June saw an uptick in the frequency and severity of ransomware attacks across the world. Although there were no global headline-making attacks like the Colonial Pipeline attack of the previous month, attackers successfully crippled several high-profile organizations like Fujifilm, Grupo Fleury and ADATA.

Ransomware by Country

Australia 3%
Japan 3%
Brazil 3%
Netherlands 3%
France 5%
Canada 5%
UK 13%
ROW 18%
USA 48%

Ransomware by Industry

Industry	Count
Government	25
Education	24
Services	23
Manufacturing	17
Healthcare	16
Technology	14
Retail	8
Utilities	6
Finance	3
Other	10

Key Trends

Average ransomware payment

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

85% of all attacks Ransomware

77% of attacks exfiltrate data
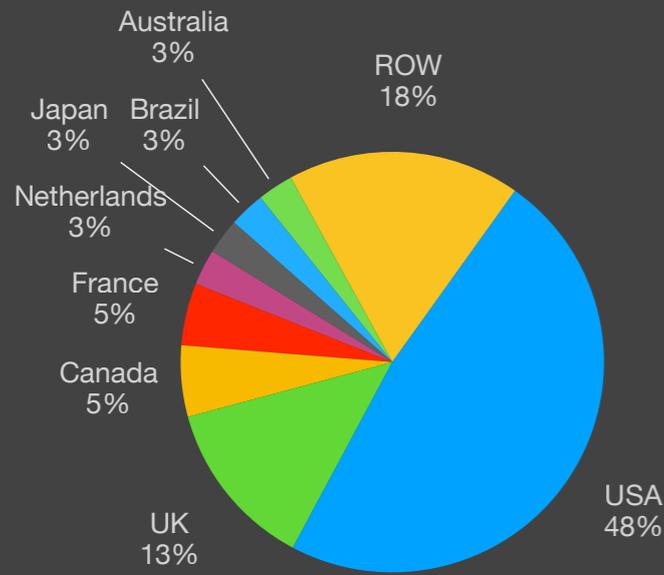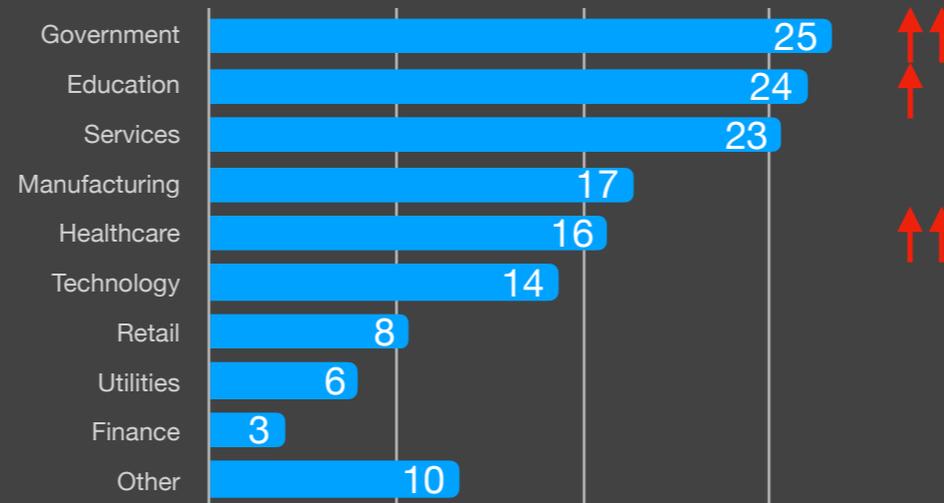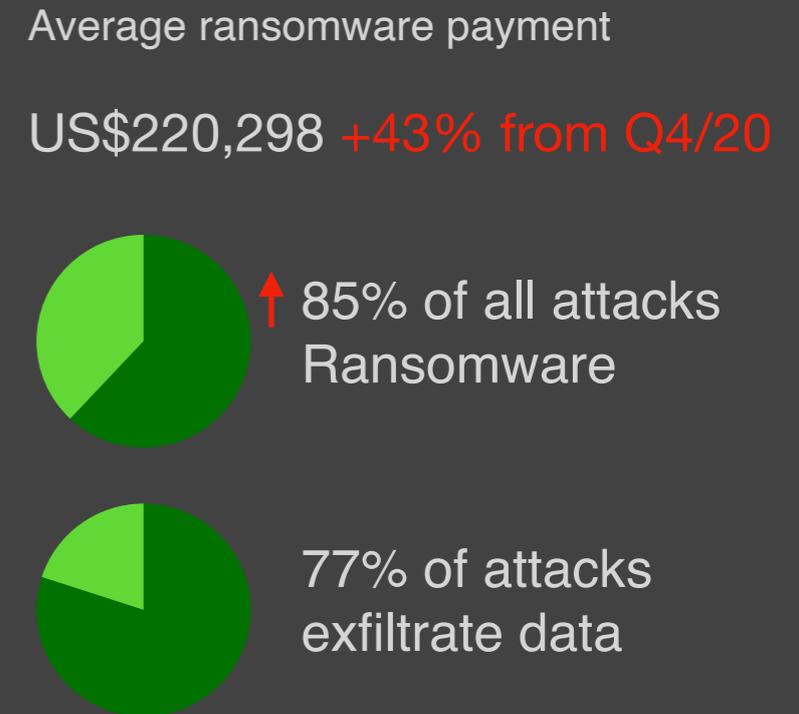
Ransomware Exfiltration

Russia 10%
China 18%
ROW 72%
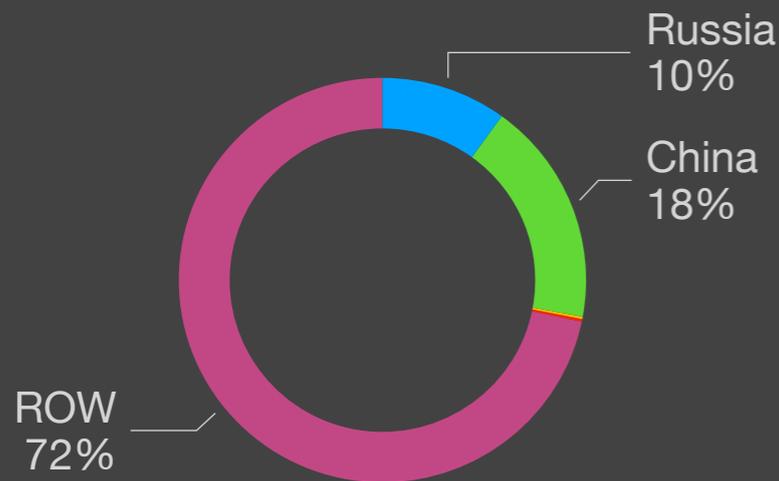
Ransomware Trend by Month

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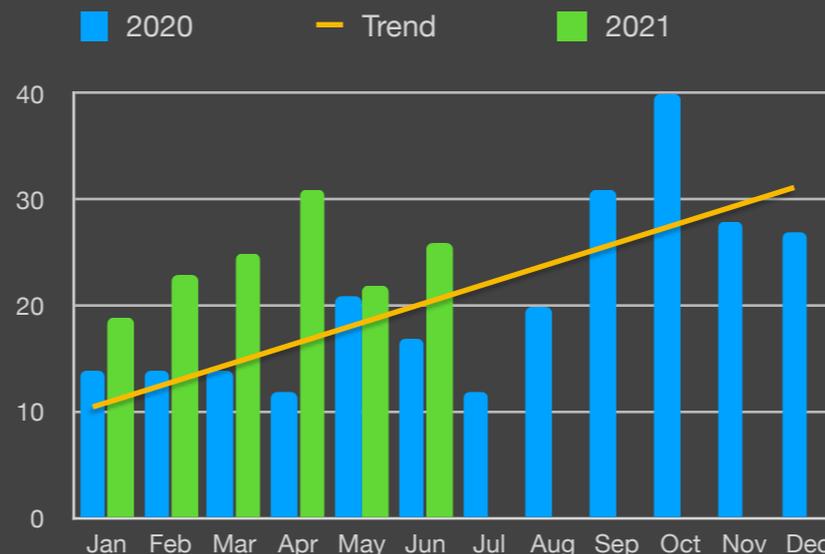
Q1-19 Q2-19 Q3-19 Q4-19 Q1-20 Q2-20 Q3-20 Q4-20 Q1-21
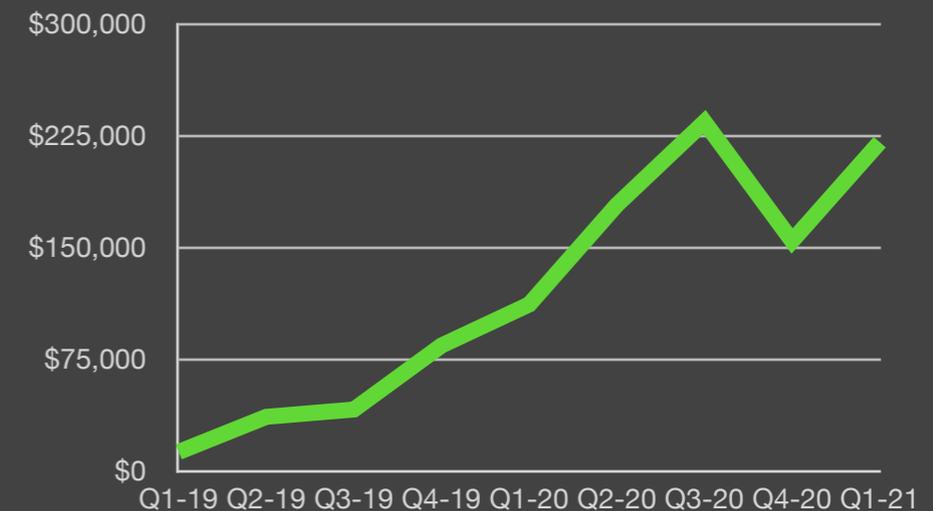
[1]Courtesy Coveware

Threats by Variant

- Egregor 6.9%
- DoppelPaymer 5.6%
- Babuk 4.2%
- Avaddon 4%
- Ryuk 4%
- Ragnar 4%
- Other 21%
- REvil 18.1%
- Conti 12.5%
- CLOP 9.7%
- Darkside 9.7%
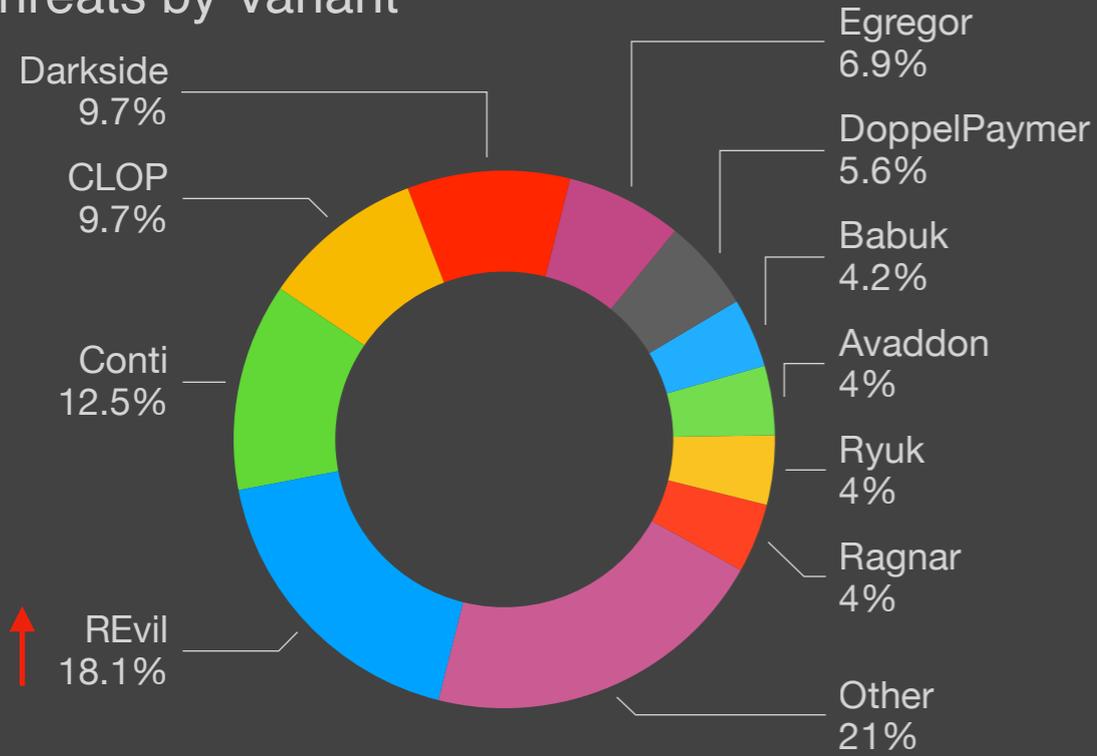
Average Size of Organization

Legend: 2020, 2021

Skewed by PrismHR

Y-axis: Employee Count (0, 27,500, 55,000, 82,500, 110,000)

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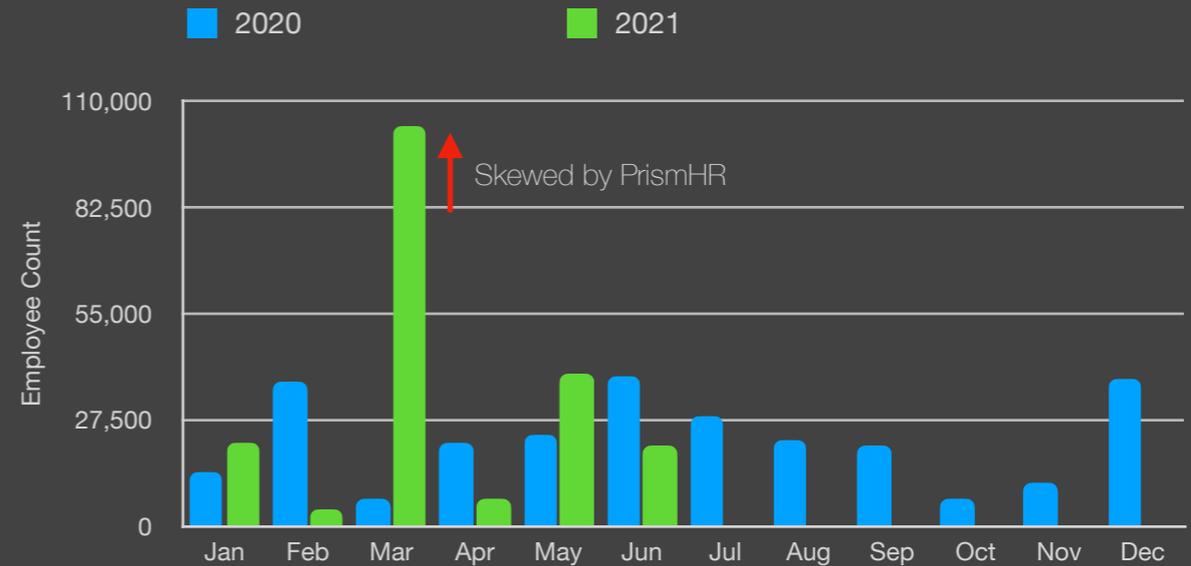
Ransomware Exfiltration Techniques

- Botnet 1%
- Dark Web 7%
- Illegal Network 92%

Common Attack Vectors[2]

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

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

X-axis: Q1-19, Q2-19, Q3-19, Q4-19, Q1-20, Q2-20, Q3-20, Q4-20, Q1-21
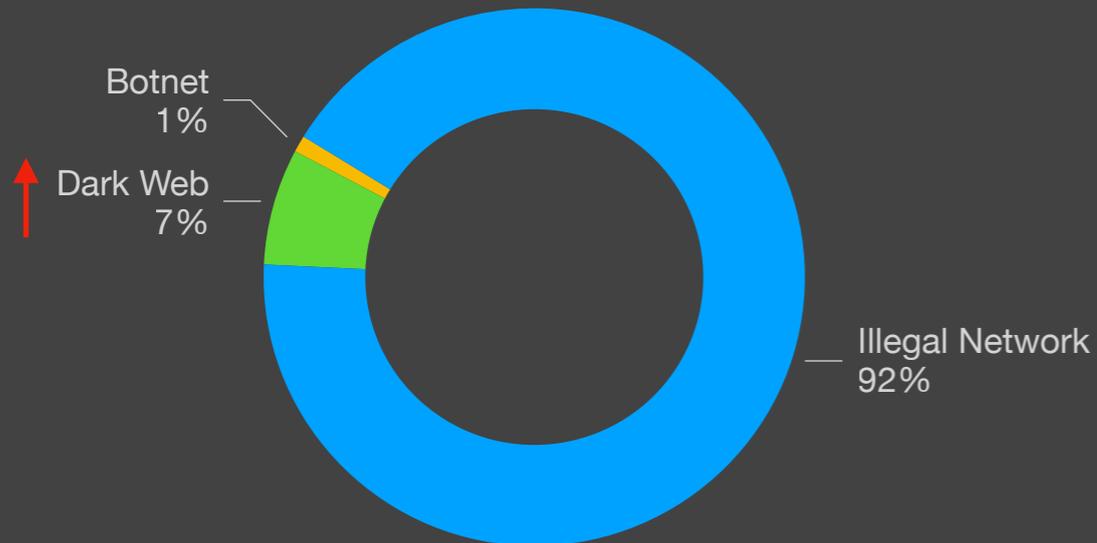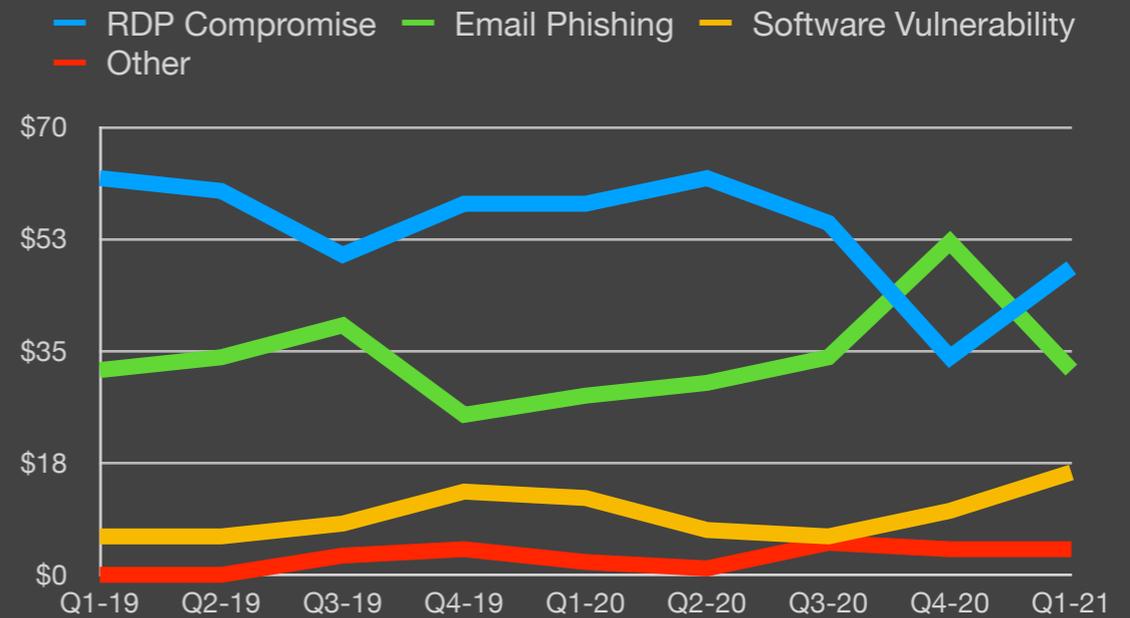
[2]Courtesy Coveware

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.