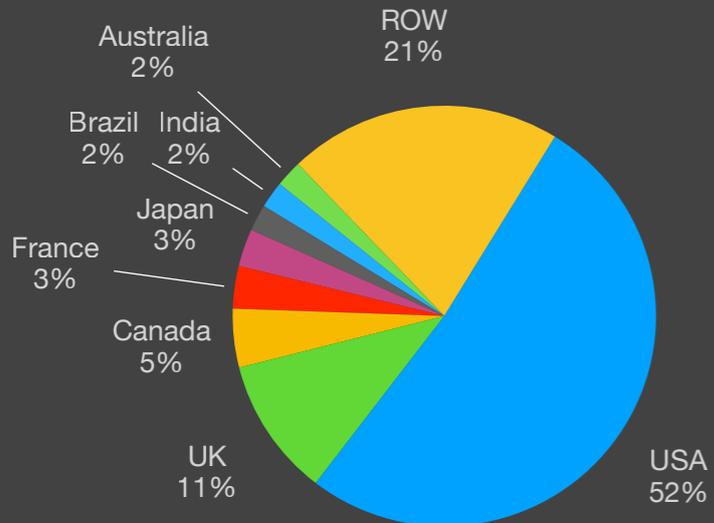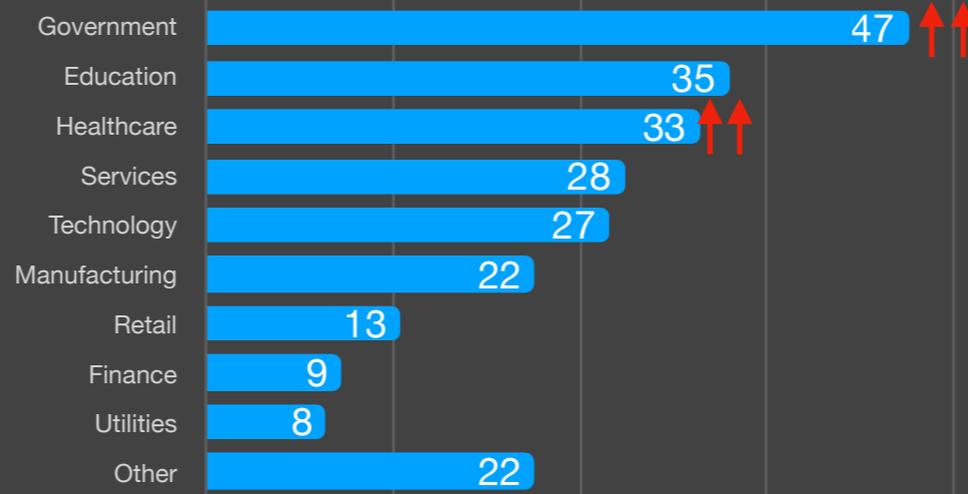In October we recorded 24 reported ransomware incidents, down from 40 in October 2020. This month saw new entries from criminal gangs Everest and Desorden and some notable attacks including Graff Diamonds in the UK. An attack on the Ferrara Candy Co. threatened supplies of Halloween staples such as candy corn, while multi-billion dollar dairy foods company Schreiber also had their production knocked offline following an attack.
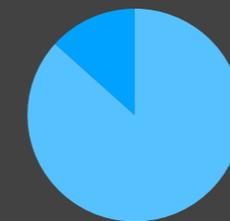
Ransomware by Country

- ROW 21%
- Australia 2%
- Brazil 2%
- India 2%
- Japan 3%
- France 3%
- Canada 5%
- UK 11%
- USA 52%

Ransomware by Industry

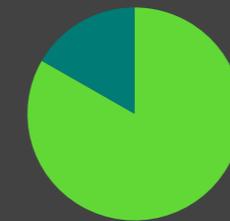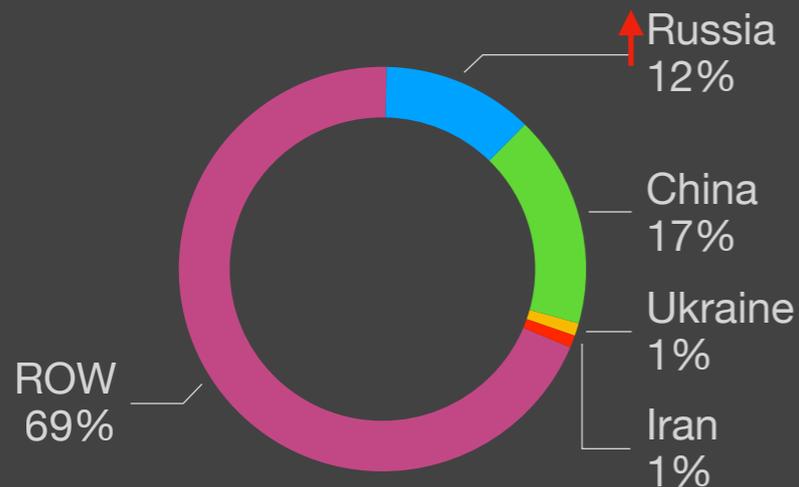| Industry	Value
Government	47 ↑↑
Education	35
Healthcare	33 ↑↑
Services	28
Technology	27
Manufacturing	22
Retail	13
Finance	9
Utilities	8
Other	22

Key Trends

Average ransomware payment

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

78% of all attacks use PowerShell

↑ 83.3% of attacks threaten to exfiltrate data
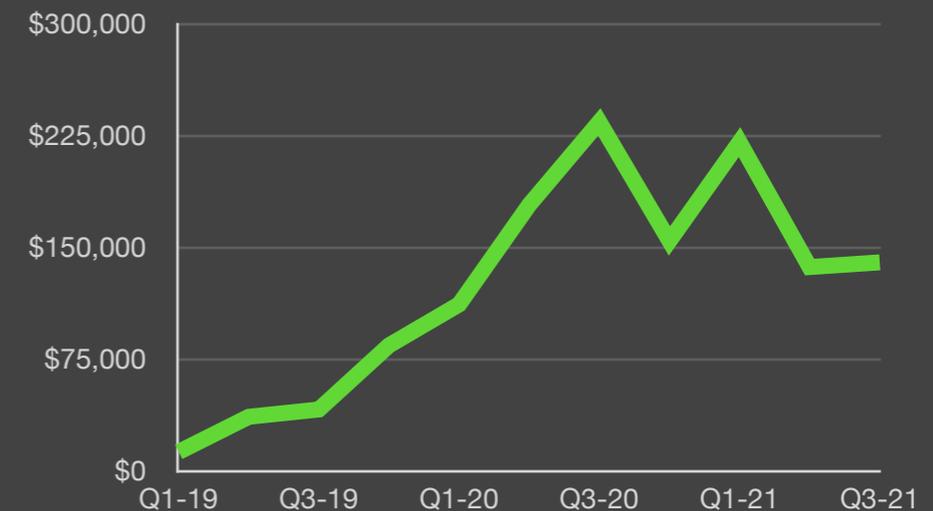
Ransomware Exfiltration

- ↑ Russia 12%
- China 17%
- Ukraine 1%
- Iran 1%
- ROW 69%

Ransomware Trend by Month

■ 2020   — Trend   ■ 2021

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

(Y-axis: 0, 10, 20, 30, 40)

Average Ransom Payout[1]

(Y-axis: $0, $75,000, $150,000, $225,000, $300,000)
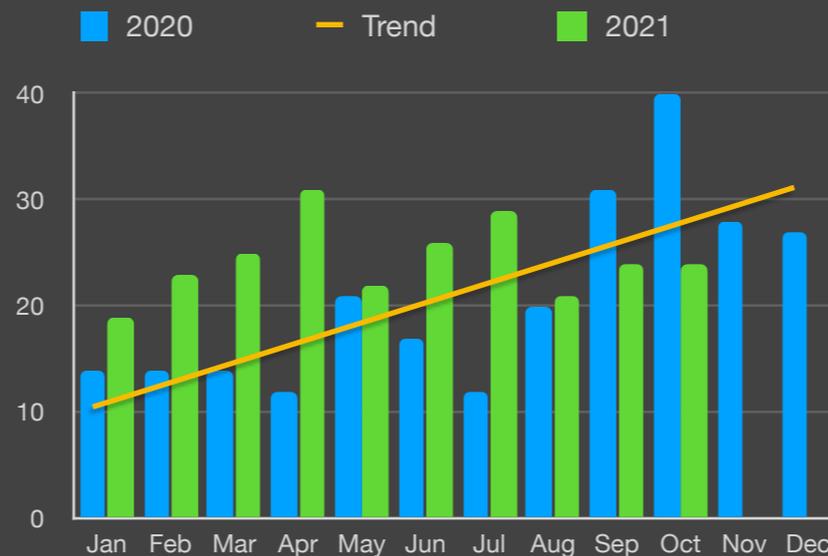
(X-axis: Q1-19, Q3-19, Q1-20, Q3-20, Q1-21, Q3-21)

[1]Courtesy Coveware

Threats by Variant

Ransom X
4.2%

CLOP
5.9%

Darkside
8.4%

Conti
12.6%

REvil
20.2%

DoppelPaymer
4.2%

BlackMatter
4.2%

Vice Society
3%

Other
37%
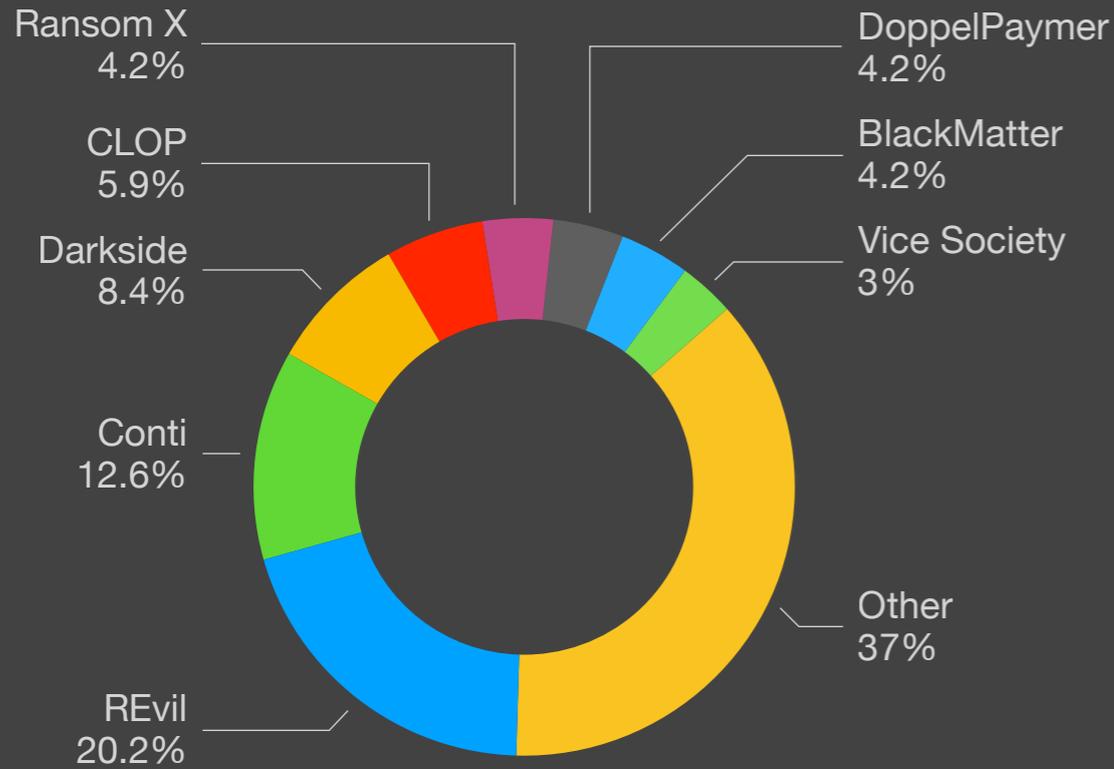
Average Size of Organization

- 2020
- 2021

Employee Count

110,000

82,500

55,000

27,500

0

Skewed by PrismHR

Shift to mid size orgs

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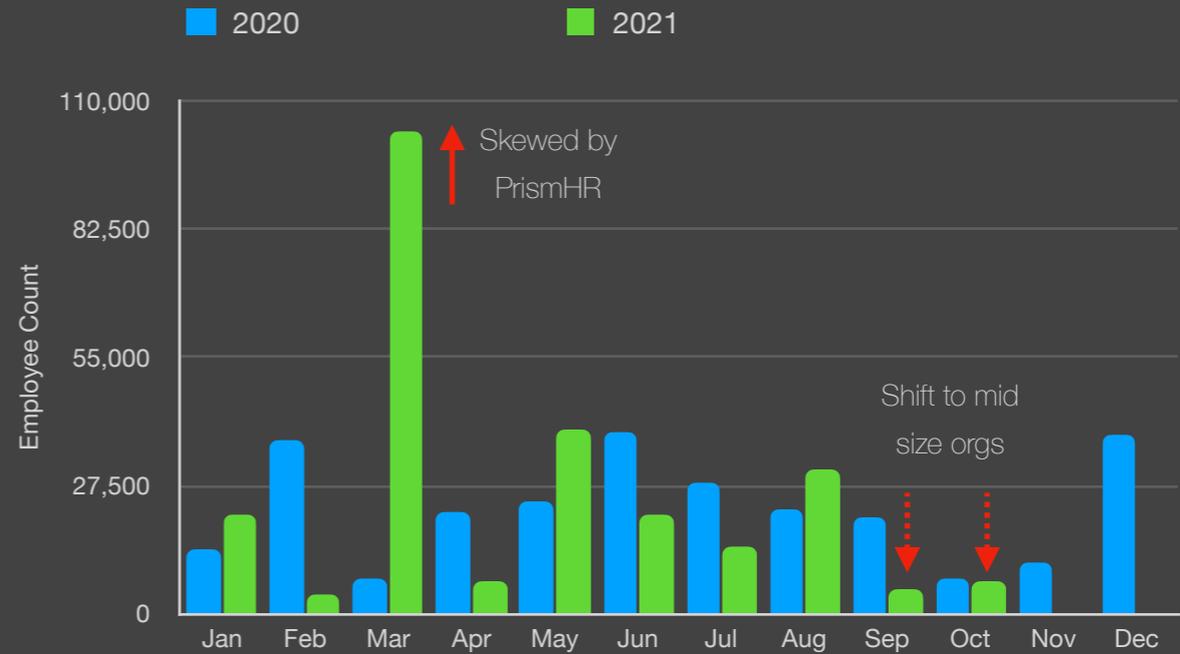
Ransomware Exfiltration Techniques

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 Q3-21
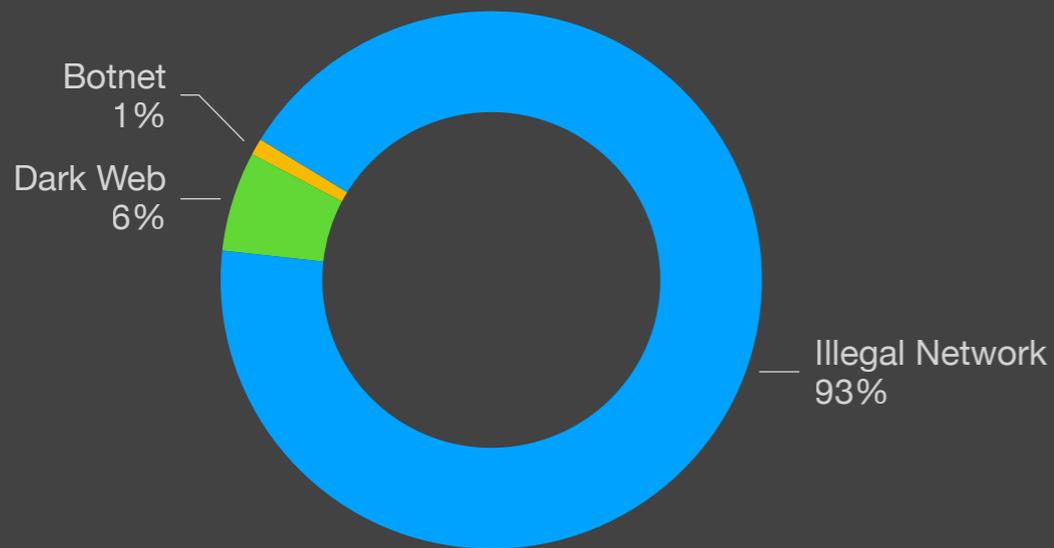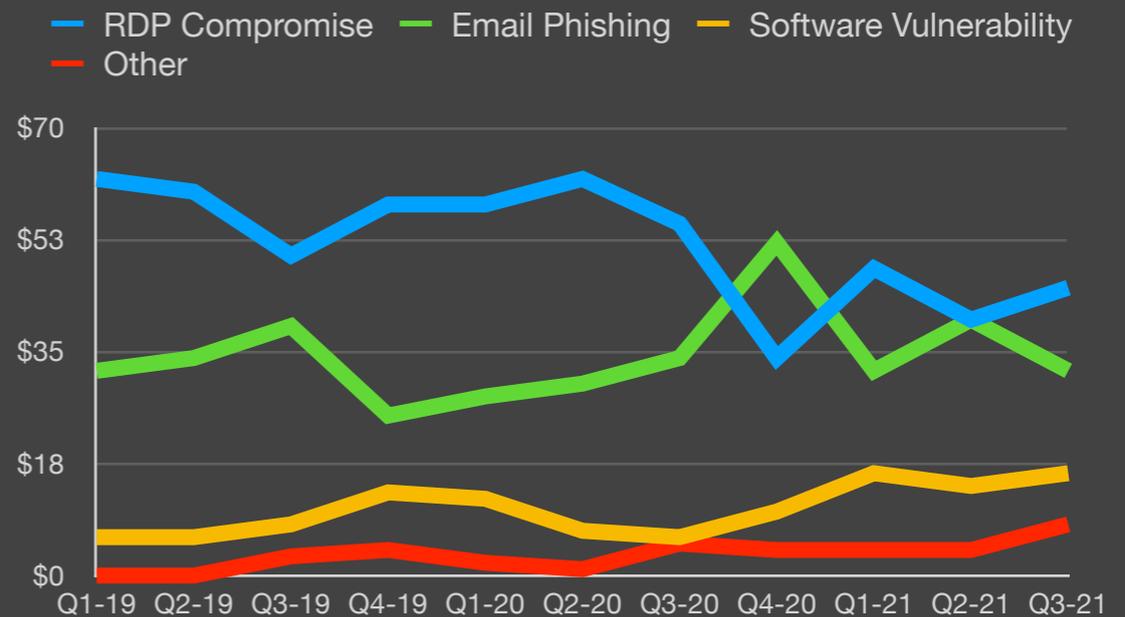
[2]Courtesy Coveware

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.