May 2023

The month of May was a record-breaker as we recorded a massive 66 publicly disclosed ransomware attacks, the highest we have ever recorded since we started this blog back in January 2020. Royal, LockBit and BlackCat were the most active during the month, while education remained the most heavily targeted sector, with a few attacks on religious organizations also noted which is an uncommon occurrence. Cybersecurity firm Dragos made headlines when they were targeted by a failed extortion attempt, while an attack on health services organization Harvard Pilgrim caused havoc for patient care, and dental insurance provider MCNA informed nearly 9 million patients that their data had been impacted by a cyber incident.

Roundup

May represents a watershed moment for Ransomware across the globe with a significant increase in the attack success rate, with a 154% increase over 2022. Notably, we saw a concerted effort to attack law firms as attackers placed increasing emphasis on data exfiltration. The value of the data continues to climb as cyber criminals look for new ways to extort organizations and their clients. This explains the 233% increase in the services industry this month.

We continue to see specific targeting of healthcare, technology, education and government with increases of 81%, 57%, 42% and 33% respectively during May. Unreported attacks are now 5 times (489%) more than reported attacks. While down from a high of 10 last month, this is a factor of the large volume of reported attacks rather than any material change in unreported attacks, which remained relatively constant at 323.

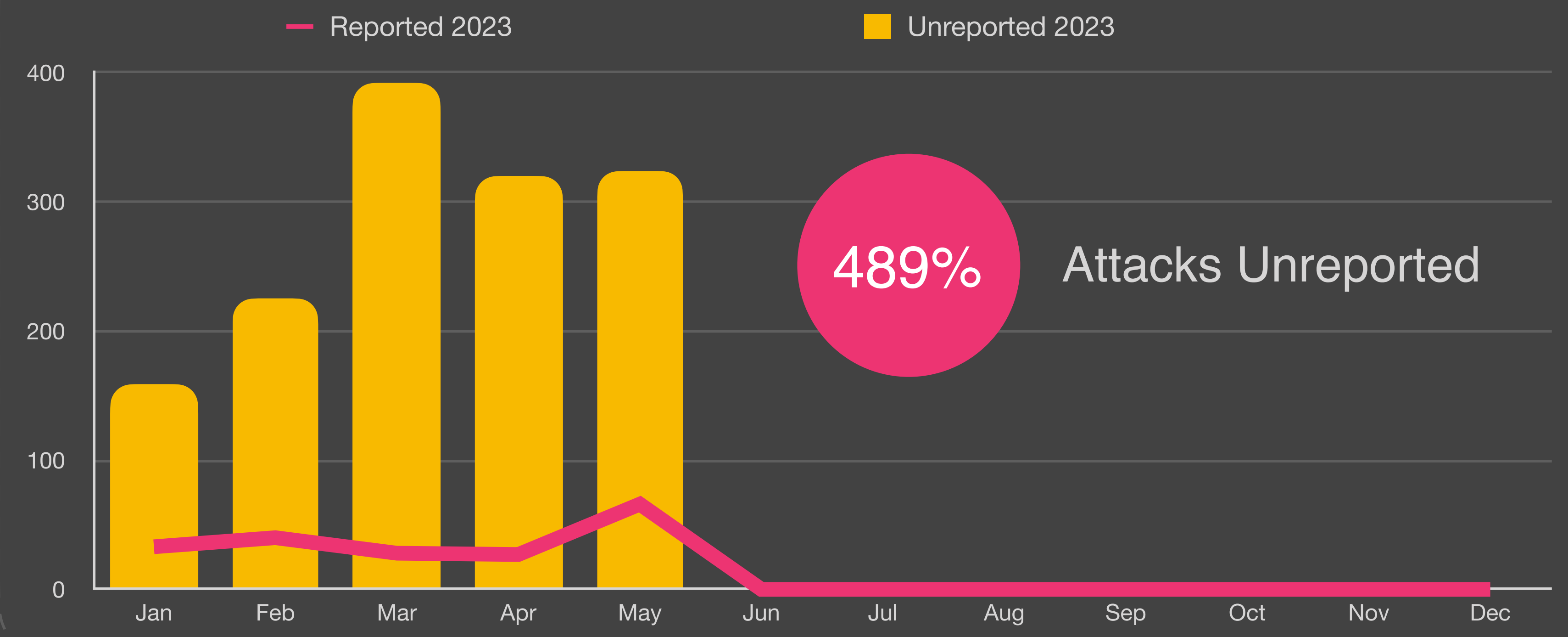
In terms of variants, this month we saw LockBit and BlackCat continue to dominate with 18.4" and 17.6% respectively, very similar to last month. This is consistent with unreported attacks, also dominated by LockBit and BlackCat, with 39.7% and 13.8% respectively.

Finally, illegal networks now dominate exfiltration techniques with 97% of all attacks, with a large majority originating and exfiltrating data to China 42% of the time, with Russia at 10%. We attribute the lower exfiltration to Russia due to the effect of sanctions, making it difficult to procure, launch and exfiltrate data to this nation.

BlackFog State of Ransomware Report

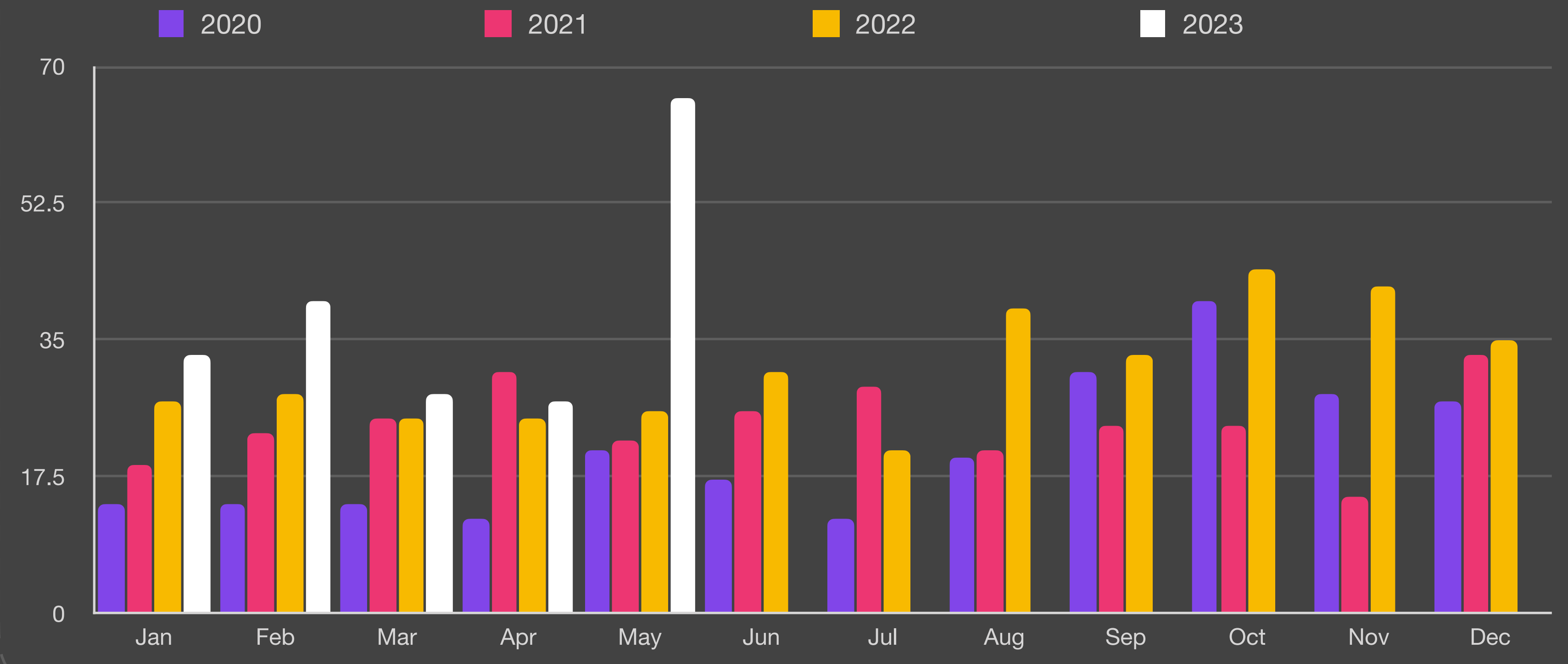
May 2023

Unreported Ransom Attacks



489% Attacks Unreported

Reported Ransomware by Month



Key Trends

489% Unreported

May Highest Ever

+154% Over 2022

73% of all attacks use PowerShell

89% of attacks exfiltrate data

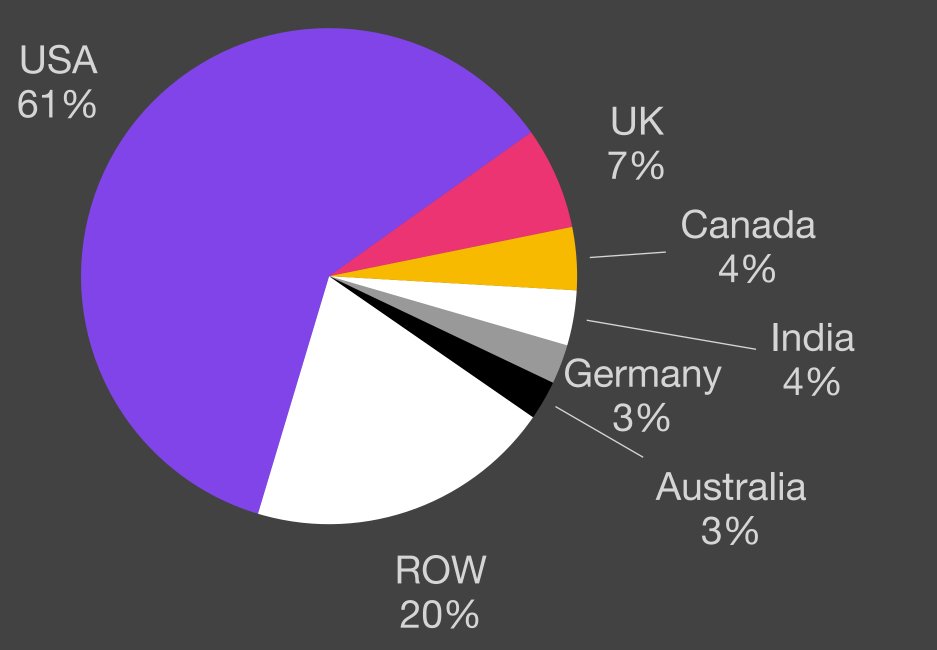
Average payout US $327,883k

-20% from Q4/22

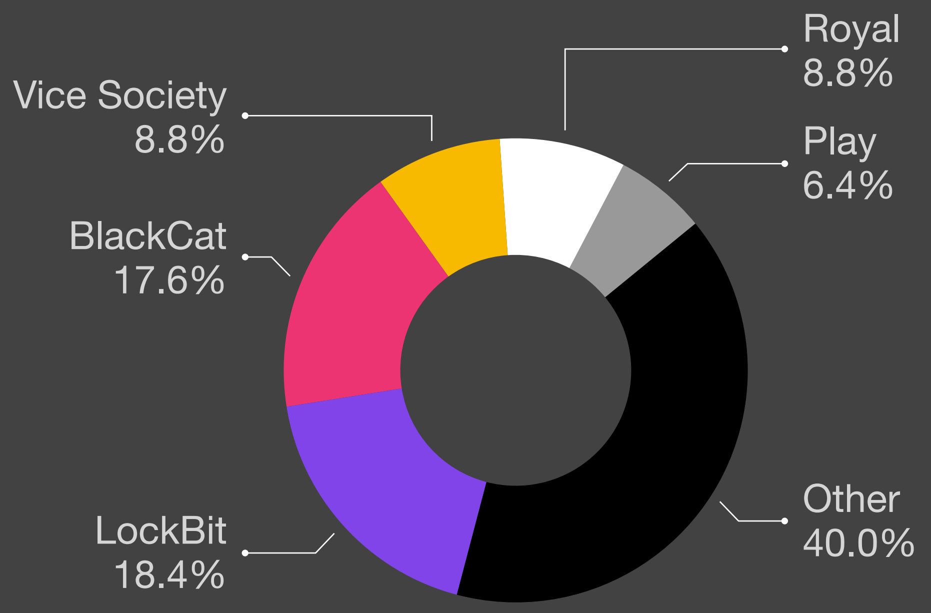
BlackFog State of Ransomware Report

May 2023

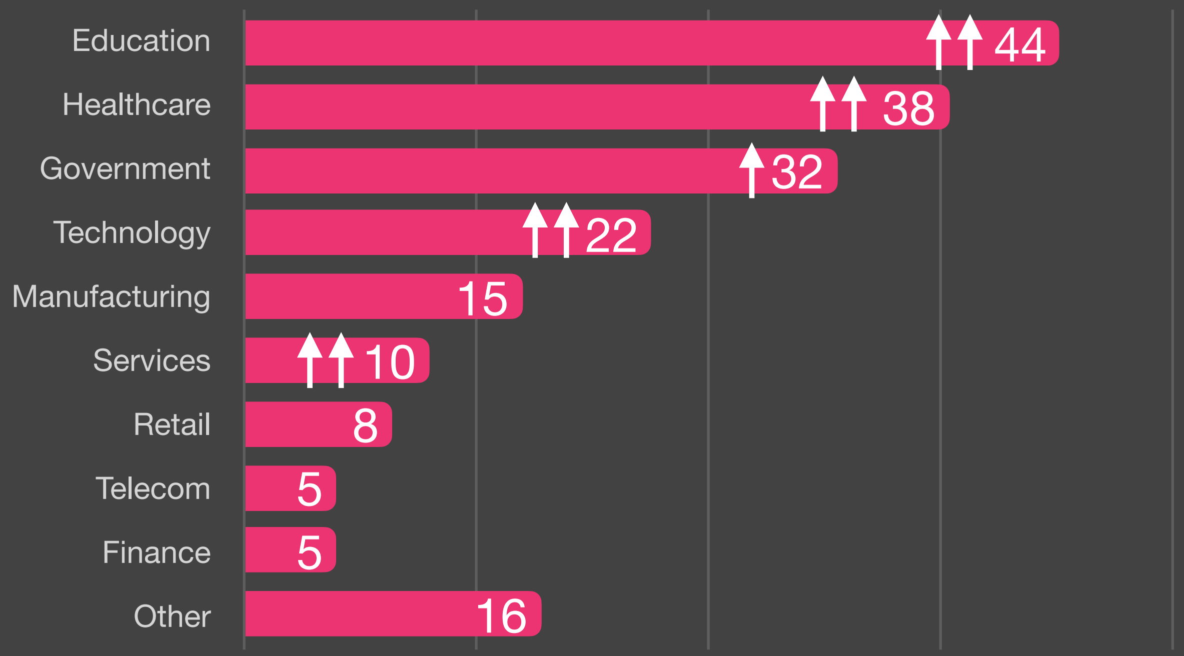
Ransomware by Country



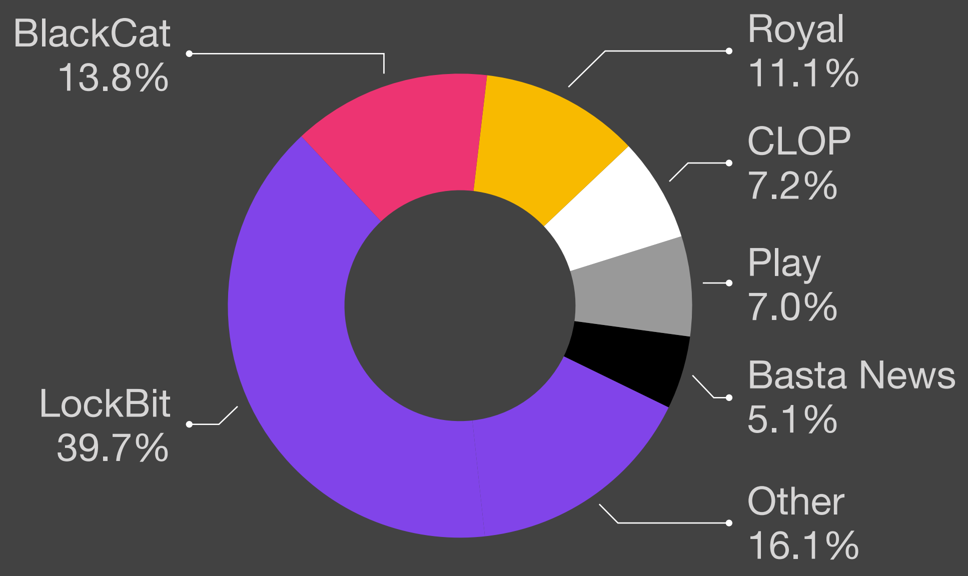
Reported Ransomware Variant



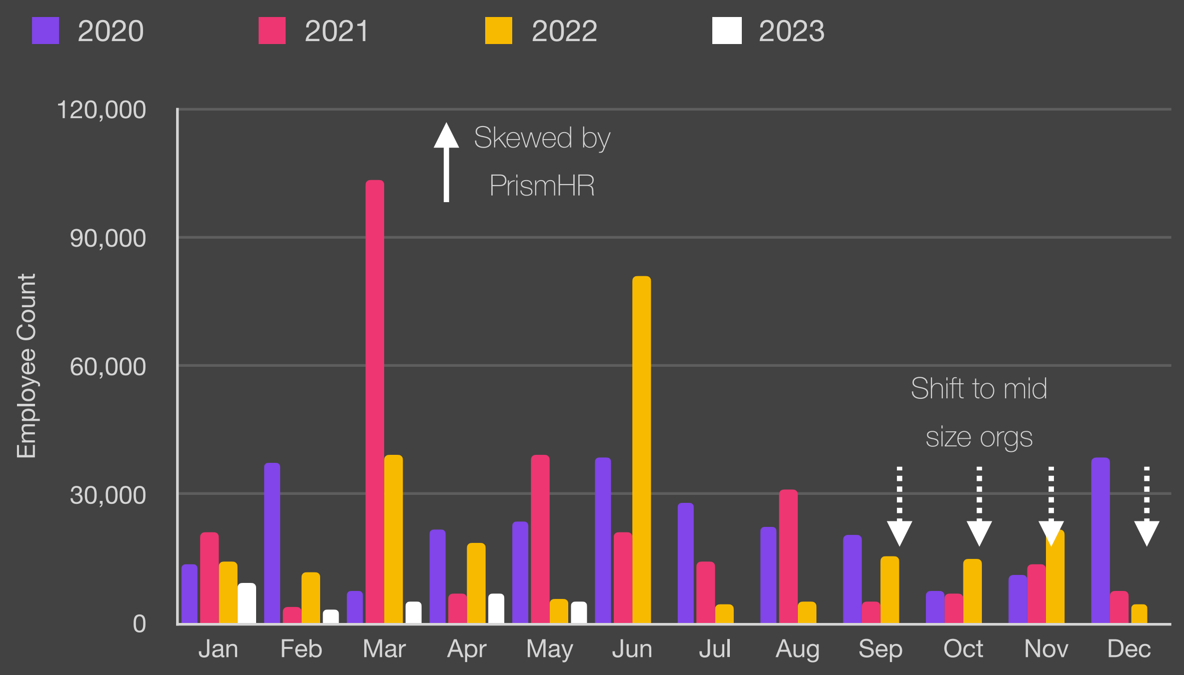
Ransomware by Industry



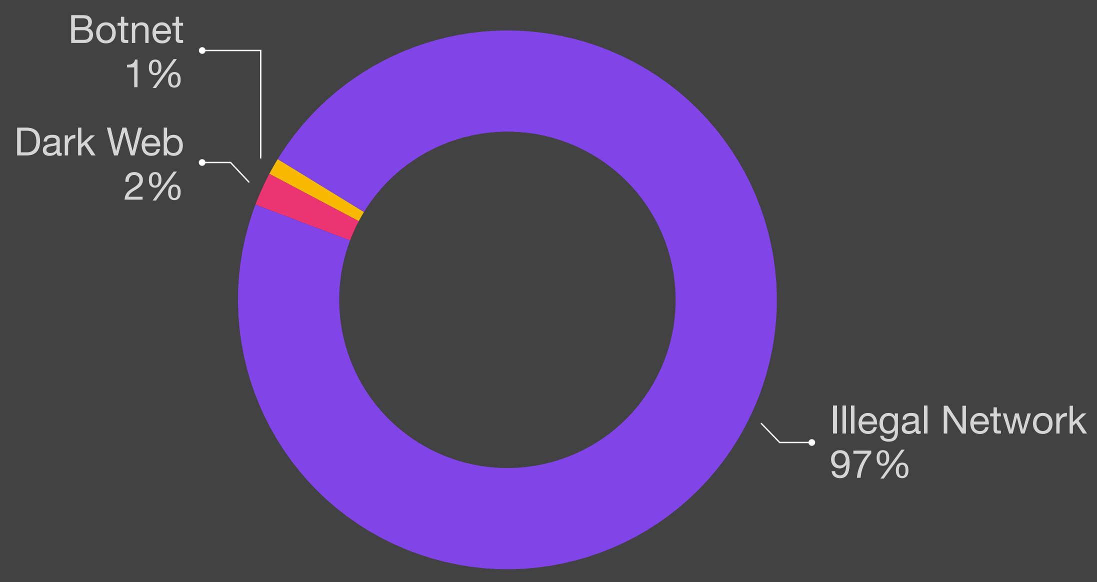
Unreported Ransomware Variant



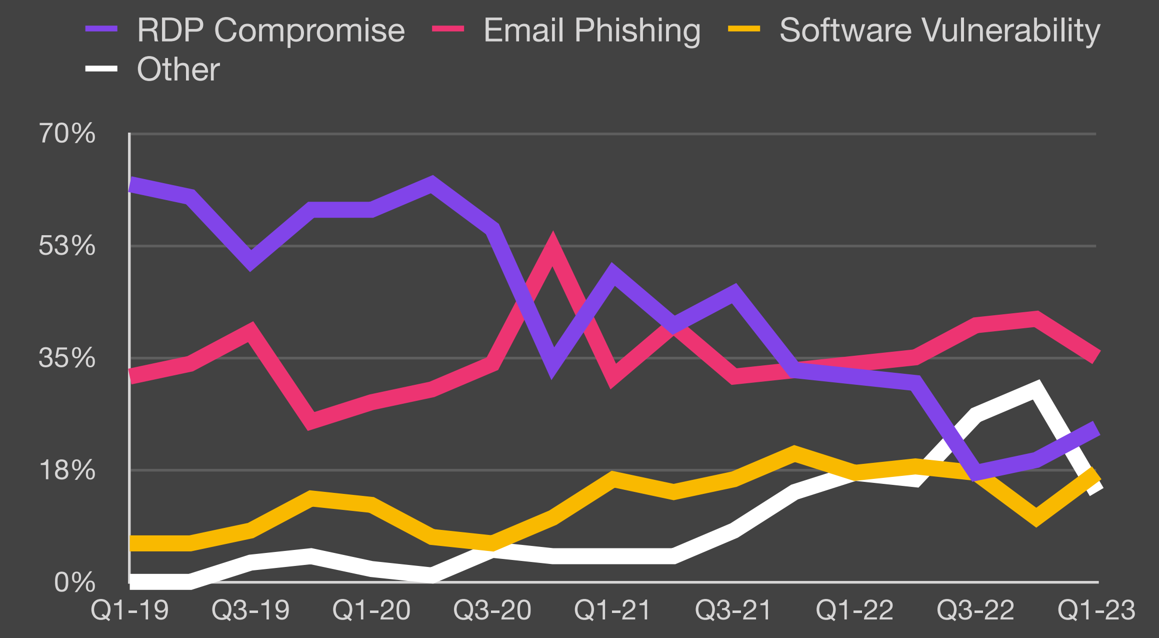
Size of Organization



Exfiltration Techniques

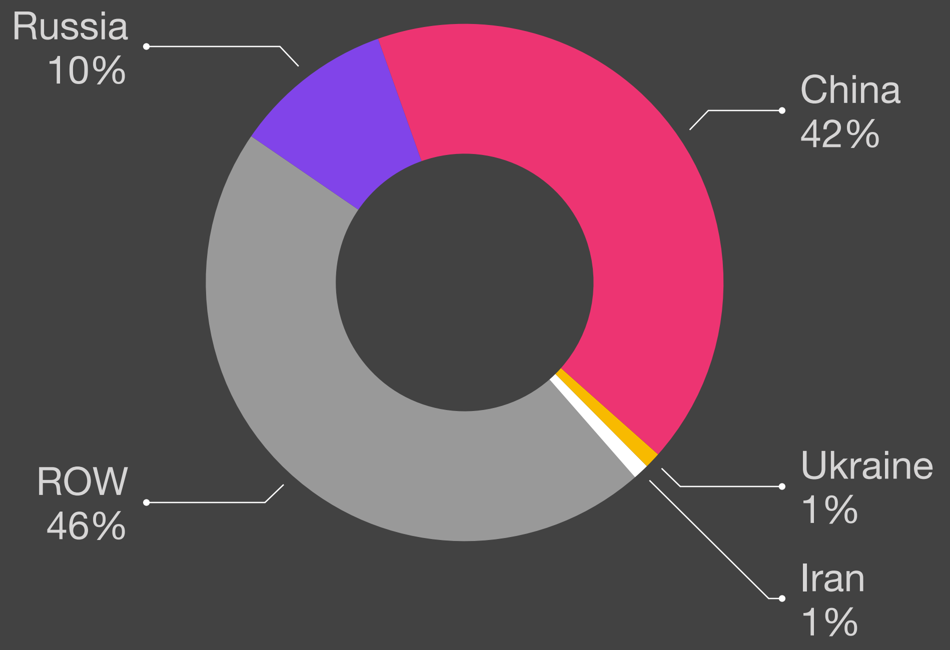


Attack Vectors[2]



[2] Courtesy Coveware

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.