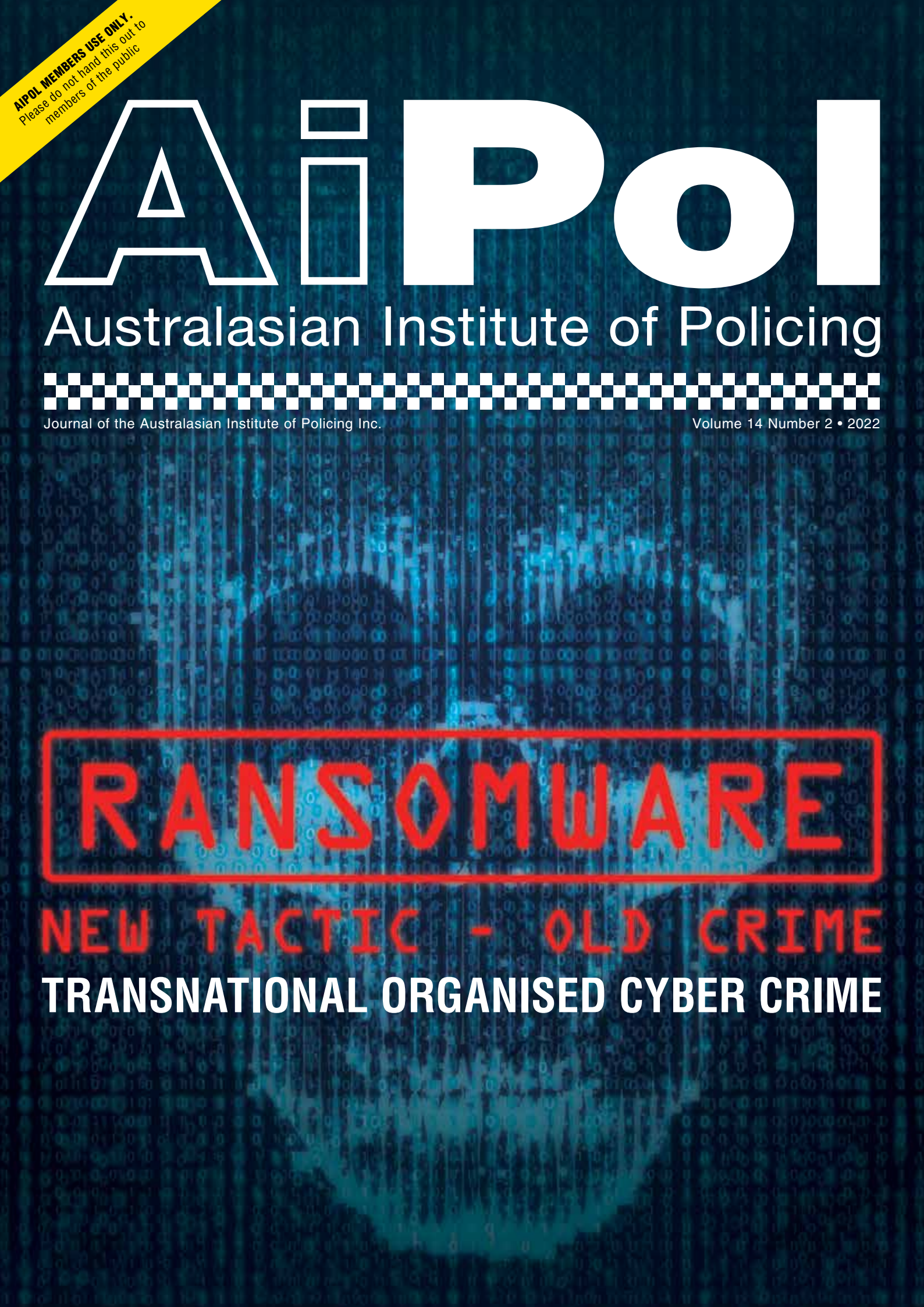
AiPol

Australasian Institute of Policing

Journal of the Australasian Institute of Policing Inc. Volume 14 Number 2 • 2022



TRANSNATIONAL ORGANISED CYBER CRIME

We're Recruiting

Securecorp is a leading national provider of Security, Electronics, Monitoring, Cleaning and Training services. First established in 1998 as a Victorian-based security and risk management business, Securecorp has since grown to a nation-wide group of companies delivering a full range of services including:

- Securecorp Security - Security Manpower Services
- Securecorp Cleaning - Cleaning Services
- Securecorp Electronics - Electronic Security Installation and Maintenance Services
- Securecorp Monitoring - Security Alarm Monitoring and Response

With offices across Australia, Securecorp today employs over 2,500 staff Australia wide with services in New Zealand.

Across all entities and services, we are focused on quality management, innovation, professional development, and exceptional service delivery.

Our dedication to operational excellence is the driving force behind the continual development of in-house systems and implementation of innovative technologies to improve efficiencies, transparency, and accountability.

You can learn more about Securecorp by visiting our website: **https://www.securecorp.com.au/**
All positions are on our careers page **https://securecorp.elmotalent.com.au/careers/SECUREcorp/jobs**

If you have any questions you can contact the National Head Office:

Phone: **(03) 8527 8888**
Email: **recruitment@securecorp.com.au**

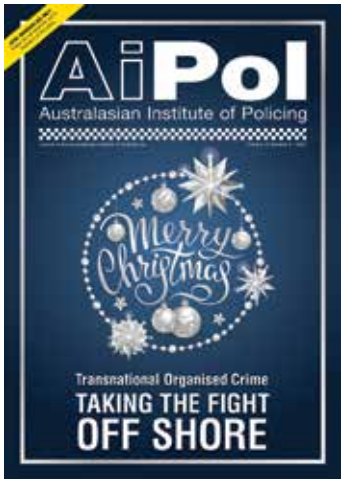
SECURECORP

www.securecorp.com.au

AiPol
Australasian Institute of Policing

Vol. 14, No. 2
June 2022

Published by the Australasian Institute of Policing Inc.
A0050444D ABN: 78 937 405 524
ISSN: 1837-7009



Visit **www.aipol.org** to view previous editions and to subscribe to receive future editions.

Contributions

Articles on issues of professional interest are sought from Australasian police officers and police academics. Articles are to be electronically provided to the Editor, aipoljournal@aipol.org. Articles are to conform to normal academic conventions. Where an article has previously been prepared during the course of employment, whether with a police service or otherwise, the contributor will be responsible for obtaining permission from that employer to submit the article for publication to Australasian Policing.
Contributors are expected to adhere to the Journal's publishing guidelines. These guidelines are available in this Journal. All papers are peer-reviewed.

Disclaimer

Copyright

Contents

ANNOUNCING THE ALL NEW

Cellebrite
GUARDIAN

Transform Your Workflow and Evidence Management

Editorial

DR AMANDA DAVIES

Editor, Assistant Professor Policing and Security at the Rabdan Academy, Abu Dhabi

Australian police and law enforcement agencies are to be commended for their initiatives and efforts in partnering across the country to respond to this criminal activity, for the future these efforts require maximum support to respond to the call by Interpol.

Dear Readers

Welcome to the latest edition of AiPOL. This edition is dedicated to the burgeoning crime associated with Ransomware.

As responding to the Covid-19 pandemic has demanded the refocusing of policing and security entities across the world, cybercrime has found opportunities to develop exponentially. In part, restrictions applied during the height of the Covid-19 pandemic has driven criminal activity inside/off the street creating an increase in the number of criminal fraternities turning to online/ internet-based crime. In parallel, cyber criminals used the pandemic to scale up their 'businesses' as evidenced in the ransomware attacks on hospitals in the USA and UK – with multimillion dollar demands at a time of the greatest health crisis of the century. Individuals did not escape the target of cybercriminals with phishing emails related to information on vaccines, medical masks, or in-demand supplies like hand sanitizers, scams offering financial assistance during the economic shutdowns in countries across the world. Globally, cyber criminals disrupted supply chains impacting the delivery of critical medical and food supplies for example.

What is ransomware, how has it morphed into one the largest criminal activities of our time and are police and security organizations winning the war against cybercrime?

An excellent article by James Sullivan (from the UKs leading defence and security think tank) and James Muir (BAE Systems applied Intelligence, UK) provides a thorough explanation of Ransomware, how criminals are utilizing ransomware and how the world of business is responding – often with multimillion dollar payments to the criminal network. An interesting point made in the article is the readily available tools used in ransomware attacks – commercial off the shelf or free tools designed for legitimate use.

Australia has not escaped major attacks as discussed in the article by Falk and Brown who explain the Australian problem. The article includes a discussion of the ransomware attacks which occurred to Australian businesses, particularly during the Covid-19 pandemic period – illustrating the threats connected to some of the largest global cybercriminal networks e.g., REvil group. The article also discusses the national survey conducted to understand the extent of the Australian public's knowledge of ransomware – results indicating the community 'generally has little understanding of ransomware'. This is disappointing for the police and law enforcement community tasked with combating cybercrime – an informed public has the potential to assist police and law enforcement agencies more adequately in their efforts.

The extent of this criminal activity is reflected by the Secretary General of Interpol, Jurgen Stock who argues the threat is too large for any one country to fight alone and the very nature of the crime with its global reach requires a global leadership response. Australian police and law enforcement agencies are to be commended for their initiatives and efforts in partnering across the country to respond to this criminal activity, for the future these efforts require maximum support to respond to the call by Interpol.

The collection of articles in this edition are timely and offer a comprehensive view of the current and potential impact of cybercrime through Ransomware on multiple facets of community well being.

Dedicated to our members and their future

QSuper

Part of Australian Retirement Trust

Visit QSuper.qld.gov.au today

Transnational Organised Cyber Crime

President's Foreword

JON HUNT-SHARMAN

President, Committee of Management, Australasian Institute of Policing

The Australian Institute of Criminology (AIC) has recently identified pure cybercrime impacting on Australia, including ransomware, to cost an estimated $3.5b in 2020-21. The Australian Cyber Security Centre (ACSC) also had a 15% increase in reports of ransomware attacks over the past 12 months.

Transnational Organised Cyber Crime (TOCC) syndicates, target Australians using cyber-enabled tools and techniques. Ransomware and cyber extortion is now the most serious cybercrime threat facing Australia due to its high financial and disruptive impacts to critical infrastructure, Australian businesses and the wider community.

TOCC syndicates utilising ransomware and Transnational Serious & Organised Crime (TSOC) groups have a common thread – Extortion. Traditional organised crime groups, such as the mafia, have used extortion as a profitable crime tool for many years. Now in the 21st Century, extortion is conducted in a more sophisticated and largely untraceable way, known as Ransomware.

Indeed, it could well be argued that some of the TOCC syndicates are just technically savvy participants committing the age old crime of extortion and simply using new tactics. Ransomware has effectively become a sophisticated billion-dollar business because of its anonymity, and its 'high-crime yield'.

There is also a second common thread between TOCC syndicates and TSOC groups: These transnational criminals are largely out of the reach of traditional law enforcement methodology.

The successful criminal prosecution of these transnational criminals for crimes

continued on page 6

continued from page 5

impacting on Australia and Australians is unlikely to succeed without greater cooperation from other nations.

The Australian Government has taken a *'Whole of Government'* approach to dealing with TOCC.

In 2017 the Australian Government identified the need to provide enhanced cyber security capabilities and a single point of advice and support on cyber security. It established the ACSC as a *'Whole of Government'* response.

The ACSC is part of the Australian Signals Directorate (ASD), which is a statutory agency. The ACSC includes staff from the:

- Australian Criminal Intelligence Commission (ACIC)
- Australian Federal Police (AFP)
- Australian Security Intelligence Organisation (ASIO)
- Australian Signals Directorate (ASD)
- Defence Intelligence Organisation (DIO)
- Digital Transformation Agency (DTA)
- Computer Emergency Response Team (CERT) and
- Department of Home Affairs Cyber Security Policy Division staff (to collaborate in providing policy advice for government).

The Australian Government identified that to be successful in the fight against TOCC syndicates, the focus must also be on prevention, detection and disruption strategies, in addition to criminal prosecution.

The collaborative approach of agencies and the hard work of their staff seconded to the ACSC has been critical in the fight against TOCC syndicates.

In October 2021, the Australian Government released its *Ransomware Action Plan*. The Plan included Policy & Operational Responses and Legislative Reforms. At the operational level it included additional funding to the ACSC, establishment of a multi-agency taskforce Operation Orcus, led by the AFP and the establishment of Joint Operations with international counterparts to strengthen shared capabilities to detect, investigate, disrupt and prosecute malicious cyber actors engaged in ransomware.

At the legislative level it included amendment to the *Autonomous Sanctions Act* and specific ransomware legislation.

In the move to further strengthen the fight against TOCC, on 2 December 2021, the Australian Parliament passed the *Autonomous Sanctions Amendment (Magnitsky-style and Other Thematic Sanctions) Act 2021 (Cth)*. The Act is designed to sanction individuals and entities responsible for certain "thematic" categories of "egregious conduct". The Act amends the Autonomous Sanctions Act 2011 (Cth) to:

- enable the imposition of autonomous sanctions to address particular issues (called thematic sanctions), as opposed to being only country-specific; and
- sets out the decision-making process for imposing targeted financial sanctions and travel bans on designated persons and entities.

Under the *Autonomous Sanctions Act* it is effectively an offence to do business with a designated person or entity other than in accordance with a permit. That is, it is an offence to directly or indirectly make an asset available to, or for, the benefit of a designated person or entity, or to deal with a designated person's or entity's assets (other than in accordance with a permit).

In February 2022 the *Autonomous Sanctions Amendment Regulations 2021* was passed by Parliament which, amongst other things, allows the Minister for Foreign Affairs to list persons and entities where satisfied that:

- they have caused, assisted with causing, or been complicit in, a cyber incident or an attempted cyber incident that is significant, or which had it occurred, would have been significant.

The previous Parliament, prior to its dissolution, was also considering the *Crimes Legislation Amendment (Ransomware Action Plan) Bill 2022*.

The *Crimes Legislation Amendment (Ransomware Action Plan) Bill 2022*, amends the *Criminal Code Act 1995* to:

- amend the geographical jurisdiction provision for computer offences;
- introduce standalone offences for extortive conduct associated with ransomware and dealing with data obtained by unauthorised access or modification;

The Australasian Institute of Policing (AiPOL) supports the *Ransomware Action Plan* and its accompanying legislations and the bipartisan view of both major political parties that such legislation is needed to fight TOCC.

- introduce aggravated offences relating to cyber attacks on critical infrastructure assets and producing, supplying or obtaining data under arrangement for payment; and
- increase maximum penalties for certain other computer offences;

The *Crimes Legislation Amendment (Ransomware Action Plan) Bill 2022*, also amends *Proceeds of Crime Act 2002* to ensure that existing information gathering powers and freezing orders in relation to financial institutions can also be exercised in relation to digital currency exchanges; and amends the *Crime Act 1914* and *Proceeds of Crime Act 2002* to ensure that law enforcement agencies can seize digital assets (including cryptocurrency) discovered during the execution of a warrant and suspected to be proceeds of crime.

The Australasian Institute of Policing (AiPOL) supports the *Ransomware Action Plan* and its accompanying legislations and the bipartisan view of both major political parties that such legislation is needed to fight TOCC.

The Australian Government and it's agencies, should be commended for taking a *'Whole of Government'* approach, however it is now time for a *'Whole of Nations'* approach.

Not withstanding the *Ransomware Action Plan*, the policy and operational response and the legislative reforms such as the *Crimes Legislation Amendment (Ransomware Action Plan) Bill 2022* and the *Autonomous Sanctions Amendment Regulations*, it is likely to be deficient against TOCC, without international collaboration.

The successful Australian *'Whole of Government'* approach now needs to be replicated as a *'Whole of Nations'* approach.

Speaking at the INTERPOL High-Level Forum on Ransomware (12 July 21), Secretary General Stock said that while some solutions existed nationally or bi-laterally, effectively preventing and disrupting ransomware meant adopting the same international collaboration used to fight terrorism, human trafficking or mafia groups such as the 'Ndrangheta.

It is now time to follow the advice of Secretary General Stock and take a stronger international collaboration approach. With the US, the UK, Canada and the EU, having similar 'Magnitsky' *Autonomous Sanctions Acts* there is a great opportunity to adopt a *'Whole of Nations'* approach under the various 'Magnitsky' legislations by ensuring identical listing of TOCC entities and individuals.

There is precedent, at the bi-lateral level the UK copied the listing decisions of the EU as far as restrictive measures concerning cyber crime. The EU adopted sanctions in July and October 2020 and in both cases the UK included the names of EU-listed persons and entities in its consolidated list of financial sanctions.

AiPOL recommends that under the powers of the *Autonomous Sanctions Amendment Regulations 2021*, the newly elected Minister for Foreign Affairs should lay the foundations for a *'Whole of Nations'* approach to TOCC, by collaborating with other like minded nations to ensure that the listing of persons and entities for cyber crime are mirrored across each jurisdiction, where possible.

Five Eyes Consulting

Australia's Trusted Information Security & IT Consultancy

We help secure and protect your organisation from Emerging Threats

ABOUT US

Five Eyes Consulting is a fast-growing Information Security and Technology consulting firm based in Canberra

WHY CHOOSE US?

With a workforce that has over 20 years of experience specialising in Cyber Security, Information Technology and Programme and Project Management, we partner with public and private sector organisations of all sizes to solve their most complex challenges

CONTACT US

contact@fiveeyes.com.au

www.fiveeyes.com.au

OUR SERVICES

Cyber Security

We provide cyber security solutions, risk management, audit and information security expertise to organisations of all sizes

Technology & Architecture

We provide specialist technical advice on the architecture, design, implementation and maintenance of enterprise ICT systems

Project Delivery

We provide a complete portfolio, programme and project delivery service that can develop and translate strategy into tangible outcomes

Immediate action required to avoid Ransomware pandemic

Secretary General calls for global leadership commitment by police and partners.

12 July 2021

INTERPOL

LYON, France
INTERPOL Secretary General Jürgen Stock has called for police agencies worldwide to form a global coalition with industry partners to prevent a potential ransomware pandemic.

Speaking at the INTERPOL High-Level Forum on Ransomware (12 July), Secretary General Stock said that while some solutions existed nationally or bi-laterally, effectively preventing and disrupting ransomware meant adopting the same international collaboration used to fight terrorism, human trafficking or mafia groups such as the 'Ndrangheta.

The call to scale up collaboration against ransomware was made in the face of its exponential growth in the wider cybercrime ecosystem, with criminals shifting their business model towards providing Ransomware-as-a-Service.

"Despite the severity of their crimes, ransomware criminals are continuously adapting their tactics, operating free of borders and with near impunity," said Secretary General Stock.

"Much like the pandemic it exploits, ransomware is evolving into different variants, delivering high financial profits to criminals."

"Ransomware has become too large of a threat for any entity or sector to address alone; the magnitude of this challenge urgently demands united global action which INTERPOL can uniquely facilitate as a neutral and trusted global partner," added Secretary General Stock.

Research from Chainalysis found that criminals made USD 350 million in 2020 from ransomware payments, representing an increase of 311 per cent in one year. Over the same period, the average ransom payment increased by 171 per cent, according to Palo Alto Networks.

Some 370 participants from public, private and international entities – including the World Economic Forum (WEF), UNODC and national computer emergency response teams – examined ransomware attacks on critical infrastructures worldwide in the past 12 months alone, including on schools, hospitals, food suppliers and a major oil pipeline.

Ransomware is emerging as the "Wild West" equivalent of digital space where anyone, at any point of time, can become a victim.

"Ransomware is emerging as the "Wild West" equivalent of digital space where anyone, at any point of time, can become a victim. Curbing ransomware demands collective efforts from all to improve cyber hygiene across sectors, to raise cost and risk to cybercriminals through disruptive efforts and to reduce payoff to the criminals," said Tal Goldstein, Head of Strategy, Centre for Cybersecurity, WEF.

"The World Economic Forum Partnership, in close collaboration with INTERPOL, has been working to shape global architectures to support such collaboration and explore ways to encourage responsible measures by the leadership of victim organisations."

With Project Gateway providing a framework which enables INTERPOL to cooperate with private partners and receive threat data directly, participants endorsed four recommendations to create a global leadership framework for action to disrupt and mitigate the impact of ransomware:

1. Prevent ransomware by raising awareness, partnerships and information sharing.
2. Aim for pre-exploit disruption of ransomware and its ecosystem through global law enforcement actions both reactively and proactively.
3. Provide in-event emergency support against ransomware attacks with the use of INTERPOL's global network and capabilities.
4. Ensure post-event support following ransomware attacks to increase resilience, agility and responsiveness.

"Policing needs to harness the insights of the cyber security industry, computer emergency response teams and other agencies to identify and disrupt cyber criminals as part of a true coalition, working together to reduce the global impact of cybercrime," concluded Secretary General Stock.

Under this framework, INTERPOL will also focus on identifying, targeting and disrupting cybercrime threat actors behind ransomware attacks by taking a regional approach for operational coordination with member countries.

GOLD COAST **DETOX** & **REHAB** SERVICES

Private Drug & Alcohol Withdrawal

7-28 day drug and alcohol withdrawal programs

Confidential, Discreet, Personal

- 24 hour medical care
- Pharmacotherapy
- Integrative therapies
- Massage, Acupuncture and Nutrition
- A comfortable, non-clinical environment
- Luxury accommodation on the beachfront

Medical supervision includes resident doctor, registered nurses and addiction counsellors

ROOMS START AT $1500 +GST PER DAY

(includes all medical services and medication, therapy, food, accommodation, airport pickup)

FOR MORE INFORMATION:

Phone: 07 5559 5811 | Email: manager@goldcoastdetoxandrehab.com

WWW.GOLDCOASTDETOXANDREHAB.COM

Ransomware: A Perfect Storm

JAMES SULLIVAN AND JAMES MUIR

Royal United Services Institute for Defence and Security Studies

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,[1] 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.[2] 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.[3] 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,[4] 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).[5]

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 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.

continued on page 12

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'.[6] The BAE Systems Incident Response team has been engaged in 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[7] 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.[8]

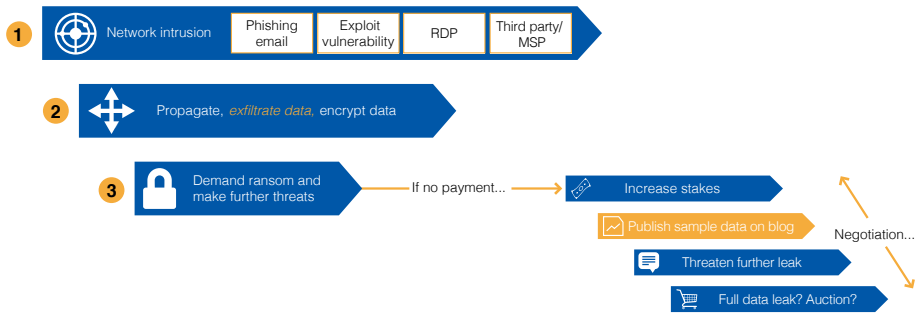
Ransomware's perfect storm

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?

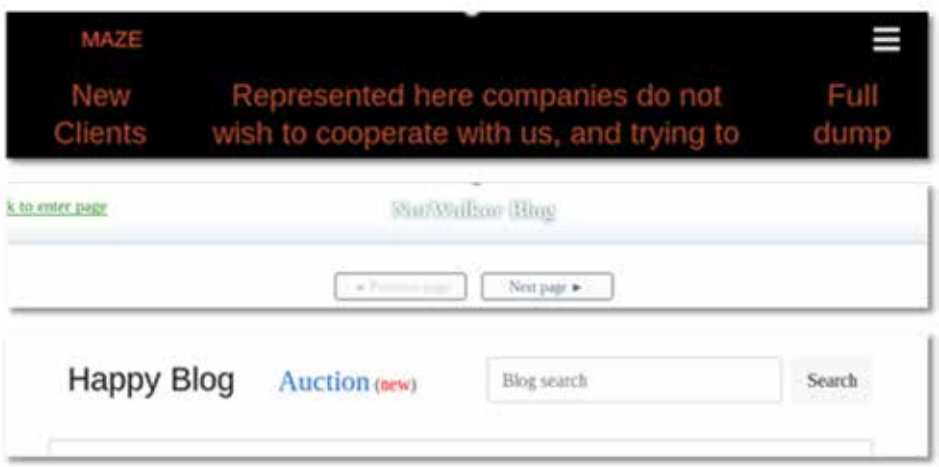
The concept of a criminal attack in which the victim's files are 'locked' (encrypted) and payment is demanded for recovery dates back to the mid-2000s.[9] In the 2010s, an increasingly popular mode of cybercrime was a ransomware attack against individuals

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



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.

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.

distributed via indiscriminate phishing campaigns. Ransomware strains such as CryptoLocker have been particularly damaging.[10]

In recent years, cybercriminal operators have increasingly targeted organisations, as opposed to individuals.[11] 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.[12] 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.[13]

Double extortion ransomware has been referred to variously as 'targeted ransomware', 'big game hunting ransomware',[14] and 'human-operated ransomware',[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.[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.

Atypical 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.

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,[17] 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.[18]

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 based on (further) extortion to encourage ransom payment.[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.[20] Another potential outcome in the extortion chain is the 'auction' of stolen data to the highest bidder.[21]

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.[22] Regulations, such as the General Data Protection Regulation (GDPR), have also effectively increased the sensitivity and value 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),[23] 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.[24]

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.[25] 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.[26] 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.[27] Recent evidence suggesting that ransomware operators are on active 'recruitment drives' for new talent are a concerning sign that the scale of the threat is still increasing.[28] Generally, ransomware operators work in a 'professional' manner, with some including 'chat/support' functions on their victim sites.[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).[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.[31]

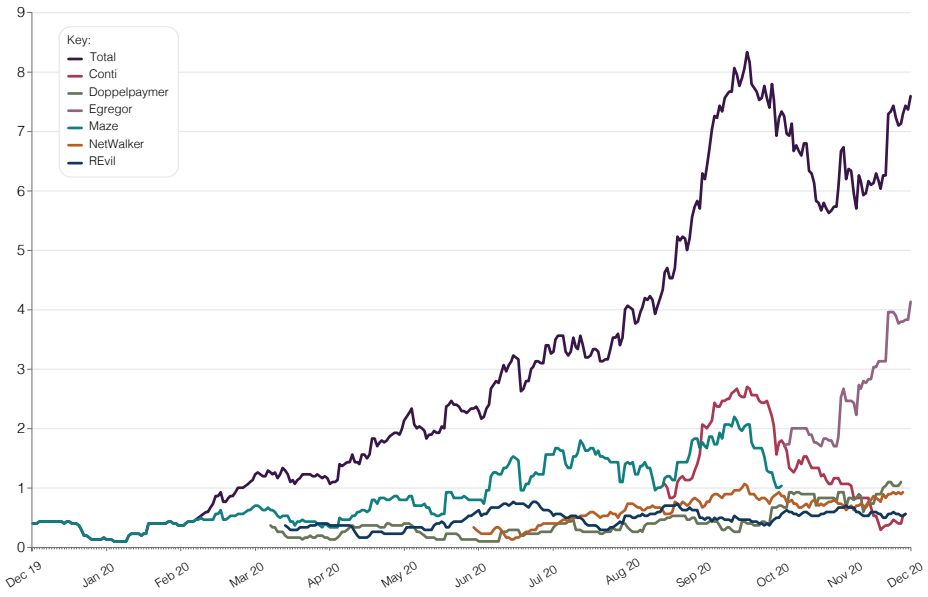
Payment as a 'solution'. While paying the ransom may in some cases be the only viable option for a company to survive, there are several drivers that may be increasing the frequency of payouts. The more organisations that pay a ransom, the more acceptable the notion of paying a ransom to solve the problem becomes. Furthermore, when an organisation has a cyber insurance policy, it might be able to claim the ransom back, which may encourage payment.[32] Besides, the cost of payment may be far lower than the potential damages to the business, especially if they cannot recover quickly.[33] There is also an 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.[34] These issues will be returned to later in this paper.

continued on page 14

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.[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.[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.[37] Industry reports have pointed to RDP being a very commonly used access vector.[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 the services of so-called 'initial access brokers', who sell access to pre-compromised corporate networks on the deep and dark web.[39]

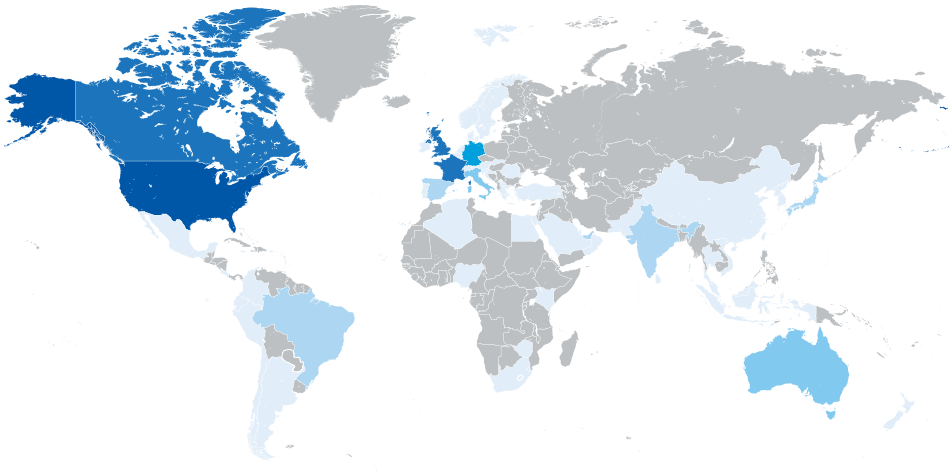
The coronavirus pandemic. The boom in remote working during the coronavirus pandemic has undoubtedly increased the potential access surface into target organisations. This is compounded by the potential for misconfigurations and vulnerabilities in new software and network equipment being rolled out across 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.

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



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.

Figure 4: Heatmap Showing Location/Headquarters of Victims Named on Ransomware Blogs



Source: Author generated, derived from analysis of 16 ransomware operator victim blogs. Note: In a case where the victim is a multinational, the location of their headquarters is recorded on the map.

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.

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 group 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

continued on page 16

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.‡

Sources: *Joe Tidy, 'Travelex Being Held to Ransom by Hackers', BBC News, 7 January 2020; †Teiss, 'Travelex Paid $2.3m in Ransom to REvil Cyber Gang', 16 April 2020, <https://www.teiss.co.uk/travelex-ransom-revil-group/>, accessed 16 November 2020; Lawrence Abrams, 'Travelex Reportedly Paid $2.3 Million Ransom to Restore Operations', Bleeping Computer, 9 April 2020, <https://www.bleepingcomputer.com/news/security/travelex-reportedly-paid-23-million-ransom-to-restore-operations/>, accessed on 16 November 2020; ‡Larry Jaffee, 'Travelex Driven into Financial Straits by Ransomware Attack', SC Media, 10 August 2020, <https://www.scmagazine.com/home/security-news/travelex-driven-into-financial-straits-by-ransomware-attack/>, accessed 16 November 2020.

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.

Sources: *Zack Whittaker, 'Garmin Confirms Ransomware Attack Took Down Services', techcrunch, 27 July 2020, <https://techcrunch.com/2020/07/27/garmin-confirmsransomware-attack-outage/>, accessed 16 November 2020; †Yahoo Finance, 'Garmin Ltd. (GRMN)', <https://uk.finance.yahoo.com/quote/GRMN/>, accessed 16 November 2020; ‡Lawrence Abrams, 'Confirmed: Garmin Received Decryptor for Wastedlocker Ransomware', Bleeping Computer, 1 August 2020, <https://www.bleepingcomputer.com/news/security/confirmed-garmin-received-decryptor-for-wastedlocker-ransomware/>, accessed 16 November 2020; §US Department of the Treasury, 'Treasury Sanctions Evil Corp, the Russia-Based Cybercriminal Group Behind Dridex Malware', press release, 5 December 2019, <https://home.treasury.gov/news/press-releases/sm845>, accessed 16 November 2020; **Alexander Martin, 'Garmin "Paid Multi-Million Dollar Ransom to Criminals Using Arete IR", Say Sources', Sky News, 3 August 2020.

continued from page 15

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.

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.

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.[43]

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.[44]

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,[45] 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,[46] 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.[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[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.[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.[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.[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.[52] The OFAC advisory highlights the increasing role that ransomware negotiation and recovery companies have played in recent years, stating:

> 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.[53]

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.

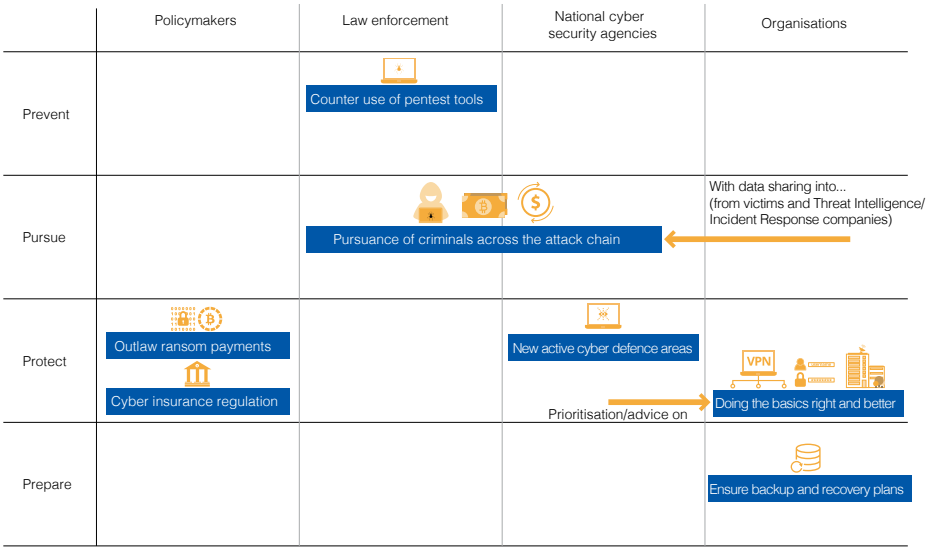
Not verifying the identity of the criminal group can make problems worse. The victim organisation and supporting companies may not have confident attribution on the ransomware operator in question, which could cause issues in interpreting documentation, such as the recent OFAC advisory. Collaboration 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,[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.[55] 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.[56] 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.

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



Source: Author generated.

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.[57]

Alongside perceptions that cyber insurance is a secretive market where pay-outs are hard to unlock,[58] 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,[59] 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 standards[63] 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.[67] Figure 5 summarises potential policy options to counter the ransomware threat. Finally, the paper suggests areas for further research.

continued on page 18

continued from page 17

Prevent

Policymakers and law enforcement officials should consider addressing the prolific use of tools designed for penetration testing/'red team' security in ransomware attacks.[68] 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 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?[73] 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).

References

1. BAE Systems Newsroom, 'BAE Systems Partners with RUSI on Cyber Security Research Programme', 4 September 2019, <https://www.baesystems.com/en/cybersecurity/article/bae-systems-partners-with-rusi-on-cyber-securityresearch-programme>, accessed 9 February 2021.

2. National Crime Agency, 'Annual Plan 2018–19', <https://www.nationalcrimeagency.gov.uk/who-we-are/publications/168-nca-annualplan-2018-19/file>, accessed 16 November 2020.

3. Alex Scroxton, 'Software AG Caught in Double Extortion Ransomware Hit', Computer Weekly, 12 October 2020, <https://www.computerweekly.com/news/252490395/Software-AG-caught-in-double-extortion-ransomwarehit>, accessed 16 November 2020; Phil Muncaster, 'Travelex Forced into Administration After Ransomware Attack', Info Security, 10 August 2020, <https://www.infosecurity-magazine.com/news/travelex-forcedadministration/>, accessed 16 November 2020.

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-yourdata-if-you-dont-pay/>, accessed 16 November 2020.

5. Debbie Walkowski, 'What is the CIA Triad?', F5 Labs, 9 July 2019, <https://www.f5.com/labs/articles/education/what-is-the-cia-triad>, accessed 16 November 2020.

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.

7. See Microsoft, 'Ransomware Groups Continue to Target Healthcare, Critical Services; Here's How to Reduce Risk', 28 April 2020.

8. US Department of the Treasury, 'Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments', 1 October 2020, <https://home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020_1.pdf>, accessed 16 November 2020.

9. BBC News, 'Extortion Virus Code Gets Cracked', 1 June 2006.

10. Leo Kelion, 'Cryptolocker Ransomware Has "Infected About 250,000 PCs"', BBC News, 24 December 2013.

11. Ronny Richardson and Max North, 'Ransomware: Evolution, Mitigation and Prevention', International Management Review (Vol. 13, No. 1, 2017), p. 13.

12. Sergiu Gatlan, 'Software AG IT Giant Hit with $23 Million Ransom by Clop Ransomware', Bleeping Computer, 9 October 2020, <https://www.bleepingcomputer.com/news/security/software-ag-it-giant-hit-with-23-millionransom-by-clop-ransomware/>, accessed 16 November 2020.

13. Lena Connolly et al., 'An Empirical Study of Ransomware Attacks on Organisations: An Assessment of Severity and Salient Factors Affecting Vulnerability', Journal of Cybersecurity (Vol. 6, No. 1, 2020).

14. Sergei Frankoff and Bex Hartley, 'Big Game Hunting: The Evolution of INDRIK SPIDER From Dridex Wire Fraud to BitPaymer Targeted Ransomware', Crowdstrike, 14 November 2018, <https://www.crowdstrike.com/blog/big-gamehunting-the-evolution-of-indrik-spider-from-dridex-wire-fraud-to-bitpaymertargeted-ransomware/>, accessed 19 January 2021.

15. Microsoft, 'Human-Operated Ransomware Attacks: A Preventable Disaster', 5 March 2020.

16. Sarah Coble, 'MAZE Relaunches "Name and Shame" Website', Info Security, 10 January 2020, <https://www.infosecurity-magazine.com/news/mazerelaunches-name-and-shame/>, accessed 16 November 2020.

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.

18. DFIR Report, 'Ryuk in 5 Hours', 18 October 2020, <https://thedfirreport.com/2020/10/18/ryuk-in-5-hours/>, accessed 16 November 2020; DFIR Report, 'NetWalker Ransomware in 1 Hour', 31 August 2020, <https://thedfirreport.com/2020/08/31/netwalker-ransomware-in-1-hour/>, accessed 16 November 2020; DFIR Report, 'Ryuk Speed Run, 2 Hours to Ransom', 5 November 2020, <https://thedfirreport.com/2020/11/05/ryuk-speed-run-2-hours-to-ransom/>, accessed 16 November 2020.

19. Paolo Passeri, 'Double Extortion Ransomware Attacks and the Role of Vulnerable Internet-Facing Systems', Info Security, 16 September 2020, <https://www.infosecurity-magazine.com/blogs/double-extortion-ransomware/>, accessed 16 November 2020.

20. Catalin Cimpanu, 'Conti (Ryuk) Joins the Ranks of Ransomware Gangs Operating Data Leak Sites', ZDNet, 25 August 2020, <https://www.zdnet.com/article/contiryuk-joins-the-ranks-of-ransomware-gangs-operating-data-leak-sites/>, accessed 16 November 2020; Cimpanu, 'Here's a List of All the Ransomware Gangs Who Will Steal and Leak Your Data If You Don't Pay'.

21. Dev Kundaliya, 'REvil Ransomware Gang Launches Auction Site to Sell Stolen Data', Computing, 3 June 2020, <https://www.computing.co.uk/news/4015981/revil-ransomware-gang-launches-auction-site-sell-stolen>, accessed 16 November 2020; Camille Singleton, 'Ransomware 2020: Attack Trends Affecting Organizations Worldwide', Security Intelligence, 28 September 2020, <https://securityintelligence.com/posts/ransomware-2020-attack-trends-newtechniques-affecting-organizations-worldwide/>, accessed 16 November 2020.

22. Ed Targett, 'Internal Data Stolen, Leaked, in REvil Attack on Electricity Market's Elexon', Computer Business Review, 1 June 2020, <https://www.cbronline.com/ news/elexon-hack-ransomware-revil>, accessed 16 November 2020; Scroxton, 'Software AG Caught in Double Extortion Ransomware Hit'.

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.

24. Teiss, 'Jack Daniel's Maker Brown-Forman Suffers REvil Ransomware Attack', 17 August 2020, <https://www.teiss.co.uk/brown-forman-revil-ransomwareattack/>, accessed 23 November 2020.

25. John Fokker and Christiaan Beek, 'McAfee ATR Analyzes Sodinokibi aka REvil Ransomware-as-a-Service – The All-Stars', McAfee, 2 October 2019, <https://www.mcafee.com/blogs/other-blogs/mcafee-labs/mcafee-atr-analyzessodinokibi-aka-revil-ransomware-as-a-service-the-all-stars/>, accessed 16 November 2020.

26. Singleton, 'Ransomware 2020'.

27. Crowdstrike, 'Double Trouble: Ransomware with Data Leak Extortion, Part 2', 6 October 2020, <https://www.crowdstrike.com/blog/double-troubleransomware-data-leak-extortion-part-2/>, accessed 16 November 2020.

continued on page 20

28. Lawrence Abrams, 'REvil Ransomware Deposits $1 Million in Hacker Recruitment Drive', Bleeping Computer, 28 September 2020, <https://www.bleepingcomputer.com/news/security/revil-ransomware-deposits-1-million-inhacker-recruitment-drive/>, accessed 16 November 2020.

29. Jack Stubbs, '"Payment Sent" – Travel Giant CWT Pays $4.5 Million Ransom to Cyber Criminals', Reuters, 31 July 2020.

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

31. Krebs on Security, 'Ransomware Group Turns to Facebook Ads', 10 November 2020, <https://krebsonsecurity.com/2020/11/ransomware-group-turns-to-facebookads/>, accessed 16 November 2020.

32. Renee Dudley, 'The Extortion Economy: How Insurance Companies Are Fueling a Rise in Ransomware Attacks', ProPublica, 27 August 2019, <https://www.propublica.org/article/the-extortion-economy-how-insurance-companies-arefueling-a-rise-in-ransomware-attacks>, accessed 16 November 2020; Danny Palmer, 'Ransomware: Cyber-Insurance Payouts are Adding to the Problem, Warn Security Experts', ZDNet, 17 September 2019, <https://www.zdnet.com/article/ransomware-cyber-insurance-payouts-are-adding-to-the-problem-warnsecurity-experts/>, accessed 16 November 2020.

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 Against Ransomware', <https://www.marsh.com/au/insights/research/cyberinsurance-supporting-fight-against-ransomware.html>, accessed 16 November 2020.

34. Graham Cluley, 'The Firms that Piggyback on Ransomware Attacks for Profit', 25 April 2018, <https://grahamcluley.com/firms-piggyback-ransomware-attacksprofit/>, accessed 16 November 2020.

35. Rob Wright, 'MSPs Scramble to Bolster Security Amid Ransomware Spike', Tech Target, 23 June 2020, <https://searchsecurity.techtarget.com/news/252485069/MSPs-scramble-to-bolster-security-amid-ransomware-spike>, accessed 16 November 2020.

36. Lena Connolly and David Wall, 'The Rise of Crypto-Ransomware in a Changing Cybercrime Landscape: Taxonomising Countermeasures, Computers and Security', Computers and Security (Vol. 87, November 2019).

37. Passeri, 'Double Extortion Ransomware Attacks and the Role of Vulnerable Internet-Facing Systems'.

38. Coveware, 'Ransomware Payments Up 33% As Maze and Sodinokibi Proliferate in Q1 2020', 29 April 2020, <https://www.coveware.com/blog/q1-2020-ransomware-marketplace-report>, accessed 16 November 2020; Catalin Cimpanu, 'Top Exploits Used by Ransomware Gangs Are VPN Bugs, But RDP Still Reigns Supreme', ZDNet, 24 August 2020, <https://www.zdnet.com/article/top-exploits-used-by-ransomware-gangs-are-vpn-bugs-but-rdp-still-reignssupreme/>, accessed 16 November 2020.

39. Victoria Kivilevich and Raveed Laeb, 'The Secret Life of an Initial Access Broker', Kela, 6 August 2020, <https://ke-la.com/the-secret-life-of-an-initial-accessbroker/>, accessed 16 November 2020.

40. Steve Ranger, 'Ransomware: Gangs Are Shifting Targets and Upping Their Ransom Demands', ZDNet, 2 October 2020, <https://www.zdnet.com/article/ransomware-gangs-are-shifting-targets-and-upping-their-ransom-demands/>, accessed 16 November 2020.

41. Data from BAE Systems Threat Intelligence.

42. National Cyber Security Centre (NCSC), 'Annual Review 2020', <https://www.ncsc.gov.uk/files/Annual-Review-2020.pdf>, accessed 16 November 2020.

43. Ionut Ilascu, 'REvil Ransomware Gang Claims Over $100 Million Profit in a Year', Bleeping Computer, 29 October 2020, <https://www.bleepingcomputer.com/news/security/revil-ransomware-gang-claims-over-100-million-profit-ina-year/>, accessed 16 November 2020; Ionut Ilascu, 'How Ryuk Ransomware Operators Made $34 Million From One Victim', Bleeping Computer, 7 November 2020, <https://www.bleepingcomputer.com/news/security/howryuk-ransomware-operators-made-34-million-from-one-victim/>, accessed 16 November 2020.

44. NCSC, 'Mitigating Malware and Ransomware Attacks', 11 September 2020, <https://www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomwareattacks/>, accessed 3 February 2021.

45. Europol, 'No More Ransom – Do You Need Help Unlocking Your Digital Life?', <https://www.europol.europa.eu/activities-services/public-awareness-andprevention-guides/no-more-ransom-do-you-need-help-unlocking-your-digital-life>, accessed 16 November 2020.

46. Josh Lake, 'What is RSA Encryption and How Does It Work?', Comparitech, 10 December 2018, <https://www.comparitech.com/blog/information-security/ rsa-encryption/>, accessed 1 February 2021.

47. RUSI, 'Cyber Attacks – What Actual Harm Do They Cause?', 18 September 2020, <https://rusi.org/event/cyber-attacks-%E2%80%93-what-actual-harm-do-theycause>, accessed 16 November 2020.

48. Mathew J Schwartz, 'Ransomware: Would Banning Ransom Payments Mitigate Threat?', Data Breach Today, 16 October 2020, <https://www.databreachtoday.com/blogs/ransomware-would-banning-ransom-payments-mitigatethreat-p-2956>, accessed 16 November 2020.

49. US Department of the Treasury, 'Treasury Sanctions Evil Corp'.

50. Davey Winder, 'Hackers Claim Trump Dirty Laundry Data Has Been Sold To "Interested Party"', Forbes, 18 May 2020.

51. US Department of the Treasury, 'Ransomware Advisory', press release, 1 October 2020, <https://home.treasury.gov/policy-issues/financial-sanctions/recent-actions/20201001>, accessed 16 November 2020; US Department of the Treasury, 'Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments'.

52. US Treasury Financial Crimes Enforcement Network, 'Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments', 1 October 2020, <https://www.fincen.gov/sites/default/files/advisory/2020-10-01/Advisory%20Ransomware%20FINAL%20508.pdf>, accessed 16 November 2020.

53. US Department of the Treasury, 'Ransomware Advisory', p. 1.

54. White House, 'Press Briefing on the Attribution of the WannaCry Malware Attack to North Korea', 19 December 2017, <https://kr.usembassy.gov/121917-pressbriefing-attribution-wannacry-malware-attack-north-korea/>, accessed 16 November 2020; HM Government, 'Foreign Office Minister Condemns Russia for NotPetya Attacks', 15 February 2018, <https://www.gov.uk/government/news/foreign-office-minister-condemns-russia-for-notpetya-attacks>, accessed 16 November 2020.

55. Ivan Kwiatkowski, Pierre Delcher and Felix Aime, 'Lazarus on the Hunt for Big Game', Securelist, 28 July 2020, <https://securelist.com/lazarus-on-the-huntfor-big-game/97757/>, accessed 16 November 2020; ClearSky Cybersecurity, 'Operation Quicksand: Muddy Water's Offensive Attack Against Israeli Organizations', October 2020, <https://www.clearskysec.com/wp-content/uploads/2020/10/Operation-Quicksand.pdf>, accessed 16 November 2020.

56. Renee Dudley and Jeff Kao, 'The Trade Secret: Firms That Promised High-Tech Ransomware Solutions Almost Always Just Pay the Hackers', ProPublica, 15 May 2019, <https://features.propublica.org/ransomware/ransomware-attack-datarecovery-firms-paying-hackers/>, accessed 16 November 2020.

57. Robin Pagnamenta, 'Daring $6m Cyber-Heist Could Be the Least of Travelex's Woes', The Telegraph, 9 January 2020.

58. Ibid.

59. Danny Palmer, 'Ransomware: Cyber-Insurance Payouts Are Adding to the Problem, Warn Security Experts', ZDNet, 17 September 2019, <https://www.zdnet.com/article/ransomware-cyber-insurance-payouts-are-adding-to-theproblem-warn-security-experts/>, accessed 16 November 2020.

60. Dan Sabbagh, 'Insurers "Funding Organised Crime" by Paying Ransomware Claims', The Guardian, 24 January 2021.

61. Liam M D Bailey, 'Mitigating Moral Hazard in Cyber-Risk Insurance', Journal of Law and Cyber Warfare (Vol. 3, No. 1, 2014), pp. 1–42.

62. Kai-Lung Hui, Wendy Wan-Yee Hui and Wei Thoo Yue, 'Cyber Insurance and Risk Management: A Normative Analysis', 14 November 2019, <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3486658>, accessed 10 September 2020.

63. For example, NIST, 'Cybersecurity Framework', <https://www.nist.gov/cyberframework>, accessed 9 February 2021; ISO, 'ISO/IEC 27001: Information Security Management', <https://www.iso.org/isoiec-27001-information-security.html>, accessed 9 February 2021; NCSC, 'Cyber Essentials: Overview', <https://www.ncsc.gov.uk/cyberessentials/overview>, accessed 9 February 2021.

64. For example, Marsh, 'Cyber Catalyst by Marsh', <https://www.marsh.com/us/campaigns/cyber-catalyst-by-marsh.html>, accessed 9 February 2021.

65. Daniel Woods et al., 'Mapping the Coverage of Security Controls in Cyber Insurance Proposal Forms', Journal of Internet Services and Applications (Vol. 8, 2017), p. 1.

66. See RUSI, 'Incentivising Cybersecurity Through Cyber Insurance', <https://rusi.org/projects/incentivising-cybersecurity-through-cyber-insurance>, accessed 16 November 2020; James Sullivan and Jason R C Nurse, 'Cyber Security Incentives and the Role of Cyber Insurance', RUSI Emerging Insights, December 2020.

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.

68. See NCSC, 'Penetration Testing', 8 August 2017, <https://www.ncsc.gov.uk/guidance/penetration-testing>, accessed 16 November 2020.

69. Europol, 'World's Most Dangerous Malware Emotet Disrupted Through Global Action', 27 January 2021, <https://www.europol.europa.eu/newsroom/news/world%E2%80%99s-most-dangerous-malware-emotet-disrupted-through-globalaction/>, accessed 3 February 2021.

70. Tom Burt, 'New Action to Combat Ransomware Ahead of U.S. Elections', Microsoft, 12 October 2020.

71. See Anton Moiseienko and Olivier Kraft, 'From Money Mules to Chain-Hopping: Targeting the Finances of Cybercrime', RUSI Occasional Papers (November 2019); US Treasury Financial Crimes Enforcement Network, 'Advisory on Ransomware'.

72. US Department of Justice, 'Department of Justice Launches Global Action Against NetWalker Ransomware', 27 January 2021, <https://www.justice.gov/opa/pr/department-justice-launches-global-action-against-netwalkerransomware/>, accessed 3 February 2021.

73. NCSC, 'Active Cyber Defence', <https://www.ncsc.gov.uk/section/productsservices/active-cyber-defence>, accessed 16 November 2020.

ROBAM, YOUR BEST CULINARY LIFESTYLE

Discover

the leading brand in household kitchen appliances, ROBAM.

Established in 1979, ROBAM Electric Appliances has specialised in manufacturing household kitchen appliances catered to the culinary conscious consumer for over 42 years. If cooking is more than a hobby and where you find your gastronomic happiness, your dream kitchen awaits!

From range hoods, domestic cooktops, disinfection cabinets, electric ovens, steam ovens, microwave ovens, dishwashers, and water purifers, ROBAM has decades of development under its hood. Boasting a long development history, high market share, large production scale, and the most comprehensive product categories - it's what makes them a strong choice when it comes to the perfect kitchen setup.

Their development and innovation of four decades have made ROBAM a widely recognised and leading brand all over the world. A little closer to home, ROBAM has been a leader in the Australian market for six years. Here in Brisbane, their one-stop experience space is one to explore. Based on 'culinary origin', ROBAM integrate modules of kitchen appliances, cooking products, and cooking classrooms to create your aspiring culinary lifestyle. Headquartered in China, ROBAM have nearly 100 of these Culinary Origin stores with the range hood and gas cooktop being the most popular appliance. It's no wonder; with the dual-core absorber 3.0 technology and three-dimensional extraction paired with a 360-degree spiral absorbing feature, they don't just add elegance and charm to the kitchen, but remove odours, irritants and grease expelled into the air seamlessly.

Kitchen is the heart of the home, and it's a sentiment ROBAM takes into their ethos every day. Devoted to continually improving people's cooking environment, ROBAM strives to not only become a leading culinary life reform but also inspire more families to enjoy the art of cooking daily. Come and see for yourself at their showroom in Underwood.

SHOP A1/15 LA1S ST UNDERWOOD

P 04 5680 3318 ROBAM.COM.AU

ROBAM
Enjoy Cooking

2021 Trends Show Increased Globalized Threat of Ransomware

CO-AUTHORED BY DEPARTMENT OF JUSTICE FEDERAL BUREAU OF INCESTIGATION, CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY, NATIONAL SECURITY AGENCY, AUSTRALIAN CYBER SECURITY CENTRE, NATIONAL CYBER SECURTY CENTRE (A PART OF GCHQ)

Summary

In 2021, cybersecurity authorities in the United States,[1,2,3] Australia,[4] and the United Kingdom[5] observed an increase in sophisticated, high-impact ransomware incidents against critical infrastructure organizations globally. The Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CISA), and the National Security Agency (NSA) observed incidents involving ransomware against 14 of the 16 U.S. critical infrastructure sectors, including the Defense Industrial Base, Emergency Services, Food and Agriculture, Government Facilities, and Information Technology Sectors. The Australian Cyber Security Centre (ACSC) observed continued ransomware targeting of Australian critical infrastructure entities, including in the Healthcare and Medical, Financial Services and Markets, Higher Education and Research, and Energy Sectors. The United Kingdom's National Cyber Security Centre (NCSC-UK) recognizes ransomware as the biggest cyber threat facing the United Kingdom. Education is one of the top UK sectors targeted by ransomware actors, but the NCSC-UK has also seen attacks targeting businesses, charities, the legal profession, and public services in the Local Government and Health Sectors.

Ransomware tactics and techniques continued to evolve in 2021, which demonstrates ransomware threat actors' growing technological sophistication and an increased ransomware threat to organizations globally.

This joint Cybersecurity Advisory—authored by cybersecurity authorities in the United States, Australia, and the United Kingdom—provides observed behaviors and trends as well as mitigation recommendations to help network defenders reduce their risk of compromise by ransomware.

Technical details

Cybersecurity authorities in the United States, Australia, and the United Kingdom observed the following behaviors and trends among cyber criminals in 2021:

- **Gaining access to networks via phishing, stolen Remote Desktop Protocols (RDP) credentials or brute force, and exploiting vulnerabilities.** Phishing emails, RDP exploitation, and exploitation of software vulnerabilities remained the top three initial infection vectors for ransomware incidents in 2021. Once a ransomware threat actor has gained code execution on a device or network access, they can deploy ransomware. **Note:** these infection vectors likely remain popular because of the increased use of remote work and schooling starting in 2020 and continuing through 2021. This increase expanded the remote attack surface and left network defenders struggling to keep pace with routine software patching.
- **Using cybercriminal services-for-hire.** The market for ransomware became increasingly "professional" in 2021, and the criminal business model of ransomware is now well established. In addition to their increased use of ransomware-as-a-service (RaaS), ransomware threat actors employed independent services to negotiate payments, assist victims with making payments, and arbitrate payment disputes between themselves and other cyber criminals. NCSC-UK observed that some ransomware threat actors offered their victims the services of a 24/7 help center to expedite ransom payment and restoration of encrypted systems or data.

Note: cybersecurity authorities in the United States, Australia, and the United Kingdom assess that if the ransomware criminal business model continues to yield financial returns for ransomware actors, ransomware incidents will become more frequent. Every time a ransom is paid, it confirms the viability and financial attractiveness of the ransomware criminal business model. Additionally, cybersecurity authorities in the United States, Australia, and the United Kingdom note that the criminal business model often complicates attribution because there are complex networks of developers, affiliates, and freelancers; it is often difficult to identify conclusively the actors behind a ransomware incident.

- **Update your operating system and software.**
- **Implement user training and phishing exercises to raise awareness about the risks of suspicious links and attachments.**
- **If you use Remote Desktop Protocol (RDP), secure and monitor it.**
- **Make an offline backup of your data.**
- **Use multifactor authentication (MFA).**

- **Sharing victim information.** Eurasian ransomware groups have shared victim information with each other, diversifying the threat to targeted organizations. For example, after announcing its shutdown, the BlackMatter ransomware group transferred its existing victims to infrastructure owned by another group, known as Lockbit 2.0. In October 2021, Conti ransomware actors began selling access to victims' networks, enabling follow-on attacks by other cyber threat actors.
- **Shifting away from "big-game" hunting in the United States.**
  - In the first half of 2021, cybersecurity authorities in the United States and Australia observed ransomware threat actors targeting "big game" organizations—i.e., perceived high-value organizations and/or those that provide critical services—in several high-profile incidents. These victims included Colonial Pipeline Company, JBS Foods, and Kaseya Limited. However, ransomware groups suffered disruptions from U.S. authorities in mid-2021. Subsequently, the FBI observed some ransomware threat actors redirecting ransomware efforts away from "big-game" and toward mid-sized victims to reduce scrutiny.
  - The ACSC observed ransomware continuing to target Australian organizations of all sizes, including critical services and "big game," throughout 2021.
  - NCSC-UK observed targeting of UK organizations of all sizes throughout the year, with some "big game" victims. Overall victims included businesses, charities, the legal profession, and public services in the Education, Local Government, and Health Sectors.
- **Diversifying approaches to extorting money.** After encrypting victim networks, ransomware threat actors increasingly used "triple extortion" by threatening to (1) publicly release stolen sensitive information, (2) disrupt the victim's internet access, and/or (3) inform the victim's partners, shareholders, or suppliers about the incident. The ACSC continued to observe "double extortion" incidents in which a threat actor uses a combination of encryption and data theft to pressure victims to pay ransom demands.

Ransomware groups have increased their impact by:

- **Targeting the cloud.** Ransomware developers targeted cloud infrastructures to exploit known vulnerabilities in cloud applications, virtual machine software, and virtual machine orchestration software. Ransomware threat actors also targeted cloud accounts, cloud application programming interfaces

continued on page 24

continued from page 23

(APIs), and data backup and storage systems to deny access to cloud resources and encrypt data. In addition to exploiting weaknesses to gain direct access, threat actors sometimes reach cloud storage systems by compromising local (on-premises) devices and moving laterally to the cloud systems. Ransomware threat actors have also targeted cloud service providers to encrypt large amounts of customer data.

- **Targeting managed service providers.** Ransomware threat actors have targeted managed service providers (MSPs). MSPs have widespread and trusted accesses into client organizations. By compromising an MSP, a ransomware threat actor could access multiple victims through one initial compromise. Cybersecurity authorities in the United States, Australia, and the United Kingdom assess there will be an increase in ransomware incidents where threat actors target MSPs to reach their clients.
- **Attacking industrial processes.** Although most ransomware incidents against critical infrastructure affect business information and technology systems, the FBI observed that several ransomware groups have developed code designed to stop critical infrastructure or industrial processes.
- **Attacking the software supply chain.** Globally, in 2021, ransomware threat actors targeted software supply chain entities to subsequently compromise and extort their customers. Targeting software supply chains allows ransomware threat actors to increase the scale of their attacks by accessing multiple victims through a single initial compromise.
- **Targeting organizations on holidays and weekends.** The FBI and CISA observed cybercriminals conducting increasingly impactful attacks against U.S. entities on holidays and weekends throughout 2021. Ransomware threat actors may view holidays and weekends—when offices are normally closed—as attractive timeframes, as there are fewer network defenders and IT support personnel at victim organizations. For more information, see joint FBI-CISA Cybersecurity Advisory, Ransomware Awareness for Holidays and Weekends.

Mitigations

Cybersecurity authorities in the United States, Australia, and the United Kingdom recommend network defenders apply the following mitigations to reduce the likelihood and impact of ransomware incidents:

- **Keep all operating systems and software up to date.** Timely patching is one of the most efficient and cost-effective steps an organization can take to minimize its exposure to cybersecurity threats. Regularly check for software updates and end of life (EOL) notifications, and prioritize patching known exploited vulnerabilities. In cloud environments, ensure that virtual machines, serverless applications, and third-party libraries are also patched regularly, as doing so is usually the customer's responsibility. Automate software security scanning and testing when possible. Consider upgrading hardware and software, as necessary, to take advantage of vendor-provided virtualization and security capabilities.
- **If you use RDP or other potentially risky services, secure and monitor them closely.**
  - Limit access to resources over internal networks, especially by restricting RDP and using virtual desktop infrastructure. After assessing risks, if RDP is deemed operationally necessary, restrict the originating sources and require MFA to mitigate credential theft and reuse. If RDP must be available externally, use a virtual private network (VPN), virtual desktop infrastructure, or other means to authenticate and secure the connection before allowing RDP to connect to internal devices. Monitor remote access/RDP logs, enforce account lockouts after a specified number of attempts to block brute force campaigns, log RDP login attempts, and disable unused remote access/RDP ports.
  - Ensure devices are properly configured and that security features are enabled. Disable ports and protocols that are not being used for a business purpose (e.g., RDP Transmission Control Protocol Port 3389).
  - Restrict Server Message Block (SMB) Protocol within the network to only access servers that are necessary, and remove or disable outdated versions of SMB (i.e., SMB version 1). Threat actors use SMB to propagate malware across organizations.
  - Review the security posture of third-party vendors and those interconnected with your organization. Ensure all connections between third-party vendors and outside software or hardware are monitored and reviewed for suspicious activity.
  - Implement listing policies for applications and remote access that only allow systems to execute known and permitted programs under an established security policy.
  - Open document readers in protected viewing modes to help prevent active content from running.
- **Implement a user training program and phishing exercises** to raise awareness among users about the risks of visiting suspicious websites, clicking on suspicious links, and opening suspicious attachments. Reinforce the appropriate user response to phishing and spearphishing emails.
- **Require MFA** for as many services as possible—particularly for webmail, VPNs, accounts that access critical systems, and privileged accounts that manage backups.
- **Require all accounts with password logins (e.g., service account, admin accounts, and domain admin accounts) to have strong, unique passwords.** Passwords should not be reused across multiple accounts or stored on the system where an adversary may have access. **Note:** devices with local admin accounts should implement a password policy, possibly using a password management solution (e.g., Local

Administrator Password Solution [LAPS]), that requires strong, unique passwords for each admin account.

- **If using Linux, use a Linux security module (such as SELinux, AppArmor, or SecComp) for defense in depth.** The security modules may prevent the operating system from making arbitrary connections, which is an effective mitigation strategy against ransomware, as well as against remote code execution (RCE).
- **Protect cloud storage by backing up to multiple locations, requiring MFA for access, and encrypting data in the cloud.** If using cloud-based key management for encryption, ensure that storage and key administration roles are separated.

Malicious cyber actors use system and network discovery techniques for network and system visibility and mapping.

To limit an adversary's ability to learn an organization's enterprise environment and to move laterally, take the following actions:

- **Segment networks.** Network segmentation can help prevent the spread of ransomware by controlling traffic flows between—and access to—various subnetworks and by restricting adversary lateral movement. Organizations with an international footprint should be aware that connectivity between their overseas arms can expand their threat surface; these organizations should implement network segmentation between international divisions where appropriate. For example, the ACSC has observed ransomware and data theft incidents in which Australian divisions of multinational companies were impacted by ransomware incidents affecting assets maintained and hosted by offshore divisions (outside their control).
- **Implement end-to-end encryption.** Deploying mutual Transport Layer Security (mTLS) can prevent eavesdropping on communications, which, in turn, can prevent cyber threat actors from gaining insights needed to advance a ransomware attack.
- **Identify, detect, and investigate abnormal activity and potential traversal of the indicated ransomware with a network-monitoring tool.** To aid in detecting the ransomware, leverage a tool that logs and reports all network traffic, including lateral movement on a network. Endpoint detection and response tools are particularly useful for detecting lateral connections as they have insight into unusual network connections for each host. Artificial intelligence (AI)-enabled network intrusion detection systems (NIDS) are also able to detect and block many anomalous behaviors associated with early stages of ransomware deployment.
- **Document external remote connections.** Organizations should document approved solutions for remote management and maintenance. If an unapproved solution is installed on a workstation, the organization should investigate it immediately. These solutions have legitimate purposes, so they will not be flagged by antivirus vendors.
- **Implement time-based access for privileged accounts.** For example, the just-in-time access method provisions privileged access when needed and can support enforcement of the principle of least privilege (as well as the zero trust model) by setting network-wide policy to automatically disable admin accounts at the Active Directory level. As needed, individual users can submit requests through an automated process that enables access to a system for a set timeframe. In cloud environments, just-in-time elevation is also appropriate and may be implemented using per-session federated claims or privileged access management tools.
- **Enforce principle of least privilege through authorization policies.** Minimize unnecessary privileges for identities. Consider privileges assigned to human identities as well as non-person (e.g., software) identities. In cloud environments, non-person identities (service accounts or roles) with excessive privileges are a key vector for lateral movement and data access. Account privileges should be clearly defined, narrowly scoped, and regularly audited against usage patterns.
- **Reduce credential exposure.** Accounts and their credentials present on hosts can enable further compromise of a network. Enforcing credential protection—by restricting where accounts and credentials can be used and by using local device credential protection features—reduces opportunities for threat actors to collect credentials for lateral movement and privilege escalation.
- **Disable unneeded command-line utilities; constrain scripting activities and permissions, and monitor their usage.** Privilege escalation and lateral movement often depend on software utilities that run from the command line. If threat actors are not able to run these tools, they will have difficulty escalating privileges and/or moving laterally. Organizations should also disable macros sent from external sources via Group Policy.
- **Maintain offline (i.e., physically disconnected) backups of data, and regularly test backup and restoration.** These practices safeguard an organization's continuity of operations or at least minimize potential downtime from an attack as well as protect against data losses. In cloud environments, consider leveraging native cloud service provider backup and restoration capabilities. To further secure cloud backups, consider separation of account roles to prevent an account that manages the backups from being used to deny or degrade the backups should the account become compromised.
- **Ensure all backup data is encrypted,** immutable (i.e., cannot be altered or deleted), and covers the entire organization's data infrastructure. Consider storing encryption keys outside the cloud. Cloud backups that are encrypted using a cloud key management service (KMS) could be affected should the cloud environment become compromised.
- **Collect telemetry from cloud environments.** Ensure that telemetry from cloud environments—including network telemetry (e.g., virtual private cloud [VPC] flow logs), identity telemetry (e.g., account sign-on, token usage, federation configuration changes), and application telemetry (e.g., file downloads, cross-organization sharing)—is retained and visible to the security team.

continued on page 26

continued from page 25

Note: critical infrastructure organizations with industrial control systems/operational technology networks should review joint CISA-FBI Cybersecurity Advisory DarkSide Ransomware: Best Practices for Preventing Business Disruption from Ransomware Attacks for more recommendations, including mitigations to reduce the risk of severe business or functional degradation should their entity fall victim to ransomware.

Responding to ransomware attacks

If a ransomware incident occurs at your organization, cybersecurity authorities in the United States, Australia, and the United Kingdom recommend organizations:

- **Follow the Ransomware Response Checklist** on p. 11 of the CISA-Multi-State Information Sharing and Analysis Center (MS-ISAC) Joint Ransomware Guide.
- **Scan backups**. If possible, scan backup data with an antivirus program to check that it is free of malware. This should be performed using an isolated, trusted system to avoid exposing backups to potential compromise.
- **Report incidents** to respective cybersecurity authorities:
  - **U.S. organizations** should report incidents immediately to the FBI at a local FBI Field Office, CISA at us-cert.cisa.gov/report, or the U.S. Secret Service at a U.S. Secret Service Field Office.
  - **Australian organizations** should report incidents to the ASD's ACSC via cyber.gov.au or call 1300 292 371 (1300 CYBER 1).
  - **UK organizations** should report incidents to NCSC-UK via report.ncsc.gov.uk and/or Action Fraud, the United Kingdom's fraud and cyber reporting centre, via actionfraud.police.uk.
- **Apply incident response best practices** found in the joint Cybersecurity Advisory, Technical Approaches to Uncovering and Remediating Malicious Activity, developed by CISA and the cybersecurity authorities of Australia, Canada, New Zealand, and the United Kingdom.

Note: cybersecurity authorities in the United States, Australia, and the United Kingdom strongly discourage paying a ransom to criminal actors. Criminal activity is motivated by financial gain, so paying a ransom may embolden adversaries to target additional organizations (or re-target the same organization) or encourage cyber criminals to engage in the distribution of ransomware. Paying the ransom also does not guarantee that a victim's files will be recovered. Additionally, reducing the financial gain of ransomware threat actors will help disrupt the ransomware criminal business model.

Additionally, NCSC-UK reminds UK organizations that paying criminals is not condoned by the UK Government. In instances where a ransom paid, victim organizations often cease engagement with authorities, who then lose visibility of the payments made. While it continues to prove challenging, the NCSC-UK has supported UK Government efforts by identifying needed policy changes—including measures about the cyber insurance industry and ransom payments—that could reduce the threat of ransomware.

Resources

- For more information and resources on protecting against and responding to ransomware, refer to StopRansomware.gov, a centralized, U.S. whole-of-government webpage providing ransomware resources and alerts.
- CISA's Ransomware Readiness Assessment is a no-cost self-assessment based on a tiered set of practices to help organizations better assess how well they are equipped to defend and recover from a ransomware incident.
- CISA offers a range of no-cost cyber hygiene services to help critical infrastructure organizations assess, identify, and reduce their exposure to threats, including ransomware. By requesting these services, organizations of any size could find ways to reduce their risk and mitigate attack vectors.
- The U.S. Department of State's Rewards for Justice (RFJ) program offers a reward of up to
- $10 million for reports of foreign government malicious activity against U.S. critical infrastructure. See the RFJ website for more information and how to report information securely.
- The ACSC recommends organizations implement eight essential mitigation strategies from the ACSC's Strategies to Mitigate Cyber Security Incidents as a cybersecurity baseline. These strategies, known as the "Essential Eight," make it much harder for adversaries to compromise systems.
- Refer to the ACSC's practical guides on how to protect yourself against ransomware attacks and what to do if you are held to ransom at cyber.gov.au.
- Refer to NCSC-UK's guides on how to protect yourself against ransomware attacks and how to respond to and recover from them at ncsc.gov.uk/ransomware/home.

References

1. United States Federal Bureau of Investigation
2. United States Cybersecurity and Infrastructure Security Agency
3. United States National Security Agency
4. Australian Cyber Security Centre
5. United Kingdom National Cyber Security Centre

Disclaimer

U.S. organizations: to report suspicious or criminal activity related to information found in this Joint Cybersecurity Advisory, contact your local FBI field office at fbi.gov/contact-us/field, or the FBI's 24/7 Cyber Watch (CyWatch) at (855) 292-3937 or by e-mail at CyWatch@fbi.gov. When available, please include the following information regarding the incident: date, time, and location of the incident; type of activity; number of people affected; type of equipment used for the activity; the name of the submitting company or organization; and a designated point of contact. To request incident response resources or technical assistance related to these threats, contact CISA at CISAServiceDesk@cisa.dhs.gov. For NSA client requirements or general cybersecurity inquiries, contact the Cybersecurity Requirements Center at 410-854-4200 or Cybersecurity_Requests@nsa.gov. Australian organizations should report incidents to the Australian Signals Directorate's (ASD's) ACSC via cyber.gov.au or call 1300 292 371 (1300 CYBER 1). U.K. organizations should report a significant cyber security incident: ncsc.gov.uk/report-an-incident (monitored 24 hrs) or for urgent assistance, call 03000 200 973.

This document is marked TLP:WHITE. Disclosure is not limited. Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction. For more information on the Traffic Light Protocol, see cisa.gov/tlp/.

Exfiltrate, encrypt, extort

The global rise of ransomware and Australia's policy options.

July 2021

RACHAEL FALK AND ANNE-LOUISE BROWN

What's the problem?

As the Covid-19 pandemic has swept across the world, another less visible epidemic has occurred concurrently—a tsunami of cybercrime producing global losses totalling more than US$1 trillion.[1] While cybercrime is huge in scale and diverse in form, there's one type that presents a unique threat to businesses and governments the world over: ransomware.

Some of the most spectacular ransomware attacks have occurred offshore, but Australia hasn't been immune. Over the past 18 months, major logistics company Toll Holdings Ltd has been hit twice; Nine Entertainment was brought to its knees by an attack that left the company struggling to televise news bulletins and produce newspapers; multiple health and aged-care providers across the country have been hit; and global meat supplies were affected after the Australian and international operations of the world's largest meat producer, JBS Foods, were brought to a standstill. It's likely that other organisations have also been hit but have kept it out of the public spotlight.

A current policy vacuum makes Australia an attractive market for these attacks, and ransomware is a problem that will only get worse unless a concerted and strategic domestic effort to thwart the attacks is developed. Developing a strategy now is essential. Not only are Australian organisations viewed as lucrative targets due to their often low cybersecurity posture, but they're also seen as soft targets. The number of attacks will continue to grow unless urgent action is taken to reduce the incentives to target Australian companies and other entities.

What's the solution?

All governments, civil society groups and businesses—large and small—need to know how to manage and mitigate the risk of ransomware, but organisations can't deal with the attacks on their own. Given the significant—and increasing—threat ransomware presents to Australia, new policy measures are fundamental to dealing with this challenge. While there's no doubt ransomware is difficult to tackle using traditional law enforcement methods because the criminal actors involved are usually located offshore, there are domestic policy levers that can be pulled, for example, to support cybersecurity uplift measures across the economy. Such action is essential because the grim reality is that, when it comes to ransomware, prevention is the best response.

This policy report addresses key areas in Australia where new policies and strategies and improved guidance are needed and also where better support for cybersecurity uplift can be achieved.

Our recommendations include arguments for greater clarity about the legality of ransomware payments, increased transparency when attacks do occur, the adoption of a mandatory reporting regime, expanding the official alert system of the Australian Cyber Security Centre (ACSC), focused education programs to improve the public's and the business community's understanding and, finally, incentivising cybersecurity uplift measures through tax, procurement and subsidy measures. We also recommend the establishment of a dedicated cross-departmental ransomware taskforce, which would include state and territory representatives, that would share threat intelligence and develop federal-level policy proposals to tackle ransomware nationally.

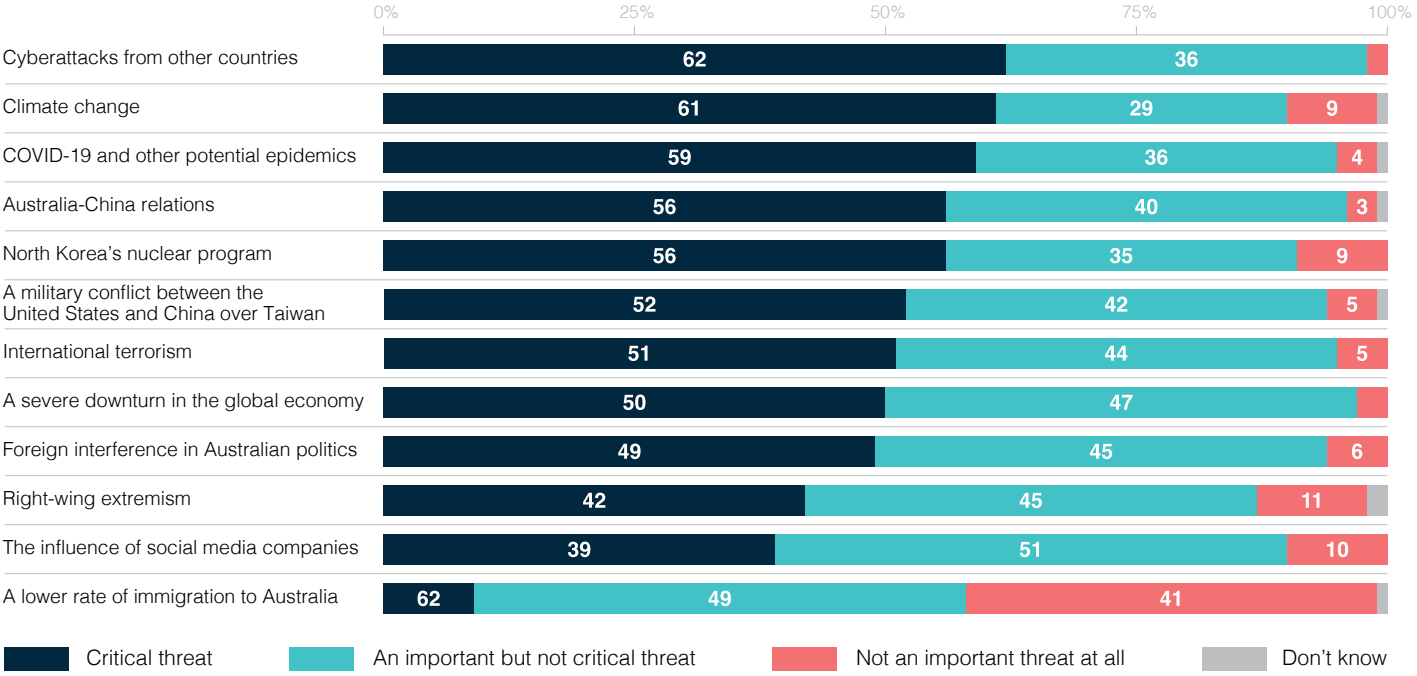
Introduction: What's ransomware?

Ransomware is a form of malware designed and deployed by state and non-state cybercriminals who seek out vulnerabilities in the computer systems of organisations, both large and small, locking up, encrypting and extracting data, and rendering computers and their files unusable.[2] Attacks are accompanied by a demand for ransom to be paid in return for decrypting and unlocking systems.

Increasingly, ransomware attacks include an extortion element that usually involves threats to leak stolen data publicly or on the dark web if payment isn't made (known as 'hack and leak') to exert pressure on the victim to pay the ransom.

continued on page 30

Figure 1: Threats to Australia's vital interests



Source: Lowy Institute Poll 2021.

continued from page 29

Furthermore, payments can be difficult to trace because they're generally made using cryptocurrency.[3] This also makes it hard—but not impossible (as we saw with the Colonial Pipeline attack)—to investigate and prosecute the criminals responsible for ransomware attacks. Generally, those criminals operate with impunity in extraterritorial jurisdictions (most notably Russian threat actors) where governments protect or tolerate them or don't have the legal systems, frameworks or capabilities in place to prosecute them.[4]

Ransomware is a form of cybercrime that's both scalable and able to be commoditised. It can be bought as a service, generally on the dark web, where ransomware criminals essentially act as 'guns for hire'. In 2020, a US analysis found buying malware online was 'incredibly easy', and that advanced malware tools sell for as little as US$50.[5] The analysis also found that 'almost all premium malware sellers provide buyers with in-depth tutorials and ideas about using their products for technically unskilled buyers.'[6]

The most common way ransomware is deployed into a system is via email phishing campaigns, remote access vulnerabilities and software vulnerabilities.[7] In the case of phishing, a criminal sends an email containing a malicious file or link that deploys malware when it's clicked. Phishing campaigns continue to evolve and are becoming increasingly sophisticated and targeted. Remote access vulnerabilities, such as weak username and password combinations, allow criminals access to and control of the computer remotely. Cybercriminals exploit such vulnerabilities via sustained attacks or by obtaining user credentials, which are often purchased on the dark web, enabling the deployment of malware onto a system.[8] Finally, cybercriminals leverage security weaknesses in popular software programs to gain control of systems and deploy ransomware.[9]

It's important to note that ransomware attacks are entirely foreseeable and almost always defendable. In the physical world, organisations pay for security alarms, high fences and sensors to protect their property. And the digital world should be no different. Ransomware is simply another crime type and the threat should be viewed as another organisational risk because, behind every ransomware attack, are cybercriminals who have watched their victim's network, laying the ground for encryption and data theft to hold the victim to ransom.

The domestic landscape

In 2019–20, the ACSC reported an increase in the number of ransomware attacks on Australian organisations, although specific metrics weren't released.[10] According to the ACSC, the top five sectors to *report* ransomware incidents during that period were health; state and territory governments; education and research; and transport and retail.[11] It's worth noting that the health sector was disproportionately affected, in line with global trends,[12] reflecting its attractiveness as a target due to the value of the troves of personal health data stored and, most importantly, the criticality of the services provided. Put simply, a ransom is more likely to be paid if human life is endangered.

It should be noted that transnational cyberattacks are a serious concern for Australians. The recently published results of the 2021 Lowy Institute Poll reported that 98% of the poll's nationally representative sample viewed 'cyber attacks from other countries' as a critical (62%) or important (36%) threat to Australia over the next decade.[13] That makes transnational cyberattacks the highest of the 12 threats to Australia's vital interests that the Lowy Institute asked people about, rating higher than climate change, Covid-19 and other potential epidemics, international terrorism, a severe downturn in the global economy and Australia–China relations.

Major reported ransomware attacks in Australia in 2020 and 2021

Major attacks on Australian targets in 2020 and so far in 2021 included the following:

- **February and May 2020: Toll Holdings**
  Employee and commercially sensitive data was stolen in two separate ransomware attacks on Toll Holdings, which is an Australian logistics giant.[14] Some of the stolen data was leaked on the dark web.[15] It's understood that Toll didn't pay either ransom.[16] As a result of the attack, the company has undertaken substantial remediation and cybersecurity uplift programs.[17]
- **May 2020: BlueScope Steel**
  A ransomware attack on a US-based system of BlueScope Steel had global ramifications, affecting production at the organisation's Port Kembla facility in Australia.[18] Details of the attack, including whether payment was made, were undisclosed.
- **June 2020 (two attacks): Lion Dairy and Drinks**
  Dairy processor and drink manufacturer Lion was forced to shut down production as a result of two separate ransomware attacks, which had significant impacts on its vast domestic supply chain.[19] Sensitive data was stolen in the attacks, and the criminals responsible threatened to publish it on the dark web.[20] It's unknown whether a ransom was paid.
- **December 2020: Law in Order**
  Law in Order provides document-management services to the legal profession and purports to have 'iron-clad security'.[21] The criminals who attacked it threatened to publish stolen data on the dark web.[22] It's unknown whether a ransom payment was made.
- **March 2021: Nine Entertainment**
  In late March, Nine Entertainment's news and newspaper production were severely damaged by a ransomware attack.[23] As a result, news teams were forced to work remotely, and most production had to be done out of Nine's Melbourne office, which was the least affected. It took weeks for production to return to normal.[24] It's unknown whether the ransom was paid.
- **March 2021: Eastern Health**
  Eastern Health, which operates several hospitals in Melbourne, was brought to a halt by a ransomware attack that resulted in multiple surgery cancellations and prevented access to patient medical records, internal emails and IT systems.[25] Systems were reportedly damaged for weeks. It's unknown whether a ransom was paid.
- **April 2021: Uniting Care Qld**
  Uniting Care Qld, which operates several hospitals and disability and aged-care facilities across the state, had its access to internal IT systems and patient records severely compromised in a ransomware attack attributed to the REvil group.[26] It's unknown whether a ransom was paid.
- **June 2021: JBS Foods**
  JBS Foods, the world's largest meat supplier, had its global production brought to a standstill by a ransomware attack affecting 47 facilities in Australia.[27] The company confirmed that it paid US$11 million to the attackers.[28]

Do Australians understand what ransomware is?

In a bid to better gauge the public's understanding of what ransomware is, what it does and what to do in the event of an attack, the Cyber Security Cooperative Research Centre conducted a nationally representative online survey of 1,000 Australian adults in April 2021 on 'Understanding ransomware'. The results—though not unexpected—painted an alarming picture of just how little the Australian public understands ransomware.

Twenty-five per cent of respondents said ransomware was the most significant cybersecurity threat to Australian businesses, coming in behind hacking (48%). Seventy-seven per cent said they wouldn't know what to do if they fell victim to a ransomware attack but, when given a set of options, 56% said they would contact the ACSC. Of the respondents, 42% said they understood how a ransomware attack occurred, and 44% indicated that they knew what happened in a ransomware attack. Respondents believed financial gain was the key aim of an attack (71%), followed by data theft (14%).

While this survey wasn't exhaustive, it clearly shows that the community, generally, has little understanding of ransomware, illustrating that a more concerted effort to educate Australians about it is required. That effort should be teamed with effective tools and policies to mitigate the risk of falling victim to a ransomware attack.

Ransomware payments and regulating cryptocurrency

Cryptocurrencies are the preferred channel of payment for ransomware attacks because of the assumed untraceability of those payments. However, successful steps are being taken to crack down on cryptocurrency providers via law enforcement and recovery action. In the US, steps have been taken to regulate the use of cryptocurrencies more tightly and to recoup stolen funds; for example, US$2.3 million was recovered after the Colonial Pipeline ransomware attack.[29]

The US Treasury announced in May 2021 that, under a proposed reporting regime, cryptocurrency transfers of more than $10,000 would have to be reported to the Internal Revenue Service—a step that could help to improve the effectiveness of

continued on page 32

continued from page 31

cryptocurrency tracking.[30] There's also a move in the US towards KYC ('know your customer') and AML (anti-money-laundering) cryptocurrency regulation. KYC policies govern the types of information banks must collect, and retain, about their customers; AML regulations require financial institutions to monitor the use of funds by their customers.[31]

In 2018, new laws came into force in Australia making it compulsory for digital currency exchange providers operating in Australia to register with AUSTRAC and comply with reporting obligations under the Anti-Money Laundering and Counter-Terrorism Financing Act 2006.[32] Under those laws, exchanges are required to collect information to establish a customer's identity, monitor transaction activity and report transactions or activity that's suspicious or involves amounts of cash over $10,000.[33]

The legality of ransomware payment in Australia

When a ransomware attack occurs, any payment made has legal implications, but in Australia the legality of such a payment is murky at best. This is an issue that needs to be addressed with haste, without the burden of bureaucratic process and a regulatory quagmire. Importantly, criminalising ransomware payment isn't the solution. Mandatory reporting of ransomware attacks, however, should be considered.

The ACSC's advice on payment is clear: don't pay.[34] At first blush, that appears to be straightforward, but any organisation faced with a ransomware attack (in which often every minute matters) grapples with the legal consequences of paying or not paying. This is a highly nuanced issue and one that other nations are also grappling with.

While the payment of a ransom should always be a last resort, criminalisation wouldn't incapacitate the real offenders; nor would it bring restitution to victims. In fact, it would have the effect of further victimising the victim. There are also ethical considerations that need to be taken into account, the central one being the notion that criminalisation could punish organisations for taking proportionate action to protect stakeholders and the community more broadly. This is especially relevant in relation to critical infrastructure entities.

In the Australian context, the Criminal Code Act's 'instrument of crime' provisions are broad. It's an offence to 'deal with' money or other property if there's a risk that the money or property will become an instrument of crime or if the payer is 'reckless' or 'negligent' about the fact that the money or property will become an instrument of crime.[35] The Criminal Code also includes terrorism funding offences, which make it illegal to intentionally 'make funds available to a [terrorist] organisation' if the funder either knows that the organisation is a terrorist organisation or is reckless about whether the organisation is a terrorist organisation.[36]

Australia is also bound by UN sanctions laws and, under the Charter of the United Nations Act 1945 (which implements UN Security Council sanctions), it's an offence to transfer assets to sanctioned people and entities or to contravene UN sanctions enforcement laws.[37] Currently, no ransomware actors are explicitly listed on the UN's sanctions list; however, sanctions laws could apply in relation to sanctioned states or to groups acting on behalf of sanctioned entities.[38]

The most commonly cited potential defence against a charge of making an 'illegal' ransomware payment is duress. A duress defence can be used if a person 'reasonably believes' that a threat made will be carried out unless an offence of ransom payment is committed, there's no reasonable way the threat can be rendered ineffective, and the conduct or payment is a reasonable response to the threat.[39] Such a defence would depend on the particular circumstances facing an organisation and its payment of a ransom.

In the US, where the Federal Bureau of Investigation (FBI) reported 2,474 ransomware incidents in 2020, ransom payment isn't illegal.[40] However, a ransomware advisory published by the US Treasury Department in October 2020 highlighted the possibility of sanction breaches that could be associated with ransomware payments to malicious cyber actors.[41] The advisory contains a list of malicious cyber actors sanctioned by the department's Office of Foreign Assets Control, signalling that ransom payments to such actors could be met with civil penalties. Of note, however, is the recognition that 'a company's self-initiated, timely, and complete report of a ransomware attack to law enforcement [will be] a significant mitigating factor in determining an appropriate enforcement outcome if the situation is later determined to have a sanctions nexus'.[42] On this point, a 2019 FBI ransomware alert highlighted the need for ransomware attacks to be reported, regardless of whether money is exchanged.[43] Interestingly, the alert highlights the challenges that affected organisations face—and a possible reticence to prosecute for payment—by stating 'the FBI understands that when businesses are faced with an inability to function, executives will evaluate all options to protect their shareholders, employees, and customers'.[44]

Given that the measures outlined in the Treasury advisory have, to date, not been applied, and the clear focus on reporting and transparency, it could be reasonably concluded in the US that there's little appetite for penalising organisations for paying ransoms. Such a model could be employed in Australia, fostering an information-sharing culture without fear of legal consequences for organisations that pay ransoms. There's also merit in the US approach of publishing a list of known malicious ransomware actors. While that wouldn't remediate the problem, it would serve to better inform organisations about cyber threat actors.

A mandatory reporting regime could take the form of a legal obligation for an organisation to report the nature and root cause of a ransomware attack to the ACSC within a prescribed time frame (for example, within 21 days). That would be in addition to real-time reporting of a cyber incident. Furthermore, this should occur regardless of whether payment is made and ensure the confidentiality of victims. It wouldn't be about naming and shaming. Rather, by compelling victimised organisations to report under law, the ACSC would have improved access to vital and timely intelligence, assisting root-cause analysis and the identification of other attack vectors. Ultimately, when published, this would help better inform other stakeholders on how to reduce vulnerabilities. It would also enhance the operation of the federal government's proposed changes to the *Security of Critical Infrastructure Act 2018*.[45]

It's worth noting recent steps that the European Commission has taken

'to tackle the rising number of serious cyber incidents', announcing on 23 June that it will build a 'Joint Cyber Unit'.[46] The aim of the unit is to provide a coordinated response to 'large-scale' cyber incidents and assist in recovery, operating at both the operational and technical levels.[47] It will involve key stakeholders from law enforcement, security, defence and diplomacy.[48] Its functions will be enhanced by a new US–EU working group, which has been established specifically to address the ransomware threat.[49]

The joint EU and US approach demonstrates that, while Australia can take significant steps to address ransomware domestically by clarifying our law, there's a vital need to work closely with allies and like-minded nations to tackle the threat globally. Longer term, sustained intelligence sharing and the adoption of responsibilities flowing from the agreed UN norms of responsible state behaviour in cyberspace will help achieve international consensus on tackling ransomware.[50] In April, to that end, the Five Eyes nations committed to tackling the growing threat of ransomware, specifically addressing the issue in the Five Country Ministerial Statement Regarding the Threat of Ransomware.[51]

What about cyber insurance?

While still relatively immature, Australia's cyber insurance market has expanded. Cyber insurance policies can be expensive, given the nature of the threat, and broad in scope, covering recovery, replacement and regulatory costs associated with a ransomware attack. Of concern, however, are policies that cover ransom costs, which could serve to encourage attacks targeted at insured entities.[52] There are also concerns that ransomware criminals might access systems in search of insurance certificates and then demand ransom payment of the specific amount covered by an insurer.[53] While there is a role for cyber insurance to play as part of an organisation's holistic cyber security strategy, it is not a silver bullet, and it can have unintended consequences. As noted above, a key risk is the targeting of insured organisations by threat actors. There is also the potential for organisations with cyber insurance to be lax in their approach to managing cyber security. As noted in the Harvard Business Review: "Insurance is important, but it's likely to take a back seat to the broader cyber security discussion...Insurance helps you recover from a situation, filling in the gaps when problems occur that you can't prevent, but attempts to prevent problems are still crucial".

Where do we go from here?

To better protect Australians and their businesses against ransomware, we believe that the three key words are transparency, education and incentivisation.

Increased transparency is vital

As it stands, there's a dearth of official public data relating to ransomware attacks in Australia. For example, and as noted above, in the 2019–20 financial year the ACSC reported an increase in the number of domestic ransomware attacks, but no specific metrics were released.[54] This is in stark contrast to the US, which has a much more transparent reporting system. The FBI publicly reported that it recorded 2,474 ransomware incidents in 2020, amounting to US$29.1 million in economic loss[55] (and that's likely to be a significant understatement of the overall incidence of ransomware attacks because reporting is voluntary).

While it's understandable that the specifics of attacks and victims aren't released into the public domain, if more insight were provided into the prevalence and root causes of ransomware crimes in Australia there would be greater onus on organisations to harden their systems against attack (especially known vulnerabilities). Furthermore, by building a public narrative on the threat landscape and threat actors, policymakers, organisations and the community more broadly would be better informed about the scale of the attacks. This would have a two-pronged effect—encouraging cybersecurity uplift across the economy and enhancing trust in government, especially in the light of the heightened reporting obligations touted for critical infrastructure entities.[56]

In April this year, the US Department of Justice established a dedicated ransomware taskforce.

A memo from Acting Deputy Attorney General John Carlin stated that 2020 had been 'the worst year' in history for ransomware and cyber extortion. He signalled that steps would be taken to deal with the root causes of ransomware, which could include actions ranging from 'takedowns of servers used to spread ransomware to seizures of these criminal enterprises' ill-gotten gains'.[57]

The US Government's Cybersecurity and Infrastructure Security Agency (CISA) also provides regular ransomware alerts and tips to the public,[58] which go into significant detail regarding the latest ransomware attacks, the systemic weaknesses that were exploited to gain access for malware to be deployed and steps organisations can take to mitigate those risks. The CISA played a pivotal role in disseminating real-time information about the Colonial Pipeline ransomware attack in May 2021,[59] which brought the major provider of fuel to the US east coast to a grinding halt.[60] The CISA kept the community and critical infrastructure entities informed during what was arguably the most serious ransomware attack the US has seen, ultimately assisting other organisations to be on guard.[61]

The US approach illustrates how comprehensive and more transparent official reporting of ransom ware attacks

continued on page 34

continued from page 33

could be used to enhance preparedness for an attack and people's understanding of the threat environment. While the ACSC does provide high-level threat intelligence to organisations, there's a requirement for those organisations to register and be accepted into the ACSC Partnership Program. In addition, the alerts and advice are quite technical, which could make them inaccessible to some organisations, especially small and medium-sized enterprises (SMEs). Hence, there's a need to build on the existing regime, with a view to enhancing transparency across the entire economy and community via public alerts and advice when ransomware attacks occur.

Education is necessary to improve knowledge and mitigate risk

While increased transparency is vital, it's of little use if organisations don't understand what ransomware is, what needs to be done to mitigate risk and haven't implemented appropriate cybersecurity controls. Many ransomware attacks would be avoidable if effective organisational cybersecurity controls were in place and good cyber hygiene was practised. Ransomware is different from most other tools used by criminals in that it can have far-reaching consequences. The threat it poses through its ability to cripple critical infrastructure makes it all the more serious. Hence, there needs to be greater focus on the basics—a concerted education campaign that explains what ransomware is, what it does and how organisations can bolster their defences.

Top of the list must be patching. Patch management is essential for effective cybersecurity and ensures that the security features of software on computers and devices are up to date. All software is prone to technical vulnerabilities and, when a vulnerability is exposed and shared, cybercriminals have a metaphorical front-door key. A 2019 report by the Ponemon Institute on vulnerability responses found that, of the 48% of organisations that had experienced data breaches in the preceding year, 60% reported that the breaches resulted from failure to patch.[62]

And that brings us to people. Amid the barrage of policies and technical guidance, it's often forgotten that the route to a cyber breach is surprisingly simple. In most cases, it comes down to a number: 1. That's the number of people a cybercriminal needs to trick to gain access to a system.

Phishing emails containing malicious links are common lures used to deploy ransomware. The FBI reported 241,342 phishing complaints in 2020 and estimated that phishing cost more than US$54 million.[63] Therefore, training employees to be better prepared to identify suspicious emails— and not to click on them—is essential. For large, well-resourced organisations, investing in threat hunting is the key.[64] In many cases, the attacker has been inside the victim's network for a significant period, watching and preparing the environment for an attack. An investment in threat hunting means that network anomalies can be more easily recognised and more swiftly contained. It could prove critical in detecting whether a cybercriminal is planning and plotting within a network.

It's the responsibility of all executives, business leaders and boards to be aware of and effectively manage cybersecurity risks, to ensure that appropriate measures are in place and to foster a culture in which cybersecurity really does matter. If cybersecurity matters to a chair and board, that will trickle down and become a priority for the whole organisation. To that end, it's also timely to note that Australian directors increasingly bear personal exposure to cyber risk liability, which may be heightened under the proposed changes to the critical infrastructure regime.

Incentivisation is needed to achieve real cybersecurity uplift

Good cyber hygiene is central to mitigating a ransomware attack, but cybersecurity uplift costs money—a cost that's borne without immediately 'tangible' results for organisations. This is especially pertinent for SMEs, which generally don't have the same level of resourcing to prioritise cybersecurity.

Hence, incentivisation has a key role to play if cyber resilience is to be applied across all levels of the economy.

A clear example of where existing mechanisms could be used to incentivise cyber uplift is via full expensing, previously known as instant asset write-offs. The temporary full expensing scheme, which was extended in the 2021–22 federal Budget, allows organisations with an annual turnover of less than $5 billion to immediately write off the business portion of the cost of eligible new assets they first use or install by 30 June 2023, with no cap on the value of new assets that can be claimed (but there may be certain cost limits on particular assets).[65] Put simply, this means organisations can make full or significant deductions for eligible purchases up front, rather than over a period of several years via depreciation. While this doesn't remove the need for initial outlays, the scheme does offer significant taxation benefits. There's clear scope for the federal government to provide clear information via the Australian Taxation Office about what cybersecurity asset purchases are covered under the scheme. As it stands, cybersecurity assets aren't clearly defined, and only bespoke in-house software is covered.[66] If the scheme were broadened to include off-the-shelf products and subscription services (such as cloud services), it would support scalable and more rapid uplift. This relatively simple incentivisation solution, which should be promoted, would have a two-pronged effect, simultaneously easing financial imposts on organisations while also hardening cybersecurity resilience across a greater cross-section of the economy.

Another option is to leverage the power of federal government procurement to drive organisational cybersecurity uplift by mandating minimum cybersecurity standards for organisations feeding into the government supply chain. This has the potential to be transformative, given the government's huge procurement spend (81,174 contracts with a combined value of $53.9 billion were published on AusTender in 2019–20).[67] Despite that massive spend, cybersecurity is mentioned only once in the *Commonwealth Procurement Rules*,[68] which recommend that cybersecurity risk be considered along with other risks and be evaluated in accordance with the government's *Protective Security Policy Framework*.[69] Cybersecurity needs to play a more prominent role in government procurement practices, not be viewed as an afterthought or secondary consideration. The important role government procurement could play in cyber uplift was highlighted by Rajiv Shah in his 2020 report *Working smarter, not harder*.[70] Shah observed that the government:

> … has an opportunity to leverage its market power to provide for broader benefits to the Australian economy and society … Setting security standards expected from its suppliers may help to lift standards across the board. Companies will be incentivised to lift their standards in order to qualify to do business with the government, and it will often be easier for them to apply those standards across their whole enterprises rather than just for their government contracts.[71]

A cybersecurity uplift grant or subsidy scheme could be considered, in the vein of a program such as the Skilling Australia's Defence Industry Grants Program.[72] That program provides grants to SMEs with fewer than 200 employees over three years, assisting the development of defence sector skills and human resources practices and training plans. The program provides SMEs that service, or intend to service, the defence industry with the capacity and skills required to operate in that supply chain.

A similar program could be introduced for organisations that feed into the whole-of-government supply chain to uplift cybersecurity resilience via both training and physical upgrades.

Another option could be to expand and extend the remit of the Cyber Security Business Connect and Protect Program beyond assistance and advice to also include financial aid to lift SME cybersecurity. As it stands, the program (which is currently closed), provides funding to 'trusted organisations' to raise awareness of cybersecurity risks to SMEs, promote action to address those risks and support and lift the cyber capability of SMEs. However, the scheme doesn't provide funding to assist SMEs in the physical implementation of cybersecurity uplift.

Policy recommendations

We make eight policy recommendations under the following themes.

Legal clarity

1. The Australian Government shouldn't criminalise the payment of ransoms. Instead, a mandatory reporting regime should be adopted, fostering an information-sharing culture without fear of legal repercussions.

2. A dedicated cross-departmental ransomware taskforce, including state and territory representatives, should be established to share threat intelligence and develop federal-level policy proposals to tackle ransomware nationally.

Greater transparency

3. The ACSC's existing official alert system should be expanded to include the real-time distribution of publicly available alerts and clear, actionable advice when ransomware attacks are reported. The alerts and advice should be updated as required.
4. The non-punitive mandatory reporting regime should require organisations to report ransomware incidents and known root causes to the ACSC within 21 days. The information would then be de-identified and distributed publicly.
5. The ACSC should publish a list of ransomware threat actors and aliases, giving details of their modus operandi and key target sectors, along with suggested mitigation methods.

Low-hanging fruit: incentivisation and education

6. The federal government should implement practical incentivisation measures to drive cybersecurity uplift across the economy via temporary full expensing and changes to procurement practices and grant or subsidy programs.
7. The government should deliver a concerted nationwide public ransomware education campaign, led by the ACSC, across all media. The campaign should highlight the key causes of ransomware vulnerability and how organisations can bolster their security, and it should draw in external expertise where necessary.
8. A business-focussed multi-media public education campaign, led by the ACSC, should be launched to educate organisations of all sizes and their people about basic cybersecurity and cyber hygiene. It should focus on the key areas of patching, multifactor authentication, legacy technology and human error.

Conclusion

Ransomware isn't an abstract possibility. In Australia, the threat's right here, right now and isn't going away. Unless a concerted effort is made to mitigate the risk, the problem could continue to get worse.

There's a key role for the Australian Government to play in leading the way, but tackling ransomware is a shared responsibility. While there's no doubt that organisations must take responsibility for ensuring that their cybersecurity posture is up to scratch, there are practical and easily implementable steps the government can take to provide clarity, guidance and support.

The ongoing ransomware attacks that continue to strike unabated around the world must act as a red flag. And, because we've been warned, we need a plan.

References

1. 'New McAfee report estimates global cybercrime losses to exceed $1 trillion', news release, McAfee, 7 December 2020, online.

2. Australian Signals Directorate (ASD), 'Ransomware', Australian Government, no date, online.

3. Cryptocurrency is digital currency secured by cryptography and based on blockchain technology. Cyber Security Industry Advisory Committee (CSIAC), Locked out: tackling Australia's ransomware threat, Department of Home Affairs, Australian Government, March 2021, 3, online.

4. CSIAC, Locked out: tackling Australia's ransomware threat, 3.

5. Edvardas Mikalauskas, 'Report: buying your own malware has never been easier', Cybernews, 28 April 2020, online.

6. Mikalauskas, 'Report: buying your own malware has never been easier'.

7. Federal Bureau of Investigation (FBI), Internet crime report 2020, US Government, 2020, 14. online.

8. FBI, Internet crime report 2020, 14.

9. FBI, Internet crime report 2020, 14.

10. ASD, Ransomware in Australia, Australian Government, October 2020, 1, online.

11. ASD, Ransomware in Australia, 5.

12. ASD, Ransomware in Australia, 4.

13. Natasha Kassam, 'Safety, security and threats to Australia's vital interests', Lowy Institute Poll 2021, Lowy Institute, Sydney, 23 June 2021, online.

14. Dean Blake, 'Toll customer data stolen in its second cyber attack of 2020', Inside Retail, 13 May 2020, online.

15. Casey Tonkin, 'Toll Group data dumped on dark web: 200GB of files stolen by ransomware group', Information Age, 21 May 2020, online.

16. Paul Smith, 'Hacked again: Toll Group systems hit by fresh ransomware attack', Australian Financial Review, 5 May 2020, online.

17. CSIAC, Locked out: tackling Australia's ransomware threat, 10.

18. Jessica Clifford, 'BlueScope Steel hit by cyber attack causing worldwide system shutdown of operations', ABC News, 15 May 2020, online.

19. Joshua Becker, 'Cyber attack halts Lion production of milk and beer', ABC News, 11 June 2020, online.

20. Ben Grubb, 'Hackers post evidence they have beer giant Lion's confidential files', Sydney Morning Herald, 19 June 2020, online.

21. 'Who we are', Law in Order, 2021, online.

22. Ronald Mizen, 'Hackers threaten to publish data from attack on legal services firm', Australian Financial Review, 24 November 2020, online.

23. Ry Crozier, 'Nine Entertainment warns ransomware recovery "will take time"', IT News, 29 March 2021, online.

24. Sophie Elsworth, 'Nine Entertainment's cyber attack woes continue to disrupt the media giant', The Australian, 5 April 2021, online.

25. Melissa Cunningham, 'Staff unable to access patient files after Eastern Health cyber attack', The Age, 29 March 2021, online.

26. Rory Callinan, 'UnitingCare cyber attack claimed by notorious ransom gang REvil/Sodin', ABC News, 6 May 2021, online.

27. 'FBI investigating JBS cyber attack that disrupted Australian meat and livestock industry', ABC News, 2 June 2021, online.

28. Ry Crozier, 'JBS Foods pays $14m to ransomware attackers', IT News, 10 June 2021, online.

29. Jack Brewster, 'US recoups "millions" in cryptocurrency ransom paid to Colonial Pipeline hackers', Forbes, 7 June 2021, online.

30. Department of the Treasury, The American Families Plan tax compliance agenda, US Government, May 2021, 21, online.

31. MintDice, 'KYC and AML: how it applies to bitcoin in the USA', Medium, 29 November 2020, online.

32. AUSTRAC, 'New Australian laws to regulate cryptocurrency providers', news release, Australian Government, 11 April 2018, online.

33. AUSTRAC, 'New Australian laws to regulate cryptocurrency providers'.

34. ASD, Ransomware in Australia.

35. Sections 400.3–400.8, Criminal Code Act 1995 (Cwlth).

36. Section 400.9, Criminal Code Act 1995 (Cwlth).

37. Part 5: 27–28, Charter of the United Nations Act 1945 (Cwlth).

38. UN, UN Security Council Consolidated List, online.

39. Section 10.2, Criminal Code Act 1995 (Cwlth).

40. FBI, Internet crime report 2020, 3.

41. Department of the Treasury, 'Advisory on potential sanctions risks for facilitating ransomware payments', US Government, 1 October 2020, 1, online.

42. Department of the Treasury, 'Advisory on potential sanctions risks for facilitating ransomware payments', 4.

43. FBI, 'High-impact ransomware attacks threaten US businesses and organizations', alert no. I-100219-PSA, US Government, 2 October 2019, online.

44. FBI, 'High-impact ransomware attacks threaten US businesses and organizations'.

45. Department of Home Affairs (DHA), 'Protecting critical infrastructure and systems of national significance: Security Legislation Amendment (Critical Infrastructure) Bill 2020', Australian Government, 2020, online.

46. European Commission (EC), 'EU Cybersecurity: Commission proposes a Joint Cyber Unit to step up response to large-scale security incidents', press release, 23 June 2021, online.

47. EC, 'EU Cybersecurity: Commission proposes a Joint Cyber Unit to step up response to large-scale security incidents'.

48. EC, 'Factsheet Joint Cyber Unit', 23 June 2021, online.

49. Laurens Cerulus, Clothilde Goujard, 'EU, US launch initiative against ransomware', Politico, 22 June 2021, online.

50. https://www.aspi.org.au/cybernorms; https://ad-aspi.s3-ap-southeast-2.amazonaws.com/2020-09/cybernorms_ENGLISH.mp4

51. 'Five Country Ministerial Statement Regarding the Threat of Ransomware', 7–8 April 2021, online.

52. CSIAC, Locked out: tackling Australia's ransomware threat, 9.

53. Alicia Hope, 'Cyber insurance firm suffers sophisticated ransomware cyber attack; data obtained may help hackers better target firm's customers', CPO Magazine, 5 April 2021, online.

54. ASD, Ransomware in Australia, 1.

55. FBI, Internet crime report 2020, 3.

56. DHA, 'Protecting critical infrastructure and systems of national significance: Security Legislation Amendment (Critical Infrastructure) Bill 2020'.

57. Charlie Osborne, 'New US Justice Department team aims to disrupt ransomware operations', ZDNet, 22 April 2021, online.

58. Cybersecurity & Infrastructure Security Agency (CISA), 'Ransomware alerts and tips', US Government, 2021, online.

59. CISA, 'DarkSide ransomware: best practices for preventing business disruption from ransomware attacks', alert AA21-131a, US Government, 11 May 2021, online.

60. Mary-Ann Russon, 'US fuel pipeline hackers "didn't mean to create problems"', BBC News, 10 May 2021, online.

61. 'Government races to secure critical infrastructure in wake of Colonial Pipeline ransomware attack', National Law Review, 3 July 2021, online.

62. Ponemon Institute LLC, Costs and consequences of gaps in vulnerability response, ServiceNow, no date, online, P5.

63. FBI, Internet crime report 2020, 3.

64. CrowdStrike, 2021 global threat report, 2021, 50, online.

65. Michael Janda, 'Federal budget leaves business owners smiling as instant investment tax breaks extended', ABC News, 13 May 2021, online.

66. Australian Taxation Office, 'In-house software', Australian Government, 23 April 2019, online.

67. Department of Finance, 'Procurement', Australian Government, no date, online.

68. Department of Finance, Commonwealth Procurement Rules, Australian Government, 14 December 2020, 20, online, P20.

69. Attorney-General's Department, 'The Protective Security Policy Framework', Australian Government, no date, online.

70. Rajiv Shah, Working smarter, not harder: leveraging government procurement to improve cybersecurity and supply chains, ASPI, Canberra, 18 August 2020, online.

71. Shah, Working smarter, not harder: leveraging government procurement to improve cybersecurity and supply chains.

72. 'Current grant opportunity view—GO4147', GrantConnect, Australian Government, 4 September 2020, online.

Is Australia a sitting duck for ransomware attacks? Yes, and the danger has been growing for 30 years

Australian organisations are a soft target for ransomware attacks, say experts who issued a fresh warning that the government needs to do more to stop agencies and businesses falling prey to cyber-crime. But in truth, the danger has been growing worldwide for more than three decades.

July 14, 2021

PAUL HASKELL-DOWLAND
Associate Dean (Computing and Security), Edith Cowan University

ANDREW WOODWARD
Executive Dean of Science, Edith Cowan University

THE CONVERSATION

Despite being a relatively new concept to the public, ransomware has roots in the late 1980s and has evolved significantly over the past decade, reaping billions of dollars in ill-gotten gains.

With names like Bad Rabbit, Chimera and GoldenEye, ransomware has established a mythical quality with an allure of mystery and fascination. Unless, of course, you are the target.

Victims have few options available to them; refusing to pay the ransom depends on having good enough backup practices to recover the corrupted or stolen data.

According to a study by security company Coveware, 51% of businesses surveyed were hit with some type of ransomware in 2020. More concerningly still, typical ransom demands are climbing dramatically, from an average of US$6,000 in 2018, to US$84,000 in 2019, and a staggering US$178,000 in 2020.

The 1989 AIDS Trojan (PC Cyborg) ransom demand. Joseph L. Popp, AIDS Information Trojan author, Public domain, via Wikimedia Commons

A brief history of ransomware

The first known example of ransomware dates back to 1988-89. Joseph Popp, a biologist, distributed floppy disks containing a survey (the "AIDS Information Introductory Diskette") to determine AIDS infection risks. Some 20,000 of them were reportedly distributed at a World Health Organization conference and via postal mailing lists. Unbeknown to those receiving the disks, it contained a virus of its own. The AIDS Trojan lay dormant on systems before locking users' files and demanding a "licence fee" to restore access.

Although the malware was inelegant and easily undone, it drew media attention at the time as a new type of cyber threat. The demand for payment (by cheque to a PO box in Panama) was primitive by comparison with modern approaches, which call for funds to be transferred electronically, often in cryptocurrencies.

It was well over a decade before ransomware truly began to proliferate. In the mid-2000s, stronger encryption allowed for more effective ransom campaigns with the use of asymmetric cryptography (in which two keys are used: one to encrypt, and a second, kept secret by the criminals, to decrypt), which meant even skilled systems administrators could no longer extract the keys from the malware.

In 2013, CryptoLocker malware rose to global dominance, partly supported by the GameOver Zeus botnet. Cryptolocker encrypted users' files, sending the unlock key to a server controlled by the criminals with a three-day deadline before the key was destroyed. The network was shut down in 2014, thanks to a major global law enforcement effort called Operation Tovar. It is estimated to have impacted more than 250,000 victims and potentially garnered 42,000 Bitcoin, worth around US$2 billion at today's valuation.

continued on page 38

In 2016 there were several high-profile incidents involving the Petya ransomware, which prevented users from accessing their hard drives. It was one of the first significant examples of Ransomware as a Service, whereby criminal gangs "sell" their ransomware tools as a managed service.

The following year saw arguably the most notorious ransomware attack of all time: the WannaCry attack. It struck hundreds of thousands of computers, including an estimated 70,000 systems at the UK National Health Service. The global impact of WannaCry has been estimated at up to US$4 billion.

More recent still was the Ryuk ransomware, which targeted local councils and national government agencies. But cyber-criminals have also attacked specific private companies, including the United States' largest refined oil distribution network, Colonial Pipeline, the multinational meat processor JBS Foods, and Australia's Channel Nine network.

CryptoLocker ransom demand. Nikolai Grigorik, CC BY-SA 4.0 https://creativecommons.org/licenses/by-sa/4.0, via Wikimedia Commons

Is all ransomware the same?

There are hundreds of types of ransomware, but they fit into a few broad categories:

Crypto ransomware

In modern crypto ransomware attacks, the malware encrypts users' files ("locking" the files to make them unreadable) and will typically involve a "key" to unlock the files being stored on a remote server controlled by the cyber-criminals. Early variants would require the victim to buy software to unlock the files.

Locker ransomware

Locker ransomware is usually a more complex type of malware that targets a user's entire operating system (such as Windows, macOS or Android), hampering their ability to use their device. Examples can include preventing the computer from booting, or forcing a ransom demand window to appear in the foreground and preventing interaction with the other applications.

Although files are not encrypted, the system is typically unusable by most users (as you would likely need another system or software to extract the files). In some cases the ransom demands refer to government agencies with threats of investigations relating to tax fraud, possession of child abuse materials, or terrorist activities.

Wannacry ransom demand with integrated multi-language support. Screenshot of a WannaCry ransomware attack on Windows 8. Public domain, via Wikimedia Commons

Leakware

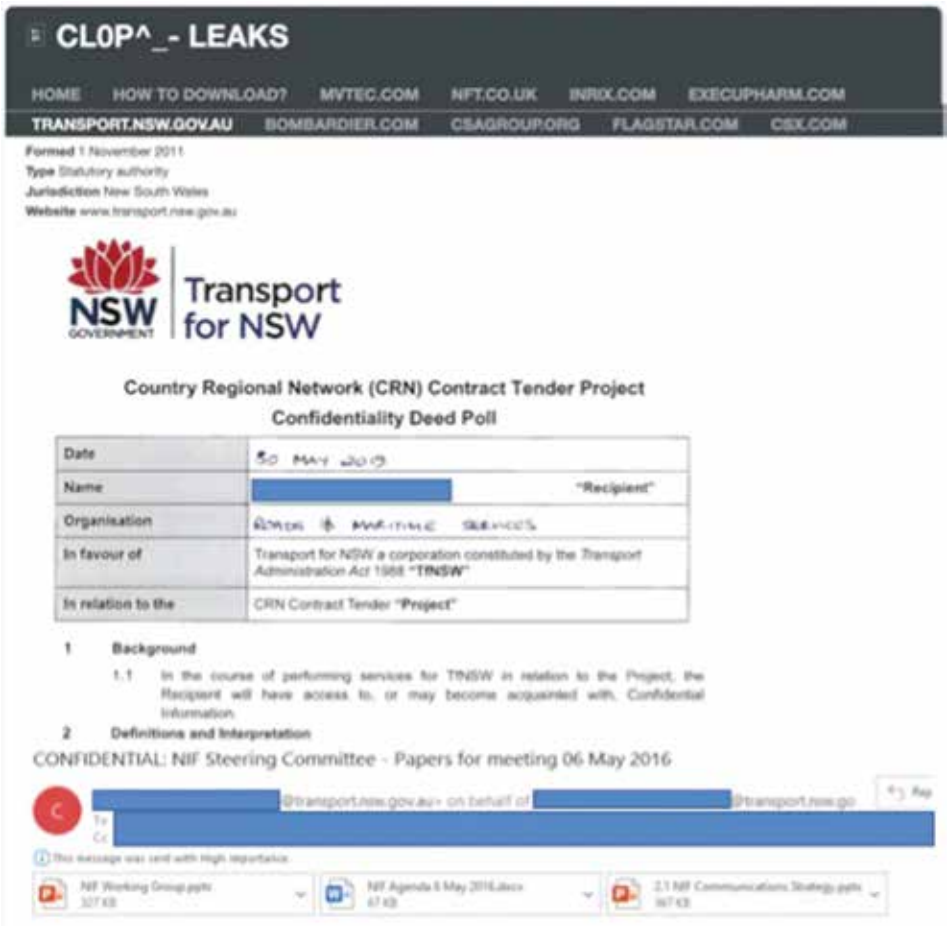
In a leakware attack, the data are not encrypted but instead are stolen from the victim and held by cyber-criminals. It is the threat of public release alone that is used to secure a ransom payment. From 2020 to 2021, reported occurrences of non-encrypted ransoms have doubled.

Double extortion

Double extortion is an alarming development whereby not only is a payment required to secure release of encrypted organisation data, but there is the added threat of public release.

This approach typically involves data being stolen from the organisation during the malware infection process, then sent

A fake FBI 'seize' notice designed to convince victims to pay the 'fine'. Motormille2, CC BY-SA 4.0 https://creativecommons.org/licenses/by-sa/4.0, via Wikimedia Commons



Screenshots from Cl0p leaks website providing access to stolen Transport NSW files (web version is not redacted). Author provided

to servers run by the cyber-criminals. To encourage payment, extracts may be posted on public-facing websites to prove possession of the data – coupled with threats to publish the remaining data.

Ransomware as a Service (RaaS)

Early ransomware was developed by individuals but, as with all software, ransomware has come of age. It is now a multibillion-dollar industry (an estimated US$20 billion in 2020) and is every bit as well designed and implemented as any commercial software.

Just as Microsoft's Office 365 has developed into a service, where instead of buying the software, you pay a monthly or yearly subscription, so has ransomware. Ransomware as a Service (RaaS) allows criminals to obtain services, typically in return for a cut of the ransom.

To pay, or not to pay?

Most law enforcement agencies recommend against ransom payments (just as many governments will not negotiate with terrorists), because it is likely to encourage future attacks. But many organisations nevertheless do pay up. Interestingly, the public sector hands over up to ten times more money to release their files than victims in the private sector.

Paying a ransom is frequently seen as the lesser of two evils, particularly for smaller organisations that would otherwise be shut down entirely by the disruption to their systems. Or, if you are lucky, the malware will already have a publicly available antidote.

But paying the ransom doesn't guarantee you'll get all your data back. By one estimate, an average of 65% of data was typically recovered after paying the ransom, and only 8% of organisations managed to restore all of it.

With criminal groups now reaping multimillion-dollar profits, ransomware attacks are likely to target larger organisations where the rewards are richer, perhaps focusing on holders of valuable intellectual property such as the health-care and medical research sectors. The Internet of Things (IoT) will likely be a target for cyber-criminals, with global networks of connected devices held to ransom.

While big organisations are likely to have appropriate technical safeguards, user education is still key – a lapse of judgement from a single person can still bring an organisation to its knees. For smaller companies, seeking (and following) cyber advice is crucial.

Given the huge scale on which cyber-criminals are now operating, we have to hope law enforcement and software security engineers can stay one step ahead.

THE CONVERSATION

https://theconversation.com/is-australia-a-sitting-duck-for-ransomware-attacks-yes-and-the-danger-has-been-growing-for-30-years-161818

Joint global ransomware operation sees arrests and criminal network dismantled

Police and private industry partnership lands ransomware criminals behind bars.

8 November 2021

INTERPOL

Singapore

A four-year operation across five continents has disrupted a ransomware cybercrime gang and seen the arrest of seven suspects believed to be behind global malware crime operations.

Codenamed 'Quicksand' (GoldDust) and carried out by 19 law enforcement agencies in 17 countries, the transcontinental operation saw officers collect and examine intelligence to establish a global threat picture about attacks by ransomware families – particularly GandCrab and Revil-Sodinokibi – and the suspects behind them.

The organized crime group that used these malwares is known for breaking into business and private networks using a range of infiltration techniques, and then deploying ransomware against their victims. The ransomware then encrypts files which are then used to blackmail companies and people into paying huge ransoms.

The suspects arrested during Operation Quicksand are suspected of perpetrating tens of thousands of ransomware infections and demanding more than EUR 200 million in ransom.

Tangible results: multiple arrests worldwide

Intelligence exchanged during the operation enabled

- Korean law enforcement to arrest three suspects in February, April and October;
- Kuwaiti authorities to arrest a man thought to have carried out ransomware attacks using the GandGrab ransomware;
- Romanian authorities to arrest two individuals suspected of ransomware cyber-attacks and believed to be responsible for 5,000 infections as well as half a million euros profit in ransom payments;
- The arrest of a man believed to be responsible for the Kaseya ransomware attack, thought to have been carried out last July by the REvil gang with more than 1,500 people and 1,000 businesses affected worldwide.

"Ransomware has become too large of a threat for any entity or sector to address alone; the magnitude of this challenge urgently demands united global action which INTERPOL can uniquely facilitate as a neutral and trusted global partner," said INTERPOL Secretary General Jürgen Stock.

"Policing needs to harness the insights of the cyber security industry to identify and disrupt cyber criminals as part of a true coalition, working together to reduce the global impact of ransomware cybercrime," added the Secretary General.

A powerful global coalition

A joint INTERPOL-Europol operation, Quicksand was coordinated from INTERPOL's Cyber Fusion Centre in Singapore where stakeholders shared live intelligence in an interactive and secure environment via INTERPOL's global network and capabilities.

Through INTERPOL's Gateway project, INTERPOL's private partners Trend Micro, CDI, Kaspersky Lab and Palo Alto Networks also contributed to investigations by sharing information and technical expertise.

Gateway boosts law enforcement and private industry partnerships to generate threat data from multiple sources and enable police authorities to prevent attacks.

Bitdefender supported operations by releasing tailor-made decryption tools to unlock ransomware and enable victims to recover files. These innovative tools enabled more than 1,400 companies to decrypt their networks, saving them almost EUR 475 million in potential losses.

KPN, McAfee, S2W helped investigations by providing cyber and malware technical expertise to INTERPOL and its member countries.

Operation Quicksand continues to supply evidence that is feeding into further cybercrime investigations and enabling the international police community to disrupt numerous channels used by cybercriminals to launder cryptocurrency and commit ransomware crime.

With the combined global financial impact in ransom payments from ransomware families believed to be within the billions of dollars and thousands of victims worldwide, INTERPOL's private partners and member countries work together to provide support to victims hit by the ransomware.

Research from Chainalysis found that criminals made USD 350 million in 2020 from ransomware payments, representing an increase of 311 per cent in one year. Over the same period, the average ransom payment increased by 171 per cent, according to Palo Alto Networks.

Participating countries included Australia, Belgium, Canada, France, Germany, The Netherlands, Luxembourg, Norway, Philippines, Poland, Romania, South Korea, Sweden, Switzerland, Kuwait, the United Kingdom and The United States.

MCS Security

A DIVISION OF MCS SECURITY GROUP PTY LTD

MCS specialises in providing security services at major commercial property sites and retail shopping centres throughout Western Australia.
MCS Security Group Pty Ltd (MCS) is a proud member of the Security Agents Institute of WA.
MCS specialises in providing security services at major commercial property sites and retail shopping centres throughout the Perth metropolitan area and regional country areas of Western Australia.
MCS also specialises in providing electronic security services which includes the design, supply, installation and commisioning of security alarms, CCTV, biometric and access control systems to the commercial, industrial and domestic sectors.
MCS Security - Equine Monitoring Systems, specialise in Wireless Float Cameras.

Ph: (08) 9301 2420

www.mcssecurity.com.au

Proudly Supporting the AiPol Journal & Local Police

Find us on Facebook

澳大利亞塔州中國佛教學院
Tasmanian Chinese Buddhist Academy of Australia

The supreme and profoundly wondrous Dharma,
With great difficulty to chance upon across billions of kalpas,
I now may witness and uphold,
And vow to understand Tathagata's true meaning.

The 14th annual Academic Symposium of the Tasmanian Chinese Buddhist Academy of Australia will be held online from 11:00 am to 3:00 pm AEDT on Sunday, 3 July, 2022.

Topic: "Jin-Gang-Dhyana Study"

With "Jin-Gang-Dhyana Study" as the topic, all friends and scholars within the Religion and within the School who have an interest in Chinese Han Transmission Tantrayana Buddhism - Holy Tantra Gu Fan Mi Jin-Gang-Dhyana Buddhism are welcomed to submit articles.

Articles written in all languages are welcomed, including Sanskrit, Pali, English, Islamic, Mongolian, Japanese, Korean, Filipino, Vietnamese and Indonesian. Please attach an English translation.