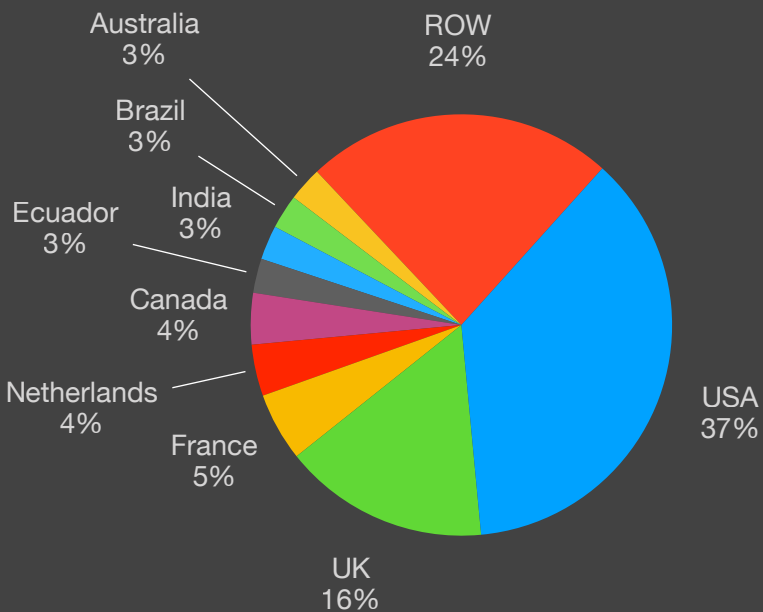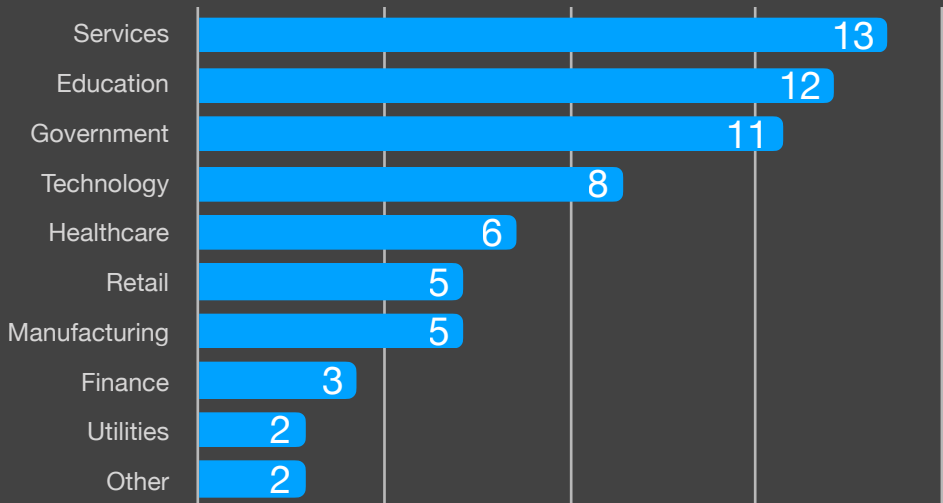In March we recorded 25 attacks, the highest month of the year so far. An attack on computer giant Acer became the largest ransom demand in history at $50 million, while ransomware attacks halted production at IoT manufacturer Sierra Wireless and beer maker Molson Coors. Here's a look at what else we uncovered during the month.
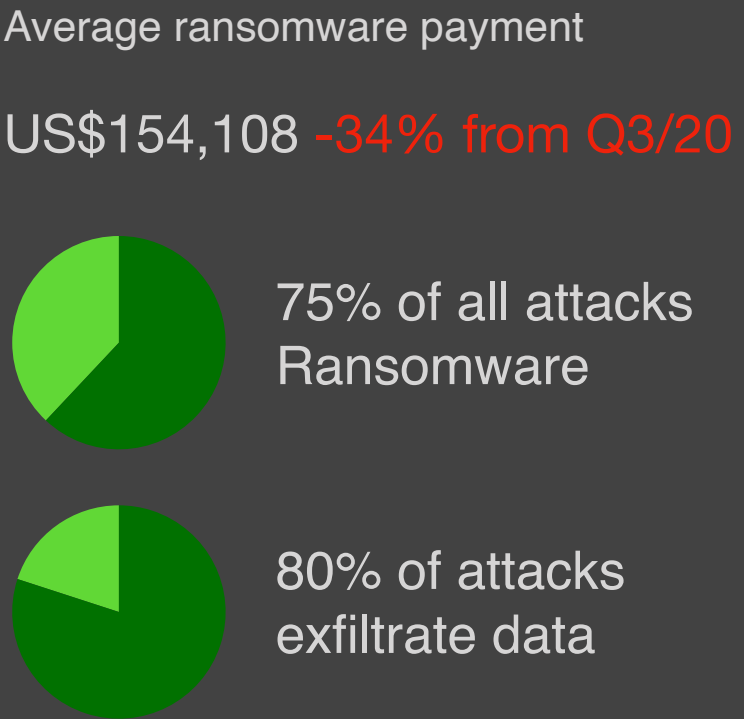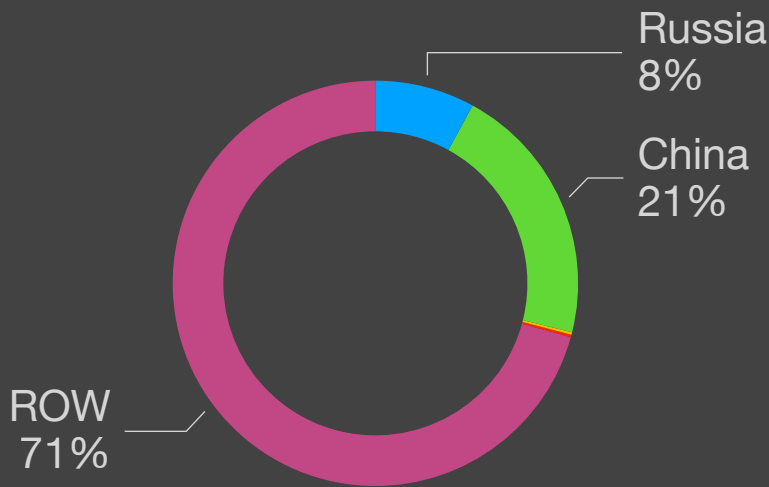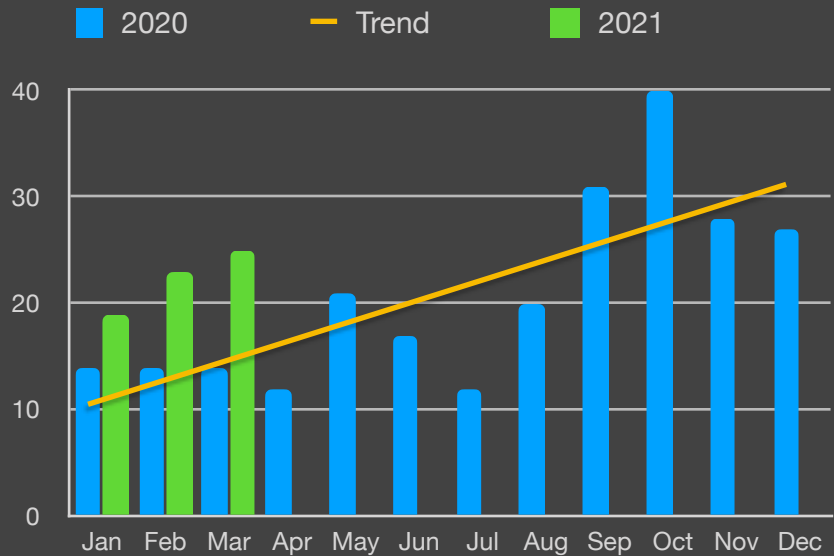
Ransomware by Country

- Australia 3%
- ROW 24%
- Brazil 3%
- India 3%
- Ecuador 3%
- Canada 4%
- Netherlands 4%
- France 5%
- UK 16%
- USA 37%

Ransomware by Industry

Industry	Count
Services	13
Education	12
Government	11
Technology	8
Healthcare	6
Retail	5
Manufacturing	5
Finance	3
Utilities	2
Other	2

Key Trends

Average ransomware payment

US$154,108 -34% from Q3/20

75% of all attacks Ransomware

80% of attacks exfiltrate data

Ransomware Exfiltration

- Russia 8%
- China 21%
- ROW 71%

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
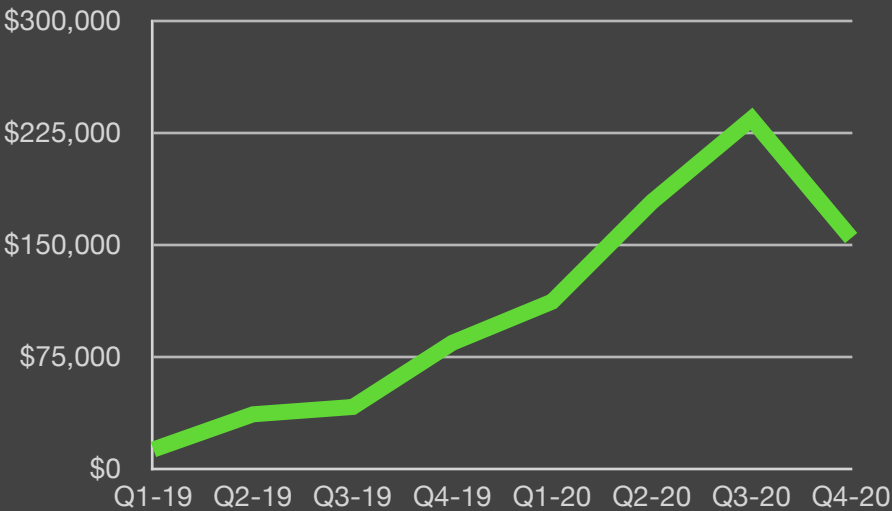
[1]Courtesy Coveware

Threats by Variant

Conti
8.9%

Egregor
11.1%

CLOP
13.3%

Darkside
6.7%

REvil
6.7%

Hotarus
4.4%

Ragnar
4.4%

DoppelPaymer
4%

Other
40%
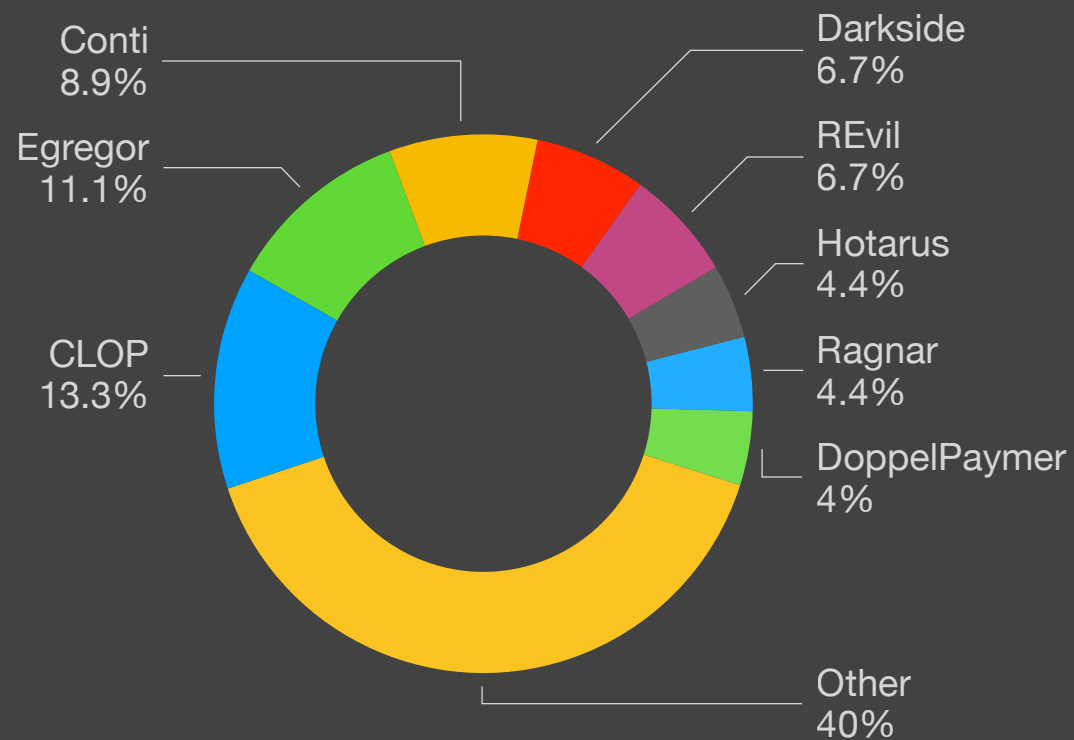
Average Size of Organization

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
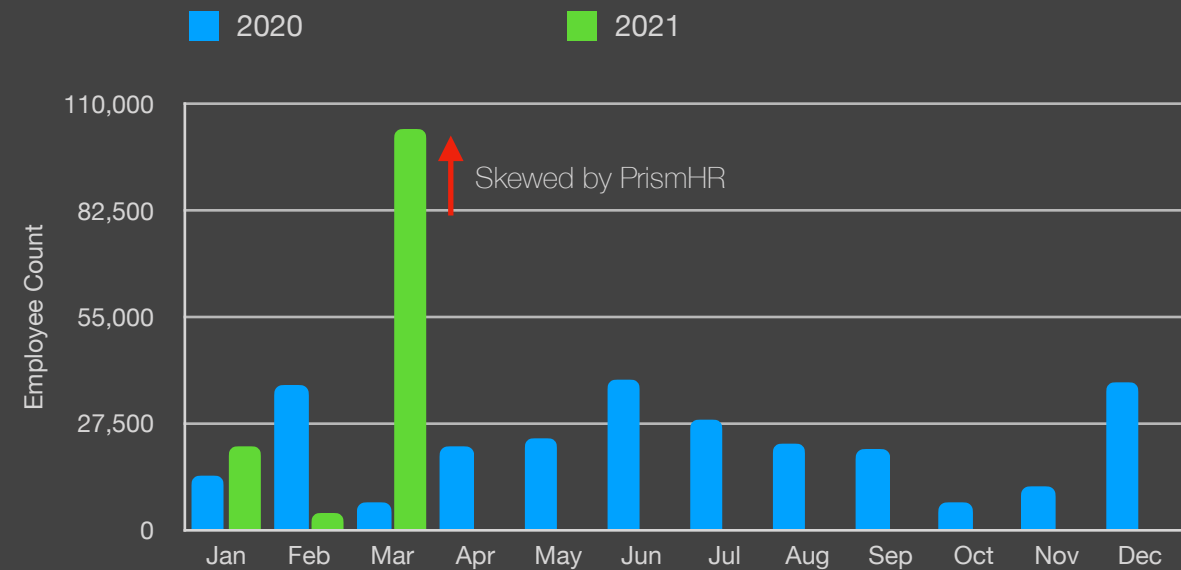
Ransomware Exfiltration Techniques

Botnet
1%

Dark Web
8%

Illegal Network
91%
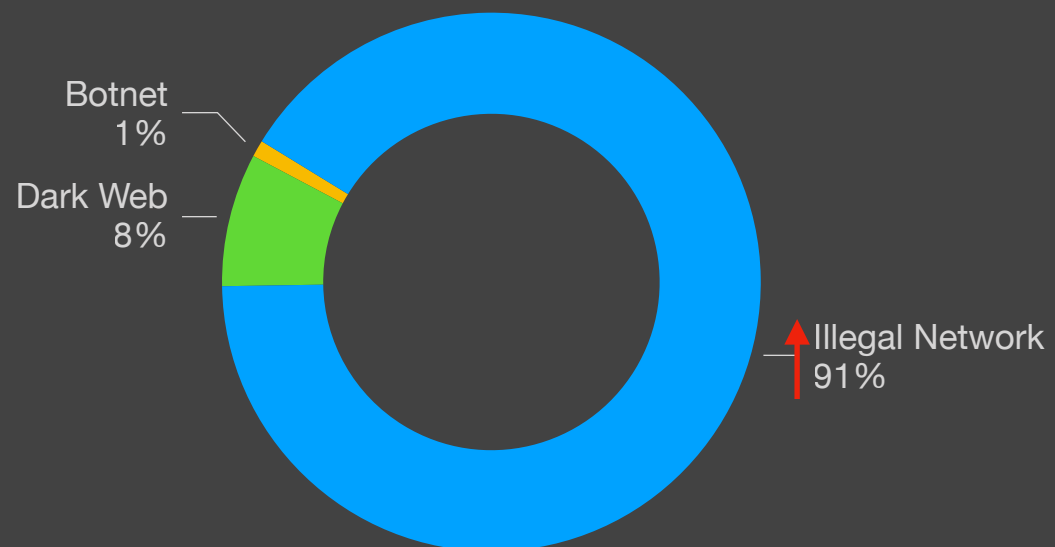
Average ransom demand by strain[2]

$500,000

$375,000

$250,000

$125,000

$420,000

$282,590

$176,190

$132,573 $130,694

$81,825 $73,920

Maze Ryuk Netwalker Zepplin DoppelPaymer Dharma Sodinokibi
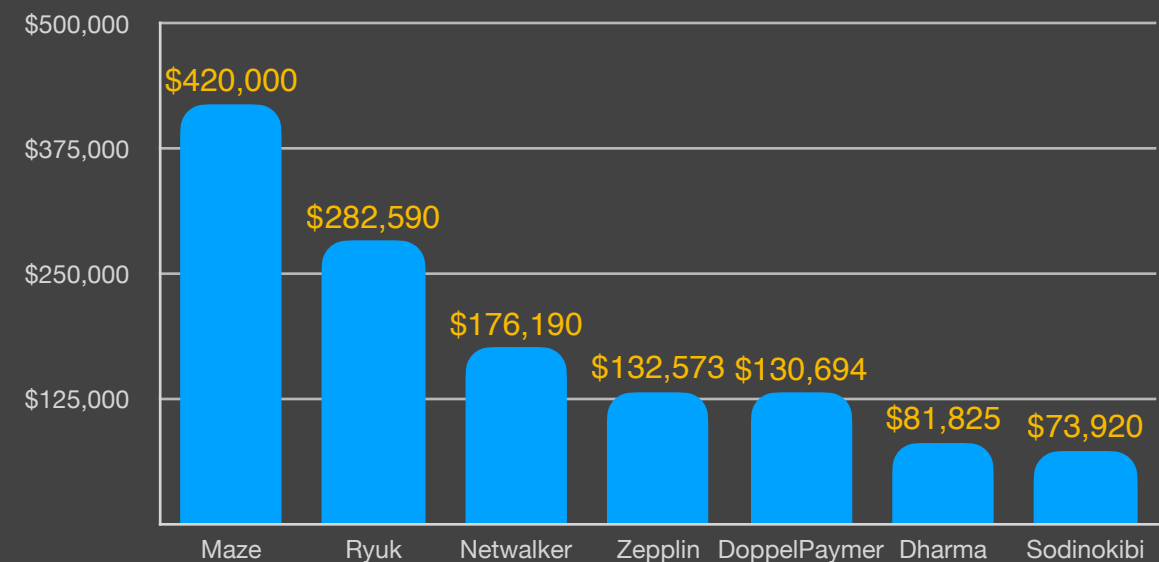
[2]Courtesy Coalition

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.