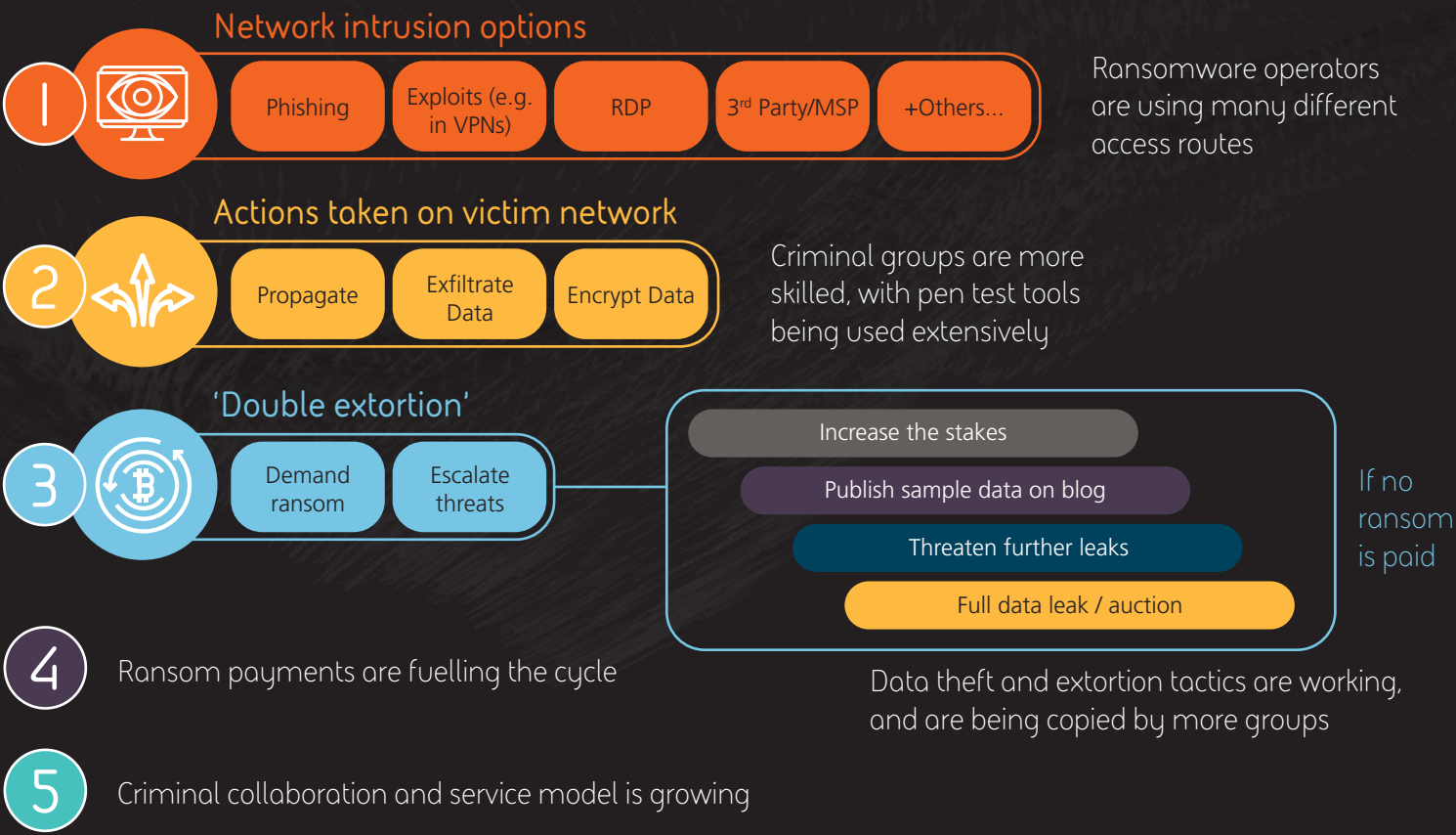# Ransomware's Perfect Storm

2020 has seen a surge in ransomware cases, with organisations falling victim across a wide range of sectors and geographies. The BAE Systems Threat Intelligence team has been tracking this closely. Here we present five key factors behind this perfect storm, as well as statistics on the scale of the problem

Simplified stages of a modern ransomware attack, and five reasons why they're so successful

1 Network intrusion options

Phishing | Exploits (e.g. in VPNs) | RDP | 3rd Party/MSP | +Others...

Ransomware operators are using many different access routes

2 Actions taken on victim network

Propagate | Exfiltrate Data | Encrypt Data

Criminal groups are more skilled, with pen test tools being used extensively

3 'Double extortion'

Demand ransom | Escalate threats

- Increase the stakes
- Publish sample data on blog
- Threaten further leaks
- Full data leak / auction

If no ransom is paid

4 Ransom payments are fuelling the cycle

Data theft and extortion tactics are working, and are being copied by more groups

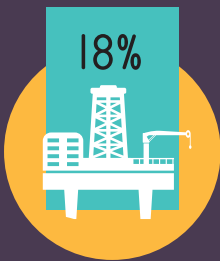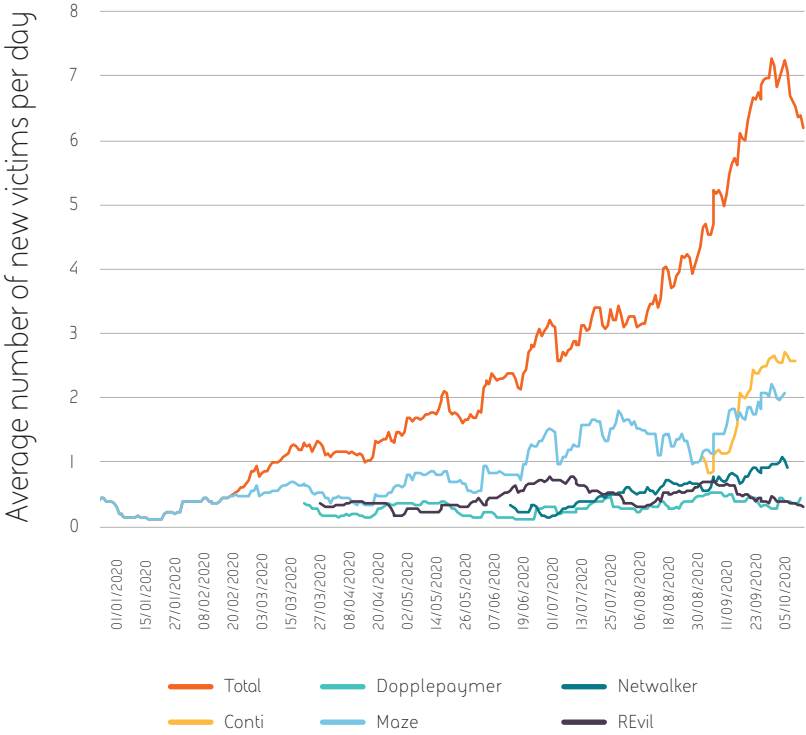**5** Criminal collaboration and service model is growing

Victim blog tracking – the scale of the problem

We have gathered blog publications indicating a total of over 800 ransomware victims by operators of 15 different ransomware campaigns
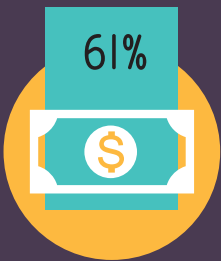
260%

Increase in number of victims identified on ransomware blogs between April and September 2020

~10% Of victims removed from ransomware blogs, indicating potential ransom payment

Average number of new victims per day

Legend: Total | Dopplepaymer | Netwalker | Conti | Maze | REvil

18% Victims from industrial and manufacturing sector

61% Victims have annual revenue less than $50m

7% Victims have annual revenue over $1bn

Global distribution of ransomware victims

United States: **59%**

Europe: **24%**

Rest of World: **17%**

BAE SYSTEMS