

# ***The Transnational Cybercrime Extortion Landscape and The Pandemic:***

*Changes in offender tactics,  
attack scalability and the  
organisation of offending”*

CEPOL, 5 May 2021

Professor David S. Wall,  
[d.s.wall@leeds.ac.uk](mailto:d.s.wall@leeds.ac.uk)



# Abstract



UNIVERSITY OF LEEDS

The sudden change in work, recreation and leisure practices brought about by lockdown and especially the shift towards working from home caught many organisations and their employees unaware.

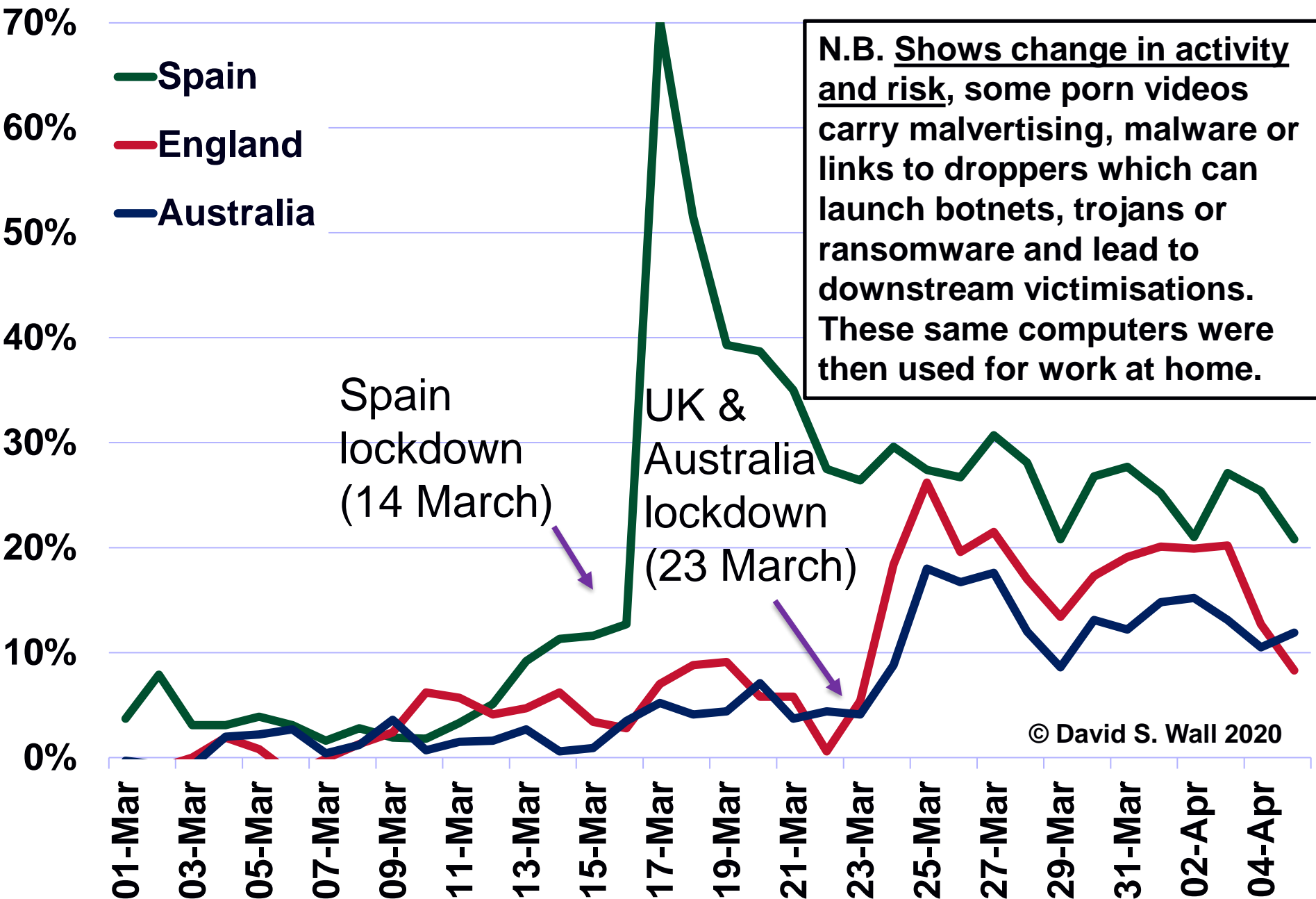
Cybercriminals shifted their target towards home workers as a way into organisations. The upshot was a massive acceleration in major cyberattacks upon organisations, but a noticeable shift in offender tactics towards naming and shaming victims and also changes in the organisation of offenders online. Such attacks impact negatively upon economies as they try to recover from the impacts of lockdown.

Drawing upon an analysis of 3800+ international ransomware cases collected for the EPSRC EMPHASIS & CRITICAL projects, this paper will chart the changes in crime, the changes in crime organisation and also their implications for transnational policing. Plus it introduces the cybersecurity data sharing paradox which impedes attempts at co-production and co-operation in providing a solution to the problem.

- 1. The lockdown disrupted normal behaviour & changed cybercrime attack vectors – accelerated exposure of new vulnerabilities and increased the scale & impact of cybercrime**
- 2. The shifts in cybercrime are best demonstrated by the evolution of ransomware tactics from RW1.0 to RW2.0 which blends social action with the science**
- 3. Cybercrime actors are now supported & facilitated, by a ‘professional’ ecosystem incentivised by the high yield**
- 4. New challenges of cybercrimes for law and enforcement**
- 5. Conclusions – Focus upon the various stages of the attack and the ecosystem surrounding the crime. Need to respond via co-production to overcome the cybersecurity data sharing paradox.**

# 1.0 Disruption to normal flows of online behaviour:

Access to Pornhub before and after the Covid-19 lockdown – *Pornhub Insights*



# 1.1 The changing cybercrime attack vectors



UNIVERSITY OF LEEDS

**The changes** (N.B. on top of already existing low level cybercrimes):

- Shift to **keystone cybercrimes** such as Data Theft, DDoS attacks, Ransomware and CryptoCrimes (and more)
- Shift **from attacking individuals to organisations** – Covid lockdown & work@home - Organisations are more lucrative.
- Shift to **using an affiliate business model** to distribute Malw
- Shift to **using more blended cybercrime tactics**, e.g. social science with science – e.g. naming and shaming + ddos etc
- Shift to **using human-operated** systems to infiltrate systems
- Shift **to using facilitators** – the cybercrime ecosystem
- Shift **to ephemeral business models** - planned obsolescence

## 1.2 The EFFECT of changing cybercrime attack vectors



UNIVERSITY OF LEEDS

**EFFECT – new tactics have increased scalability and impact**

- Increase in the overall volume of Cybercrime
- Increase in the level of harm caused by Cybercrime – financial, disruption, even physical harm, death?
- Increase in economic yield and payment streams
- Cybercrime is now a viable career choice
- A renewed criminal appetite for more cybercrime, especially keystone cybercrimes which harvest data
- Cybercrime is now supported by a larger ecosystem
- Cyberinsurance pays the ransom and fuels the crime – private interests clash with the public interest
- Cybercrime is becoming harder to police

## 2. Shifts in cybercrime demonstrated by the evolution of ransomware from RW1.0 to 2.0



**N.B. Lockdown accelerated changes that were already taking place.**

**Ransomware is a blended crime** as it *comprises more than one crime* and *combines the science with social actions* (social engineering)

There are **two important aspects of a ransomware attack** a) getting into the system and attacking it b) and getting victims to pay the ransom.

### **a) Changes in attack tactics**

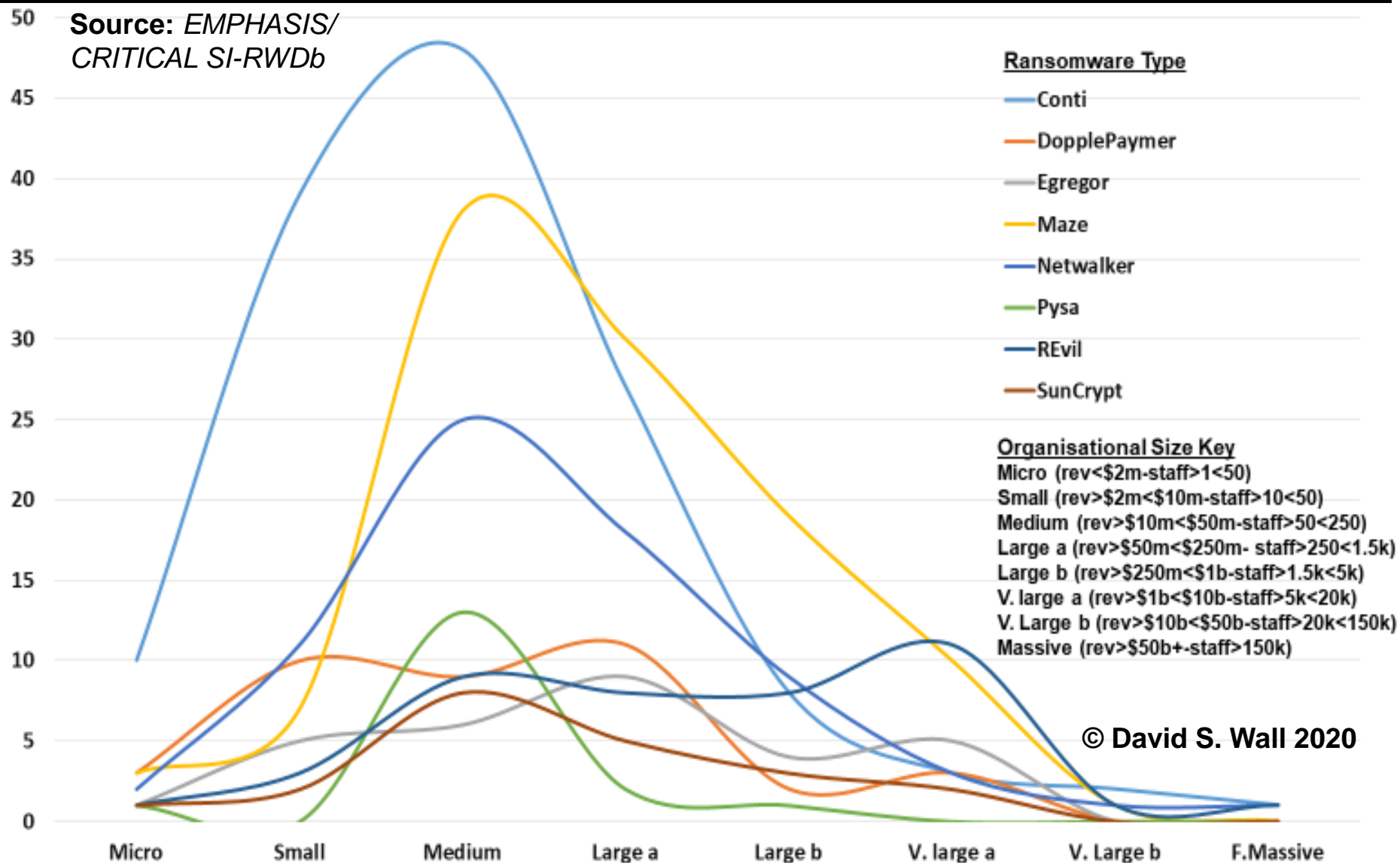
- big game hunting - phishing to ensnare key managers who have access
- exploiting lockdown disruption and insecure work-from-home systems
- once in an organisation, hackers move laterally to find key data to steal and plant encryption process – may be in the system for up to a year!
- encrypt at vulnerable times e.g. public holidays to compromise businesses
- attacking managing and cloud based service providers (1 attack hits 7-10 or more client organisations) & supply chain to scale up the attack
- tend to target small & medium (\$2m-\$10m-10-50 staff & \$10m-\$50m-50-250 staff) sized businesses (see graph) – security less sophisticated & can pay big ransom, usually part of supply chain so more impact?
- double attack – selling on unpatched vulnerabilities to other RW groups



## 2.2 Ransomware type by Organisational size – June-Oct 2020 $n=500$ cases



UNIVERSITY OF LEEDS





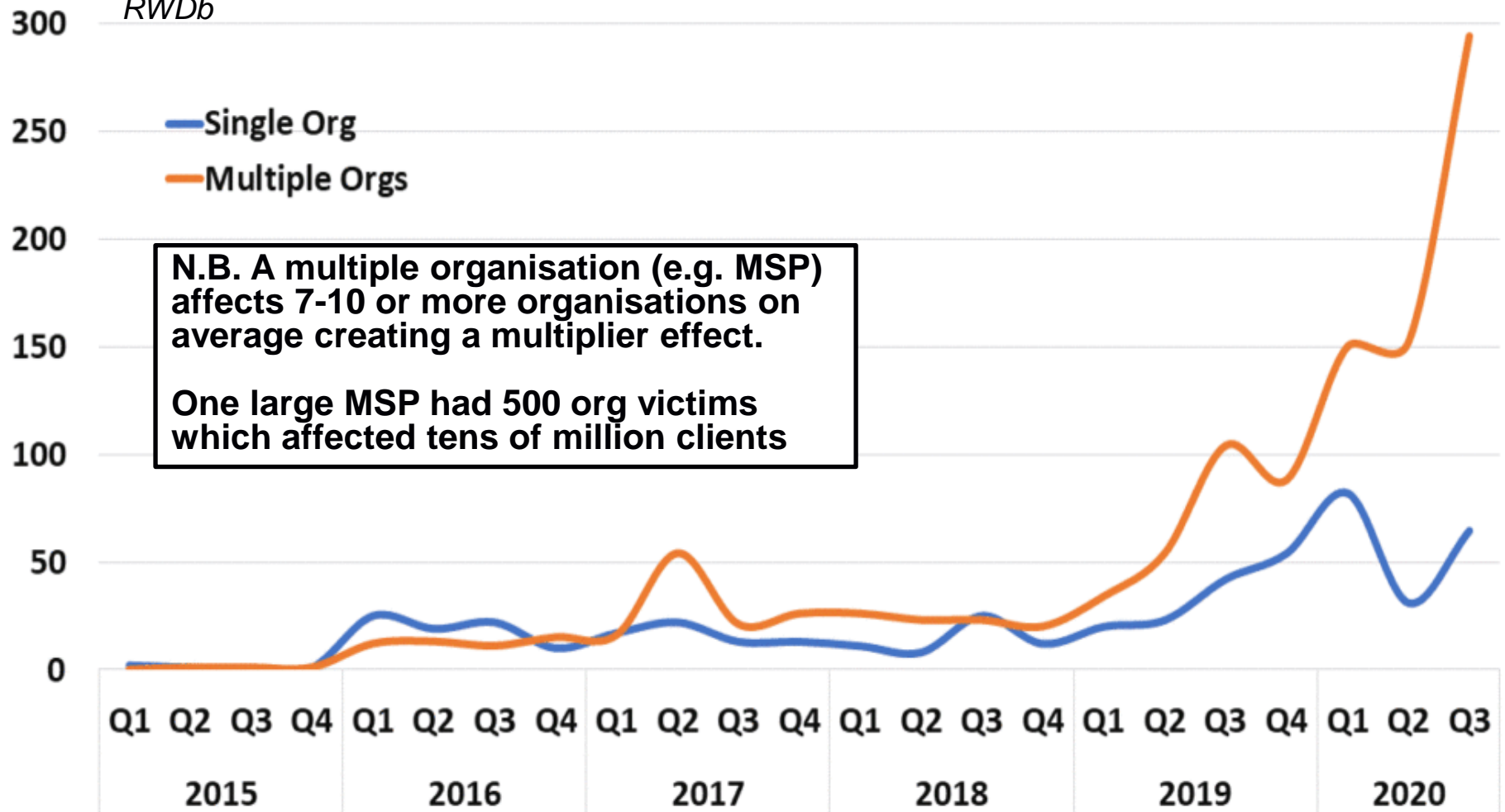
## 2.3 Changes in single vs. multiple attacks



UNIVERSITY OF LEEDS

Source: EMPHASIS/  
CRITICAL Main  
RWDb

### Single vs multiple (complex) organisational victims



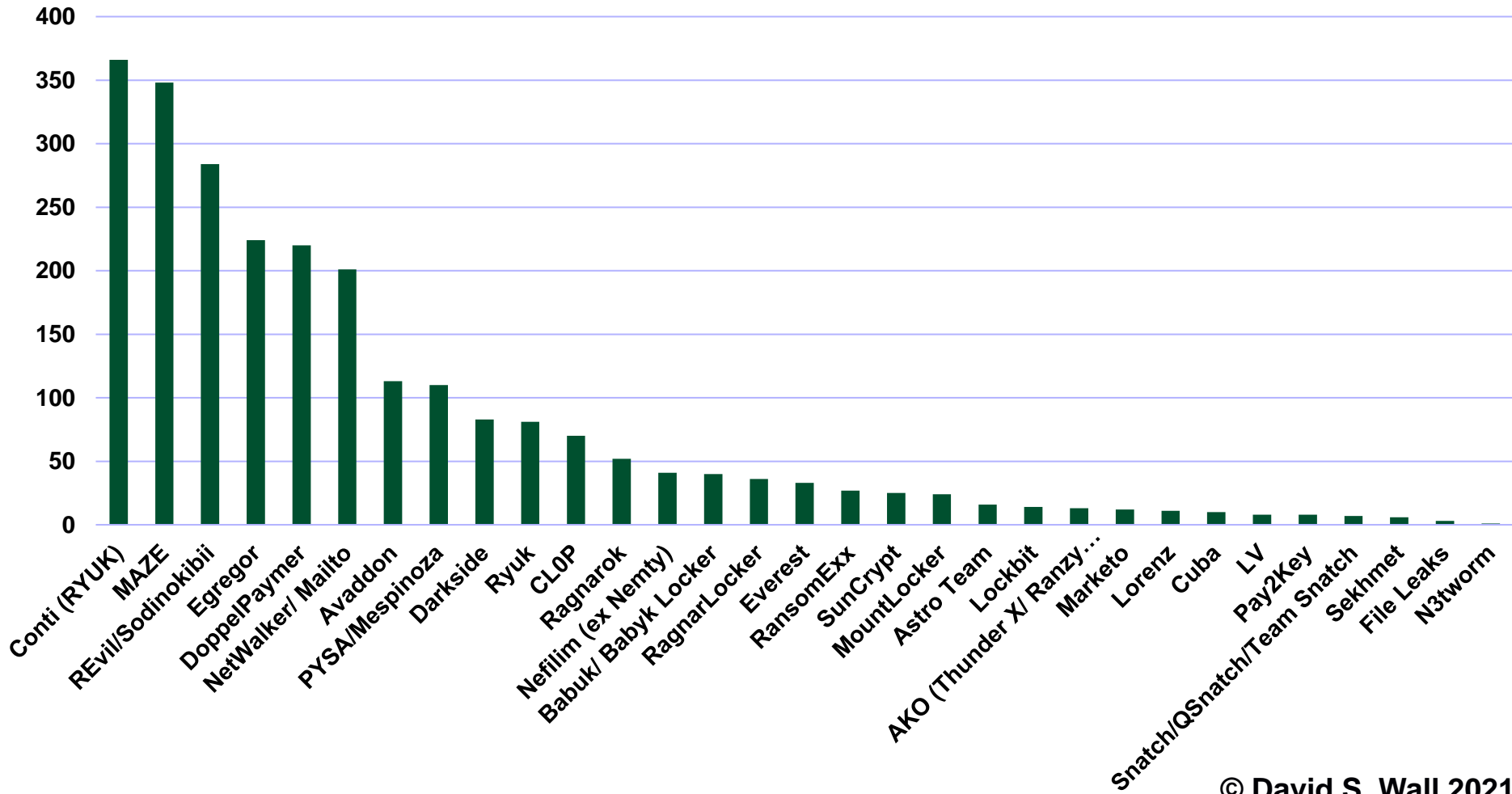
# Ransomware Gangs & Victimisations



UNIVERSITY OF LEEDS

## Ransomware Victims (Organisations) - Jan 19 - April 21

(2500 Orgs - 32 Groups - source EMPHASIS/CONTRAILS Main RW Db)



## 2.4 CONT ... Shifts in cybercrime - the evolution of ransomware



UNIVERSITY OF LEEDS

### **b) making victims pay the ransom by employing new tactics to increase victim fear & disruption - & pay ransom**

- *exfiltrating confidential business information & trade secrets before encryption – which they publish if ransom not paid*
- *naming and shaming victims online on offender www sites*
- *developing RW cartels (e.g. sharing naming www sites) - publishing portions of stolen data to show i) proof of attack ii) 5% after week 1 ii) 10% after week 2 and so on iii) all data*
- *taking out Facebook ads to shame victims (RagnarLocker)*
- *some RW now include DDoS attacks during demand period*
- *some levy 2 ransoms 1<sup>st</sup> for decryption key 2<sup>nd</sup> to delete data*
- *when ransom not paid, data is often publicly auctioned off*
- **ransomware attacks should be regarded as major data theft incidents – reporting data losses will help statistics, see later discussion**

## 2.5 Naming and Shaming Victims



UNIVERSITY OF LEEDS

A screenshot from ShadowIntel (cybersecurity company) which provided details of the victims of the various ransomware groups that were ‘allegedly’ part of a ransomware cartel. The ‘service’ was provided because the cartel’s name and shame www site was situated on Tor and not readily accessible. It names the victim, shows its worth, and size and how much data has been dumped. When a main part of the cartel group announced it was ceasing business at the end of October, ShadowIntel also disappeared about that time.


The Shadow Intelligence ransomware breach monitoring service has detected a newly published disclosure.

This ransomware newsletter serves to inform our subscribers when any of the notorious ransomware groups disclose having allegedly breached a new victim organization or when they have leaked compromised data of a previously allegedly breached organization.

RANSOMWARE	Maze
VICTIM	Jekyll Island - Full dump (100%)
INDUSTRY	Professional & Consumer Services
SECTOR	Facilities
REVENUE	\$40 Million
EMPLOYEES	200
PUBLICLY DISCLOSED	No
COUNTRY	United States
ISO2	US
VICTIM URL	<a href="https://www.jekyllisland.com">https://www.jekyllisland.com</a>
DESCRIPTION	Jekyll Island is an island located on the coast of Georgia mid-point between Savannah and Jacksonville, Florida.

Respectfully,  
Shadow Intelligence

[Twitt](#)



# WARNING

Your personal files are encrypted

**11:57:**

Your documents, photos, databases and other important files have strongest encryption and unique key, generated for this computer. key is stored on a secret Internet server and nobody can decrypt you pay and obtain the private key. The server will eliminate the key after specified in this window.

Open <http://bs7aygqtd2rnjl4o.onion.link> or <http://bs7aygqtd2rnjl4o.torstorm.org> or <http://bs7aygqtd2rnjl4o.tor2web.org> in your browser. They are public gates to the secret server.

If you have problems with gates, use direct connection:  
1) Download TOR Browser from <http://torproject.org>  
2) In the Tor Browser open the <http://bs7aygqtd2rnjl4o.onion> (Note that this server is available via Tor Browser only. Retry in 1 min if not reachable).

Write in the following public key in the input from on server:



Main Full dump

Contact Us

Millwright Regional Council of Ontario, the company does not want to cooperate with us, so we give them **240 hours** to communicate and cooperate with us. If this does not happen before the time counter expires, we will leak valuable company documents. We have investment documents, financial documents and reports, income statements, agreements and contracts, and more.

Also remember that data cannot be decrypted without our general decryptor. And your site will be attacked by a DDoS attack.

**BABUK**

## Metropolitan Police Department DC

mpdc.dc.gov stolen more 250 GB data



**BABUK**

## Hello World 2

### PD and Closed

Hello! We are happy to inform you that PD was our last goal, only they now determine whether the leak will be or not, in any case, regardless of the outcome of events with PD, the babuk project will be closed, its source codes will be made publicly available, we will do something like Open Source RaaS, everyone can make their own product based on our product and finish with the rest of the RaaS

Everest ransom team

OLD

# Department of Agriculture

This is customer data, employee data and other very important documents

Company:	Department of Agriculture
Address:	Elliptical Road, Dillman, Quezon City, Philippines
Website:	<a href="https://www.da.gov.ph/">https://www.da.gov.ph/</a>
Email:	info@da.gov.ph
Phone:	63289288741 63282732474
Files:	coming soon
Published data:	24 GB

### DarkSide Leaks

## OAK VALLEY COMMUNITY BANK - More then 75 GB of sensitive data

Included:


- Credit Reports
- Financial documentation
- Insurances
- Declarations
- Correspondence
- Loan Documents
- Passports and driver licences

All data are fresh and will be stored on our CDN server for the next 6 month if you don't pay.  
If you need proofs, we will provide you with them.

Some examples of your sensitive data:

such an organization has huge security gaps, we will publish as possible and pay us, otherwise we will publish

### Home Page of Ragnar\_Locker Leaks site



#### WALL OF SHAME

Here will be permanent list of companies who would like to keep in secret the info leakage, exposing themselves and their customers, partners to even greater risk than a bug-hunting reward!

company.  
updated 10/13/2020 12:00  
views: 4647 | Published: 10/08/2020 15:19:52

**Source: Darktracer**





Thursday at 14:40

#1

Hello! We are starting a set of a limited number of advertisements for our product, more precisely, 3 products:

- 1) Win Ransom
- 2) Esxi Ransom
- 3) Nas Ransom

**Common in all three lockers:** [the ability to put arguments at startup, written in native languages, an innovative and thoughtful approach to the cryptoscheme of the Ransom, offline storage of master keys]

If someone starts claiming that new algorithms = new security threats, then we are ready to defend our position by screenshots of our partners' payments.

#### Distinctive points:

---> windows: [stained encryption, freeing files, own implementation of a thread pool with a queue, debugging, connecting hidden drives]

---> esxi: [special encryption scheme for virtual machines, hyperthreading with queue, log and statistics on completion to the console]

---> nas: [support two main types of NAS (QNAP, Synology), smudge encryption, log to console]

From the very beginning of development, tests were carried out exclusively in combat conditions, all bugs were caught and fixed 'on the fly' (thanks to researchers)

There is a blog, the data that is merged into the blog is hosted on our servers

#### Mass Media about us:

<https://www.mcafee.com/blogs/other-blogs/mcafee-labs/babuk-ransomware/>  
<https://www.computerweekly.com/news/252496839/Babuk-ransomware-unsophisticated-but-highly-dangerous>  
<https://www.computerweekly.com/news/252495684/Serco-confirms-Babuk-ransomware-attack>  
<https://blog.cyberint.com/babuk-locker>  
<https://threatpost.com/ransomware-babuk-locker-large-corporations/162836/>  
<https://www.bleepingcomputer.com/news/the-first-new-enterprise-ransomware-of-2021/>  
<https://www.zdnet.com/article/ransom-esxi-exploits-to-encrypt-virtual-hard-disks/>  
<https://www.healthcareitnews.com/news/hind-nhs-test-and-trace-hit-ransomware-attack>

# Ransomware Gang Recruitment

Source: Darktracer

#### White list:

- 1) Hospitals (Exception only private plastic clinics and dentistry)
- 2) Charitable foundations and associations that have no income
- 3) Companies with an annual turnover of less than \$ 30 million for a zoomed
- 4) The following list of countries: CIS, China, Vietnam, Cyprus, RF

**We do not need fans to cover the network through GPO, etc. without understanding virtualizations, as well as**

**fans do not turn off the AV, but drag the virtual machine into the network, lure a bunch of disks there and encrypt it over the network.**

**Locker is tailored for complex server infrastructures ESXi, Hyper-V**

## What do you need to get to us?

1. Speak Russian fluently (no google translate)
2. Have a short interview regarding hyper-v and esxi (if you have never worked with this, you may not even write)
3. Show screenshots of payments from other PP
4. Or make a deposit in your profile in the amount of 15,000 USD

NO AVATAR

darksupp

Welcome to DarkSide

Premium

check in : 04.11.2020

Posts : 17

Reactions : 28

Deposit : 23.0008 \$

Yesterday at 23:41

Thread Starter

#6

#### Next updates:

- Automatic test decrypts. From this moment on, the whole process from cryptographing the target to the withdrawal of funds is automated and does not require the participation of a support.
- DDOS targets (L3, L7) are available, at our expense, we hold for a long time until the target goes online.

Now about the important thing, we have grown enough both in terms of the client base and in relation to other projects (based on the analysis of public information) and are ready to expand our and partner teams in two directions:

#### • Pentesting networks.

We are looking for one person or a team, integrate into the work environment and provide employment. A high percentage, the ability to make networks that cannot be realized alone. New experience and stable income.

#### • Supply of networks.

Working both with us and with partners, before issuing networks, we will provide statistics of partner payments (as agreed). When delivering on our product and paying the ransom, we will guarantee an honest distribution of funds. Dashboard for monitoring the results for your target. We only accept networks where you run our payload.

In the two directions above, you need to write in the LAN with the topic "Penetration Testing" or "Networks" and pass an interview.

## 2.6 There are nine basic stages to a ransomware attack



UNIVERSITY OF LEEDS

1. Identify the best victims to attack – the reconnaissance
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. Monetaring the crime – cryptocurrency into fiat money
9. Post-crime - “getting away” with the crime once completed



### 3. Cybercrime is now supported by an 'professional' ecosystem



UNIVERSITY OF LEEDS

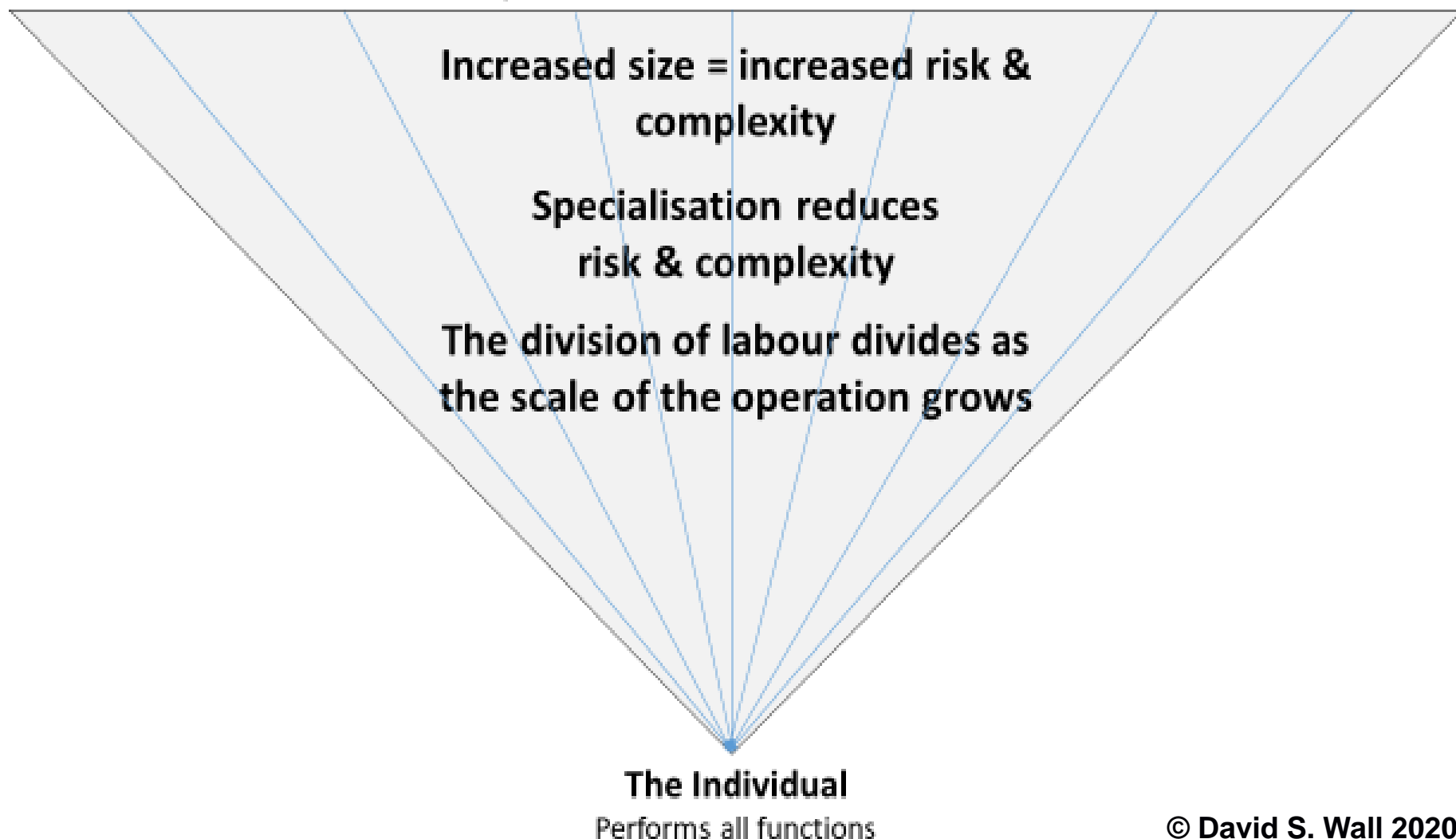
- a) **Cybercrime facilitated by Cryptocurrencies** – Bitcoin is the chosen value-exchange. Crime has arguably, has kept the value of Bitcoin high! Orgs now keep stocks of BTC
- b) **The economic yield is changing criminal career choices** – offenders choosing crime as a career because of income. Either as a primary offender carrying out the crime, or as a secondary offender facilitating it.
- c) **Creating new forms of online organised crime groups** – that are not Mafia types, but ephemeral and fluid. The new online OCGs are built around key skill sets (brokers) and affiliates, which form the cybercrime ecosystem. They tend to be flat ephemeral structures with planned obsolescence & not hierarchical and sustained (like Mafias) – relatively disorganised by comparison. See next slide.

# 3.1 Making cybercrime pay and moving from a hobby to a career choice



UNIVERSITY OF LEEDS

Databrokers – Crimeware aas – Spammers – Darkmarket – Botherders – IT Services - Monetisers



## 3.2 The Cybercrime Ecosystem



UNIVERSITY OF LEEDS

© David S. Wall 2021

### DATABROKERS

Sell/ Trade Stolen Datasets

Sell Victim profiles

Sell Access to Illegal data streaming

*Data is used by offender groups in different ways*

### DARKMARKETEERS

Providing selling/ trading services  
(usually via the ToR network)

### ENGAGERS

Engage victims and sell  
on details

### CRIMEWARE-as-a service

Rent out:

DDoS Stressers

Ransomware-as-a-service

Spam-ware-as-a-service

Botnets (Botherders)

### MONETIZERS

Organise and Manage a financial  
return

Crypto-exchange

Money laundering

Money mules

Financial advisers

### BULLETPROOF HOSTERS

Web hosts which allow criminal  
www materials

### CRIME IT SERVICE BROKERS

Sell and write code

Sell vulnerabilities (Bug Brokers)

### NEGOTIATORS

Negotiate with offenders –  
e.g ransom

# 4. 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 eng & 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.
- Not helped by the fact that:
  - *Ransomware is largely under-reported*, though some offenders publish victims names.
  - *Ransomware is under-prosecuted*, which means little court experience across the CJS.
  - *Policing ransomware becomes problematic when victims and offenders are in different jurisdictions* or more than one (see the Blackbaud case).
  - *Ransomware may be big globally, but is small locally*, so local police get little experience of dealing with the crime. However, the UK ROCU model connects local and national police regionally and is fairly well regarded by police and also respected by industry.

## 5. Conclusions – overcoming the cybersecurity data sharing paradox



UNIVERSITY OF LEEDS

- Lockdown has accelerated cybercrime trends already in play.
- Ransomware is now big business and is changing the way offenders organise themselves online. Is not only developing a professional ecosystem, but providing alternative career choices.
- The public interests differ from the private interests and *while we all agree on the problem and end goal, basically we disagree about how to achieve them*, so we do not actually work together and share data (cybersecurity data sharing paradox).
- *At a basic level* breaking down the cybercrime process into stages enables LE to focus on the various stages of the attack (inc. the components of the cybercrime ecosystem).
- *At a broader level* solutions need to respond via a co-production to overcome the cybersecurity data sharing paradox
- CyCri is bigger than governments (WEF) - New anti-RW initiatives – no more ransom – IST Task force – White House?

# References [From the EPSRC EMPHASIS/ CRITICAL/ TAKEDOWN Projects]



UNIVERSITY OF LEEDS

- **Atapour-Abarghouei, A., McGough, S. and Wall, D.S. (2020)** 'Resolving the cybersecurity Data Sharing Paradox to scale up cybersecurity via a co-production approach towards data sharing,' *Proceedings of the 4th International Workshop on Big Data Analytics for Cyber Intelligence and Defense*, 2020 IEEE International Conference on Big Data (IEEE Big Data 2020) December 10-13. <https://arxiv.org/pdf/2011.12709.pdf>
- **Connolly, A. and Wall, D.S. (2019)** 'The Rise of Crypto-Ransomware in a Changing Cybercrime Landscape: Taxonomising Countermeasures, *Computers and Security*, 87(Nov), Available online 10 July, <https://doi.org/10.1016/j.cose.2019.101568>
- **Goldsmith, A. and Wall, D.S. (2019)** 'The seductions of cybercrime: adolescence and the thrills of digital transgression', *European Journal of Criminology*, Advance Online First from 9 Dec., <https://doi.org/10.1177%2F1477370819887305>
- **Musotto, R. and Wall, D.S. (2020)** 'More Amazon than Mafia: More Amazon than Mafia: Analysing a DDoS Stresser Service as Organised CyberCrime', *Trends in Organized Crime*, <https://doi.org/10.1007/s12117-020-09397-5>
- **Porcedda, M.G. and Wall, D.S. (2019)** 'Cascade and Chain Effects in Big Data Cybercrime: Lessons from the TalkTalk hack', *proceedings of WACCO 2019: 1st Workshop on Attackers and Cyber-Crime Operations*, IEEE Euro S&P 2019, Stockholm, Sweden, 20 June [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3429958](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3429958)
- **Wall, D.S. (2017)** 'Crime, security and information communication technologies, in *The Oxford Handbook of the Law and Regulation of Technology*, Oxford: Oxford University Press. [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3005872](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3005872)
- **Wall, D.S. (forthcoming)** 'Cybercrime: The Internet as a Conduit for Transnational Organised Criminal Activity', Allum, F. and Gilmour, S. (eds) *Routledge Handbook on Transnational Organised Crime*, 2nd Edition, Routledge [uses Ransomware as example of modern cybercrime]