Introduction

December wrapped up a hectic year for ransomware, with 69 publicly reported attacks. The healthcare, manufacturing, and services sectors each topped the list with 8 attacks, followed closely by retail, government, utilities, and education, which reported 6 incidents each. While 21 attacks still remain unclaimed, 28 different ransomware groups claimed attacks during the month. Key incidents included the suspected breach of Deloitte data, Black Basta's attack on UK telecom giant BT, and CLOP's exploitation of zero-day vulnerabilities in Cleo's software.

Roundup

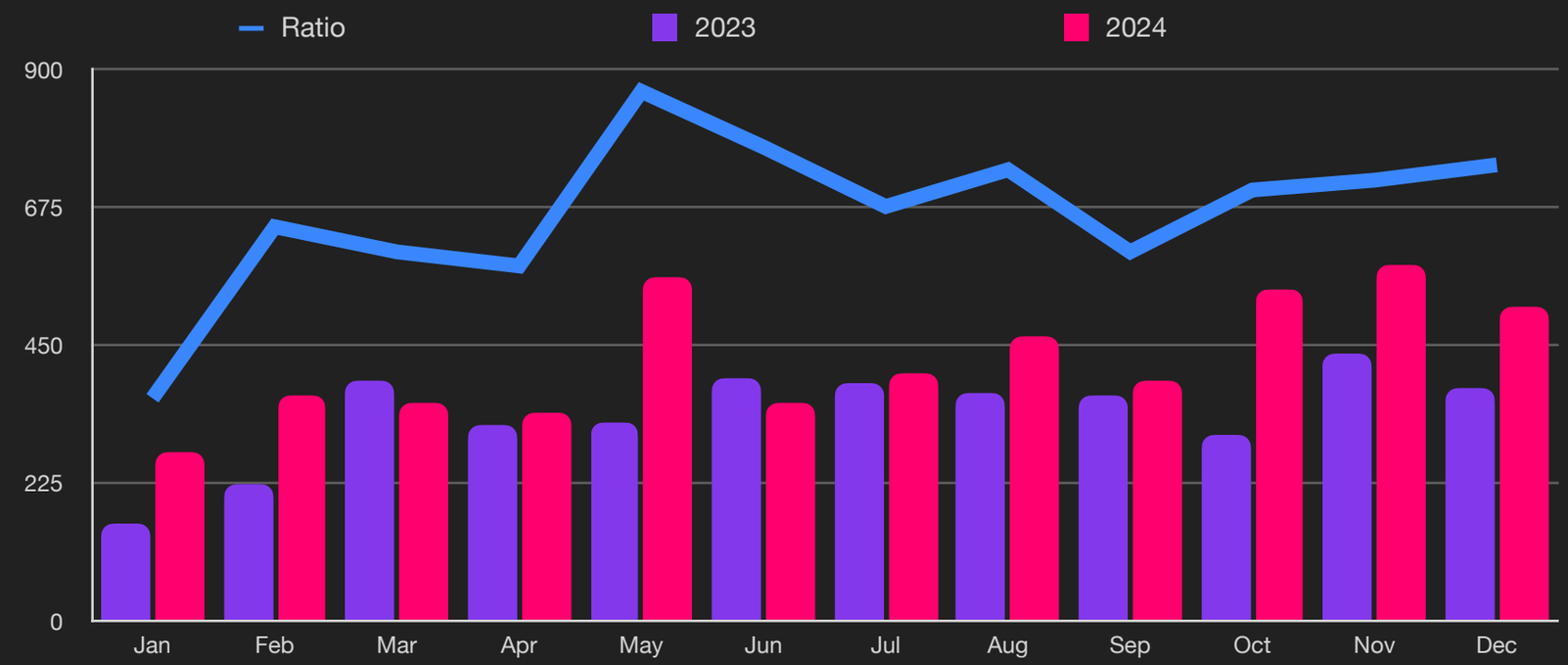
The last month of 2024 finished the year with the 4th highest number of attacks and the second highest December on record. Similarly, we saw a high volume of undisclosed attacks with 514 for the month and a 7.5 to 1 ratio of unreported to reported attacks.

From an industry perspective, Healthcare saw an increase of 13% followed by Services and Manufacturing with increases of 17% and 15% respectively. The most targeted sectors for the year were Healthcare, Government and Education by a significant margin. In fact Healthcare was more than 30% higher than Government and 70% more than education.

As with November the effects of Ransomhub attacks continue to impact reported attacks this month with an increase of 9% and a further 18% increase in unreported attacks. We also saw a large increase in reported attacks from Rhysida (26%) and unreported attacks from Akira (31%).

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.

Unreported Ransomware Attacks



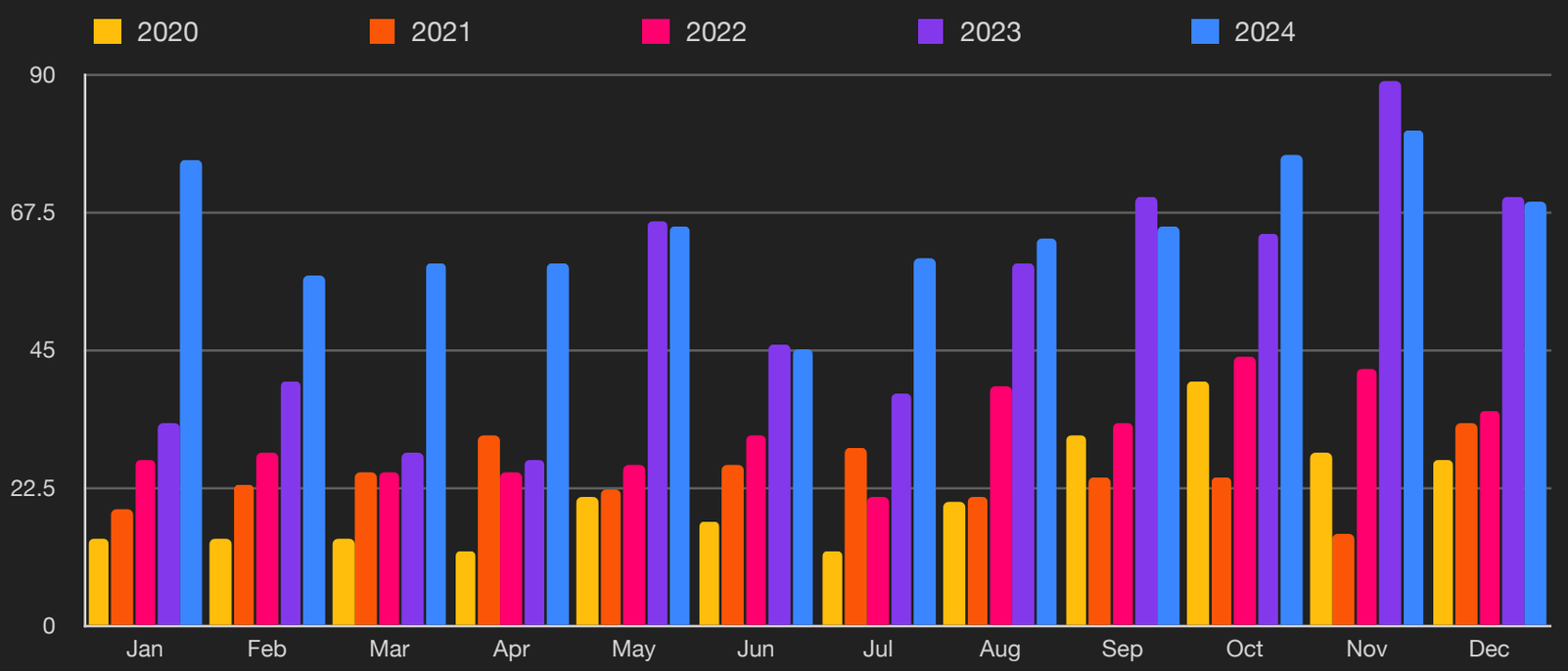
Key Trends

745% Unreported

4th Highest of Year

56% of all attacks use PowerShell

Reported Ransomware by Month



94% of attacks exfiltrate data

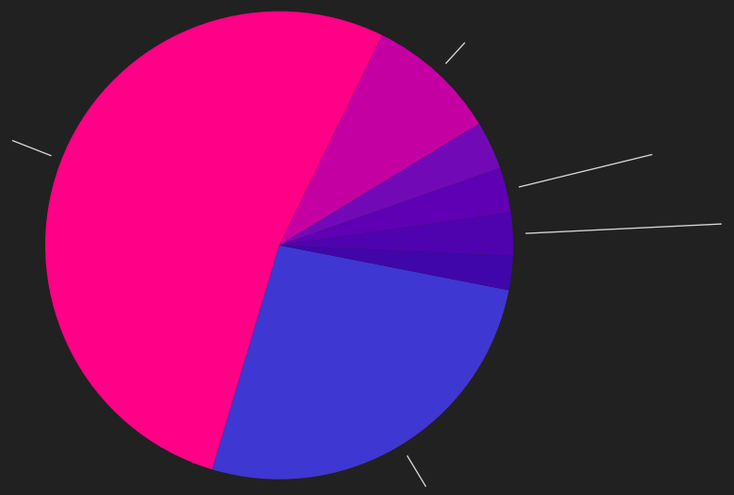
28% of exfiltration victims pay

-15% from Q2/24

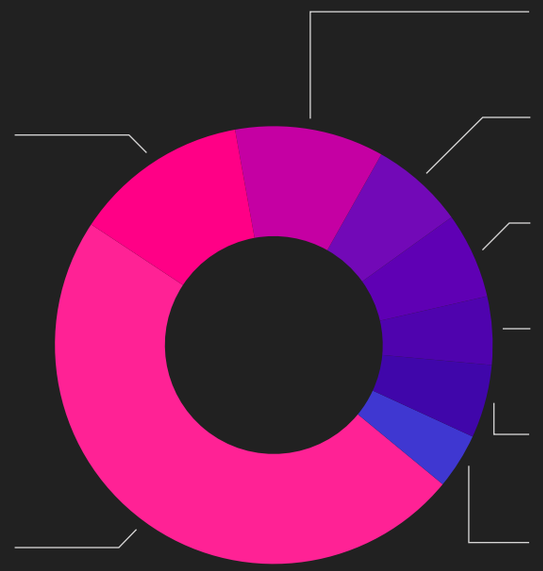
Average payout US $479,237

+23% from Q2/24

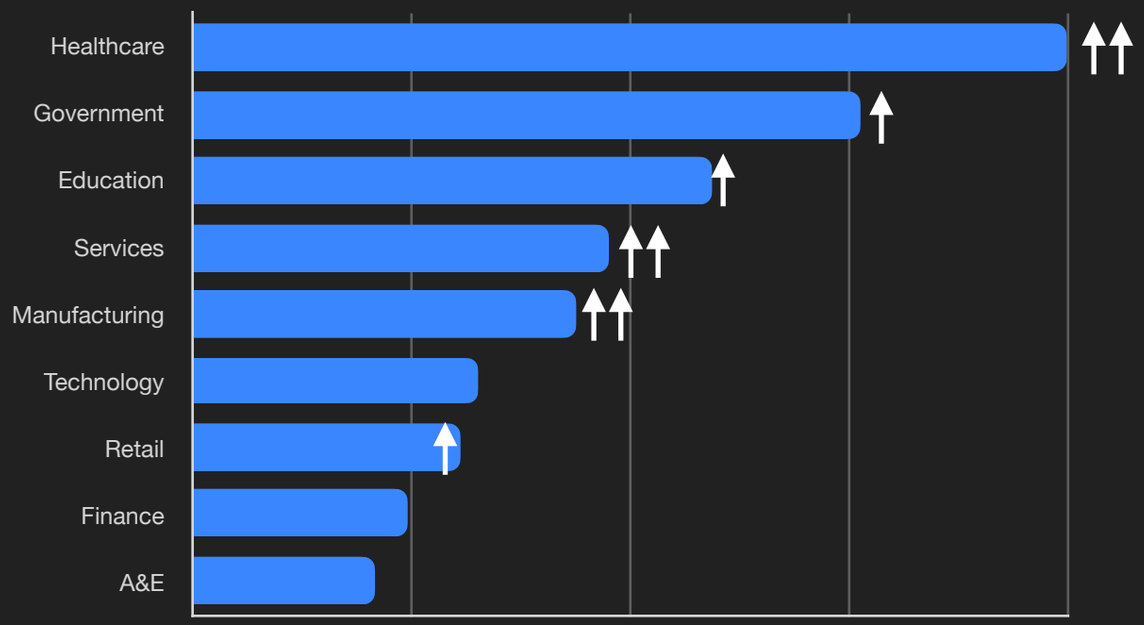
Ransomware by Country



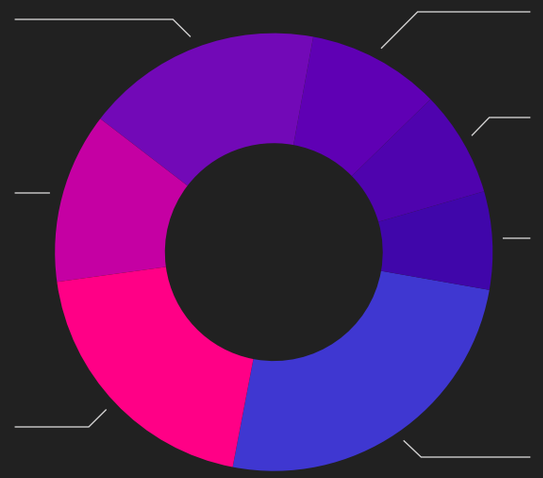
Ransomware Variant (Reported)



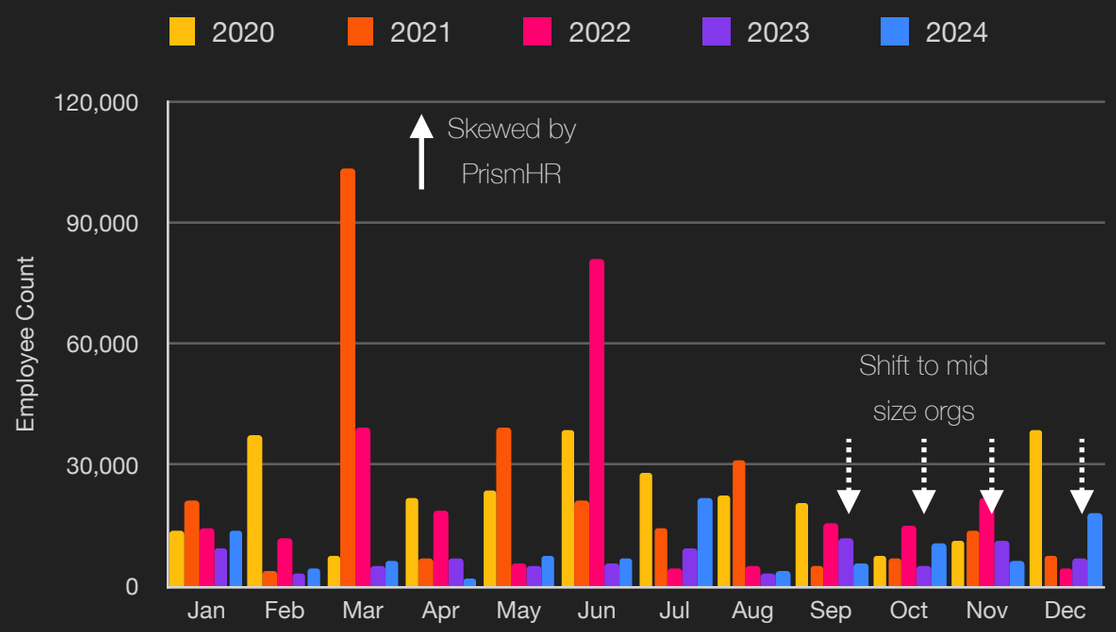
Ransomware by Industry



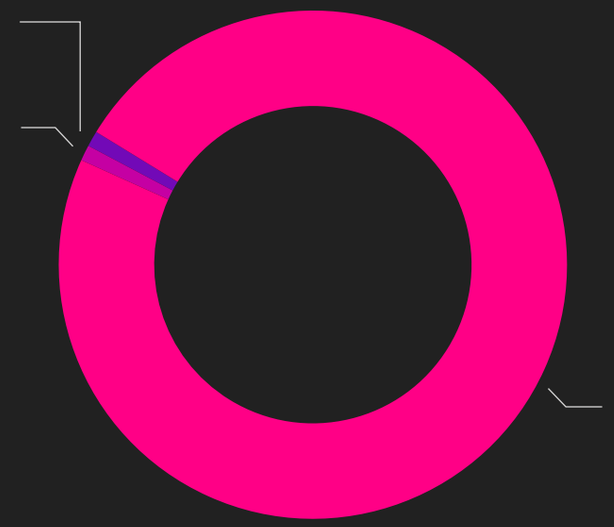
Ransomware Variant (Unreported)



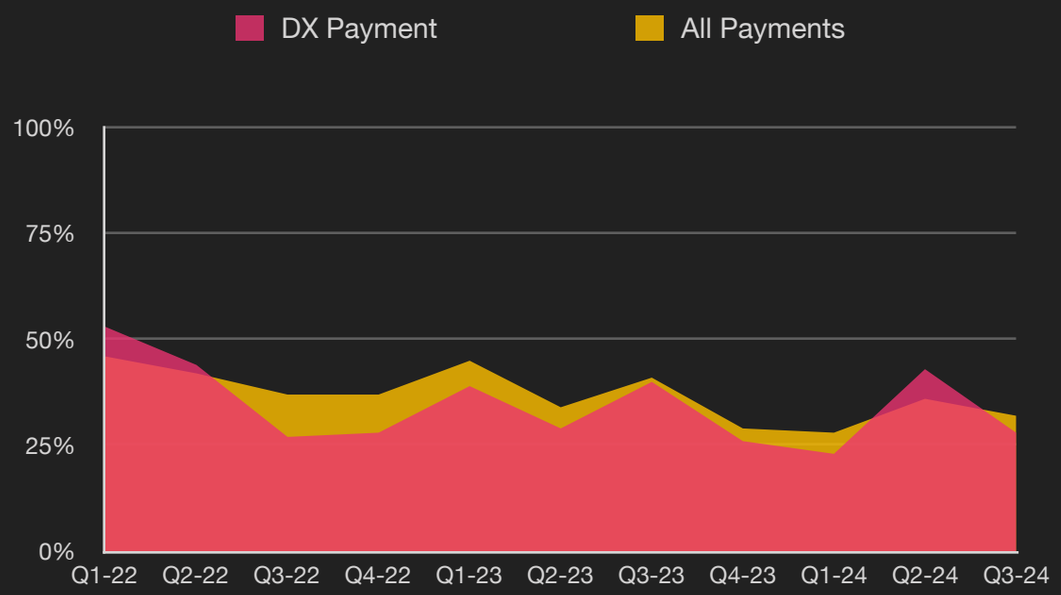
Size of Organization



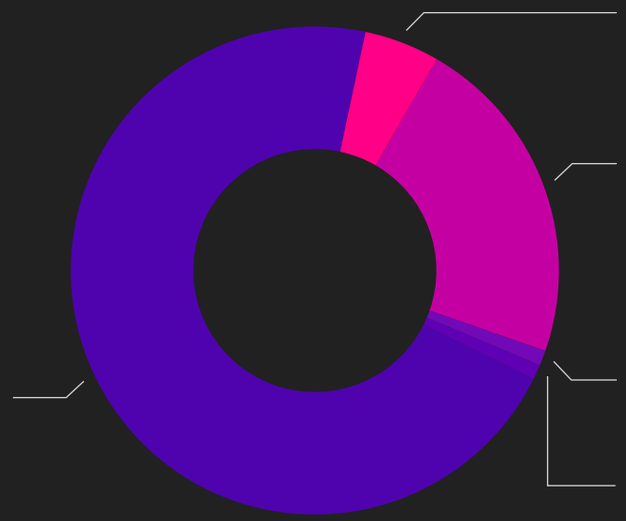
Exfiltration Techniques



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.