Introduction

In February we recorded 57 publicly disclosed ransomware attacks, a 43% increase over last year's figures. February saw the temporary takedown of LockBit, which did slow the operation down for a few days, but didn't stop them from carrying out nine attacks, the same amount as BlackCat. Some attacks dominated headlines this month including **Lurie Children's Hospital**, **Fulton County**, **Hipocrate Information Systems** in Romania and **Epic Games**.

Roundup

The momentum from January continues with an all time record for February, with a total of 57 reported attacks, an increase of 43% from 2023. Unreported attacks were also up, with a 63% increase over 2023. While we expected to see some stabilization in the unreported to reported ratio this month we saw it increase to 644%, nearly double that of last month. This indicates that many organizations are still not complying with the new SEC incident disclosure rules.

February also saw a high volume of attacks on the government, manufacturing and healthcare sectors with increases of 150%, 114% and 113% respectively. Education sector remained the leading sector with a 43% increase this month.

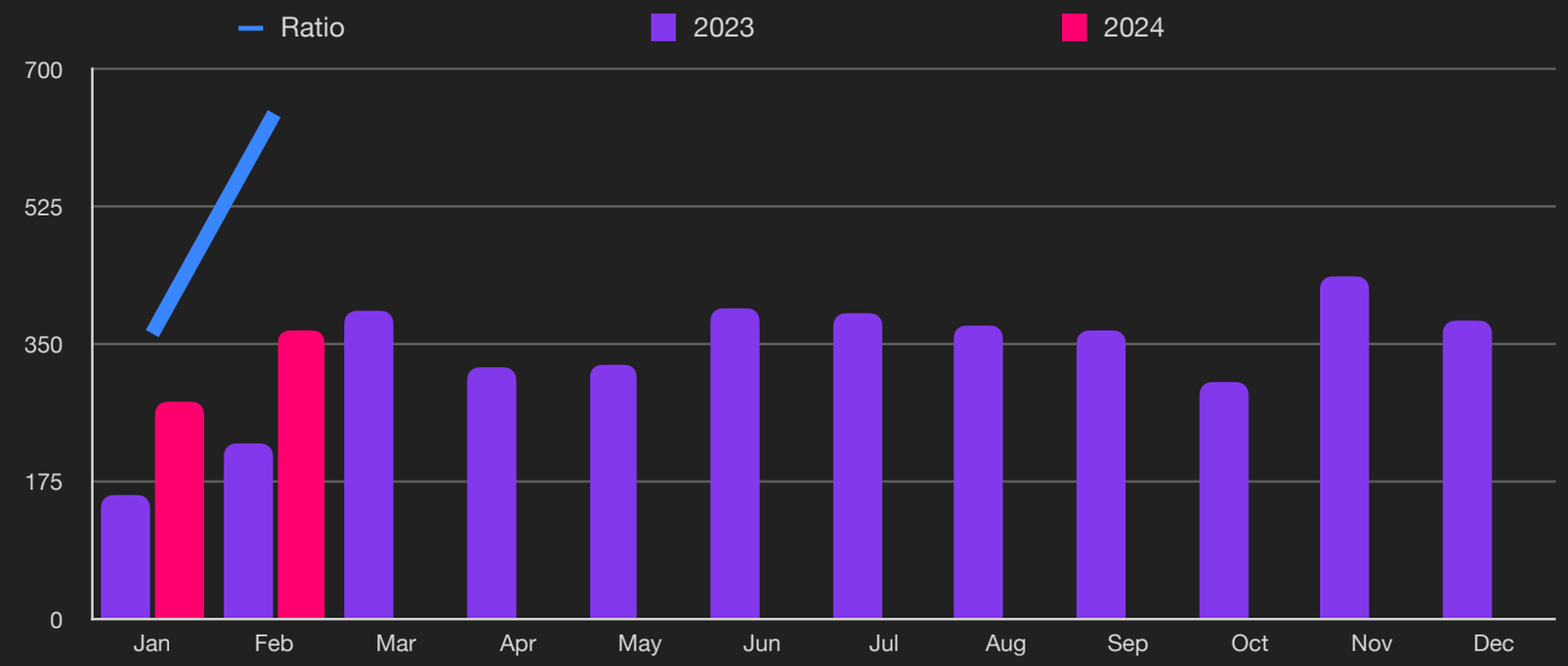
LockBit continues as the dominant ransomware variant with 27.2% of reported and 32.5% of unreported attacks followed by BlackCat. We also saw a new variant "Hunters", a derivative of Hive, enter the charts in 4th place in unreported attacks and expect to see this evolve in the coming months. Hunters International purchased the assets of Hive after the takedown in 2023.

Finally, data exfiltration is now involved in 91% of all attacks. As the primary goal of all attacks, data exfiltration ensures that attackers can threaten and sell victims data for years to come, regardless of whether payments are made or not. Once data loss has occurred there is no way to put the genie back in the bottle. This month we also see China and Russia dominate as the leading destinations for exfiltrated data with 18% and 8% respectively.

BlackFog State of Ransomware Report

February 2024

Unreported Ransomware Attacks

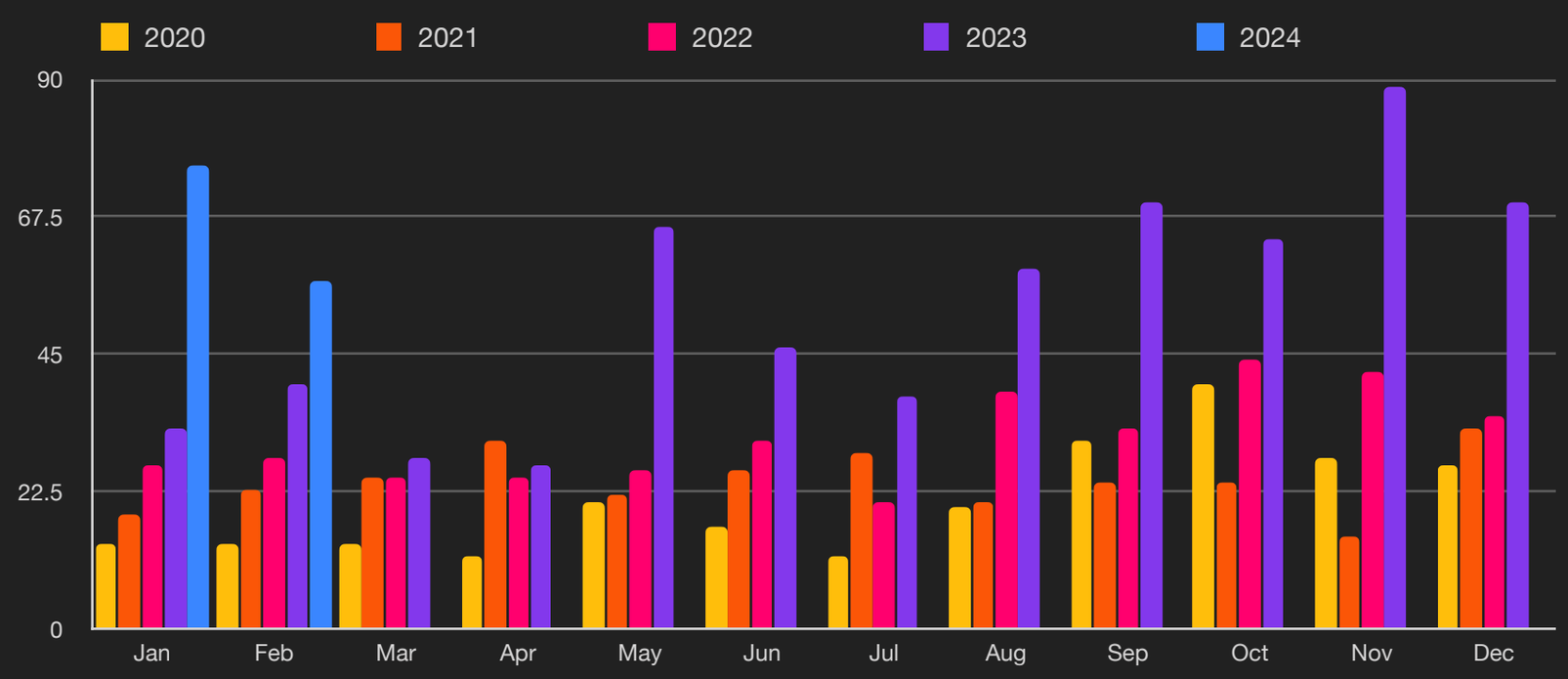


Key Trends

644% Unreported

1st Highest February

Reported Ransomware by Month



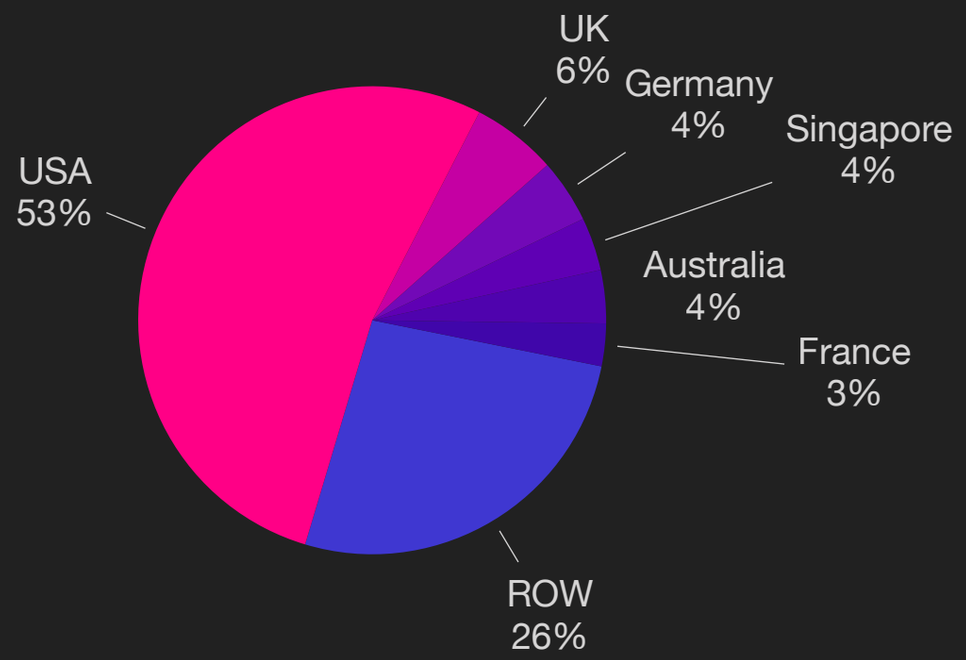
41% of all attacks use PowerShell

91% of attacks exfiltrate data

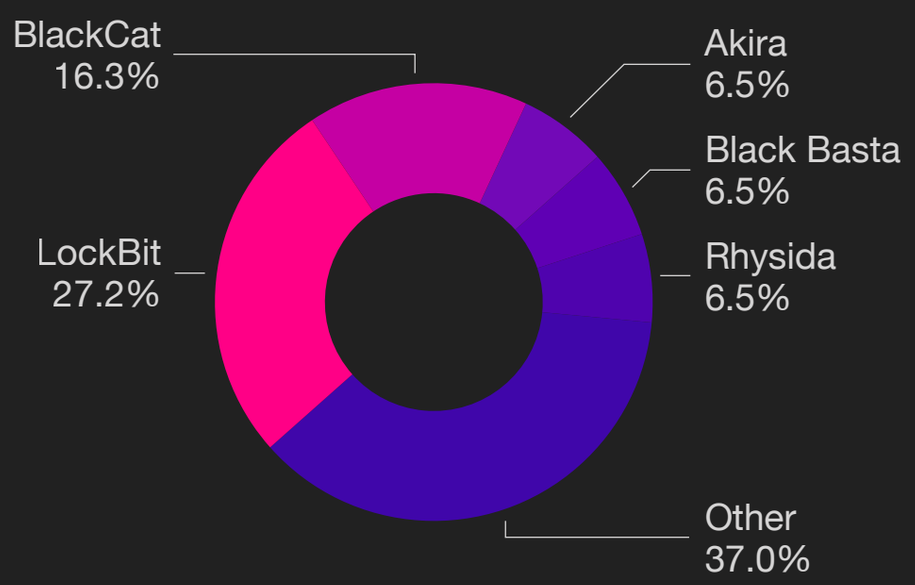
Average payout US $568,705

-33% from Q3/23

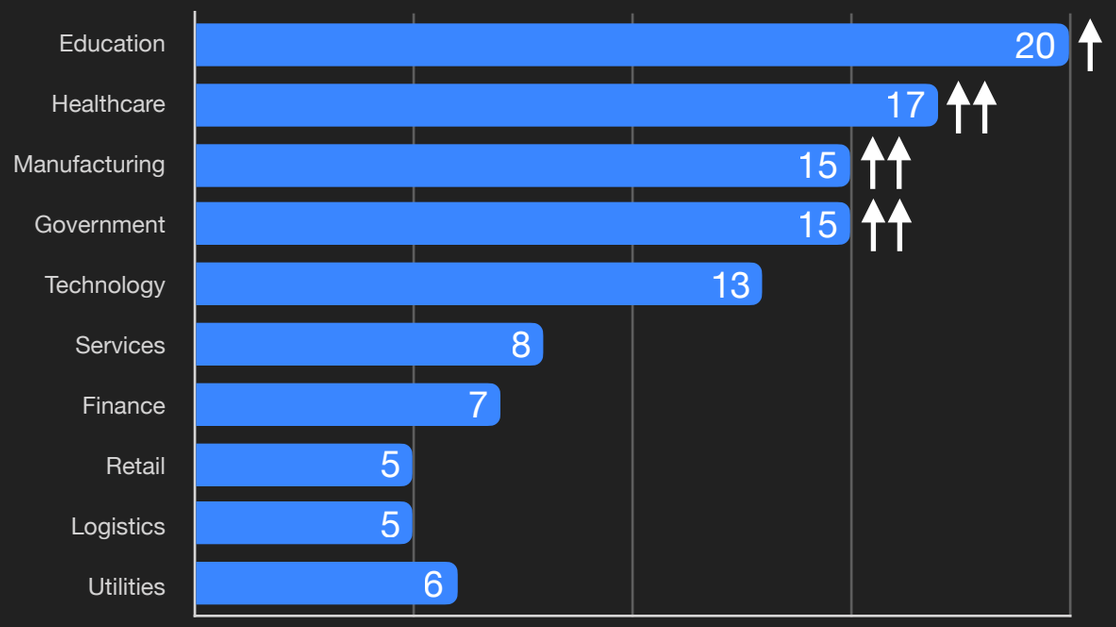
Ransomware by Country



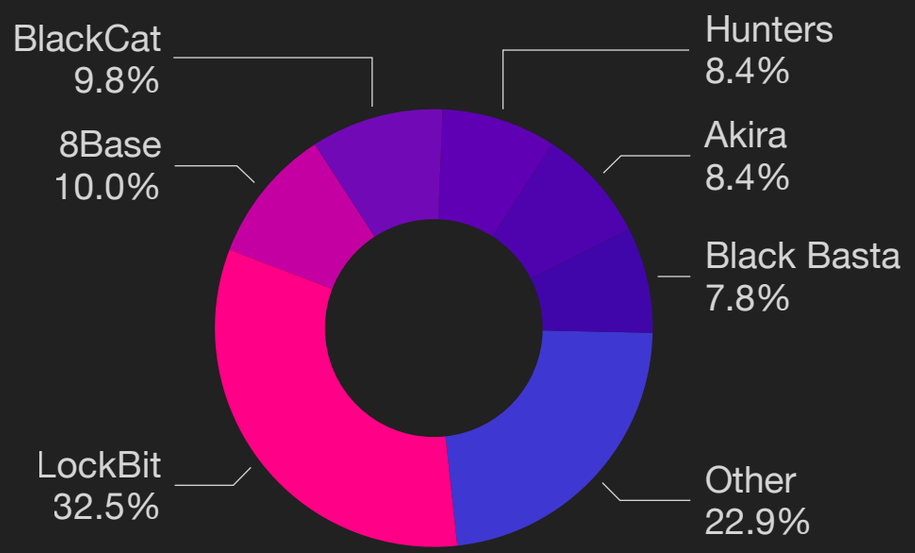
Ransomware Variant (Reported)



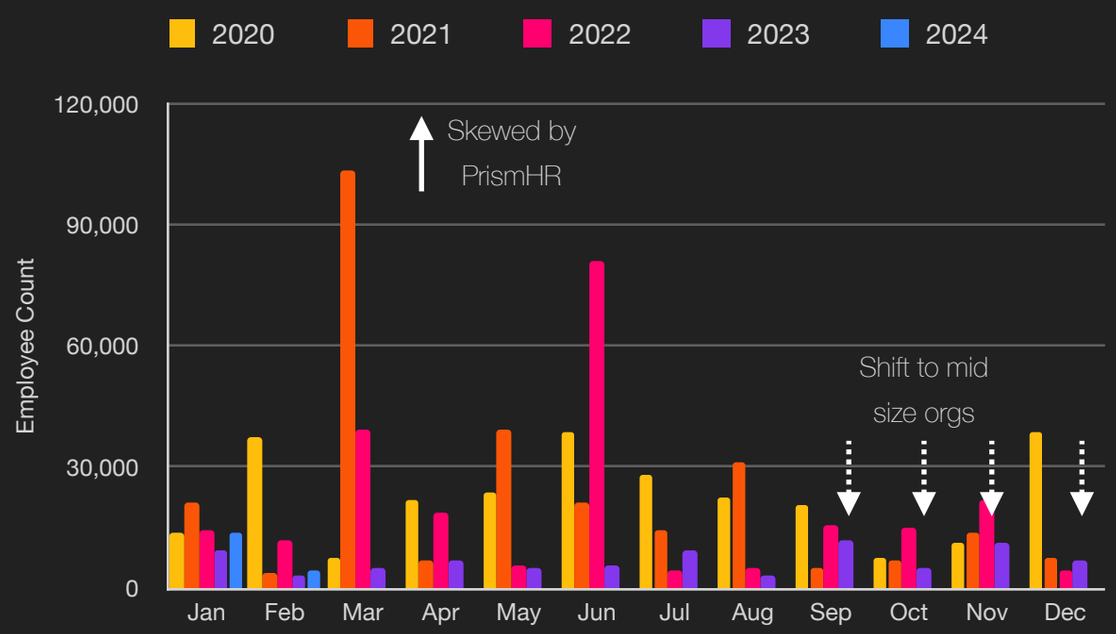
Ransomware by Industry



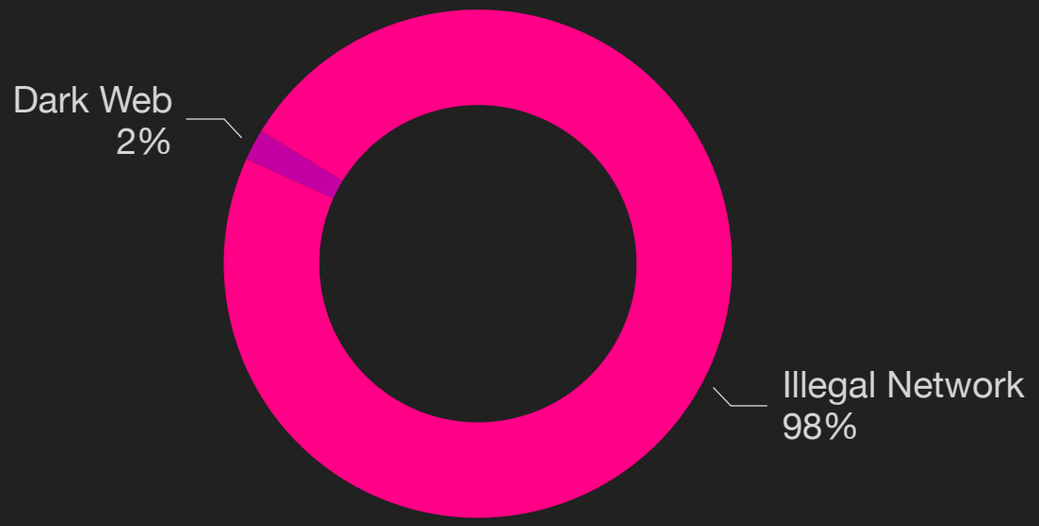
Ransomware Variant (Unreported)



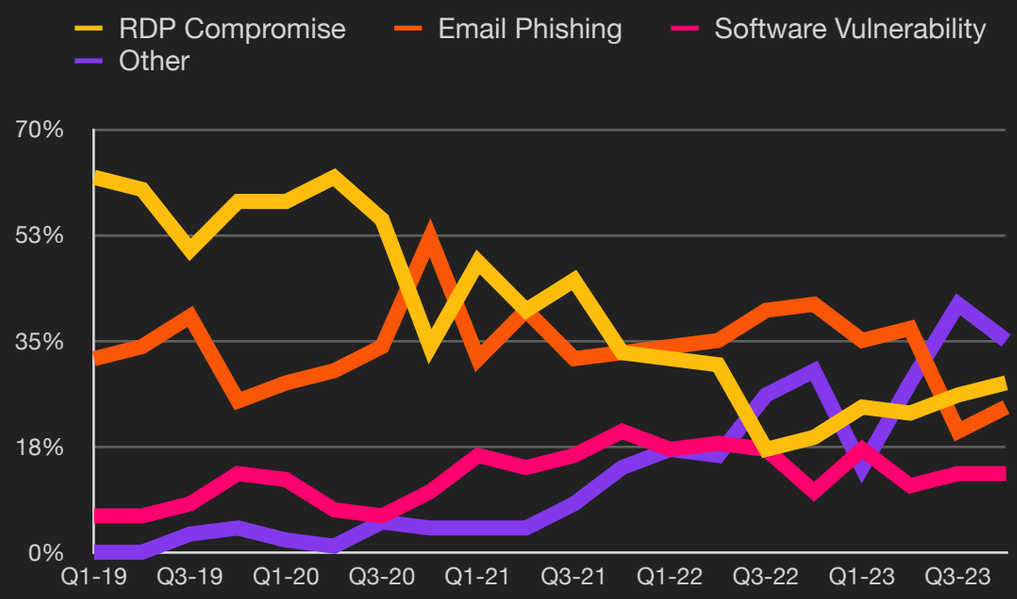
Size of Organization



Exfiltration Techniques

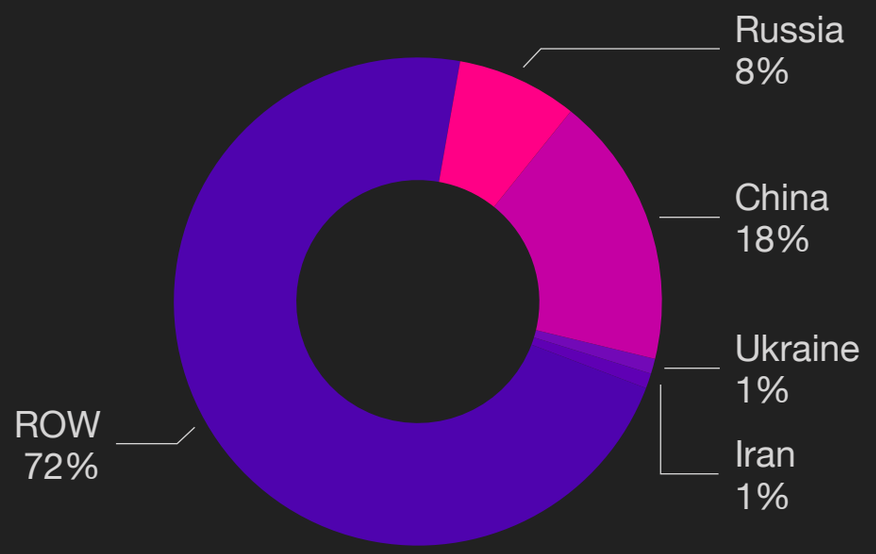


Attack Vectors[2]



[2]Courtesy Coveware

Exfiltration by 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.