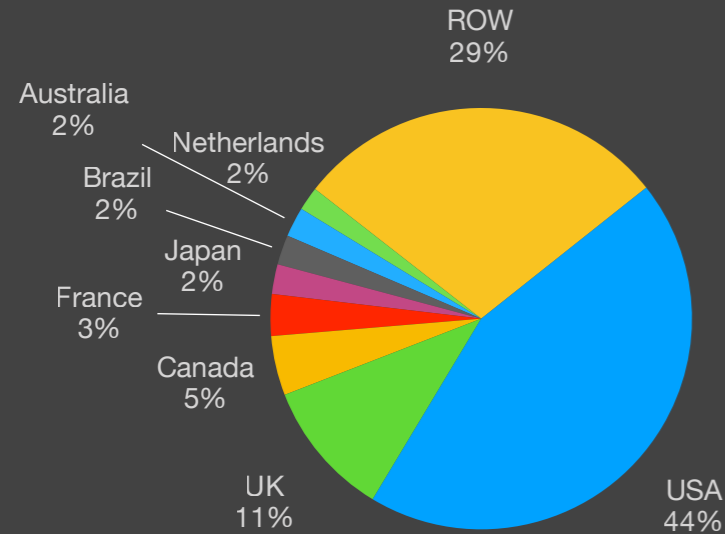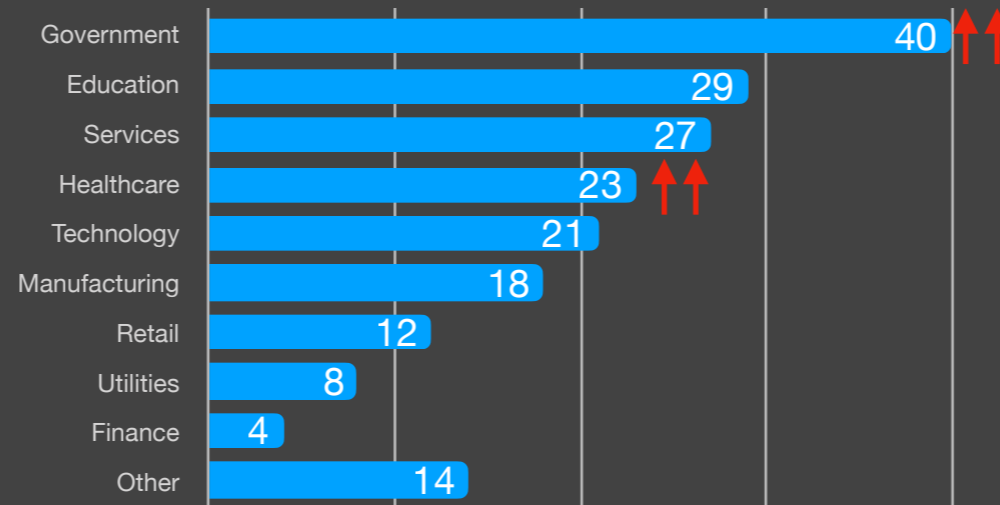In August we uncovered 21 reported ransomware attacks with government and healthcare being the most targeted during the month. The first healthcare incident took place in Italy where the Italian vaccination registration system was taken offline by RansomEXX. While US based Eskenazi Health and Memorial Health System were forced to divert ambulances and cancel procedures due to ransomware attacks.
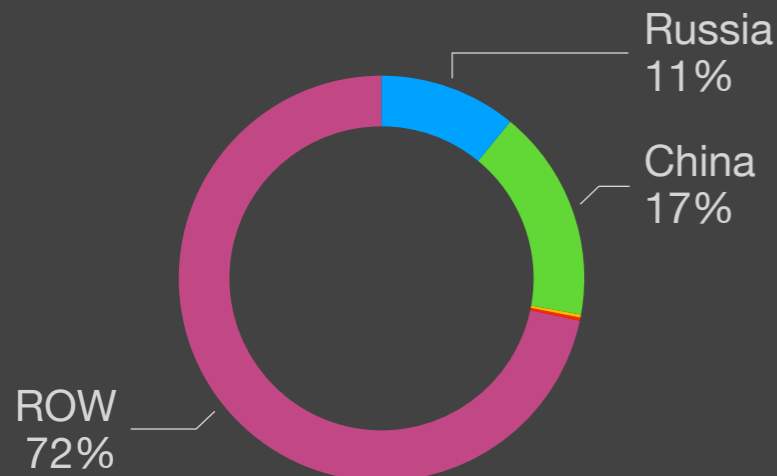
Ransomware by Country

- ROW 29%
- Australia 2%
- Netherlands 2%
- Brazil 2%
- Japan 2%
- France 3%
- Canada 5%
- UK 11%
- USA 44%

Ransomware by Industry

- Government 40 ↑↑
- Education 29
- Services 27
- Healthcare 23 ↑↑
- Technology 21
- Manufacturing 18
- Retail 12
- Utilities 8
- Finance 4
- Other 14

Key Trends

Average ransomware payment

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

↑ 85% of all attacks Ransomware

81% of attacks threaten to exfiltrate data

Ransomware Exfiltration

- Russia 11%
- China 17%
- ROW 72%

Ransomware Trend by Month

- 2020
- Trend
- 2021

Jan Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec

Average Ransom Payout[1]

$300,000
$225,000
$150,000
$75,000
$0

Q1-19 Q3-19 Q1-20 Q3-20 Q1-21

Threats by Variant

Conti 12.6% ↑
Darkside 8.4%
CLOP 7.4%
Ransom X 5.3% ↑↑
REvil 23.2%
DoppelPaymer 4.2%
Egregor 4.2%
LockBit 4%
Other 31%
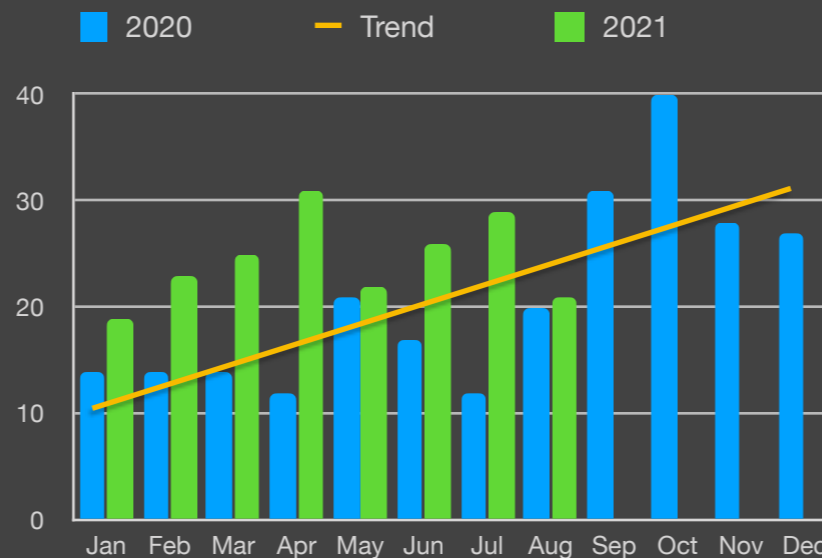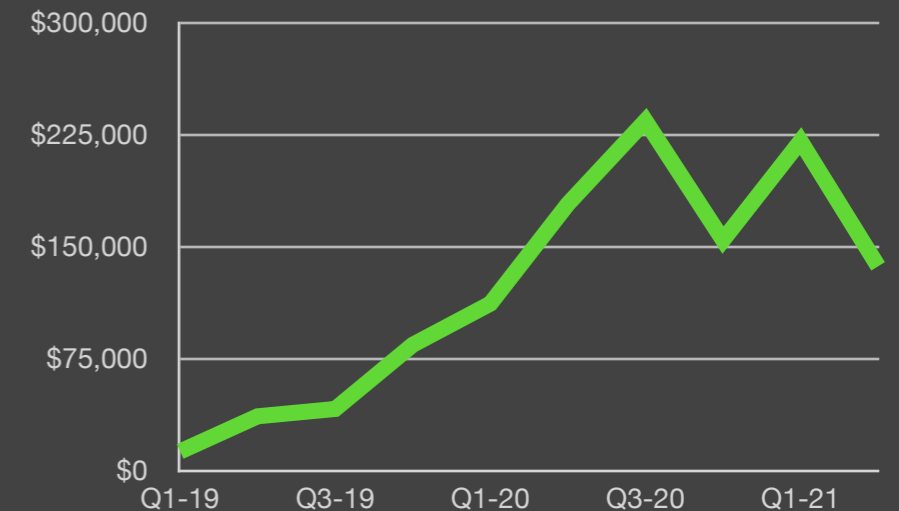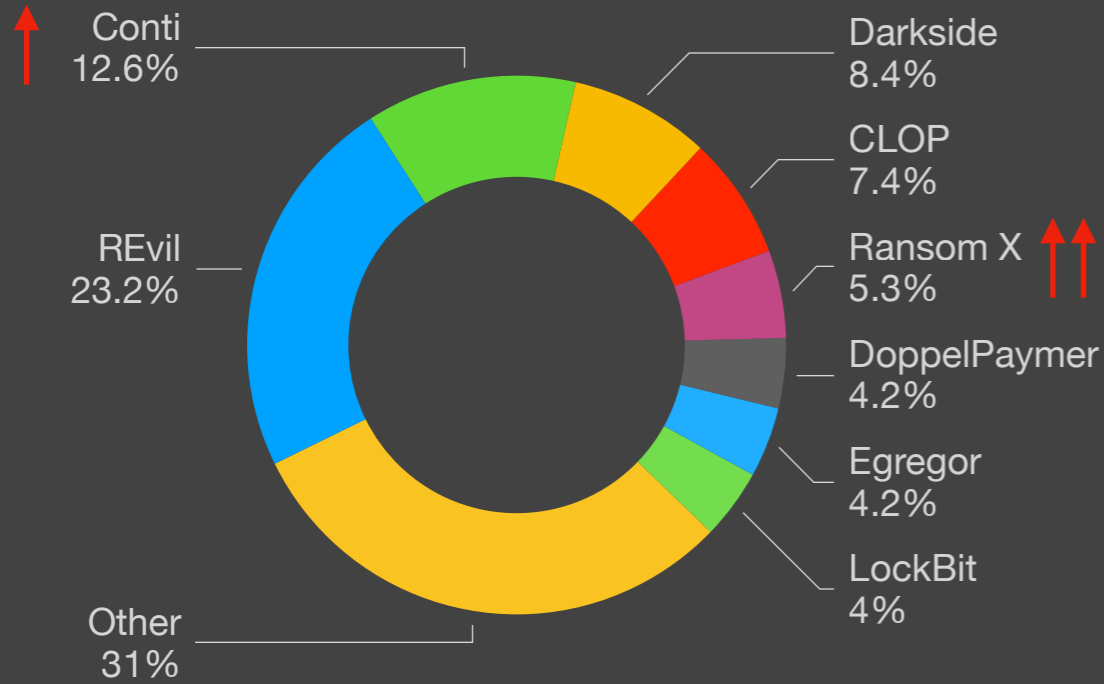
Average Size of Organization

■ 2020   ■ 2021

Skewed by PrismHR ↑

Employee Count
110,000
82,500
55,000
27,500
0

Jan Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec
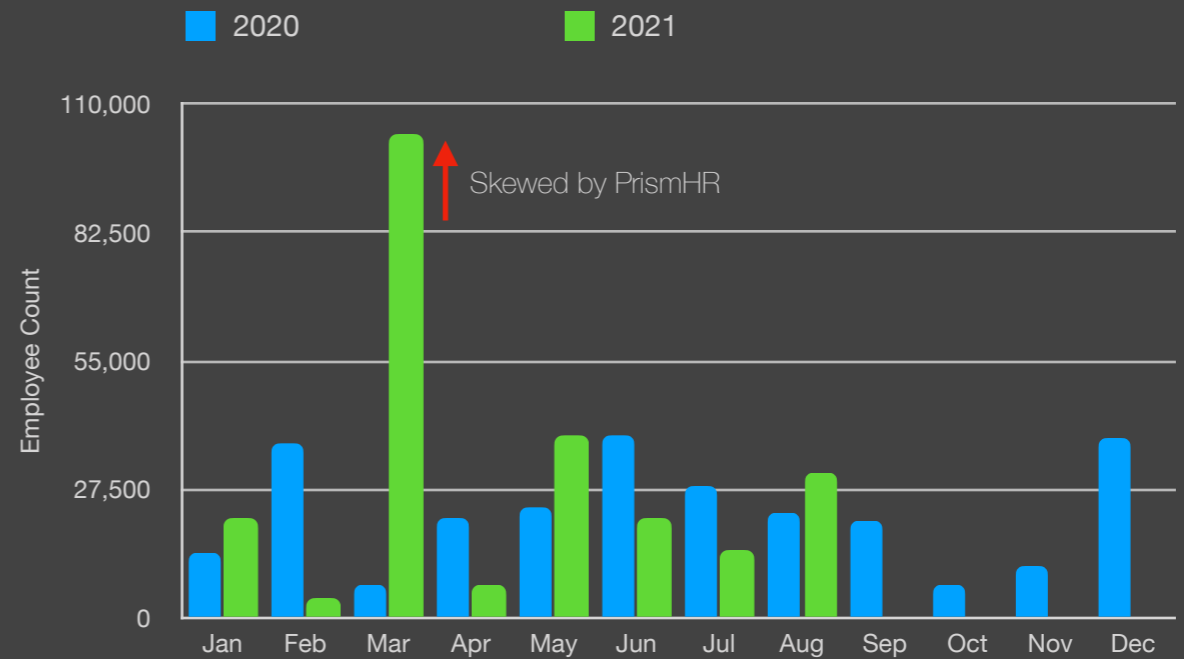
Ransomware Exfiltration Techniques

Botnet 1%
Dark Web 6%
Illegal Network 93%

Common Attack Vectors[2]

— RDP Compromise   — Email Phishing   — Software Vulnerability
— Other

$70
$53
$35
$18
$0

Q1-19 Q2-19 Q3-19 Q4-19 Q1-20 Q2-20 Q3-20 Q4-20 Q1-21 Q2-21
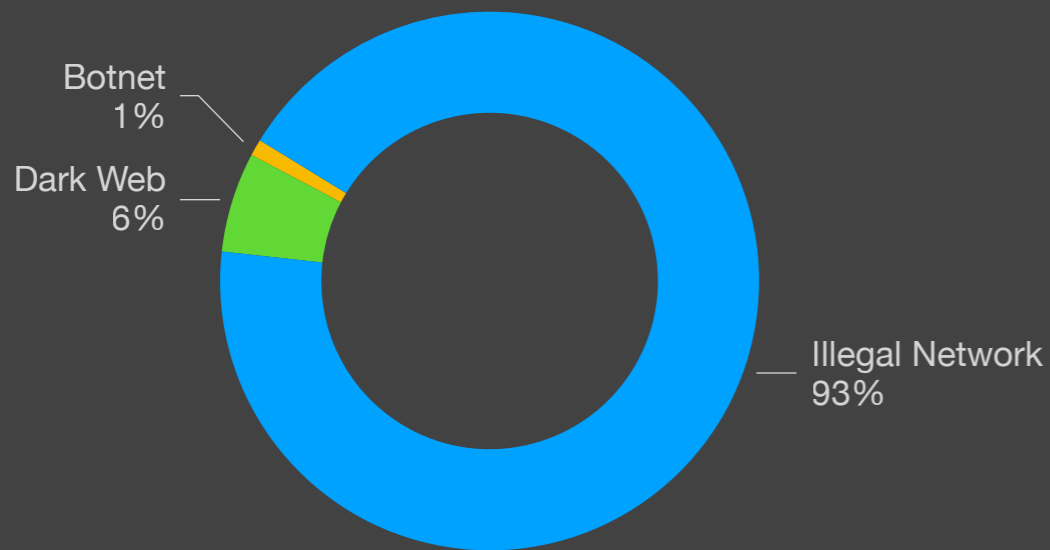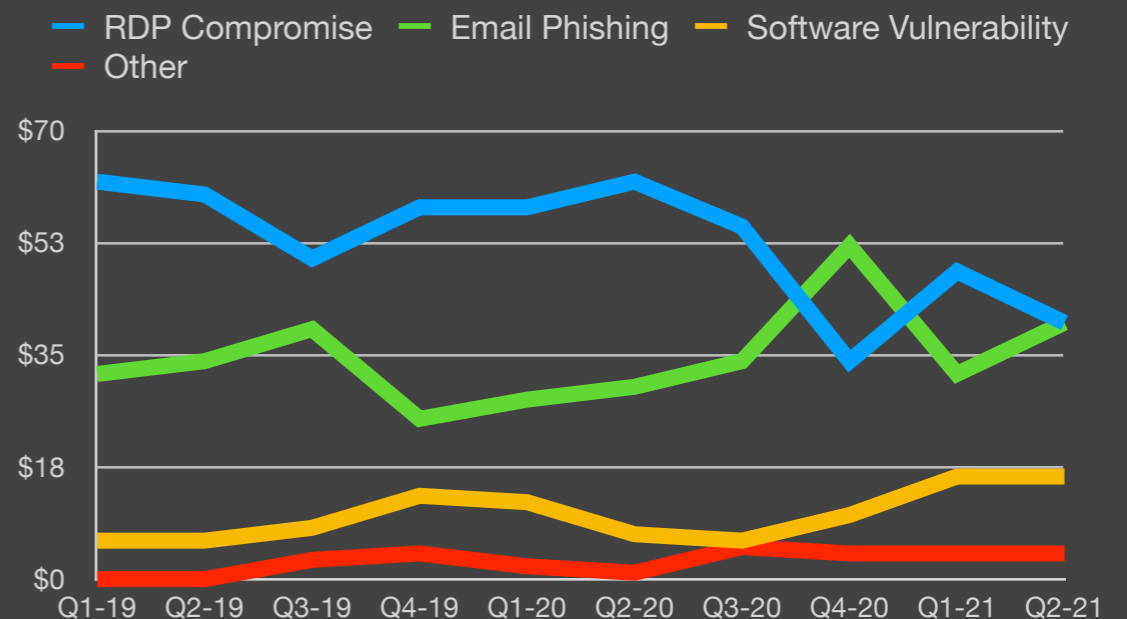
[2]Courtesy Coveware

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.