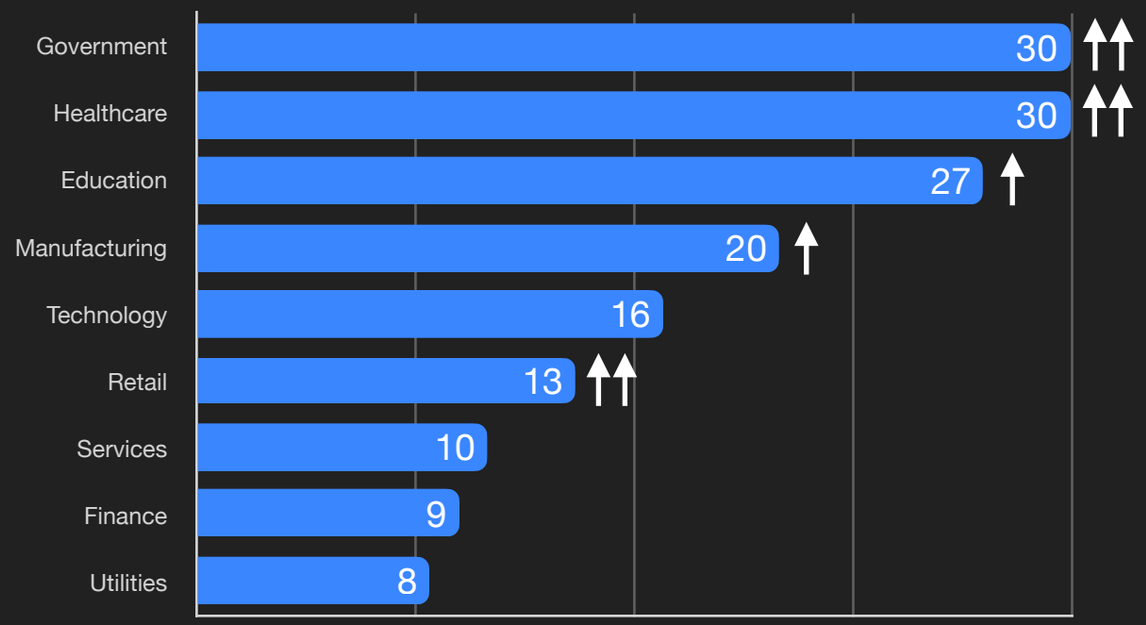
Ransomware by Country



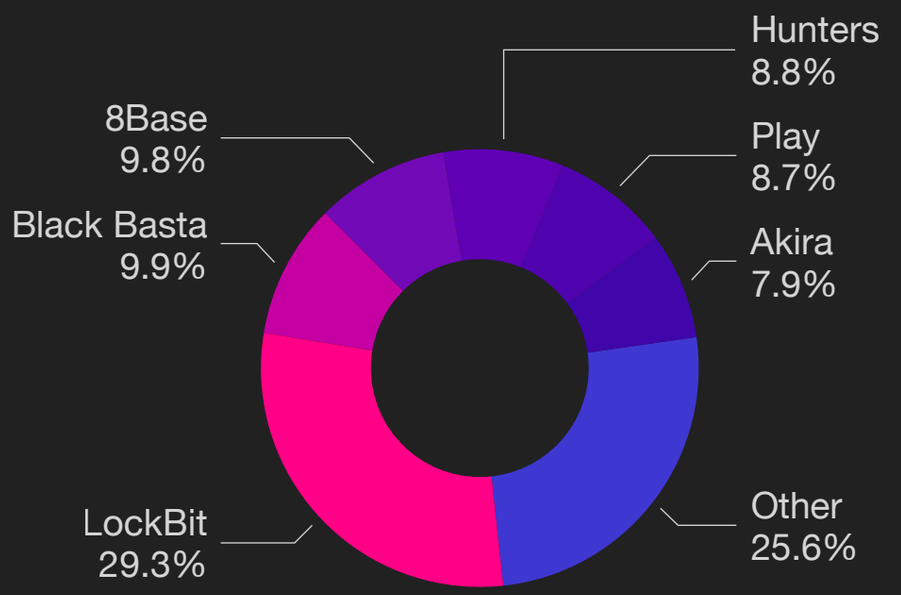
Ransomware Variant (Reported)



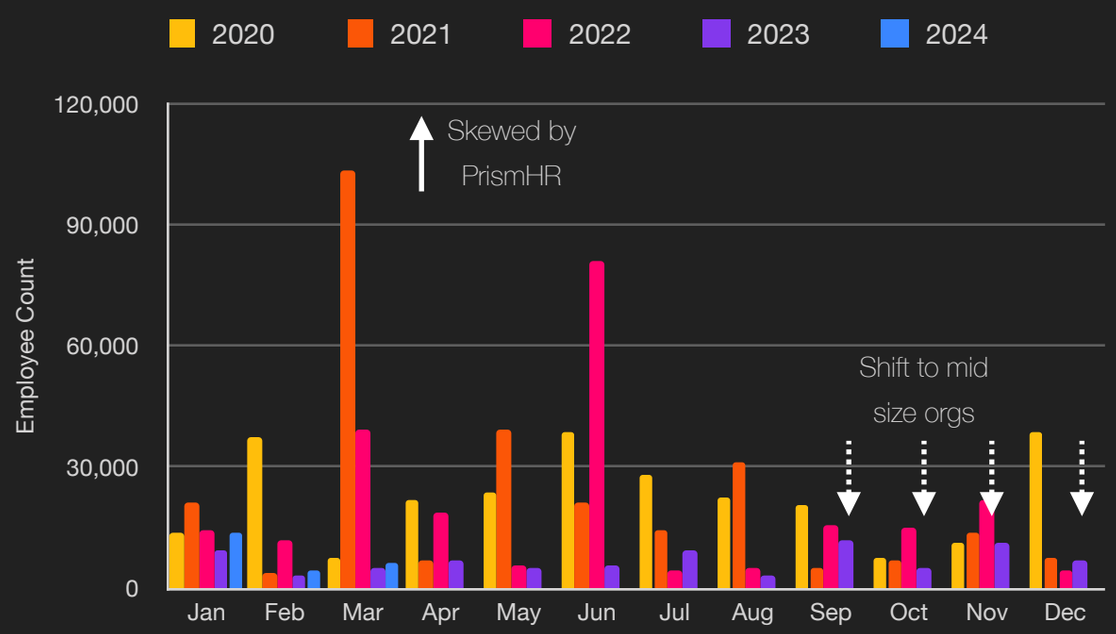
Ransomware by Industry



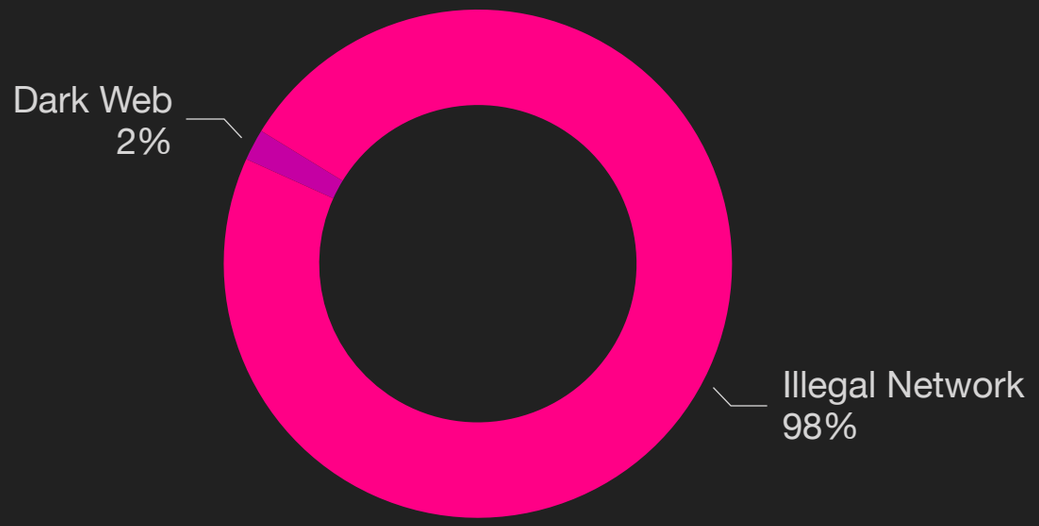
Ransomware Variant (Unreported)



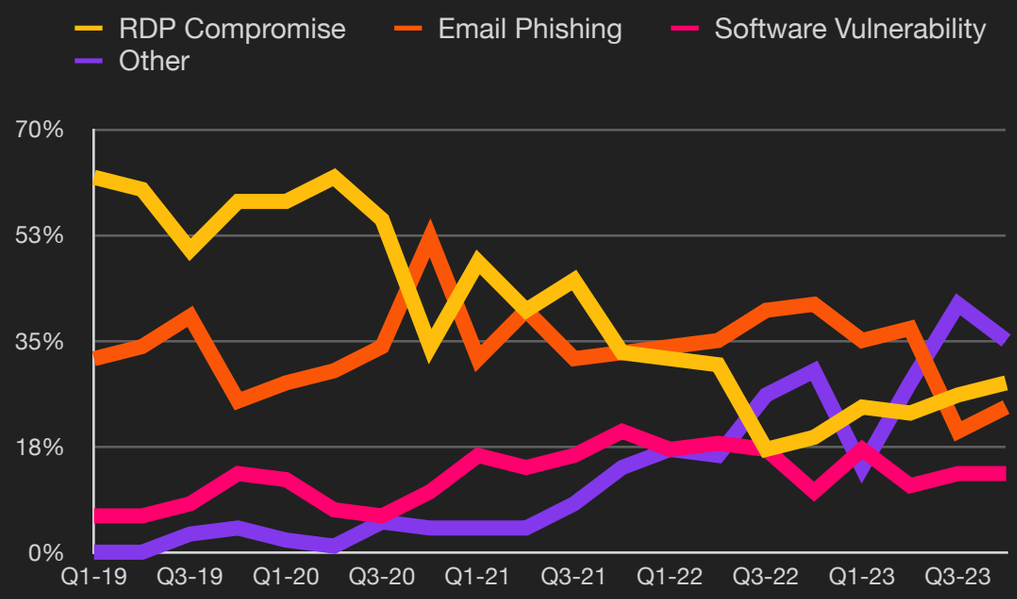
Size of Organization



Exfiltration Techniques

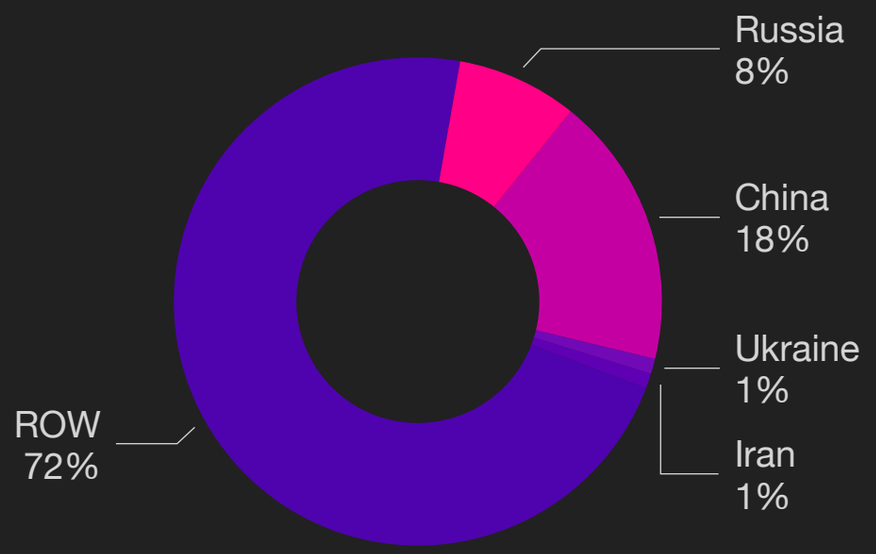


Attack Vectors[2]



[2]Courtesy Coveware

Exfiltration by 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.