Introduction

For the first time this year we saw the monthly total of disclosed attacks fall less than the previous year, if only by one incident! By contrast however, we saw the number of unreported attacks skyrocket and reach the highest level we've ever recorded. May saw 65 attacks make news, including Panda Group, the largest Chinese fast food chain in the US, Indian food production company DoubleHorse and Canadian retailer London Drugs who were forced to close 80 stores after an attack by LockBit.

Roundup

May saw our second highest month of the year with a total of 65 reported attacks and a record 562 unreported attacks. The high number of unreported attacks meant our ratio of reported to unreported was also the highest of the year at 865%, or nearly 9 times the number of reported attacks.

From a sector perspective we saw the healthcare sector continue to dominate with a total of 57 attacks, an increase of 30% from last month. Closely followed was education, services and manufacturing sectors with increases of 29%, 28% and 24% respectively, with the government sector increasing by a modest 14% in comparison.

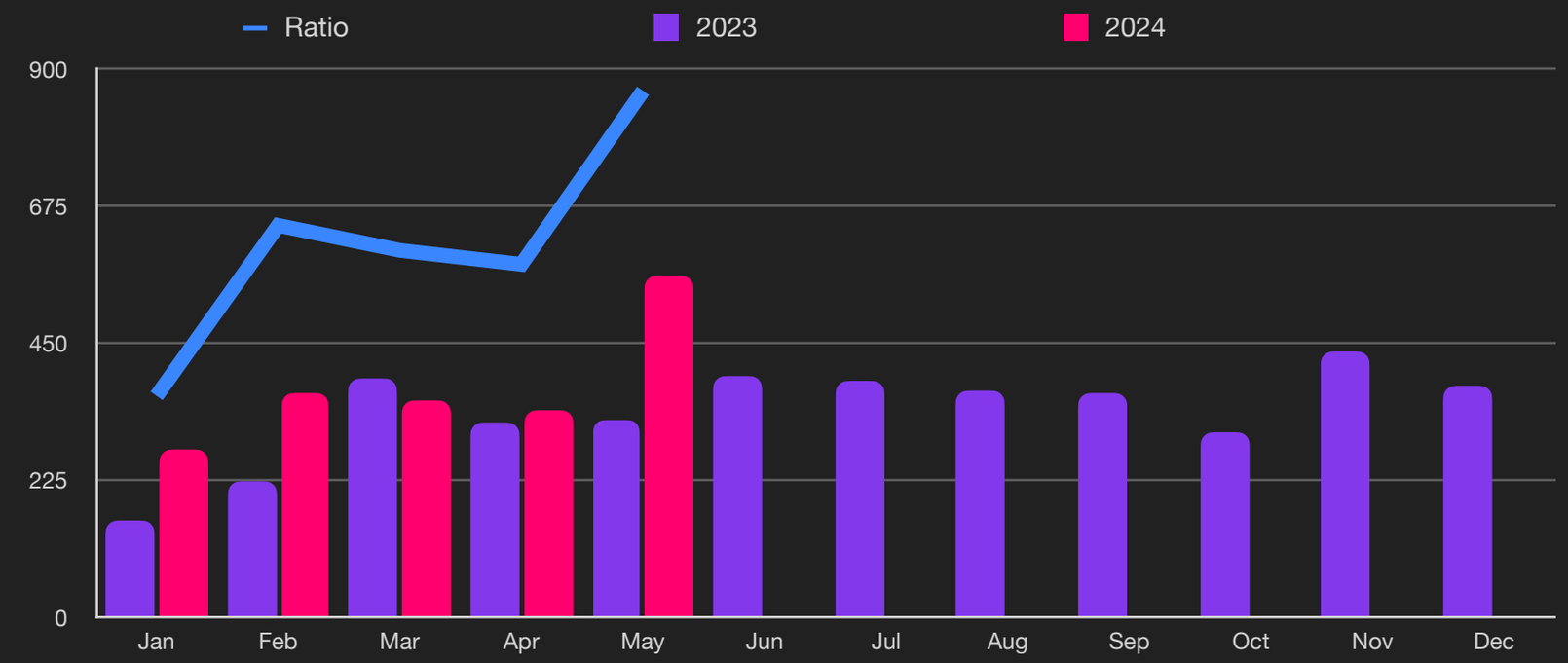
In terms of variants LockBit continued to dominate in both reported and unreported attacks with increases of 32% and 82% respectively. We expect to see these numbers further impact the reported attacks in the coming months. This month we also saw a 29% increase in Medusa in terms of reported attacks.

Lastly, we saw the number of Powershell attacks increase to 51%, a 6% increase from last month, with 92% of all attacks involving some form of data exfiltration. China and Russia continued as the leading destinations of data exfiltration with 15% and 6% respectively.

BlackFog State of Ransomware Report

May 2024

Unreported Ransomware Attacks

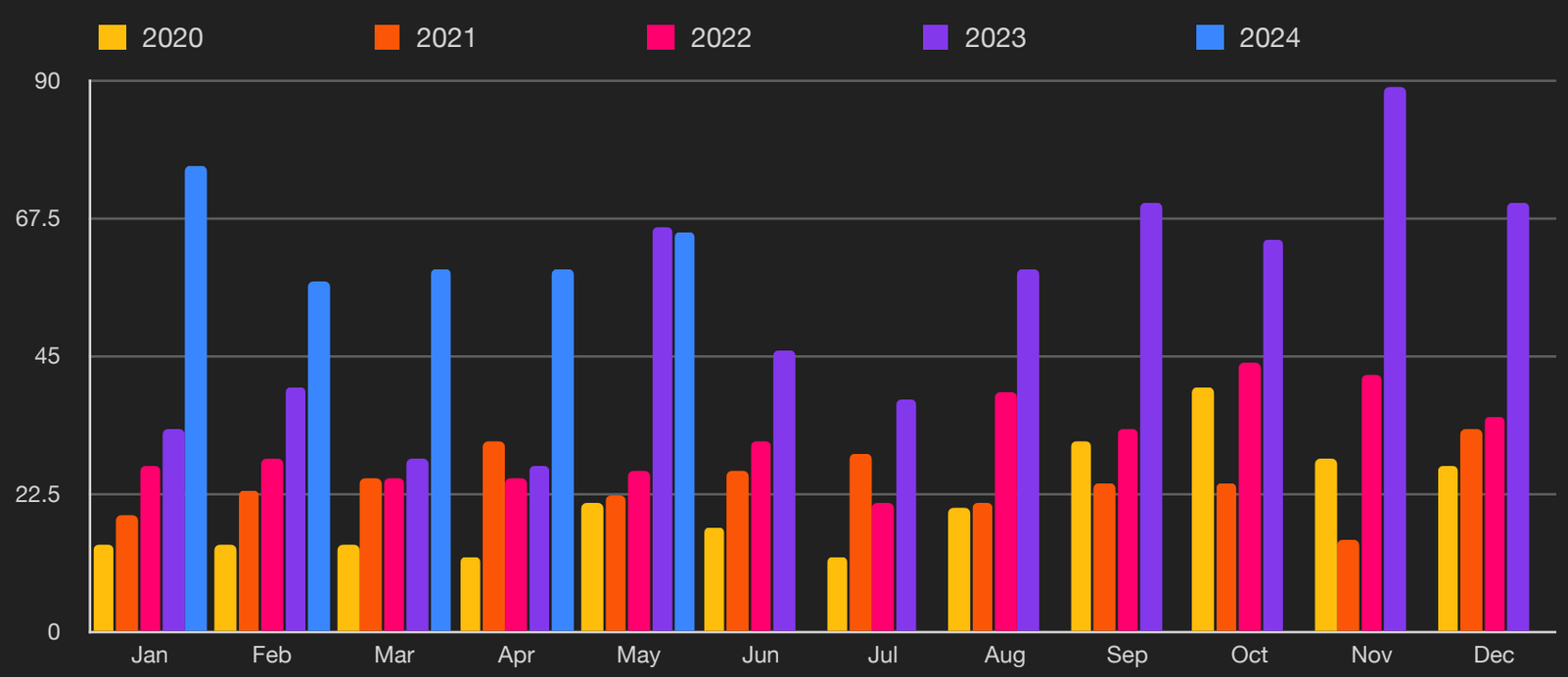


Key Trends

865% Unreported

1st Highest Unreported

Reported Ransomware by Month



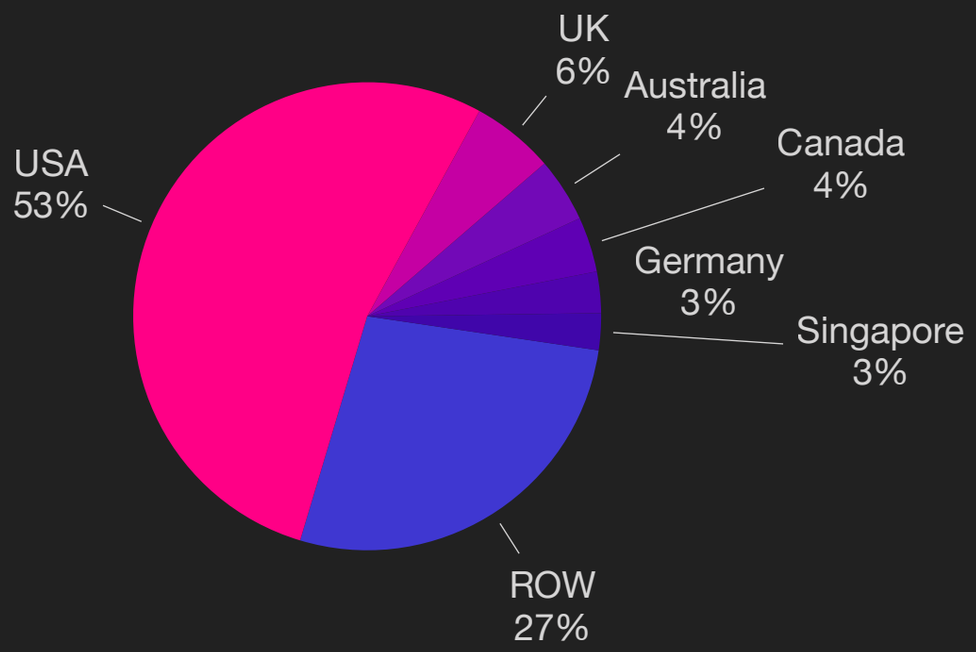
51% of all attacks use PowerShell

92% of attacks exfiltrate data

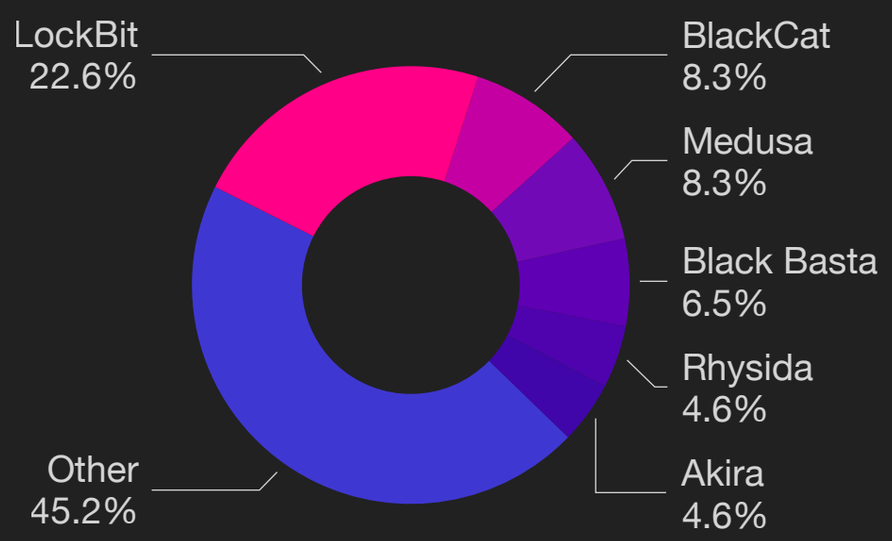
Average payout US $381,980

-32% from Q4/23

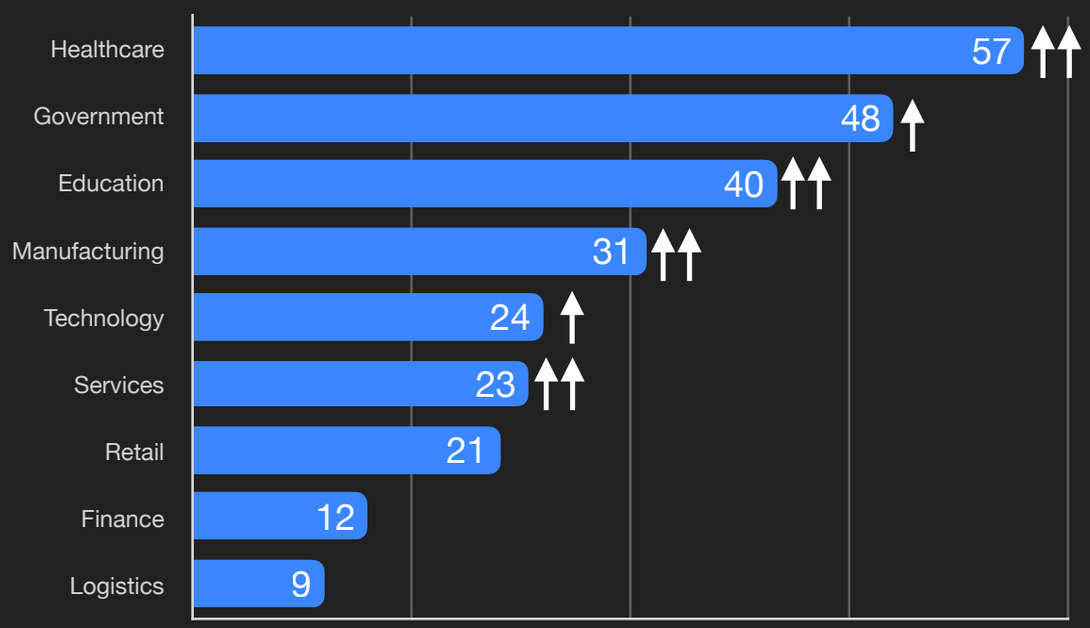
Ransomware by Country



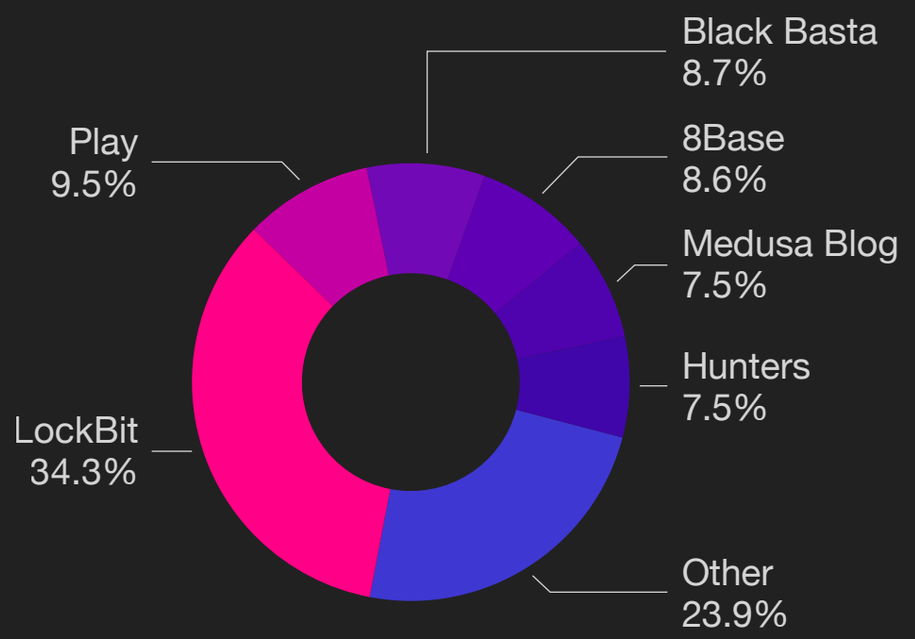
Ransomware Variant (Reported)



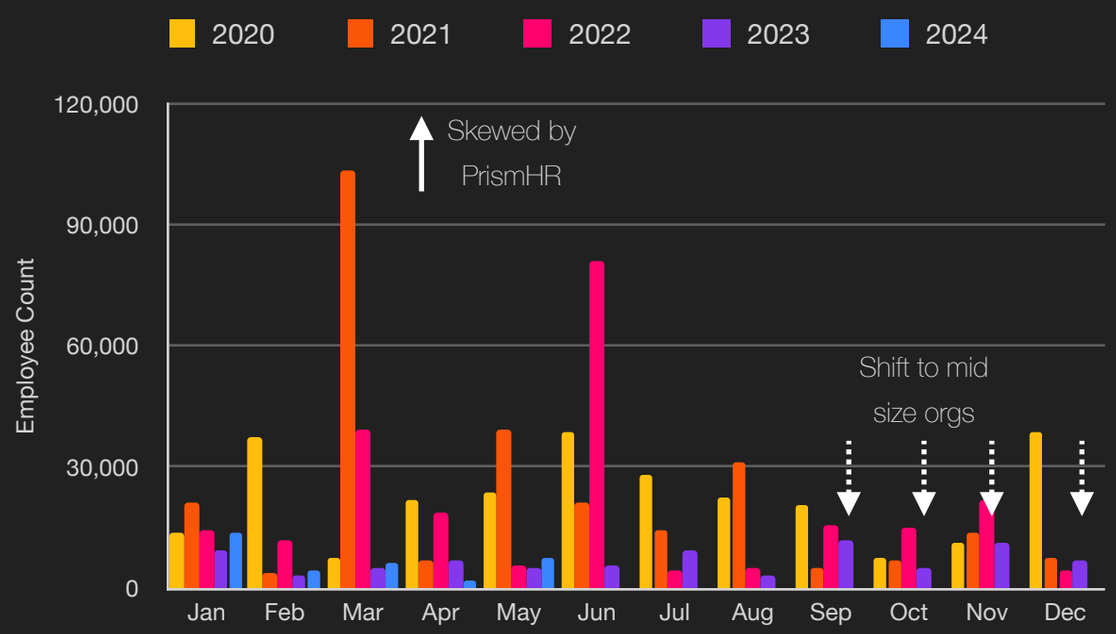
Ransomware by Industry



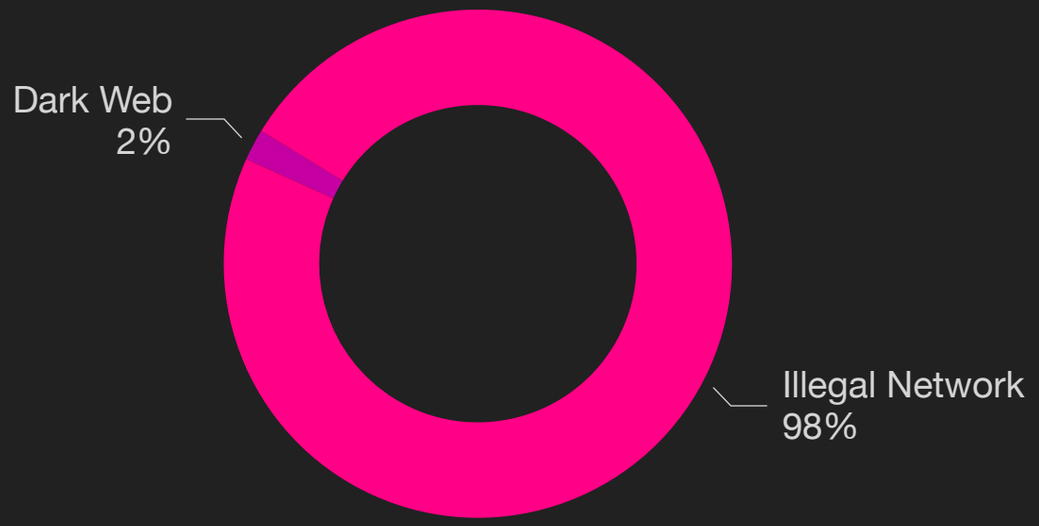
Ransomware Variant (Unreported)



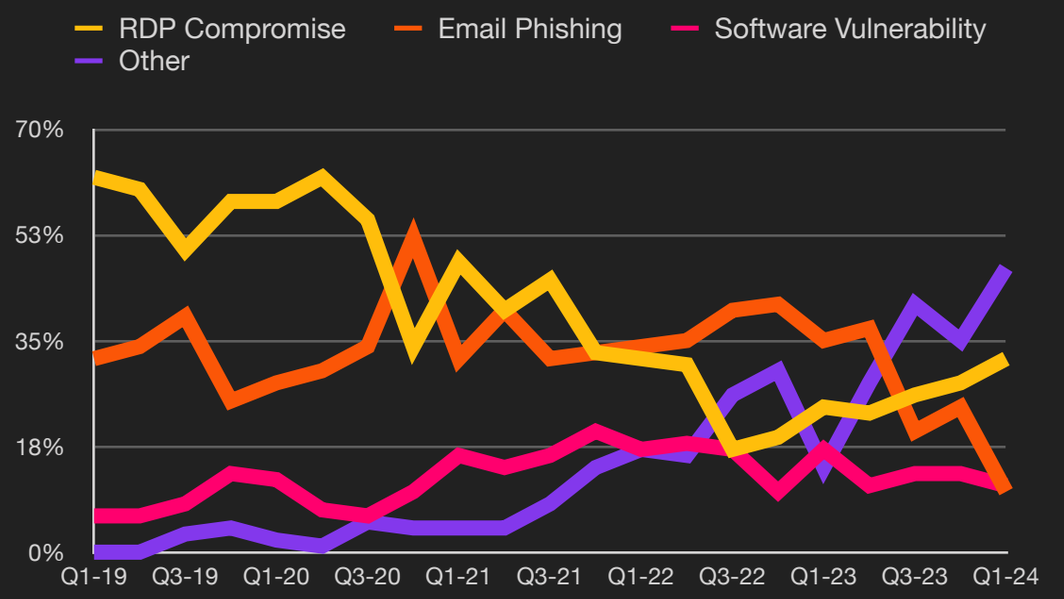
Size of Organization



Exfiltration Techniques

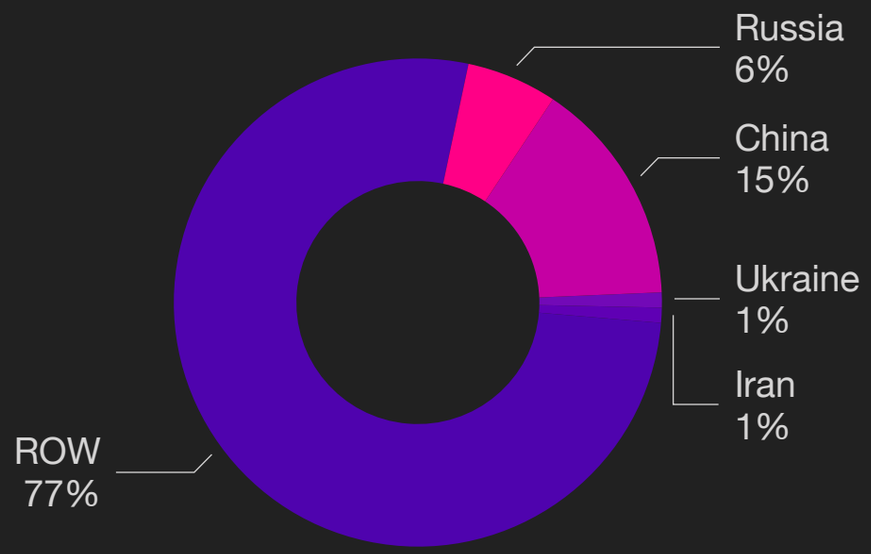


Attack Vectors[2]



[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.