Introduction

This month seen some big stories make the headlines including Qilin's attack on Synnovis causing major disruption to NHS hospitals in London and BlackSuit's attack on CDK Global, forcing hundreds of car dealerships across North America offline. LockBit was the most active variant, claiming responsibility for 13% of June's incidents. Healthcare was the highest targeted industry reporting 12 attacks, closely followed by government with 10 attacks.

Roundup

In June we saw an easing of the overall threat numbers for the year with 45 total attacks. Historically still very high, it represents the second highest June on record. It demonstrates just how normalized these attacks have become. Despite the lower number of attacks for the month, the ratio of unreported attacks remains high at 774%, reflecting the sheer volume of attacks that still go unreported.

Healthcare takes center stage this month with and increase of 25% from May, followed by government and technology with increases of 23% and 21% respectively. Unlike most months the education sector took a well earned break from the record books with only an 8% increase.

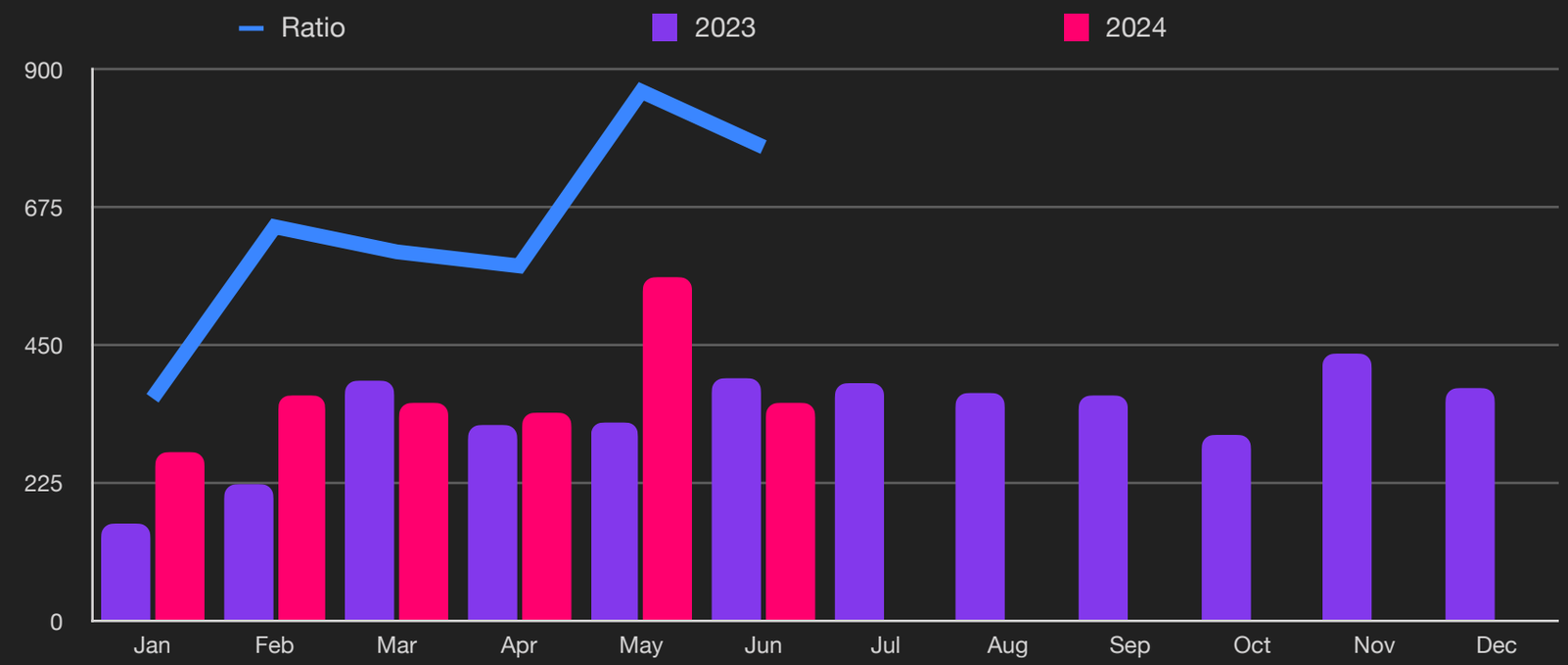
In terms of variants, Play was the biggest mover this month with a 33% increase in attacks followed by Black Basta and Medusa with 14% and 13% respectively. This follows the large increase in unreported attacks from Medusa last month, typically a leading indicator of disclosed attacks in subsequent months. While Lockbit is still the leading variant by a significant margin, we only saw a modest gain of 3% this month.

Finally, data exfiltration is now involved in 93% of all attacks with PowerShell the leading vector at 62%, an 11% gain from the previous month. China and Russia also continue to dominate as the leading destinations for exfiltrated data with 15% and 6% respectively.

BlackFog State of Ransomware Report

June 2024

Unreported Ransomware Attacks



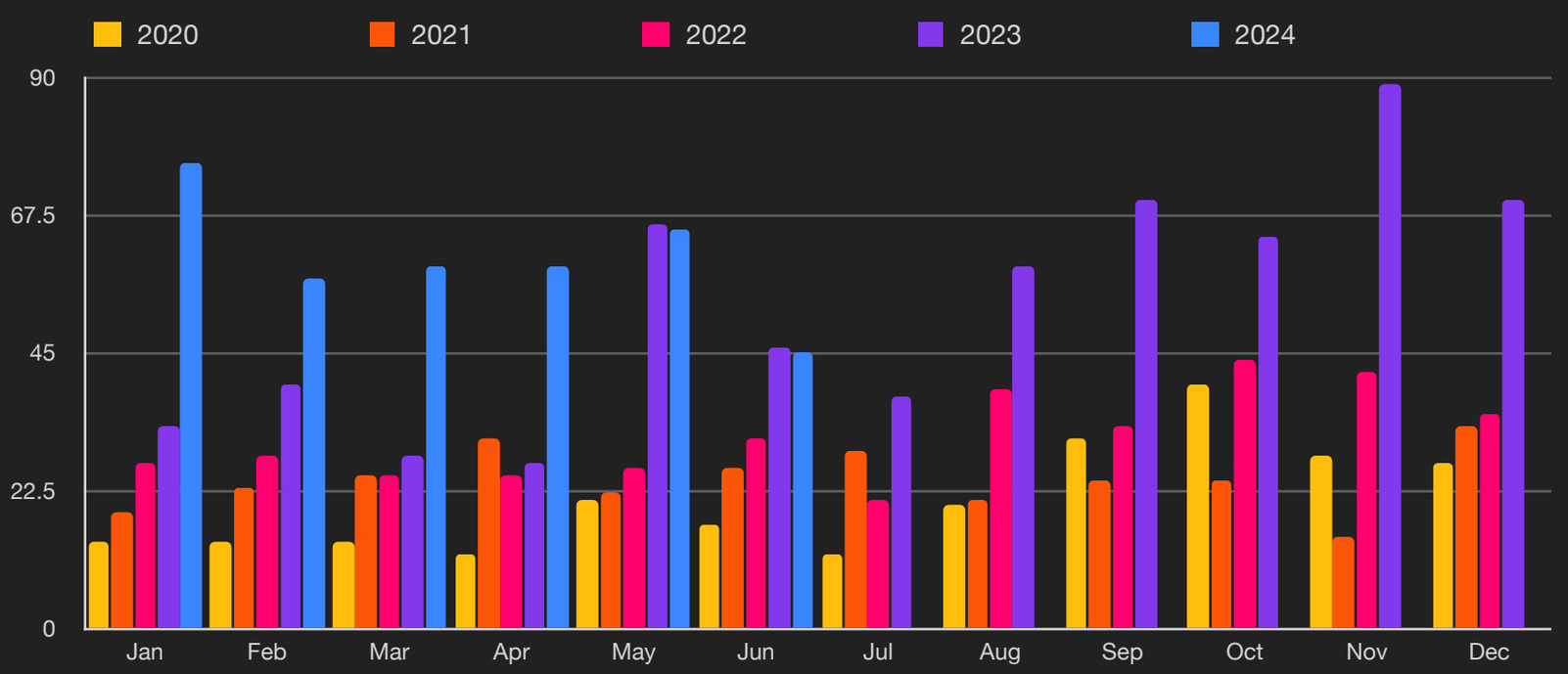
Key Trends

774% Unreported

2nd Highest June

Lowest of Year

Reported Ransomware by Month



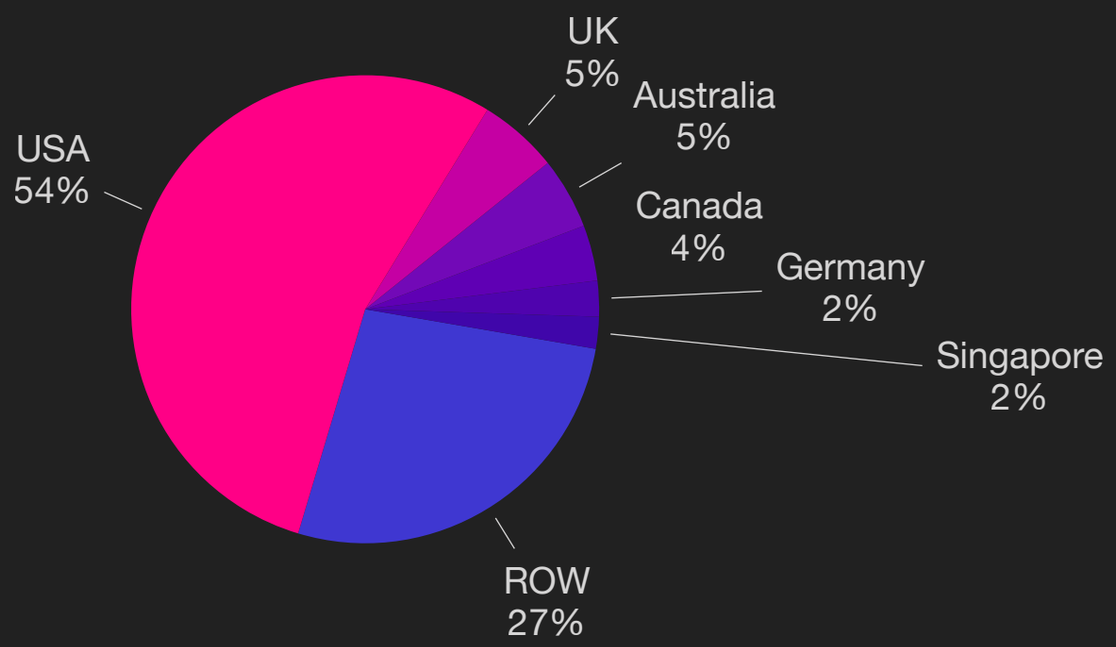
62% of all attacks use PowerShell

93% of attacks exfiltrate data

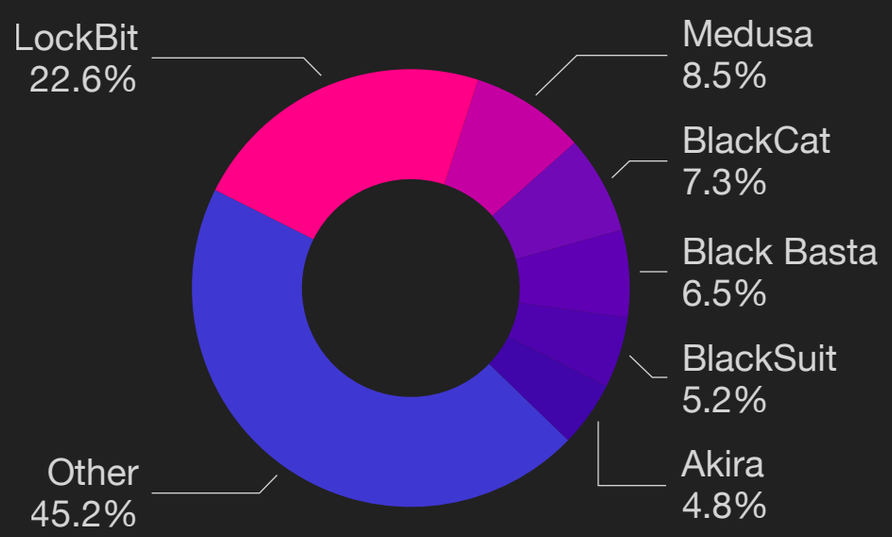
Average payout US $381,980

-32% from Q4/23

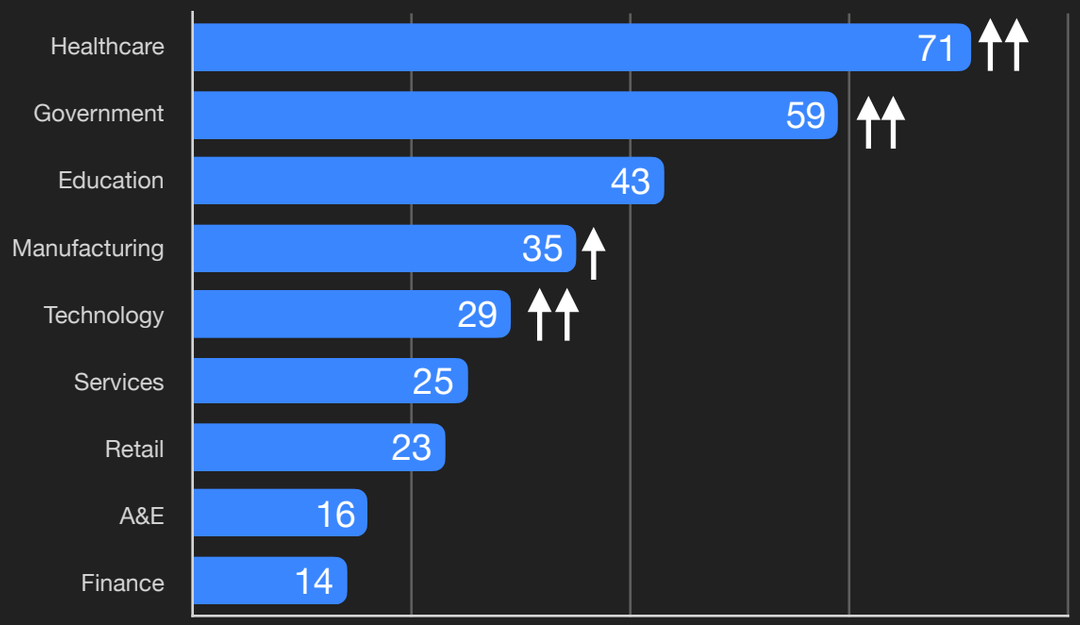
Ransomware by Country



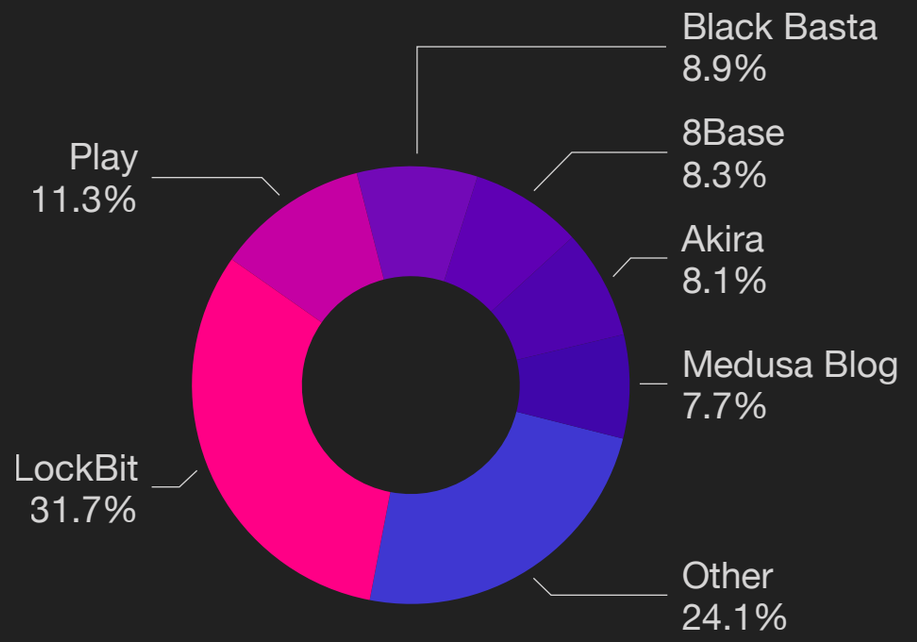
Ransomware Variant (Reported)



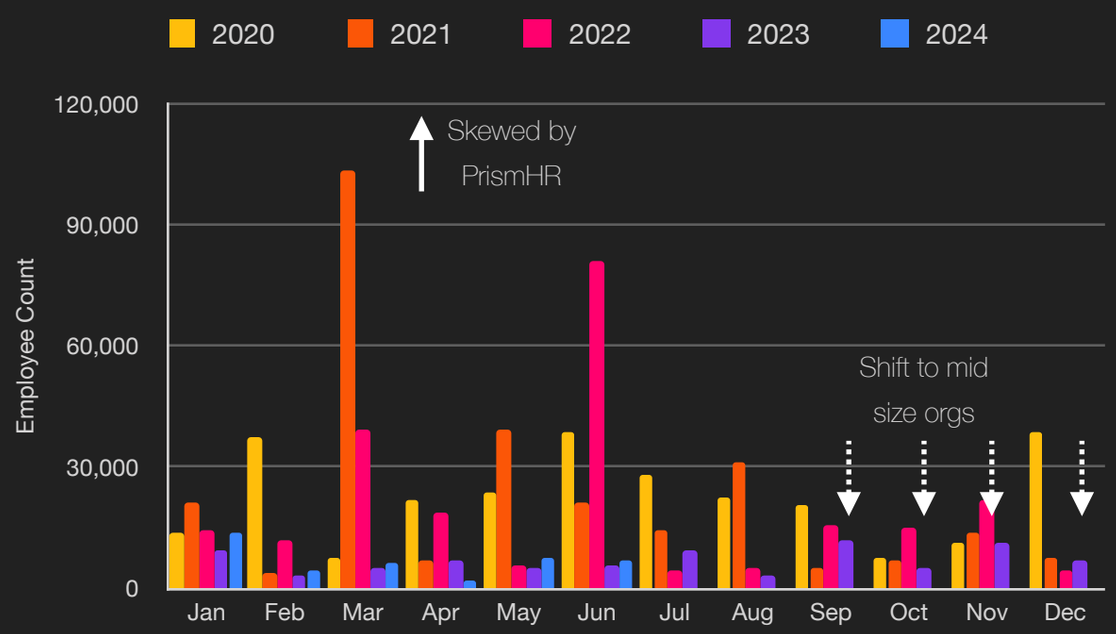
Ransomware by Industry



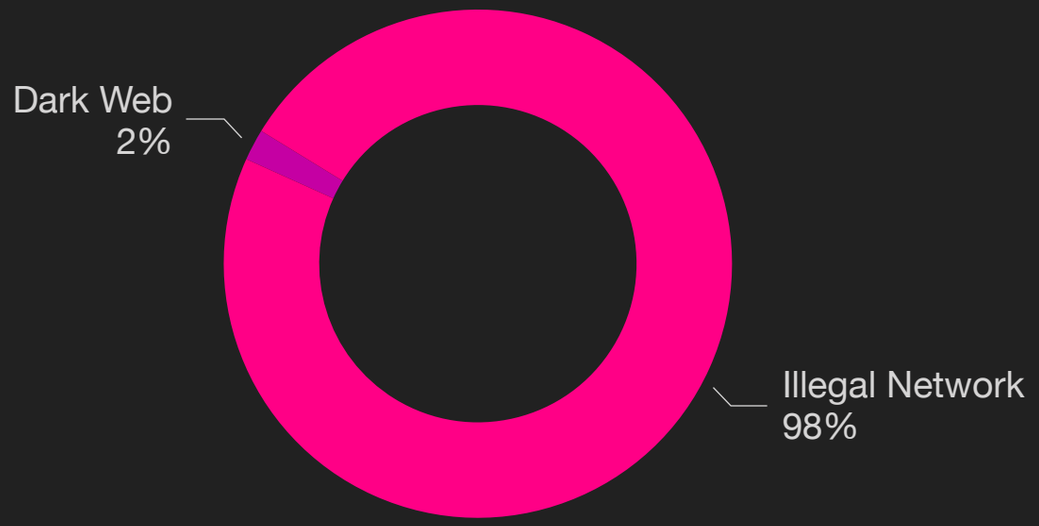
Ransomware Variant (Unreported)



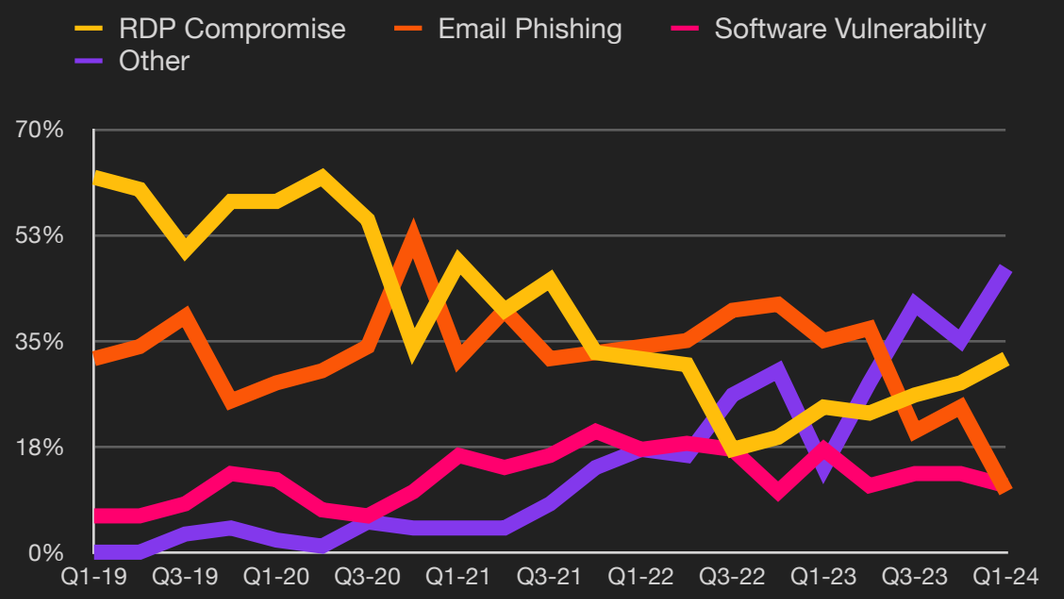
Size of Organization



Exfiltration Techniques

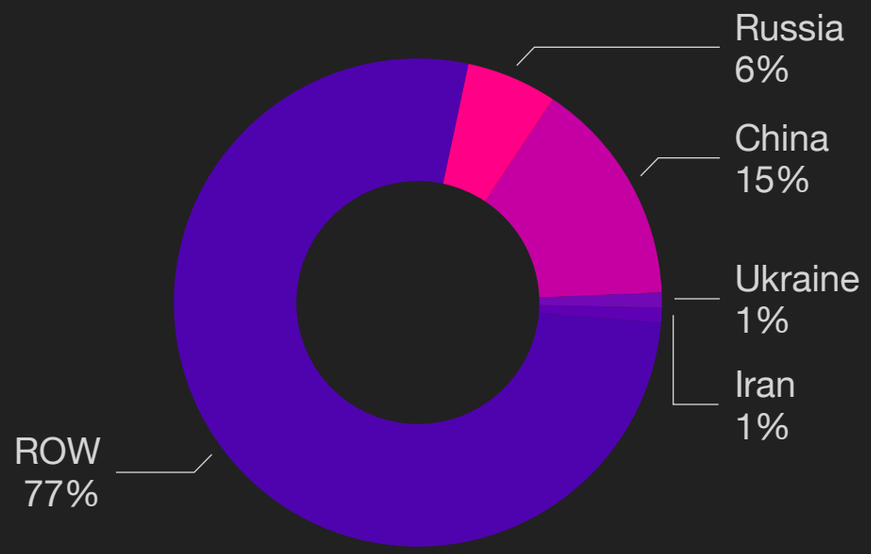


Attack Vectors[2]



[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.