

certnz

Quarterly Report



April - June 2017

EXECUTIVE SUMMARY

Welcome to the first quarterly report from CERT NZ.

The threat of cyber attack is real and growing. CERT NZ is a government-backed specialist cyber security unit dedicated to gathering information on cyber threats and incidents in New Zealand and overseas. We offer advice and assistance to organisations and the public on how to avoid and manage cyber risks.

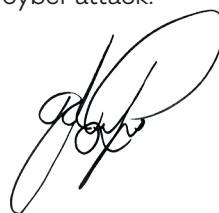
Since our launch on 11 April 2017, we have analysed some significant trends in local cyber security data:

- There have been a total of 364 cyber incidents reported to CERT NZ by New Zealand individuals and organisations.
- Many of these incidents were phishing attacks – 96 incidents or 34% of the total. Phishing consists of email, text, or website attacks designed to convince users they are genuine, but end up tricking them into giving up information, their credentials, or their money.
- New Zealanders have suffered financial losses totalling more than \$700,000 due to cyber security incidents in the last three months alone, according to the reports we have received.
- The international ransomware attack WannaCry led to a big spike in reports of ransomware attacks in mid-May – but WannaCry only accounted for six of these reports in New Zealand.

Ransomware is an increasingly common cyber threat – malicious software that encrypts all the data on your computer and then demands a ransom for decryption – and we have included a special section at the end of this report to provide more insight into its effects in New Zealand.

If you or your organisation experiences a cyber security threat – or if you suspect you may have been exposed to one – contact CERT NZ via www.cert.govt.nz any time or call **0800 CERT NZ** from 7am to 7pm, Monday to Friday.

We're here to help you protect yourself and your business and help you respond if you find yourself under cyber attack.



Rob Pope
Director, CERT NZ

“ There have been a total of **364** cyber security incidents reported by New Zealand individuals and organisations. ”

INTRODUCING CERT NZ

CERT NZ is a new government organisation established to improve cyber security in New Zealand.

What does 'CERT' stand for? A CERT is a Computer Emergency Response Team, an expert group of people that handles cyber security incidents. There are more than 100 CERT organisations worldwide and now New Zealand has its own, CERT NZ, the world's newest CERT, which launched on 11 April 2017.

Who we are and what we do

CERT NZ is a specialist cyber security unit and part of the Ministry of Business, Innovation and Employment (MBIE). We gather information on cyber threats and incidents in New Zealand and overseas, and advise businesses of all sizes and the public on how to avoid and manage cyber security risks.

If any individual or organisation needs to report a cyber security problem, we are a first port of call via www.cert.govt.nz or through 0800 CERT NZ. Our team of cyber security experts will look into the incident, provide advice, and, if necessary, refer it to another agency such as NZ Police or Netsafe with the customer's consent. CERT NZ also works with other government agencies to refer and respond to cyber security threats where appropriate, including the Department of Internal Affairs and the National Cyber Security Centre.

We also report on threats by analysing international incidents and trends, track and analyse local data, co-ordinate multi-agency responses to cyber threats and incidents, and generally raise awareness of cyber security and best practice in New Zealand.

What is in this report?

Although we have only been in operation since April, we are already building a picture of the cyber threat landscape specific to New Zealand. Even at this early stage, we have seen some interesting trends in the data that we want to share in this report. This report is the first in what will be a regular reporting series providing updates and analysis about the latest cyber security trends from our sources and partners, in New Zealand and around the world.

A word about information

This report is based on a small set of data gathered during a short period of time and is drawn from incidents reported by individuals and organisations. This places some limits on the information we can share.

When people report incidents to us, the details can be sensitive, so we only gather the information they feel comfortable providing. Sometimes CERT NZ may ask for more information about an incident to gain a better understanding or to perform technical investigations. Before sharing specific details about any incident, CERT NZ seeks consent from whoever reported it.

Because of these limitations and sensitivities, we are not always able to verify all the information we receive, although we endeavour to. All information provided to CERT NZ is treated in accordance with our Privacy and Information statement¹, which is published on our website. This report is subject to the CERT NZ standard disclaimer².

Incident reporting to CERT NZ

Anyone can report a cyber security incident to CERT NZ, from IT professionals and security personnel to members of the general public, businesses, and government entities. We also receive incident notifications from our international CERT counterparts when they identify affected New Zealand organisations in their investigations.

¹ <https://www.cert.govt.nz/about/privacy-and-information-statement/>

² <https://www.cert.govt.nz/about/disclaimer/>

RESULTS

In the first three months of reporting CERT NZ saw 364 incidents reported across the country. These incidents varied from highly publicised ransomware to scam and fraud cases. Phishing was the most common with 96 individual incidents.

Breakdown by response: all reported incidents

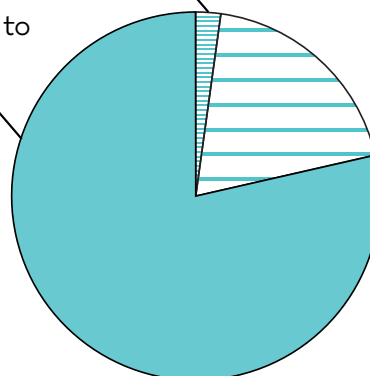
364

Incident reports received for the 11 April – 30 June 2017 period.

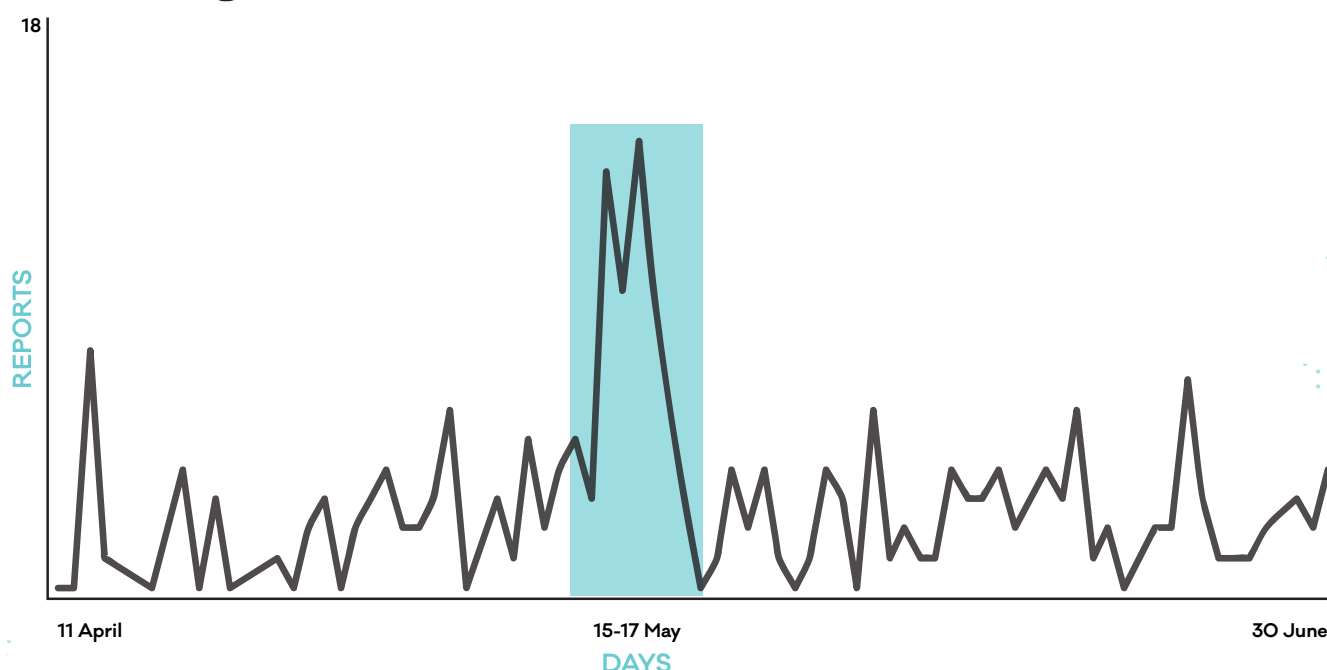
8 reports referred to Netsafe

286 reports responded to directly by CERT NZ

70 reports referred to NZ Police



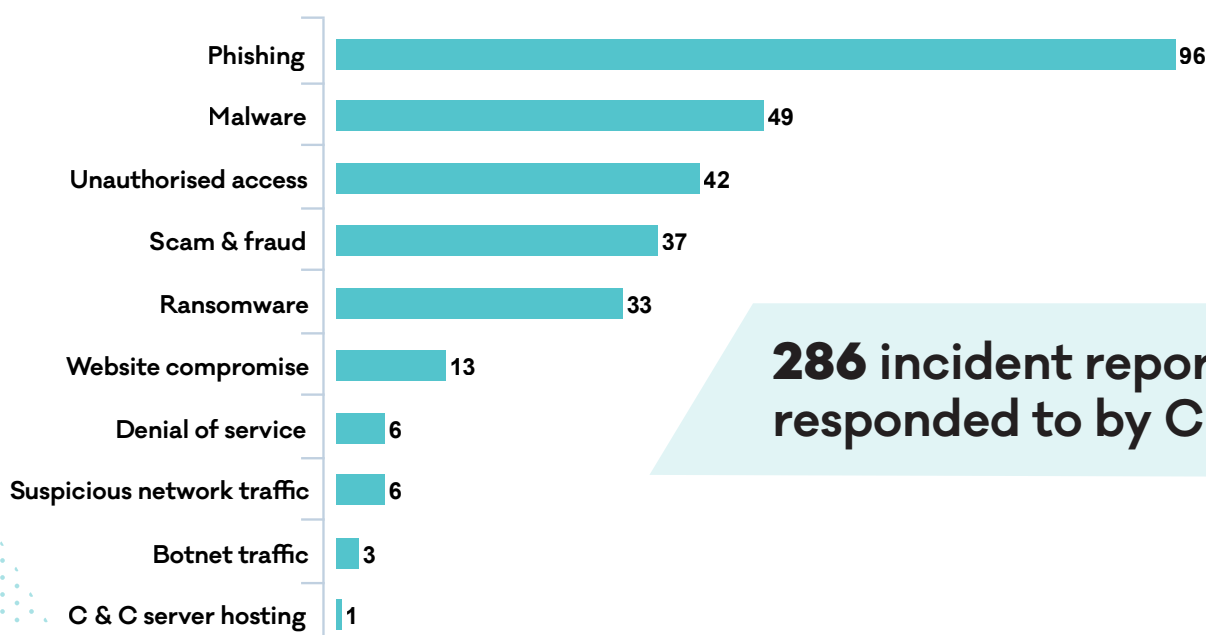
Reporting spike in May



We noticed a big increase in the volume of reports from 15 to 17 May. This reporting spike immediately followed the WannaCry ransomware event that occurred on 13 and 14 May (in New Zealand). While the incident received significant global coverage, CERT NZ received only 6 incident reports of WannaCry infections at the time. However, during that week we received an increase in other incidents reported, including 12 other ransomware incidents.

Interestingly, in the two weeks following WannaCry, no ransomware reports were received. This may be the result of 'reporting fatigue' of ransomware issues, or, it may indicate that heightened public awareness of the ransomware threat resulted in fewer infections. We will continue to report on and analyse these kinds of trends to identify their root causes.

Breakdown by category: incidents CERT NZ responded to directly



286 incident reports were
responded to by CERT NZ

Incident categories

These are the broad categories that we currently group incident reports into. We will continue to refine these categories as our data set grows.

Phishing

Phishing is a type of email scam. The sender pretends to be a trustworthy organisation — like a bank or government agency — in an attempt to get you to provide them with personal information, particularly financial details.

Malware

Malware refers to any kind of malicious software designed to damage or harm a computer system.

Unauthorised access

The term 'unauthorised access' describes the act of directly — or indirectly — accessing information online without authorisation.

Scams & fraud

Online scams are intended to manipulate or trick people into giving away their personal details, financial details, or money.

Ransomware

Ransomware is a type of malicious software that denies a user access to their files or computer system unless they pay a ransom.

Website compromise

When websites are compromised, defaced, or exploited by attackers for malicious purposes, such as spreading malware to unsuspecting visitors.

Denial of service

Denial-of-service (DoS) attacks aim to restrict or impair access to a computer system or network. They typically target servers to make websites and payment services unavailable — preventing legitimate users from accessing the online information or services they need.

Suspicious network traffic

Early warning of potential activities by would-be attackers trying to find insecure points or vulnerabilities in networks, infrastructure, or computers.

Botnet traffic

Networks of infected computers or devices that can be remotely controlled as a group without their owners' knowledge. Often used to perform malicious activities such as sending spam, or launching Denial-of-Service attacks.

C & C server hosting

A system used as a command-and-control point by a botnet.

Phishing dominates overall

These results are broadly reflective of what is being seen globally, with phishing making up about a third of all reported incidents. Phishing was reported almost twice as commonly as malware reports at **17%**, followed by unauthorised access (**15%**), scams and fraud (**13%**), and ransomware (**12%**).

PHISHING MAKES UP ABOUT A THIRD OF ALL REPORTED INCIDENTS

Case Study: Phishing

Recently we received an incident report about a phishing campaign that claimed to be from a well-known New Zealand company. The phishing emails were sent from a .nz email address, and had links in them directing victims to fake websites that tricked users into providing financial details. The sites were very convincing and well made, making it difficult to tell they were fakes at a glance.

We identified the ISP that the email address used, and working with them we blocked the email address from sending any further phishing emails. We also contacted some of our international CERT partners in countries that the fake websites were hosted in, to ask them to take action and block the fake websites.

With both of these measures, the phishing campaign was effectively stopped. New Zealanders were no longer getting the emails, and those that did couldn't fall victim to the fake website as it had been taken down.

Thanks to the connections established with the international CERT community, we were able to rapidly assist the take down of the phishing campaign and contain the incident.

Case Study: Email compromise

A small business discovered that an attacker had gained unauthorised access into their business email system.

They didn't know why someone wanted to gain access to their systems, but suspected it was financially motivated. The business reported it to us and we provided advice to them for their situation.

We recommended a range of actions for the business to protect themselves including to:

- immediately change all of their passwords
- enable two-factor authentication for their users when logging in to systems
- block the IP addresses the attacker had been using

- monitor their access logs to check the attacker hadn't gained unauthorised access to other business systems, and
- check auto-forwarding rules on their email to make sure the attacker hadn't set them up to be sent to them after they were locked out.

With cases like this, where an attacker gains unauthorised access to a system, there are often a number of measures, checks and steps that need to be taken to 're-secure' the system, in addition to just changing passwords. They can take considerable time and expense to recover from, and may require the expertise of an IT security specialist.

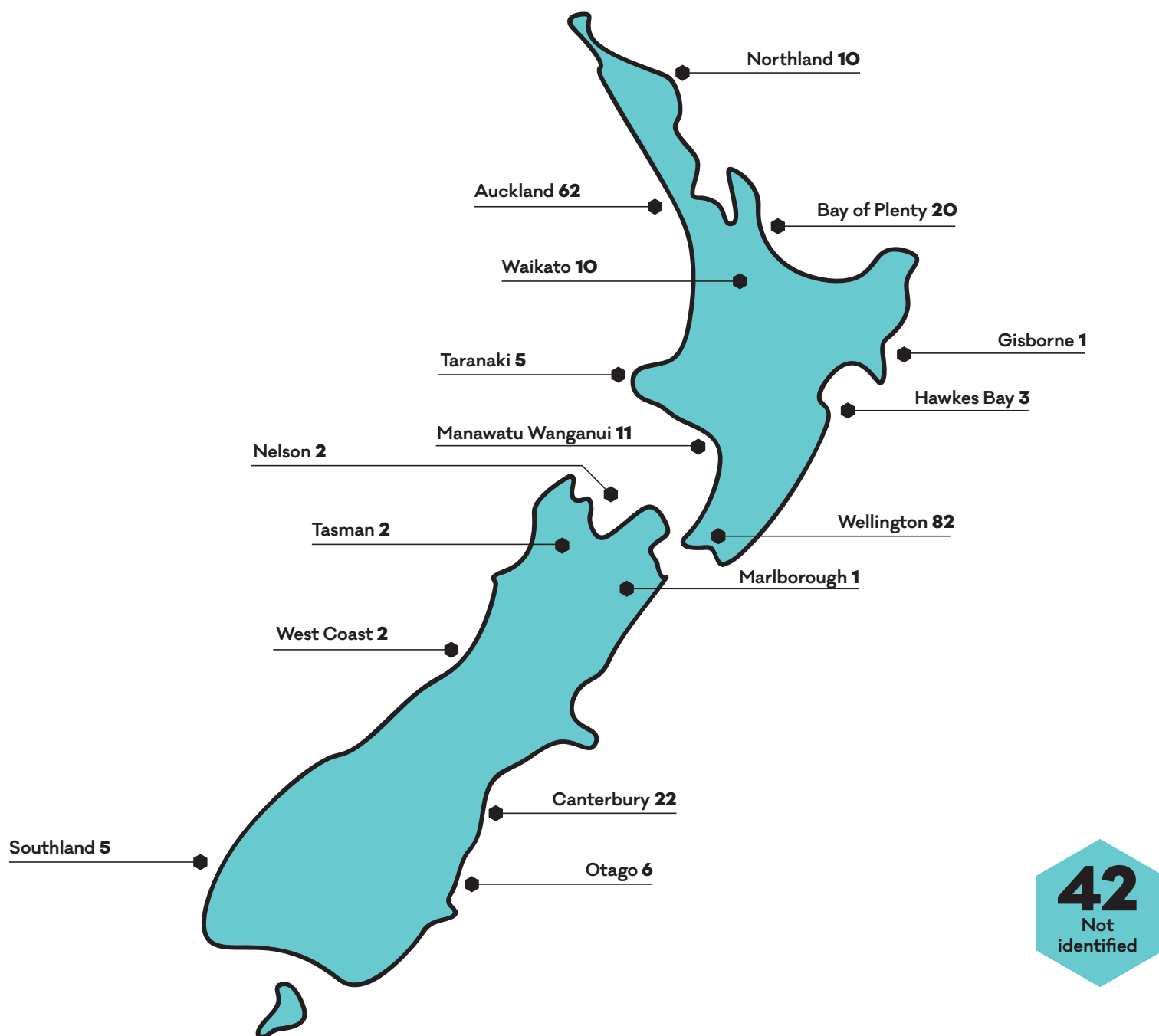
We also share information to help businesses protect themselves to avoid compromise in the first place and recover quickly if they do.

Reporting by Region

CERT NZ also captures the regions that incident reports are made from. The number of incidents received by region is represented below.

Most regions reported a broad spread of incident types, consistent with the overall trend in the report. The largest number of reports made by region were from Wellington (**82**), then Auckland (**62**). A large proportion of people reporting to CERT NZ chose not share the region they are from. **42** reports had no location recorded.

Over time as the number of reports grows, more identifiable trends may be able to be observed with this data set.



IMPACTS

Over \$730,000

in direct financial loss has been reported to CERT NZ during the last three months.

Cyber security incidents are inflicting significant losses on New Zealanders – in fact, **28% of people reporting incidents to CERT NZ have suffered some form of loss**, including considerable financial loss. Incidents reported to CERT NZ so far this year, including incidents referred to NZ Police or Netsafe for investigation, have reported direct financial costs totalling \$731,813.80.

As we build up a picture of how cyber security incidents are affecting New Zealanders, we must take into account more than just the possible financial costs of incidents. People have reported being affected by other losses such as data loss, reputational loss, intellectual property theft, technical damage, and operational impacts, all of which can hold considerable value.

Losses from incidents reported to CERT NZ

28% of the 286 incidents reported to CERT have reported some form of loss. Incident reporters are asked to outline what types of loss they have experienced, across six broad categories. From the total number of incidents reported, the types of loss experienced are broken down by percentage as follows:

8%

Data loss: Loss of data, business records, personal records, and /or intellectual property.

3%

Reputational loss: Damage to the reputation an individual, business, or organisation as a result of being the victim of an incident.

7%

Operational impacts: The time, staff, and resources required to recover from an incident, which can affect normal business operations and result in loss of business productivity

2%

Technical damage: Impacts on services, such as email, phone systems or websites, resulting in disruption to a business or organisation.

5%

Financial loss: The direct financial costs of an incident. It could be directly in the form of money lost as a result of an incident, but can also include the costs of recovery, such as contracting IT security services or investing in new security systems.

12%

Other: Includes specific types of loss not covered in the other categories, such as a victim being used to host or distribute malware to infect their customers.

Note: some incidents may have reported experiencing multiple types of loss.

Case Study: Unauthorised access

An individual saw activity on their computers and mobile devices which suggested someone else was accessing their personal accounts and logged the incident with us.

They wanted to stop it and forward it to the Police, but were concerned about lack of proof. We gathered information about the types of device, operating system and apps they were using, helped the individual identify ways they could lock them down and capture any unauthorised activity on them.

We also suggested they enlist the help of an IT service provider, who helped them get the access logs for some of their devices and applications. Ultimately this proved successful in capturing the information needed to verify that someone had been accessing the accounts, and that they had been using the password to one main app that gave them access to a lot of other apps. Once this came to light, the individual had the information they needed to make a formal complaint to the New Zealand Police for investigation.

FOCUS ON RANSOMWARE

Ransomware attacks are causing losses to New Zealanders. Here's what you need to know.

What is ransomware?

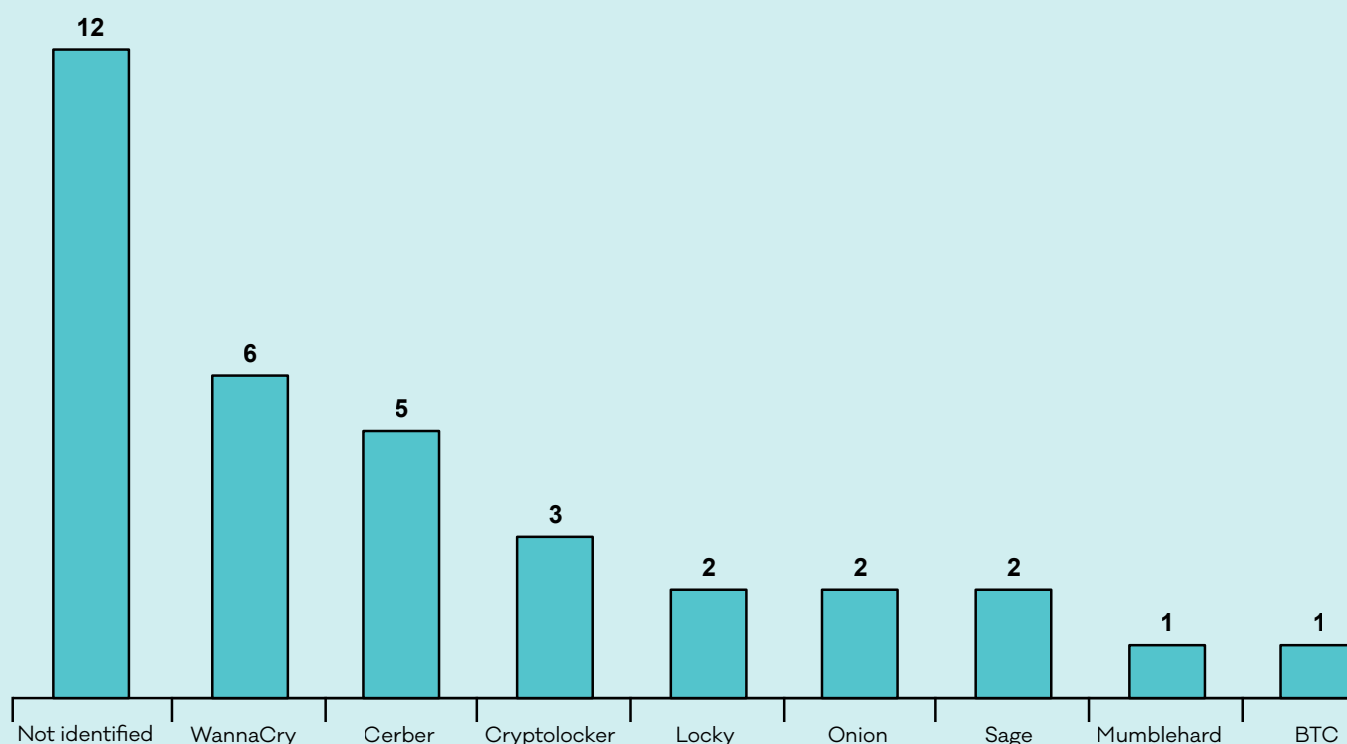
Ransomware is a type of malicious software that denies a user access to their files or computer system unless they pay a ransom. Ransomware can get into your computer in the same way that malware or a virus does. This can be from visiting unsafe or suspicious websites, opening emails or files from someone you don't know, clicking on malicious links in social media, like Facebook posts, or through vulnerabilities in your operating system.

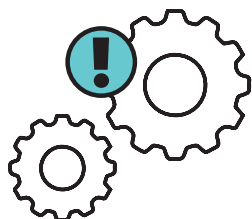
CERT NZ does not advise that people pay ransoms; there is no guarantee that paying the ransom will help get your files back and you may be targeted in the future because now the attackers know you will pay.

How is it affecting New Zealanders?

During the reporting period, two ransomware variants received major global attention: WannaCry and NotPetya. CERT NZ only received six reports of WannaCry affecting New Zealanders during this time, along with several other ransomware variants. No reports of NotPetya ransomware were received.

Ransomware attacks reported by New Zealanders: 11 April – 30 June 2017

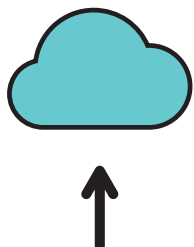




/// **Always update your operating system** and your apps when new versions are available. You can set this up to happen automatically with Windows and a lot of other applications like Office.

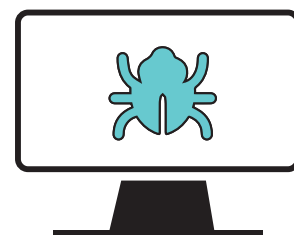


/// **Don't enable macros** in Microsoft Office.



/// **Make sure you back up your files** regularly. This includes the files on your computers, phones and any other devices you have. You can:

- do an 'offline' or 'cold' backup. Back up the data to an external hard drive and then remove the hard drive from your device.
- do a cloud backup to an online hosting service.



/// **Install antivirus software** on your computer if you don't already have it, and update it regularly.



/// **Install a firewall** on your computer to stop traffic from untrustworthy sources getting into your computer.



/// If you have your own business, make sure you **keep your support contracts up-to-date**.

Protecting yourself against ransomware

You can do a range of things to reduce the likelihood of a ransomware attack on your computer

WANNACRY

- WannaCry was a newly discovered ransomware variant, which made headlines globally in May 2017 after it compromised a number of networks around the world, including those of several health providers in the United Kingdom.
- The name 'WannaCry' (also known as 'Wana DecryptOr', 'WannaCryptor', or 'WCRY') is based on the encrypted file extension: '.wcrpy'.
- Like other ransomware, WannaCry blocked access to each computer and demanded approximately \$430 (NZD) to unlock it. Even if the victim paid the ransom, it was highly unlikely they would recover their files.
- The ransomware spread rapidly via a vulnerability in computers running unpatched versions of Windows by exploiting flaws in Microsoft Windows SMB Server. Once a single computer in a network was infected with WannaCry, the ransomware looked for other vulnerable computers on the network and infected them as well.
- This ransomware exploited a known Windows vulnerability known as 'EternalBlue'. Microsoft had released a patch (MS17-010) in March 2017 to address this vulnerability.
- CERT NZ published an advisory in response to the event which contained preventative measures and mitigations to protect networks.
- In the days following the attack, CERT NZ received 6 incident reports of WannaCry infections from small businesses. These were all followed up individually however we were not able to get sufficient information to verify the reports as definite cases of WannaCry.

NOTPETYA

- On June 28, a new ransomware variant called NotPetya (initially reported to be a known variant called Petya, hence the name) affected Microsoft Windows devices globally.
- In many ways the ransomware behaved similarly to WannaCry — it infected unpatched Windows devices by exploiting a vulnerability in SMB server. However unlike WannaCry, the malware was spread through a combination of the EternalBlue exploit, harvested credentials, and either PsExec, WMI, or both. As such, a device that has been patched against the EternalBlue vulnerability could still be compromised by an unpatched, infected device on the same network.
- CERT NZ issued an advisory highlighting the importance of ensuring that all devices on networks are patched.
- NotPetya was considerably more destructive than previous variants, as it effectively encrypted the hard drives of its victims (rather than just the files). Due to the way the ransom was demanded, it was highly unlikely that the victims who paid would have their hard drives decrypted.
- It was initially feared the malware would spread widely, however ultimately there were no reports of infected devices in New Zealand. The impacts were mostly observed affecting one country in particular, Ukraine, along with a number of companies in Europe.
- The disruptive effects of the malware globally did cause downstream impacts for several New Zealand companies with multinational links, however, CERT NZ received no specific reports of NotPetya compromises in New Zealand.

CERBER

- Unlike WannaCry and NotPetya, the Cerber ransomware has not received significant media attention in New Zealand, however CERT NZ has received 5 reports of the malware affecting businesses and causing them significant harm or loss.
- Of the 5 reports of Cerber, all of the victims reported experiencing loss such as technical damage, financial, and data losses, as well as negative operational and reputational impacts.
- The ransomware itself is a refined version of several prior variants, and was first seen in early 2016. It is highly customisable and is principally spread via infected email attachments designed to trick users into opening them.
- It can also be spread by tricking victims into visiting compromised websites that host exploit kits able to infect users without detection until the ransomware is executed.
- Once infected the Cerber ransomware encrypts key files on the victim's system and provides a ransom message demanding payment of 1.24 bitcoins in order to return the files.
- Once encrypted, there is little chance of recovering the files.

More tips for
staying safe online
can be found at
www.cert.govt.nz