EMERGING INSIGHTS

Ransomware: A Perfect Storm

James Sullivan and James Muir
ACKNOWLEDGEMENTS

The idea behind this Emerging Insights paper was to combine BAE Systems Applied Intelligence’s technical analysis of the ransomware threat with RUSI’s expertise in cyber strategy and policy. While BAE is a founding partner of RUSI’s cyber research programme, this paper has undergone a full peer review process to adhere to RUSI’s values of independence and objectivity.

The authors gratefully acknowledge the advice and comments from all who provided their time to help with this research, especially Sneha Dawda and Jamie MacColl. Many thanks go to Ciaran Martin and David Wall for reviewing the paper. Thanks also to RUSI’s publications team for helping to publish this research.

EXECUTIVE SUMMARY

This Emerging Insights paper calls for a new set of policy interventions to reduce the threat from ransomware. Options range from introducing legislation to prevent ransom payments, to tackling the use of penetration testing tools used in ransomware attacks, to national-level mechanisms to bolster preparedness for a ransomware attack. This paper intends to be a platform for further debate on global ransomware policy choices.

The research for this paper highlights how ransomware attacks continue to have a significant impact on businesses and organisations across the globe, resulting in high levels of cost and disruption. Using BAE Systems’s threat intelligence capability, this paper explores the methods, impact and mitigation of ransomware attacks in detail. Case studies reveal the success and popularity of ‘double extortion’ ransomware attacks which include data theft. The research also describes the range of attack vectors and exposed attack surface available to ransomware operators and reveals how different criminal ransomware operators collaborate and learn from each other. In the context of a global pandemic, the paper shows how cyber criminals continue to exploit victims and cause disruption with impunity.

The paper underlines the complexities that businesses and governments face when deciding whether to pay a ransom following a ransomware attack. Complications include paying criminals that are subject to indictments or sanctions, the potentially questionable role of ransomware recovery negotiators, and the arguably misunderstood role of cyber

insurance companies. Further research is needed to determine the true impact of these auxiliary complexities.

Finally, the paper urgently calls for a new set of policy interventions based on the ‘Prevent, Pursue, Protect and Prepare’ approach to tackling cybercrime. In doing so, this research highlights a type of cybercrime that is spiralling out of control and requires urgent policy intervention.

INTRODUCTION

The damage caused to organisations by ransomware attacks in 2020 was unprecedented. Many rendered their victims unable to operate or access critical information. A modern ransomware attack can be thought of as a ‘denial of business’ attack, and organisations across all sectors have fallen victim to this type of compromise. Rather than wait for a technical solution, some organisations have paid the ransoms demanded by criminal groups to restore their services. Moreover, the number of groups launching ransomware attacks is growing month on month, and most of these groups are now employing a tactic known as ‘double extortion’. In effect, victim organisations are now being held to ransom not only on availability (they are unable to operate systems or access files) but also on confidentiality (their data, intellectual property or other sensitive information is stolen in the attack and is threatened with public release).

This paper analyses the threat from ransomware, the scale of the problem and the ‘perfect storm’ of factors that have led to an increase in profits from this type of cybercrime. Double extortion ransomware attacks bring with them a host of policy issues. Examination of the ecosystem

4. At the start of 2020, only one ransomware operator was using this technique. There are now over 15 groups performing ‘double extortion’ ransomware attacks. Data provided by BAE Systems Threat Intelligence team. See also Catalin Cimpanu, ‘Here’s a List of All the Ransomware Gangs Who Will Steal and Leak Your Data If You Don’t Pay’, ZDNet, 21 April 2020, <https://www.zdnet.com/article/heres-a-list-of-all-the-ransomware-gangs-who-will-steal-and-leak-your-data-if-you-dont-pay/>, accessed 16 November 2020.
on both the criminal and victim sides shows that complex issues are at play: while ransom payment may be a regrettable ‘last resort’ for some victims and a ‘quick solution’ for others, all ransom payments fuel the cybercriminal cycle.

This paper explores the lifecycle of a ransomware attack and presents recent case studies. It then outlines potential interventions that may be required to reduce the threat, highlighting the complexities associated with payments and recovery. It concludes by proposing policy options for governments, law enforcement and businesses to consider.

**METHODOLOGY**

This paper draws on data from the BAE Systems Threat Intelligence team, who closely monitored the ransomware threat throughout 2020 and examined and aggregated data from ransomware ‘victim blogs’. The BAE Systems Incident Response team has been engaged in several ransomware incidents in 2020 and 2021, and this paper draws on insights into ransomware attack techniques gained from these engagements.

One limitation to this paper’s approach has been that it mainly relied on data from the cyber security industry, and data from one company only, although it covers the majority of known ransomware operators using the double extortion approach. Nevertheless, where possible, the primary data has been supported by an open source literature review of threat reports, blogs and information security news. This review mainly focuses on articles published in 2020, but earlier references are included where relevant. Recent advisories from the US government assist in the understanding of auxiliary complexities that drive ransom payments.

---

6. Ransomware victim blogs are typically hosted on the dark web. These are discussed in greater detail later in this paper. This information is not available in aggregate in the public domain. In brief, these sites are monitored for changes, which raise an alert to an analyst. Any new organisations named on these victim blogs are then researched using open sources to identify their sector, location and revenue. A total of 16 ransomware operator victim blogs have been monitored during the research for this paper. The reporting period for this data, based on the dates given on blog posts, is 16 November 2019 to 4 December 2020.


RANSOMWARE’S PERFECT STORM

This section provides an overview of how the ransomware threat has evolved and the nature of a typical ransomware attack in 2020. There is a particular focus on the ‘double extortion’ threat. The section then analyses the ‘perfect storm’ of factors that have contributed to ransomware attacks of this type being so successful and prevalent in 2020 and into 2021. This perfect storm is a combination of criminal collaboration, vulnerabilities presenting initial access vectors and a snowball effect of ransom payments driving further ransomware attacks. The paper quantifies the scale of the problem with data drawn from the monitoring of ‘victim blogs’, which are used by ransomware operators to threaten victims. The section ends by highlighting two case studies from recent attacks, one of which used data theft, while the other did not.

BACKGROUND: HOW DID WE GET HERE?

The concept of a criminal attack in which the victim’s files are ‘locked’ (encrypted) and payment is demanded for recovery dates back to the mid-2000s. In the 2010s, an increasingly popular mode of cybercrime was a ransomware attack against individuals distributed via indiscriminate phishing campaigns. Ransomware strains such as CryptoLocker have been particularly damaging.

In recent years, cybercriminal operators have increasingly targeted organisations, as opposed to individuals. These more tailored operations, which often involve careful reconnaissance and preparation, have enabled attackers to identify the most sensitive systems and data in a victim’s network. As a result, they can deploy ransomware and/or exfiltrate data to maximise leverage. The ransom demands made in attacks against organisations are higher than those against individuals – a typical ransom for an attack against an individual may have been $500, whereas recent attacks against organisations are now typically at least six-figure sums. One recent attack against German IT company Software AG is reported to have come with a ransom demand of over $20 million. However, Lena Connolly and colleagues note that an organisation’s size does not have a strong bearing on the severity of a ransomware attack’s impact (defined by Connolly as a combination of business disruption, recovery time, number and criticality of

affected systems/devices, and information loss) with cyber security maturity playing a more decisive role.\textsuperscript{13}

Double extortion ransomware has been referred to variously as ‘targeted ransomware’, ‘big game hunting ransomware’,\textsuperscript{14} and ‘human-operated ransomware’,\textsuperscript{15} and the phenomenon has grown in popularity with cybercriminals and become a significant societal problem. One cybercriminal group, known as ‘Maze’, is thought to have been the first to employ the double extortion tactic of data theft and extortion in November and December 2019.\textsuperscript{16} This has triggered further acceleration in the scale and potency of the threat. While this paper focuses on the double extortion variant of the ransomware attack, which is increasingly common, it is important to note that ransomware attacks without data theft and extortion still take place and are effective.

A TYPICAL RANSOMWARE ATTACK IN 2020

Figure 1 outlines the three main stages of a typical ransomware attack in 2020, which this paper defines as a targeted attack against an organisation during which data is stolen and used as leverage in the event that ransom payment is not forthcoming from the victim.

Figure 1: Simplified Stages of a Modern Ransomware Attack with Data Theft and Extortion

<table>
<thead>
<tr>
<th>Stage</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Phishing email, exploit vulnerability</td>
</tr>
<tr>
<td>2</td>
<td>Propagate, exfiltrate data, encrypt data</td>
</tr>
<tr>
<td>3</td>
<td>Demand ransom and make further threats</td>
</tr>
</tbody>
</table>

One recent attack against German IT company Software AG is reported to have come with a ransom demand of over $20 million.

---

Source: Author generated. This summary diagram is an aggregate picture of a typical ‘double extortion’ ransomware attack in 2020, as informed by open source blogs and reports on ransomware operators and attacks, and BAE Systems Threat Intelligence and Incident Response data.

In step 1, the criminal attacker attempts a network intrusion via different methods. The main four types of access vector are shown in the diagram. Initial access is explored later in the paper.

In step 2, the attacker attempts to turn their initial foothold within an organisation into a full-blown presence in the victim’s network, by seeking to elevate privileges and access as many systems as possible. Attackers will attempt to gain domain administrator rights, seek out ‘critical’ systems and identify online backups – if these can be encrypted, the victim is far more likely to consider paying the ransom. This step is actually a set of steps that all occur within the victim’s network and require a functioning ‘command and control’ channel to the attacker – penetration testing tools, such as Cobalt Strike, are commonly used for this purpose. As part of this process, attackers will also identify and exfiltrate any data that can be used to increase leverage on the victim. They will also look to find the best way of simultaneously deploying their ransomware when the time is right, often using existing enterprise IT management packages for that purpose. Attackers have made big strides in perfecting this aspect of the attack. In 2018 and 2019, it was typical that this stage could take weeks or months to achieve (and would not include the data exfiltration activity). Recent reports have indicated ‘end-to-end’ ransomware attacks taking as little as two hours.

With the ransomware deployed and havoc caused in the target organisation, step 3 – demanding the ransom – is initiated through a message presented as part of the ransomware execution, an email to the organisation, or other means. What follows beyond this point is the biggest area of recent evolution in a typical ransomware attack, with operators of the Maze, REvil and many other ransomware strains moving towards a business model

---

17. Cobalt Strike, Metasploit and Powershell Empire are prime examples of tools that are designed to be used in legitimate penetration testing and ‘red team’ security engagements, where a ‘red’ team acts as an attacker and a ‘blue’ team acts as a defender, in order to test a network’s security. These tools have, however, been co-opted by threat actors from across the threat landscape (criminal and state actors), who can use them for a range of quick and useful attack functions.

based on (further) extortion to encourage ransom payment.\textsuperscript{19} The data stolen from the victim network in step 2 is the key to this tactic. Numerous ransomware operators have taken to making threats based on this stolen data, followed by publication of sample data to their public ‘blog’ sites.\textsuperscript{20} Another potential outcome in the extortion chain is the ‘auction’ of stolen data to the highest bidder.\textsuperscript{21}

**Figure 2:** Banners of Ransomware Victim Blogs Operated by Maze (Top), NetWalker (Middle) and REvil (Bottom)

Source: Composite of three screenshots taken in July 2020, showing the ‘banner’ presented on the respective ransomware operator victim blogs shown (Maze, NetWalker and REvil). Maze refers to its victims as ‘clients’. A link to the REvil operator ‘auction’ site is also visible on the REvil banner.

Ransomware operators have also shown that they are prepared to seek out and use the most sensitive information they can find within an organisation for leverage – for example, passport scans, personal information and contract information.\textsuperscript{22} Regulations, such as the General Data Protection Regulation (GDPR), have also effectively increased the sensitivity and value

\begin{itemize}
of personally identifiable information to its processors – and therefore also the potential leverage it provides to extortionists – owing to the substantive potential fines that may be issued as a result of breaches.

Ransom demands will eventually be doubled as operators seek to put further pressure on victims into paying up. Small initial data leaks will be made (typically 1–5% of the total volume), and further or full leaks threatened.

Data theft also functions as a ‘back-up plan’ should the operators run into difficulties in deploying the ransomware itself – the stolen data can be sufficient to attempt to extort a ransom payment from the victim.

CONTRIBUTING FACTORS

There are several factors that make modern ransomware attacks a ‘perfect storm’:

- **Criminal services and collaboration.** Many ransomware variants are distributed on a ‘ransomware-as-a-service’ or affiliate model, where those conducting the attacks take a cut of the proceeds, and the top-level organisers typically provide the ransomware itself and handling of the extortion/payment process. This level of organisation and collaboration within the cybercriminal landscape comes with a number of benefits to the criminal side, and appears to be working well for organisations such as REvil. Although there is undoubtedly competition and rivalry between sets, having different organised criminal groups specialise in different services (for example, ransomware development or initial access) is an efficient model that allows them to increase the tempo and volume of their operations. Collaboration in the hosting of victim data on multiple ransomware operator blogs has also been observed. Recent evidence suggesting that ransomware operators are on active ‘recruitment drives’

---

23. These figures are generally in the range that is claimed on ransomware victim blogs, and comparison of data volumes of initial and full leaks confirms that these are accurate.


EMERGING INSIGHTS

for new talent are a concerning sign that the scale of the threat is still increasing.\(^\text{28}\) Generally, ransomware operators work in a ‘professional’ manner, with some including ‘chat/support’ functions on their victim sites.\(^\text{29}\)

- **Building on past success.** Ransomware operators learn from their own successes and failures, as well as those of others. Each news headline that reports a successful ransomware attack – and a payout from the victim (who was potentially left with no other option) – is encouraging to the cybercriminal ecosystem. While ransomware attacks without data theft still occur, the double extortion approach has been picked up by more and more groups, encouraged by successes and increasing ransom payments, with notable attacks against Travelex, CWT, Garmin and other major companies (see case studies below).\(^\text{30}\) Ransomware operators have also demonstrated increasingly innovative ways to market their operations – both to other cybercriminals and to their victims. For instance, the group behind Ragnar Locker ransomware has started using paid Facebook adverts to increase pressure on one of their recent victims, Campari Group.\(^\text{31}\)

- **Payment as a ‘solution’**. While paying the ransom may in some cases be the only viable option for a company to survive, there are several drivers that may be increasing the frequency of payouts. The more organisations that pay a ransom, the more acceptable the notion of paying a ransom to solve the problem becomes. Furthermore, when an organisation has a cyber insurance policy, it might be able to claim the ransom back, which may encourage payment.\(^\text{32}\) Besides, the cost of payment may be far lower than the potential damages to the business, especially if they cannot recover quickly.\(^\text{33}\)

---


30. Cimpanu, ‘Here’s a List of All the Ransomware Gangs Who Will Steal and Leak Your Data If You Don’t Pay’.


33. There is evidence to suggest cyber insurers are, in some cases, working to prevent ransoms being paid. See Marsh, ‘Cyber Insurance is Supporting the Fight
increasing use of ransomware ‘recovery’ companies. In some cases, these companies will simply act as middlemen and drive down the ransom demand and agree an amount (as well as taking a cut), as opposed to undertaking a technical recovery.\textsuperscript{34} These issues will be returned to later in this paper.

- **Range of initial access vectors.** As shown in Figure 1, there is considerable variety in the type of initial access vectors seen and reported in ransomware cases. The use of spear-phishing emails, exploitation of vulnerabilities in external-facing infrastructure and brute force attacks on services, such as Remote Desktop Protocol (RDP), can theoretically allow for a wide net to be cast in the search for potential victims. Compromise of managed service providers (MSPs) has also proved fruitful for a number of ransomware groups.\textsuperscript{35} Research has highlighted that both human (social engineering) and technical vulnerabilities are exploited in ransomware attacks, and that this creates difficulties in establishing effective countermeasures.\textsuperscript{36} Furthermore, 2019 and 2020 were prolific years for the exploitation of critical vulnerabilities in external-facing infrastructure, which is quickly followed by public proof-of-concept code on open source repositories like GitHub. Vulnerabilities in Citrix, Pulse Secure, Palo Alto and Fortinet VPNs have been connected with a large number of ransomware attacks.\textsuperscript{37} Industry reports have pointed to RDP being a very commonly used access vector.\textsuperscript{38} It is also worth noting that in many cases ransomware groups no longer even need to go to the trouble of personally gaining access to victims. They can now employ

---


\textsuperscript{37} Passeri, ‘Double Extortion Ransomware Attacks and the Role of Vulnerable Internet-Facing Systems’.

the services of so-called ‘initial access brokers’, who sell access to pre-compromised corporate networks on the deep and dark web.39

• **The coronavirus pandemic.** The boom in remote working during the coronavirus pandemic has undoubtedly increased the potential access surface into target organisations. This is compounded by the potential for misconfigurations and vulnerabilities in new software and network equipment being rolled out across many organisations, as well as weaknesses in home IT. Proving a statistical link between the coronavirus pandemic and the increased frequency of successful ransomware attacks would be difficult, but the increased attack surface and the use of coronavirus-themed phishing emails (which has been rampant across all areas of the threat landscape) are two factors which could potentially explain the increase in ransomware attacks during the pandemic. Further factors are likely to have played a part. While it has been pointed out that the prevalence of RDP as an intrusion vector is not a result of increased remote working – it has consistently been used by ransomware gangs6 – the increased uptake of VPN services using Citrix, Pulse Secure, Fortinet, Palo Alto solutions and others is an important contributor to the increased attack surface. Many of these VPNs have been used as initial access points in ransomware attacks (and other threat activity) when vulnerabilities have not been patched. Furthermore, with many organisations in sectors typically favoured by ransomware operators (for example, healthcare, local government or education) vastly increasing their use of and reliance on remote IT services, victims may be more inclined to pay to restore services than under ‘normal’ conditions.

**THE SCALE OF THE PROBLEM**

Throughout 2020, the BAE Systems Threat Intelligence team studied ransomware operator ‘victim’ blogs and tracked additions and removals of victim organisations to these blogs. It should be noted that some ransomware operators may only publish victim information in cases where initial ransom negotiations fail, so these numbers are an underestimate of the number of successful attacks during the reporting period. Moreover, as stated before, ransomware attacks without the inclusion of data theft and extortion still occur (see, for example, the Garmin case study) and are not accounted for in these statistics.

Blog publications surveyed for this paper indicate a total of over 1,200 ransomware attacks by operators of 16 different ransomware strains, with victims from 63 countries. A graph of new victims over time for different ransomware groups monitored is shown in Figure 3. There has been a sharp increase in this type of activity, and between October and June 2020,

---

BAE Systems saw an over 200% increase in new victim publications across monitored blogs.

**Figure 3:** Daily Rates of New Victim Posts to Ransomware Blogs in 2020

![Graph showing daily rates of new victim posts to ransomware blogs in 2020.](image)

*Source: Author generated and based on data collected by BAE Systems Threat Intelligence.*

*Note: The 16 ransomware operator victim blogs were monitored, and the dates of new victim publications were recorded. These are shown in the graph as a rolling average.*

During BAE Systems’s monitoring period (November 2019–December 2020), approximately 10% of victims were removed from blogs, suggesting a potential baseline rate of one ransom payment in 10 attacks. However, ransom payment rates are hard to measure, and are likely to vary by group – and some payments may be made before the escalation to the name-and-shame on the victim blog. IBM has estimated that approximately one-third of REvil attacks have resulted in ransom payment.40

The majority of ransomware victims named on blogs are organisations that are based or headquartered in the US, which make up approximately 60% of victims. A heat map of global victim locations is shown in Figure 4. As can be seen, there are no victims in Russia and many other post-Soviet countries from the ransomware operators tracked, which is in keeping with the majority of cybercriminal activity launched from a Russian-speaking nexus (most of the ransomware operators in this dataset are believed to be based in Russia).

Organisations of a vast range of revenue sizes have been impacted, ranging from small to medium-sized enterprises (SMEs) to household name multinationals. Ransomware operators are known to scale their ransom demand based on victim revenue. The median victim size by revenue is approximately $40 million, meaning that the majority of victim organisations are SMEs, but over 100 victim organisations named on ransomware blogs have annual revenues in excess of $1 billion, and many of these are multinationals.41

A broad range of sectors is seen in the victim data. The overall trend is indicative of a wide net being cast and the opportunity for attack being taken thereafter, which tallies with use of widespread ‘scanning’ for known vulnerabilities or other weaknesses in public-facing IT infrastructure as a precursor to an attempted intrusion. However, it is possible that some groups operate on a more sector-by-sector approach. More victims from the industrial/manufacturing sector appear on victim blogs than from any other (nearly 20% of victims in total), although this could reflect that a large number of organisations are defined under this heading. The retail, transportation, health, finance and legal sectors are all high on the list, as well as education and government. While full insight into ransomware operator targeting preferences is difficult to gain, targeting specific sectors due to the value of their data and the criticality of their operations (and thus their willingness to pay) is one driver behind the modus operandi of some ransomware sets; others are likely to take a more opportunistic approach.

41. Data from BAE Systems Threat Intelligence.
The National Cyber Security Centre’s (NCSC) Annual Review 2020 also highlights the extent of ransomware attacks, with NCSC Incident Management handling more than three times the number of ransomware incidents compared with the previous year.42

KEY CASE STUDIES

This section focuses on two ransomware attack case studies: Travelex and Garmin. While many other ransomware attacks could have been covered, these case studies present important points relevant to the impact on victim organisations, as well as policy problems which will be covered later in the paper.

Case Study 1: Travelex

On 31 December 2019, the London-based foreign currency exchange Travelex was hit by a ransomware attack which crippled its network and resulted in the perpetrators allegedly stealing 5GB of documents.* The attackers – affiliates of the REvil ransomware operation – demanded that Travelex pay $6 million to restore their systems and prevent the stolen data from being leaked online.

This attack had a devastating effect on Travelex, reducing their operations to pen and paper transactions and impacting a wide range of retail banks who relied on their currency services. Reports estimated that the attack ultimately cost the firm over £25 million and put their parent company, Finablr, under significant financial pressure, with $2.3 million reportedly paid in ransom.† Travelex subsequently filed for bankruptcy, citing the coronavirus pandemic and the cyber attack as key factors.‡


Over 100 victim organisations named on ransomware blogs have annual revenues in excess of $1 billion, and many of these are multinationals.

Case Study 2: Garmin

The sport and fitness technology company Garmin became another victim of a targeted ransomware attack in 2020. It announced on 27 July that a five-day outage starting on 23 July was due to ransomware. The incident affected numerous Garmin online services, its website and customer support. During the outage, Garmin’s share price fell approximately 10%, but this has since recovered with no seemingly lasting effect.

Garmin were able to restore services, but reports surfaced that the company had obtained a decryptor in order to do so. The ransomware used is known as ‘WastedLocker’, which is linked to the criminal group Evil Corp, sanctioned by the US Department of the Treasury in 2019. The ransom amount is not known, but is thought to be a multi-million-dollar figure, with the initial demand allegedly $10 million. This was more akin to a ‘traditional’ ransomware attack in that data theft was not believed to have been carried out or used as leverage.

It is claimed that payment was made via a third party – a ‘ransomware negotiation’ business named Arete IR. It is also claimed that Garmin initially approached another ransomware recovery company, who refused to get involved because the attackers were Evil Corp, thus running the risk of breaking sanction rules.


AUXILIARY COMPLEXITIES

This section explores the evolving complexities surrounding the payment of a ransom. Paying criminals to restore encrypted and/or stolen data has always been seen as somewhat taboo, but increased rates of payment and many notable headline ransom payments – from both government and commercial victims – have arguably made it more ‘acceptable’ to do so.

The section reflects on example cases of ransomware attacks, and reviews important developments from the US Department of the Treasury on the facilitation of ransom payments.
PAYMENT OF A RANSOM DEMAND TO A CRIMINAL GROUP

A thorny issue in the context of ransomware attack is that any ransom payment made to obtain a decryptor and restore services directly funds the cybercriminal ecosystem. Ransomware against organisations is a thriving business and is reportedly worth over $100 million per year for successful criminal groups, such as REvil. Each ransom payment creates further incentives not only for the ransomware operator in question, but for others as well – both existing operators and new entrants. Furthermore, each payment acts as a soft ‘normaliser’ for the act of making a payment, which has always been against prevailing advice.

Of course, ransom payment may be the only viable option for a victim organisation. The following circumstances can make this scenario more likely:

- The entire operation may be completely down, losing income and customers each day.
- The organisation may be unable to restore from backups (either the ransomware impacted these too, backups were not used or backup recovery failed).
- Technical decryption is much harder now for ransomware attacks targeting organisations than for those targeted at individuals. While recovery tools have become available for many ransomware strains through the ‘No More Ransom’ project, the bulk of these are for strains of ransomware targeted at individuals, where cryptographic implementations are often weak, and encryption keys are often shared between victims. The criminal groups undertaking ransomware attacks against organisations have generally implemented their malware and encryption schemes more professionally, often using properly implemented RSA-2048 encryption, and thus technical recovery is likely to be impossible if backups do not survive the attack.


This leaves a tricky policy problem. Ciaran Martin, former head of the NCSC, suggested that if he had ‘one policy card to play’, it would be making the payment of ransoms in ransomware attacks illegal in the UK.\textsuperscript{47} While this is a bold stance, it could have a positive impact on cyber security from a UK perspective:

- UK organisations would be incentivised to bolster their cyber security efforts in key areas, knowing that payment of a ransom cannot be seen as a solution.
- Ransomware operators would likely expend less effort in targeting and compromising UK organisations.

However, Martin has also highlighted that a focus on ransomware from government alone is not the solution, and that it should also be a major area of focus in the wider cyber security community\textsuperscript{48} to identify new and improved ways to help organisations prepare for and defend against ransomware attacks.

**PAYMENT TO A POTENTIALLY SANCTIONED ENTITY**

The issue of payment to a cybercriminal group is further complicated by the fact that some criminal operators are subject to indictments and/or sanctions, typically by the US government. For example, the ‘WastedLocker’ ransomware that impacted Garmin has been linked to the cybercriminal entity Evil Corp, which was sanctioned by the US in 2019.\textsuperscript{49}

The REvil group were unofficially labelled as ‘terrorists’ by the Grubman Shire Meiselas & Sacks law firm after they threatened to leak stolen data related to Donald Trump.\textsuperscript{50} It is entirely possible that more cybercriminal entities involved in ransomware attacks on organisations will be sanctioned or indicted in the months and years to come.

In a public advisory on this issue, the US Department of the Treasury’s Office of Foreign Assets Control (OFAC) announced on 1 October 2020 that OFAC regulations may be violated in cases where ransom payments are made to blocked individuals or entities.\textsuperscript{51} The US Department of the Treasury's
Financial Crimes Enforcement Network (FinCEN) also published an advisory on the same day, focusing on the importance of reporting attacks and sharing information, as well as red flags around ransomware attacks of which financial organisations should be aware.\textsuperscript{52} The OFAC advisory highlights the increasing role that ransomware negotiation and recovery companies have played in recent years, stating:

\begin{quote}
Companies that facilitate ransomware payments to cyber actors on behalf of victims, including financial institutions, cyber insurance firms, and companies involved in digital forensics and incident response, not only encourage future ransomware payment demands but also may risk violating OFAC regulations.\textsuperscript{53}
\end{quote}

Taken together, the OFAC and FinCEN advisories – and the scale of the problem outlined above – paint a complex picture for financial organisations and cyber insurance firms. The role of ‘ransomware response’ companies is also likely to receive additional scrutiny because of the OFAC and FinCEN advisories. A likely outcome of any infringement on OFAC regulations would be a fine for the party/parties that were deemed to have been involved.

Not verifying the identity of the criminal group can make problems worse. The victim organisation and supporting companies may not have confident attribution on the ransomware operator in question, which could cause issues in interpreting documentation, such as the recent OFAC advisory. Collaboration between criminal groups is common, and thus payment to one ransomware operator may indirectly be benefiting another (potentially sanctioned) entity.

Further complications can arise where ransomware is used by state-affiliated actors as opposed to criminal ones: the WannaCry and NotPetya attacks set a precedent here. In these attacks, attributed to North Korea and Russia respectively,\textsuperscript{54} ransomware-like malware was combined with aggressive techniques for spreading the infection, resulting in significant impacts against victims globally. There have been recent industry reports suggesting that both North Korean and Iranian government proxies are


using ransomware. The goals of this activity are not wholly clear at present and questions over attribution remain. Crucially, though, both Iran and North Korea are covered by OFAC country embargoes.

**IMPLICATIONS FOR RANSOMWARE NEGOTIATION AND RECOVERY COMPANIES**

While it could be argued that companies that assist victims in ransom negotiation, payment and technical recovery are providing a valuable service (and one that is very much market driven), there has long been a sense of societal unease about this market. It should not be forgotten that these companies are getting paid by the victim for their services, and that this could take the form of a top-up to the ransom agreed, or some other calculation. A number of companies have made a name for themselves in this area. The OFAC and FinCEN advisories will likely make for uncomfortable reading for these companies, especially as it is likely that further criminal entities involved in ransomware attacks against organisations may be sanctioned and/or indicted in future.

**IMPLICATIONS FOR CYBER INSURANCE**

The cyber insurance industry has boomed in recent years, with awareness of it raised by major events, such as the NotPetya attack in 2017, and the adoption of new regulations, such as GDPR, potentially driving an increase in policy uptake from organisations. However, the extent to which cyber insurance policies cover the losses from ransomware attacks remains unclear.

Alongside perceptions that cyber insurance is a secretive market where pay-outs are hard to unlock, the OFAC and FinCEN advisories are notable in that they mention cyber insurance firms as being potentially involved in facilitating payments to hostile cyber actors. There has been anecdotal evidence that some cyber insurers have been inclined to encourage policy-holders to pay ransoms for some time, potentially driven by the calculation that the (negotiated) ransom demand is far smaller than the cost.

---


of attempting a recovery ‘from scratch’. This sentiment was recently echoed by Ciaran Martin, who warned: ‘At the moment, companies have incentives to pay ransoms to make sure this all goes away’.60

Another question this provokes is whether holding a cyber insurance policy with ransomware coverage could in fact drive organisations to deprioritise cyber security spending. Some argue that taking out a cyber insurance policy could actually discourage secure behaviours, a concept known as ‘moral hazard’.61 Several studies have found that organisations are less likely to invest in risk prevention if they think that their cyber insurance policy will resolve (and/or cover the cost of) an incident anyway.62

In addition, there are varying approaches that cyber insurers may take to assess cyber risk within organisations and there is ambiguity over what constitutes ‘good’ cyber security behaviours. Cyber security standards63 play a role in how policies are underwritten and which controls organisations introduce to improve their cyber security.64 Yet, different cyber insurers require different security controls to underwrite a policy.65 The role of cyber insurance in mitigating or encouraging ransomware attacks is part of a wider debate on whether cyber insurance actually serves to incentivise better cyber security practices.66

---

CONCLUSIONS

Potential courses of action for organisations, policymakers, law enforcement and national-level cyber security agencies are outlined in this section. It categorises potential approaches using the ‘four Ps’: ‘Prevent, Pursue, Protect and Prepare’, followed by a set of questions designed to provoke debate in these areas. Figure 5 summarises potential policy options to counter the ransomware threat. Finally, the paper suggests areas for further research.

**Figure 5: Summary of Areas of Potential Action to Counter the Ransomware Threat**

<table>
<thead>
<tr>
<th>Action</th>
<th>Policymakers</th>
<th>Law enforcement</th>
<th>National cyber security agencies</th>
<th>Organisations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prevent</td>
<td></td>
<td>Counter use of pentest tools</td>
<td>With data sharing into... (from victims and Threat Intelligence/Incident Response companies)</td>
<td></td>
</tr>
<tr>
<td>Pursue</td>
<td></td>
<td>Pursuance of criminals across the attack chain</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Protect</td>
<td>Outlaw ransom payments</td>
<td>New active cyber defence areas</td>
<td>Prioritisation/Advice on</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cyber insurance regulation</td>
<td></td>
<td>Doing the basics right and better</td>
<td></td>
</tr>
<tr>
<td>Prepare</td>
<td></td>
<td></td>
<td>Ensure backup and recovery plans</td>
<td></td>
</tr>
</tbody>
</table>

*Source: Author generated.*

**PREVENT**

Policymakers and law enforcement officials should consider addressing the prolific use of tools designed for penetration testing/‘red team’ security in ransomware attacks. Many of the tools used by criminal operators are either free or commercial tools (often cracked versions) which are designed for legitimate use. These tools have long been abused by hostile cyber actors and have systemically lowered the barrier to entry for would-be criminal

---

67. These are the same ‘Ps’ as the UK’s CONTEST counterterrorism strategy, as these cover relevant mitigation areas effectively and concisely. To be clear, this is not an attempt to draw any parallels between ransomware and terrorism. The ‘four Ps’ are used commonly by UK law enforcement for other crime types including cybercrime.

groups (these tools are also heavily used by state actors). Examples include Cobalt Strike, PowerShell Empire and Metasploit.

- Is there anything that can be done to address this from a regulatory perspective?
- Is there anything that can be done to address this from a technical perspective? Can this feed into pursuit activities (see below)?

Pursue

Coordinated law enforcement responses to organised cybercrime have scored many successes in the past, although progress against cybercriminal groups based in Russia has been far more difficult to achieve. To get on top of the current problem, these efforts will need to be significantly scaled up, and new initiatives to accelerate progress will be needed. The questions below are also likely to be relevant to national-level cyber security agencies:

- Can national- and international-level schemes for the pursuit of ransomware operators be established?
- Can investigatory teams seeking to establish operator identities and methods get access to more data from threat intelligence and incident response efforts conducted by specialist companies? How can this best be facilitated?
- Can these efforts be turned into technical disruption activity, and the pursuit and arrest of those involved? Are penetration testing tools a suitable substrate for disruption, or is further coordinated action against precursors such as Emotet,\(^{69}\) Trickbot\(^ {70}\) and other criminal malware needed? Can technical disruption by itself ever be more than ‘whack-a-mole’?
- Can gains be made in the pursuit of entities involved in the facilitation of laundering cryptocurrency ransom payments (for example, cryptocurrency services or third parties, which may enable scaling across multiple ransomware operators)\(^ {71}\)? Does the seizure of the cryptocurrency proceeds of cybercrime – such as in recent action against NetWalker ransomware – make these disruption operations more effective, and does this dissuade criminal activity from these operators?\(^ {72}\)

PROTECT

Unfortunately, ransomware operators have used numerous strategies for the initial stages of their compromise and are quick to take advantage of new opportunities that may arise. Once inside a network, operators are skilled at maximising their presence through lateral movement and ultimately maximising the impact of the ransomware once deployed.

The best strategy for organisations to protect against ransomware attacks should start with ‘doing the basics right’, which is easy to say but can be very tricky to enact. While this list is not prescriptive nor sufficient to ensure security against attack, the following steps are likely to be highly effective in mitigating the threat:

- Ensure timely patching of any critical vulnerabilities in external-facing infrastructure (web servers, VPN infrastructure).
- Use multifactor authentication where possible on vulnerable services, for example, RDP.
- Employ application allow-listing on enterprise estates.
- Reinforce phishing awareness through regular exercises.

At a higher level, there are broader questions related to the guidance on and measurement of cyber security best practice, which may relate to policymakers and national-level cyber security bodies.

- Are there any ‘quick wins’ that can be found in this area?
- In the UK, are there elements of the NCSC’s Active Cyber Defence programme that can be extended or designed to help protect specifically against ransomware attack? For example, can DNS-level and similar protections be broadened to cover a greater number of organisations within and outside government?

Furthermore, policymakers should carefully examine the feasibility and suitability of making ransom payment illegal in the UK, which could lead in turn to a ‘protective’ effect resulting from the discouragement of ransomware attacks against UK targets.

- Is a complete outlawing of ransom payment possible?
- If not, could measures be put in place to ensure that payments are only made when all other options have been exhausted and where the alternatives are deemed to be less desirable than a payment?
- Are there regulatory steps that can be taken in the area of cyber insurance and ‘ransomware recovery’ that could have a positive effect on the situation?

PREPARE

Organisations across all sectors should appreciate that they could potentially be hit by a ransomware attack at any moment – no organisation should consider themselves immune from this threat. Ransomware attacks should be recognised as an organisational risk such that appropriate governance and resources around it can be put in place. Preparedness in the event of a ransomware attack should be focused on effective organisational incident response and ensuring that adequate backup mechanisms are in place (with offline backups a priority). Furthermore, these processes should ensure backups can be restored in an effective and timely manner.

The fact that so many ransomware attacks cannot be recovered from backups indicates that there is a systemic problem in this area. Policymakers and national-level cyber security bodies may be able to influence change here.

- Can a mechanism be found to provide strong guidance and, potentially, enforcement of the need for appropriate backup measures across the UK, perhaps on a sector-by-sector basis?

ABOUT THE AUTHORS

James Sullivan is Director of Cyber Research at RUSI. His research focuses on national cyber strategies, the globalisation of technology, cyber resilience, cybercrime, and issues relating to offensive cyber.

James Muir leads on thematic and technology threat research at BAE Systems Applied Intelligence. He is a secondee with the UK government's National Cyber Security Centre's Industry 100 scheme.
About RUSI

The Royal United Services Institute (RUSI) is the world’s oldest and the UK’s leading defence and security think tank. Its mission is to inform, influence and enhance public debate on a safer and more stable world. RUSI is a research-led institute, producing independent, practical and innovative analysis to address today’s complex challenges.

Since its foundation in 1831, RUSI has relied on its members to support its activities. Together with revenue from research, publications and conferences, RUSI has sustained its political independence for 190 years.

The views expressed in this publication are those of the authors, and do not necessarily reflect the views of RUSI or any other institution.

Published in 2021 by the Royal United Services Institute for Defence and Security Studies. RUSI is a registered charity (No. 210639).

This work is licensed under a Creative Commons Attribution – Non-Commercial – No-Derivatives 4.0 International Licence. For more information, see <http://creativecommons.org/licenses/by-nc-nd/4.0/>.