June 2023

June was the second busiest month of 2023 with 46 publicly disclosed ransomware attacks recorded, not including the victims of the MOVEit attack. Education and healthcare continue to remain two of the most targeted sectors, with eleven and nine attacks respectively. Data exfiltration remains the tactic of choice as cybercriminals continue to focus on extortion. Beverley Hills Plastic Surgery, University of Manchester and Reddit all made headlines when threat actors threatened to publish troves of personal information exfiltrated during the attacks.

Clop made the majority of ransomware headlines this month following a vulnerability in MOVEit file transfer software. Many prominent organizations fell victim to this attack including British multinational gas & oil company Shell, global accounting firm PwC and a number of US state governments. Those impacted had until June 21st to negotiate with the ransomware group before data was published. The current victim list is massive and growing, and Clop continues to share new entries every day, you can read the victim list in our dedicated MOVEit blog, which is updated with new information as the story unfolds.

Roundup

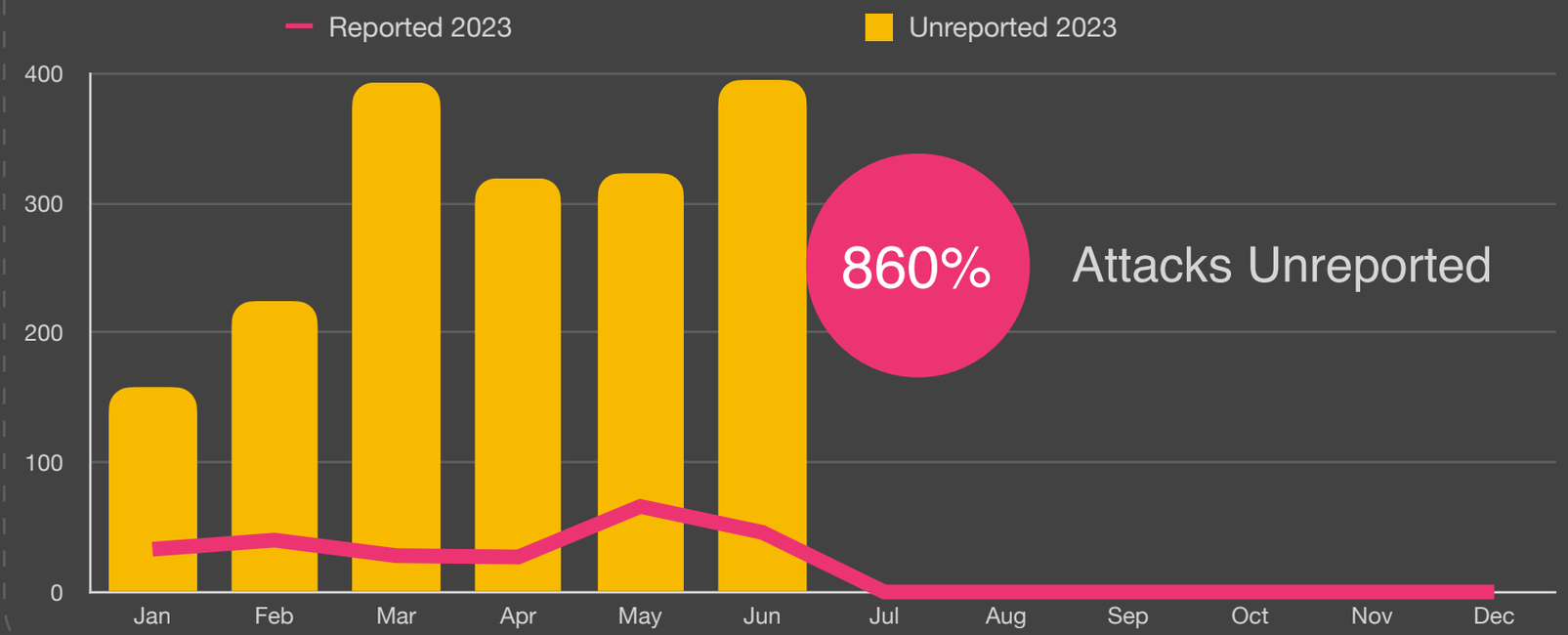
After an all time record in May, June sees a continuation of this trend with the second highest number of ransomware attacks on record with 46 publicly disclosed, and a record 396 undisclosed attacks. This represents a ratio of 8.6:1 of unreported to reported attacks, or 860% going unreported, fueled in part by the MOVEit attack and the CLOP ransomware variant.

This month education, healthcare and manufacturing dominated, with increases of 25%, 26% and 27% respectively. Government attacks showed one of the smallest increases of the year of only 12.5% but remains the third highest targeted sector.

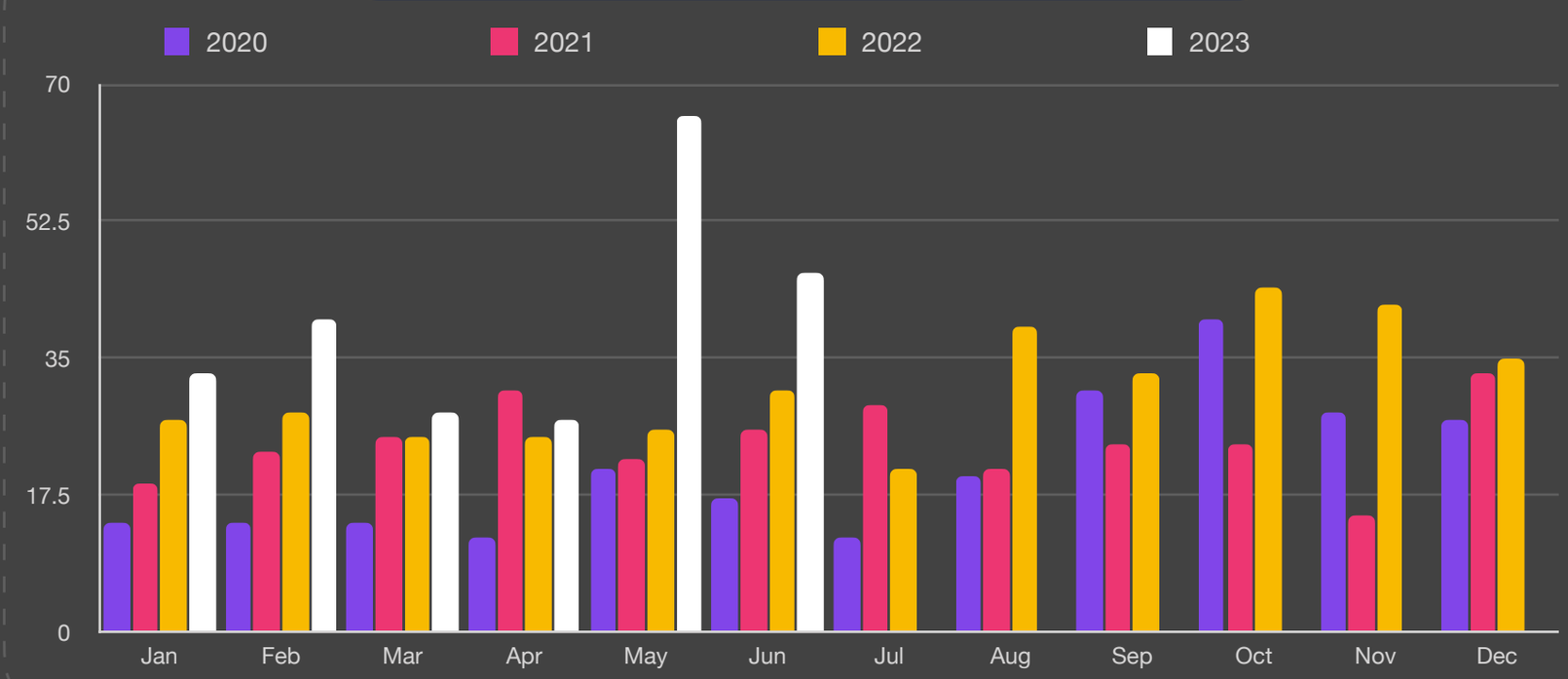
In June, BlackCat and LockBit were the two dominant variants at 18.1% and 16.8% respectively. This closely mirrors the the unreported attack variants, representing 50% of all successful attacks. With the sheer volume of attacks from CLOP we expect this to change over the coming months.

Finally, we saw illegal networks continue to dominate exfiltration techniques with 97% of all attacks. A large majority of ransomware is now originating and exfiltrating data to China 43% of the time, with Russia at 10%.

Unreported Ransom Attacks



Reported Ransomware by Month



Key Trends

860% Unreported

Jun Highest Unreported of 2023

2nd 2nd Highest Reported Ever

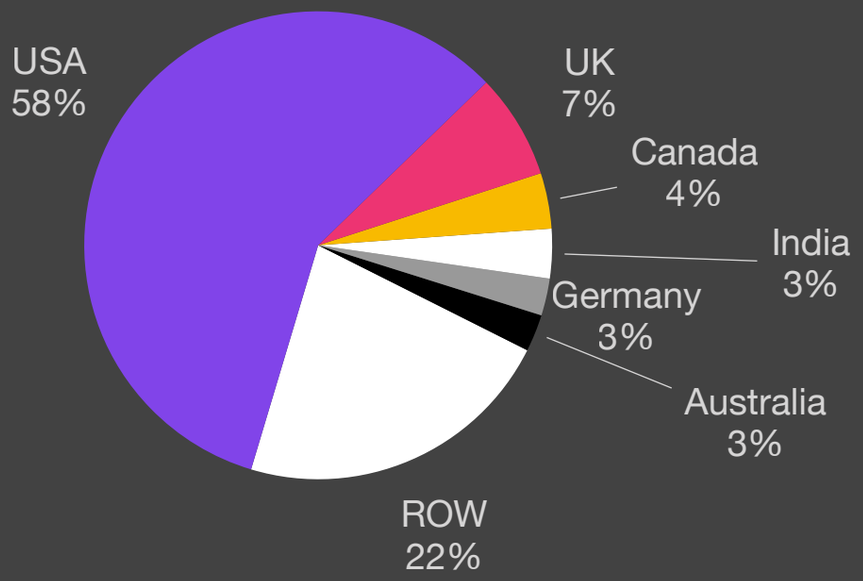
69% of all attacks use PowerShell

89% of attacks exfiltrate data

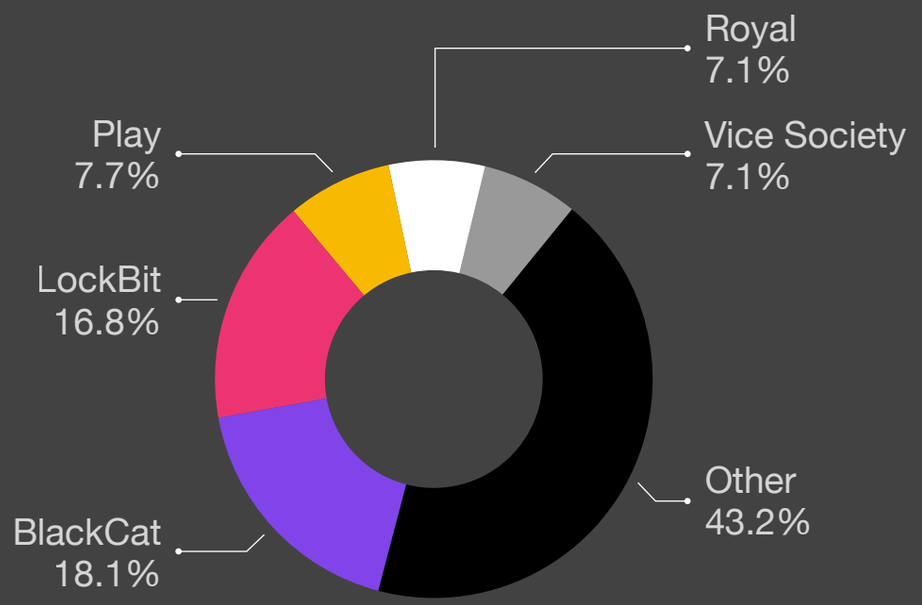
Average payout US $327,883k

-20% from Q4/22

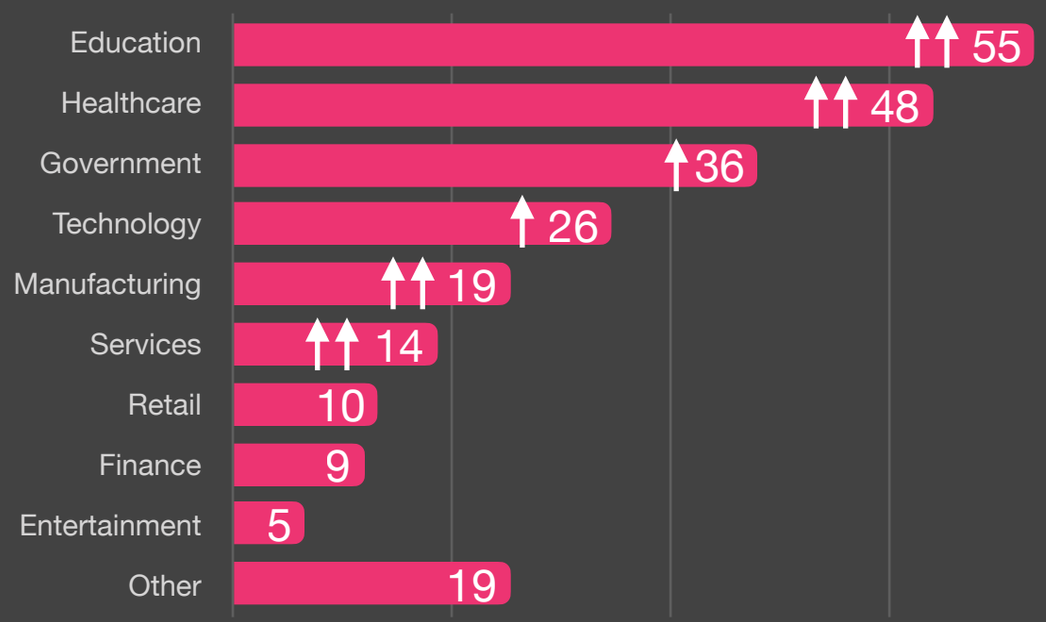
Ransomware by Country



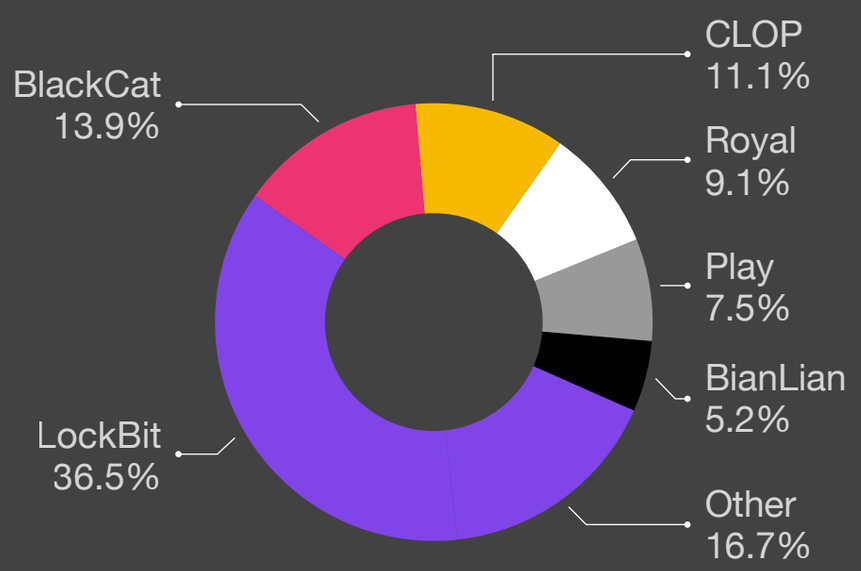
Reported Ransomware Variant



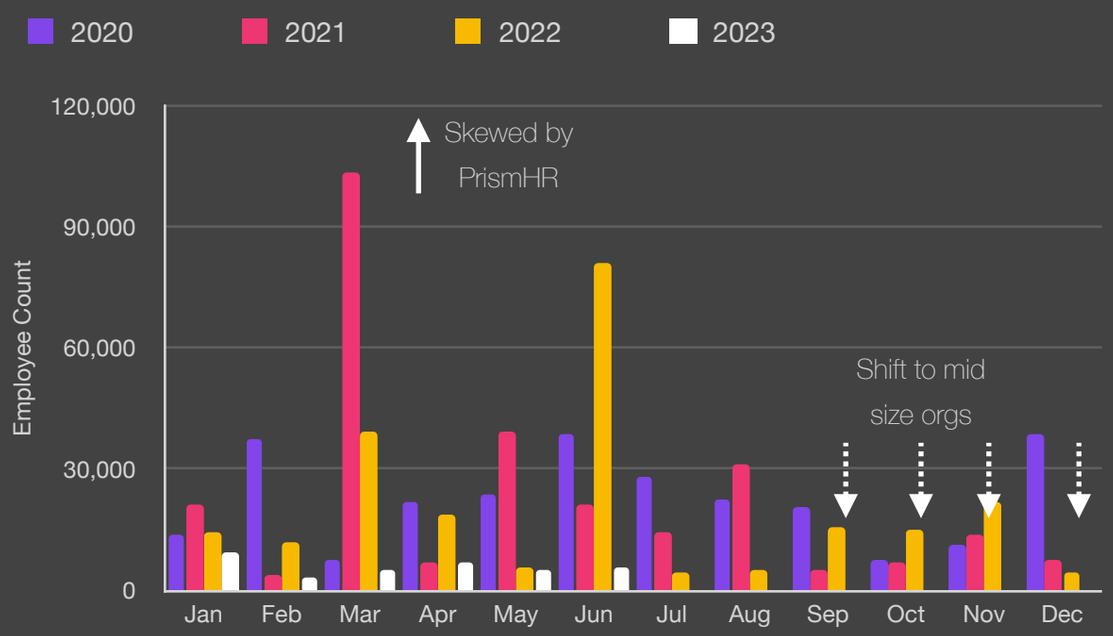
Ransomware by Industry



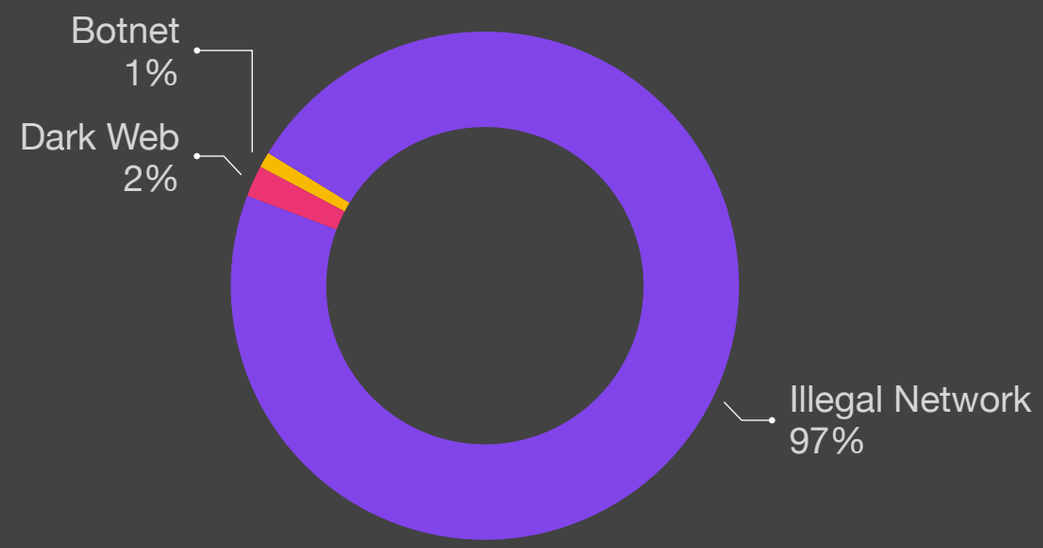
Unreported Ransomware Variant



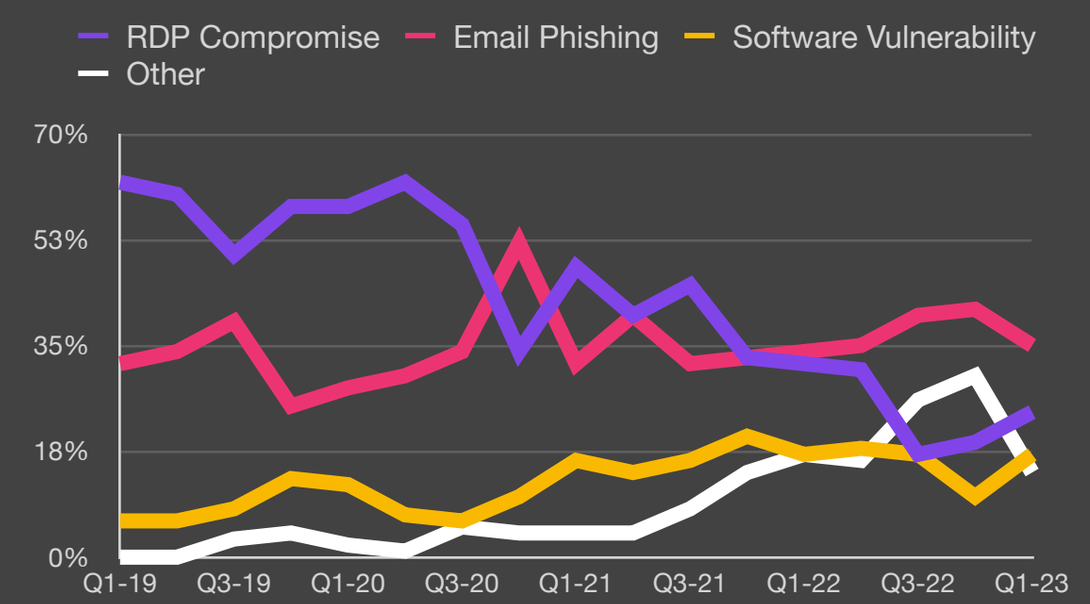
Size of Organization



Exfiltration Techniques

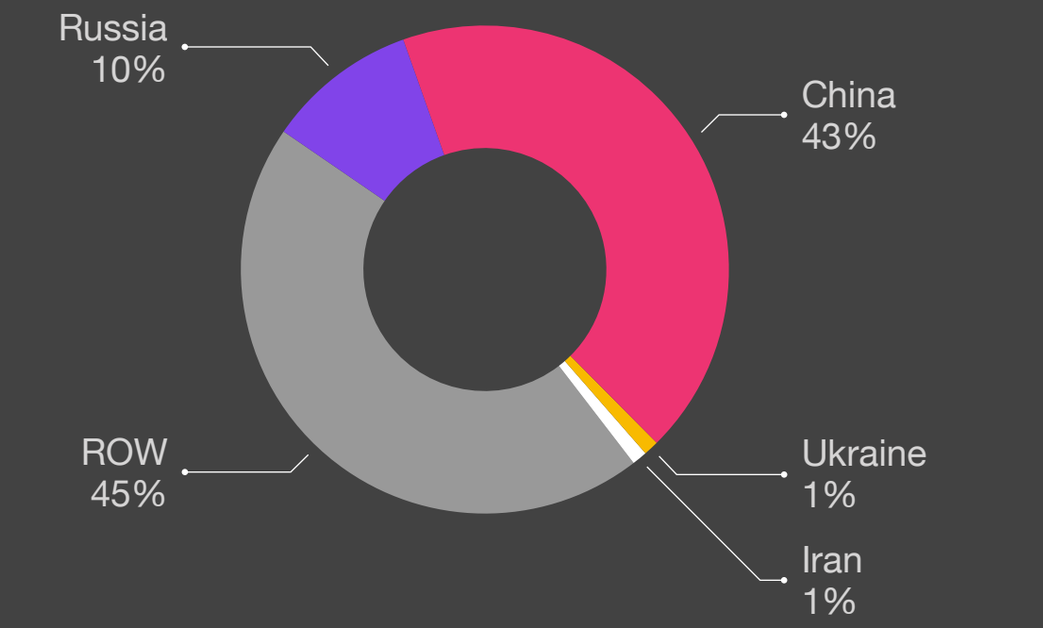


Attack Vectors[2]



[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.