BlackFog State of Ransomware Report

November 2024

Introduction

November saw 81 publicly reported ransomware attacks, marking the highest monthly total of the year to date. Government took the brunt of the attacks this month with sixteen recorded in total. RansomHub remained the most active ransomware variant, though notably, new groups emerging in November were responsible for 10% of the incidents. While many attacks captured media attention, one of the most extensively covered was the attack on Blue Yonder, due to the ongoing issues with mega retailers such as Starbucks and Morrisons.

Roundup

As in past years, the holiday season saw an increase in the number of publicly disclosed attacks with a record 81 during the month of November. We also saw a record in the number of undisclosed attacks with a total of 583 for the month, with a ratio of 7.2 to 1 unreported to reported attacks.

From an industry perspective we saw the greatest increase in Education with a a 19% increase followed by Government, Services and Healthcare with increases of 15%, 12% and 8% respectively. Healthcare remains the most targeted sector as we lead into the holidays, closely followed by Government and Education.

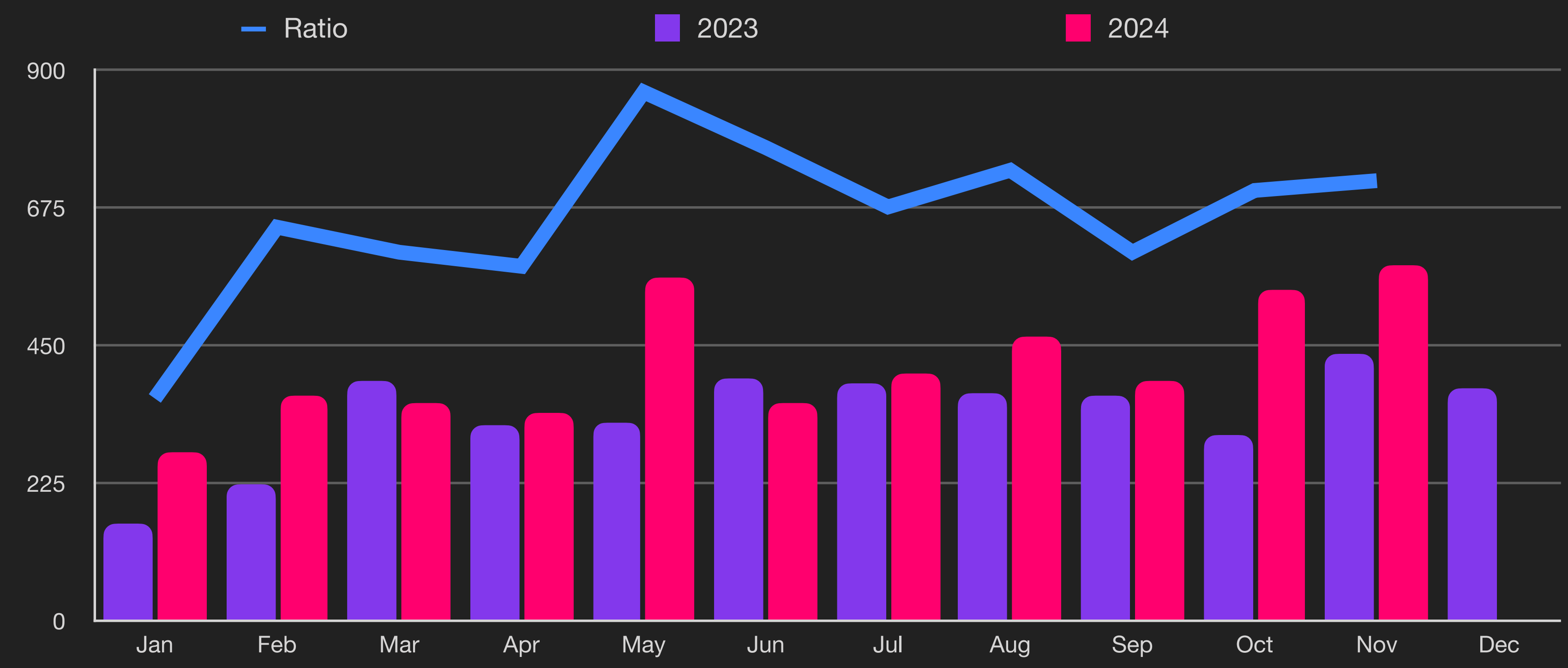
November also saw Ransomhub continue to dominate the number of successful attacks with an increase of 23%, followed by BlackSuit and Medusa with increases of 13% and 9% respectively. This follows a large increase in attacks using RansomHub in September and October. This month we saw a 26% rise in unreported attacks using RansomHub, so we expect this trend will continue.

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.

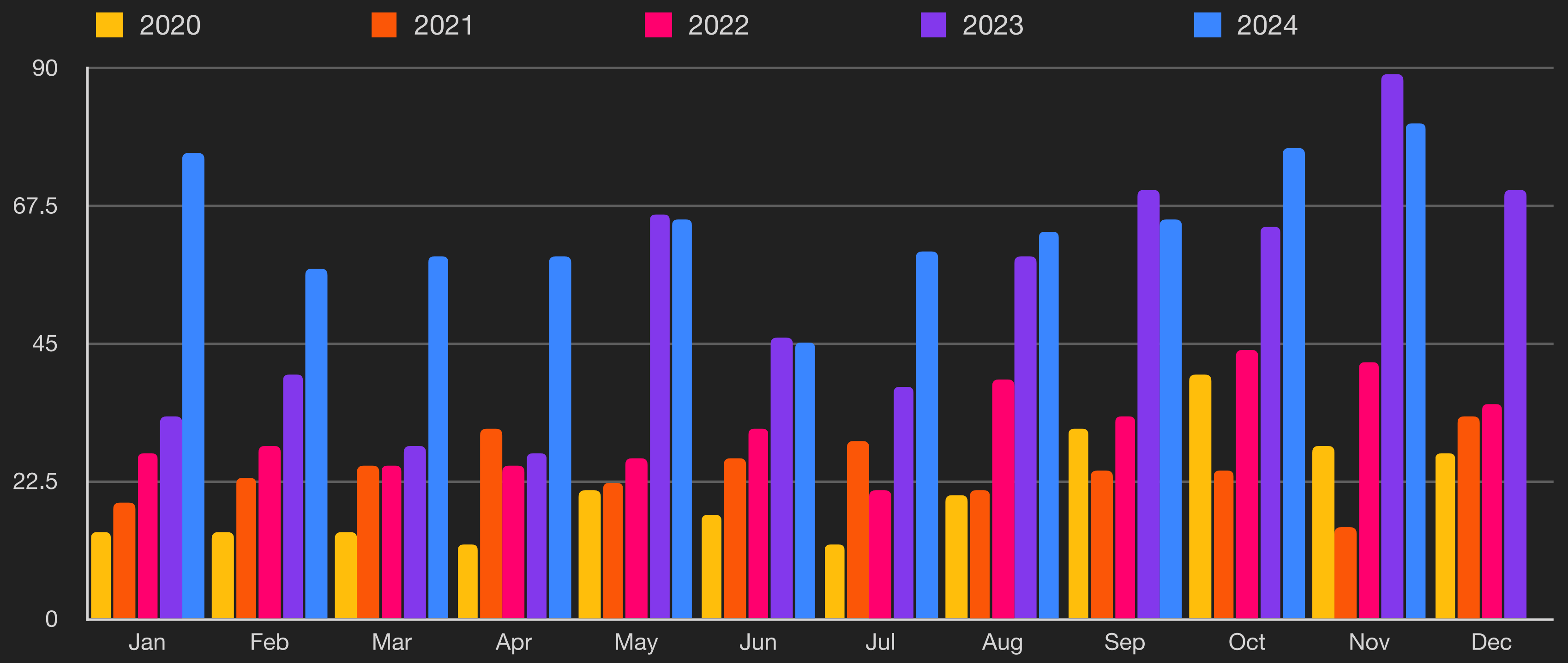
BlackFog State of Ransomware Report

November 2024

Unreported Ransomware Attacks



Reported Ransomware by Month



Key Trends

720% Unreported

1st Highest of Year

57% of all attacks use PowerShell

94% of attacks exfiltrate data

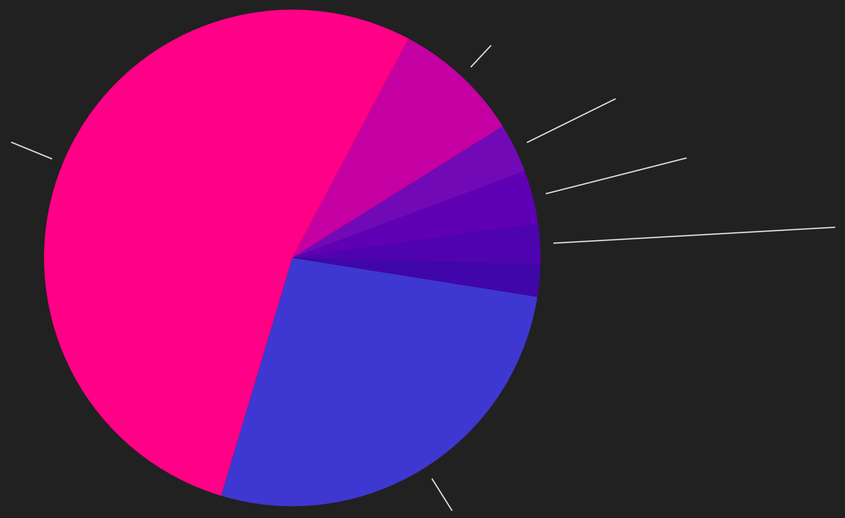
28% of exfiltration victims pay

-15% from Q2/24

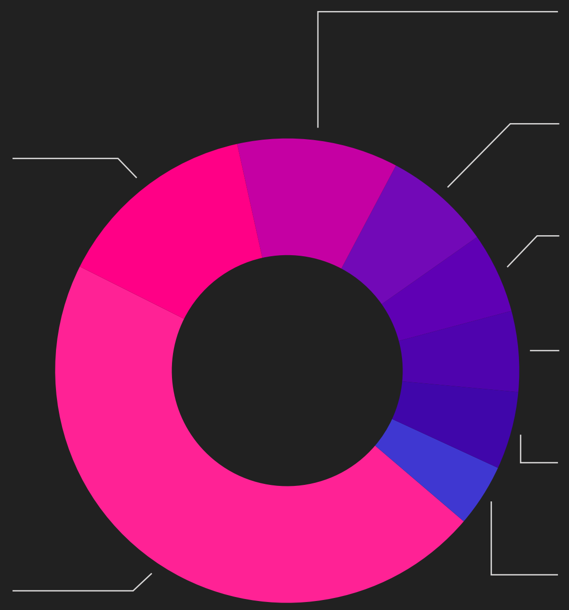
Average payout US $479,237

+23% from Q2/24

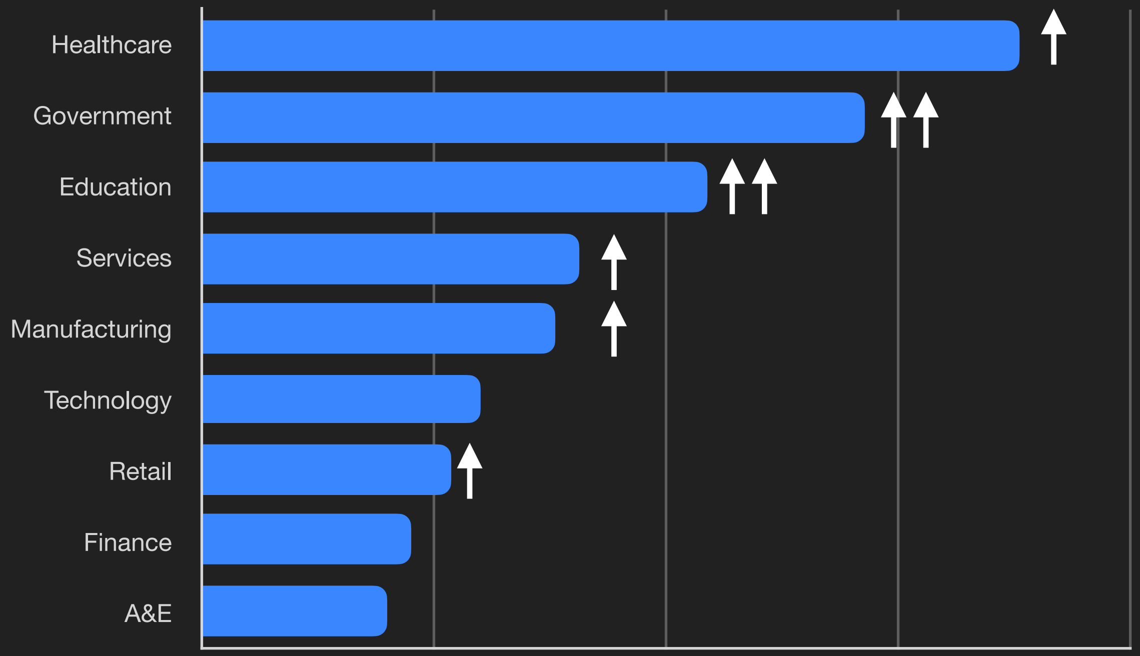
Ransomware by Country



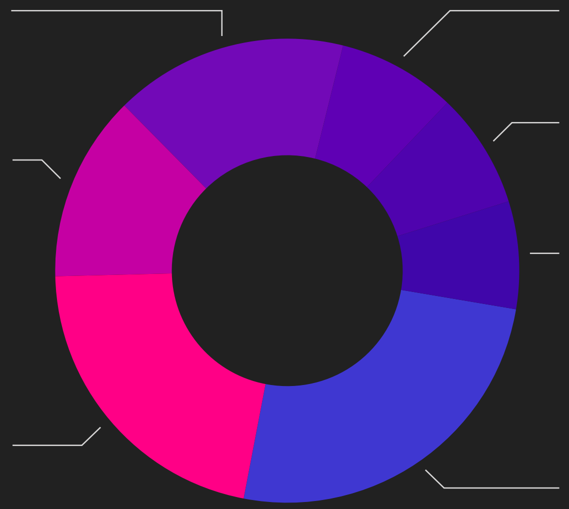
Ransomware Variant (Reported)



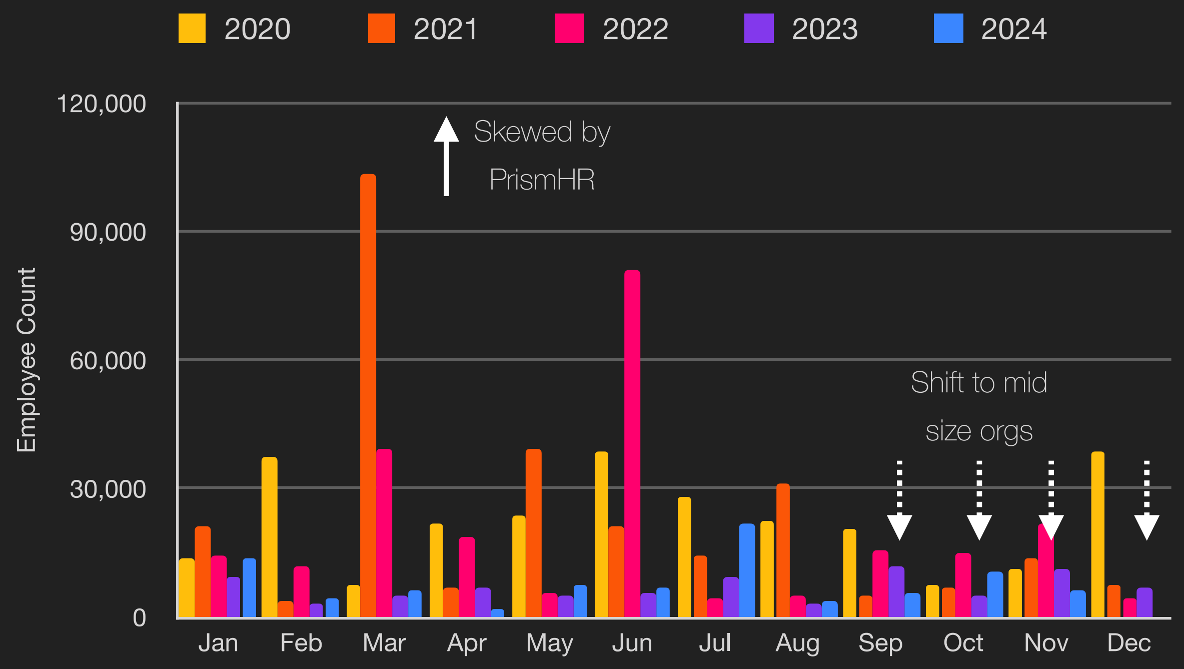
Ransomware by Industry



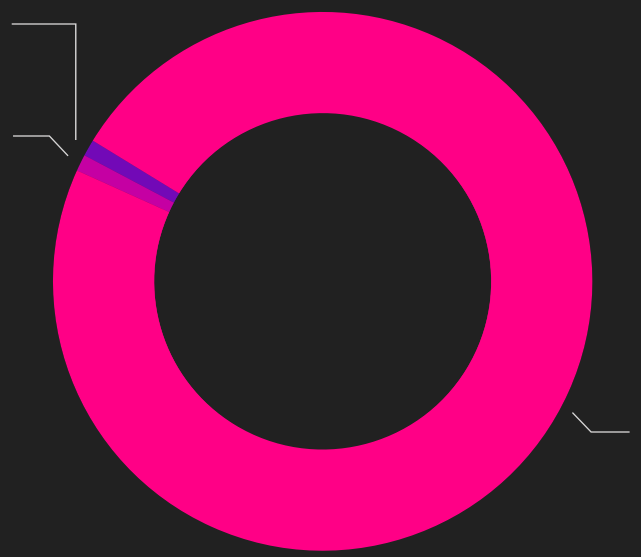
Ransomware Variant (Unreported)



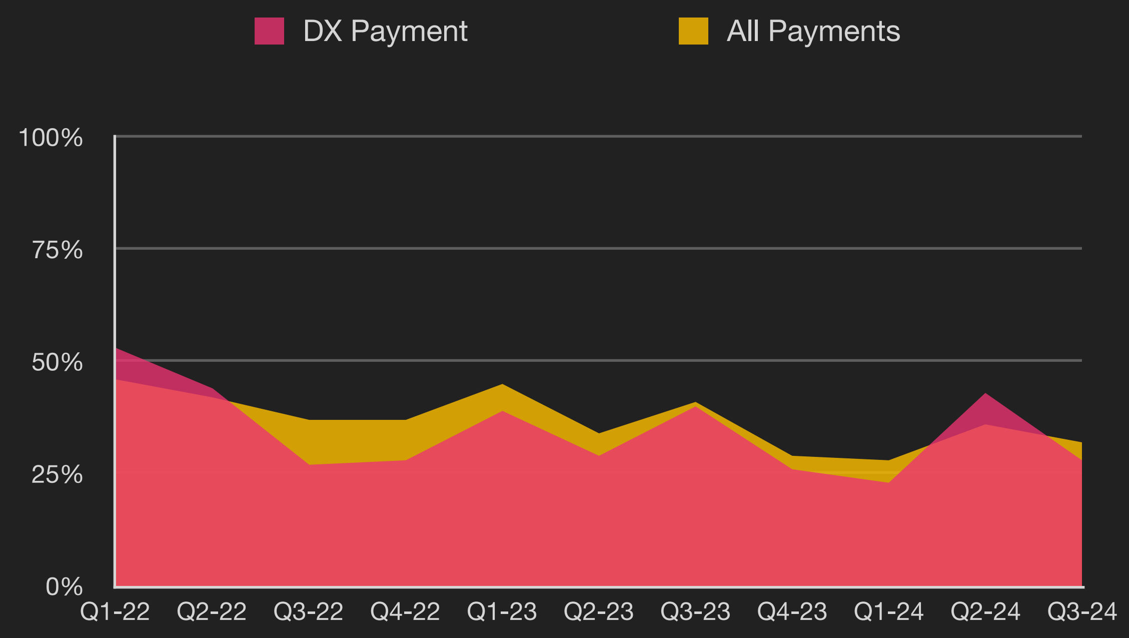
Size of Organization



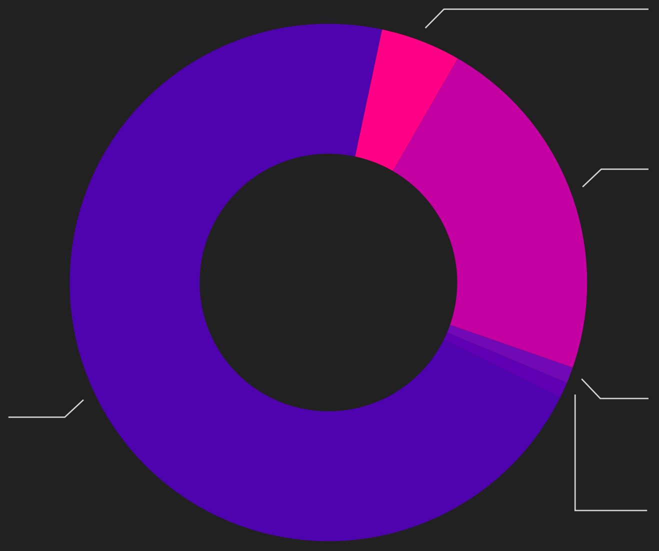
Exfiltration Techniques



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.