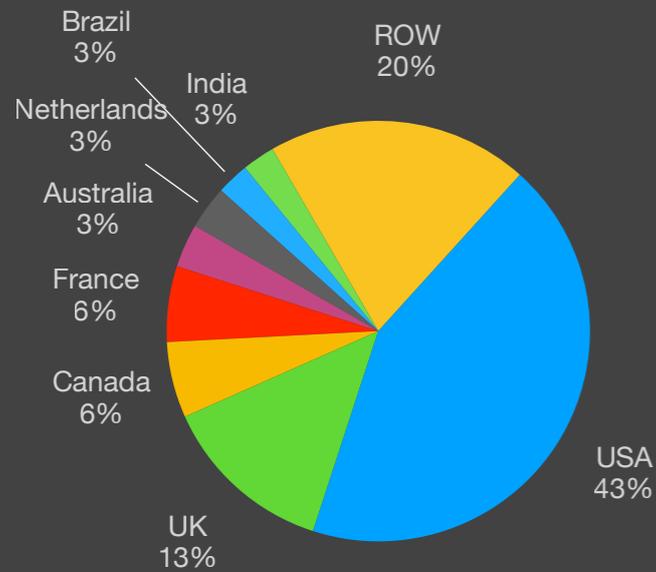
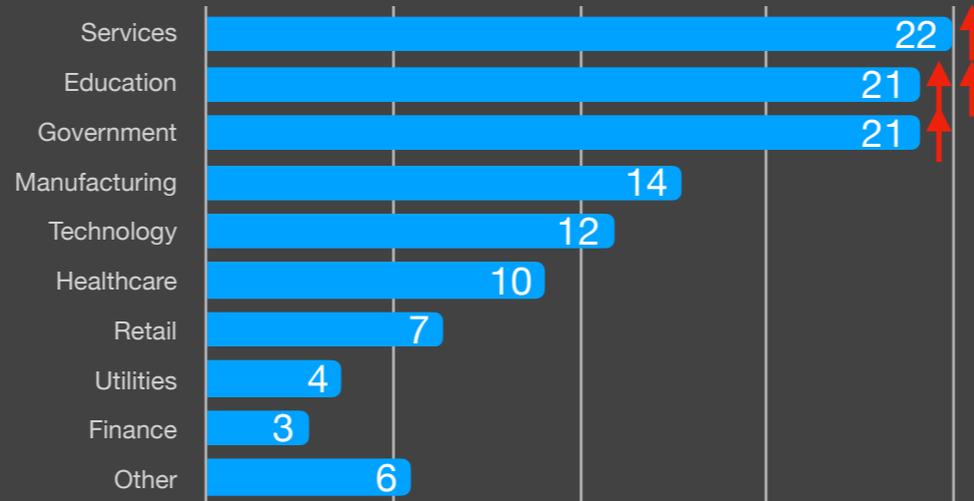


In May we uncovered 22 ransomware attacks, up just one from May 2020. The most high-profile attack of the month goes to Colonial Pipeline. An attack on the largest fuel pipeline in the US made headlines worldwide and caused havoc throughout several states in the US as the outages caused a shortage of gas. Here's a snapshot of what other attacks made headlines during the month.

Ransomware by Country



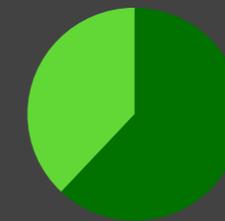
Ransomware by Industry



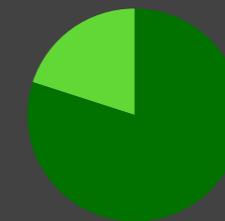
Key Trends

Average ransomware payment

US\$220,298 **+43% from Q4/20**

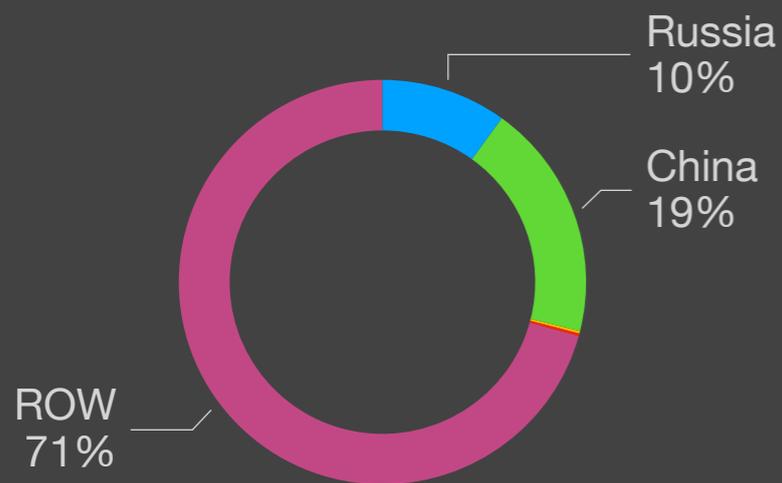


↑ 85% of all attacks Ransomware

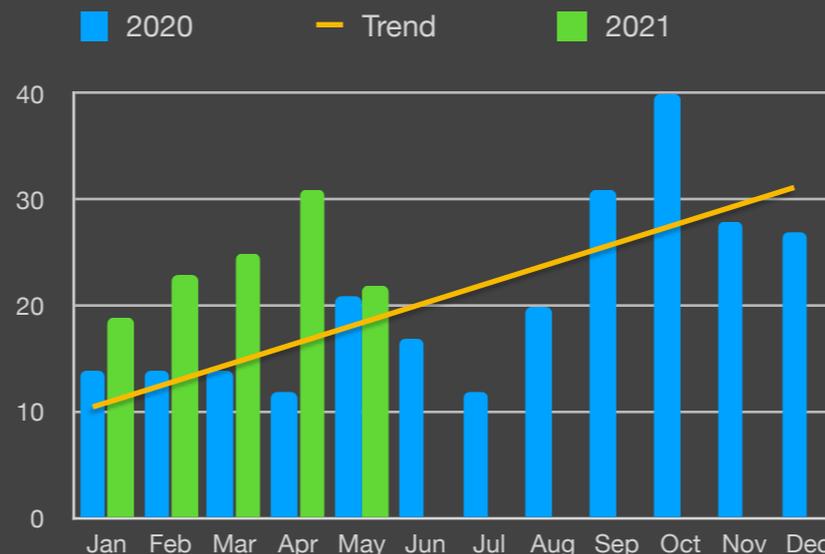


77% of attacks exfiltrate data

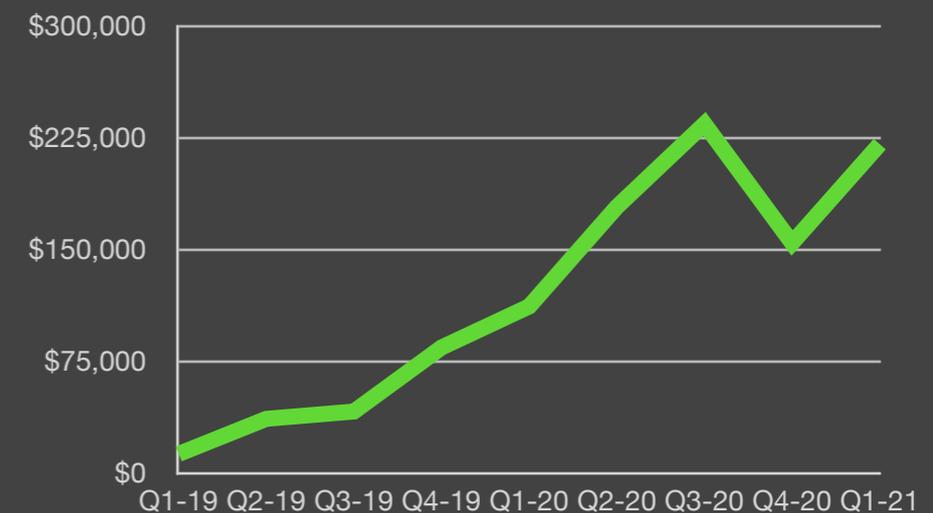
Ransomware Exfiltration



Ransomware Trend by Month

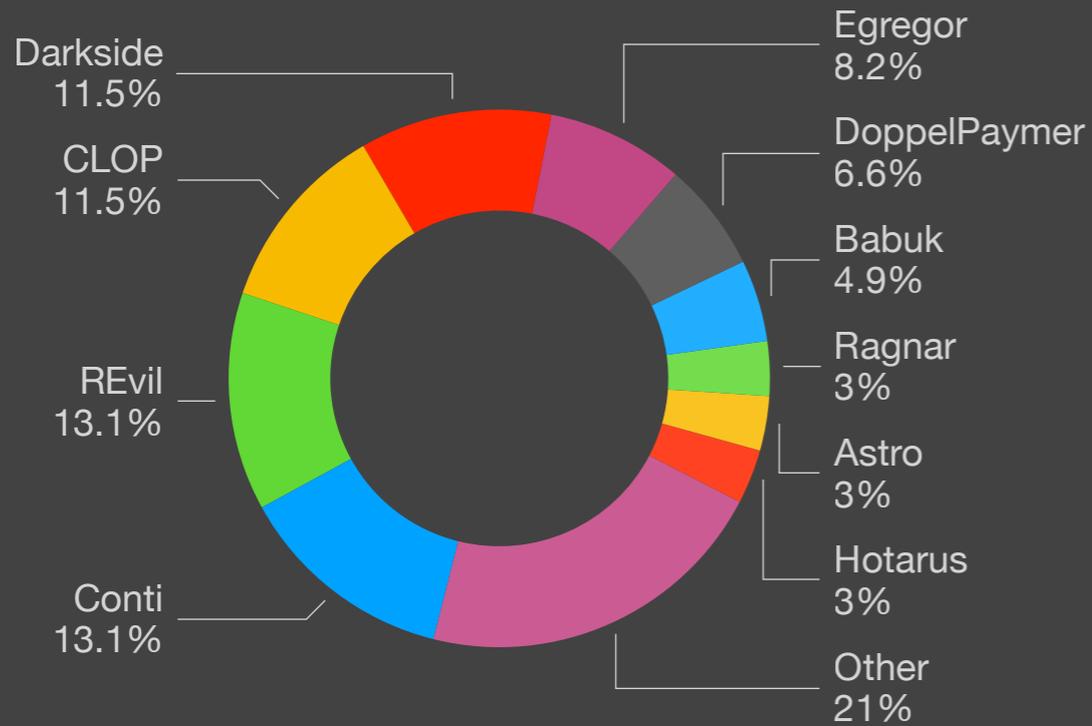


Average Ransom Payout¹

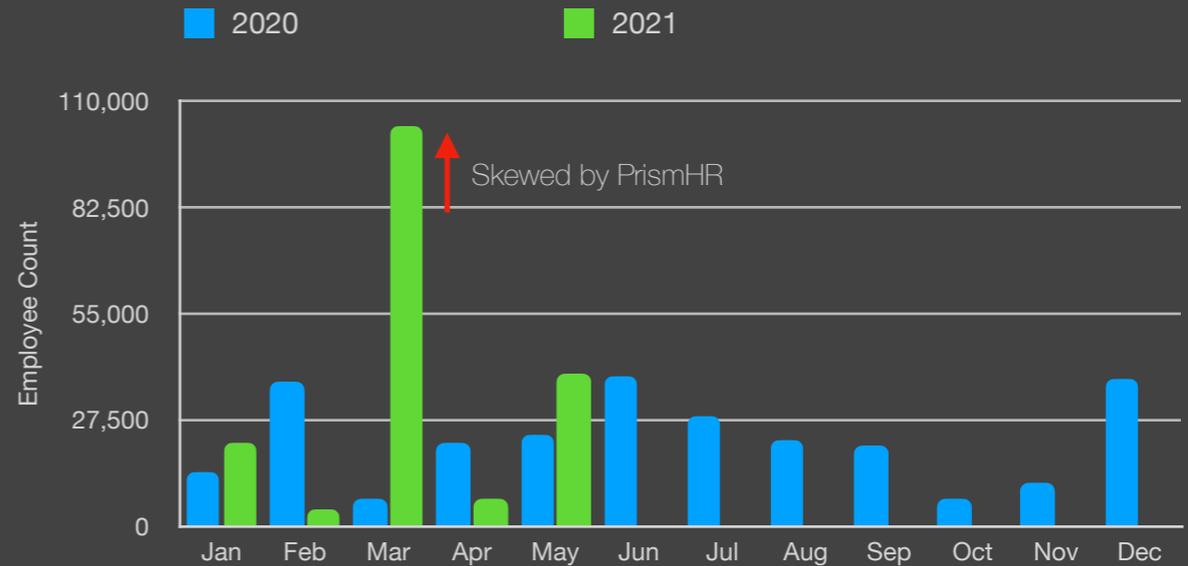


¹Courtesy Coveware

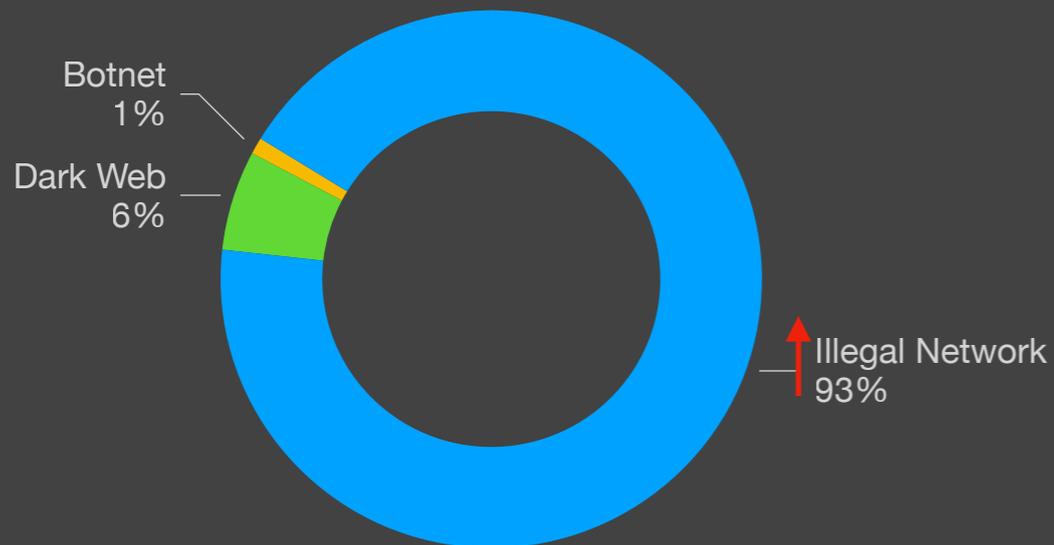
Threats by Variant



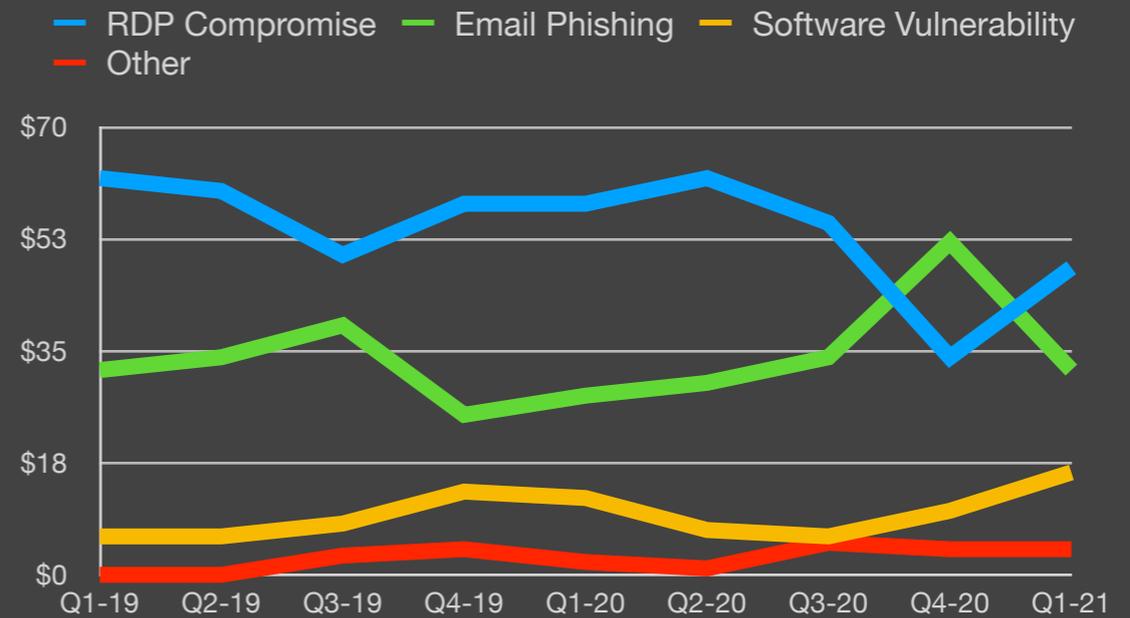
Average Size of Organization



Ransomware Exfiltration Techniques



Common Attack Vectors²



²Courtesy Coveware



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.