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
Abstract

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

N.B. Shows change in activity and risk, some porn videos carry malvertising, malware or links to droppers which can launch botnets, trojans or ransomware and lead to downstream victimisations. These same computers were then used for work at home.
1.1 The changing cybercrime attack vectors

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

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

Source: EMPHASIS/CRITICAL SI-RWDb
2.3 Changes in single vs. multiple attacks

Source: EMPHASIS/Critical Main RWDb

N.B. A multiple organisation (e.g. MSP) affects 7-10 or more organisations on average creating a multiplier effect.

One large MSP had 500 org victims which affected tens of million clients.
Ransomware Gangs & Victimisations

Ransomware Victims (Organisations) - Jan 19 - April 21
(2500 Orgs - 32 Groups - source EMPHASIS/CONTRAILS Main RW Db)

© David S. Wall 2021
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 1st for decryption key 2nd 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 helps statistics, see later discussion
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.
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.

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

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

### DarkSide Leaks

**OAK VALLEY COMMUNITY BANK - More than 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:

**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.

**Source: Darktracer**
Ransomware Gang Recruitment

Source: Darktracer

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
2.6 There are nine basic stages to a ransomware attack

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. Monetarising 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

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

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

Increased size = increased risk & complexity

Specialisation reduces risk & complexity

The division of labour divides as the scale of the operation grows

The Individual
Performs all functions
3.2 The Cybercrime Ecosystem

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)

Crime as a Service
- Rent out:
  - DDoS Stressers
  - Ransomware-as-a-service
  - Spam-ware-as-a-service
  - Botnets (Botherders)

Bulletproof Hosters
- Web hosts which allow criminal www materials

Crime IT Service Brokers
- Sell and write code
- Sell vulnerabilities (Bug Brokers)

Monetizers
- Organise and Manage a financial return
- Crypto-exchange
- Money laundering
- Money mules
- Financial advisers

Negotiators
- Negotiate with offenders – e.g. ransom

Engagers
- Engage victims and sell on details
4. The new challenges of cybercrime for law and enforcement

- **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

• 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?


