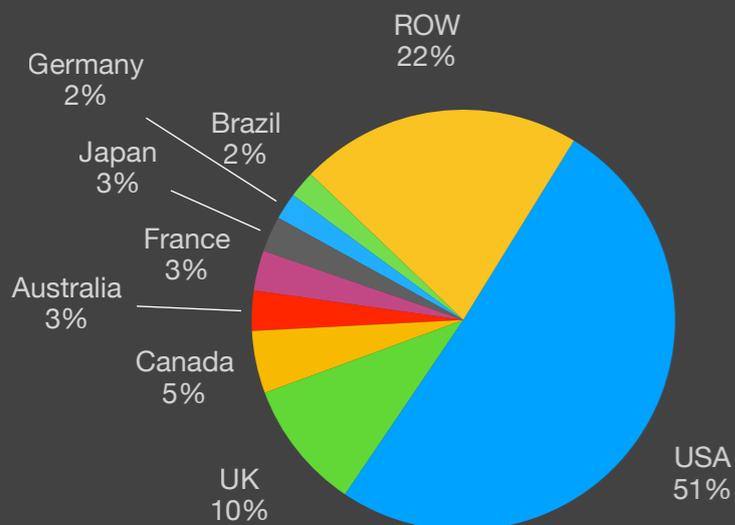


December was the busiest month of 2021 with 33 ransomware attacks being publicly reported. We saw several high profile attacks including car manufacturer Volvo who lost R&D when they were hit with ransomware, and Nordic Choice Hotels whose guests found themselves locked out of their hotel rooms following an attack by the Conti gang. Perhaps the most interesting was an incident at tech company Asurian where a former disgruntled employee stole a company laptop and exfiltrated data before posing as an anonymous ransomware hacker, extorting them out of \$300,000!

## Ransomware by Country



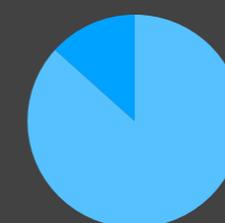
## Ransomware by Industry



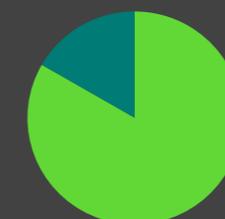
## Key Trends

Average ransomware payment

US\$139,739 +2.3% from Q2/21

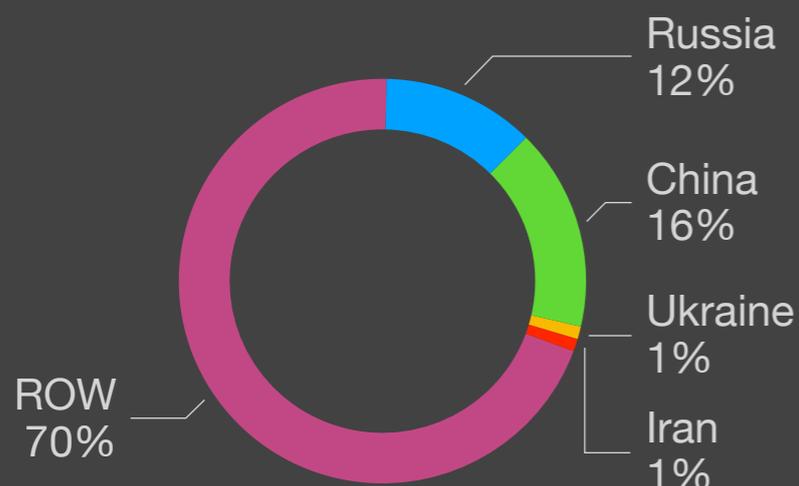


80% of all attacks use PowerShell

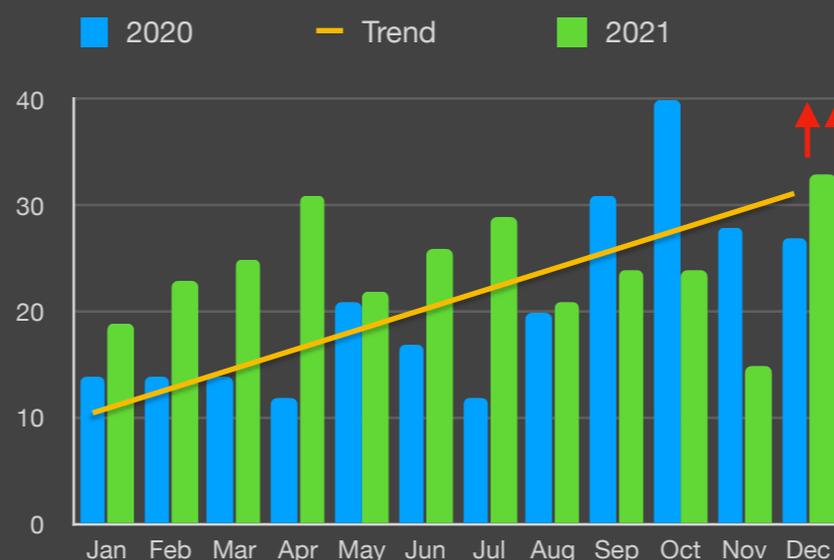


80% of ransomware attacks exfiltrate data

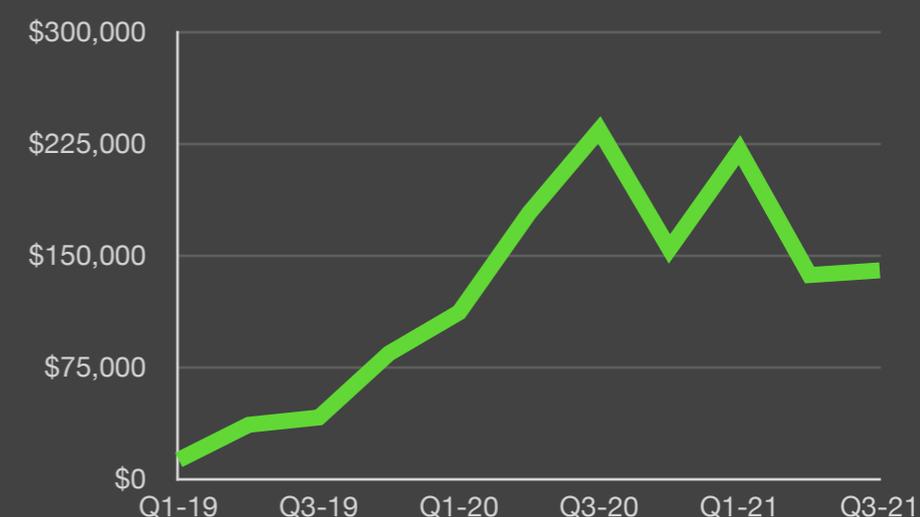
## Ransomware Exfiltration



## Ransomware Trend by Month

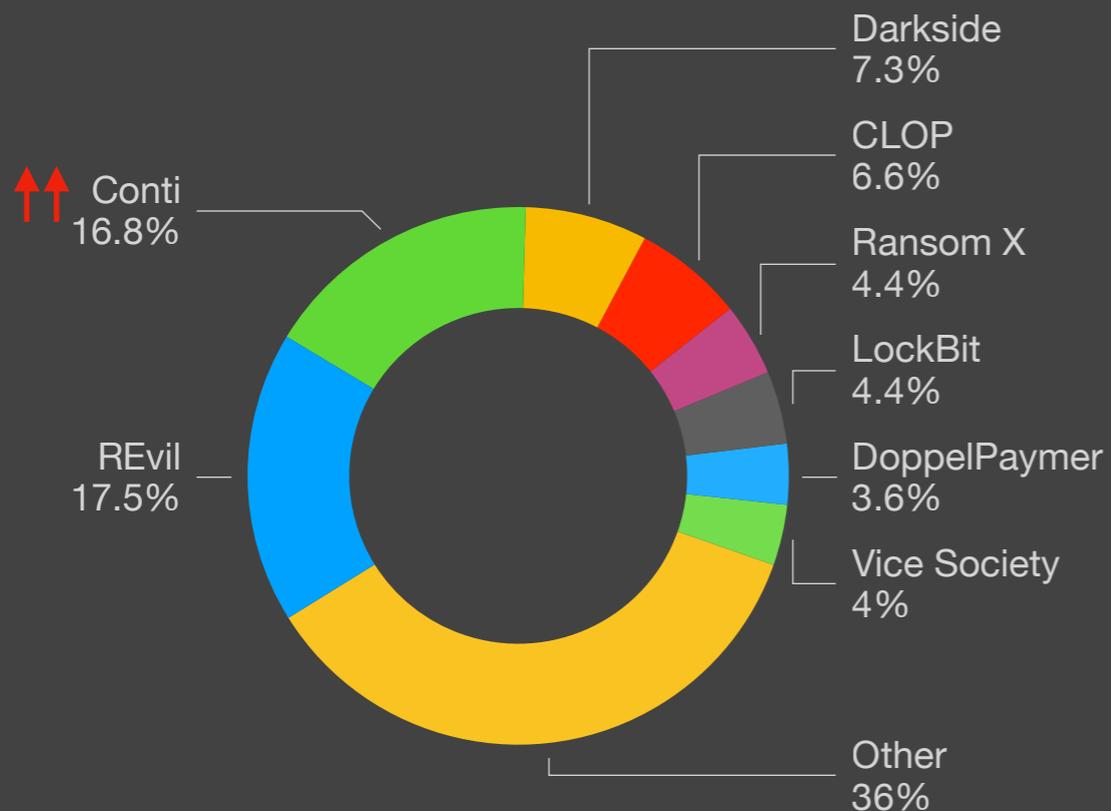


## Average Ransom Payout<sup>1</sup>

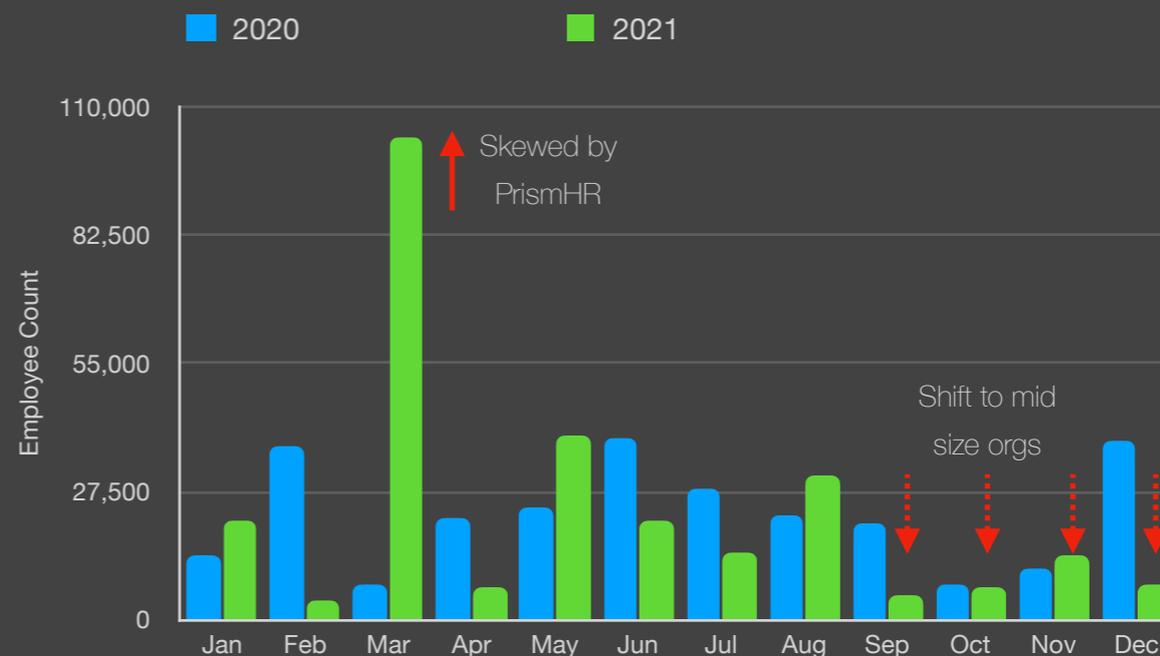


<sup>1</sup>Courtesy Coveware

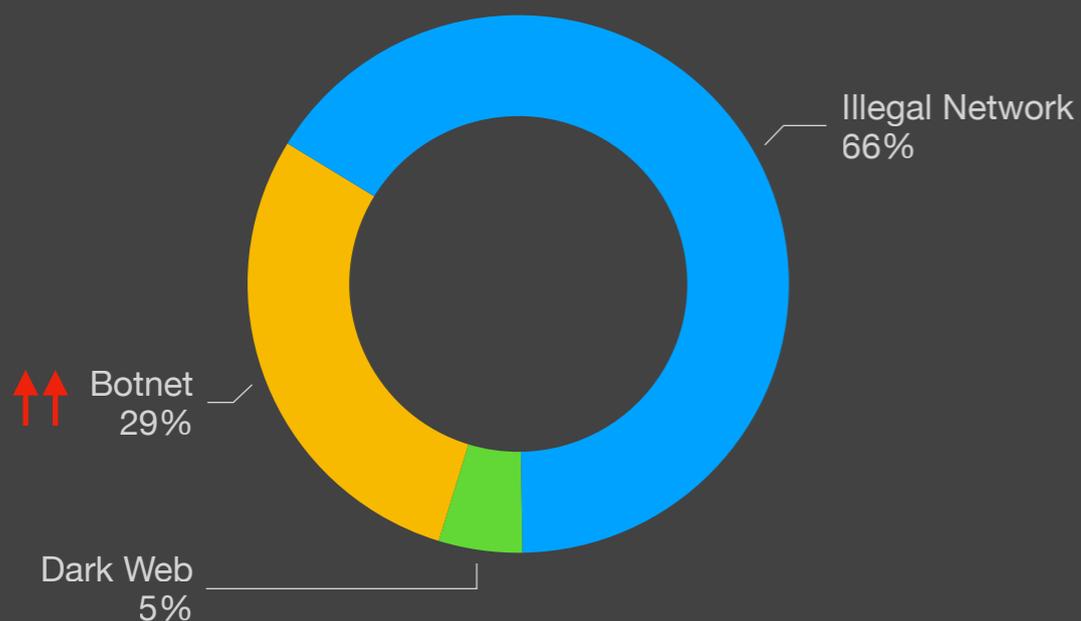
### Threats by Variant



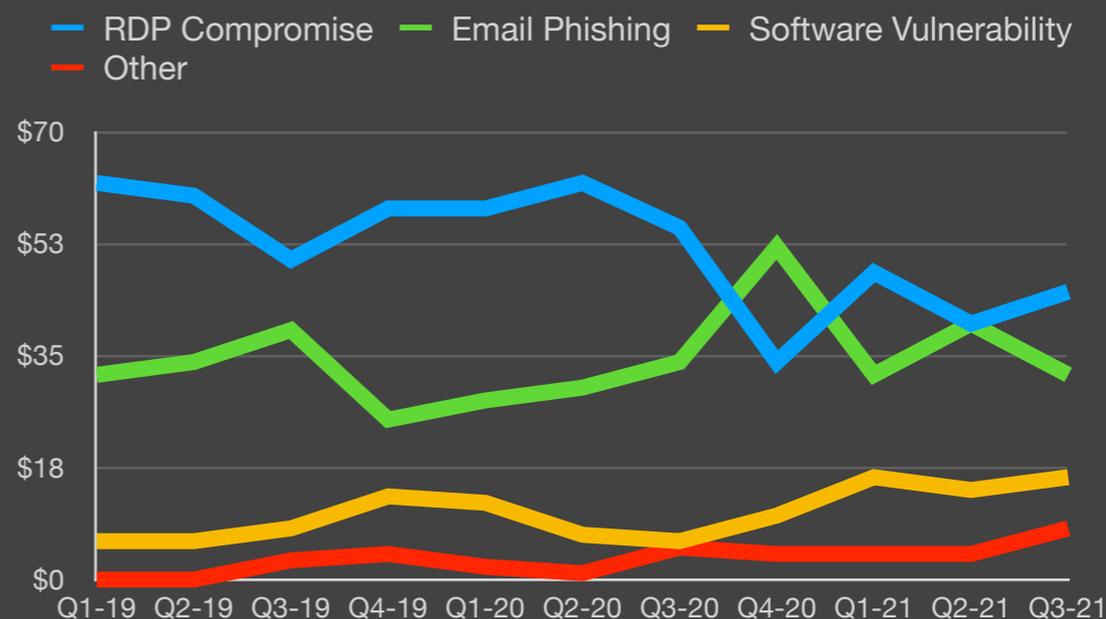
### Average Size of Organization



### Ransomware Exfiltration Techniques



### Common Attack Vectors<sup>2</sup>



<sup>2</sup>Courtesy 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.