Centre for Criminal Justice Studies
School of Law

UNIVERSITY OF LEEDS

Understanding the challenge: how cybercrime has evolved to become a modern Serious Organised Crime

Maximising Impact from Serious Organised Crime Research, Cyber Crimes & Online Criminal Markets. University of Cambridge, Sept. 16th 2021

Professor David S. Wall,

d.s.wall@leeds.ac.uk

Picture: https://www.pixelstalk.net/wp-content/uploads/2016/04/HACKER-hack-hacking-internet-computer-anarchy-sadic-virus-dark-anonymous-code-binary.jpg

Interdisciplinary Cybercrime Research At Leeds – Work in Progress

UNIVERSITY OF LEEDS

I am interested in changes in the cybercrime threat landscape, especially the ways that offenders have become more adaptive and organised to challenge law enforcement. I am also interested in potential for offenders to develop powerful, sustainable online organised crime groups. I draw from three research projects.

- **Combatting cRiminals in The Cloud (EPSRC CRITiCal) 2015-22**
- **Ransomware and Cybercrimes of Extortion (EPSRC/ ESRC EMPHASIS)** (EconoMical, PsycHologicAl and Societal Impact of RanSomware (2017 –2019)
- **Understanding Organised Crime and Terrorist Networks** (H2020 2016-19)

A recent article relevant to this presentation is:

Wall, D.S. (2021) 'The Transnational Cybercrime Extortion Landscape and the Pandemic: changes in ransomware offender tactics, attack scalability and the organisation of offending', *European Law Enforcement Research Bulletin, 22,* (publication forthcoming) ***PREPRINT available***
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3908159

1. Cybercrime as (Transnational) modern serious organised crime

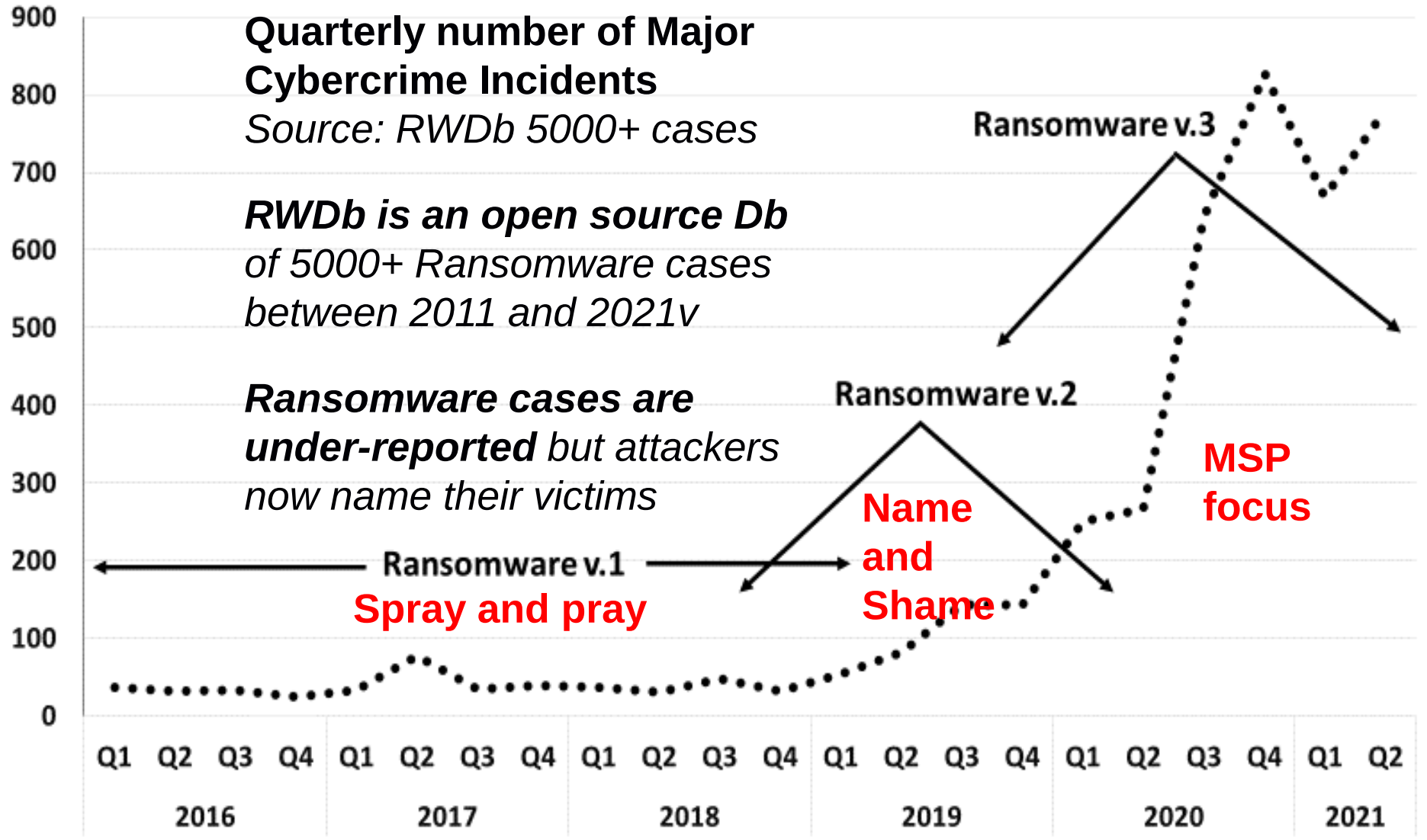
UNIVERSITY OF LEEDS

My research into cybercrime is finding that

- *Cybercrime offenders are more professional than before*. From a business studies manual and NOT organised crime playbook.
- *More ruthless,* now *triple extortion methods, N&S, Data, DDoS*
- *The increased yield* of proceeds from cybercrime is causing skilled potential actors to choose cybercrime as a career
- *Offenders are supported by, or are part of, a cybercrime ecosystem* which facilitates cybercrimes – RaaS, Data Market.
- *The cybercrime ecosystem system is the new face of organised crime*, with specialist services run by brokers/ kinpins
- *There is no one Mr or Mrs Big*. E.g. recent ransomware arrests got the bit players (monetiser), so only disrupted operations
- *Offenders are incredibly adaptive*, but cybersecurity and law enforcement tend to be rule based and irrelatively inflexible – there are still elements of reassurance policing to be seen.

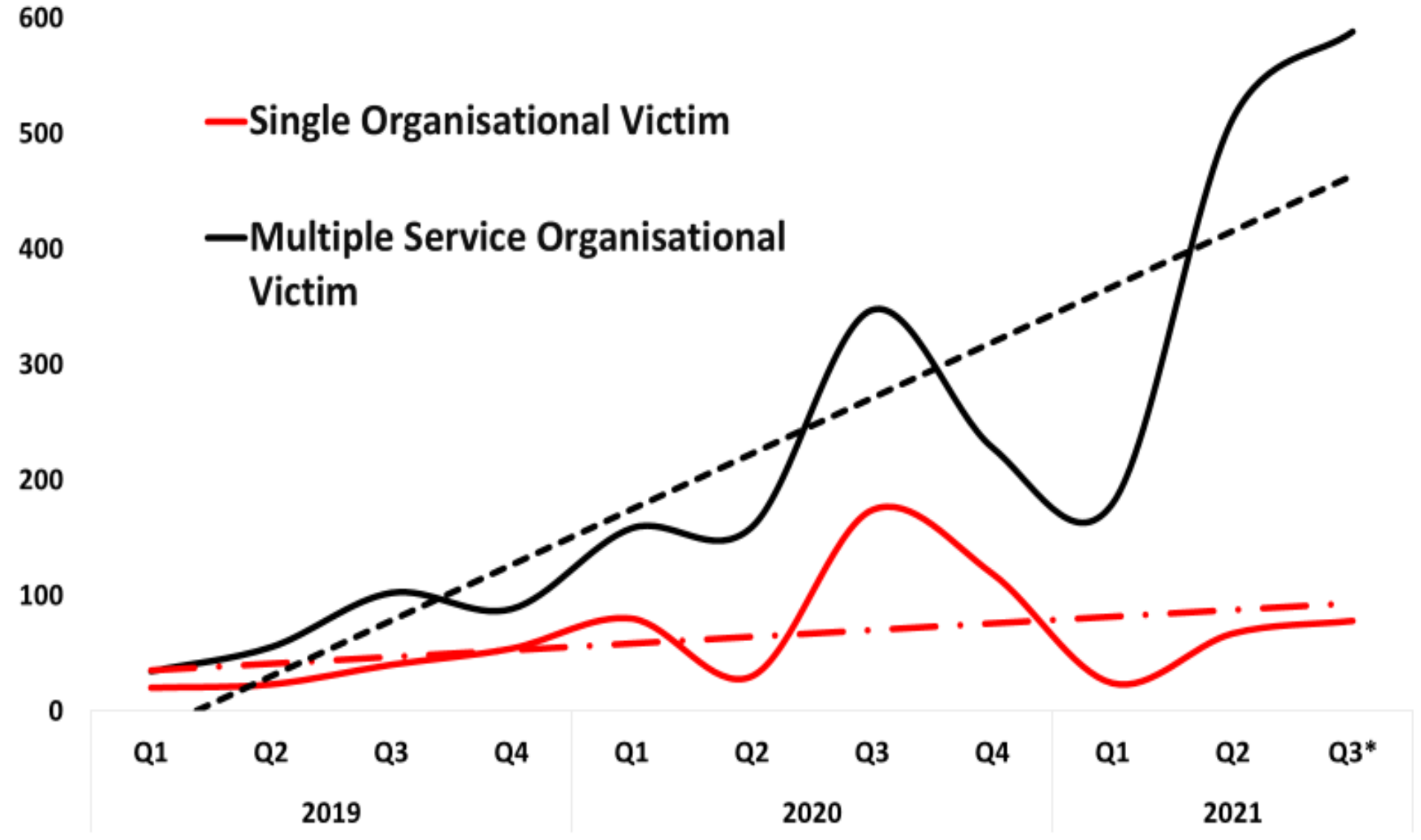
2. The evolution of ransomware as a modern cybercrime RW1-RW3

UNIVERSITY OF LEEDS



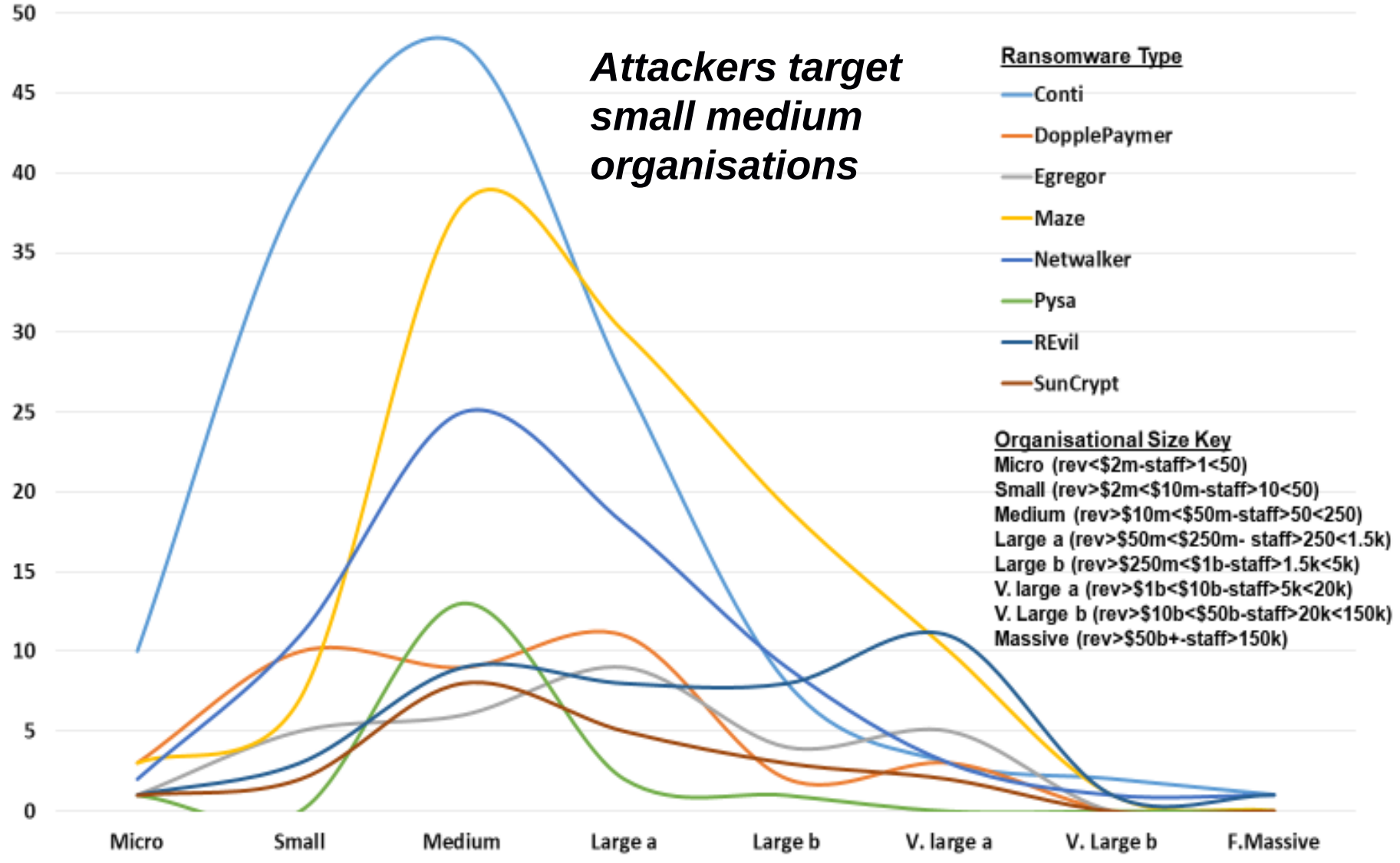
3. Increase in scalability – increasing attacks on Multiple Service Providers and The Supply Chain

UNIVERSITY OF LEEDS



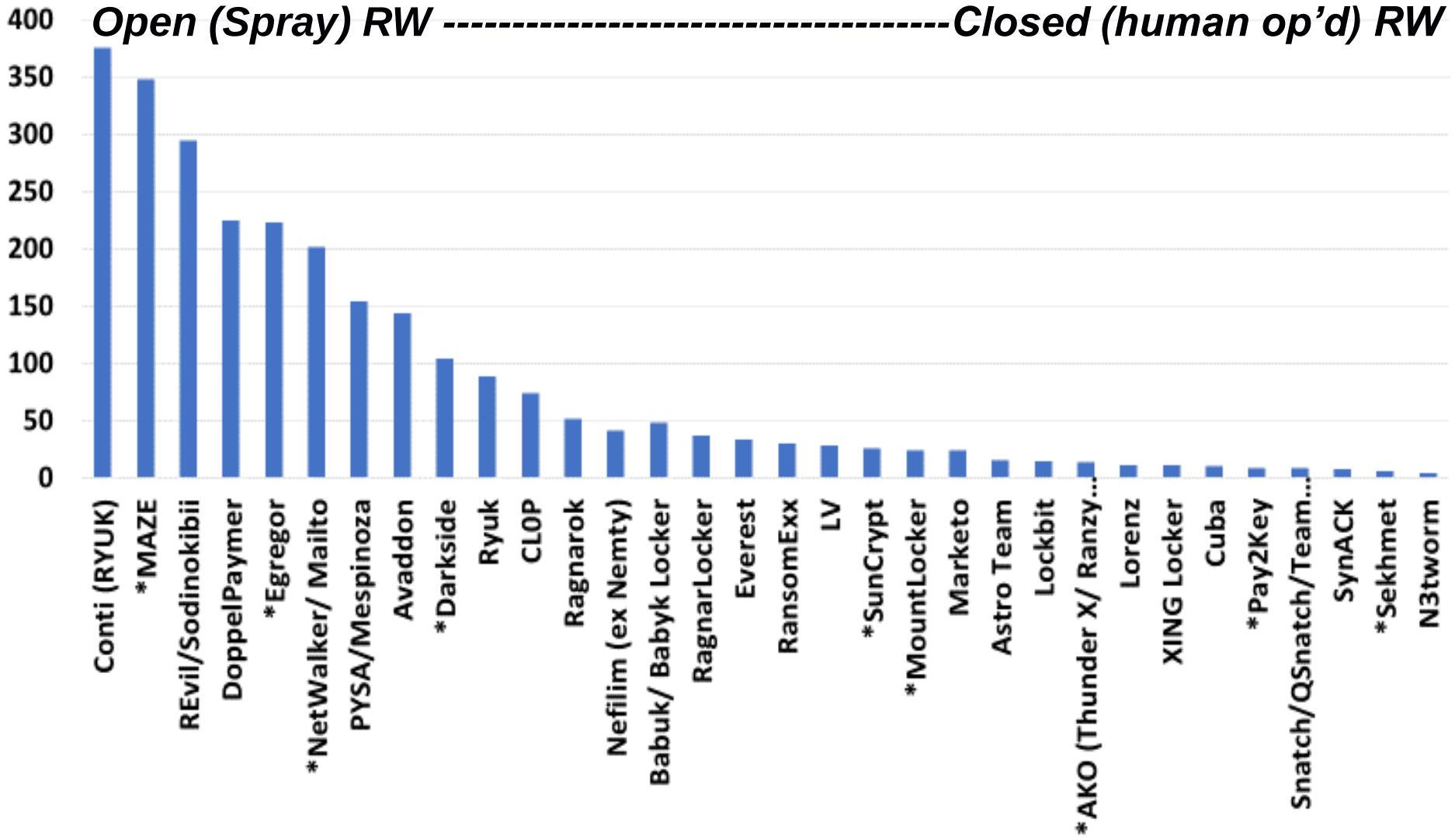
4. Profile of business victims – Jan 2020 – June 2021

UNIVERSITY OF LEEDS



5. Profile of attack groups – Jan 2020 – June 2021 by volume

UNIVERSITY OF LEEDS



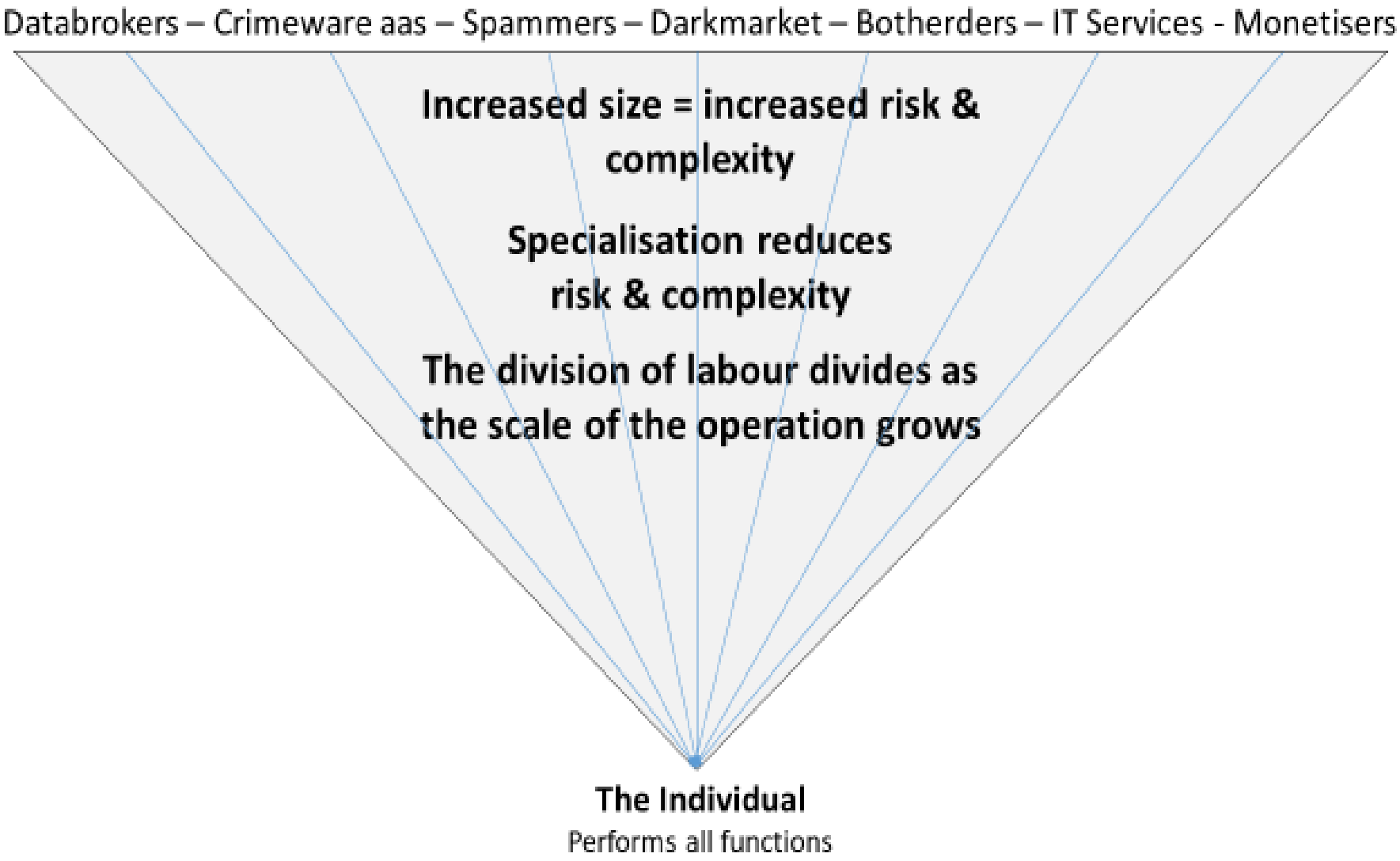
6. There are nine basic stages to a ransomware attack

UNIVERSITY OF LEEDS

1. Identify the best victims to attack – the reconnaisance
2. Gaining ‘initial access’ by infiltrating the victim’s network
3. Escalating computing access privileges in the system
4. Identifying key organisational data that will hurt when lost
5. Exfiltrating the key data and installing ransomware
6. Naming and shaming victims & levying the ransom demand
7. Payment of the ransom demand in cryptocurrency
8. Monetarising the crime – cryptocurrency into fiat money
9. Post-crime - “getting away” with the crime once completed

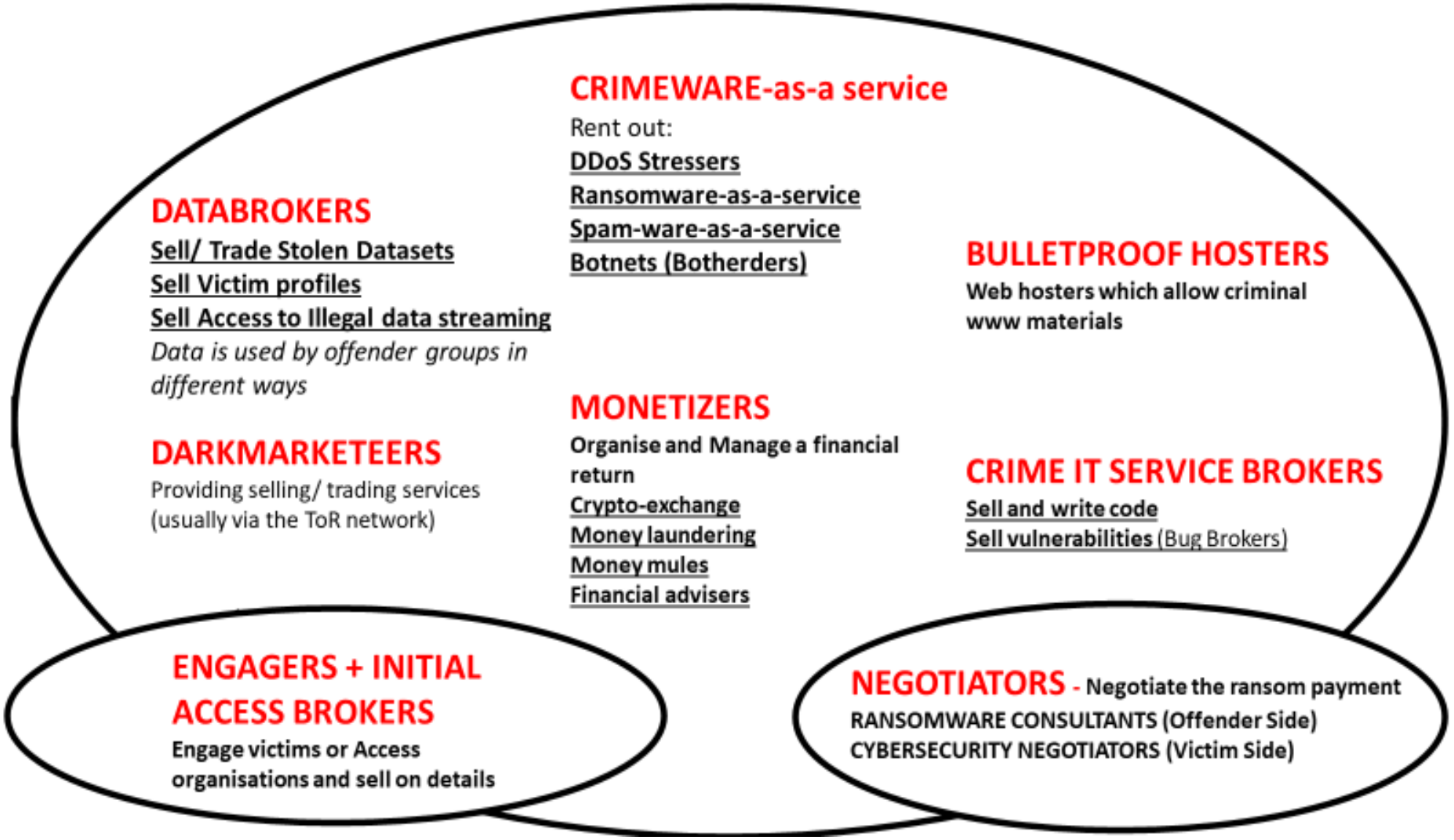
7. From hobby to profession – making cybercrime pay - Scaling up Cybercrime

UNIVERSITY OF LEEDS



8. The Cybercrime Ecosystem

UNIVERSITY OF LEEDS



9. Conclusion: The new challenges of cybercrime for law and enforcement

UNIVERSITY OF LEEDS

- ***Ransomware is a blended cybercrime*** as it i) comprises more than one crime and ii) combines the social with science – social engineering & negotiators.
- ***Statistically, ransomware is problematic and hard to record***. In the UK, the 'ransom' and 'ware' are recorded as different statistics. They also constitute different bodies of law and fall under different policing agencies.
- ***These agencies have untrusted relationships with industry***, especially when victims pay the ransom because they i) do not want their victimisation to become public and ii) want to resolve the matter quickly.
- ***Public and private interests often clash*** to hinder the search for justice.
- *Needs co-ownership of problem to co-produce the solution*