March 2023

March saw the lowest number so far this year with 28 publicly disclosed attacks, representing a 12% increase over 2021 and 2022. As usual, education was heavily targeted during the month and it continues to be the number one vertical, ahead of both government and healthcare. High profile incidents included Maximum Industries, the company responsible for making parts for SpaceX. The LockBit gang claimed the attack and disclosed that they had managed to exfiltrate blueprints. The Clop gang also made news when they launched attacks using a vulnerability in Fortra's GoAnywhere software to steal data from around 130 organizations, with new victim names continuing to make the news.

Roundup

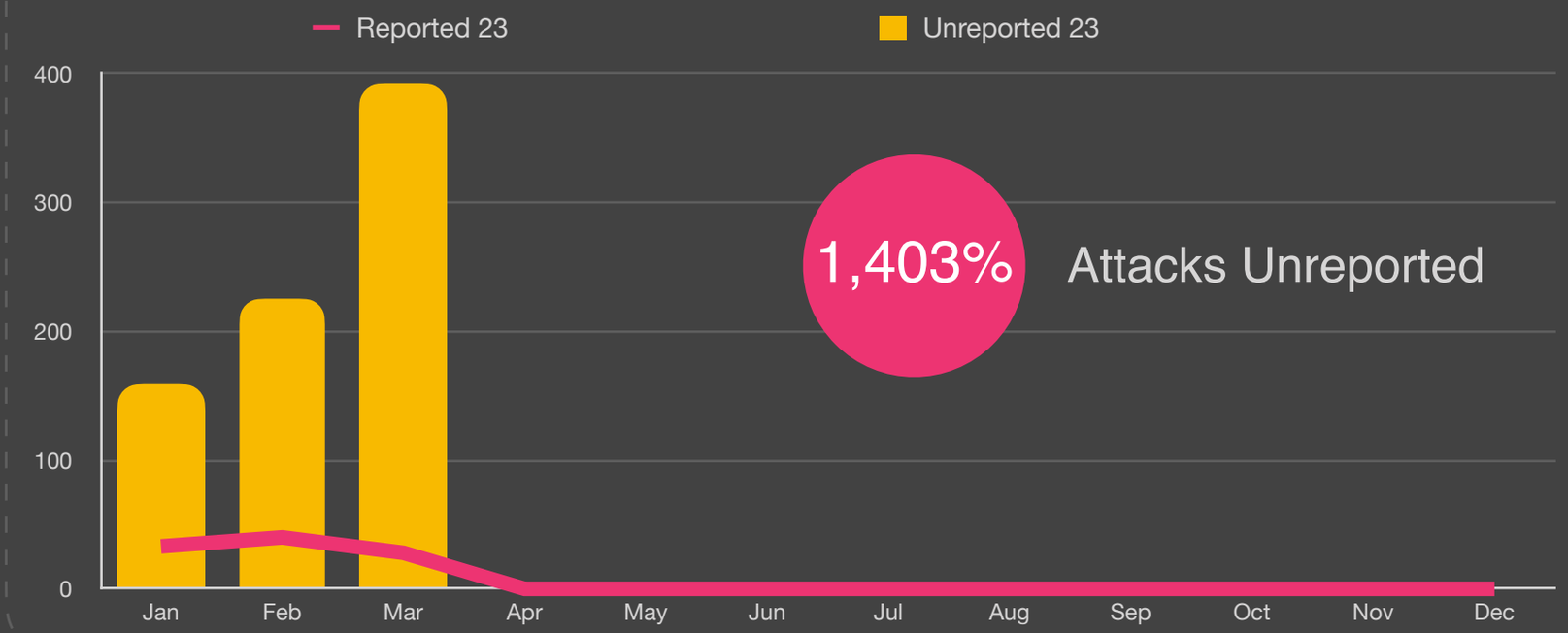
March witnessed a total of 28 ransomware attacks. While lower than January and February, this still represents a 4 year high, with a 12% increase over previous years. Most notably we continue to see the flow on effects from unreported attacks. March saw 1,403% of attacks going unreported, up from 478% and 543% in January and February respectively. Nearly a 3 fold increase from previous months.

March also saw Education increase its lead as the most targeted sector, increasing by more than 53%, with 26 attacks for the year, followed by government and healthcare with increases of 33% and 13% respectively.

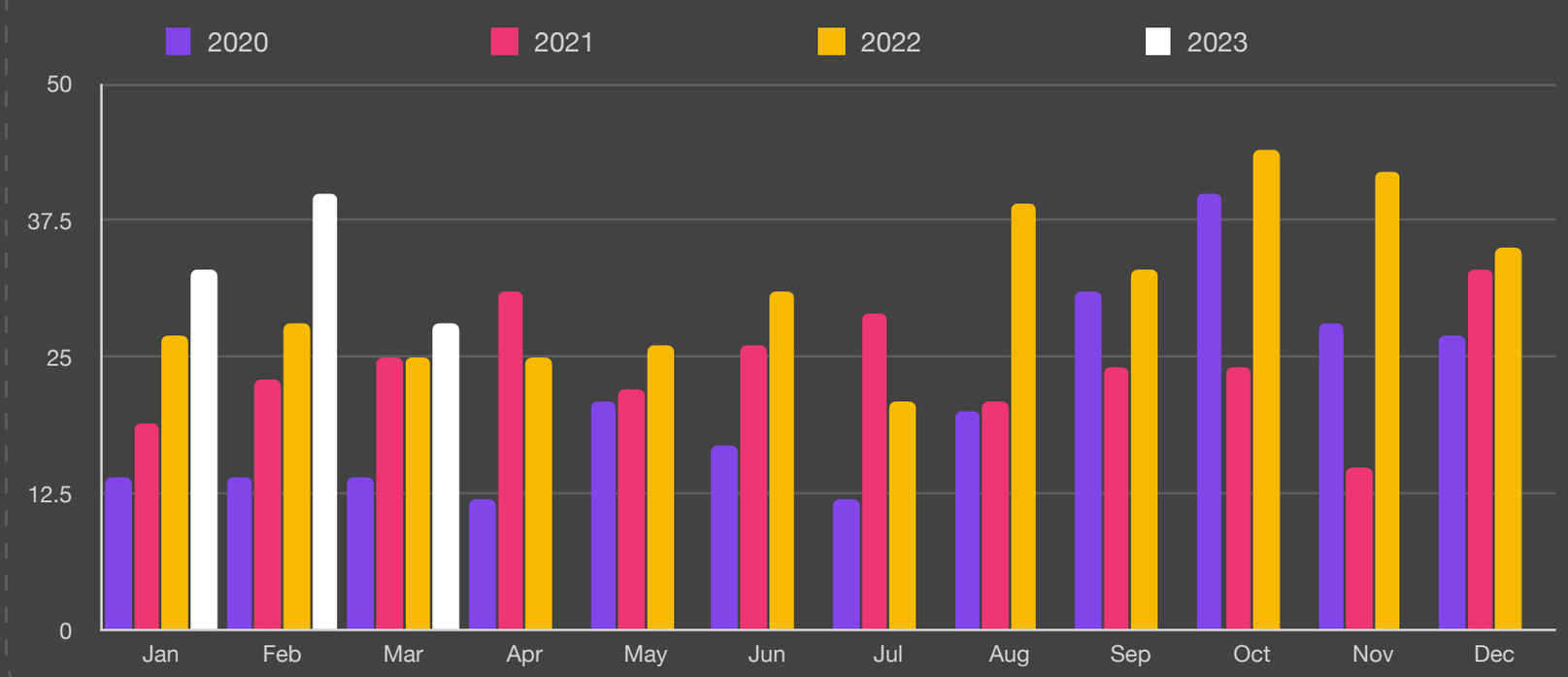
LockBit continues to dominate as the key ransomware variant with 24.3% of reported attacks and 41.4% of unreported attacks. It should be noted that the sheer volume of unreported attacks this month was dominated by LockBit, and we expect this to be reflected in the disclosed attacks over the coming months. Similarly, both CLOP and Royal were highly leveraged in unreported attacks with 11.4% each.

Lastly, we note that it is now becoming less common for attacks to remain unclaimed as ransomware gangs seek notoriety, with only 14% unclaimed this month. We have also seen continued use of data exfiltration in more that 88% of attacks, with March witnessing a significant increase in the use of illegal networks, up 14% to 94% since February.

Unreported Ransom Attacks



Reported Ransomware by Month



Key Trends

1,403% Unreported

Mar Highest Mar in 4 years

+12% Over 2021,2022

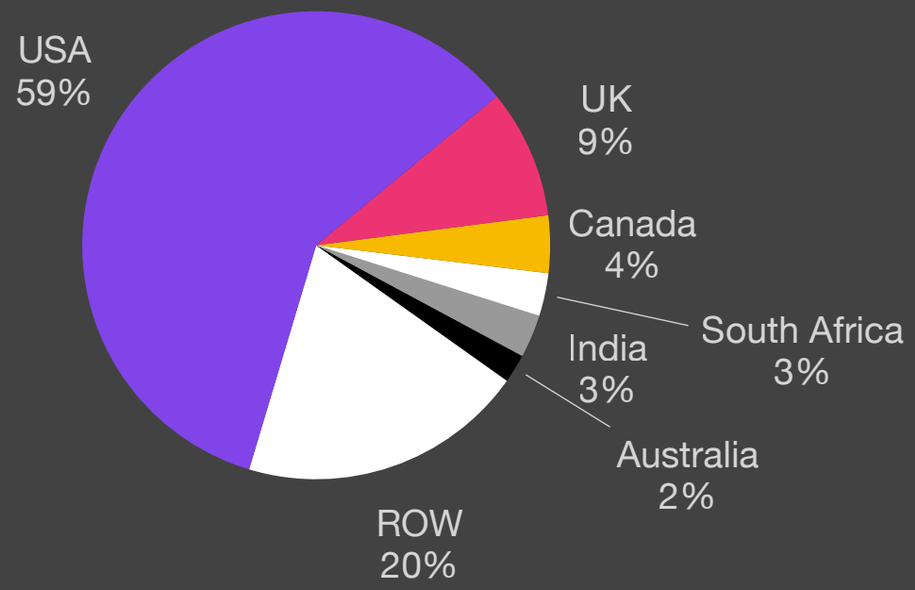
84% of all attacks use PowerShell

88% of attacks exfiltrate data

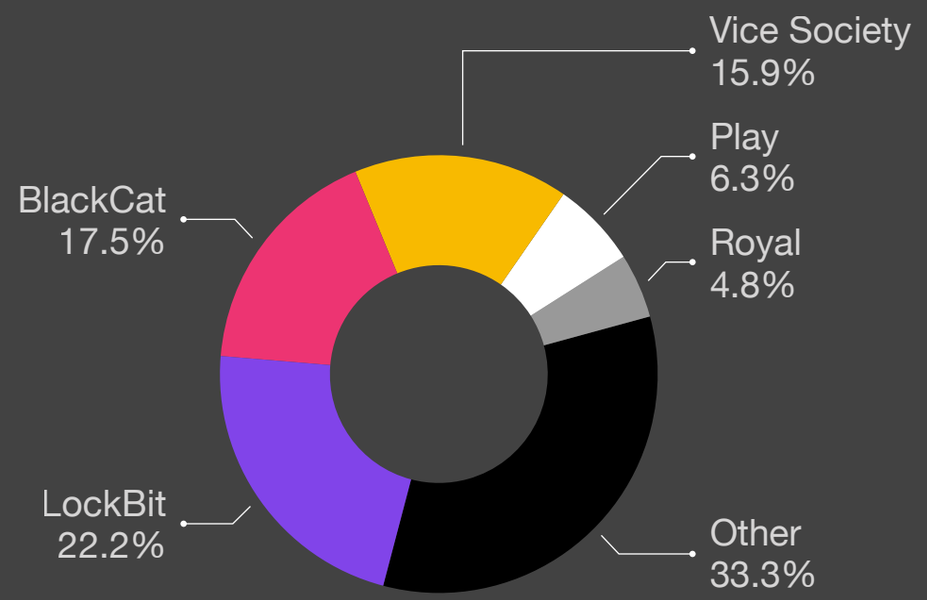
Average payout US $408,644k

+58% from Q3/22

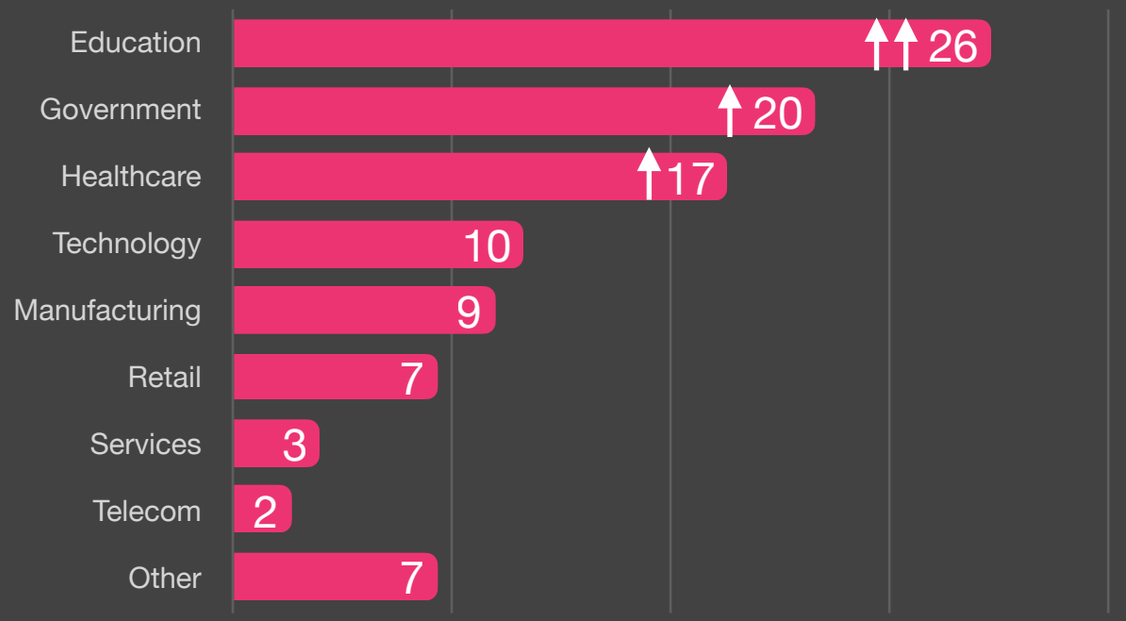
Ransomware by Country



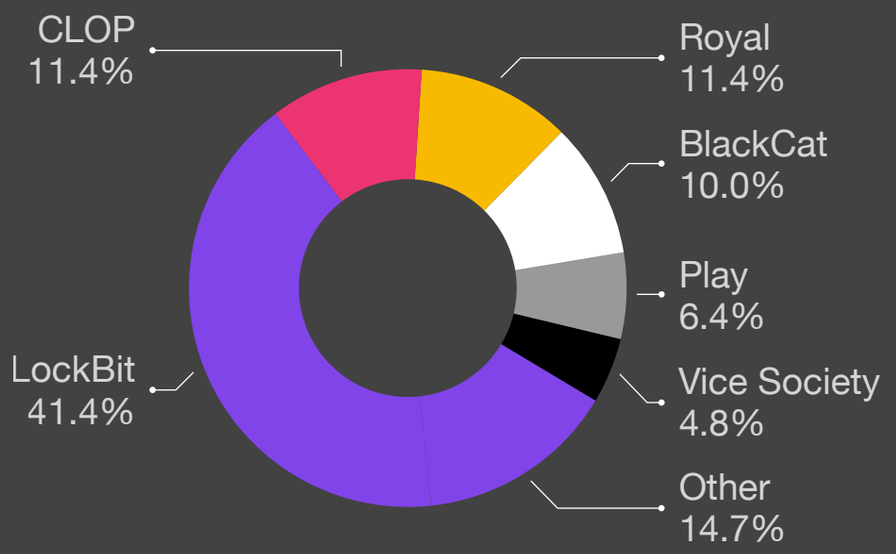
Reported Ransomware Variant



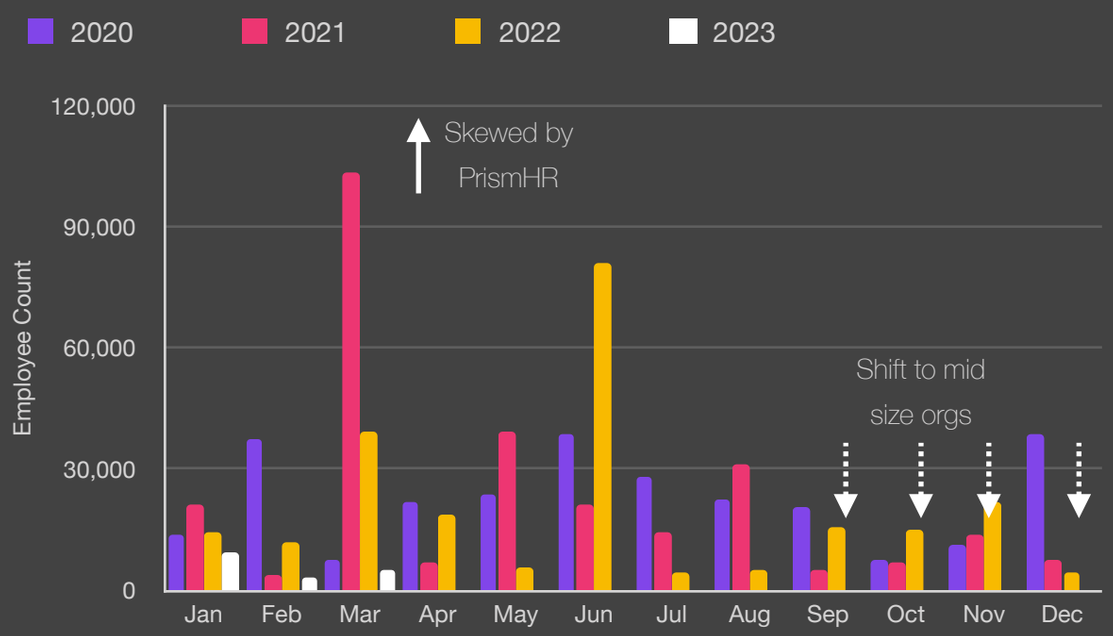
Ransomware by Industry



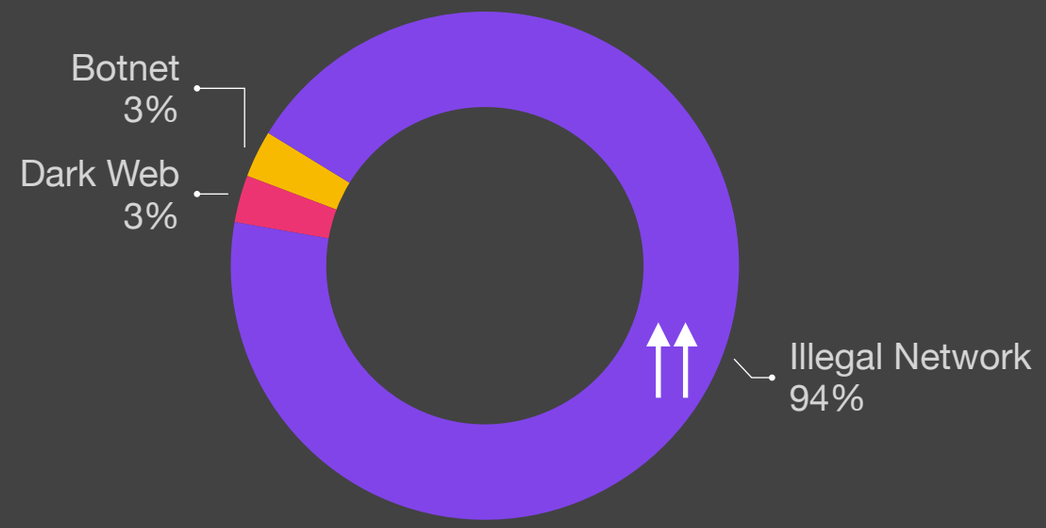
Unreported Ransomware Variant



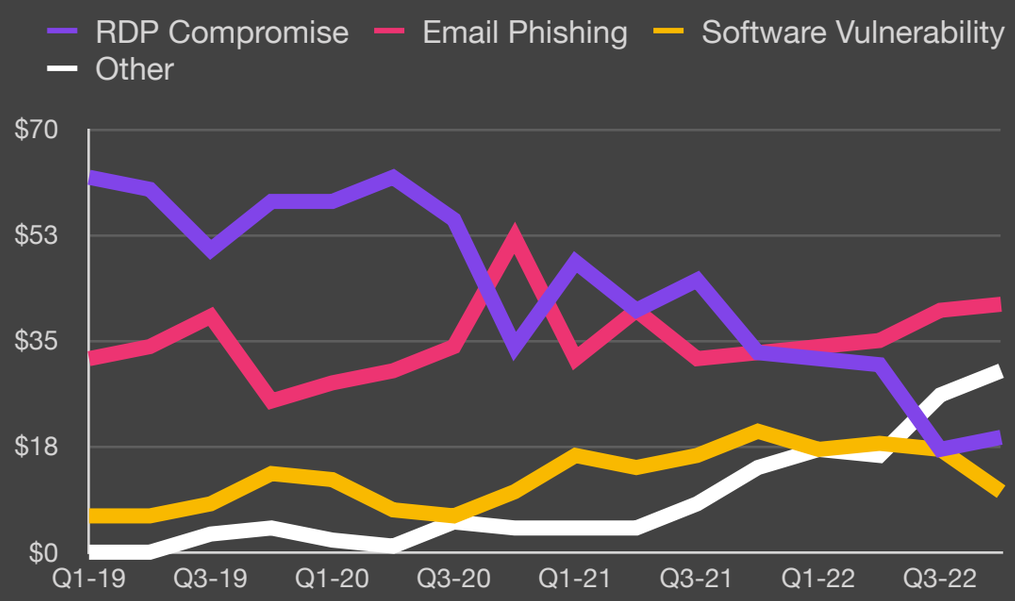
Size of Organization



Exfiltration Techniques

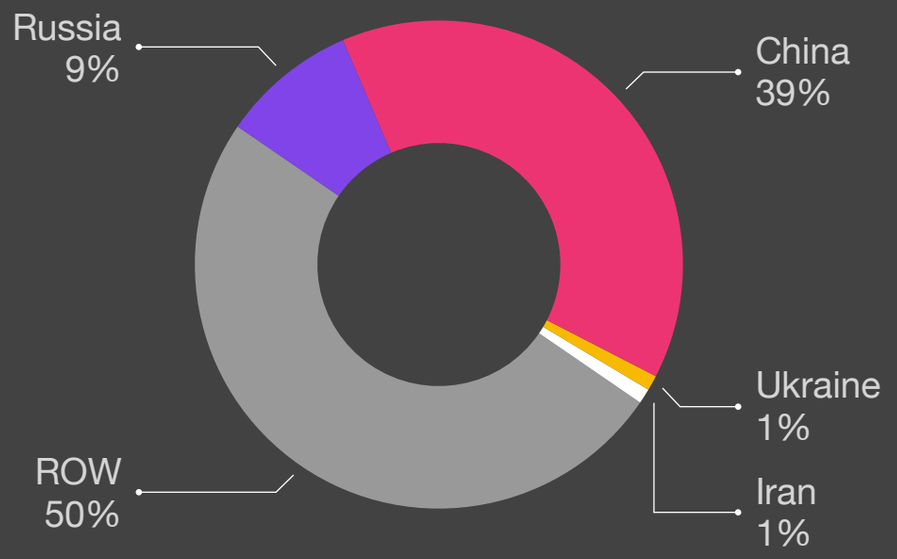


Attack Vectors[2]



[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.