November 2023

We recorded eighty-nine publicly disclosed ransomware attacks in November, the highest number we've recorded since starting our State of Ransomware blog in 2020. This figure represents a massive 112% increase on 2022's recorded attacks. LockBit and BlackCat continue to be the two top variants, with 20 and 15 attacks respectively. Healthcare was the hardest hit industry with 21 incidents recorded, including the attack on **Ardent Health Services** which caused chaos across various states over Thanksgiving. Other notable attacks this month include **ICBC**, **SIRVA** and **Fidelity National Financial**.

Roundup

Another month, another record. November surprised us with the sheer volume of attacks. Not only did it break an all time record with 89 attacks, it was 27% more than the previous best in September. The unreported to reported ratio continues to remain stable this month at 492% continuing the trend with companies reporting breaches more often. The significant fines now being imposed by regulators will ensure this moves even lower in the coming months.

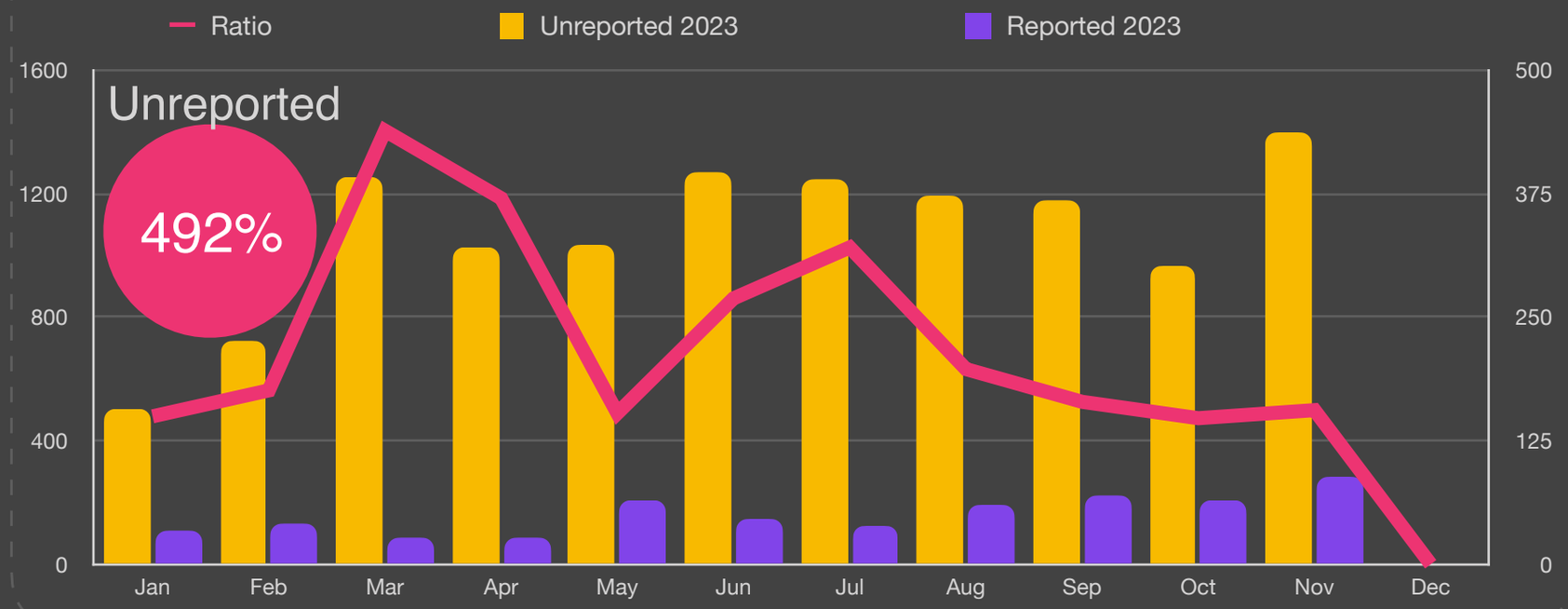
The SEC rules require registrants to disclose material cybersecurity incidents they experience within four days and to report on an annual basis material information regarding their cybersecurity risk management, strategy and governance. The orders are effective on or about December 18, 2023.

We saw the Healthcare and Manufacturing sectors grow significantly with increases of 21% and 20% respectively and the Finance sector by a massive 83%, effectively doubling the number of attacks in only one month. This does not bode well coming into the holiday season with the banks and financial institutions under significant pressure.

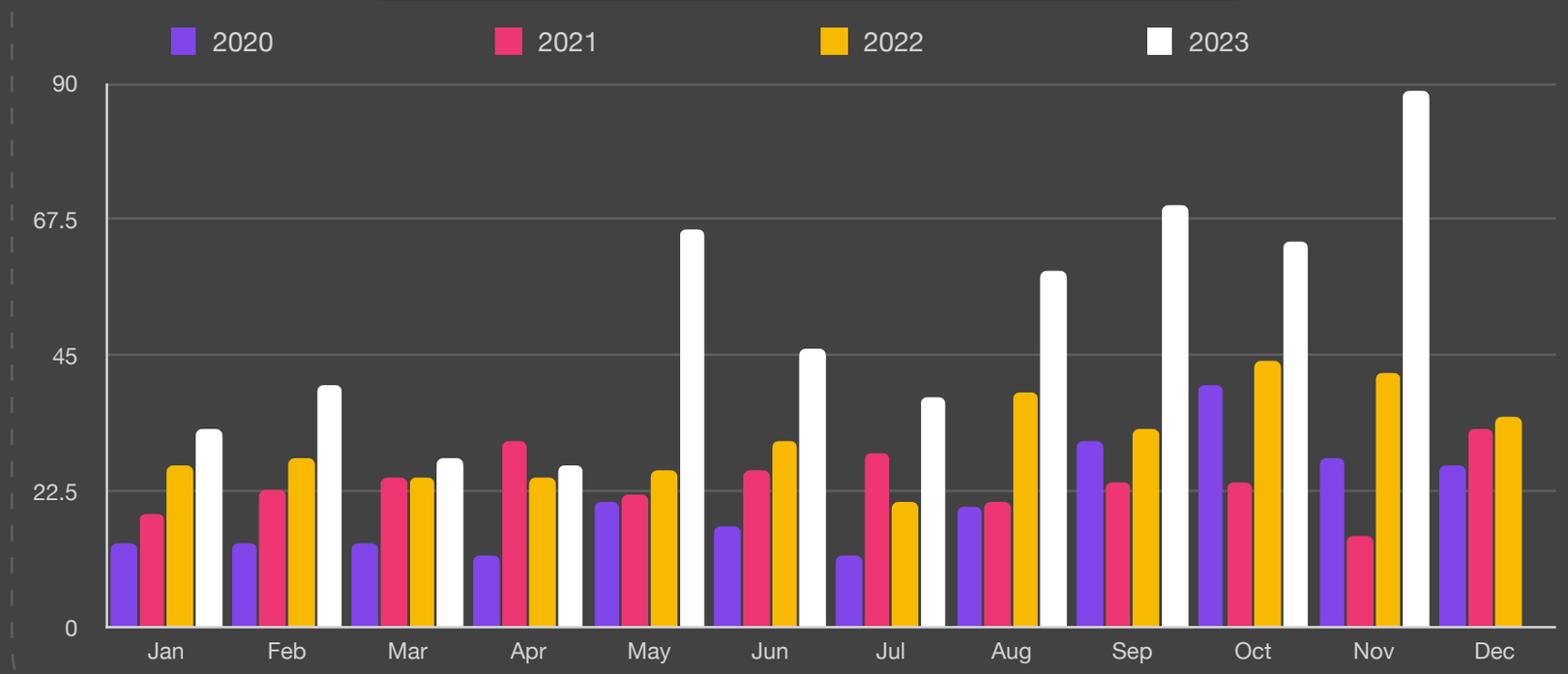
In terms of variants we see LockBit and BlackCat continue to dominate reported attacks, both at 19.2% each. LockBit also dominates the unreported attacks at 34.9% and BlackCat at 14.2%. As in previous months, data exfiltration continues to dominate as the primary mechanism for extortion at 90% with traffic flowing to China at 30% and Russia 9% of the time.

Copyright © 2023 BlackFog, Inc. Key statistics compiled and collected by BlackFog from various sources including BlackFog Enterprise. May only be used with attribution link to blackfog.com

Unreported Ransom Attacks



Reported Ransomware by Month



Key Trends

492% Unreported

1st Highest of Year

1st Highest Ransom Payouts

48% of all attacks use PowerShell

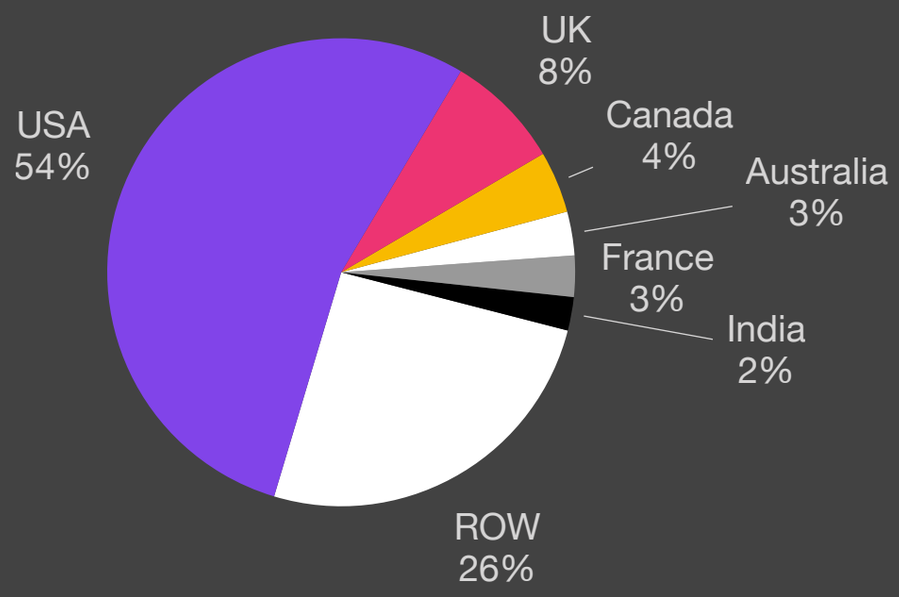
90% of attacks exfiltrate data

Average payout US $850,700

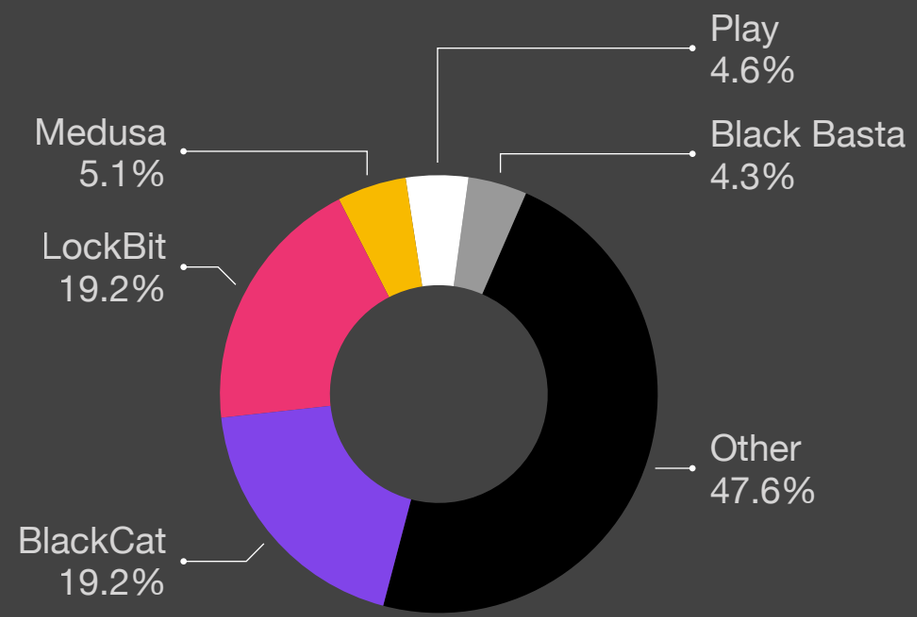
+15% from Q2/23

Copyright © 2023 BlackFog, Inc. Key statistics compiled and collected by BlackFog from various sources including BlackFog Enterprise. May only be used with attribution link to blackfog.com

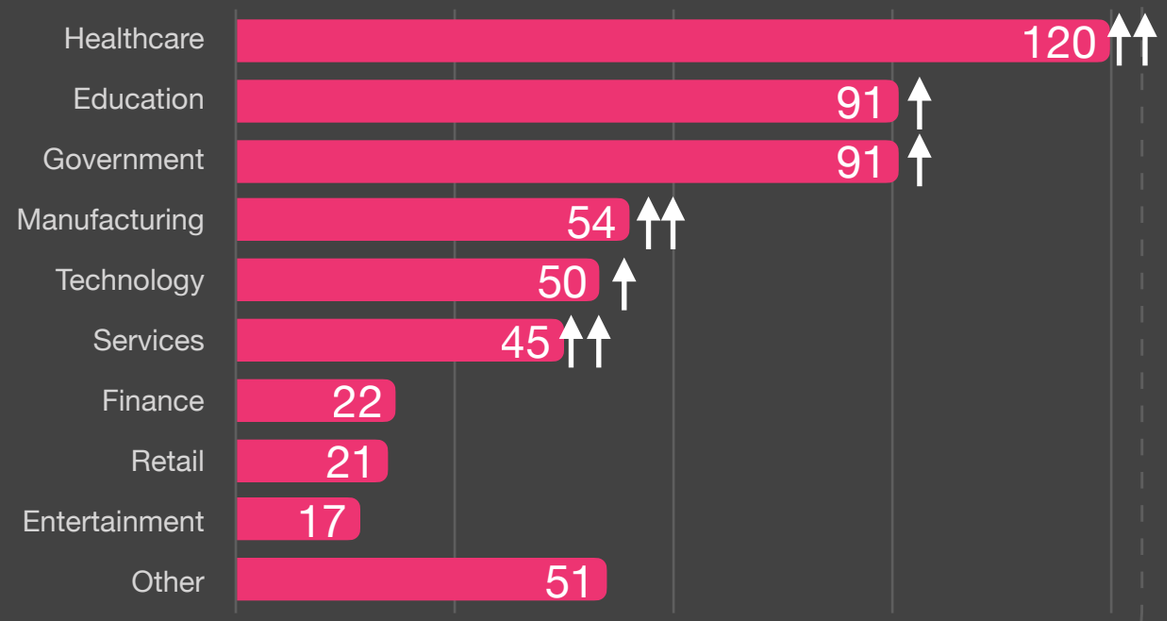
Ransomware by Country



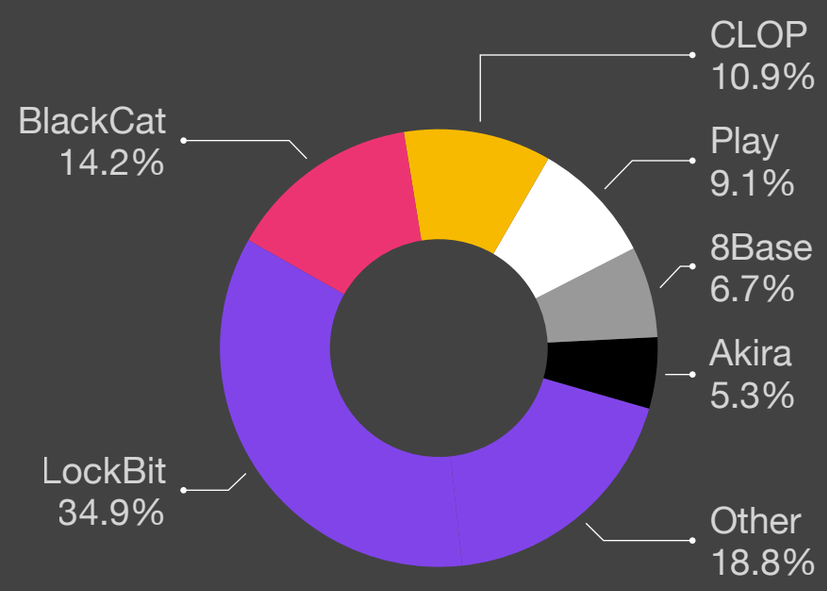
Reported Ransomware Variant



Ransomware by Industry

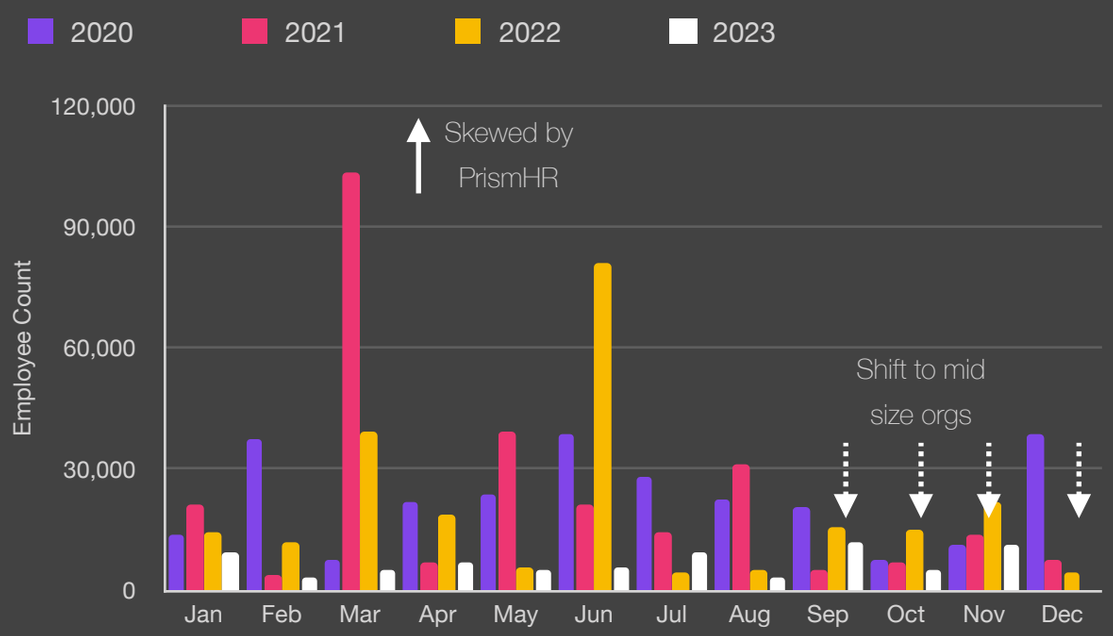


Unreported Ransomware Variant

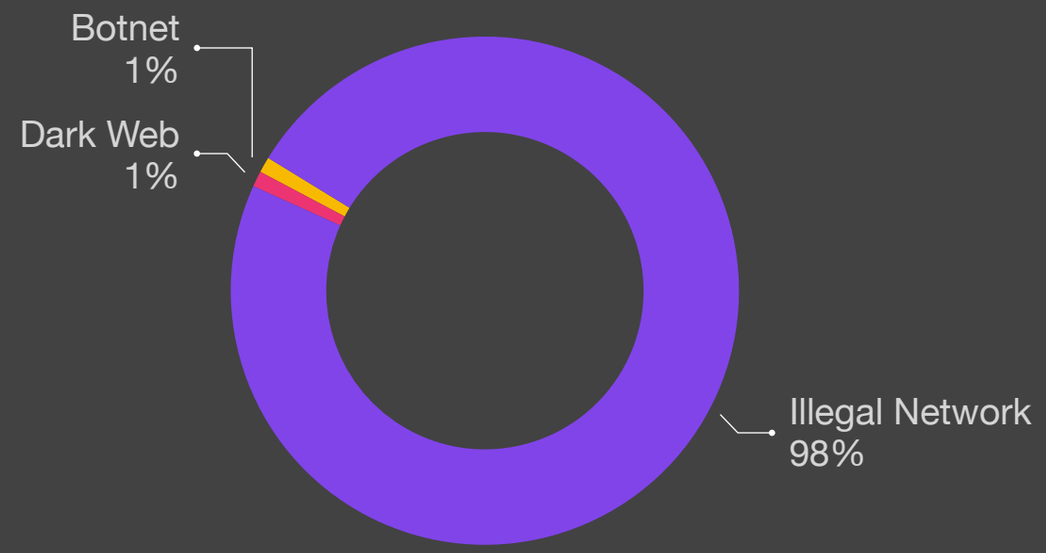


Copyright © 2023 BlackFog, Inc. Key statistics compiled and collected by BlackFog from various sources including BlackFog Enterprise. May only be used with attribution link to blackfog.com

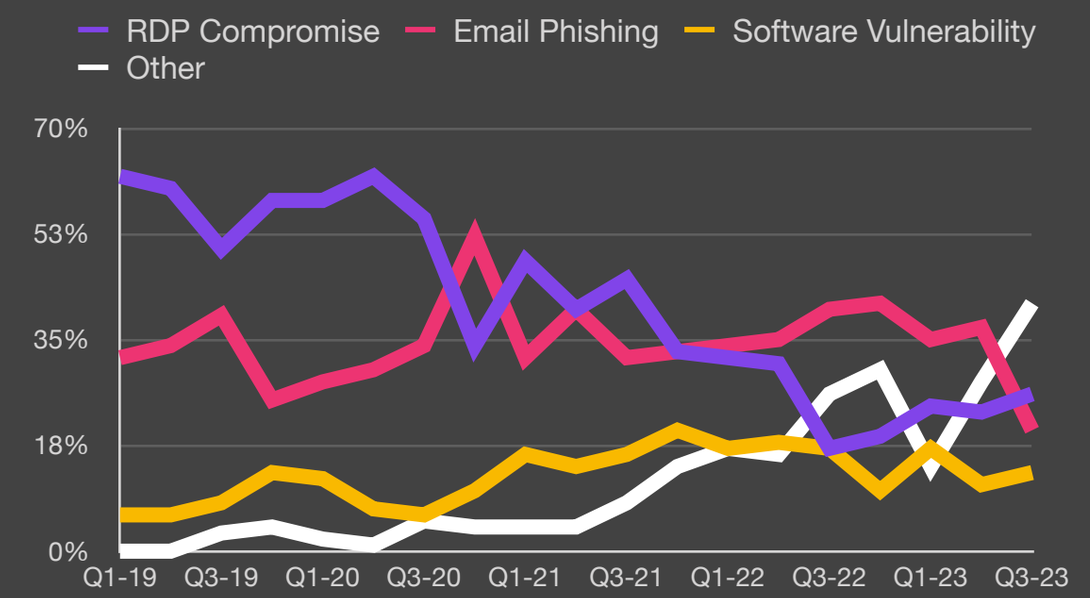
Size of Organization



Exfiltration Techniques

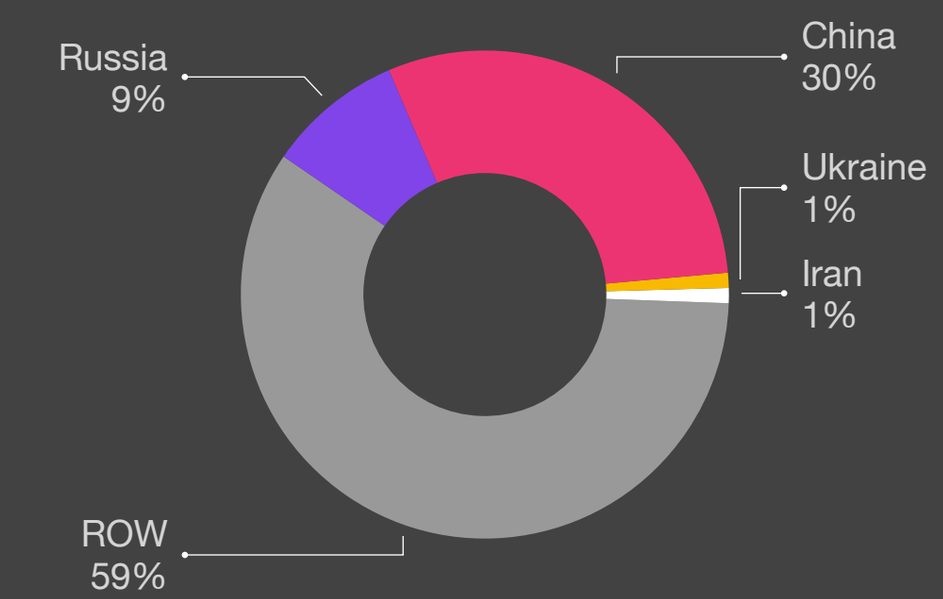


Attack Vectors[2]



[2]Courtesy Coveware

Ransomware Exfiltration Country



Copyright © 2023 BlackFog, Inc. Key statistics compiled and collected by BlackFog from various sources including BlackFog Enterprise. May only be used with attribution link to blackfog.com

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.

Copyright © 2023 BlackFog, Inc. Key statistics compiled and collected by BlackFog from various sources including BlackFog Enterprise. May only be used with attribution link to blackfog.com