Introduction

With 77 publicly disclosed ransomware attacks, October takes the title for highest number of attacks recorded in 2024 so far. This marks a significant 20% rise compared to October 2023. Healthcare continued to top targeted verticals with 23% of attacks, with the services industry following closely behind. New ransomware gang Sarcoma made waves this month, joining RansomHub as the most active variants for the month.

Roundup

As we head into the holiday season, we are breaking new records with 77 publicly disclosed attacks in October, the highest of the year and the second highest in 5 years. Interestingly, we are seeing the same trend in unreported attacks with 542 attacks and the second highest on record with a 7 to 1 ratio of unreported to reported attacks.

Sector wise we saw the most dramatic increase in Services, with a massive 35% increase, followed by Healthcare and Manufacturing with increase of 18% and 16% respectively. Only modest increases were seen with Education and Government, with 9% and 8% respectively.

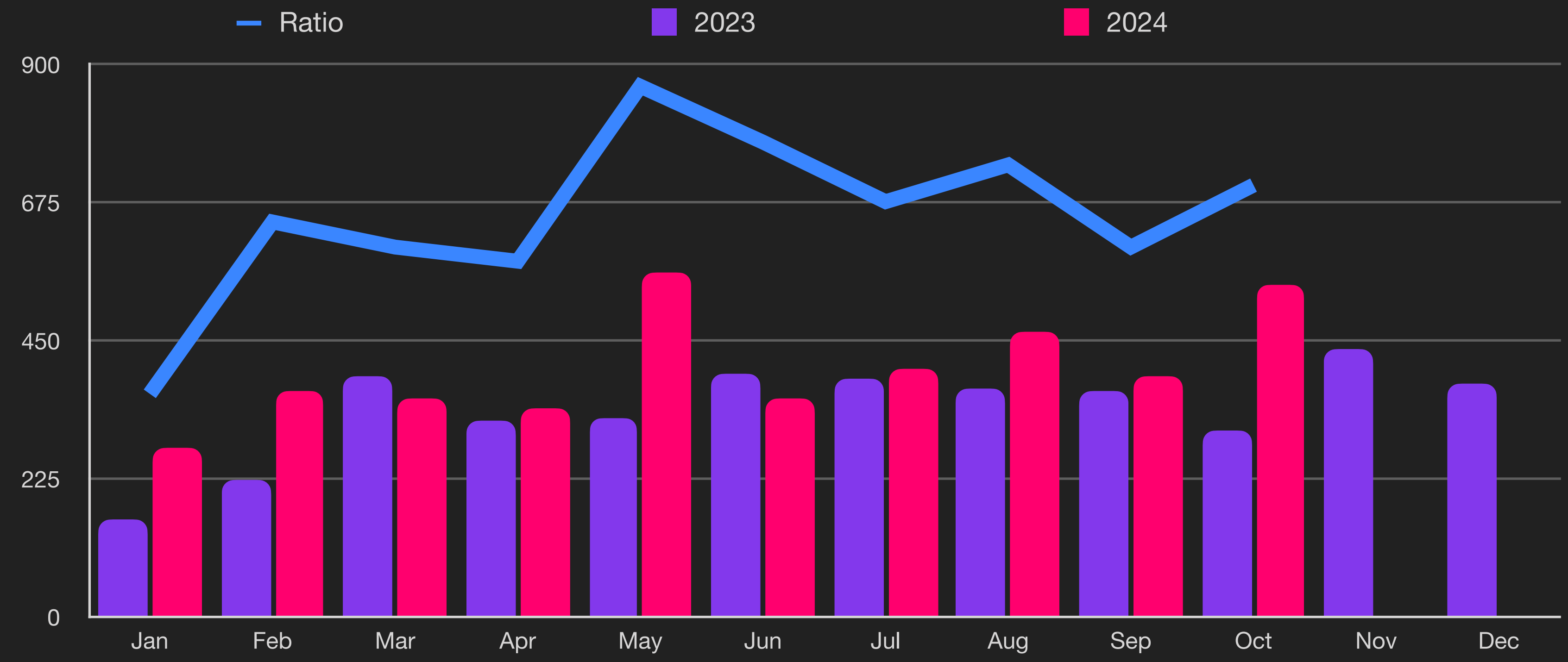
As we saw in September RansomHub dominates the number of successful attacks with a 63% increase over last month as victims begin to disclose unreported attacks from last month. We expect this to continue next month as RansomHub continues to be an effective variant with a 40% increase in unreported attacks during October. This month we also saw Play increase by 19% from the previous month.

China and Russia continue to dominate data exfiltration with 22% and 5% respectively, relying on illegal networks to exfiltrate data to remote servers. Lastly, The average ransomware payout is up 23% from last quarter to $479,237.

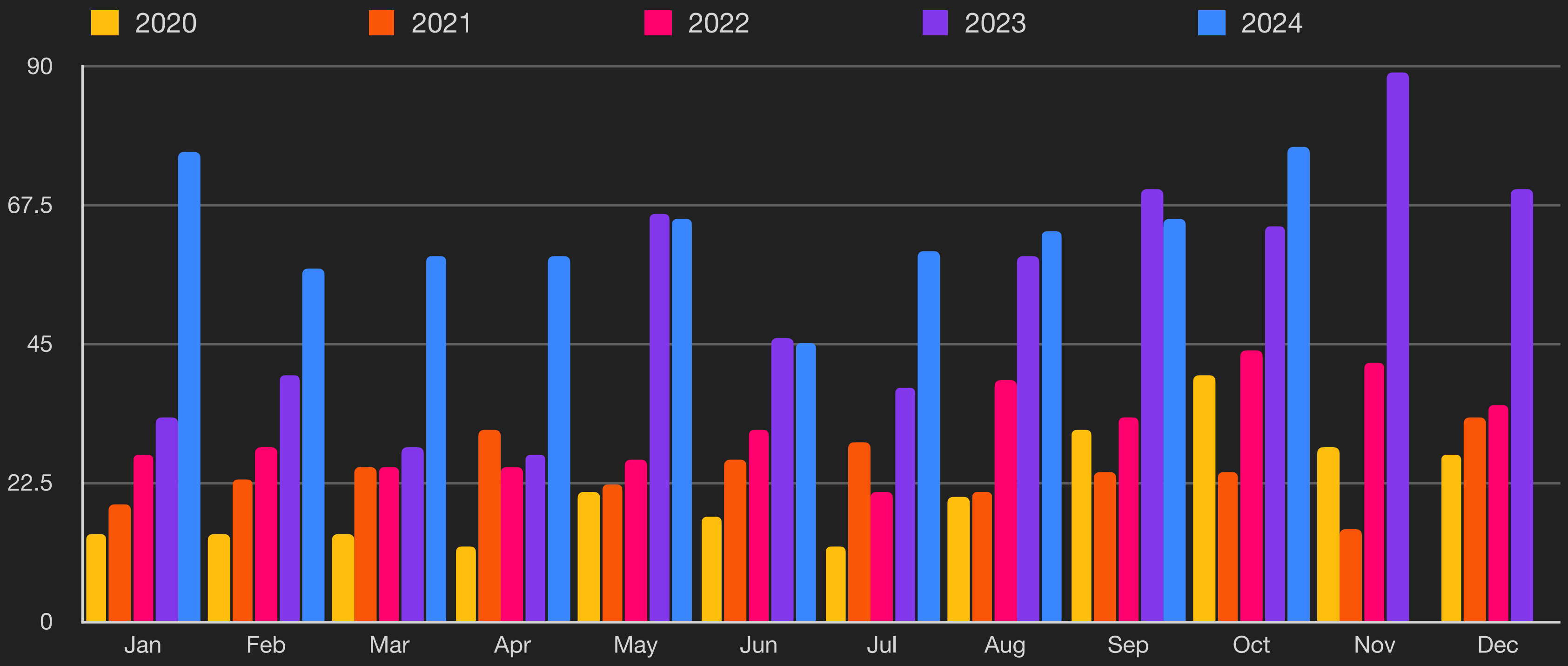
BlackFog State of Ransomware Report

October 2024

Unreported Ransomware Attacks



Reported Ransomware by Month



Key Trends

704% Unreported

1st Highest of Year

58% of all attacks use PowerShell

93% of attacks exfiltrate data

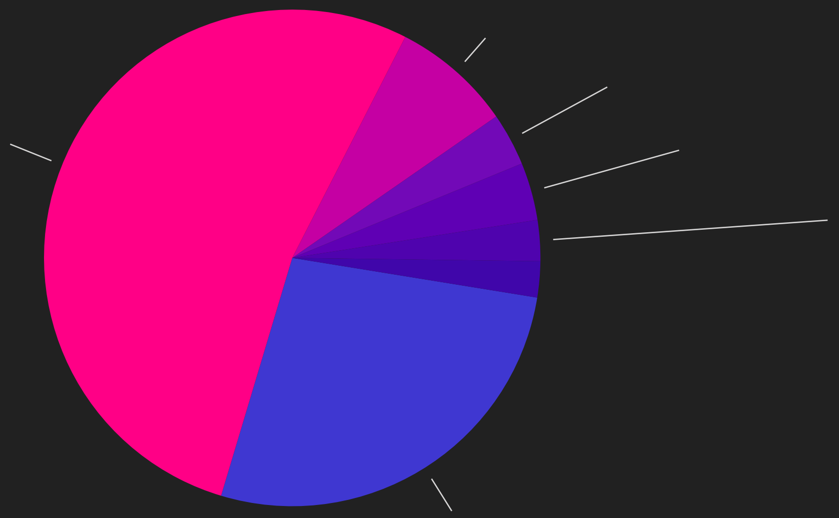
28% of exfiltration victims pay
-15% from Q2/24

Average payout US $479,237
+23% from Q2/24

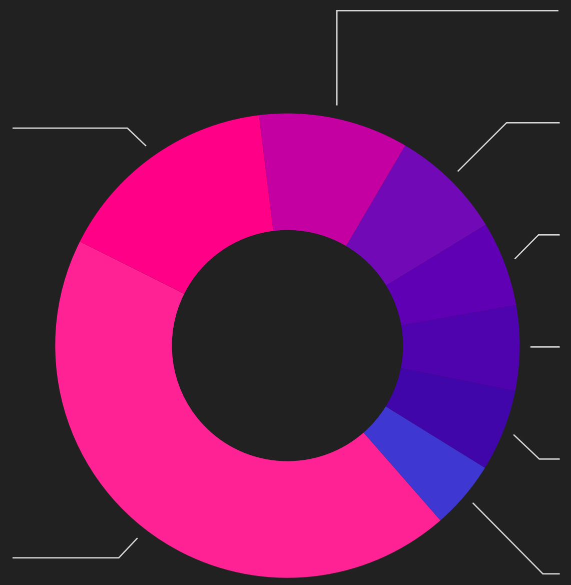
BlackFog State of Ransomware Report

October 2024

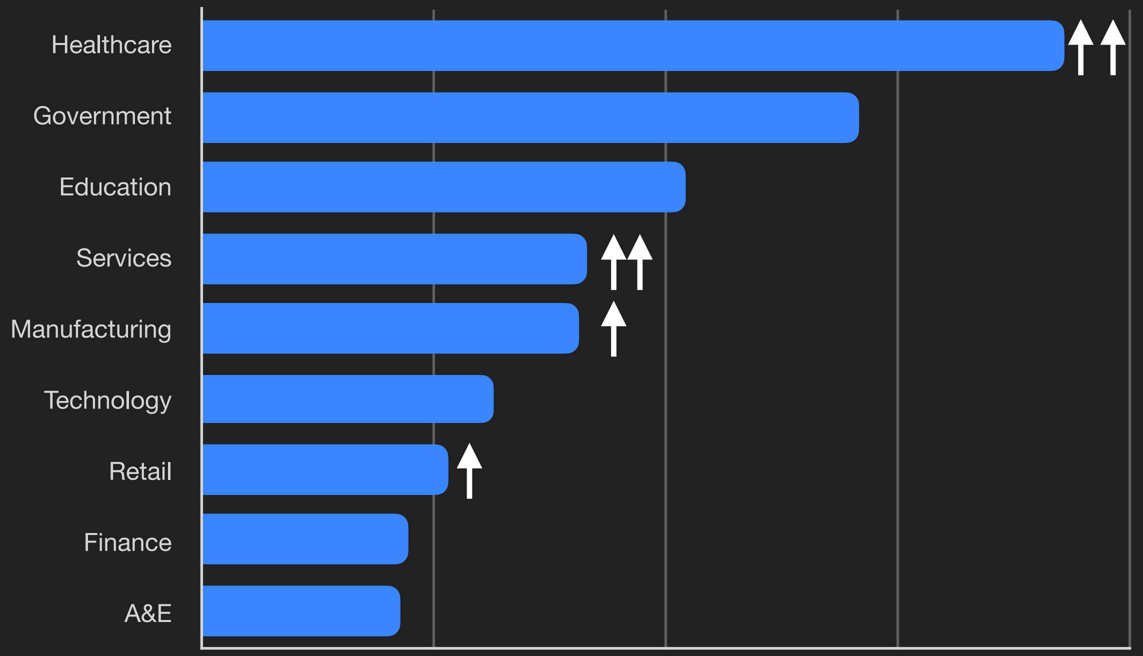
Ransomware by Country



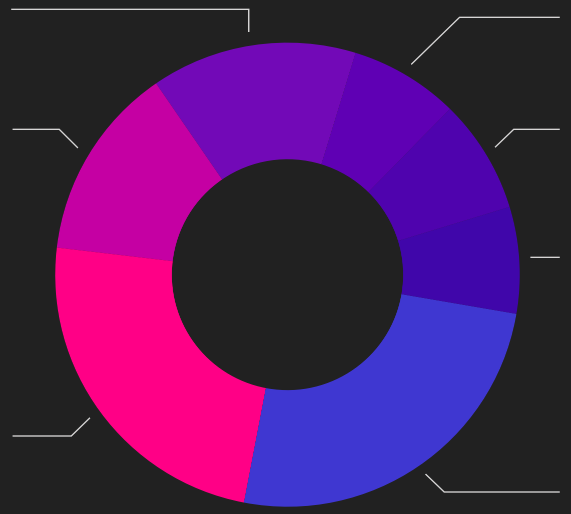
Ransomware Variant (Reported)



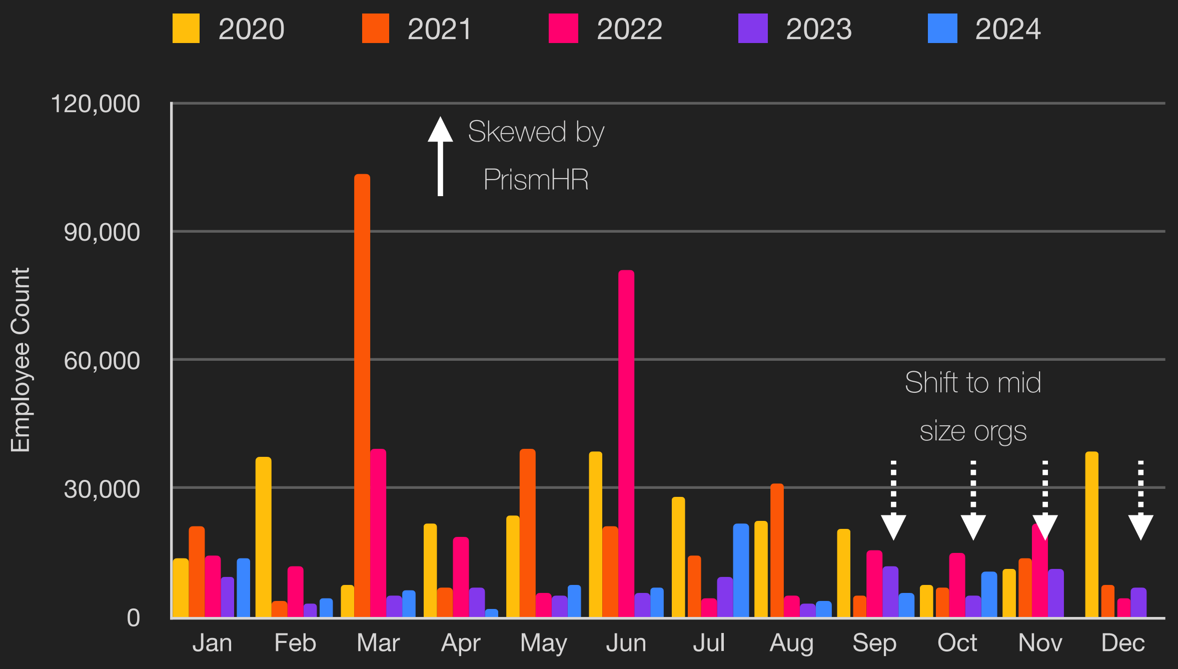
Ransomware by Industry



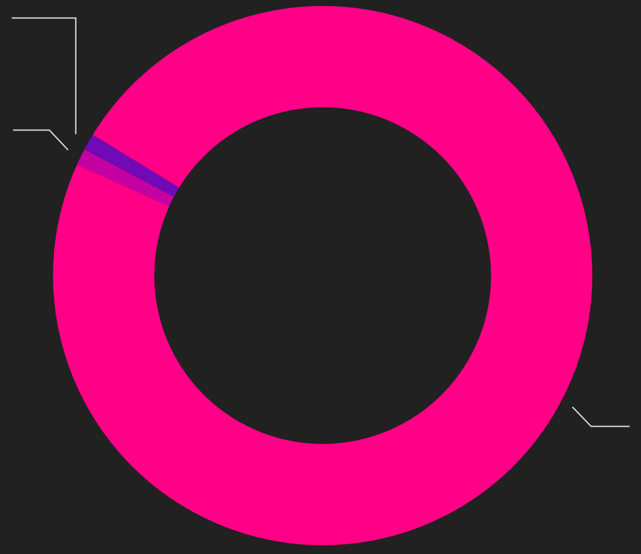
Ransomware Variant (Unreported)



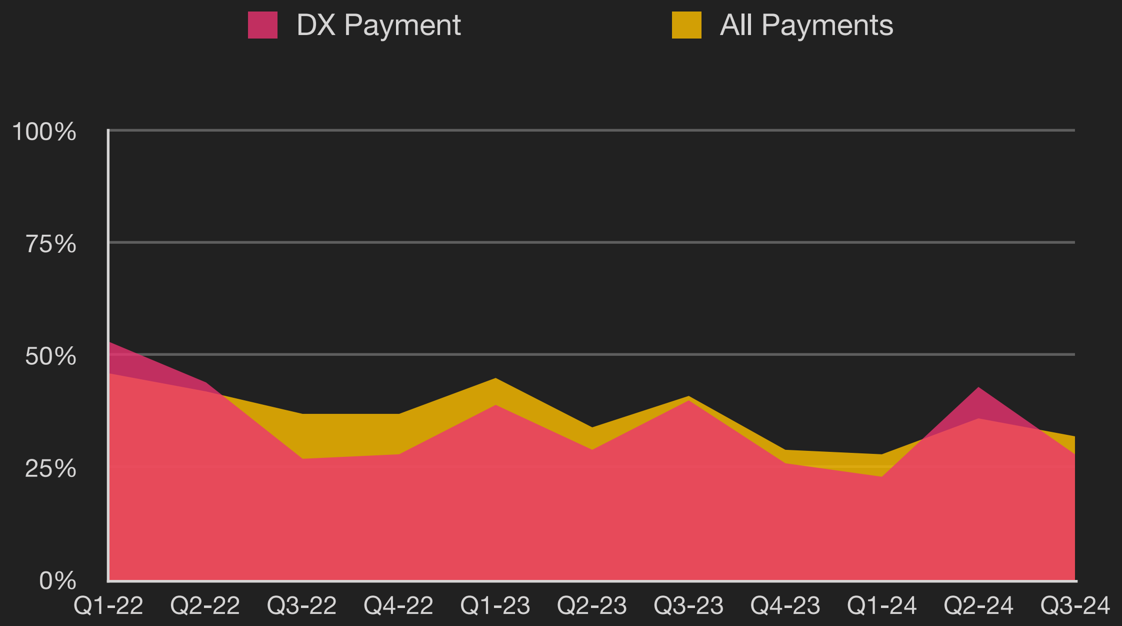
Size of Organization



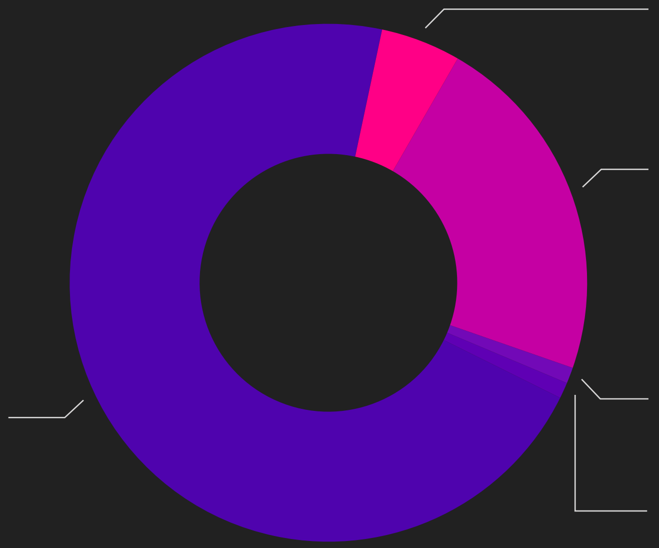
Exfiltration Techniques



Exfiltration Payment Rates[2]



Exfiltration by Country



[2] Courtesy 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.