

## Introduction

We recorded 65 publicly disclosed attacks in September, making it the joint second highest month of the year so far. Healthcare was the highest targeted vertical, closely followed by education and government. RansomHub led the way claiming 17% of all attacks recorded, making it the second month this variant has been the highest performer. A few large organizations made ransomware news including [Seattle-Tacoma International Airport](#), [Kawasaki Motors](#) and [Kuwait Health Ministry](#).

## Roundup

September saw the second highest number of ransomware attacks of the year with 65 publicly disclosed attacks and 392 undisclosed attacks. This represents a ratio of 6 to 1 undisclosed to disclosed attacks for the month.

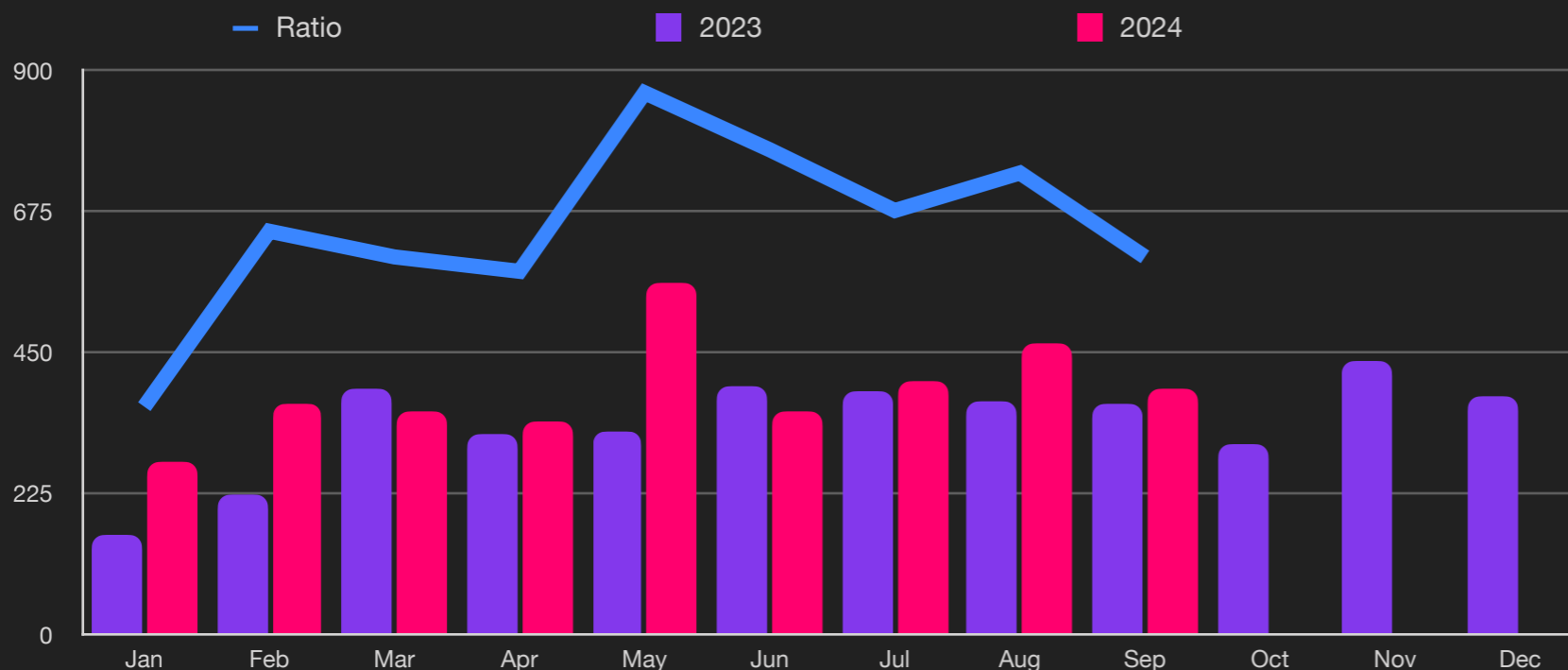
The most dramatic change we saw this month from a sector perspective was the finance sector, seeing a 47% increase in attacks. The sectors of Healthcare, Government and Education continue to lead the way with increases of 13%, 15% and 18% respectively. Healthcare and Government are now more than double every other sector except Education as we move into the 4th quarter.

From a variant perspective we saw the biggest gains with Hunters International group with a 22% increase, followed by Medusa with 16%, reflecting their success across a broad range of sectors. In terms of unreported attacks, we saw a massive increase in attacks from RansomHub, with 53% growth this month, and expect this to be reflected in the reported attacks over the coming months.

China continues to dominate data exfiltration this month, with a 2% increase to 22%, following the 4% increase last month. Russia remains stable at around 5%, with 93% of all attacks involving some form of data exfiltration.



### Unreported Ransomware Attacks



### Key Trends

**603%** Unreported

**2nd** Highest of Year

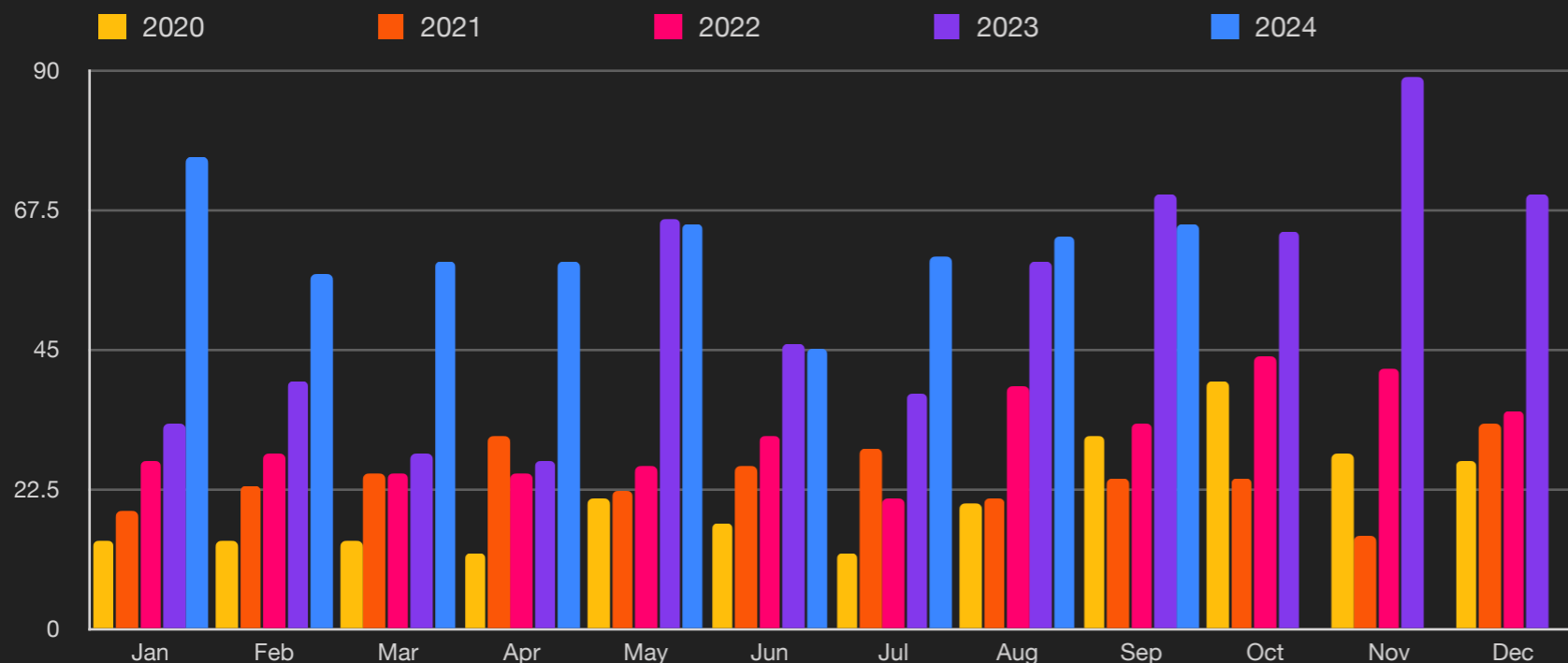
**>** 58% of all attacks use PowerShell

**↑** 93% of attacks exfiltrate data

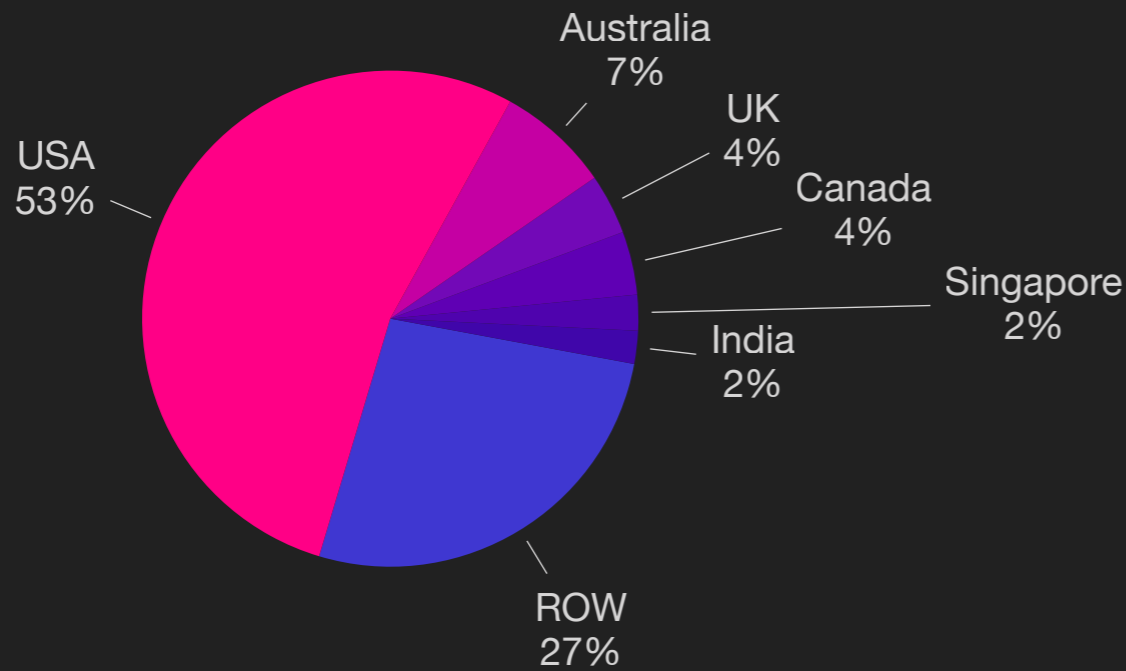
**↑** 43% of exfiltration victims pay vs 36%  
**+20% from Q1/24**

**\$** Average payout US \$391,015  
**+2.4% from Q1/24**

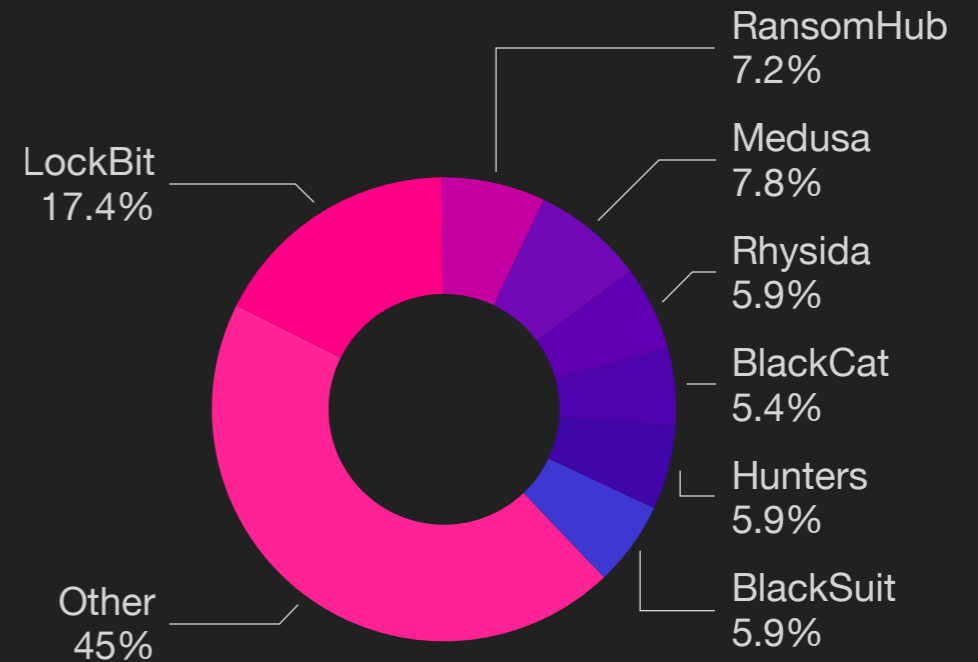
### Reported Ransomware by Month



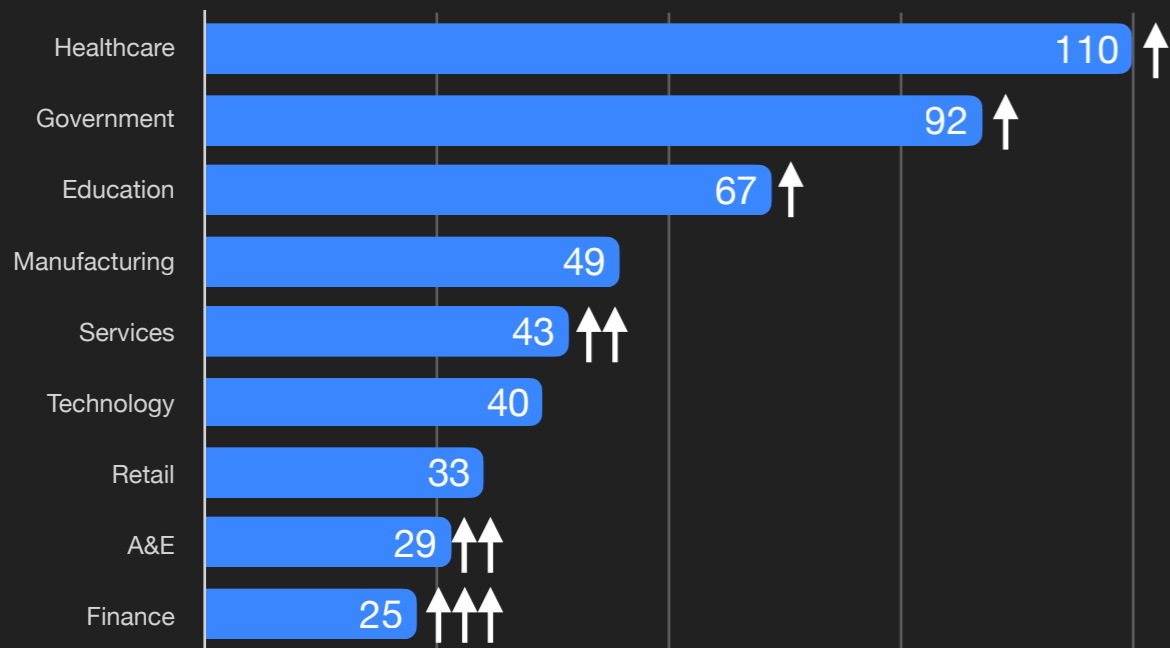
Ransomware by Country



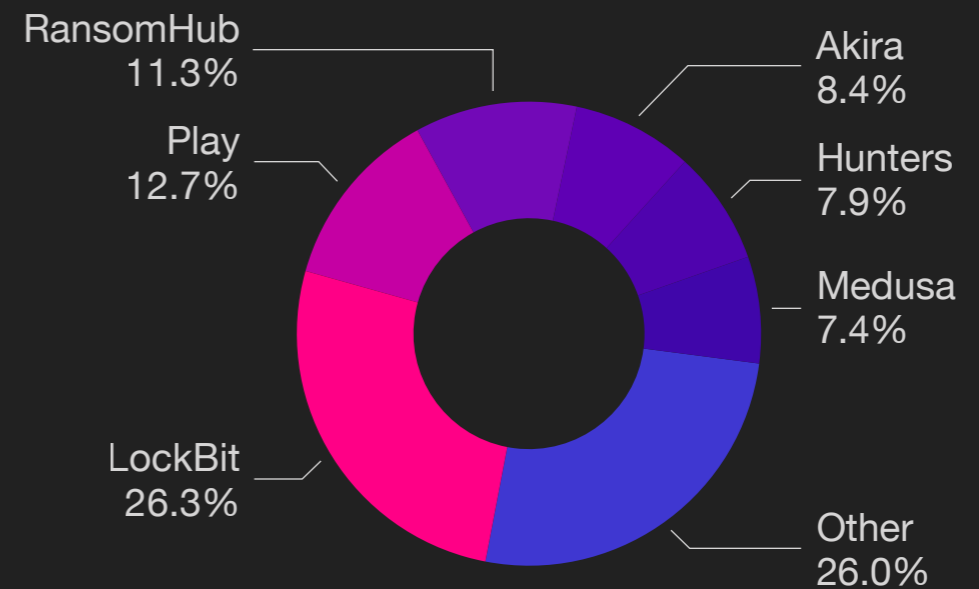
Ransomware Variant (Reported)



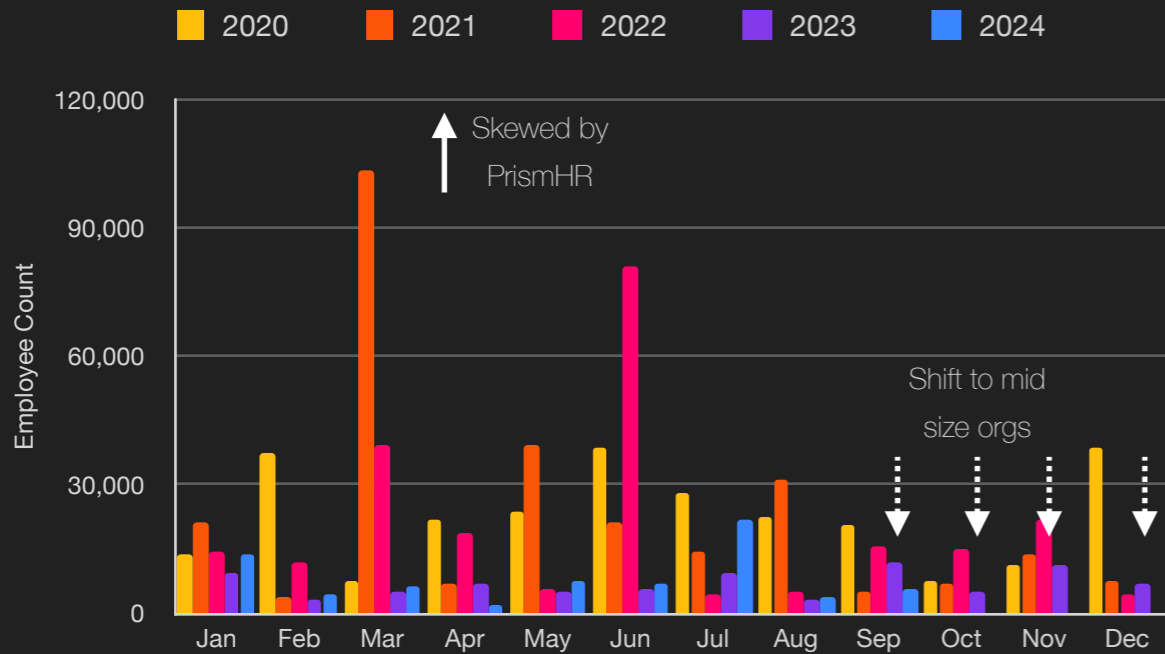
Ransomware by Industry



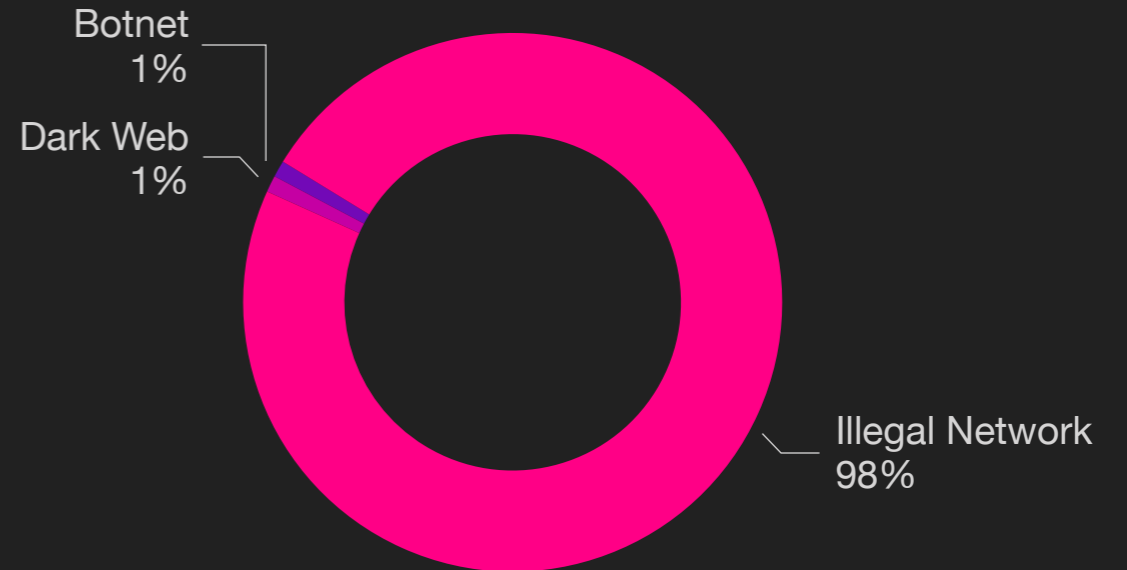
Ransomware Variant (Unreported)



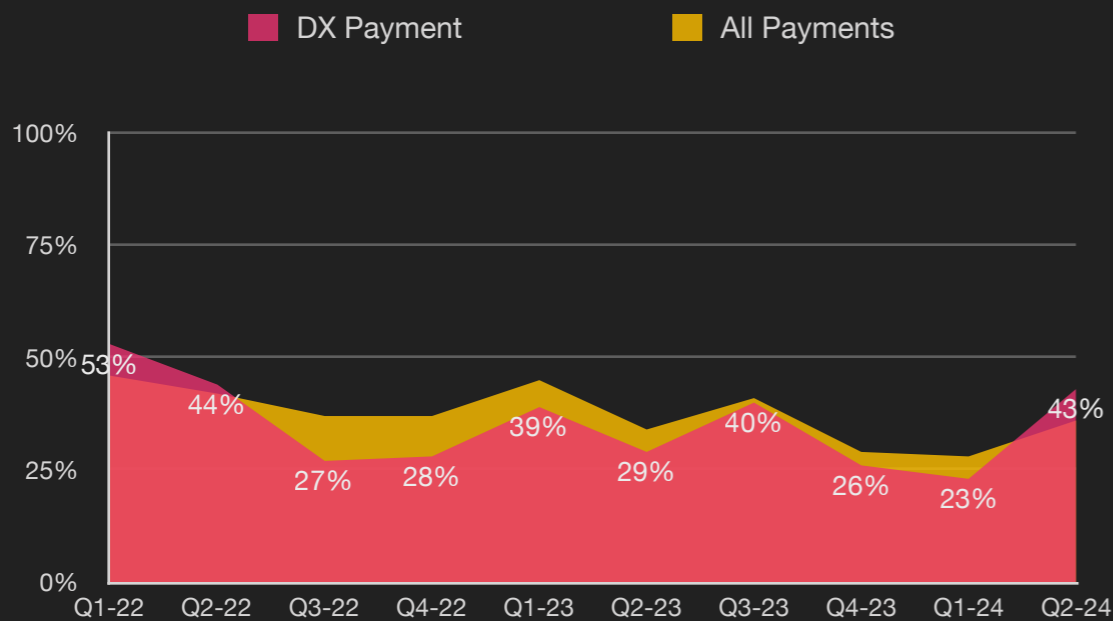
Size of Organization



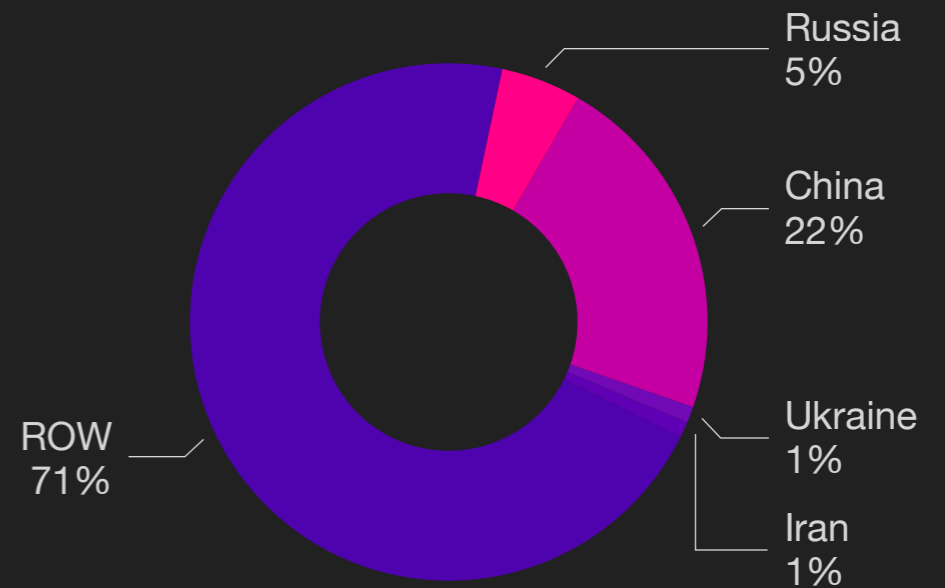
Exfiltration Techniques



Exfiltration Payment Rates<sup>2</sup>



Exfiltration by Country



<sup>2</sup>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.

