Beyond The Blame Game

Time for A National Ransomware Strategy

February 2021

Kristina Keneally

Deputy Labor Leader in the Senate
Shadow Minister for Home Affairs
Shadow Minister for Immigration and Citizenship
Shadow Minister for Government Accountability

Tim Watts

Shadow Assistant Minister for Communications
Shadow Assistant Minister for Cyber Security

ON YOUR SIDE. Labor

Contents

Introduction

According to the Australian Cyber Security Centre, 'ransomware' – malicious software deployed by criminal groups to deny access to an organisation's IT systems and data until a ransom is paid – is now the biggest cyber threat facing Australian businesses and government.

Chris Krebs, former director of the US Department of Homeland Security's Cybersecurity Infrastructure Security Agency, recently told the US House Committee on Homeland Security that ransomware was the nation's top cyber threat.

None of these interventions are silver bullets. But the threat of ransomware isn't going anywhere soon, and the government cannot leave it to Australian organisations to confront this challenge alone.

It is time for a National Ransomware Strategy.

An Intolerable Cost Burden

This combination of organisational innovation and international impunity has significantly increased the scale and severity of ransomware attacks over the past 12 months. While the cost is hard to accurately quantify, the scale is enormous.

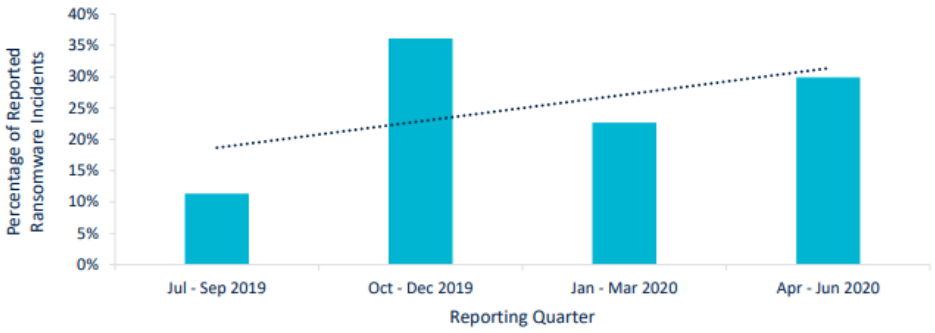
Security firm, Emsisoft received 452,151 submissions to its ransomware identification service from confirmed ransomware attacks around the world in 2019. Extrapolating estimates of ransom demands and down time caused by ransomware incidents, it is estimated that the global cost of ransomware in 2019 was a minimum of US$42.4 billion and a best estimate of US$169.7 billion.

Australia hasn't been spared from these trends; Emsisoft received 2,874 submissions to its ransomware identification service from ransomware attacks on Australian organisations in 2019. It has estimated that these ransomware attacks cost the Australian economy US$1.1 billion. A survey of senior IT decision makers by technology firm Crowdstrike reported that a greater percentage of Australian organisations have dealt with ransomware attacks in the last 12 months than the global average.

While these firms recognise the significant limitations of their methodology, broad analysis of this kind does underscore the sheer scale of the challenge of ransomware. Even more concerningly, the consensus amongst industry professionals is that the problem has become significantly worse since this analysis was done.

And the costs of ransomware aren't just financial, the system down time caused by ransomware attacks can cause serious physical harm. While the potential beer shortages from the Lion ransomware attack may not inspire government intervention, the WannaCry ransomware attack brought the UK's National Health Service to a halt, resulting in the cancellation of 19 000 medical appointments including heart surgeries. 2020 also saw what is believed to be the first death as a result of ransomware; in Germany a woman died after a ransomware attack against University Hospital Düsseldorf meant that her ambulance had to be redirected to another hospital 20 miles away.

The ACSC has not published specific statistics on the number of ransomware attacks in Australia, but has noted the upwards trajectory of ransomware incidents reported in its *Ransomware in Australia* report.



Ransomware-related incidents reported to the ACSC (Ransomware In Australia)

An Evolving Threat

The Emergence of 'Big Game Hunting'

Over the last two years, ransomware attacks have increasingly been defined by a new strategy known as 'big game hunting'. According to the US Internet Crime Complaint Centre (C3) and the FBI, over this period ransomware attacks have become:

> *"more targeted, sophisticated, and costly…Since early 2018, the incidence of broad, indiscriminate ransomware campaigns has sharply declined, but the losses from ransomware attacks have increased significantly."*

While in the past ransomware campaigns were generally automated, self-perpetuating and opportunistic, today, 'big game hunting' ransomware groups invest significant time and effort into researching targets ahead of potential campaigns to assess the potential return on investment of a campaign.

This has led to the increased targeting of larger organisations with a low tolerance for down-time like manufacturing, healthcare and government targets. Organisations with operational technology (OT) networks have become an increasingly common target as part of this trend. With Coverware estimating that ransomware attacks resulted in an average of 19 days of IT system downtime within target organisations in 2020, the pressure to pay is significant.

During this reconnaissance period, ransomware crews investigate not only the financial health of organisations, but also potential points of leverage that may increase the chances of an organisation paying a ransom, including the most sensitive time to initiate an attack.

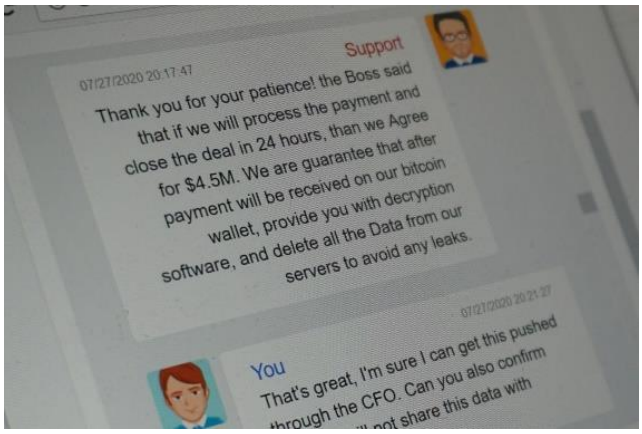
These sophisticated ransomware crews have also innovated new methods of maximising pressure on targets to pay, including 'double extortion' schemes which combine traditional IT system ransoms with an additional threat to publish an organisation's confidential information online if payment is not forthcoming. This double extortion ransomware model is particularly threatening to professional services firms whose business relies on their ability to protect the confidentiality of client data.

As a result, many ransomware victims are paying up. Proofpoint's 2020 State of the Phish report found that 33% of respondents who has suffered ransomware attacks chose to pay the ransom, as did 27% of respondents to Crowdstrike's 2020 Global Attitude Survey. This data reinforces anecdotal evidence from a leader of the REvil ransomware group who claimed in a recent interview that "*around one-third of all companies quietly negotiate to pay the ransom*".

Franchising Ransomware – 'Crime as a Service'

As the financial returns have grown, so too has the sophistication of the organisational models of the criminal groups operating ransomware businesses. Today, a relatively small number of more technically sophisticated ransomware crews develop, market, sell, and maintain their own variants of ransomware code along with supporting 'customer' negotiation and payment services that they then licence to a larger number of 'affiliates' to use against target organisations in exchange for a cut of the ransom.

This 'Crime as a Service' model has allowed for specialisation throughout the ransomware ecosystem. An extensive network of online forums have emerged to allow criminals to sell distinct steps in ransomware attacks like access to compromised systems. The ability for criminals with limited technical expertise to obtain access to sophisticated ransomware software and supporting services has significantly increased the potential number of actors able to undertake ransomware attacks in recent years.



A victim negotiates with a ransomware operator (Reuters)

International Impunity

The recent growth in ransomware has also been enabled by the relationship between ransomware crews and the countries from which they operate.

Many ransomware crews are effectively modern-day privateers, operating with the understanding that their host countries will turn a blind eye to their activities and will not cooperate with international law enforcement actions against them so long as they refrain from targeting local organisations.

Ransomware is costing jobs and investment within Australian businesses and it's getting worse. It's time the government acted.

The Need for Government Leadership on Ransomware

The Morrison Government's 2020 Cyber Security Strategy rightly identifies that individual organisations have the primary responsibility for securing their own networks against any cyber threat, including ransomware.

However, this is far from the end of the story.

Government has a range of policy tools that only it can deploy in an effort to reduce the overall volume of ransomware attacks. These include options like regulation making, law enforcement, diplomacy, international agreement making, offensive cyber operations as well as the imposition of sanctions. While individual organisations will always be primarily responsible for securing their own networks, governments can intervene strategically to shape the overall threat environment in ways that make Australian targets less attractive.

The case for government leadership is particularly compelling when confronted by a threat where the actions of one organisation help shape the nature of the threat faced by others. When an organisation decides that it is in its own best interest to pay a ransom, it increases the resources

available to ransomware crews to mount further, more sophisticated attacks against other targets. When a series of organisations from particular countries or particular industry sectors make ransomware payments it can create a reputation that these countries or industries are valuable targets, increasing the number of future attacks. While network security might be an organisational challenge, Australia's response to ransomware is a problem which requires collective action and can be influenced by the policy and regulatory framework employed by the Australian Government.

As Ivan Kwiatkowski, cybersecurity researcher at Kaspersky's global research and analysis has puts it:

> *"we cannot hope that the problem can be solved by a collectively ethical behaviour: the overall strategy must be steered by the national authorities."*

The former director of the UK's National Cyber Security Centre, Ciaran Martin agrees, recently declaring:

> *"It's time to do something because we're getting cleaned out left, right and centre… Services are being disrupted and millions of pounds are being lost… We need to do something to catapult ransomware up the priority ladder for cybersecurity agencies, governments and industry people who care about cybersecurity."*

The newly launched global multi-stakeholder Ransomware Task Force sums up the current situation when it declared:

> *"the global community can no longer afford to address ransomware on a case-by-case basis — now is the time for comprehensive and decisive action… ransomware is too large of a threat for any one entity to address".*

A National Ransomware Strategy

Australia needs a comprehensive National Ransomware Strategy designed to reduce the attractiveness of Australian targets in the eyes of cyber criminals.

As Dr Ian Levy, the technical director of the UK's National Cyber Security Centre has said:

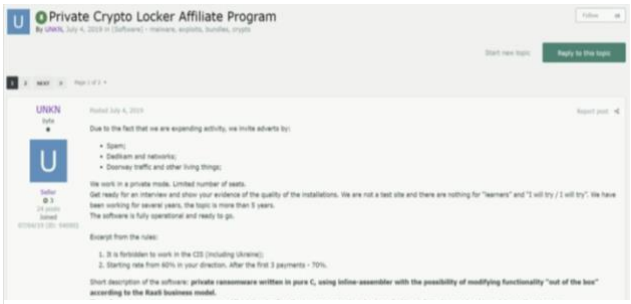
> *"cyber crime really does run on a return on investment model, and if we can affect that, we can demotivate attackers from targeting the UK."*

The evolution of ransomware from an automated, indiscriminate crime of opportunity into a crime undertaken by sophisticated criminal organisations who carefully select their targets presents an opportunity as well as a challenge for Australia. While the emergence of sophisticated criminal organisations directing ransomware attacks has increased the volume and scale of ransomware attacks, it also creates a new point of intervention that can be targeted by national governments.

If sophisticated ransomware crews are now making premeditated assessments about the potential returns of attacks on particular targets, it is open to the Australian government to pursue a strategy that seeks to shape those assessments by making Australian targets less attractive.

There is reason to believe this is now possible. The way that ransomware operators engage with their affiliates clearly shows that these organisations respond to incentives when selecting targets.

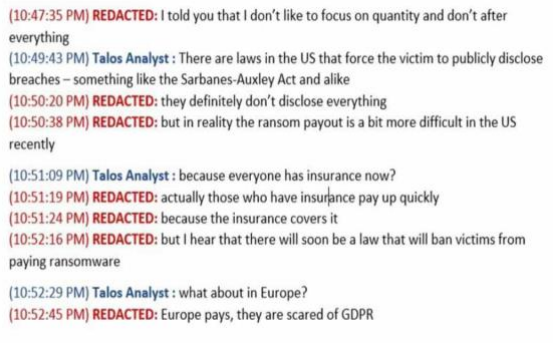
For reasons that are easily inferred, these agreements regularly explicitly ban affiliates from targeting organisations located in Russia or nations within the 'Commonwealth of Independent States', the former Soviet Bloc.



A ransomware crew's advertisement specifies that affiliates may not target organisations within 'CIS', the former Soviet

According to Carnegie, "*malware used by Russian and east European cybercriminals is often designed so that it purposefully avoids infecting computers if the program detects the potential victim is a native resident*".

Beyond this, anecdotal evidence strongly suggests that ransomware operators are aware of the national contexts that potential target organisations operate in and actively assess their potential return on investment.


(10:47:35 PM) **REDACTED:** I told you that I don't like to focus on quantity and don't after everything
(10:49:43 PM) **Talos Analyst :** There are laws in the US that force the victim to publicly disclose breaches – something like the Sarbanes-Auxley Act and alike
(10:50:20 PM) **REDACTED:** they definitely don't disclose everything
(10:50:38 PM) **REDACTED:** but in reality the ransom payout is a bit more difficult in the US recently

(10:51:09 PM) **Talos Analyst :** because everyone has insurance now?
(10:51:19 PM) **REDACTED:** actually those who have insurance pay up quickly
(10:51:24 PM) **REDACTED:** because the insurance covers it
(10:52:16 PM) **REDACTED:** but I hear that there will soon be a law that will ban victims from paying ransomware

(10:52:29 PM) **Talos Analyst :** what about in Europe?
(10:52:45 PM) **REDACTED:** Europe pays, they are scared of GDPR

A ransomware operator compares the potential returns of targets in different jurisdictions (Cisco Talos)

A recent interview between cyber security research firm Cisco Talos and a ransomware operator revealed that the actor *"has geographic preferences"* based on both perceptions of the cybersecurity posture of organisations within particular regions, and a surprisingly deep familiarity with the national regulatory environments of target organisations.

At one point, the operator even reveals familiarity with policy proposals to ban ransomware payments.

In the actor's own words:

> *"I do not like to work in the U.S. because getting paid is harder there, the EU pays better and more."*

The Australian government should be pursuing a National Ransomware Strategy which seeks to alter the return on investment of ransomware groups that target Australian organisations. To do this, it should pursue a range of initiatives designed to *increase the costs* of mounting campaigns against Australian organisations and to *reduce the returns* that are realised from such campaigns. None of these initiatives alone will be silver bullets, but collectively, over time, they may help to create the perception in the minds of attackers that Australian targets are not worth the effort.

Imposing Costs

The Australian government has tools that it can use to impose costs on ransomware crews that target Australians, including *law enforcement action, targeted international sanctions* and *offensive cyber operations.*

Law Enforcement

The Status Quo – Impunity

Ransomware is largely a crime of impunity in Australia today. While ransomware attacks are clearly criminal offences under Sections 477 and 478 of the Commonwealth Criminal Code, punishable by up to ten years' imprisonment, prosecutions are rare.

The Office of the Australian Information Commissioner was notified of only 69 ransomware attacks involving breaches of personal information that were likely to result in serious harm in 2020. Further, the 69 notifiable data breaches categorised by the OAIC as ransomware attacks are just a subset of the 622 data breach notifications resulting from malicious or criminal acts. Many of these notified data breaches could have been precursors to ransomware attacks including incidents that the OAIC categorises as 'phishing', 'brute force attacks', 'hacking', 'malware', and other forms of credential theft.

It is unknown how many successful ransomware attacks occurred in which the affected organisations determined that the incident did not meet this OAIC threshold, although the 2874 submissions received by Emsisoft to its ransomware identification service from ransomware attacks on Australian organisations in 2019 suggests the number of unreported incidents could be significant. The OAIC has itself noted a trend towards organisations downplaying incidents and delaying data breach notifications. In addition to these raw numbers, Australia has recently seen high impact ransomware campaigns against high profile targets like Toll Group, Bluescope Steel, Lion, Spotless, Regis Healthcare, Law in Order, and regional Victorian hospitals.

In the face of the prevalence of these attacks, the Australian Federal Police has advised the Senate that while it has a *"number"* of ongoing investigations into ransomware attacks, over the past 12 months, it only *"charged one individual in Australia with criminal offences related to ransomware".* While state and territory police share responsibility for investigating ransomware attacks against individuals, state governments and small to medium enterprises, it is unclear from public records how many charges have been laid in relation to investigations of this kind.

Ultimately, while the incidence of ransomware attacks against Australian targets is common, Australian law enforcement action against perpetrators is rare. The likelihood for law enforcement action is so low that it would have little impact on a ransomware crew's decision to target an Australian organisation.

Australia is not unique in this respect. As recognised in the Paris Call for Trust and Stability in Cyberspace, the transnational nature of ransomware crimes is a challenge for governments around the world and a 'Cyber Enforcement Gap' has been observed in many jurisdictions. However, if Australia wants to impose sufficient costs on ransomware crews to deter attacks on Australian targets, we need to put an end to this legal impunity.

Measuring Progress

The first step towards closing the cyber enforcement gap in Australia should be measuring performance. At present, the incidence and costs of ransomware and the effectiveness of law

enforcement actions in response are nearly entirely opaque to policy makers and the general public.

Without quality data, it is difficult for policy makers and the general public to properly gauge the scale of the problem of ransomware and the effectiveness of the law enforcement response. It makes it too easy for government to hide the scale of the problem and avoid internal and external pressure for change. We need more people asking why the cyber enforcement gap exists and what can be done to close it.

This kind of transparency is particularly important at a time that the government is making new investments in the capabilities of the AFP's Cybercrime Operations' investigators, technical specialists, and intelligence officers. The AFP has told the Senate that its role is to work in partnership with a range of security and law enforcement agencies to prevent, disrupt, and investigate ransomware attacks. Given the rapidly growing scale of the threat posed by ransomware, we need to be able to measure its effectiveness in this regard.

Ongoing cyber crime data collection and publication is needed to drive improvement and spur innovation within governments and law enforcement agencies in the fight against ransomware. Given this, the government should consider asking the Australian Institute of Criminology to work with the Australian Criminal Intelligence Commission and the Australian Cyber Security Centre to publish authoritative statistics on the incidence and cost of ransomware in Australia. It should also consider establishing a centralised reporting data base for ransomware prosecutions undertaken by state and federal authorities.

International Cooperation

Authoritative data on the costs of ransomware and the scale of the cyber enforcement gap could form the basis of a new Australian diplomatic push for greater international cooperation to arrest and charge individuals within ransomware crews.

While Australia's cyber diplomacy has been world leading in helping to set international norms for responsible state behaviour in this domain in recent years, in the face of the global wave of ransomware, it is now time for a greater diplomatic focus on practical measures to advance international law enforcement cooperation in investigating and prosecuting cybercrime.

At present, much of the problem of the practical legal impunity of ransomware crews stems from the lack of cooperation of the Eastern European countries that play host to many of these actors. There are limits to Australia's ability to directly influence these countries. However, there are many nations around the world that share Australia's interest in ending impunity for ransomware attackers. An activist approach to fighting ransomware would see the Australian government building coalitions of nations to pressure recalcitrant governments to stop ignoring and harbouring transnational ransomware groups, and to develop mutual law enforcement assistance agreements with these states. As a start, Australia could seek to lift the priority of this issue within groupings like the Five Eyes and the G20.

Beyond such a general diplomatic push, there are two specific areas that the Australian government should consider a more concerted international effort: *aggressive participation in joint international law enforcement operations and regional cooperation to prevent the emergence of new affiliate host countries.*

Aggressive Participation in Joint International Law Enforcement Operations

While Australian law enforcement agencies have been part of some significant international cybercrime cooperation success stories, Australian law enforcement agencies need to be more aggressively and visibly involved in international operations against ransomware operators and pursuing those who target Australia. Ransomware crews need to know that if they target Australian organisations, the talents and resources of Australia's law enforcement agencies will be a driving force in international law enforcement responses.

Screen Capture from Emotet Law Enforcement Raids (Youtube)

In this respect, the recent coordinated international operation against Emotet was notable for the public absence of the involvement of Australian law enforcement. While there was no lack of Australian organisations targeted by Emotet, Australian law enforcement were not publicly involved in the international takedown operation. Law enforcement agencies from the United States, Canada, France, Germany, the Netherlands, United Kingdom and officials in Lithuania, Sweden, and Ukraine were all recognised in media releases publicising the action, but not Australian law enforcement. It may be that none of the infrastructure associated with this malware operated within Australian jurisdictions and that Australian agencies were not able to participate in the initial disruption operation, but Australian law enforcement agencies should always be at the table in operations like this seeking subsequent prosecutions on behalf of Australian victims.

Regional Cooperation to Prevent the Emergence of New Affiliate Host Countries

While ransomware crews are currently predominantly based in Eastern Europe, the lower barriers to entry and increased scope for specialisation enabled by growth in the ransomware-as-a-service and affiliate organisational models behind ransomware campaigns, creates a real threat that ransomware groups will emerge in Indo-Pacific jurisdictions with weaker cybercrime law enforcement capability.

While *'stronger cybercrime prevention, prosecution and cooperation'* is one of eight goals in DFAT's 2017 International Cyber Engagement Strategy, it is difficult to discern tangible outcomes of these efforts from the latest Progress Report. Australian aid initiatives that deliver training and cybercrime law enforcement capacity building programs throughout our region are welcome, but we need to make more progress in specific, tangible international law enforcement cooperation.

In particular, greater focus is needed to promote international agreements that enable mutual legal assistance and intelligence sharing on cybercrimes like ransomware. Australia should be prioritising promotion of the ratification of the Budapest Convention on Cybercrime within the Indo-pacific, which in spite of the work of the Australian government to support Tonga's ratification of the agreement, remains at very low levels throughout our region, particularly in Southeast Asia.

Australia's efforts also need to be much more geographically focused. It is unclear how the government has chosen the nations with which it has undertaken cyber diplomacy initiatives in cybercrime, or what the underlying strategy is. Rather than engaging with regional partners on a

seemingly ad hoc basis, we should be focusing our efforts on nations that we have assessed could become emerging cybercrime hubs. As the Australian Strategic Policy Institute (ASPI) has argued:

> *"some Southeast Asian countries are emerging as bases for serious regional, and even global, cybercrime threats. We're not proactively tackling the locations where the cybercrime threat develops and matures."*

We need a harder edge to our cyber diplomacy in these emerging hubs, focused on providing resources for capacity building, training for cyber investigators (legal and technical), and anti-corruption programs. The AFP is currently establishing new cybercrime liaison officers in Europe, Africa and North America, but cooperation in Southeast Asia should be a greater focus.

There is more that Australia could be doing to develop cybercrime prevention programs in these emerging cybercrime hubs, using our aid programs to develop diversion programs and even skilled migration pathways for young, technically savvy people in these countries to help them to forge legitimate careers in cybersecurity in the region.

ASPI has criticised current Australian efforts, stating it "*lacks specificity in its implementation*". These efforts should be expanded to include increased engagement with south Asian and south-east Asian countries that host a greater portion of cyber criminals than the Pacific islands where current efforts are focused.

Targeted Sanctions

Where law enforcement action is not possible due to an ongoing lack of cooperation with the law enforcement agencies of nations that play host to ransomware crews, the Australian Government should consider engaging with like-minded countries to impose travel and asset sanctions on ransomware gangs and their enablers.

Sanctions of this kind would not be without international precedent. The U.S. Treasury Department has added ransomware operators to their list of sanctioned entities. In mid-2020 the EU imposed sanctions, including a travel ban and asset freeze, on individuals involved in the WannaCry, NotPetya and Operation Cloud Hopper attacks.

While the costs of limiting the travel and investment opportunities of Eastern European based targets in Australia may be limited, Australia could seek reciprocal recognition of these sanctions among like-minded nations, seeking to expand their scope as far as possible throughout the developed world. While not decisive, such sanctions may provide a useful irritant to ransomware crews, helping to deter them from targeting Australian organisations. If nothing else, such actions will help draw international attention to the problem of international law enforcement cooperation against ransomware crews.

Encouragingly, the Department of Home Affairs, responding to questioning in Senate Estimates, has indicated that sanctions of this kind are already under consideration by the Department of Foreign Affairs and Trade.

Offensive Cyber Operations

Where there is no prospect for law enforcement action against ransomware crews, Australia should seek to impose costs on ransomware crews that target Australian organisations by seeking to disrupt their activities through offensive cyber operations.

Offensive cyber operations can take a wide range of forms depending on the nature of the adversary and their operations. An increasingly prevalent strategy for offensive cyber operations that has emerged in recent years is '*persistent engagement*'. Persistent engagement is a strategy of continuously disrupting the activities of an adversary in order to increase the cost of certain behaviours and to degrade their capabilities over time. It has been described by Professor Bobby Chesney, University of Texas, as "*putting sand in the gears"* of the adversary. This may in time incentivise the adversary to shift their choice of target or give up altogether.

Sometimes these operations can be dramatically cloak and dagger. As Chris Krebs, the former director of the US Cybersecurity and Infrastructure Security Agency has described the potential scope of these operations:

> *"You actually deploy title ten employees [civilians employed by the military], like Cyber Command, and you deploy intelligence capabilities. You direct message them, saying, 'We know who you are, stop or we're going to come after you, using information warfare.' You dox them. There are things you can do."*

While counter-intelligence style offensive cyber operations like this are dramatic, often offensive cyber operations aim to have an incremental effect. As the Cambridge Cybercrime Centre has suggested, these operations:

> *"might productively focus on the economics of attention and boredom – how boring and laborious can we make this work before people quit? By making this work more boring, interventions can have a real impact on these markets by encouraging 'burnout'."*

Persistent engagement strategies are already being implemented by partner countries in response to ransomware and similar threats such as the Trickbot and Emotet botnets. In both these cases nation state forces targeted the command and control (C2) infrastructure of these botnets. During the Trickbot operation, US forces also inserted significant amounts of fake data into the stolen banking data that Trickbot had accumulated, adding cost. Professor Chesney observed that:

> *"If nothing else, this move would have created a lot of resource-consuming headaches for TrickBot's operators as they set about to fix the mess."*

Even with the demonstrated ability of Trickbot to re-establish its C2 infrastructure Professor Chesney says:

> *"the world is better off with TrickBot repeatedly disrupted in this way, even if its operators are able to restore functions each time… a major benefit of disruptive operations, especially if the friction can be sustained over time. On this view, the operations not only have moments of direct disruptive impact, but they also consume scarce target resources and thus in opportunity-cost terms reduce the target's overall capability to cause harm."*

The Australian Government already engages in some offensive operations against cyber criminals, initiated by law enforcement agencies and supported by the Australian Signals Directorate. In April 2020 Minister for Defence Reynolds stated that:

> *"We are hitting back through the Australian Signals Directorate, who have already successfully disrupted activities from foreign criminals by disabling their infrastructure and blocking their access to stolen information."*

The Secretary of the Department of Home Affairs gave a further flavour of the nature of these capabilities in response to questioning in Senate Estimates:

> *"ASD has the highest level... of intelligence collection in cyber and of cyber-disruption. They're the offensive systems that Mr Turnbull announced back in 2016, which up until that point were classified—we couldn't speak about them publicly. We developed those for war, we developed those for going after terrorists, and we developed those capabilities for other very high-end conflict. What we've done now is to start to apply those offensive tools, in ways that Ms Noble and others and the ministers have spoken about, against criminals."*

However, the criteria that the government applies when determining what criminal organisations are targeted in this way and in what circumstances has been publicly disclosed.

When asked in Senate Estimates whether such a policy framework guiding the use of offensive cyber capabilities against criminal organisations existed within government, ASD responded simply that:

> *"Operations to counter serious offshore cyber criminals are conducted by ASD in close cooperation with law enforcement agencies."*

Every offensive cyber mission is targeted and proportionate, supported by a strong framework of legislation and policy, and subject to ASD's oversight framework, including by the Inspector-General of Intelligence and Security."

The Secretary of the Department of Home Affairs further elaborated in a separate hearing that:

> *"(ASD) have in the past few years… chosen some targets in collaboration with law enforcement to go after, and they've disrupted them. Obviously we don't want to give away how we select our targets or why we go after particular targets, but at the moment they are pushing forward to see what results they get, what yields they get.*
>
> *Obviously the more criminal activities they take out with the most targeted attacks—that tells them something.*
>
> *But I really don't want to go much more deeply into how they go about that, because once you get into target selection it gives the adversary a sense of whether they're next or how we actually assess targets for selection."*

This reluctance to publicly discuss the policy framework that Australian law enforcement agencies use to guide their decision to launch offensive cyber operations against criminal groups is worth testing. Arguably, this is an area where we *should* want to signal more specific intent. As Ciaran Martin, the former Director the UK's National Cyber Security Centre has written, absent specificity, public statements that governments will *"impose costs"* through offence cyber operations risk becoming a *"catchy, useful political slogan devoid of meaning, substance and—consequently—impact."* Martin makes it clear that offensive operations against cyber criminals, particularly ransomware crews, are valuable but we need to think clearly about the specific effects of specific actions against specific adversaries in order to understand whether *"imposing costs"* will actually have a deterrent effect.

For the reasons outlined at the beginning of this discussion paper, there is reason to think that offensive cyber operations in response to the targeting of Australian organisations could alter the ROI calculations of ransomware crews. But this will only happen if these crews have a clear

understanding of the relationship between cause and effect. To effectively shape the calculus of ransomware crews, the government should consider clearly articulating a policy framework outlining the kinds of consequences ransomware crews should expect for targeting Australian organisations.

Reducing Returns

The primary tools available to the government to reduce the returns of ransomware attacks on Australian organisations are *imposing controls on ransomware payments*, *cracking down on rogue bitcoin exchanges* and *hardening network security* of public and private organisations within Australia.

An indicted member of the Evil Corp ransomware gang (Wired)

Imposing controls on ransomware payments

The most direct way that the Australian government could influence the returns received by ransomware crews for targeting Australian organisations would be the regulate the payment of ransoms by Australian organisations.

The bottom line of the return on investment for ransomware attacks is the willingness of target organisations to pay ransoms. As Charles Carmakal, the CTO of respected cyber security group Mandiant put it:

> *"the reason why there's such a big ransomware problem today is because so many criminals are getting paid."*

If Australian organisations can develop a reputation for being less likely to pay ransoms than targets in other jurisdictions, the return on investment for targeting Australian organisations will fall and so too will targeted ransomware attacks against Australian organisations.

The ACSC currently advises against Australian victims of ransomware attacks paying ransoms, noting that:

> *"payment of the ransom may increase an organisation's vulnerability to future ransomware incidents. In addition, there is no guarantee that payment will undo the damage."*

This is consistent with the standard advice provided to victims around the world by cyber security experts responding to ransomware incidents. Despite this, international evidence suggests that around one third of victims do pay, and there is no evidence to suggest these rates are lower in Australia.

Given this, as part of a strategy to change the calculus of ransomware operators targeting Australia, the government should seriously consider implementing government controls on the payment of ransoms.

Indeed, an increasing number of cyber security experts and policy makers around the world are arguing for outright bans on the payment of ransoms. Brett Callow, a cybersecurity expert at Emsisoft has argued that:

> *"the only solution to the worsening ransomware problem is a complete prohibition on the payment of ransoms."*

The former Director of the UK's NCSC Ciaran, Martin has similarly commented that:

> *"if I had one policy card to play in the next year, I would ask for a serious examination of whether we should change the law to make it illegal for organisations in the U.K. to pay ransoms in the case of ransomware."*

Chris Krebs, the former Director of the US Cybersecurity and Infrastructure Security Agency noted in evidence to the US congress that:

> *"The simple fact right now is ransomware is a business and business is good. It's simply too easy for criminals to extract value and...it is primarily driven by the ubiquity of crypto currencies and the ability to anonymously transact illicit activities… Should it be legal to pay ransom? When you think about terrorism and the payment of ransom that is typically unlawful."*

There are however real trade-offs involved with taking such an approach.

While most cyber security experts advise organisations against paying ransoms as a general principle, most also note that organisations may confront extreme situations where the payment of a ransom may be necessary where down time threatens human life, as it may do within certain healthcare or critical infrastructure operators.

The Secretary of the Department of Home Affairs has acknowledged these complexities in evidence to Senate Estimates, noting:

> *"It's a complex policy question. It's no different from the advice that governments give against the payment of kidnap ransoms. Sometimes private citizens choose to do so because of concern about threats to loved ones… I think the moral dilemma that has arisen in the pre-cyberworld is outlawing ransoms paid to kidnappers. Governments don't do it, but typically they haven't criminalised it because there are often some difficult moral dilemmas there if a person has been bodily kidnapped. Whether the same moral questions arise in relation to the locking up of data is something we will have to consider separately."*

There are other options for regulating ransomware payments, short of an outright ban, that should also be explored. In particular, the government should seriously investigate implementing controls on paying these ransoms, with a presumption that approval would only be given in exceptional circumstances. This approval process would also allow the government to collect valuable data

that can be used to analyse the trends of ransomware attacks and to better measure the effectiveness of its response.

The U.S. Treasury Department has added ransomware operators to their list of sanctioned entities, this action makes the payment of ransoms to these entities illegal. However, organisations may apply to the Office of Foreign Assets Control within the US Treasury for an exemption allowing them to make a payment. The Treasury guidance on ransom payments indicates that *"ransomware payments demanded as a result of malicious cyber-enabled activities will be reviewed by OFAC on a case-by-case basis with a presumption of denial."* An exemption model could make it significantly more difficult for Australian organisations to make ransom payments, while also potentially allowing critical infrastructure operators, healthcare providers and similar entities with no tolerance for downtime to make payments in emergency situations to quickly restart operations.

Some may argue that this model will encourage attackers to mount more extreme attacks and target the entities that are most likely to obtain exemptions. However, this would only occur if the ROI of mounting these attacks was better than the ROI for targeting organisations in jurisdictions that did not ban ransom payments. While this is a dynamic field it seems more likely that a ban on ransom payments by Australian organisations would lead to these organisations being targeted less frequently.

The Secretary of the Department of Home Affairs has indicated under questioning that the government's policy towards ransomware payments is "under review". Given this, the government should seek views from industry and cyber security experts give serious consideration to regulating ransomware payments with the objective of reducing the returns of targeting Australian organisations.

Restrictions on the use of cryptocurrency

Another way that government can seek to reduce the returns of ransomware attacks on Australian organisations is targeting the rogue cryptocurrency exchanges that enable ransomware payments.

Cryptocurrencies have been a crucial enabling technology for the growth of ransomware by providing a system for the payment of ransoms that is anonymous and outside existing global payments architecture. The absence of a central organisation controlling cryptocurrencies has made the enforcement of existing 'know your customer' anti-money laundering laws far more challenging in this context.

The central role of cryptocurrency in enabling ransomware attacks was starkly highlighted this question and answer as part of in a recent interview with a ransomware operator,

> *Q: If there were no cryptocurrency, how would that have impacted FonixCrypter? Would it have made it harder to do business?*
>
> *A: Sure. I don't know any other way than cryptocurrency.*

The issue has become significant enough that in her recent confirmation hearings, the US Treasury Secretary, Janet Yellen highlighted concerns about the prevalence of the use of cryptocurrencies to fund cyber crime,

> *"Cryptocurrencies are a particular concern... I think many are used—at least in a transactions sense—mainly for illicit financing."*

Given this, Yellen indicated that she wanted to:

> *"examine ways in which we can curtail their use and make sure that [money laundering] doesn't occur through those channels."*

Recent research from Chainalysis, a cryptocurrency research firm, has found that the bulk of ransomware payments are laundered through a small number of bitcoin wallets. Research from Advintel and HYAS has further suggested that ransomware payments of this kind are further only cashed out into hard currency through a limited number of bitcoin exchanges. This suggests that targeted law enforcement efforts against a small number of strategic points of intervention may have a significant impact on the ability of ransomware crews to transform ransom demands into useable currency (though the experience of law enforcement action against entities like btc-e and eGold before it suggest that this could require continuing efforts as ransomware crews move to different services).

In this context, the Australian government should actively engage with US Treasury, which has already proposed some regulatory actions, to explore ways of cooperating on international efforts to prevent the laundering of ransomware payments through bitcoin exchanges, including the development and enforcement of record keeping rules.

Building resilience against ransomware attacks within Australian organisations

Perhaps the simplest way to reduce the returns of ransomware attacks on Australian organisations is lifting the overall level of resilience of the IT networks of Australian organisations.

As Chris Krebs told a recent Congressional hearing:

> *"to start we have to improve defences… against this ongoing scourge of ransomware."*

As Ciaran Martin argued:

> *"cybersecurity is fundamentally attritional. Hardening defenses doesn't immunize against attack, but over the long haul it yields results."*

Unfortunately, there is evidence that despite the increasing threat of ransomware, Australian organisations are still not appreciating the importance of building the resilience of their networks against this threat.

Private Sector Entities

Amidst the increasing tide of ransomware attacks on US organisations last year, we asked the Parliamentary Library to compare the number of times Australian and US organisations highlighted the risk of 'ransomware' in documents submitted to the Australian Securities Exchange and the US Securities and Exchange Commission in the calendar year 2019. The disparity was stark. Of the 108,334 documents submitted to the ASX, just 24, 0.2 per cent, contained a reference to ransomware. Of the 113,937 documents filed with the SEC, 1,139 contained the term, a rate five times higher than in Australia. These documents included annual reports and their company risk assessments, but ransomware wasn't appearing on their radar.

There is a similar lack of engagement with small and medium business. While the Australian Cyber Security Centre has a series of practical guides for small business on its cyber.gov.au website that if implemented by an SME would make a real contribution to protecting themselves against ransomware attacks, answers to Senate Estimates Questions on Notice in late 2020 indicated that their usage remains low. While there are well over 2 million SMEs in Australia, the ACSC's

Small Business Guide, the most popular document targeted as SMEs had just 46,400 views and 8,500 downloads in just over a year since it was launched.

The Federal Government is not effectively communicating cyber security messages to the private sector entities. Instead of creating webpages, the Federal government should consider putting greater effort into pushing its message out through intermediaries that have existing relationships of trust with SMEs, like bank managers, insurers, industry groups, or local business associations.

In the face of this growing threat, the government needs to do a better job of getting the word out about what Australian private sector companies need to do to protect themselves against this threat.

Commonwealth entities

There is a similar lack of urgency to improve the cyber resilience of Commonwealth government entities. Despite it being mandatory for Commonwealth entities to implement the Australian Signals Directorate's 'Top Four' mitigations since April 2013, the government's own 2019 Cybersecurity Posture Report found that implementation of these baseline measures *"remains at low levels across the Australian government"*. Barely a quarter of Commonwealth entities whose cyber resilience was audited by the ANAO were found to have implemented the Top Four. The situation is so dire that the Auditor-General highlighted these ongoing cyber resilience failures as one of the issues of concern in his agenda setting mid-term report.

The Parliamentary Joint Committee of Public Accounts and Audit's (JCPAA) recent inquiry into the issue found that a lack of accountability was to blame for the these ongoing Commonwealth cyber resilience failures. The bi-partisan final report of the JCPAA's Cyber Resilience inquiry includes a series of recommendations, supported by both Government and Opposition committee members, for driving change in this regard, including that the ANAO be asked to conduct an annual limited assurance review of cyber resilience across all Commonwealth entities.

Agreeing to the recommendations of this bipartisan report would be a good place for the government to start to build the resilience of its own networks against ransomware attacks.

Communicating Australia's National Ransomware Strategy

Given that the objective of such a strategy is to shape the decision making of criminal groups, this strategy should be clearly communicated to the world at large. At a minimum, the responsible Minister, the Minister for Home Affairs, Peter Dutton, should deliver a Ministerial Statement in Parliament outlining the Australian Government's approach. Unfortunately, despite the growing threat of ransomware to the nation, Peter Dutton has never used the word 'ransomware' in the Parliament.

To clearly communicate the intentions of the Australian Government as part of a National Ransomware Strategy, the government should first appoint a dedicated member of the Executive with responsibility for cyber security. This is an important signal to adversaries indicating that the Australian government takes cyber security seriously.

A dedicated Minister provides a chief spokesperson through which the Commonwealth government can articulate its priorities and approach to cyber security. Industry stakeholders such as Telstra, Microsoft, PwC and CISO Lens have all called for a dedicated Minister for Cyber Security to drive policy development and engage with industry.

This Minister would be uniquely placed to support the cyber security industry, drive policy development within government, influence organisations to lift their cyber security and engage in international coalition building.


ON YOUR SIDE.
Labor