Australian Government

AUSTRAC

DETECTING AND REPORTING

RANSOMWARE

FINANCIAL CRIME GUIDE

APRIL 2022

COPYRIGHT

© Commonwealth of Australia 2022
All material presented in this publication is provided under a Creative Commons Attribution 4.0 International licence.

For the avoidance of doubt, this means this licence only applies to material as set out in this document.

The details of the relevant licence conditions are available on the Creative Commons website as is the full legal code for the CC BY 4.0 licence (creativecommons.org/licenses).

USE OF THE COMMONWEALTH COAT OF ARMS

The terms under which the Coat of Arms can be used are detailed on the It's an Honour website (pmc.gov.au/government/its-honour).

CONTENTS

HOW TO USE THIS FINANCIAL CRIME GUIDE

AUSTRAC has developed this financial crime guide to help businesses understand and identify the signs of ransomware attacks in Australia. The indicators and behaviours in this financial crime guide can be used by financial services businesses to review their profiling and transaction monitoring programs, to target, identify and stop transactions associated with ransomware attacks. Financial services businesses have a crucial role in protecting Australians against ransomware by understanding the financial indicators of this crime type and reporting suspicious financial activity to AUSTRAC.

No single financial indicator will be a definitive way to identify if an entity is involved with ransomware. Financial services businesses should use a combination of indicators and business knowledge to monitor and identify potential suspicious activity. Where suspicious activity is identified, enhanced customer due diligence should be conducted in accordance with the business's anti-money laundering and counter-terrorism financing (AML/CTF) program.

The intelligence and information shared by financial services businesses is critical in helping AUSTRAC and government partners protect the community and Australia's financial system from criminals.

ABOUT FINANCIAL CRIME GUIDES

Financial crime guides provide information about the financial aspects of different crime types. They include case studies and indicators that can be used to identify if this offending could be occurring.

They are developed in partnership with relevant government agencies and our industry partners.

SUSPICIOUS MATTER REPORTING (SMR):

If you identify possible ransomware or other criminal activity through financial transactions and determine you need to submit an SMR; including clear transactional, behavioural and non-financial indicators in your report will help AUSTRAC and our law enforcement partners respond and take action.

INTRODUCTION

Ransomware is a serious cyber threat. The Australian Cyber Security Centre (ACSC) reports that in the 2020-21 financial year, there were almost 500 reports of ransomware attacks – an increase of around 15 percent from the previous year.[1] Ransomware continues to evolve and adapt to the changing environment it operates in.

Digital currencies such as Bitcoin have enabled cybercriminals to request higher ransom amounts and more easily receive payments, increasing the profitability and attractiveness of ransomware. Ongoing developments in technology, methodology and new tactics have also contributed to the increasing popularity of ransomware among cybercriminals and a rise in the number of ransomware attacks.

An early form of ransomware was first seen in 1989 when malware was installed on computers via floppy discs and victims were instructed to make payment via mail. Over time, ransomware evolved and the first modern version (involving the use of PGPCoder, a Trojan that encrypts files) appeared in 2005.

The widespread adoption of working, shopping and learning remotely has provided even more opportunities for cybercriminals to use ransomware. Cybercriminals are continually adapting to evolving technologies, becoming more sophisticated and resourceful.

Financial services businesses have an important role to detect and report financial flows related to ransomware and stop ransomware payments, because they are a key point where criminals interact with the legitimate financial system.

AUSTRALIA'S RANSOMWARE ACTION PLAN

Australia's national ransomware action plan provides information on how Australia is responding to the threat of ransomware and where victims can go for help. It provides valuable information and should be read in conjunction with this financial crime guide.

Read the action plan: homeaffairs.gov.au/about-us/our-portfolios/cyber-security/strategy/australias-ransomware-action-plan

1 cyber.gov.au/acsc/view-all-content/reports-and-statistics/acsc-annual-cyber-threat-report-2020-21

OVERVIEW OF RANSOMWARE

Ransomware is a type of malicious software (malware) that can encrypt files and render a victim's computer unusable. Cybercriminals try to infect a computer or network with this malware, and then demand a ransom to unlock or decrypt the victim's files. Payment is usually demanded in digital currency such as Bitcoin.

Businesses and organisations that fall victim to ransomware often fail to report this to police or agencies like the ACSC. This may be due to fear of damaging their reputation, losing customers, the impact on their revenue, or compliance action from the government. There is also no guarantee that the payment will lead to data being recovered, prevent information from being on-sold to other criminals, or that victims won't be attacked again. Each ransomware payment incentivises cybercriminals, perpetuates the crime, and puts other Australian organisations at risk.

To improve their chances of success and profitability, criminals have adopted the following strategies:

- Targeting large organisations (known as 'big game hunting') to demand larger ransom payments.
- Forming partnerships with other cybercriminals, to share resources and expertise.
- Double extortion, by not only encrypting data and demanding a ransom, but also threatening to publish the data. This threat is often followed through, and sensitive data is uploaded to dedicated leak sites, allowing other cybercriminals to steal personal information.
- Requesting payment in digital currencies that are harder to trace (known as privacy coins) to obscure ransomware payments.
- Operating via Ransomware as a Service (RaaS) business models, using malware provided by other cybercriminals for a fee.

HOW A COMPUTER MIGHT BE INFECTED WITH RANSOMWARE

Ransomware can be deployed in a number of ways, including:

- Remote Desktop Protocol (RDP) that is not protected from the internet.
- Infected USB sticks that pass on and install malware on between machines.
- Taking advantage of vulnerabilities in unpatched software (known as exploits).
- Victims unknowingly visiting infected websites and becoming infected with malware.
- Pirated software that has malware added, which is then installed on a computer by a user.
- Phishing emails that entice victims to open attachments or click links which launch the malware.
- 'Malvertising' where a cybercriminal rents ad space on a website, luring a victim to click on an advertisement. The ad is linked to a hacking toolkit known as an 'exploit kit', which scans the victim's machine for a vulnerability, installing ransomware if possible.

Malware - Software that is specifically designed to disrupt, damage, or gain unauthorised access to a computer system.

Remote Desktop Protocol (RDP) - A network communications protocol developed by Microsoft which provides a user with remote access to their physical work desktop computers.

RANSOMWARE TYPES

The most common types of ransomware:

Crypto ransomware - encrypts files within a system but doesn't disable basic computer functions.

Lockers - locks basic computer functions, rendering it inoperable. Complete destruction of data is unlikely.

Scareware - a fake software claiming to have detected a virus and demanding a payment to fix the issue.

AN ORGANISED CRIME: THE RANSOMWARE ECOSYSTEM

Ransomware exists in a symbiotic ecosystem. Even people with very little experience in coding or cybercrime can access all the services and tools required to carry out a ransomware attack on the darknet. These include:

- **Ransomware as a Service (RaaS**) - a business model increasingly used by cybercriminals, where ransomware administrators or creators charge a fee to affiliates for the use of their malware and may take a percentage of earnings from successful attacks. RaaS administrators will also support affiliates seeking further assistance during the process.
- **Infrastructure as a Service** - a third party will provide the cybercriminal with the infrastructure required to carry out a ransomware attack, such as email services or domain registration services that provide the cybercriminal with anonymity on the network.
- **Access as a Service** - offers cybercriminals network access to an already compromised machine or network.
- **Exploit kits** - assist in scanning networks for vulnerabilities, providing an entry point into the machine.
- **Post-attack services** - employees of ransomware administrators will assist victims through the payment process.

THE RANSOMWARE PAYMENT CYCLE

FLOW OF FUNDS

Following the money trail of ransomware is difficult. Cybercriminals use many methods to try and conceal the origin and destination of ransomware payments before the digital currency arrives at the final wallet under their control.

A wallet, or virtual wallet, is a collection of private keys and corresponding addresses (which enable the transfer of digital currency) under the control of an entity. Some of the ways criminals try and conceal their payments include:

- Use of privacy coins. Privacy coins are digital currencies that provide enhanced anonymity by obscuring the amount, destination and origin of transactions.
- Chain-hopping. This is where one digital currency is exchanged for another. The digital currency is moved from one blockchain to another, hence the term 'chain-hopping'.
- Directing a ransomware payment via multiple intermediary digital currency addresses, exchanges and mixers. Mixers increase anonymity by mixing the customer's digital currency with the transactions of others before being redirected back to the customer.
- Use of mule accounts. A mule account is created using a stolen or fake identity or, a legitimate account held by another party who is complicit in its use.

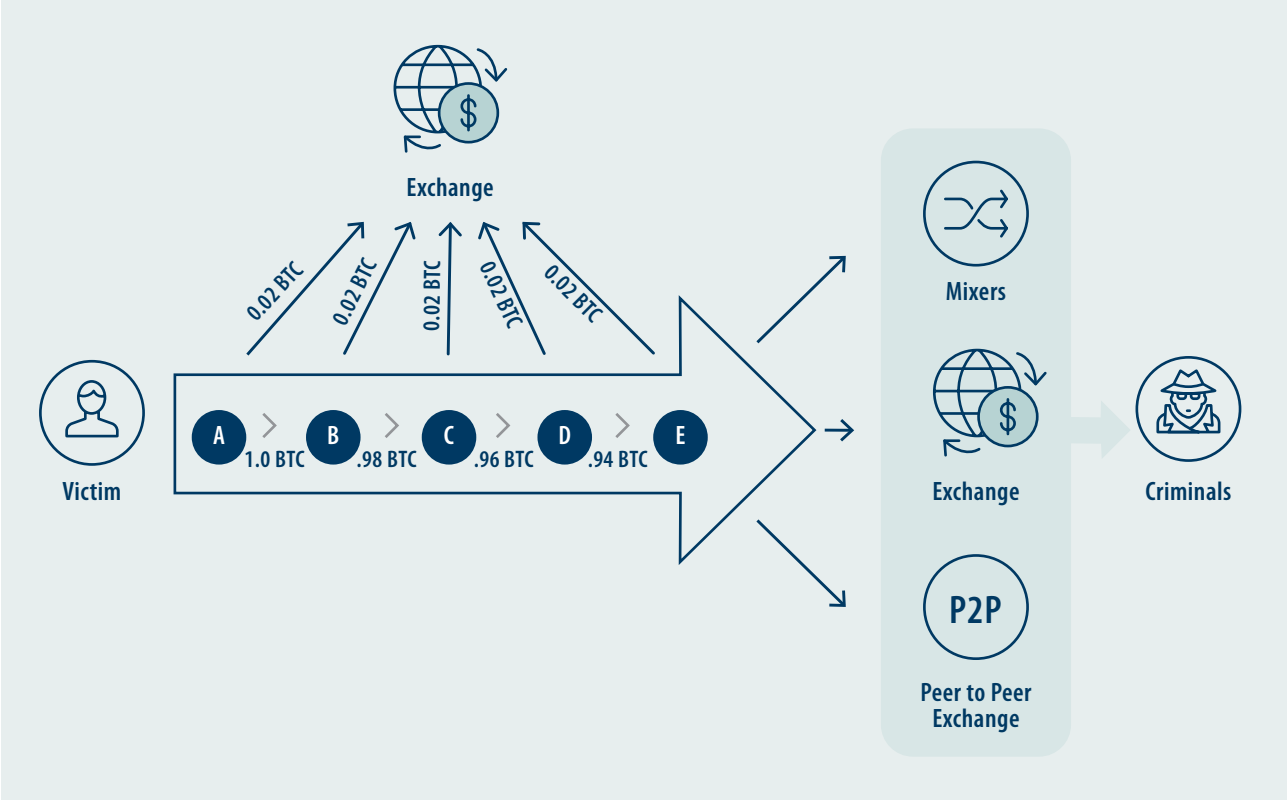
OBSCURING THE FLOW OF FUNDS FROM A VICTIM TO THE CYBERCRIMINAL

Cybercriminals will use sophisticated methods to try and obscure the true ownership and flow of funds. In the example below, wallet addresses 'B', 'C' and 'D' are part of a peel chain. A 'peel chain' is a transaction pattern created when a large amount of cryptocurrency is sent through a series of transactions. In each of these transactions, a small amount of the funds 'peels off' this chain of transactions to another address, typically held with a digital currency exchange. The goal is to make it difficult to tell where the funds originated.

This is a common method of trying to distance someone from the final wallet address.

1. The victim is instructed to pay the ransom in a digital currency such as Bitcoin (BTC), to wallet address **A**. This wallet may have been created by the cybercriminal in another person's name.
2. The BTC from wallet **A** is sent to wallets **B**, **C** and **D**, and finally wallet **E**. Each of these wallets is controlled by the cybercriminal or their associates.
3. The cybercriminal sends the BTC to one or more other exchanges (often exchanges perceived to have weak or no know your customer (KYC) controls), mixers and peer-to-peer (P2P) exchanges to further obscure the money trail.
4. Finally, the cybercriminal will receive the BTC. They often receive this into a private wallet, or cash out the BTC using multiple exchanges and services.

Simple money trail example when viewed through blockchain analysis software:



At each stage of the process, criminals will often try to select a digital currency exchange they perceive to have weak KYC and AML controls. They may also use private wallet addresses that do not have KYC or identity verification safeguards. They will cash out their digital currency using services which are less likely to report suspicious activity, such as exchanges they perceive as weak, P2P exchanges or gambling services.

Cybercriminals may use part of the ransom they receive to pay for services that helped them carry out the ransomware attack, such as RaaS administrators and Post-Attack services.

Peer-to-peer (P2P) exchange - A platform that allows users to trade directly with each other and negotiate a price for the digital asset they are selling or buying.

THE ROLE OF DATA RECOVERY FIRMS AND INSURANCE COMPANIES

Data recovery firms have become increasingly popular, alongside the rise of ransomware. They exist as an intermediary between victim and cybercriminal, primarily to assist with decryption of files but also as negotiators. While their services play an important role in the ransomware landscape, their existence may also have the effect of enabling ransomware, funding other crimes and, like any other industry, be vulnerable to exploitation.

Cyber insurance companies may cover ransomware incidents and many offer financial incentives to encourage strong cybersecurity practices. However, similar to the dual nature of data recovery firms, ransom payments from insurance may be used to fund other crimes.

FINANCIAL INDICATORS

VICTIM

TRANSACTIONS AND ACCOUNTS

- A customer increases the limit on their account and then quickly sends funds to a third party.
- A business that would not normally be expected to transact in digital currency is attempting to do so.
- A customer seems anxious or impatient with the time taken to make a large outgoing payment.
- A transaction occurs between an organisation and a data recovery firm or cyber insurance company.
- Customer seems overly concerned with the speed of a transaction and or withdrawal approvals.
- Following an initial large digital currency transfer, a customer has little or no further digital currency activity.
- Customer's digital currency account is linked to or funded by multiple bank accounts at several different institutions.
- A customer's digital currency address has sent funds to a ransomware address identified in the media or open source.
- A business customer's operations appear to have changed significantly, e.g. no longer transacting, operations have come to a halt, significantly downsizing.
- A newly on-boarded customer wants to make an immediate and large purchase of digital currency, followed by an immediate withdrawal to an external digital currency address.

BEHAVIOURAL AND ON-BOARDING

- A customer says that their transaction is in response to a cyber-attack.
- A customer is evasive when asked about the reason for their transaction.
- A customer shows little knowledge of digital currency during on-boarding.
- The customer has been reported in the media as being subject to a ransomware attack.
- Customer mentions an "adviser" or that they are being assisted to purchase cryptocurrency.

RANSOMWARE CYBERCRIMINAL

BEHAVIOURAL AND ON-BOARDING

- Verification information is a photograph of data on a computer screen.
- IP addresses match other accounts operated by the exchange/service.
- Customer's language or syntax does not match the customer's demographic.
- Customer presents ID or images with a file name containing "WhatsApp image" or similar
- Publicly available information or World-Check indicates the customer is known to law enforcement.
- KYC information shows the customer holds an email account known for high privacy such as Tutanota or Protonmail.
- Inconsistent identification details or an attempt to create an account with a false identity.
- Images of ID appear to be kept in a holder or wallet, indicating the person may be trying to hide that the ID is a single sheet of paper.
- Accounts that appear to have the characteristics of a mule account, such as multiple accounts linked to the same contact details, addresses shared under different names, or customers saying they are transacting for someone else.
- The customer appears to use a Virtual Private Network (VPN). VPNs provide online privacy and anonymity by creating a private network from a public internet connection. VPNs mask a user's IP address and establish a secure, encrypted connection.

BLOCKCHAIN ANALYTIC SOFTWARE

Blockchain analytic software are tools that can be used to follow and examine digital currency transactions and addresses. This software also provides tools to further investigate entities linked through addresses. Businesses may consider using blockchain analytic software to enhance their ability to monitor transactions. Some indicators you could identify using blockchain analytic software include:

- If a customer's digital currency address is directly linked to a known ransomware address.
- If a customer's digital currency address is indirectly linked to a known ransomware address, particularly where there is evidence of a peel chain towards the cluster. A cluster is a collection of addresses which blockchain analytic software determines are controlled by one entity and likely to be part of the same wallet.
- A customer uncharacteristically sends a large amount of digital currency to an unrelated address and this digital currency ends up at a mixer or high-risk exchange.
- A customer's addresses show high exposure to high-risk exchanges, mixing services, peer-to-peer exchanges, scam activity clusters, fraud shops, and gambling services, but in contrast, low exposure to more legitimate exchanges and services.

REPORTING RANSOMWARE RELATED PAYMENTS

Victims are often reluctant to report an attack and simply want to regain access to their machines and data to resume business.

Where possible, encourage your customers to report ransomware incidents to the ACSC's ReportCyber service and law enforcement. Where possible, businesses should seek further information from these customers and any others that disclose their transactions relate to ransomware payments. Including the following information in your reports related to ransomware transactions will aid further investigation by AUSTRAC and law enforcement agencies:

- Any images or copies of ransom notes.
- Business name of the victim.
- Time and date of payment if successful.
- Unique identifiers such as the user's device ID.
- Transaction hash for the ransomware payment.
- IP address used at the time of the ransomware payment.
- Wallet addresses given to the customer by the cybercriminal.
- Whether the customer reported the incident to ReportCyber or police.
- The name of the data recovery firm used by the customer if applicable.
- Wallet address of the customer who has made the ransomware payment.
- Software and device information such as the operating system or browser.
- Potential links to other businesses or individuals via compromised computer.
- Screenshots taken at any stage of the ransomware incident by victim/customer.
- Use of the term 'ransomware' in the 'grounds for suspicion' and or 'reason for suspicion' fields.
- Contact details that the customer has for the perpetrator (e.g. contact email/ telephone number).

CONTACT THE AUSTRALIAN CYBER SECURITY CENTRE

To report a ransomware attack or another cyber threat, and for help and advice on what to do, visit the ACSC at cyber.gov.au.

You must still submit an SMR for any suspicious activity, even if you are reporting the incident to another agency such as the ACSC.

CASE STUDY 1: RANSOMWARE EVIL

REvil (short for Ransomware Evil), also known as Sodinokibi, is a type of RaaS, 'leased' to affiliates wishing to carry out an attack. Once criminal affiliates have infiltrated a network, stolen as much data as possible and gained administrative access, REvil is deployed and a ransom demand is made. REvil affiliates typically use double extortion, threatening to post the data on a dedicated website called *Happy Blog*.

In May 2021, affiliates using REvil attacked JBS, the world's largest meat processing company. The ransomware affected servers supporting North American and Australian IT systems, bringing JBS's operations to a halt. The shut-down saw temporary lay-offs at some plants in Australia and farmers reported that shipments of livestock were cancelled. JBS's back-up servers were not affected and, with the assistance of a cybersecurity firm, operations resumed within a few days. Despite this, JBS elected to pay a $14.2 million ransom in Bitcoin to avoid unforeseen implications and data extortion.

In July 2021, REvil's website and *Happy Blog* shut down, vanishing from the internet and leaving many victims unable to recover their data.

CASE STUDY 2: WANNACRY

In May 2017, the ransomware WannaCry infected more than 230,000 computers in 150 different countries. The malware used took advantage of weaknesses in the Microsoft Windows operating system using a hack known as EternalBlue.

The perpetrators demanded $300 worth in Bitcoin, later increasing this to $600, and threatened to delete all files on the victim's system, if payment wasn't received. Some victims chose to pay the ransom. It is unknown exactly how many victims were able to recover their data.

The WannaCry ransomware campaign was estimated to have collectively cost victims $4 billion and dangerously impacted the health system, particularly in the UK where ambulances were rerouted, leaving people in need of urgent care.

Using financial intelligence from financial services businesses, AUSTRAC used specialised tools to provide the Australian Government with intelligence regarding the financial impact of WannaCry.

REPORTING SUSPICIOUS BEHAVIOUR

Observing one of these indicators may not suggest illegal activity on its own. If you see a combination of indicators or observe other activity that raises suspicion, submit a suspicious matter report to AUSTRAC when appropriate.

High-quality, accurate and timely SMRs give us the best chance to detect, deter and disrupt ransomware attacks and other criminal activity.

To find out more visit: austrac.gov.au/smr

FOR MORE INFORMATION

If you have questions about your AUSTRAC compliance obligations, please email contact@austrac.gov.au or phone 1300 021 037.

If you see something suspicious and report it to police, you must also report it to AUSTRAC. You must submit an SMR to AUSTRAC if you suspect on reasonable grounds that a customer is not who they claim to be, or the designated service relates to terrorism financing, money laundering, an offence against a Commonwealth, State or Territory law, proceeds of crime, or tax evasion.

AUSTRAC.GOV.AU

1300 021 037

contact@austrac.gov.au