certnz

Quarterly Report: Highlights Q2 2021

1 April - 30 June

New Zealand Government

Director's message

Rob Pope, Director

Four years on from CERT NZ's establishment, we've responded to almost 20,000 incident reports.

This quarter we continue to see New Zealanders impacted by cyber security incidents, and attacks increase in sophistication and complexity. However, this doesn't mean we're fighting a losing battle. There's also an upside of steady report numbers, and that's the positive shift we're beginning to see in New Zealanders' attitudes and collective responsibility towards experiencing a cyber security incident.

As a country we're moving away from 'the shame' of being affected by a cyber security incident and becoming more willing to report, ask for help and share lessons learned – examples of this include the case study in this report and an uptake in people sharing and identifying with incident information on our social channels. The more we all do this, the more awareness and knowledge we're building, and the more we're helping each other to keep secure online.

Four years on from CERT NZ's establishment, we've responded to almost 20,000 incident reports. The information from these reports have helped us gain a deeper understanding of the cyber security threats New Zealanders face, and in turn identify the security measures needed to protect against them.

These insights help us provide timely information during incident response and assisting those experiencing immediate risk. They are also the basis for the proactive work we do. We use them to develop and share actionable advice to help all New Zealanders step up their cyber security defences.

So each time a New Zealander turns on two-factor authentication, implements a critical control or reports an incident it's not just a win for CERT NZ, it's a win for all of us as we continue to work together to build our country's online security and confidence.

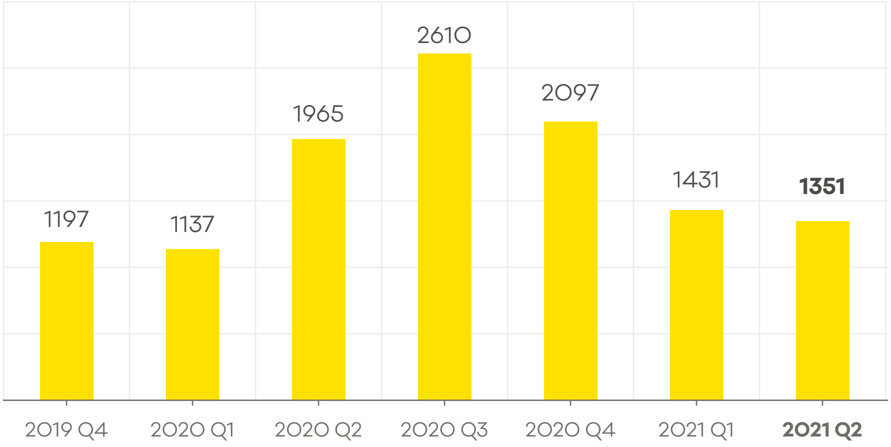
Incidents responded to by CERT NZ

1,351

incidents were responded to by CERT NZ in Q2 2021.

▼ **6% decrease**

from Q1 2021.



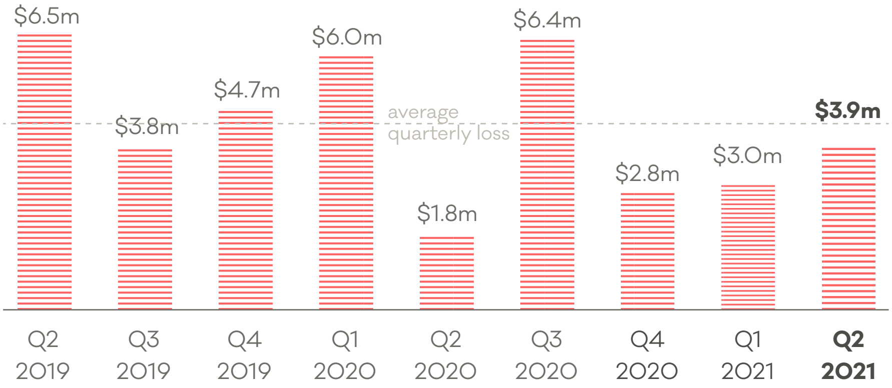
Direct financial loss

$3.9m

in direct financial loss was reported in Q2 2021.

▲ **30% increase**

from Q1 2021 with 17% of incidents reporting direct financial loss.



Putting data in perspective

Average incidents*

1,624

Average loss*

$4.0m

Total losses reported to CERT NZ

$59.9m

since Q2 2017

*figures based on previous eight quarters

For more on the New Zealand threat landscape in Q2 2021, see the CERT NZ Quarterly Report: Data Landscape. **www.cert.govt.nz/about/quarterly-report/quarter-two-report-2021**

Breakdown by incident category

		From previous quarter
Phishing and credential harvesting	**618**	▼ **5%**
Scams and fraud	390	▼ 14%
Unauthorised access	**171**	▲ **37%**
Malware	32	▼ 20%
Ransomware	**30**	▲ **150%**
Website compromise	19	▼ 37%
Suspicous network traffic	9	▲ 125%
Denial of service	5	▼ 17%
Botnet traffic	2	▼ 82%
Other	75	▼ 21%

150% increase in ransomware reports from Q1 2021

37% increase in unauthorised access reports from Q1 2021

Phishing and credential harvesting reports decreased 5% from Q1 2021

Ransomware on the rise

The number of ransomware reports responded to by CERT NZ has increased by 150% from Q1. There were 30 reports about ransomware in Q2, mostly from businesses and organisations. While most ransomware incidents don't report direct financial loss, the costs of recovery can be significant, and include data loss and operational impact.

Ransomware is a type of malicious software that can get into a computer system in a number of ways. For instance, when someone clicks on a link or attachment in a phishing email, or through weaknesses in out-of-date software. Once ransomware has infected a computer it encrypts files so they can't be read or accessed. Then a ransom is demanded for the files to be restored, with costs varying from a few hundred to millions of dollars.

As reflected in CERT NZ data, these types of attacks have grown in number and impact over the past two years. Attacks on businesses and organisations around the globe have increased in scale and severity, impacting private and public services, and disrupting the lives of many people.

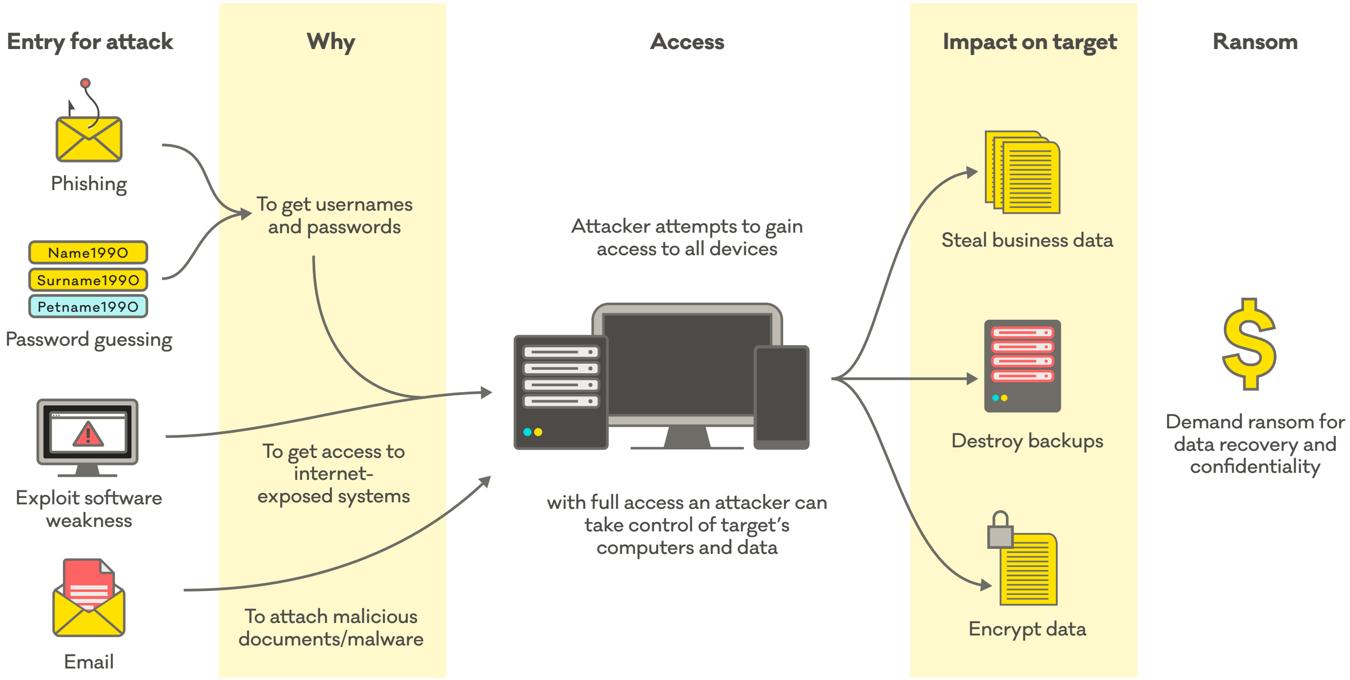
Why is it increasing?

Ransomware attacks are financially motivated. In some instances, ransoms have been paid. This has resulted in an increase of criminal groups carrying out these attacks.

How it works?

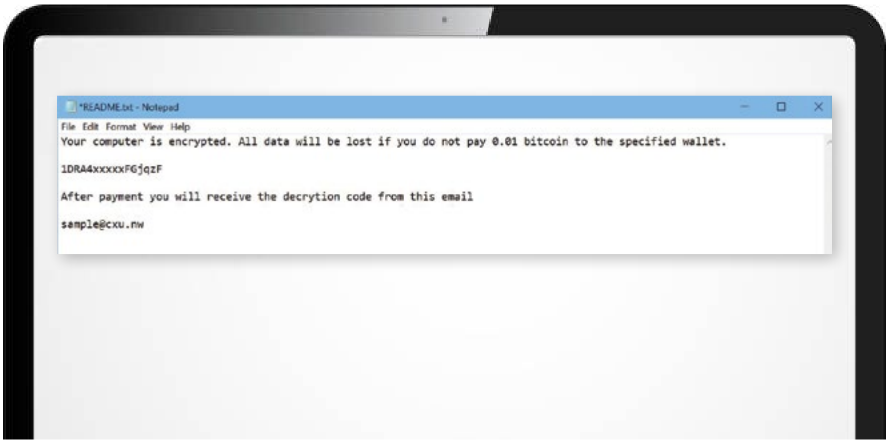
Different ransomware variants use different techniques to try and access devices and encrypt files. However, there are some common ways this happens, and most ransomware attacks follow one of a few predictable paths – see diagram below.

How ransomware works


Entry for attack
Why
Access
Impact on target
Ransom
Phishing
Name1990
Surname1990
Petname1990
Password guessing
To get usernames and passwords
Exploit software weakness
To get access to internet-exposed systems
Email
To attach malicious documents/malware
Attacker attempts to gain access to all devices
with full access an attacker can take control of target's computers and data
Steal business data
Destroy backups
Encrypt data
$
Demand ransom for data recovery and confidentiality

What does ransomware look like?

A ransomware attack is accompanied by a README.txt file pop-up or a change to your desktop background. Another indication of a ransomware infection is being unable to access or open any files.



```
Your computer is encrypted. All data will be lost if you do not pay 0.01 bitcoin to the specified wallet.

1DRA4xxxxxFGjqzF

After payment you will receive the decrytion code from this email

sample@cxu.nw
```

If you've been affected

If you receive a ransomware notification, disconnect your computer from your network and isolate the machine to prevent the malicious software spreading further. Simply do this by unplugging your cords and router. Then seek the advice of an IT professional to help investigate which computers are affected, and work out how to get back up and running.

CERT NZ does not recommend paying the ransom. Payment does not guarantee that all your data will be decrypted, and you'll still likely need IT professional help. It may also open you up to future cyber security attacks as attackers may believe you are willing to pay.

Be prepared

No matter what kind of cyber security incident you face, it's important to have an incident response and recovery plan. Having a plan and testing it will make it faster and easier to deal with the real thing. If you need some help preparing your incident response plan, follow the step-by-step guide on our website[1].

Prevention is key

There are different variants of ransomware, however the motivations and outcomes are the same. Attackers are motivated by financial gain, and recipients are left with encrypted data. The best thing you can do is apply preventative steps.

1. Keep your operating system and apps up-to-date. You can set this up to happen automatically with major operating systems like Windows and MacOS, and common applications like Office.
2. Make sure you back up your files regularly to an external hard drive or cloud service. Keep your backup disconnected from your computer. That way it can't be destroyed in an attack, and you will be able to restore from backup if you need to.
3. Install antivirus software and update it regularly.
4. Talk to your IT provider about applying the CERT NZ critical controls that are relevant to your business[2].
5. If you think you've been affected by ransomware, you can report it to CERT NZ **www.cert.govt.nz/report**.

[1] https://www.cert.govt.nz/business/guides/incident-response-plan/

[2] https://www.cert.govt.nz/it-specialists/guides/how-ransomware-happens-and-how-to-stop-it/

Retailer recovers from ransomware

Businesses and organisations of all sizes are increasingly experiencing the impacts of ransomware compromises, and the impacts are not only financial, as one business experienced.

In a recent case, a medium-sized retail store was targeted by a ransomware. An employee went to activate the office computer and encountered a black screen with icons. When hovering over the icons, pop-ups appeared with a prompt to click on a link to pay a ransom, in Bitcoin, to recover the files.

The employee didn't click any icons or attempt to make payment. Instead, they phoned a colleague and waited for IT assistance. IT identified the files had been encrypted and the likely source of the ransomware was an insecure service accessible from the internet, meaning the business's computer system was exposed. As the computer had been left idle and connected to the internet, attackers had taken the opportunity and exploited the service.

Although the business regularly backed up files, unfortunately the hard drive had been left connected to the computer, meaning that not only were the files on the computer encrypted but the backup files also. The ransomware also affected business systems including a retail programme which recorded inventory and synced with the e-commerce part of their website.

In response, the retailer took the business offline and removed all files and programmes from the infected machine. The business had to rebuild their supplier and customer databases from scratch, as well as do a full stocktake to rebuild inventory. With additional support from their point-of-sale provider some files were able to be recovered.

Although the business didn't pay the ransom, the impacts of the attack did have financial implications and resulted in significant data loss and operational impact.

As a result of the ransomware attack, the retailer is now taking additional steps to secure their system. For example by backing up all data regularly and keeping these backups disconnected from the network, applying security and installing antivirus software. In addition to these steps, the retailer is keeping staff up-to-date on cyber security practices like keeping backups offline.

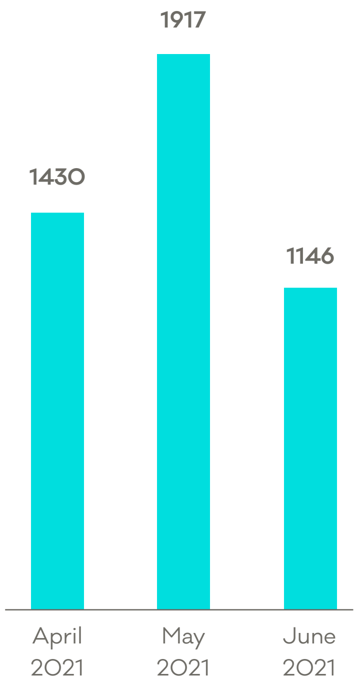
These cases show how easily a ransomware attack can happen, and that anyone can be a target. However, it's not all bad. There are simple measures businesses can put in place to up their cyber defences.

Check out page 5 for ransomware prevention tips.

Weak and default passwords make for easy targets

Alongside the data from incidents directly reported, CERT NZ also analyses and monitors cyber security information provided by local and international partners. In Q2, CERT NZ identified almost 4,500 brute force incidents involving New Zealand internet-enabled devices like routers and WiFi cameras, where attackers targeted weak or default usernames and passwords.

Brute force attacks involving New Zealand internet-enabled devices



Brute force is a method attackers use to guess passwords to access online accounts and internet-enabled devices.

In the case of internet-enabled devices, the attackers begin by scanning the internet for accessible devices. Once an accessible device is identified, the attacker will use brute force software to repeatedly guess the passwords. This can take anywhere from a few seconds to hours. The stronger the password is, the longer an attack will take and the more likely an attacker is to give up before guessing the password.

If the brute force attack succeeds, the attacker can then carry out a wide range of malicious activity depending on what is accessed. This can include accessing private data like footage from internet-connected security and TV cameras. Attackers can also use the infected device to spread further malware and brute force other devices.

Protecting your internet-enabled devices

Devices like routers and WiFi cameras often have pre-configured usernames and default passwords. Even if the passwords look strong, they're often commonly used and attackers can target them.

To protect against brute force attacks, CERT NZ recommends anyone with an internet-enabled device to update the default usernames and passwords where possible, using long, strong and unique passwords[3]. Refer to the device's user manual for instructions on how to update these settings.

If you have experienced a cyber security issue,
report it to CERT NZ at **www.cert.govt.nz/report** or call us on **0800 CERT NZ (0800 2378 69)**

[3] https://www.cert.govt.nz/individuals/guides/how-to-create-a-good-password/

Cryptocurrency-investment scams on the rise

Cryptocurrency-investment scams made up 13% of the total direct financial loss in Q2, with a total of $500,000. Reports about this type of scam have been steadily increasing, up 50% from last quarter.

These types of scams happen when attackers attempt to trick people into sending money to take part in fake cryptocurrency-investment opportunities and exchanges. These scams are often distributed by emails, text messages, phone calls or through fake websites. They advertise cryptocurrency-investment opportunities with substantial and guaranteed financial returns, or offer direct sales of cryptocurrencies like Bitcoins, Litecoins or other altcoins, which don't result in any transfer once payment is made.

Many of the cryptocurrency-investment scams reported to CERT NZ use common scam techniques. For example, the language used in the scams often replicates investment-style communications to appear legitimate. They also often create a sense of urgency to encourage the recipient to act quickly and not miss out on the 'investment opportunity'. These scams are becoming more difficult to spot, and in some cases, the recipient may not realise the scam until the attacker ceases to respond once payment has been made. In other cases, the scam may not be apparent until the target requests to withdraw their investment. Following their request, the scammer asks them to pay a withdrawal fee, as a way to steal more money, and this doesn't result in any return of the investment.

Protecting from cryptocurrency-investment scams

- Be wary of any investment opportunities sent by someone you don't know, or that seem out of character for someone you do know. If you're unsure, contact the sender to check first.
- Cryptocurrencies are high risk and highly volatile – the price can go up and down very quickly. Investment opportunities offering high, guaranteed returns are likely too good to be true.
- All unsolicited marketing emails in New Zealand are illegal[4] so if you receive an investment offer from someone you've never been in contact with, it's likely illegitimate.

What to do if you think you've been caught up in a cryptocurrency-investment scam

- Contact the service provider for your online accounts – like your bank or your email provider. Let them know what's happened and ask what they can do to help.
- Cease any communications and payments with the sender.
- Change the passwords for any online accounts you think may have been affected by the scam[5].
- Get a free credit check done. This will let you see if any accounts have been opened in your name. There are three main credit check companies in NZ, and you'll have to contact all of them. You can ask to have your credit record corrected if there's any suspicious activity on it.

If you think you've been affected by a scam, you can report it to CERT NZ **www.cert.govt.nz/report**.

[4] https://www.dia.govt.nz/Spam-NZ-Spam-Law-for-Businesses
[5] https://www.cert.govt.nz/individuals/guides/how-to-create-a-good-password/