The Transnational Cybercrime Extortion Landscape and the Pandemic: Changes in ransomware offender tactics, attack scalability and the organisation of offending

David S. Wall
School of Law, University of Leeds

Abstract
The sudden disruption of work, recreation and leisure practices caused by the COVID-19 lockdown caught many organisations and their employees unaware, especially during the move towards working from home. This led adaptive cybercriminals to shift their own focus towards home workers as a way into organisational networks. The upshot was a massive acceleration in major cyberattacks upon organisations and a noticeable shift in offender tactics which scale up levels of fear in victims to encourage payment of the ransom. Such tactics include a shift towards naming and shaming victims, the theft of commercially sensitive data and attacks targeting organisations which provide services to other organisations. These developments have also led to changes in the organisation of offenders online. Such attacks negatively impact upon national and international economies as they try to recover from lockdown. Drawing upon an analysis of 4000+ cases of ransomware attacks collected for the EPSRC EMPHASIS & CRITICAL research projects, this paper charts the evolution of ransomware as a modern cybercrime and also changes in the organisation of cyber-criminals as well as highlighting some of the implications for transnational policing.

Keywords: Cybercrime, Ransomware, Crime and the Pandemic, Organised Cybercrime, Policing cybercrime

Introduction[1]

The 2020 COVID-19 lockdown immediately disrupted the routine behaviour of billions of people globally by suddenly forcing them to stay indoors and, in many cases, work at home. In order to pass their time many took to their computer devices for leisure and pleasure and to communicate with others. Very often, workers had to use their personal computing equipment along with varying levels of personal security and risk awareness. These changes in routine behaviour were not lost on criminals who quickly adapted in order to defraud individuals and organisations or gain access to their networks to inflict more cybercrime. While there were no new patterns of cybercrime victimisation, other than pandemic specific scams, there was, however, a visible change in cybercrime attack vectors which accelerated the exposure of new pandemic related vulnerabilities and increased the overall scale and impact of cybercrime. These changes are best demonstrated by the case of ransomware, which seeks to encrypt the victim's data and de-encrypt it once a ransom payment

[1] This article is based upon a paper delivered at the CEPOL (European Union Agency for Law Enforcement Training) Annual Research Conference, Featured Presentation 16.00, 5 May 2021. https://conference.cepol.europa.eu/cepol-online-conference-2021/talk/DBR7WE/

has been made. Through a gradual process of evolution, ransomware has effectively become a sophisticated billion-dollar business and ransomware actors are now supported and facilitated, by a 'professional' ecosystem that is incentivised by the high crime yield. Not only does this high yield provide serious future career alternatives for hackers during a time when job market security is uncertain, but it also introduces serious new challenges for law and enforcement as well as hindering economic recovery from the lockdown.

The first part of this article looks at how lockdown disrupted routine behaviours and changed cybercrime attack vectors. The second part explores the evolution of ransomware tactics to show how changes in cybercrime have accelerated because of lockdown. The third part shows how cybercrime actors are now supported by a 'professional' ecosystem incentivised by the high yield which facilitates modern cybercrime. Before concluding, the fourth part will briefly outline some of the new challenges that modern cybercrimes are posing for law makers and law enforcement, not least the need to focus different resources upon the various stages of the ransomware attack so that they can more effectively respond co-productively with cybersecurity stakeholders.

1. Lockdown and the disruption of routine behaviours

Different national announcements of lockdown took place over a period of weeks in March 2020 (see BBC, 2020)[2]. As indicated above, the public were forced to stay indoors to prevent the spread of the virus and many took to their computers to pass the time, but very often used those same computers to also work from home. To illustrate the disruption of routine behaviours *Pornhub*, a site which enables pornographic materials to be uploaded and accessed by users, revealed in their 'insights' section[3] the changes in access to their web sites worldwide. Figure 1 plots these reworked access statistics to show the changes on three dates where various countries decided to lockdown (March 11, March 14, and March 23). The data show large spikes in access, which indicate marked changes in user's online behaviour and activities and also changes in their perceptions of risk, accepting more risk, either for gain or excitement or both, although not discussed here further, see the application of Katz's 'sneaky thrills' to cybercrime in Goldsmith & Wall (2019).

Pornographic videos and other accessed materials[4] are known vehicles for carrying malicious advertising (malvertising), malware (malicious software) or links to droppers which can launch botnets, trojans or ransomware and lead to further victimisations (Dashevsky, 2017). Please note, however, that this is not to suggest that pornographic materials are the only means of delivering malicious software. Computer Gaming, for example, is also known for making users vulnerable to victimisation. The key point here is that computer devices mainly used for leisure purposes were, after lockdown, often the same computers that were also used for working at home. Because of this many organisations were caught unawares and were forced to quickly improvise to improve their safety, although some were clearly not quick enough.

Changing cybercrime attack vectors

The increase in vulnerabilities arising from using personal computers for work and also any changes in perceptions of risk arising from working in an unsupervised setting did not go unnoticed by cyber offenders. Adaptive offenders exploited the new situation by, on the one hand, mounting arrange of COVID related scams and frauds, such as fake PPE materials, fake COVID medication through to fake COVID inoculation certificates and also Tax refund scams (Action Fraud, 2020). On the other hand, the changed situation also provoked an expansion in phishing expeditions, which send out provocative emails designed to 'engage' a public with more time on its hands. Phishers, who usually send spams out on behalf of clients (scammers or engagers[5]) as-a-service, deliberately "use human cognitive and behavioural attributes to design phishing attacks and to trick their victims into taking desired actions" (Abroshan et al., 2021). Using the COVID pretext, spam emails either sought to directly scam recipients, usual-

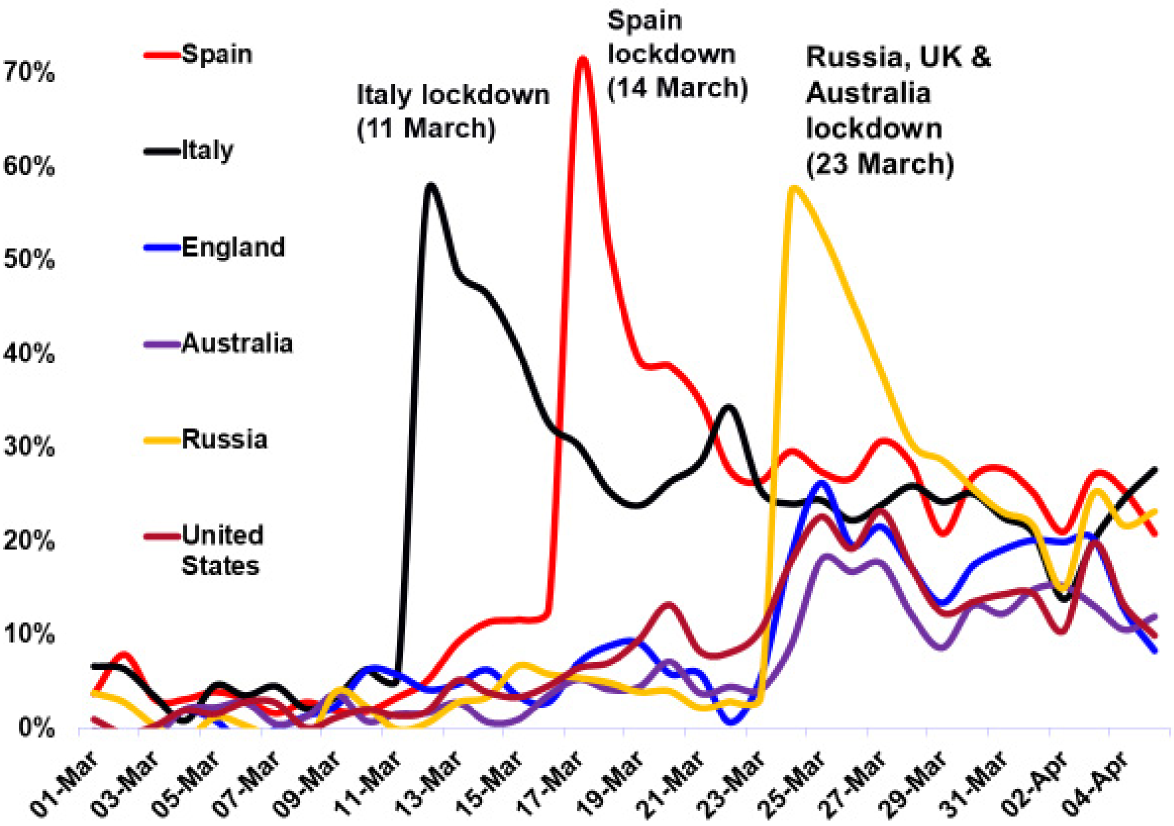
[2] This paper focusses upon the initial 2020 Q1 lockdown which occurred very quickly and caused the most disruption to established behaviours and practices. Adaptation to the change prepared the public and organisations for subsequent lockdowns and did not have such as sudden impact upon behaviours as Figure 2 indicates.

[3] N.B. URL not supplied. I am grateful to Pornhub insights for supplying these statistics. Italy, Spain, Russia, UK, Australia chosen because of lockdown dates to visualise its impact.

[4] This is meant as a statement of a general change in behaviour across the field and does not suggest that Pornhub specifically would be prone to these malicious downloads.

[5] I am differentiating here between scammers who seek to trick recipients into parting with money and engagers who seek essential information about recipients to use against them in the future.

Figure 1 Disruption to normal flows of online behaviour: Access to Pornhub before and after the COVID-19 lockdown in 2020 – source: reworked Pornhub Insights Data ©David S. Wall 2021



ly putting a COVID twist on the everyday scam emails (NCSC, 2020), or they sought to 'engage' recipients in other ways, if only to get them to respond. Sometimes simply by provoking recipients to elicit a rude response from them. In the latter case any response provides the engager with basic information that the email account is active and often some basic contact details also if the responder includes their signature. This information is particularly useful if the signature relates to the recipient's workplace as it indicates to the engager that the responder could be further pursued and provoked into providing more information that could be used to gain access to their work organisation[6].

The outcome of these phishing 'engagements' is that, on top of already existing low-level cybercrimes (bulk scams and minor hacks etc.), there was also an increase in higher-level keystone cybercrimes such as data theft, DDoS attacks, ransomware and cryptocrimes (and more). IBM found that ransomware and data theft were in the top three cyberthreats, with data theft having increased by 160% since 2019 (IBM, 2021: 7). They are called Keystone cybercrimes here because they support further cybercrimes. Data theft, for example, is an essential part of most modern cybercrimes and can be sold in dark markets (Hutchings & Holt, 2015) and used to launch low level cybercrimes (see further the discussion over cybercrime cascades in Porcedda & Wall, 2019; 2021).

There has also been a noticeable change in offender tactics, accelerated by the COVID lockdown vulnerabilities identified earlier, from attacking individuals towards attacking organisations - which are much more lucrative targets than individuals. Importantly, lower-level ransomware attacks on individuals appear to remain much as before, but what the data and cybersecurity literature indicates that either new sets of criminal actors have entered the field or existing actors have escalated their ambitions (see for example Accenture, 2021).

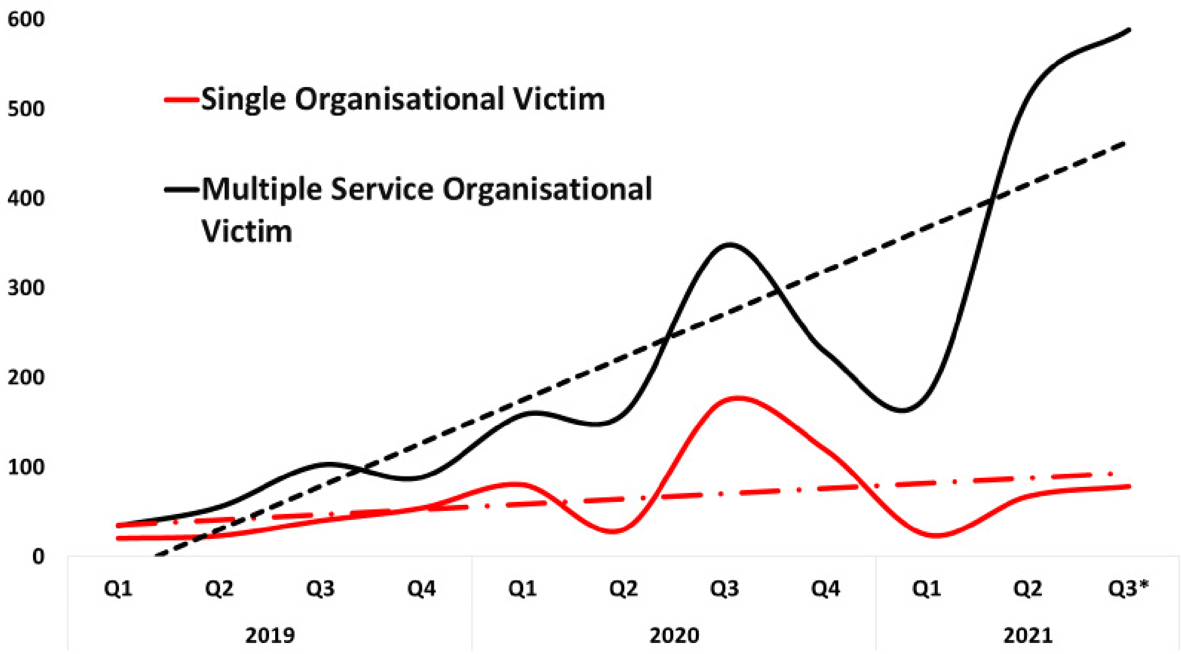
[6] See further Abroshan et al., (2021) for their useful discussion on the act of phishing.

In order to commit a cybercrime, offenders are increasingly using more blended tactics that combine more social action with scientific tactics. Encryption plus data exfiltration and naming and shaming victims, as well as using DDoS attacks create even more fear of business disruption and compliance (Abrams, 2021a). On the technical side, ransomware operators have also begun using affiliate business models in their crimeware-as-a-service market to distribute malware to victims (see Kivilevich, 2020). On the social side they are also using human-operators to infiltrate networks (explained later). Offenders are themselves using various facilitators or brokers to help them facilitate their crimes which constitute the cybercrime ecosystem. Finally, there has been a noticeable shift towards ransomware operators designing ephemeral business models around their cybercrime operations which plan-in a sudden obsolescence to frustrate law enforcement efforts (Connolly & Wall, 2019).

The *effect* of changing cybercrime attack vectors

The effects of changing cybercrime attack vectors are manyfold, to the point that they are now a serious threat to global economies and the post COVID economic revival. On the one hand the financial impact is crudely measured in billions of dollars. Emsisoft (2021) examined the impact on 10 western countries and estimated that $18 billion was paid in ransoms in 2020 and that the overall cost of repairing damage could be as much as $80 billion (Emsisoft, 2021). On the other hand, the financial impact is a direct result of the increase in the scalability and overall impact of cybercrime activities which is illustrated in Figures 2 and 3 which both show the sudden rise in Q2 2020 in the overall volume of attacks (against an already rising trendline) as these tactics become effective. The decline in Q4 2020 and Q1 2021 is due to various ransomware gangs, such as MAZE, stopping their practice. The rise in Q2 2020 is partly due to them rebranding and relaunching, but also could be related to lockdowns during the second or third wave of COVID.

Figure 2: Increase in attacks multiple service victims 2019-2021 (with trendlines) N.B. Q3* 2021 is estimated from 1 month of data (Source: Main EMPHASIS RWDb n=4500+, ©David S. Wall 2021



The high incidence of ransom payment, as indicated above in the Emsisoft (2021) research, is a major incentive to offenders. This figure is driven by the increased use of cyber-insurance by victims. Whilst cyber-insurance does help them recover from attacks, the insurance companies' tactic of tending to pay the ransom to get the business operating again as soon as possible is controversial as it inadvertently fuels the crime (Scroxton, 2021).

The growth in the economic yield from cybercrime not only increases the criminal appetite and encourages more cybercrime, especially the keystone cybercrimes which harvest data for use in further crime. As mentioned in the introduction, the high yield combined with the demands for skills created by the cybercrime ecosystem unfortunately provides serious future career alternatives and further training for hackers in an uncertain job market. Moreover, all these effects create serious new challenges for law and enforcement, making it harder to police.

2. The evolution of cybercrime demonstrated by the development of ransomware from RWv.1 to RWv.2 to RWv.3

Lockdown provided a fertile environment for accelerating trends in cybercrime that were already starting to take place and ransomware is a useful case study of a modern cybercrime which can illustrate this. The following findings are drawn from two EPSRC funded research projects into ransomware (EMPHASIS) and Cybercrime in the Cloud (CRITiCaL) and also informed by analysis of an open-source database of over 4500+ ransomware attacks compiled for these projects between 2011 and today[7].

Ransomware has always been a blended cybercrime as it *comprises more than one crime*, a computer misuse offence, and a crime of extortion, but the distribution of the blend has changed overtime as it has evolved. Figure 3 indicates three approximate phases of the evolution of ransomware which are related to the balance of misuse and extortion and the ways it is organised and delivered.

In the RWv.1 era (approx. 2011-2018)[8], the main modus operandi was to send out ransomware as an attachment in a phishing expedition (spamming) and to use the text of the message to get the recipient to open the email and respond. When responded to, the attachment or link, infected the recipient's computer causing them to pay the ransom to obtain a decryptor. These were fairly unsophisticated low-yield operations which relied on bulk-victimisation.

The RWv.2 era, in contrast (2018-2021), stepped up attacks on businesses away from individuals, and from late 2019, introduced additional social and business pressures into the mix. Not only did the attackers steal essential data before encryption but they also named and shamed businesses via their web sites. Both, to force victims into paying the ransom.

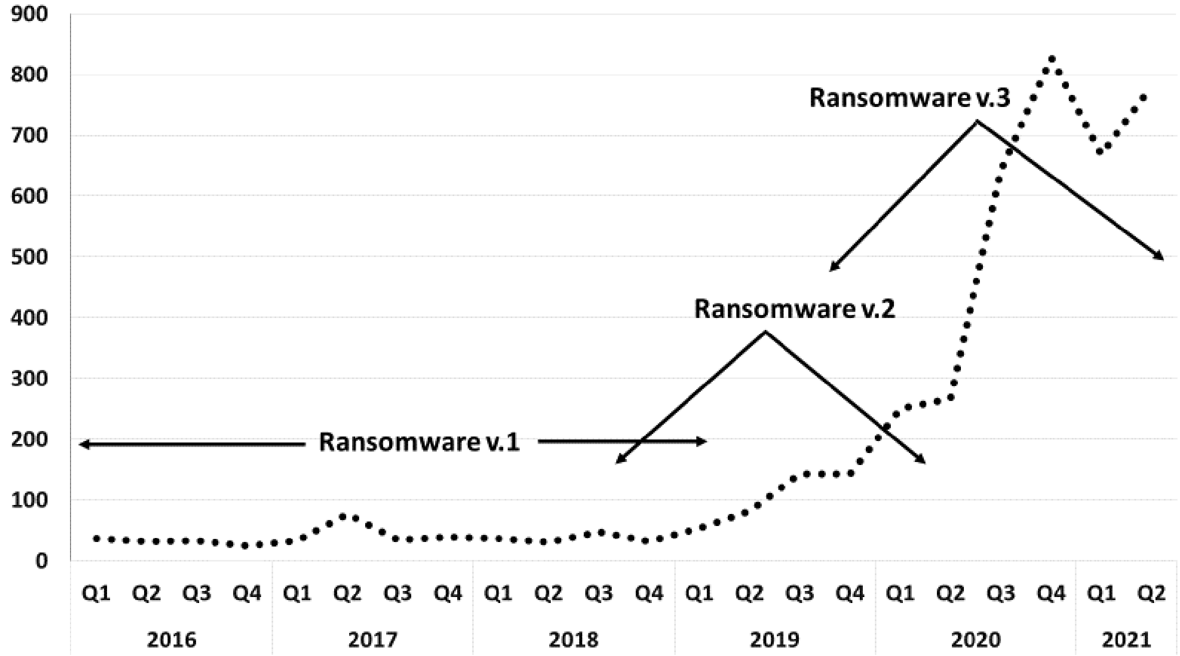
The RWv.3 era began to creep in from late 2019 to overtake RWv.2. Using similar tactics on businesses to those in RW v.2, RWv.3 combines these with additional higher order hacking skills to enter networks and move laterally across them to make the attack more effective. Some attacks are also 'human operated' rather than use the 'spray and prey' (attack everybody and see who falls victim) approach. In addition, RWv.3 offenders increase the scalability of their attacks by tending to attack multiple service providers and their supply chains to make secondary victims of the primary victim's clients and increase their pain enough to pay the ransom. Collectively, these actions increased the overall scale of attacks. What was a simple automated crime has become industrialised, for want of a better expression, by combining more *science* related skills with more intense *social actions* ranging from socially engineering victims into responding and also human-operated ransomware.

There are two important aspects of a ransomware attack a) getting into the system (*infiltration*) and attacking it b) and (*exfiltration*) stealing key data and getting victims to pay the ransom by creating fear and furthering their pain.

[7] N.B. There is a long list of caveats with regard to the ransomware data that will be explained in future publications, it is open source, mainly gathered by keyword searches. Since 2018/19 the attackers have changed the nature of their attacks and also (since 2019) publicly named victims. This information has leaked out to the public by journalists writing in the public interest, but is itself controversial as it arguably adds another layer of victimisation (see Brian Kreb's 2021 article).

[8] N.B. The dates are approximate. This describes the crypto-ransomware era and please note that there were pre-crypto ransomware eras (see further Connolly & Wall, 2019).

Figure 3: The evolution of ransomware that increase the scalability of attacks (*Source:* Main EMPHASIS RWDb n=4500+, ©David S. Wall 2021



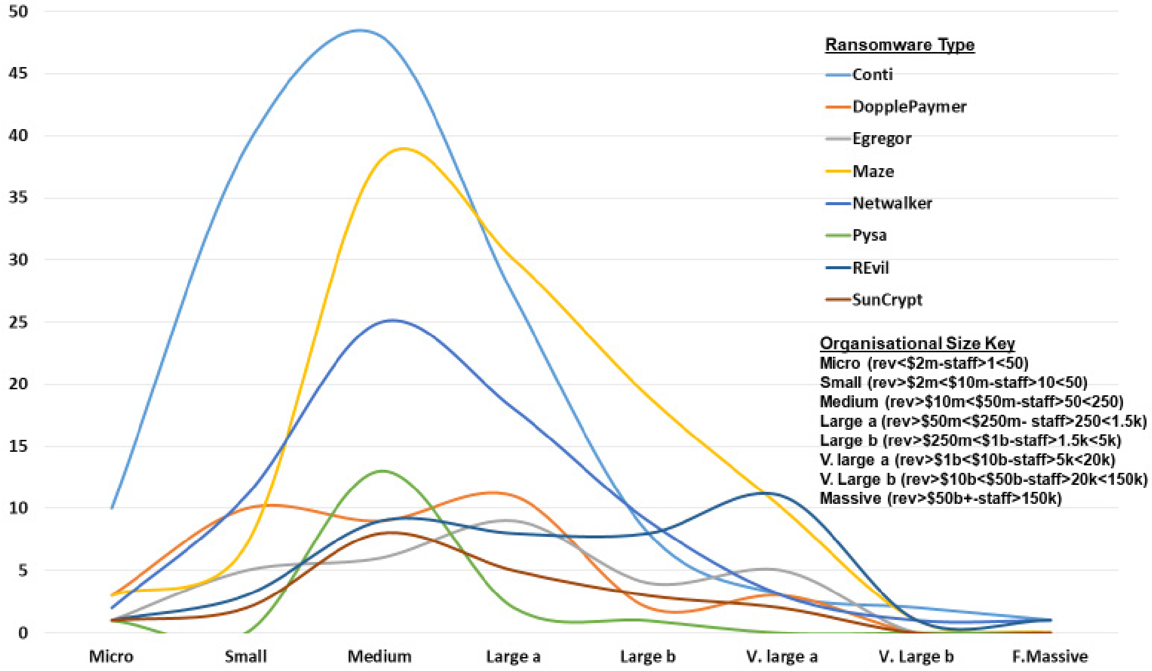
Infiltrating networks

As ransomware operators moved from RW1 to RW2 there was a noticeable shift in infiltration tactics away from 'spray and prey' tactics in phishing practices towards big game hunting. Big game hunting is a targeted phishing attack deliberately designed to ensnare specific groups. In the case of ransomware attacks, the focus is upon key managers in organisations who have access to the business network and often have higher user privileges. Big game hunting was accelerated by exploiting lockdown disruption and insecure work-from-home systems. Once in an organisation, hackers move laterally to find key data to steal and plant the encryption process. They may be in a network for anything from two weeks to over a year (Ilascu, 2020).

Attackers seem to activate the encryption process at vulnerable times for an organisation, especially at the start of public holidays when staffing tends to be at its lowest (Connolly & Wall, 2019; 10). The evidence is that ransomware gangs are increasingly attacking managed service providers and cloud-based-services, as described in RWv.3. Here, one attack hits between seven to ten of the victim's client organisations and their supply chains, and scales up the impact of the attack. In some cases, tens if not hundreds of secondary victims were involved also resulting in class actions and fines from information commissioners, which intensifies the pressure on the primary victim to resolve the situation quickly (Gatlan, 2020). The statistics and trendlines in Figure 2 & 3 show how attacks on multiple service organisations have markedly increased since mid-2019 as RWv.3 developed traction.

One rather surprising finding from the analysis of the data was that ransomware gangs tend to target SMEs (small & medium sized enterprises) ($2m-$10m-10-50 staff & $10m-$50m-50-250 staff) rather than very large business (see Figure 4). One reason for this may be that the cybersecurity of SMEs is less sophisticated, yet they can still afford cyber-insurance or to directly pay a relatively large ransom (see Figure 4). Very often these victims are part of a supply chain, so their own victimisation also impacts upon their clients. Repeat victimisation is becoming a new feature of ransomware following an increase in double attacks. This is either because the 'initial access brokers', who gain access to networks and then sell the access credentials to ransomware gangs sometimes install additional backdoors and also sell the details of these unpatched vulnerabilities to other ransomware groups (De Blasi, 2021). Or, sometimes ransomware attackers (affiliates) will use two types of ransomware, layering them on top of each other to 'net them the most money for the least amount of effort' (Callow cited by Newman, 2021).

Figure 4 Ransomware type by Organisational size – Data snapshot of the top 8 ransomware groups, June-Oct 2020 ***n=500 cases*** *(Source:* N&S RWDB, ©David S. Wall 2021)



Exfiltration

Once the encryption process has taken place, the ransomware gangs seek to make victims pay the ransom by disrupting their business flow. New tactics are constantly being employed to increase victims' fear and discomfort. They do this by naming the victims on their own 'leak' sites, often publishing an example of confidential business information, sometimes including trade secrets exfiltrated. The ransom note usually states that if the ransom is not paid in cryptocurrency by a specific deadline, then further portions of the stolen data will be published on the leak site. To make their operations more effective and compete successfully in a competitive market for victims some ransomware operators such as MAZE have formed cartels, in which they shared resources (for a fee) such as their leak websites where they publicly humiliate victim organisations in to paying the ransom demand[9].

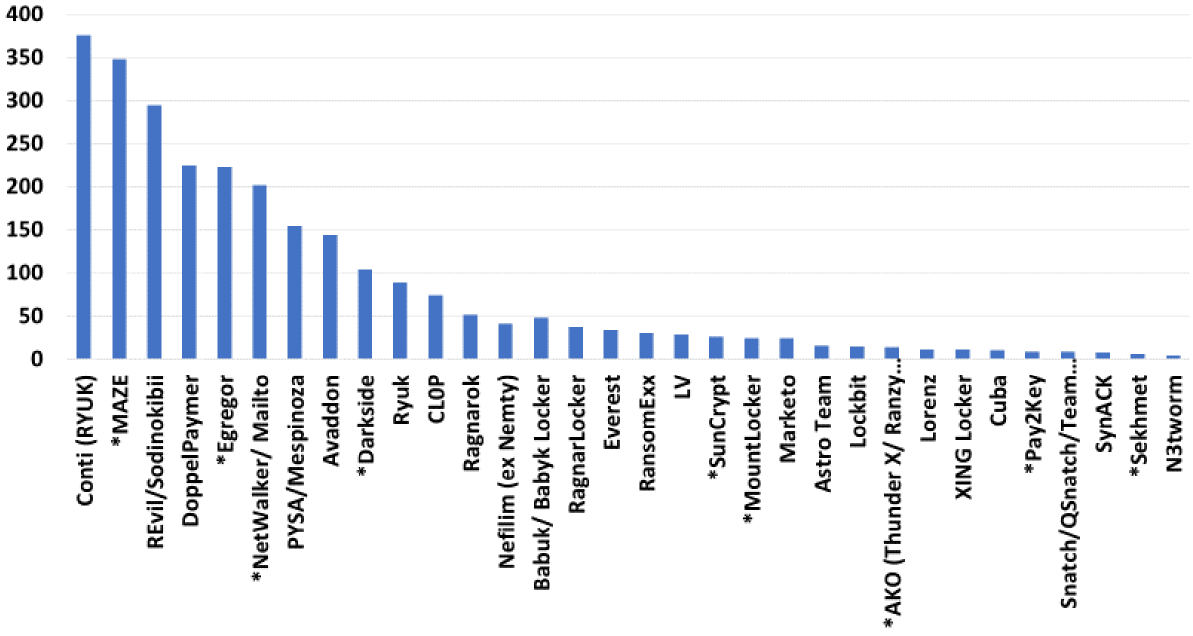
A further threat was to publicly auction off the stolen data if the ransom is not paid[10]. Others levy two ransoms, the first is for the decryption key and the second to delete the copied data so that if cannot be reused (Krebs, 2020). Because of the central importance of data in a ransomware attack, ransomware attacks should now be regarded as major data theft incidents, plus officially reported data losses helps the statistics. The next stage of ransomware Rv.4 will probably be characterised by data becoming the key focus of ransomware as it develops into data extortion (Acronis, 2020) and/or by statecraft and the deliberate targeting of specific infrastructures (NCST, 2021).

Figure 5 shows the major ransomware groups/ gangs currently operating or have operated since 2019 (those presently dormant are prefixed with a * - which could quickly change as they rebrand). Fig. 5 illustrates both the number of victimisations and also the volume of specific ransomware gang operations. Importantly, the number of victimisations is not an indication of their success. Some of the groups with smaller numbers of victims are primarily 'human operated' and focus upon infiltrating the larger organisations and have, as such, a much higher rate of victimisation to ransom payment.

[9] The MAZE group which ceased in late October 2020, affiliated various other ransomware gangs (Lockbit, Suncrypt, RagnarLocker) although they and also analysts have since stated that the MAZE cartel was not actually a cartel (DiMaggio, 2021).

[10] One group (RagnarLocker) even took out Facebook ads to further shame their victims (Bracken, 2020), and some Ransomware groups now include DDoS attacks during demand period (Abrams, 2021).

Figure 5 The most prevalent Ransomware gangs in terms of organisational victimisation - Jan 2019 - May 2021
(2676 Orgs - 32 Groups (with over 4 victims) - *source* EMPHASIS/CONTRAILS Main RW Db). © David S. Wall 2021



N.B. * denotes not functioning at time of writing in May 2021.

3. Support from a transnational organised 'professional' ecosystem

A deeper look at the infiltration and exfiltration of a ransomware attack process reveals *nine distinct stages* which each require the application of different specialised skill sets to make them successful. These stages illustrate how the attack process has become more specialised and even professionalised as ransomware has developed. The analysis also clearly illustrates that each stage is developing its own practices alongside detailed skill sets and tailored organisational forms and bespoke business models to make the services available to clients. This specialisation steps up scalability. In theory, an individual (the lone operator or single empowered agent - Pease, 2001) could carry out each of the functions needed to perform each stage of the attack such as phishing for credentials, exploiting vulnerabilities, infiltrating and exfiltrating and then monetizing the crime. The problem for the lone offender, however, is that these processes are not only laborious and time consuming, but the yield is low, and the risk of capture is high. In order to make cybercrime pay and turn it from a hobby to a career choice, primary offenders need to outsource some of the basic functions of the crime to organised specialists with highly developed skills sets and organisations in order to increase their crime yield and lower their risk of capture. Figure 6 shows this transition from hobby to career criminal.

The following nine stages of ransomware are ideal types as the organisation of ransomware groups can vary considerably, but this model identifies both the component stages and also the key skill sets needed to carry it out.

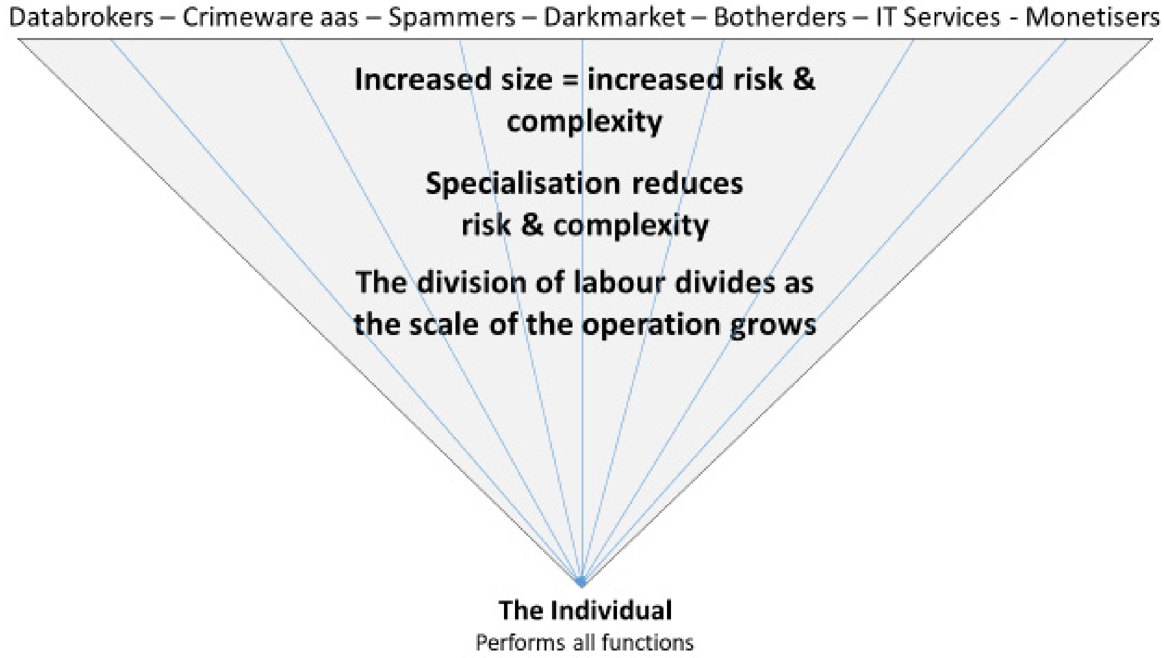
1. *Reconnaissance of potential victims and identification of access points to networks.*

Knowledge is gathered about whether a vulnerability such as a zero-day exploit can be applied to a particular organisation's network. This information is often identified by a specialist who compiles it and sells it to other offenders, for example, an 'initial access broker' via one of the forums or dark market sites.

2. *Gaining 'initial access' to the victim's network.*

The application of the vulnerabilities in stage 1 is often applied by an 'initial access broker', who is either commissioned to gain access, or sells on the access credentials directly via a forum or dark market site. If the latter, this data may be bought by an affiliate of a ransomware group who is trusted by the operators to use their ransomware for a fee.

Figure 6: From hobby to career cybercrime © David S. Wall 2021


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. *Escalating computing access privileges in the system.*

Once in a victim's network the 'affiliate' will seek to increase their user privileges and move laterally across it. As with information gained from earlier stages, these advanced credentials may also be sold on or developed by the attacker (the affiliate).

4. *Identifying key organisational data that will cause most pain when taken.*

During the process of lateral movement, the affiliate will seek out the victims most precious data, especially as commercially sensitive business data in the form of personal details of employees, suppliers, or clients.

5. *Exfiltrating the key data and installing ransomware.*

Attackers will copy the data and exfiltrate it before setting in place the brand of ransomware to which they are affiliated. Once exfiltration is completed, they will plan the activation of the encryption process, usually when the organisation is at its most vulnerable, for example at the beginning of a holiday period (Connolly & Wall, 2019; 10).

6. *Naming and shaming victims & levying the ransom demand.*

Once encryption has been activated, affiliates will use the ransomware brand's specific leak web site to name and shame the victim. Initially they will make public, evidence of the attack, then portions of the data if the payment deadlines are not met. After encryption, some ransomware groups also bombard their victims with DDoS attacks to hinder attempts to restore functionality to their systems. Other groups also use other media, such as Facebook advertisements (RagnarLocker).

7. *Payment of the ransom demand in cryptocurrency.*

Ransom payment amounts in cryptocurrency will have been set by a 'ransomware consultant' who based them on the victim's worth as estimated from information gathered during infiltration and lateral movement across the victim's network. Victims are usually given precise instructions by their attackers about their attack and how to pay the ransom, often including a third-party call centre hired to assist victims buying cryptocurrency to make the payments.

8. *Monetarising the crime.*

Once the ransom has been paid, it has to be converted from cryptocurrency into fiat (government-issued) money. To assist with this, the attackers hire in the services of monetisers who will launder the cryptocurrency via various means (including an army of money mules) to turn it into untraceable cash.

9. *Post-crime "getting away" with it.*

Once the attackers have received their fiat money, they then have to invest it in such a way that it avoids the banks' suspicious transactions radar. Post-crime is possibly the stage which carries most risk for the offender. For this purpose, a different set of financial advice will be sought which locates the crime gains in the legitimate economy.

This brief summary of the stages of a ransomware attack suggests that the key attackers (usually affiliates of the operators) are not usually involved in all of the main stages of the attack and facilitate the attacks by either hiring in a range of skill sets, or outsourcing services, or buy access information (or all three). Identifying these specific stages is useful for the discussion over policing ransomware because they suggest and profile some 'pinch' points where law enforcement and cybersecurity could focus resources in order to interrupt the ransomware victimisation cycle. Importantly, they also suggest some useful principles for understanding the structure of the organisation of cybercrime.

The emergence of the cybercrime ecosystem

The success of ransomware has led to the creation of a cybercrime ecosystem. New forms of online organised crime groups are emerging to commercially deliver key skill sets and services to those wanting to launch ransomware attacks. Importantly, these organisational forms tend to be flat ephemeral structures, often with planned-in obsolescence. They are not hierarchical and sustained (like Mafias), in fact they are relatively disorganised by comparison.

The Cybercrime Ecosystem (see Figure 7) enables the various cybercrimes to be carried out more effectively whilst minimising risk and maximising the return to the offenders. It gives offenders without skill sets access to those who have them and the organisation to carry them out. The skill levels and resources required to launch such attacks are now much higher and greater than the lone operator - the single empowered agent - could ever muster. The modern ransomware process, in effect, symbolises the industrialisation of cybercrime. Functions that were once performed by an individual are now performed by other more specialised and skilled individuals who are highly organised, even though this may be in a distributed, rather than hierarchical manner of the traditional organisation (Musotto & Wall, 2019). What is clear from the ransomware timelines illustrated earlier in Figures 2 & 3 is the upscale in both the volume and also the impact of the attacks. This upscale is the product of rationalisation (whether intentional or not) within the organisation of cybercrime and also changes in tactics to adapt to changing markets for victims for which offender groups fiercely compete. Recall, the shift outlined earlier, in targeting attacks from individuals towards organisations and latterly to Multiple Service Organisations (MSOs) which provide services for other organisations. On average a victimised MSO affects 10+ client organisations and in turn their thousands or even millions of their clients[11].

Ransomware as a service

Central to the cybercrime ecosystem as it applies to ransomware is the emergence of Ransomware as a service (RaaS) in which operators rent out their ransomware to attackers (as affiliates) for a fee or a percentage of the ransom. Some RaaS is *open* to anybody who will pay, other RaaS is *closed* and operators will only accept known and trusted individuals as affiliates in return for a percentage of the ransom (Coveware, 2021). There is also a division between 'spray and pray' and human operated RaaS which, respectively, map on to the 'open' and 'closed' models. The former is usually bulk delivered by phishing (spammed) emails which trick (socially engineer) victims into opening an attachment or URL link so as to infect their computer. The latter is operated by individuals who infiltrate networks and manipulate their way around them, rather like a virtual burglar.

Melandab and colleagues researched the sale of RaaS on popular web forums and dark markets prior to Q4 2019. They found that the impact of the earlier 'open' RaaS was much more limited than was often declared in the cybersecurity media (Melandab et al., 2020). They also found that ransomware becomes a serious threat when committed by experienced professional cybercriminals who use darknet forums as a recruitment ground for their operations. Both Melandab et al. (2020), Coveware, (2021) and other commentators have found that the ransomware operators, who own and operate the malware are different actors to the affiliates who rent the ransomware to use it to attack. So, ransomware operators not only spread their risk, effectively hiding behind affiliates, but they also plan obsolescence into their business model. Groups such as MAZE, NEMTY and various others abruptly ceased operations when they were most successful and cashed

[11] A calculation based upon the EMPHASIS research.

out without giving any warning and abandoned anything left, thus leaving little trail to follow. Some operators, such as SHADE left the field and even posted decryption keys when they shut down (Abrams, 2020).

Further conceptualisation of the Cybercrime Ecosystem

The emergence of a cybercrime ecosystem to help facilitate all aspects of cybercrime is key to understanding the increase in cybercrime victimisation. Aspects of this ecosystem were illustrated earlier in the nine-stage analysis of a ransomware attack. At each stage various services, information or data are required to organise and facilitate the crime and enact it. There are eight key services that are required to achieve this.

- *Databrokers* trade in stolen datasets, potential victim profiles and also provide access to illegal data streaming. This data can be used in different ways by different offender groups in both the formation and the delivery of the services.
- *Crimeware-as-a-service (CaaS) operators* may develop and hire out, for example, Ransomware-as-a-service, DDoS (Stressers) or other malware (e.g., Zeus banking trojans). CaaS may also include spammers who hire out spamware-as-a-service for phishers, scammers and fraudsters, and bot-herders who rent out command and control botnets (robot networks) which send out emails in mass volumes. Often these services are automated via a dashboard for buyers to buy a specific service, choosing the size and type of attack and also the victim group which itself is the product of acquired data. Very often CaaS brokers will market their services with trial offers and run them as subscription services (see Musotto & Wall, 2020).
- The *Darkmarketeers* provide, sell, or trade services, usually via the ToR network (Onion Router) and notable dark markets have included Silk Road 1 & 2, Dream Market etc.
- *Bullet Proof Hosters*, as the title indicates, run 'Bullet Proof' hosting services that provide 'protected' networked services that for a price allow unrestricted content to be uploaded and disseminated. Such services could be used, for example, to host dark markets or a ransomware victim leak www site. They effectively reduce client risk and protect clients from being caught, which is covered by the premium paid for the service.
- *Monetisers* organise and manage a financial return to the attackers by laundering cryptocurrency and turning it into fiat currency (for a fee).
- *Bug (Crime IT) Brokers* support the various Crimeware as a Service by writing and selling code and vulnerabilities[12], also solving any additional coding problems attackers may have.
- The *Infiltration brokers* are *'Engagers'* who 'engage' with victims via their responses to phishing and obtain credentials and sell or pass this information on to 'Initial Access Brokers' who gain entry and sell the access details.
- The final group are *Negotiators* who negotiate the amount of the ransom payment. They comprise of 'Ransomware Consultants' on the offender side (Gemini, 2021) and 'Negotiators' on behalf of the victim. Both are crucial to ransomware operation (Murphy, 2021).

The services are not arranged in Figure 7 in any particular order because there is no set order, however, together they form the cybercriminal ecosystem that enables ransomware and, more specifically, modern cybercrime more generally.

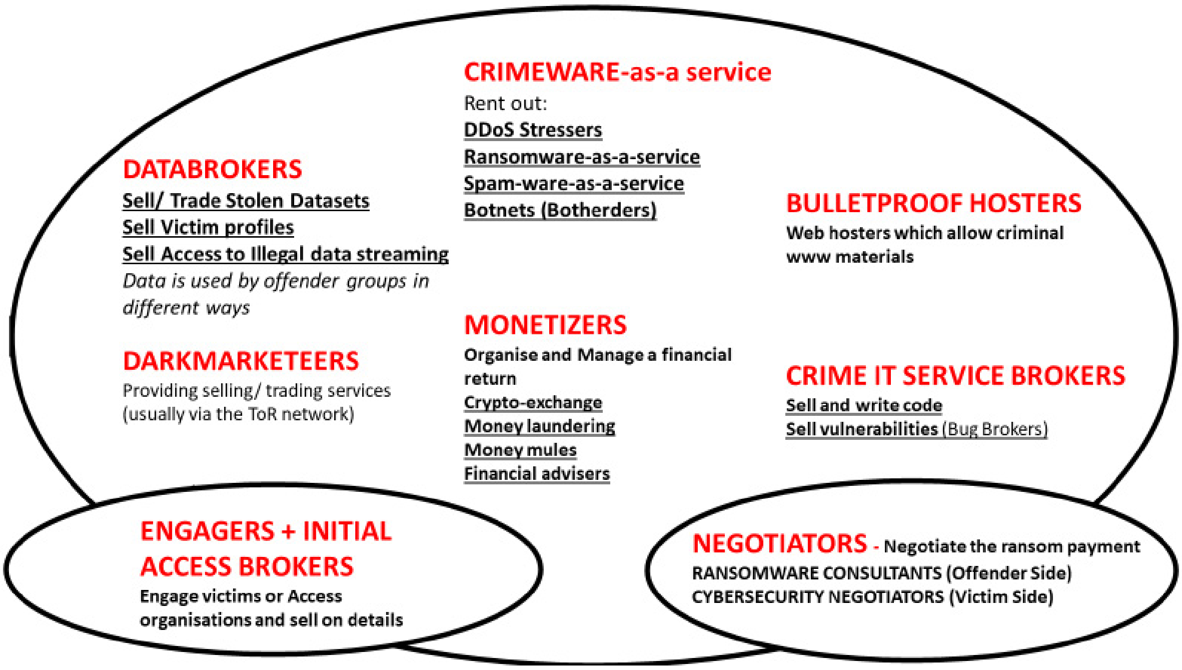
These roles are in a constant state of flux as both technologies and crime practices evolve. They 'automate' roles once performed by lone offenders and help the attacker (primary offender) to reach the scalability and volume of crime needed to achieve a sizable return for their investment. Buying in a particular service from the cybercrime ecosystem not only saves the offender time but can also offset liability. Each service tends to be run by one or more kingpins in the more traditional organised crime parlance. They frequently recruit affiliates to distribute their service, usually for a percentage of the profit or a flat fee. In effect, this is the new face of transnational organised crime. It is distributed rather than hierarchical and appears disorganised by comparison.

4. The new challenges of cybercrime for law and enforcement

The developments described above are generating new challenges for law and its enforcement. They are also burdening policing services that are themselves struggling to maintain their own level of service during periods of lockdowns. One of the main challenges is that ransomware is a blended cybercrime, in fact, a collection of cybercrimes that once stood on their own and hard to conceptualise in law. In the UK ransomware is both a computer misuse crime and also a crime of extortion (and various other offences relating to phishing and the theft and abuse of personal information and even money laundering) - very different types

[12] This is part of the research completed for the CRITiCAL project and is forthcoming. An early outline is found in a paper 'Cybercrime Kingpins' delivered at the American Society of Criminology in San Francisco on 14 Nov. 2019.

Figure 7: The Cybercrime Ecosystem


CRIMEWARE-as-a service
Rent out:
DDoS Stressers
Ransomware-as-a-service
Spam-ware-as-a-service
Botnets (Botherders)
DATABROKERS
Sell/ Trade Stolen Datasets
Sell Victim profiles
Sell Access to Illegal data streaming
Data is used by offender groups in different ways
BULLETPROOF HOSTERS
Web hosters which allow criminal www materials
MONETIZERS
Organise and Manage a financial return
Crypto-exchange
Money laundering
Money mules
Financial advisers
DARKMARKETEERS
Providing selling/ trading services (usually via the ToR network)
CRIME IT SERVICE BROKERS
Sell and write code
Sell vulnerabilities (Bug Brokers)
ENGAGERS + INITIAL ACCESS BROKERS
Engage victims or Access organisations and sell on details
NEGOTIATORS - Negotiate the ransom payment
RANSOMWARE CONSULTANTS (Offender Side)
CYBERSECURITY NEGOTIATORS (Victim Side)

© David S. Wall 2021

of offending. Each component also falls under different bodies of law which not only makes ransomware statistically problematic and hard to record, because in the UK the 'ransom' and the 'ware' can be recorded in either the computer misuse or economic crime statistics. But it also means that the responsibility for policing them (technically) fall under different policing agencies[13]. Agencies, which often have untrusted relationships with industry, especially when victims pay the ransom because they do not want their victimisation to become public for commercial reasons and want to resolve the matter quickly and privately – which leads to under-reporting. Even though the data exfiltration tactic has made ransomware a data breach issue which has led to naming the breaches being considered as fair game for many journalists and commentators. This conflict between the public and private interest hinders the search for justice and is one area then needs to be resolved if intelligence and data is to be shared to resolve this common problem.

Because ransomware is under-reported, it is therefore under-prosecuted, which means little court experience across the criminal justice system. Its transnational nature is also problematic as many attack groups deliberately seek victims in other jurisdictions due to cumbersome cross-border legal and policing rules. The final problem for policing is that ransomware may be big globally, but is small locally, so local police get little experience of dealing with the crime. The UK ROCU (Regional Organised Crime Unit) model, however, connects local and national police forces regionally and it is fairly well regarded by police officers and also respected by industry (see Connolly & Wall, 2019).

Yet, despite these systemic hurdles, there have been a number of significant policing successes. The transnational interdisciplinary and cross-sector 'No More Ransomware' project has broadly been successful in galvanising 170 partners from the public and private sector. Its decryptors "have helped more than six million people to recover their files for free", allegedly saving at least €1billion in ransomware payments (Gatlan, 2021). There have also been a number of examples of cross sector interventions which have resulted in law enforcement taking down botnets that distribute ransomware across the networks prior to attacks (e.g., TrickBot in Oct 2020, Emotet in Jan 2021). Also, taken

[13] Different UK police forces can separately carry responsibilities for cybercrime and economic crimes. Overlying this, the National Crime Agency can carry responsibilities for offences which span arrange of regions. In practice, these differences are largely resolved by the Regional Organised Crime Units (ROCU) which interface the different agencies involved.

down have been bullet proof hosting services such as Maxided (Osborne, 2018) which hosted now defunct cryptomarkets such as Silk Road, Hansa etc. Furthermore, there have also been significant arrests of ransomware operators, for example, in July 2020 in Belarus the operators of GandCrab (RaaS) ransomware operators which ran between Jan 2018 and Mid-2019 were arrested. This was followed by the arrest of a GandCrab affiliate in March 2021 in South Korea. Furthermore, members of the Egregor (RaaS) ransomware group which ran between Sept. 2020 and Feb 2021 and which allegedly comprised of members of the MAZE group, were arrested in the Ukraine in Feb 2021 (Abrams, 2021b). Also helping the policing mission have been the ransomware groups by hindering each other's operations[14], which could either indicate the strength of competition between the various ransomware operators illustrated earlier or it could simply be sour grapes by rivals (Schwartz, 2021).

The main challenges for police forces lie in working out who the actual offenders are in complex cybercrimes like ransomware and to be able to apply the relevant bodies of law to prosecute them, especially as the organisation of the crime is so distributed and there are a number of different actors involved.

Conclusions

Rather than generate new cybercrime opportunities, the COVID-19 lockdown has led to the acceleration of cybercrime trends that were already in play. In this sense, the lockdown was not transformative for cybercrime, but it was an important enabler. Highly adaptive offender groups took advantage of new opportunities presented by the lockdown disruptions, as they so often tend to do. What these lockdown-accelerated trends have done is to illustrate that ransomware is not only a major form of modern transnational organised crime, but it has become a multi-billion-dollar industry which keeps on growing and will continue to grow (Ilascu, 2021). It is also changing the way that criminals organise themselves online. Modern cyber-offenders appear to be following a business manual rather than an organised crime playbook. The complex and specialised organisation of ransomware and other major cybercrimes is not only developing a professional ecosystem to enable and support it, but it is also providing offenders with alternative career choices.

If ransomware is an example of cybercrime as industry, because its evolution bears the hallmarks of industrialisation, then it also creates a perfect storm for law enforcement by introducing a number of contradictions that frustrate its prevention, mitigation, and investigation. Central to the discussion over the policing (investigation), mitigation and prevention of ransomware is a decades-old divide between the public interest and the private interests. Even after three decades of cybercrime, it is still the case that whilst the various parties involved in policing cybercrime still all agree on the problem and end goal, they still disagree about how to achieve them. As a consequence, the various stakeholders, at a broader level, rarely work together and share data as they need to do if they are going to co-own the problem and work together to co-produce a solution by sharing data and expertise. At a more basic level, however, one way of beginning this process is to break down the attack process into the various stages and focus upon these in order to stop the attack. This includes also focusing upon the various components of the cybercrime ecosystem.

Recognising the different stages of the attacks will enable law enforcement and cybersecurity to more effectively apply the right skill sets and marshal the key agencies involved to achieve the correct and most effective and appropriate level of Policing. This analysis will hopefully augment some of the bigger governmental programmes that have been announced this past year, such as the multi-skilled and multi-agency Ransomware Task Force (IST, 2021). Also, the continuation of the anti-ransomware initiatives such as no more ransom.org. To paraphrase the World Economic Forum, cybercrime is much bigger than governments (Mee & Chandrasekhar, 2021). Everyone involved has to work together and co-own the problem in order to co-produce the solution, words that are easier to say than put into practice.

Funding

This research is based upon work funded by the EMPHASIS ('EconoMical, PsycHologicAl & Societal Impact of RanSomware' - EPSRC, EP/P011772/1) and CRITiCal ('Combatting cRiminals In The Cloud' - EPSRC EP/M020576/1) project.

[14] The REvil (Sodinokibi) ransomware gang, for example, claimed to have identified the real identities of the persons behind the MAZE service, their rival, stating that they have direct connections with the Russian Government and comprise of eight individuals who are involved with the Russian FSB.

Acknowledgements

Many thanks to the anonymous reviewers for their comments on an earlier draft; to Harri Wall for reading and commenting on the final draft. I am also grateful to various partners and colleagues at the Centre for Criminal Justice Studies at Leeds and to Diana and Charl at OrangeCyberdefense for their help and support. The views expressed in this article are my own views and not those of partners, funding agency or other participants on the projects.

References

- Abrams, L. (2020a) List of ransomware that leaks victims' stolen files if not paid. *BleepingComputer.* 26 May.
  Available from: https://www.bleepingcomputer.com/news/security/list-of-ransomware-that-leaks-victims-stolen-files-if-not-paid/ [Accessed 26 May 2021].
- Abrams, L. (2020b) Ransomware recruits affiliates with huge payouts, automated leaks. *BleepingComputer.* 15 May.
  Available from: https://www.bleepingcomputer.com/news/security/ransomware-recruits-affiliates-with-huge-payouts-automated-leaks/ [Accessed 26 May 2021].
- Abrams, L. (2021a) Another ransomware now uses DDoS attacks to force victims to pay. *BleepingComputer.* 24 January.
  Available from: https://www.bleepingcomputer.com/news/security/another-ransomware-now-uses-ddos-attacks-to-force-victims-to-pay/ [Accessed 26 May 2021].
- Abrams, L. (2021b) 'GandCrab ransomware affiliate arrested for phishing attacks'. *BleepingComputer*. 9 March.
  Available from: https://www.bleepingcomputer.com/news/security/gandcrab-ransomware-affiliate-arrested-for-phishing-attacks/ [Accessed 5 August 2021]
- Abroshan, H., Devos, J., Poels, G. & Laermans, E. (2021) Phishing Happens Beyond Technology: The Effects of Human Behaviors and Demographics on Each Step of a Phishing Process. *IEEE Access* (Vol. 9).
  Available from: https://doi.org/10.1109/ACCESS.2021.3066383 [Accessed 5 August 2021]
- Accenture (2021) *2021 Cyber Threat Intelligence Report*. Accenture.
  Available from: https://www.accenture.com/_acnmedia/PDF-158/Accenture-2021-Cyber-Threat-Intelligence-Report.pdf#zoom=40
- Acronis (2020) Acronis Cyberthreats report 2020: Global cybersecurity trends overview and predictions for 2021, *Acronis.*
  Available from: https://www.acronis.com/en-us/lp/cyberthreats-report-2020 [Accessed 26 May 2021].
- Action Fraud (2020) Criminals preying on our financial worries as they spoof government websites to take your money. *Action Fraud*. 19 April.
  Available from: https://www.actionfraud.police.uk/news/criminals-are-exploiting-the-covid-19-pandemic-to-defraud-innocent-people-including-sending-fake-emails-and-texts-purporting-to-be-from-government [Accessed 26 May 2021].
- BBC (2020) Coronavirus: The world in lockdown in maps and charts. *BBC News Online*. 7 April.
  Available from: https://www.bbc.com/news/world-52103747 [Accessed 26 May 2021].
- Bracken, B. (2020) Ragnar Locker Ransomware Gang Takes Out Facebook Ads in Key New Tactic. *threatpost*. 11 November.
  Available from: https://threatpost.com/ragnar-locker-ransomware-facebook-ads/161133/ [Accessed 26 May 2021].
- Connolly, A. & Wall, D.S. (2019) The Rise of Crypto-Ransomware in a Changing Cybercrime Landscape: Taxonomising Countermeasures. *Computers & Security*. 87(Nov).
  Available from: https://doi.org/10.1016/j.cose.2019.101568 [Accessed 26 May 2021].
- Coveware (2020) The Marriage of Data Exfiltration and Ransomware. *Coveware Blog*. 10 January.
  Available from: https://www.coveware.com/blog/marriage-ransomware-data-breach [Accessed 26 May 2021].
- Coveware (2021) Ransomware Payments Fall as Fewer Companies Pay Data Exfiltration Extortion Demands, Ransomware Marketplace Report Q4 2020. *Coveware Blog*. 1 February.
  Available from: https://www.coveware.com/blog/ransomware-marketplace-report-q4-2020 [Accessed 26 May 2021].
- Dashevsky, E. (2017) Just how much malware is on free porn sites? *PC World*. 17 April.
  Available from: https://www.pcworld.com/article/2034864/just-how-much-malware-is-on-free-porn-sites-.html [Accessed 26 May 2021].
- De Blasi, S. (2021) The Rise of Initial Access Brokers. *digital shadows*. 22 February.
  Available from: https://www.digitalshadows.com/blog-and-research/rise-of-initial-access-brokers/ [Accessed 26 May 2021].
- DiMaggio, J. (2021) Ransom Mafia. Analysis of the World's First Ransomware Cartel. *Analyst1*. 7 April.
  Available from: https://analyst1.com/file-assets/RANSOM-MAFIA-ANALYSIS-OF-THE-WORLD%E2%80%99S-FIRST-RANSOMWARE-CARTEL.pdf [Accessed 26 May 2021].
- Emsisoft (2021) The cost of ransomware in 2021: A country-by-country analysis. Emsisoft Malware Lab, 27 April.
  Available from: https://blog.emsisoft.com/en/38426/the-cost-of-ransomware-in-2021-a-country-by-country-analysis/ [Accessed 5 August 2021].
- Gatlan, S. (2020) Blackbaud sued in 23 class action lawsuits after ransomware attack. *BleepingComputer*. 3 November.
  Available from: https://www.bleepingcomputer.com/news/security/blackbaud-sued-in-23-class-action-lawsuits-after-ransomware-attack/ [Accessed 26 May 2021].

- Gatlan, S. (2020) No More Ransom saves almost €1 billion in ransomware payments in 5 years. *BleepingComputer*. 26 July. Available from: https://www.bleepingcomputer.com/news/security/no-more-ransom-saves-almost-1-billion-in-ransomware-payments-in-5-years/ [Accessed 5 August 2021].
- Gemini (2021) Ransomware Unmasked: Dispute Reveals Ransomware TTPs. *Gemini Advisory*. 26 May. Available from: https://geminiadvisory.io/ransomware-unmasked/ [Accessed 26 May 2021].
- Hutchings, A. & Holt, T. J. (2015) A crime script analysis of the online stolen data market. *British Journal of Criminology*, 55(3): 596-614. Available from: http://bjc.oxfordjournals.org/content/55/3/596.full [Accessed 26 May 2021]
- IBM (2021) IBM X-Force Threat Intelligence Index 2021. *IBM*. Available from: https://www.ibm.com/security/data-breach/threat-intelligence [Accessed 26 May 2021].
- Ilascu, I. (2020) Ryuk ransomware deployed two weeks after Trickbot infection. *BleepingComputer*. 23 June. Available from: https://www.bleepingcomputer.com/news/security/ryuk-ransomware-deployed-two-weeks-after-trickbot-infection/ [Accessed 26 May 2021].
- Ilascu, I. (2021) Ransomware is a multi-billion industry and it keeps growing. *BleepingComputer*. 4 March. Available from: https://www.bleepingcomputer.com/news/security/ransomware-is-a-multi-billion-industry-and-it-keeps-growing/ [Accessed 26 May 2021].
- IST (2021) RTF Report: Combatting Ransomware - A Comprehensive Framework for Action: Key Recommendations from the Ransomware Task Force. *Institute for Security and Technology*. April. Available from: https://securityandtechnology.org/ransomwaretaskforce/report/ [Accessed 26 May 2021].
- Krebs, B. (2020) Ransomware Gangs Don't Need PR Help. *Krebs On Security*. 1 July. Available from: https://krebsonsecurity.com/2020/07/ransomware-gangs-dont-need-pr-help/?web_view=true [Accessed 26 May 2021].
- Kivilevich, V. (2020) The Secret Life of an Initial Access Broker. *KELA*. 6 August. Available from: https://ke-la.com/the-secret-life-of-an-initial-access-broker/ [Accessed 26 May 2021].
- Mee, P. & Chandrasekhar, C. (2021) Cybersecurity is too big a job for governments or business to handle alone. *World Economic Forum*. 3 May. Available from: https://www.weforum.org/agenda/2021/05/cybersecurity-governments-business/ [Accessed 26 May 2021].
- Melandab, P., Bayoumya, Y. & Sindrea, G., (2020) The Ransomware-as-a-Service economy within the darknet. *Computers & Security*. 92 (May): 1-9. Available from: https://doi.org/10.1016/j.cose.2020.101762 [Accessed 26 May 2021].
- Microsoft (2020) Human-operated ransomware attacks: A preventable disaster. Microsoft 365 Defender Threat Intelligence Team. Available from: https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/
- Murphy, H. (2021) The negotiators taking on the ransomware hackers. *Financial Times*. 17 February. Available from: https://www.ft.com/content/c0def43a-6949-44ca-86ff-f28daa3818be [Accessed 26 May 2021].
- Musotto, R. & Wall, D.S. (2020) More Amazon than Mafia: Analysing a DDoS Stresser Service as Organised CyberCrime. *Trends in Organized Crime*. Online. Available from: https://doi.org/10.1007/s12117-020-09397-5 [Accessed 26 May 2021].
- NCSC (2020) Cyber experts step in as criminals seek to exploit Coronavirus fears. *NCSC Advisory*. 16 March. Available from: https://www.ncsc.gov.uk/news/cyber-experts-step-criminals-exploit-coronavirus[Accessed 26 May 2021].
- NCST (2021) Ryuk Ransomware Operators Shift Tactics to Target Victims. *National Cyber Security News Today*. 27 May. Available from: https://nationalcybersecuritynews.today/ryuk-ransomware-operators-shift-tactics-to-target-victims-malware-ransomware/ [Accessed 26 May 2021].
- Newman, L. (2021) Ransomware's Dangerous New Trick Is Double-Encrypting Your Data. *WIRED*. 17 May. Available from: https://www.wired.com/story/ransomware-double-encryption/ [Accessed 26 May 2021].
- Osborne, C. (2019) MaxiDed, dead: Law enforcement closes hosting service linked to criminal activity. ZDNET. 17 May. Available from: https://www.zdnet.com/article/maxided-dead-law-enforcement-takes-down-bulletproof-hosting-linked-to-criminal-activity/ [Accessed 5 August 2021].
- Pease, K. (2001) Crime futures and foresight: challenging criminal behaviour in the information age. In. D. S. Wall (ed.). *Crime and the Internet*. London, Routledge. 18–28.
- Porcedda, M.G. & 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. Available from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3429958 [Accessed 26 May 2021].
- Porcedda, M.G. & Wall, D.S. (2021) Modelling the Cybercrime Cascade Effect of Data Theft, *proceedings of the IEEE Workshop on Attackers and Cyber-Crime Operations* (WACCO 2021), September 7 (forthcoming).

- Schwartz, M., (2021) Do Ransomware Operators Have a Russian Government Nexus? *Bank Info Security*. 4 February. Available from: https://www.bankinfosecurity.com/do-ransomware-operators-have-russian-government-nexus-a-15925 [Accessed 26 May 2021].
- Scroxton, A. (2021) Is it time to ban ransomware insurance payments? *ComputerWeekly*. 11 Feb. Available from: https://www.computerweekly.com/feature/Is-it-time-to-ban-ransomware-insurance-payments [Accessed 26 May 2021].
- Wall. D.S. (2021) Cybercrime: The Internet as a Conduit for Transnational Organised Criminal Activity. In. F. Allum & S. Gilmour (eds) *Routledge Handbook on Transnational Organised Crime*, 2nd Edition. London, Routledge.