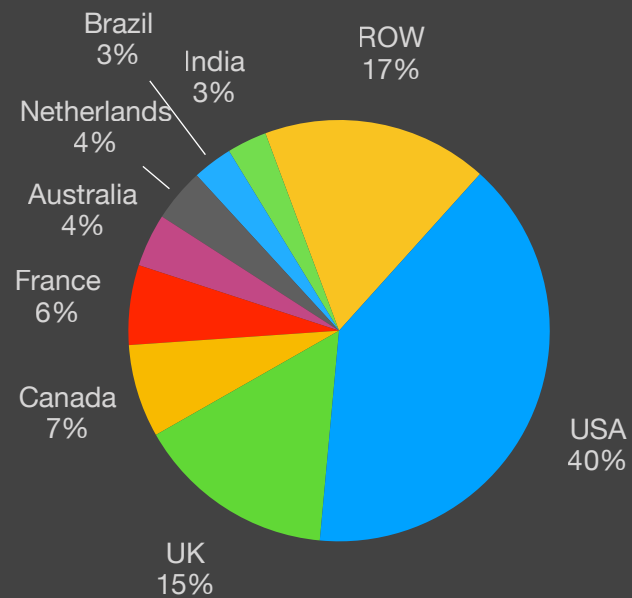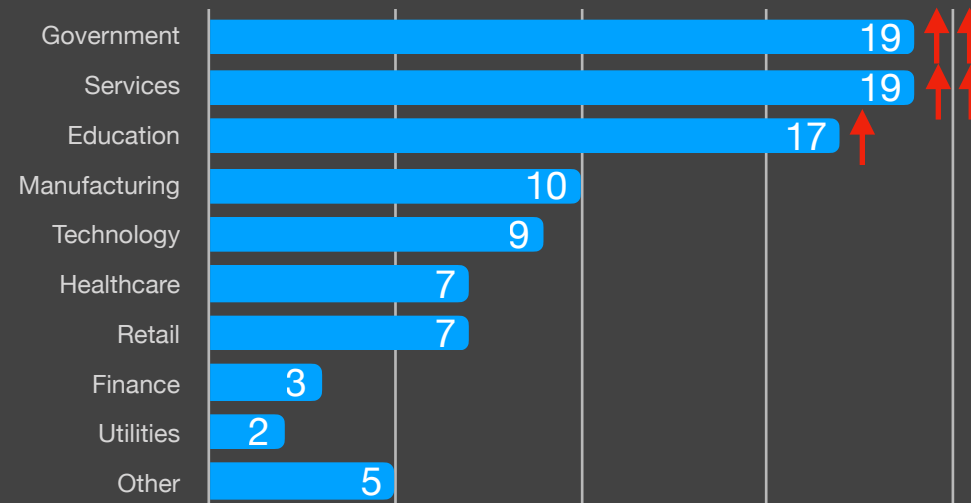In April we uncovered a whopping 31 ransomware attacks, the busiest month of the year so far and up from just 12 in April 2020. The NBA made headlines when the Babuk gang revealed they had exfiltrated 500GBs of sensitive player data, while the REvil gang demanded $25 million from leading French pharmaceutical company Pierre Fabre and an attack on a Dutch logistics company caused a shortage of cheese in supermarkets in the Netherlands.
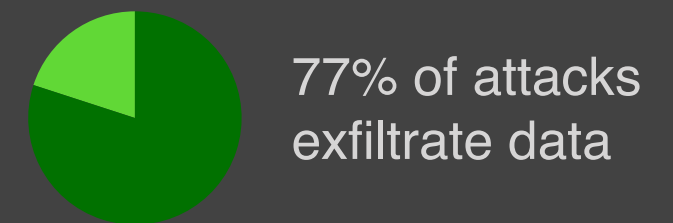
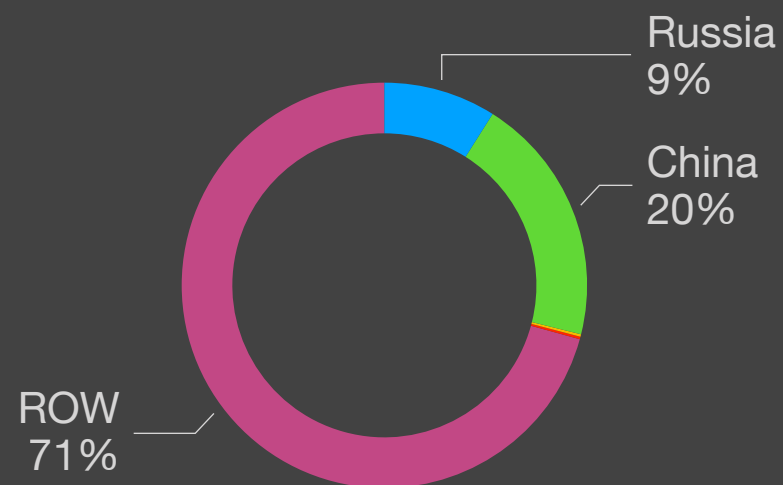## Ransomware by Country

Pie chart "Ransomware by Country":
- USA 40%
- ROW 17%
- UK 15%
- Canada 7%
- France 6%
- Australia 4%
- Netherlands 4%
- Brazil 3%
- India 3%

Ransomware by Industry

Industry	Count
Government	19
Services	19
Education	17
Manufacturing	10
Technology	9
Healthcare	7
Retail	7
Finance	3
Utilities	2
Other	5

Key Trends

Average ransomware payment

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

85% of all attacks Ransomware

77% of attacks exfiltrate data

Ransomware Exfiltration

- Russia 9%
- China 20%
- ROW 71%

Ransomware Trend by Month

Legend: 2020, Trend, 2021 (Jan–Dec)

Average Ransom Payout[1]

Line chart from Q1-19 to Q1-21, y-axis $0 to $300,000 ($75,000, $150,000, $225,000 gridlines).

Threats by Variant

Egregor 9.6%
Conti 11.5%
CLOP 13.5%
REvil 15.4%
Darkside 7.7%
DoppelPaymer 5.8%
Babuk 3.8%
Ragnar 4%
Astro 4%
Hotarus 4%
Other 21%

Average Size of Organization

Legend: 2020, 2021

Employee Count

Y-axis: 110,000 / 82,500 / 55,000 / 27,500 / 0

X-axis: Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, Dec

Skewed by PrismHR

Ransomware Exfiltration Techniques

Botnet 1%
Dark Web 8%
Illegal Network 91%

Common Attack Vectors[2]

Legend: RDP Compromise — Email Phishing — Software Vulnerability — Other

Y-axis: $70 / $53 / $35 / $18 / $0

X-axis: Q1-19, Q2-19, Q3-19, Q4-19, Q1-20, Q2-20, Q3-20, Q4-20, Q1-21

[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.