MAGELLAN
EXPERTS IN GLOBAL INVESTING

Ransomware is so rife it's a threat to national security

Cracking down on cryptocurrencies might ruin the risk-reward calculation for criminals.

Tobias Vernon of the UK owns two small galleries that sell 20th-century ceramics and artworks. Thanks to marketing efforts, the business has almost 50,000 Instagram followers.[1]

One weekend in May, an email appeared from Instagram congratulating the business for getting a 'blue tick', which bestows on the account 'authentic presence'. Vernon, thrilled, clicked the link in the email and logged in. Not long after, Instagram told Vernon the account's email and username had changed. A message soon appeared: "We have seized control of your Instagram account …We require US$1,000 to grant you your account back."

Vernon eventually paid US$750 in bitcoin to Russians, who released the account. But get this. Three days later, Vernon got an Instagram message from a bakery in Australia that had been hacked by the same group. The baker had been told to contact Vernon for a Tripadvisor-style testimonial that the hackers were trustworthy, so to speak, in that they would release the kidnapped device when paid.

Such traumas are proliferating because the malware-based crime known as ransomware is reaching menacing proportions. Criminally installed encryption that is reversed only by ransom is rising "almost exponentially" in the words of FBI Director Christopher Wray because the virtual private networks that enable working from home have made business systems more vulnerable.[2] US cyber-security firm Mimecast found that 61% of the 1,225 global IT firms it surveyed suffered ransomware attacks in 2020, a 20-point jump from 2019.[3] The Australian Cyber Security Centre, a government agency, said ransomware attacks in Australia rose 15% last financial year to 500 incidents.[4] Global security group, Institute for Security and Technology, estimates 2,400 ransomware victims in the US paid nearly US$350 million in ransom in 2020, a 311% jump in payments from 2019. Ransomware "is an urgent national security risk" because "attacks on the energy grid, on a nuclear plant, waste-treatment facilities … could have devastating consequences," the institute cautioned.[5]

As such warnings signal, ransomware has evolved from a cottage industry into something resembling a "criminal franchising arrangement", according to the Australian Cyber Security Centre.[6] At its most elaborate, the crime starts with hackers who penetrate a network. They then sell these 'keys' to scammers who contact ransomware-as-a-service groups that peddle malware for a percentage of the plunder. The attackers infiltrate systems to make them inoperable, lock out owners and steal data. They demand a ransom to release devices and sometimes threaten to leak stolen data, the virtual world's equivalent to shooting one of the hostages, especially if victims contact law-enforcement authorities.[7] Ransom paid, the victims are sent a 'decrypter key' to unlock their systems that often never operate as well as before, or never work again. Crypto launderers are on hand to hide the criminal origins of ransom payments. Governments hostile to the west protect these thieves who give themselves names such as DarkSide and REvil, shortened from Ransomware-Evil.

Nothing seems safe from virtual kidnappers. Businesses, charities, essential services, governments, hospitals, the military, the police, schools and software providers have suffered what is a paralysing blow to operations. Ireland's health system has been targeted; so too Italy's vaccination booking system and the US Coast Guard. When pursuing healthcare facilities – and 560 in the US were targeted in 2020[8] – the scammers don't seem to care if people die when equipment and surgeries stop. Last October, for example, the University of Vermont Medical Center couldn't treat some chemotherapy patients after a ransomware attack destroyed their records.[9]

Among notable attacks this year, in March, US insurer CNA Financial reportedly paid a then-record US$40 million ransom.[10] In May, ransomware disrupted Colonial Pipeline, which carries 45% of US east coast fuel supplies, for 11 days until a US$$4.3 million ransom was paid for a malfunctioning decrypter key. In July, a ransomware attack on the US-based software company Kaseya was notable for gifting up to 1,500 global victims to the criminals and that the ransom demand was a record US$70 million.[11] The biggest ransomware attack in terms of victims is still the 'WannaCry' one in 2017, when up to 300,000 computers were infected though the criminals received limited payment.[12]

Ransomware is flourishing because the risk-reward calculation favours the attackers. Even if paying ransoms risks reputational damage, what choice do companies have but to pay a government-protected group that might destroy their mission-critical computer system? Paying the ransom, however, often fails as a solution. The Mimecast survey found that 52% of ransomware victims paid the ransom but only 66% of those recovered their data – the others were double-crossed.[13]

To reduce the reward part of the criminal equation, the Australian Cyber Security Centre[14] and the FBI[15] discourage ransom payments. Some people oppose the concept of ransomware insurance (offered by companies now swamped with claims).[16] US sanctions outlaw ransom payments to blacklisted groups such as Russia's cybercriminal Evil Corp.[17] This has prompted some to call for all ransom payments to be illegal. But acceding to the demands of non-virtual crooks is legal and often wise.

The hope is that the risk part of the calculation might increase to the detriment of the scammers because western governments are enhancing and coordinating efforts to stop ransom attacks. Among steps, the White House in May issued an executive order to encourage government and private-sector cooperation on cybersecurity.[18] In July, the US government released a national security memorandum to protect infrastructure from cyberattack.[19] In August, US President Joe Biden hosted Big Tech CEOs and others to tell them to prioritise cyberdefence.

Officials are warning internet users to be better prepared for these attacks. Back up data. Hang onto old hardware in case systems need rebuilding. Use strong passwords and multifactor authentication. Have response plans. Use encryption. Install anti-malware defences. Patch vulnerabilities. Segment networks. Hire skilled security teams and train staff to detect phishing.[20]

Governments are acting because they concede national security is under threat. Proof of this is that in April Biden met Russian President Vladimir Putin and reportedly told his counterpart to rein in ransom criminals and listed the industries that were off limits.[21]

Eradicating the threat seems far off. Computer systems are impossible to secure and it's expensive to try. Phishing emails and other scams too easily trick people into installing malware. Enough employees are willing to sell passwords on the 'dark web'. Perhaps, though, the greatest asset ransomware criminals have is that cryptocurrencies are hard to trace. Many advise that a government crackdown on cryptos is the best way to reduce the menace. The US's unprecedented move in September to blacklist a Russian-owned crypto exchange shows Washington might agree.[22] Something needs to tackle this mobster shakeout for using the web before the damage reaches national-security proportions.

Even if defensive efforts increase, ransomware appears unbeatable when five billion people are connected to the internet. As ransomware is online, the public seems to be unable to come to terms with the magnitude of the threat, which hampers the fightback. It's too true that ransomware would exist even if cryptos didn't. But it might barely register as a danger because how would the criminal be paid? Some victims refuse to pay and the criminals back down. Apple in May declined to pay a US$50 million ransom, as did Dublin when Ireland's health system was stricken. But for some of these non-payers, the recovery costs and wider damage exceeded the ransom. The 'WannaCry' attack emanating from North Korea generated little ransom for the attackers but according to the world's anti-laundering body caused an estimated US$8 billion in damages to hospitals, banks and businesses across the world.[23]

Such calculations show that the ransomware threat needs to be taken much more seriously. The non-virtual world provides the clue to defeating the menace. Kidnapping is a rare crime nowadays because the police caught kidnappers when they spent the cash. The solution to ransomware might be to regulate cryptocurrencies, possibly – as is the intention of China's ban on crypto activities – to the point where they are unviable.

CRIMINAL TOOL

On September 7, El Salvador became the first country in the world to accept bitcoin as legal tender (along with the US dollar). Allowing people to shop for everyday items and pay taxes with the cryptocurrency marketed under the local name for cool (Chivo) was beset with teething problems, especially given that most Salvadorans don't have internet access. The government-run bitcoin e-wallet went offline for hours and didn't appear on major app stores. Many people were unable to sign up as users. Others demonstrated against bitcoin's use. The value of bitcoin dived more than 10% on the day, where a shift in bitcoin's value is a liability for the government.[24]

While most of the start-up hitches will be overcome, the experiment could fail for many reasons including that most locals seem against the idea. One looming problem for El Salvador if bitcoin use were to become extensive is the Financial Action Task Force, an intergovernmental body created to combat money laundering, might blacklist the country, which would be a blow to its financial sector. The task force is concerned about bitcoin because its design makes it hard for operators to comply with global 'know your customer' rules imposed to combat the money laundering that enables terrorism and cybercrimes such as ransomware. These know-your-customer rules mean financial intermediaries must know the true name of their users, monitor their transactions and report suspicious activities to authorities. Even with these rules, the UN estimates that US$2 trillion is laundered each year.[25]

Cryptos are making it easier to launder money. It's no coincidence that ransomware has boomed as cryptocurrencies soared in popularity. The borderless, decentralised and anonymous nature of bitcoin transactions means no trusted third party such as a central bank, bank or payments company is involved; 'decentralised finance', or 'DeFi', does away with these third parties and DeFi players boast how they do not care who their customers are.[26] Such attitudes have allowed ransomware criminals who demand payment in bitcoin to designated wallets to develop techniques that cloud the source of their funds.

The 'chainhopping' technique entails exchanging the bitcoin loot for other cryptos via any number of crypto exchanges. 'Tumbler' or 'mixing' services blend legitimate and ill-gotten cryptocurrencies before redistributing them. Further obscurity can be gained by using 'money-mule' service providers who set up accounts with false or stolen credentials. Some ransomware criminals demand ransoms be paid in 'privacy coins' – cryptos such as Dash, Monero and Zeash that make payments untraceable.[27] One technique is to use 'ring signatures' where so many parties sign a transaction no one knows which party initiated it.[28]

To be sure, in some ways, the blockchain makes it easier to track cryptos than it is to trace physical cash. But there are too many ways it doesn't. In a victory against ransomware criminals, the US government tracked and retrieved much of the bitcoin ransom paid to the DarkSide ransomware group behind the heist of Colonial Pipeline.[29] Such successes for law enforcement officials, however, will likely only make ransomware criminals refine how they hide their spoils.

Western governments do have options if they want to change the risk-reward equation against ransomware scammers. A first step would be to widen know-your-customer and anti-money-laundering laws to include crypto exchanges. The

next move would be to sanction crypto exchanges that fail to meet standards – as the US Department of the Treasury did in September when it banned US citizens and companies from transacting with the Russian-controlled SUEX OTC digital currency exchange. The next step for authorities would be to deny foreign banks and crypto exchanges access to the global US-dollar-based banking system unless they show they are equipped and willing to expose digital ransoms. This is a potent threat because much crypto is exchanged for cash. If these steps fail, western governments could even become aggressive online to disrupt ransomware groups. Officials could hack the servers enabling cryptocurrencies such that they can't function. (Private companies cannot legally hack back at criminals.) Another option for western governments is to pressure the countries that house cybercriminals.[30] They could follow China's lead: Beijing in September listed money laundering as one of the many reasons it expanded its crackdown on cryptos by declaring all activities related to digital coins are "illegal".[31]

Such actions might mean the world loses the (disputed) benefits of cryptocurrencies. But that's part of the cost-benefit analysis governments need to undertake to defeat the scammers that hound legitimate users of the internet, be they UK gallery owners or bakers in Australia.

By Michael Collins, Investment Specialist

[1] Tobias Vernon. 'Phishing trip.' 7 August 2021. The Spectator. spectator.co.uk/article/i-was-held-to-ransom-by-hackers

[2] Axios. 'FBI director says cyber threat is increasing 'almost exponentially' 10 June 2021. https://www.axios.com/fbi-director-warns-cybersecurity-6678e54c-560d-4f41-b556-9c95c1fd78e4.html

[3] Mimecast report. '61% of organisations were infected with ransomware in 2020.' 20 April 2021. mimecast.com/resources/press-releases/dates/2021/4/the-state-of-email-security-report/

[4] The Australian Cyber Security Centre. 'ACSC annual cyber threat report'. 1 July 2020 to 30 June 2021. Page 30 of pdf version. cyber.gov.au/acsc/view-all-content/publications/acsc-annual-cyber-threat-report-2020-21

[5] Institute for Security and Technology. RTF report: Combatting ransomware. securityandtechnology.org/ransomwaretaskforce/report/. Dollar amounts on page 7 of the report.

[6] The Australian Cyber Security Centre. Op cit. Page 31

[7] NBC News. 'the battle between the US and ransomware hackers is escalating.' 22 September 2021. nbcnews.com/tech/security/battle-us-ransomware-hackers-escalating-rcna2129

[8] Institute for Security and Technology. Op cit.

[9] 'Patients of a Vermont hospital are left 'in the dark' after a cyberattack.' The New York Times. 26 November 2020. nytimes.com/2020/11/26/us/hospital-cyber-attack.html

[10] Bloomberg News. 'CNA Financial paid $40 million in ransom after March cyberattack.' 21 May 2021. bloomberg.com/news/articles/2021-05-20/cna-financial-paid-40-million-in-ransom-after-march-cyberattack

[11] Reuters. 'Up to 1,000 businesses affected by ransomware attack, US firm's CEO says.' 6 July 2021. Schools in New Zealand were closed and tills at Sweden's Coop grocery chain stopped working. reuters.com/technology/hackers-demand-70-million-liberate-data-held-by-companies-hit-mass-cyberattack-2021-07-05/

[12] BeforeCrypt, ransomware experts. 'The biggest ransomware attacks ever: Top 10 biggest ransomware payments.' 19 June 2021. beforecrypt.com/en/biggest-ransomware-attacks-ever/

[13] Mimecast. Op cit.

[14] The Australian Cyber Security Centre. Op cit. Page 31.

[15] 'The FBI does not support paying a ransom.' See FBI website. Scams and safety. 'Ransomware'. Undated. fbi.gov/scams-and-safety/common-scams-and-crimes/ransomware

[16] See 'Surge in hacking claims forces ransomware insurers to weigh risks.' 6 June 2021. The Telegraph. telegraph.co.uk/business/2021/06/06/time-stop-paying-ransoms-get-hackers-companies-backs/

[17] US Department of the Treasury. 'Treasury sanctions Evil Corp, the Russia-based cybercriminal group behind Dridex malware.' 5 December 2019. home.treasury.gov/news/press-releases/sm845#

[18] The White House. Executive order on improving the nation's cybersecurity.' 12 May 2021. whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

[19] The White House. 'National Security memorandum on improving cybersecurity for critical infrastructure control systems.' 28 July 2021. whitehouse.gov/briefing-room/statements-releases/2021/07/28/national-security-memorandum-on-improving-cybersecurity-for-critical-infrastructure-control-systems/

[20] US government. Cybersecurity & Infrastructure Security Agency. 'Ransomware guide.' September 2020. https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C.pdf

[21] The White House. 'Readout of President Joseph R. Biden, Jr. call with President Vladimir Putin of Russia.' 13 April 2021. whitehouse.gov/briefing-room/statements-releases/2021/04/13/readout-of-president-joseph-r-biden-jr-call-with-president-vladimir-putin-of-russia-4-13/

[22] US Department of the Treasury. 'Treasury takes robust actions to counter ransomware.' Media release. 21 September 2021. home.treasury.gov/news/press-releases/jy0364

[23] Financial Action Task Force website. 'Virtual assets.' gafi.org/publications/virtualassets/documents/virtual-assets.html

[24] See WIRED. 'El Salvador's bitcoin gamble is off to a rocky start.' 7 September 2021. wired.com/story/el-salvador-bitcoin-rocky-start/

[25] UN. Office on Drugs and Crime. 'Money laundering.' unodc.org/unodc/en/money-laundering/overview.html

[26] See 'Cryptocurrency: Rise of decentralised finance sparks 'dirty money' fears.' 15 September 2021. ft.com/content/beeb2f8c-99ec-494b-aa76-a7be0bf9dae6

[27] Institute for Security and Technology. Op cit. Page 14.

[28] See Vinc Breaker. 'Identity hiding ring signatures zero knowledge proof.' 27 March 2020. vincbreaker.me/2020/03/27/IHRSZKP/

[29] Bloomberg News. 'Colonial Hackers Broke the Fundamental Bitcoin Rule.' 8 June 2021. bloomberg.com/opinion/articles/2021-06-08/colonial-hackers-led-the-fbi-down-a-hot-wallet-trail-to-bitcoin-ransom

[30] See Paul Rosenzweig, consultant on cybersecurity. Guest essay. 'There's a better way to stop ransomware attacks.' The New York Times. 31 August 2021. nytimes.com/2021/08/31/opinion/ransomware-bitcoin-cybersecurity.html

[31] Financial Times. 'China expands crackdown by declaring all crypto activities 'illegal''. 24 September 2021. ft.com/content/31f7edf7-8e05-46e1-8b13-061532f8db5f

info@magellangroup.com.au +61 2 9235 4888