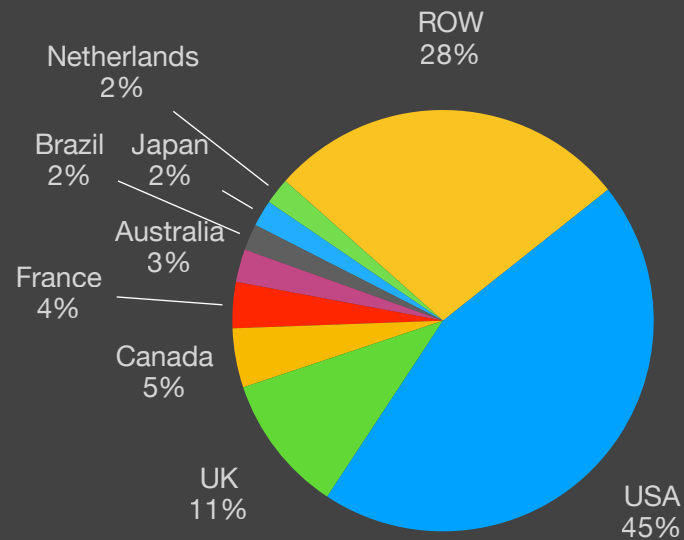
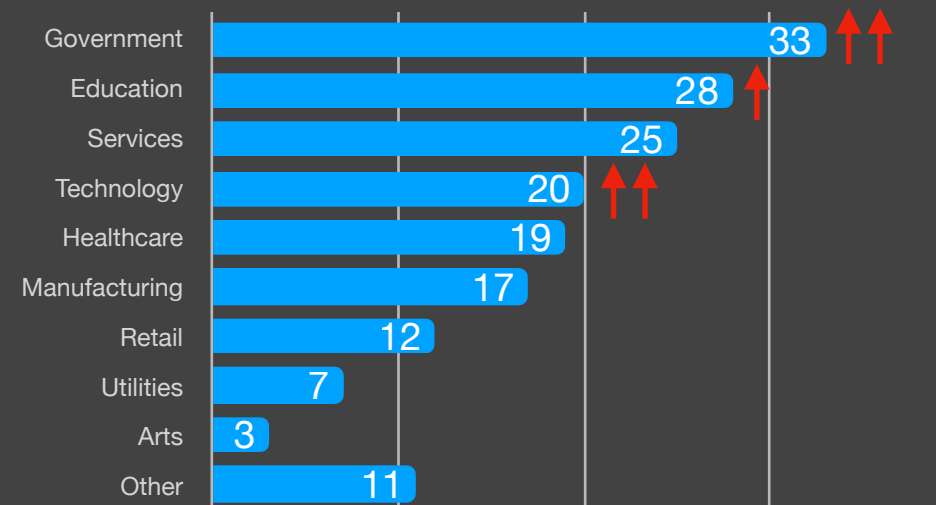


July racked up 29 ransomware attacks, up from just 12 reported in the same month last year. The REvil gang was particularly busy with their attack on Kaseya which resulted in a 70 million USD ransom. The incident affected up to 1500 organizations including a large chain of supermarkets in Sweden, an animal hospital in Maine and a school district in Tennessee. In an interesting turn of events the Babuk gang became victims of ransomware at the hands of an unknown group who took control of their Dark Web forum and demanded a \$5000 ransom which they refused to pay.

Ransomware by Country



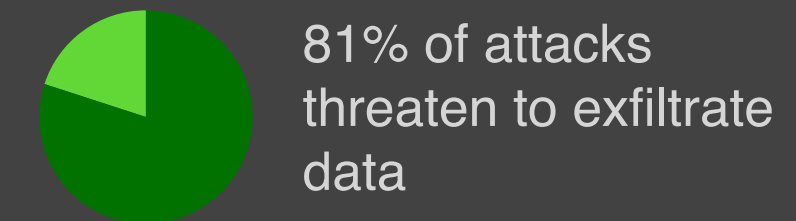
Ransomware by Industry



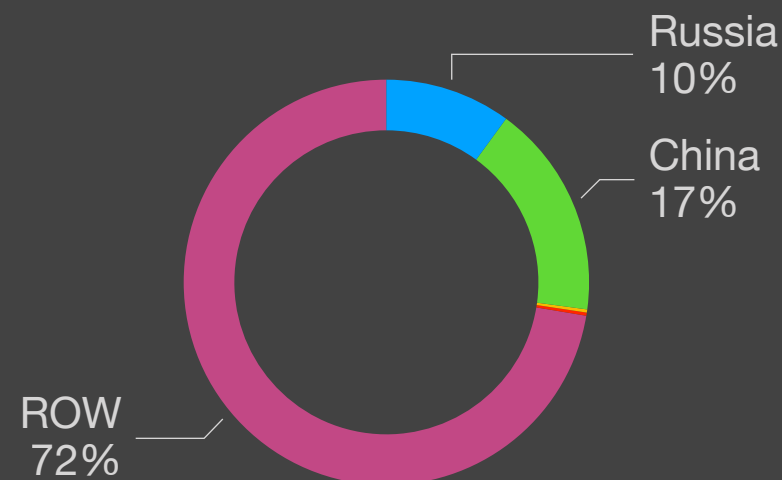
Key Trends

Average ransomware payment

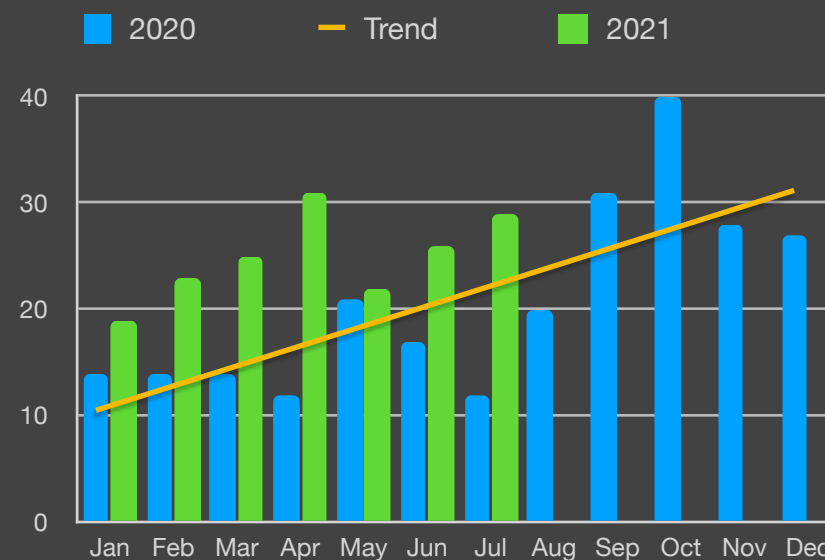
US\$135,576 -38% from Q1/21



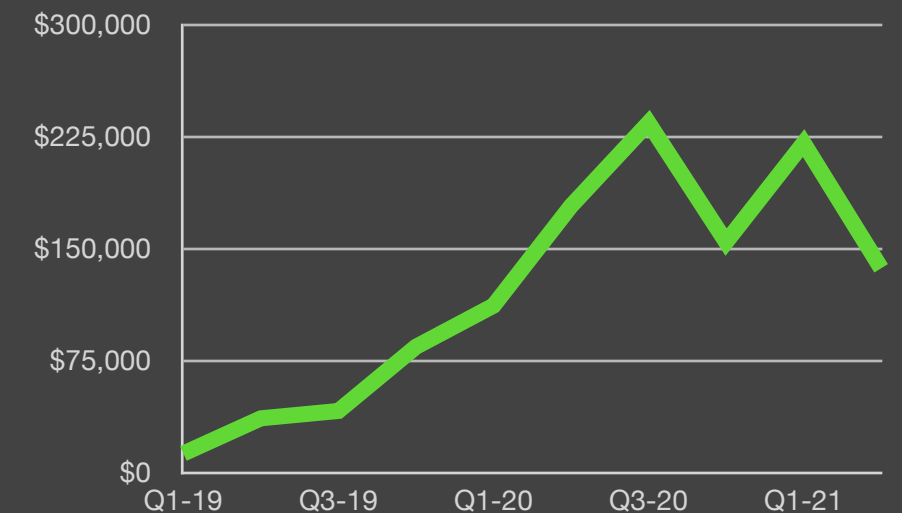
Ransomware Exfiltration



Ransomware Trend by Month

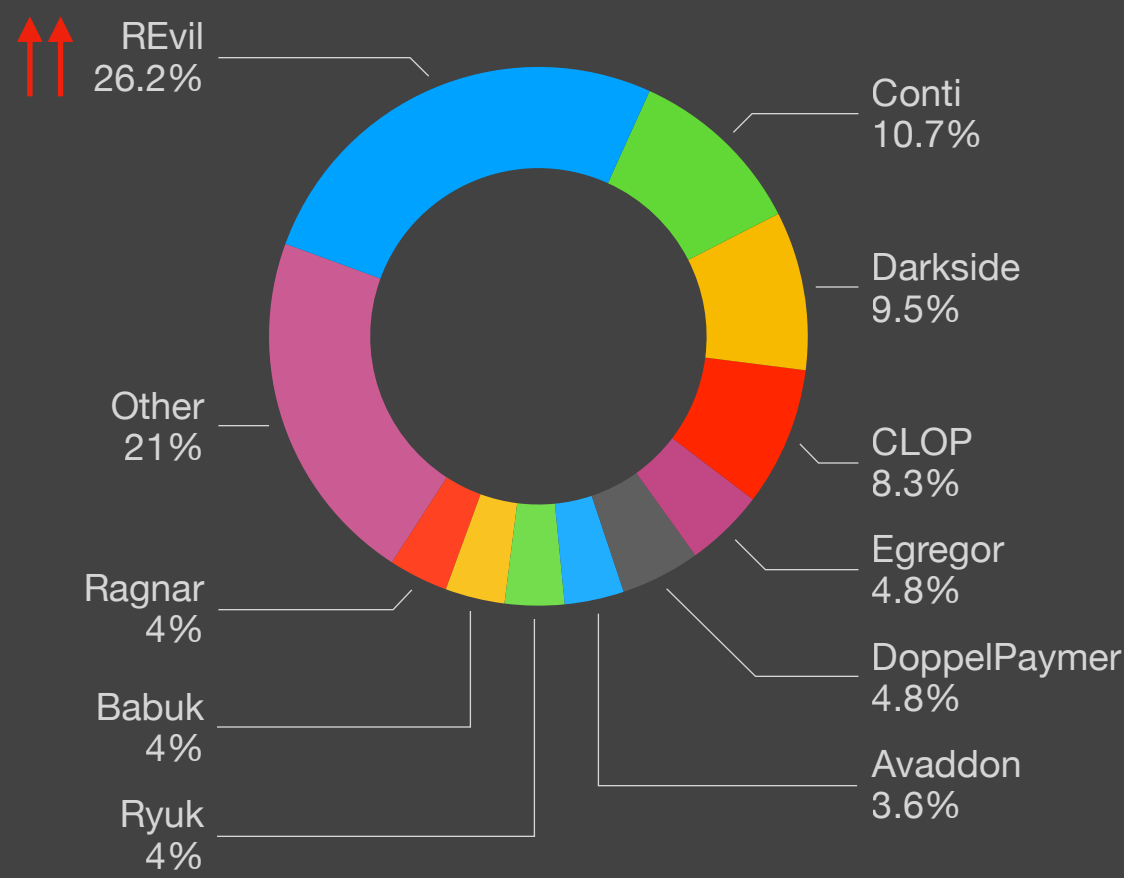


Average Ransom Payout¹

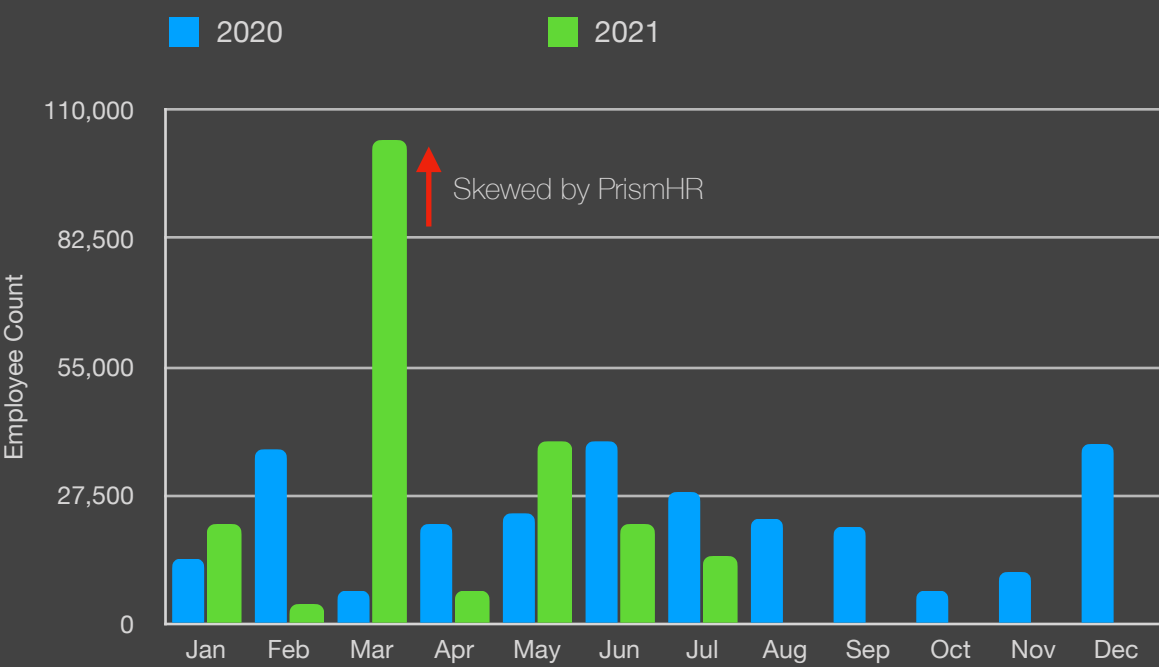


¹Courtesy Coveware

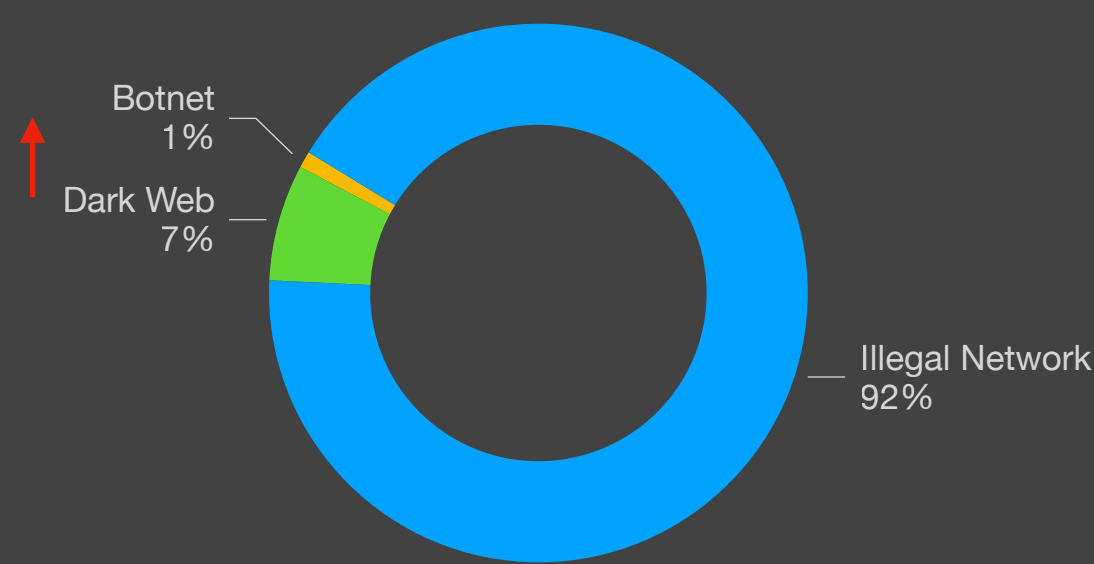
Threats by Variant



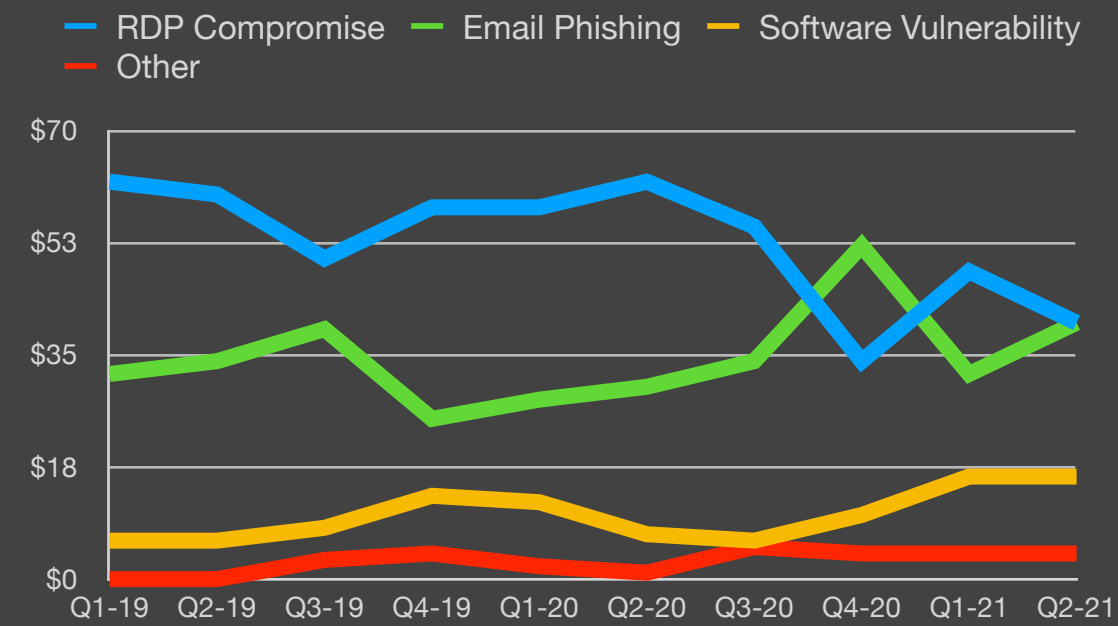
Average Size of Organization



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.