

## April 2023

April was the quietest month for reported ransomware attacks this year with 27 incidents making the news, up from 25 in the previous year. Data giant Western Digital was held to ransom by the BlackCat criminal gang who extorted them for an 8 figure sum. While luxury German shipbuilder Lüerssen suffered an attack over the Easter break which reportedly caused much of the firm's operations to come to a standstill as a result.

## Roundup

Vendors within the security industry have recently reported a decreasing number of ransomware attacks. This is NOT a trend we are seeing. In fact, we continue to see a large volume of attacks consistent with previous months and the continued trend of under reporting.

Our data comes from many sources including the dark web and victims own public statements. Attacks are still at historically high levels since we began recording attacks 4 years ago. As we have also noted, unreported attacks continue to escalate and there is often considerable lag time between an attack and disclosure. There is also a growing trend by organizations to delay, and even cover up breaches due to the stigma associated with an attack.

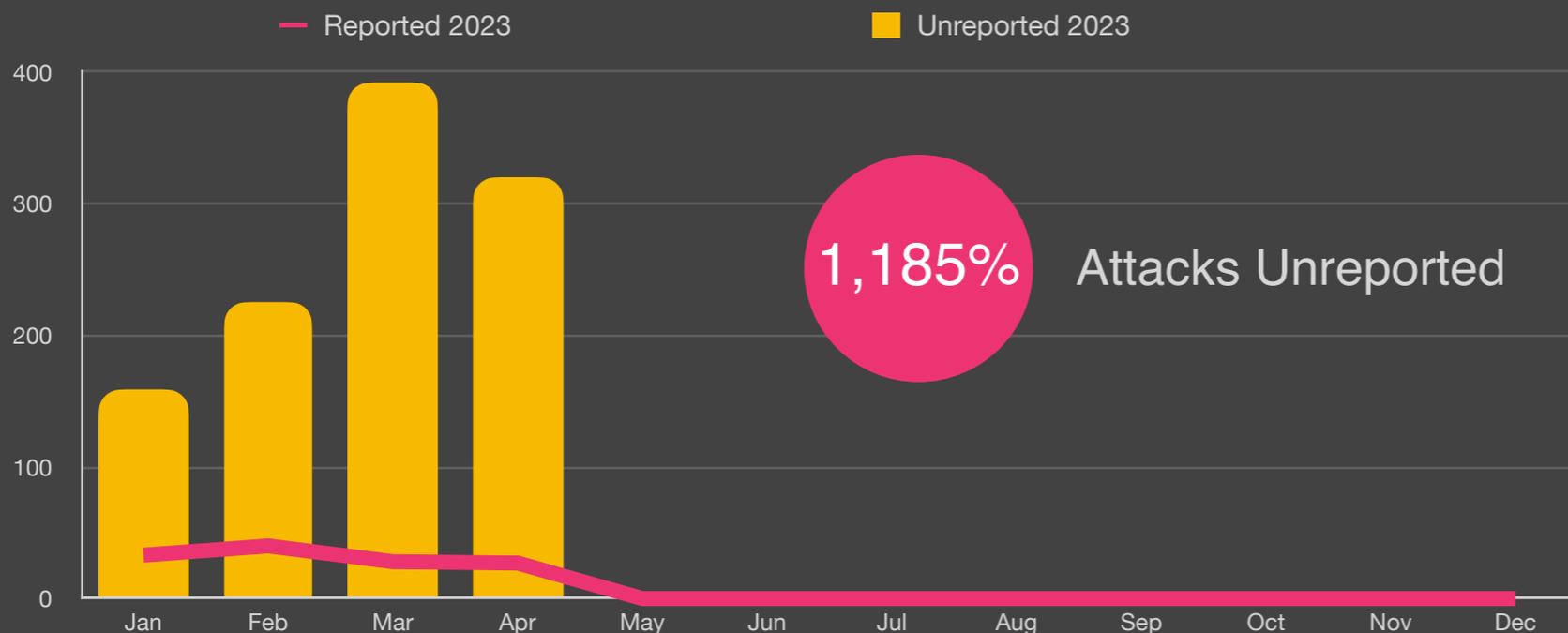
In April we saw continued growth in education, government and healthcare of 19%, 20% and 24% respectively, with the tech sector seeing the biggest growth of 40% this month. Unreported attacks are now 10 times those of reported.

From a variant perspective we see that Lockbit continues to dominate with 20% of reported and 41% of unreported and is by far the dominant player right now. This month we have also seen a high volume of attacks from Bast News as it continues to have success exfiltrating data.

Lastly, we see that exfiltration is now involved in 89% of all attacks with more than 41% going to China and 10% to Russia.



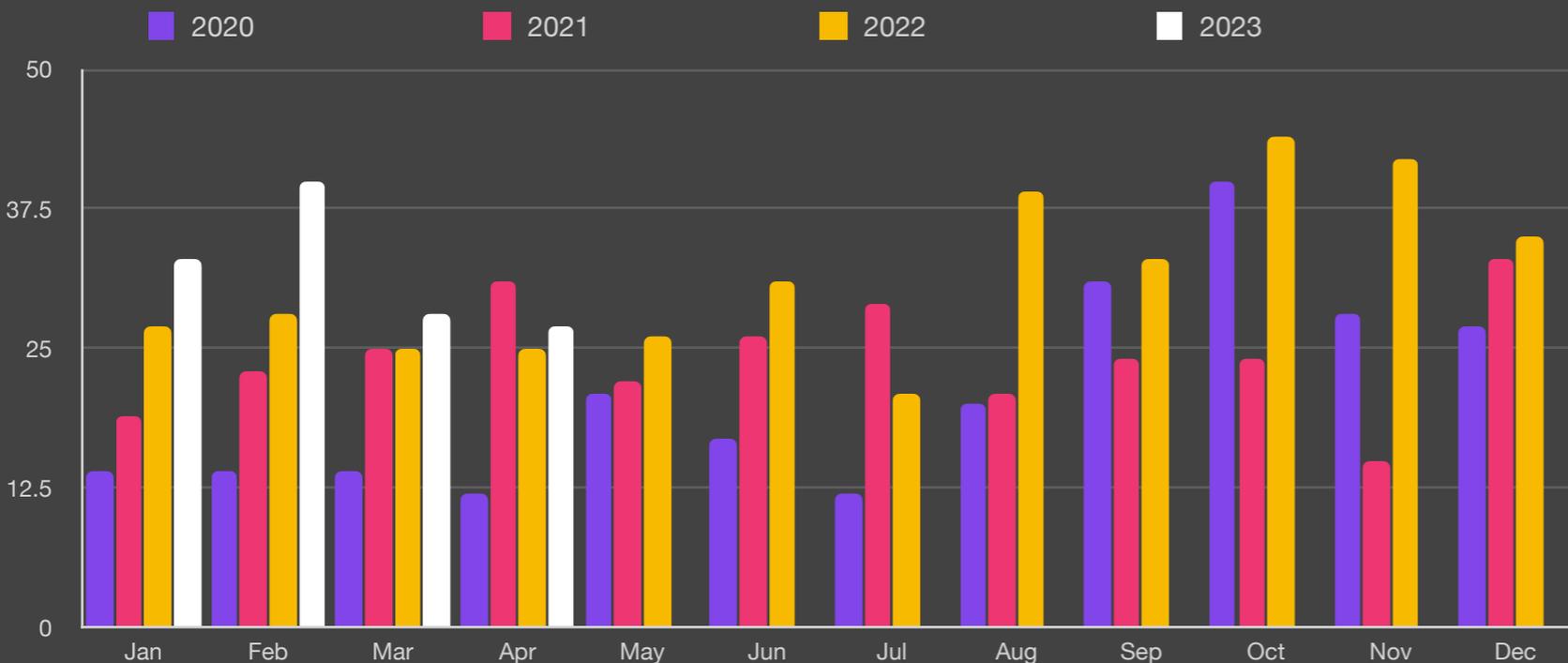
### Unreported Ransom Attacks



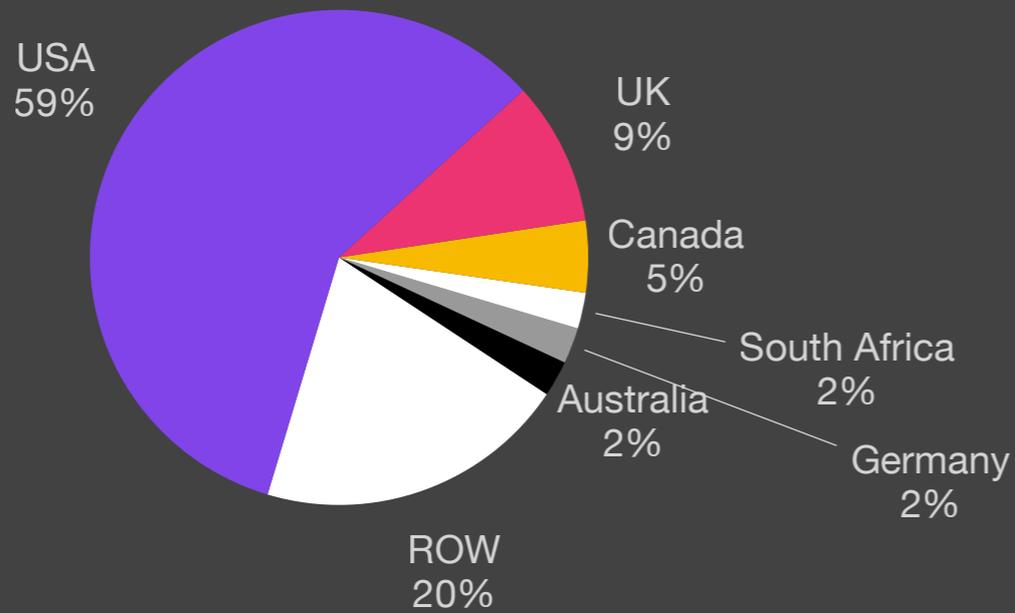
### Key Trends

- 1,185%** Unreported
- Apr** 2nd Highest in 4 years
- +8%** Over 2022
-  76% of all attacks use PowerShell
-  89% of attacks exfiltrate data
-  Average payout US \$327,883k  
-20% from Q4/22

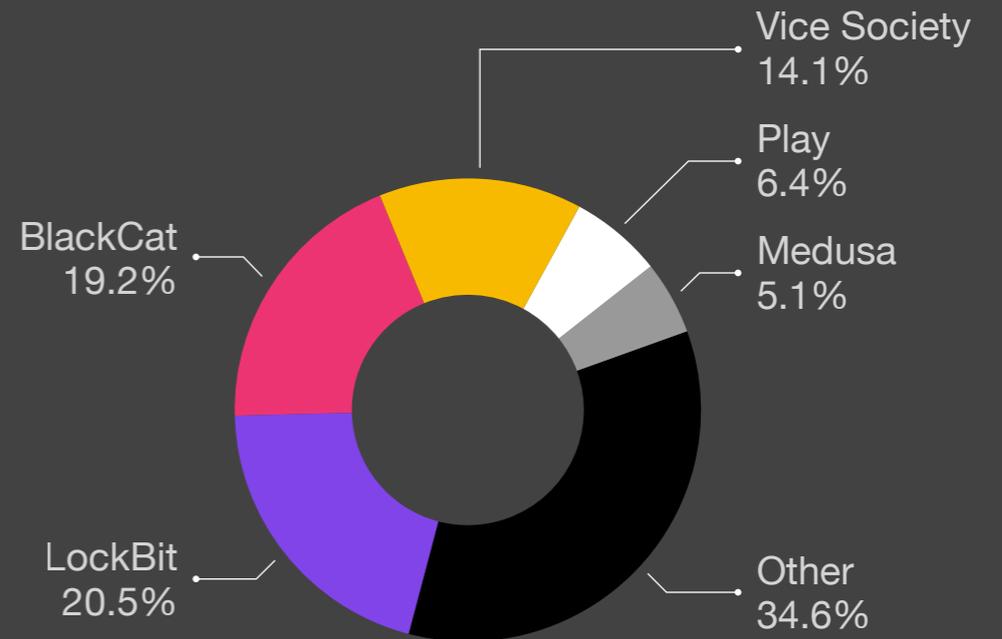
### Reported Ransomware by Month



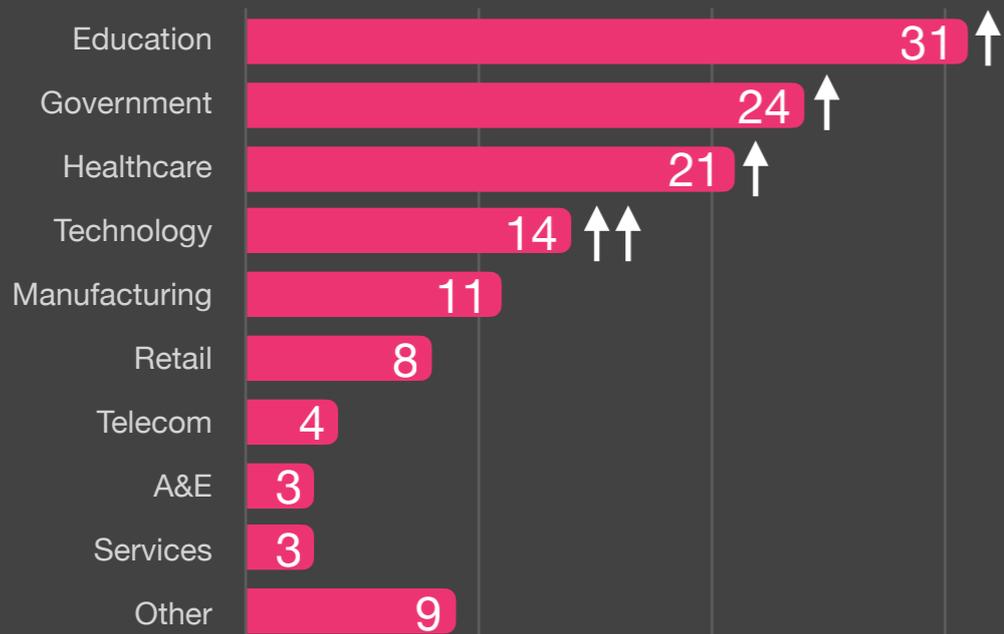
Ransomware by Country



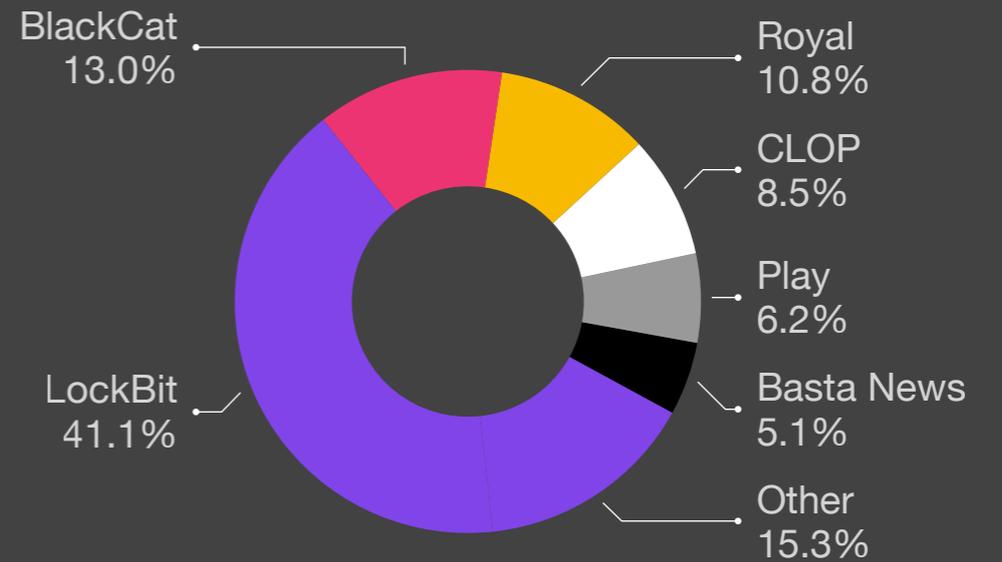
Reported Ransomware Variant



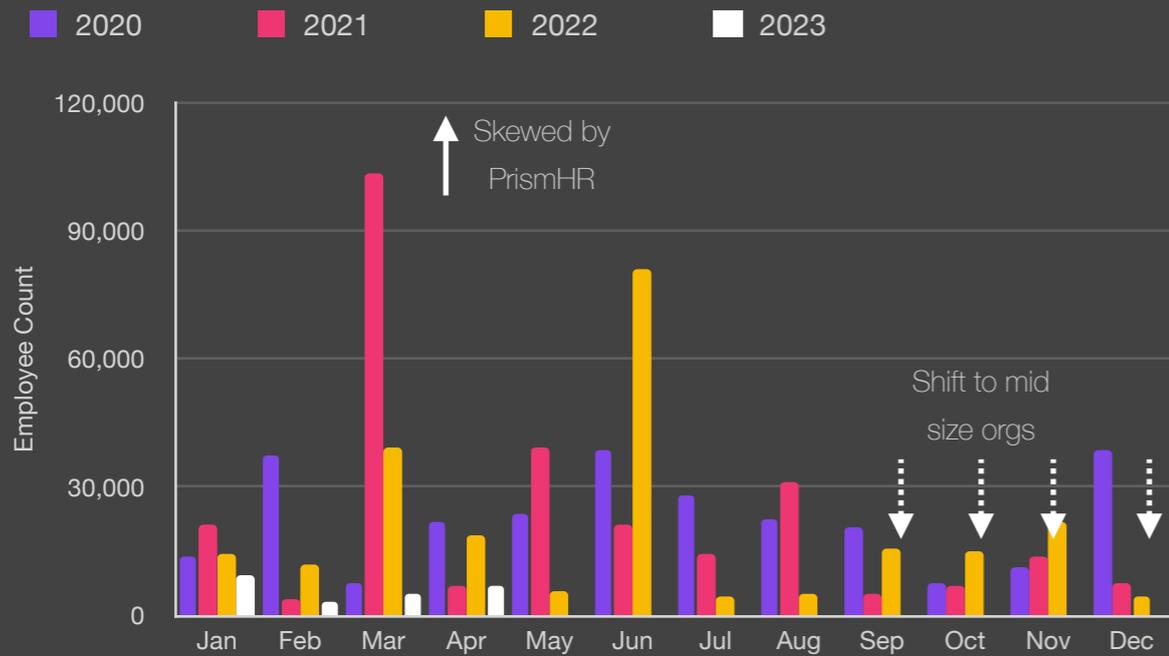
Ransomware by Industry



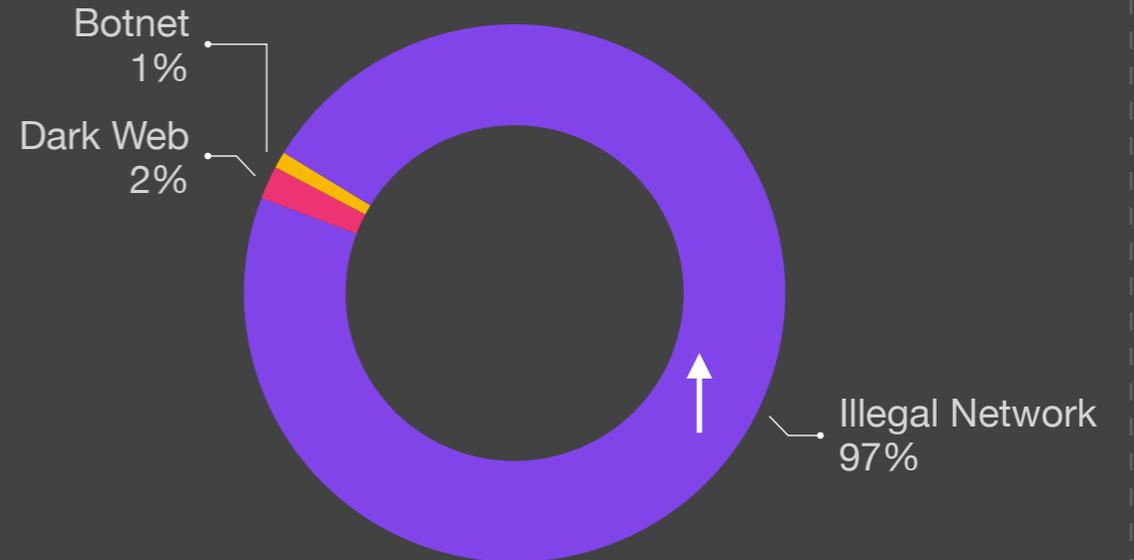
Unreported Ransomware Variant



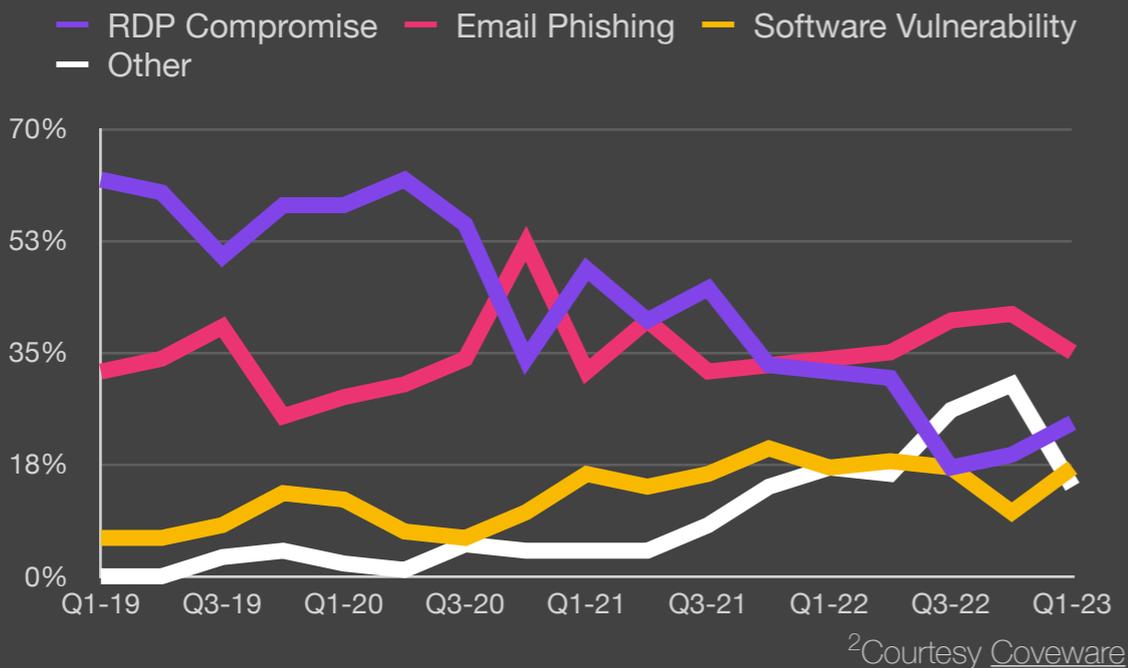
### Size of Organization



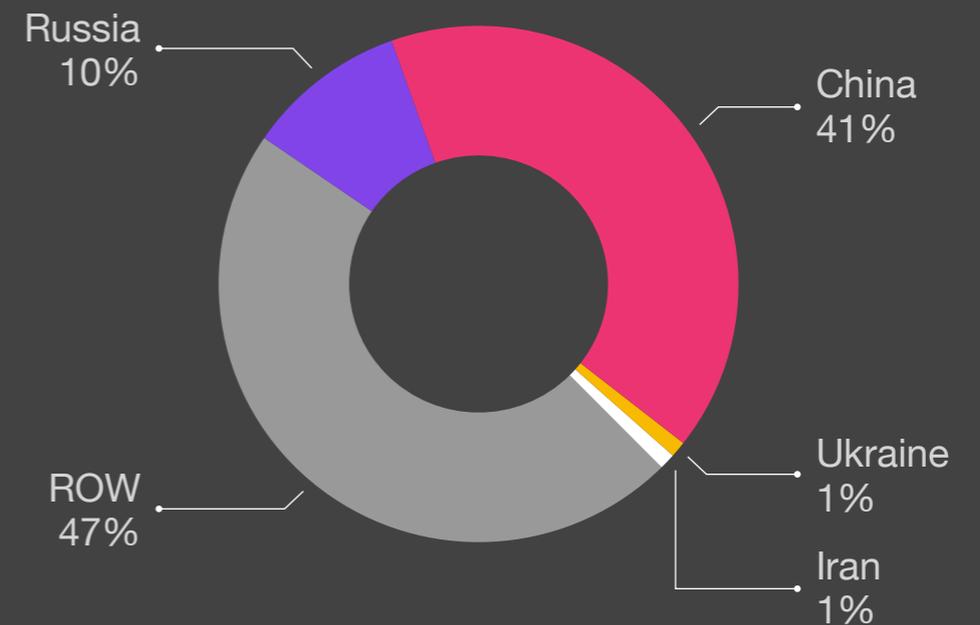
### Exfiltration Techniques



### Attack Vectors<sup>2</sup>



### Ransomware Exfiltration 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.