certnz

Q1

JAN_TO_MAR_2022

CYBER SECURITY INSIGHTS

The biggest catch

IN THIS ISSUE

Te Kāwanatanga o Aotearoa
New Zealand Government

Q1 CYBER SECURITY INSIGHTS

Director's message

Rob Pope, Director

After a record number of cyber security incidents at the end of 2021, CERT NZ figures show a decrease in reports this quarter. Although this may sound like good news, it doesn't mean we can approach our online security with any complacency. It's quite the opposite, in fact.

Between January and March of this year, we received over 2,300 reports across the country and saw attackers using a range of new methods to try to get their hands on people's finances and personal information.

These incident reports provide CERT NZ with fresh insights on the cyber security threat landscape and enable us to share relevant information and advice on the current risks New Zealanders are facing. Examples in this update show attackers continue to use phishing as a stepping stone to other types of attacks and that they are also targeting the increasing popularity of non-fungible tokens (NFTs) to carry out various kinds of scams.

But while attackers use ever-evolving methods, our advice to help safeguard from these attacks remains constant. We need to keep doing what we know works best and continue to improve our cyber defences.

Whether it's for a large company detecting and responding to threats, or a casual internet user setting up two-factor authentication to protect their email account, CERT NZ is here to provide step-by-step advice for all New Zealanders.

If we all put in the mahi and take one step at a time to improve our online security, this will go a long way to keeping ourselves better protected and help build a more cyber resilient Aotearoa New Zealand.

AT A GLANCE...

Average incidents reported per quarter

2,227

Average loss reported per quarter

$4m

Total losses reported to CERT NZ

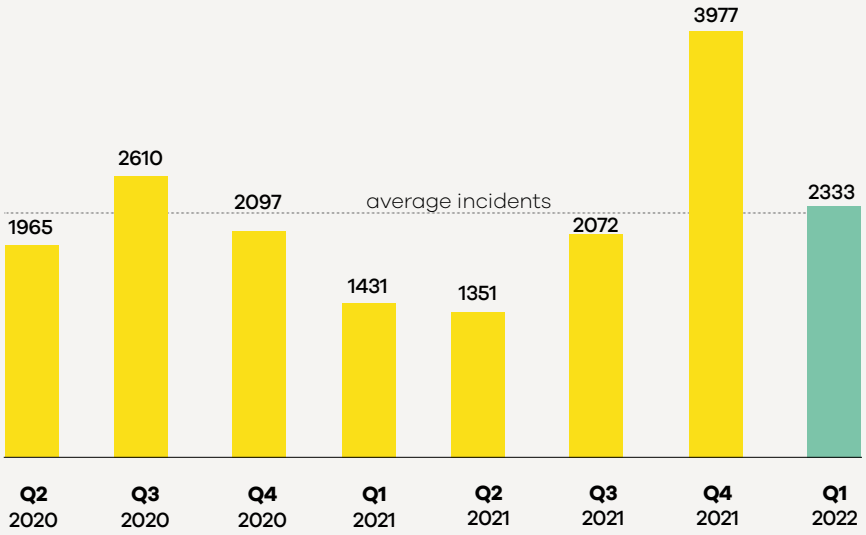
$31.5m

Figures based on previous eight quarters

INCIDENTS RESPONDED TO BY CERT NZ

2,333
incidents were responded to by CERT NZ in Q1 2022.

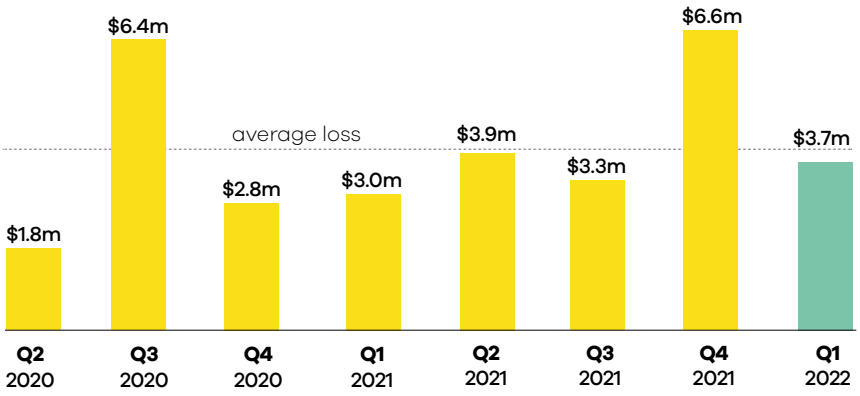
▼41%
decrease from Q4 2021.



DIRECT FINANCIAL LOSS

$3.7m
in direct financial loss was reported in Q1 2022.

▼44%
decrease from Q4 2021, with 30% of incidents reporting financial loss.



BREAKDOWN BY INCIDENT CATEGORY

▼95%
decrease in malware reports from Q4 2021.

Reports of Flubot malware have decreased from previous quarters.

▲31%
increase in ransomware reports from 13 in Q4 2021 to 17 in Q1 2022.

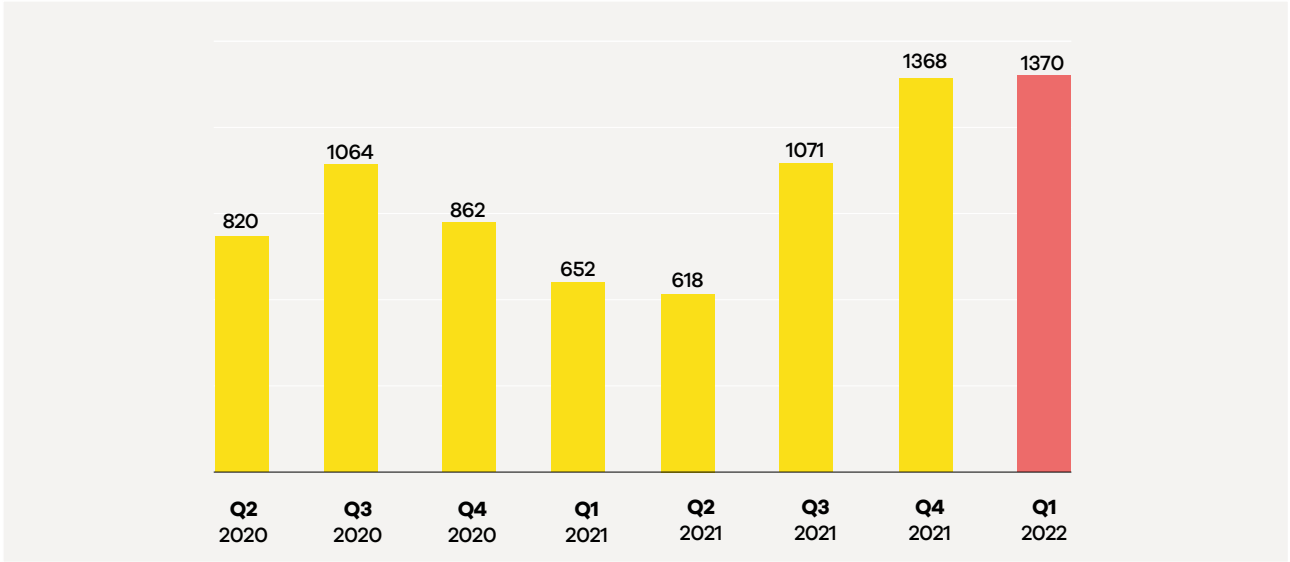
		From previous quarter
Phishing and credential harvesting	1370	▲ 0.1%
Scams and fraud	565	▼ 0.5%
Unauthorised access	228	▼ 3.8%
Malware	**81**	**▼ 95.3%**
Website compromise	24	▼ 11.1%
Ransomware	**17**	**▲ 30.8%**
Botnet traffic	7	▲ 600%
Denial of service	4	▼ 66.7%
C and C server hosting	4	▲ 300%
Suspicious traffic	1	● 0%
Attack on system	0	● 0%
Other	32	▼ 22%

For more on the New Zealand threat landscape in Q1 2022, see The CERT NZ Quarter One: Data Landscape.

The biggest catch

Phishing and credential harvesting is consistently the most reported incident category to CERT NZ, making up 59% of reports this quarter. On average, CERT NZ receives 73% more reports about this category than any other.

PHISHING AND CREDENTIAL HARVESTING REPORTS (last 8 quarters)



WHAT IS PHISHING AND WHY IS IT SO COMMON?

Phishing tries to mimic an authentic communication from a trusted source, usually through email or SMS. The intent is to try to trick the recipient into taking an action, like clicking on a link or providing personal or financial information.

There are a couple of reasons why phishing is so common.

First, phishing is low cost and easy to do. Unlike some types of cyber attacks, it doesn't require significant technical ability to be successful. Instead, it relies primarily on social engineering to try to trick people.

This links to the second reason. While networks and systems are constantly being upgraded to keep attackers out, people can make mistakes. The attackers behind these campaigns are aware of this and sometimes use sophisticated methods to get the response they want. They are constantly evolving their approach and use social engineering tactics, like urgency, fear and opportunity to prompt the recipient to respond. In some cases, they'll try to use authoritative language and emotional levers like a penalty or a fine to prompt action. In other cases, they create fake scenarios that reflect current events to make the communication seem more plausible. For example, CERT NZ saw an increase in phishing attempts focused on COVID-19 during the vaccine roll out.

Most phishing attempts aren't targeted at a specific person or group. Attackers usually cast their net wide to include anyone who uses technology to communicate. This means campaigns will target thousands of people, so, even if only a small percentage of recipients are tricked into responding, the attackers' gains can be substantial.

> "Attackers use social engineering tactics, like urgency, fear and opportunity, to prompt the recipient to respond."

WHAT CERT NZ IS SEEING

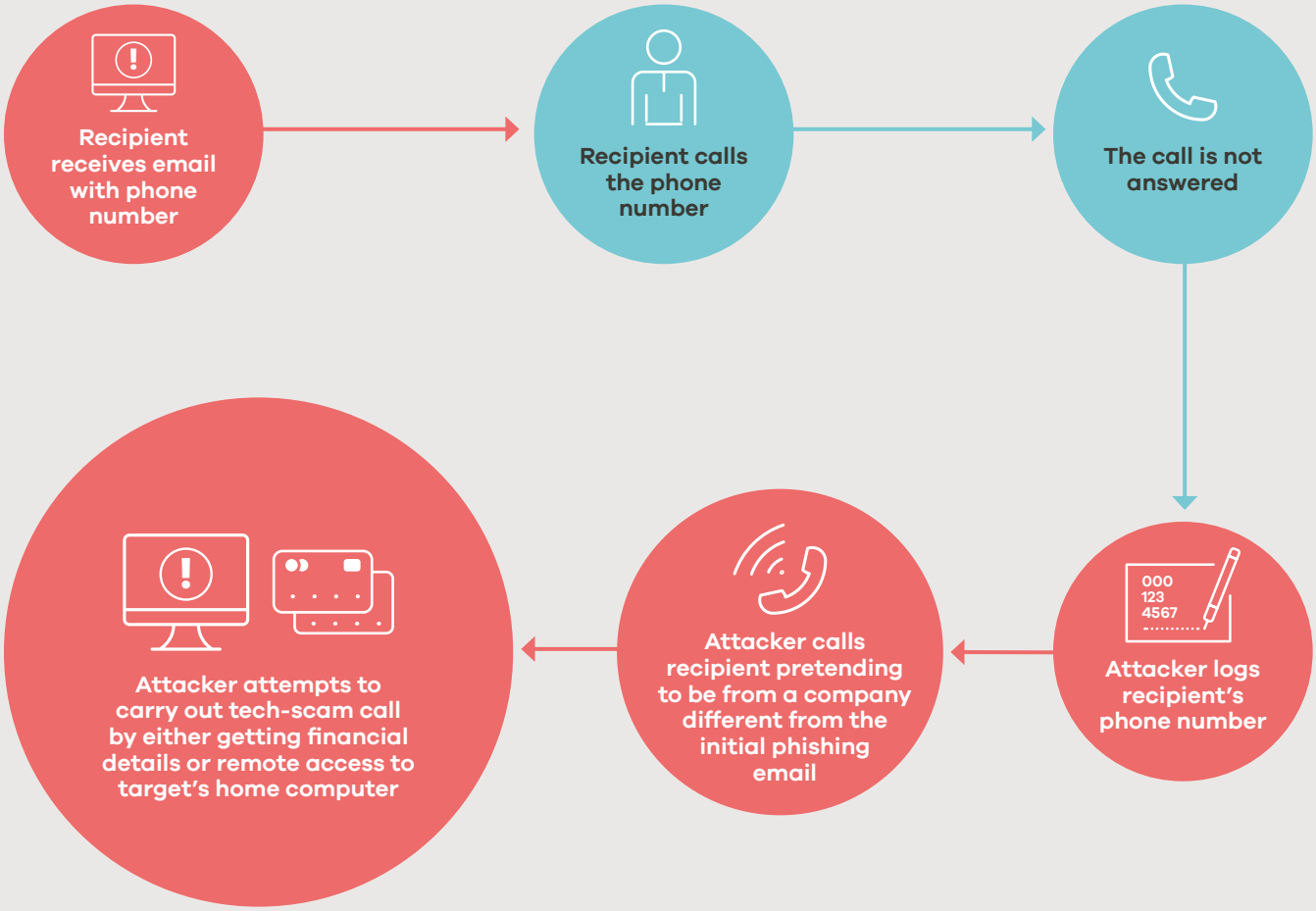
Phishing has evolved from the infamous 'Nigerian Prince inheritance' emails to far more plausible communications pretending to be from well-known brands and organisations.

Incidents reported to CERT NZ this quarter have included both common phishing attempts, as well as some newer campaigns, from impersonation of government agencies and banks to messages posing as software retailers and charities.

In terms of tactics, in quarter one, CERT NZ received reports of email phishing attempts designed to prompt a strong emotional response. This ranged from fake relief efforts for Ukraine through to attempts at localised messages with phishing emails written in te reo Māori. Another new example is attackers using phishing to identify potential targets for tech-scam calls, as highlighted in the following case study.

CASE STUDY

HOW PHISHING CAMPAIGNS CAN LEAD TO TECH-SCAM CALLS



Phishing leads to tech-scam call

Phishing and credential harvesting are precursors to other cyber attacks. In quarter one, a phishing campaign distributed by both email and text, prompted recipients to call a number to cancel an expensive anti-virus subscription before being charged a significant sum the following day.

However, no such subscription existed. It was a scam tactic using urgency and the fear of losing money to try to get the recipient to call the number.

If the recipient called the number, the call wasn't answered. Instead, the attackers collected the caller's number as someone potentially worth targeting.

Later, the attackers called the recipient pretending to be from a tech-support service or bank unrelated to the initial subscription-based phishing message. They would then attempt to get the recipient to provide banking information or remote access to their home computer.

Received a tech-scam call?

- Banks and legitimate organisations don't ask for personal or financial information over the phone nor request remote access. If you receive a call requesting these things, it's likely a scam. Don't provide any personal or financial information over the phone or allow the caller to have remote access to your PC or device.
- If you think the call is legitimate, you can decline to respond and then call the company yourself using the contact number listed on the company's official website.

CERT NZ ADVICE AND MITIGATIONS

Phishing campaigns are always evolving, however advice to help protect against them remains the same.

If you are unsure about a communication you've received:

Go direct. Type the URL into the address bar or use bookmarks to access websites rather than clicking links in emails or texts.

Just ask. If you're unsure about an email or text you've received, it's a good idea to check in with the sender via another method like phone or text, or run it past a colleague, friend or family member.

Two steps that help keep your accounts secure

Use unique passwords on all your online accounts (and a password manager to help remember them) that way, if you share your account information in a phishing attack, your other accounts won't be affected. You'll only need to update the password for the compromised account.

Use two-factor authentication (2FA)[1] on accounts where possible. It provides an extra layer of security on your account in case your password is compromised.

[1] www.cert.govt.nz/individuals/guides/two-factor-authentication/

SINCE CERT NZ LAUNCHED IN 2017, WE'VE:

- received more than **12,342** phishing and credential harvesting reports
- worked with affected organisations and individuals to help them recover
- helped take down thousands of phishing websites and disrupted campaigns before they reach New Zealanders
- investigated the software that attackers use to distribute phishing campaigns and used the findings to develop preventions and mitigations to help protect against them.

REPORT IT

If you suspect that you may have received a phishing attempt, or have fallen victim to a phishing scam, you can report it to CERT NZ: www.cert.govt.nz/report.

You can find more information about phishing on our website: www.cert.govt.nz/individuals/common-threats/phishing/.

International insights

In this section, we cover common incident types that our international partners have seen this quarter.

Flubot and smishing

The Flubot malware campaign continues to make waves across the globe, after New Zealand's peak at the end of 2021. Noticeably, we have seen cases with our closest partners. Canada has noted that people should continue to be vigilant against all types of smishing campaigns. We continue to see global trends towards this type of incident, and campaigns like Flubot may come around again.

Ransomware

Ransomware cases continue to increase in sophistication and impact internationally. SingCert[2] noted this incident type as the main ongoing threat, and the Australian Cyber Security Centre also noted the increase in attacks, publishing a general advisory with UK and US partners to help organisations up their defences.

[2] www.csa.gov.sg/en/singcert/Publications/2021-key-trends-and-takeaways

Attackers target NFTs ...

Techniques that attackers use are constantly evolving to reflect people's interests and where they're spending their money. An example of this is the increasing reports related to non-fungible tokens (NFTs) in quarter one.

Non-fungible tokens (NFTs) are digital certificates of ownership that can only be bought using cryptocurrency. Each one is 'minted' to be unique. An NFT links to an item, such as a piece of digital art, and verifies who owns it using blockchain technology.

An NFT campaign is often related to the release of a certain art or game project with the minting of a limited number of individual pieces. Creators will offer these as pre-orders.

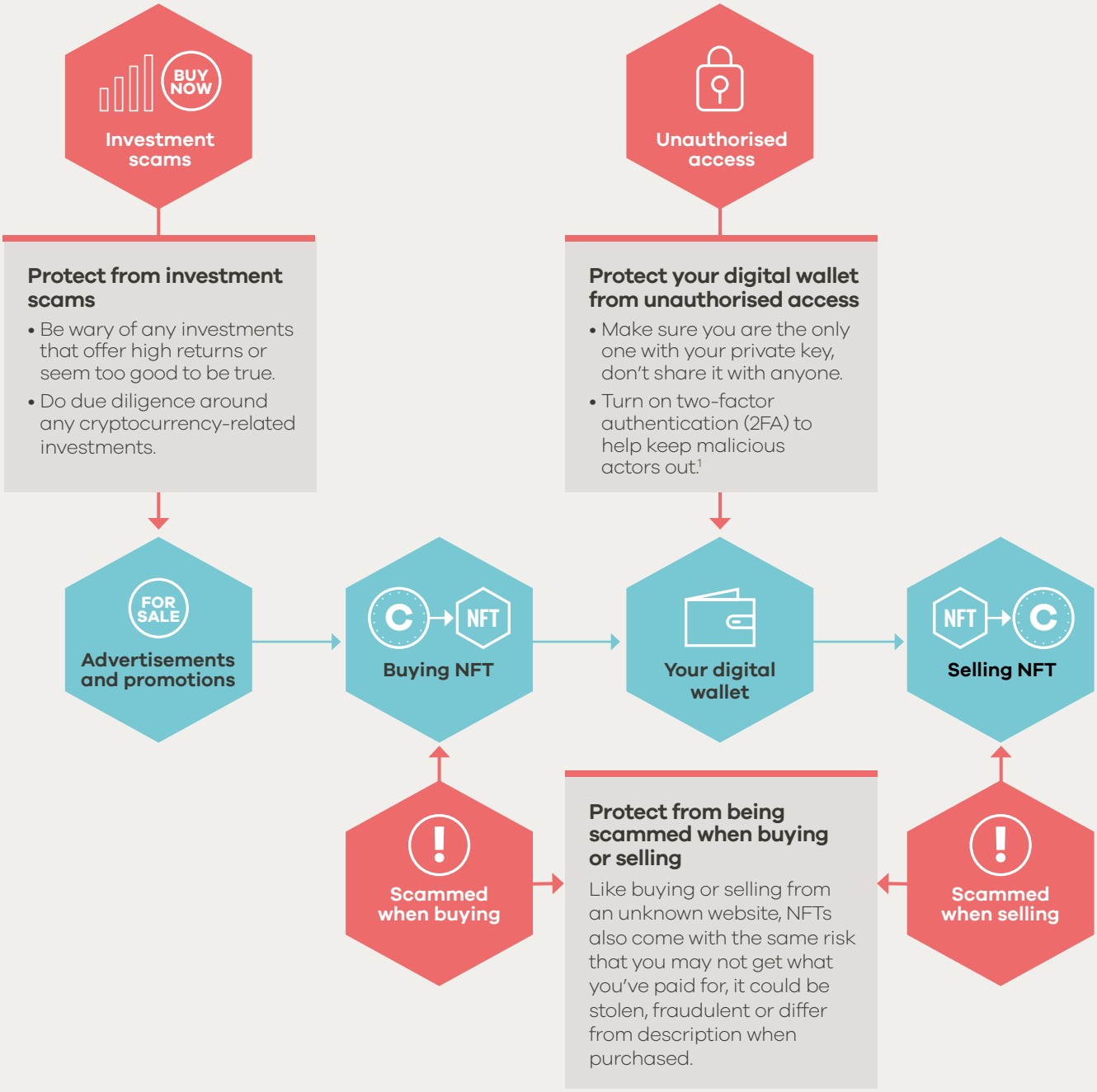
Like many online transactions, NFTs come with their own set of potential cyber security risks.

Types of incidents reported to CERT NZ range from unauthorised access to scams involving buying and selling NFTs and fake investments.

With eight reports about NFT-related incidents this quarter, and associated financial loss close to $50,000, CERT NZ anticipates attackers will leverage the increasing popularity of NFTs for their gain.

NFTs appeal to attackers because they are still mostly unregulated and payments are difficult to reverse or retrieve. The NFT market can be heavily hyped with high-profile projects and the estimated resale values can create a fear of missing out. Attackers can use this to try to trick people into taking part in their scam.

POTENTIAL THREATS IN THE NFT TRADING PROCESS

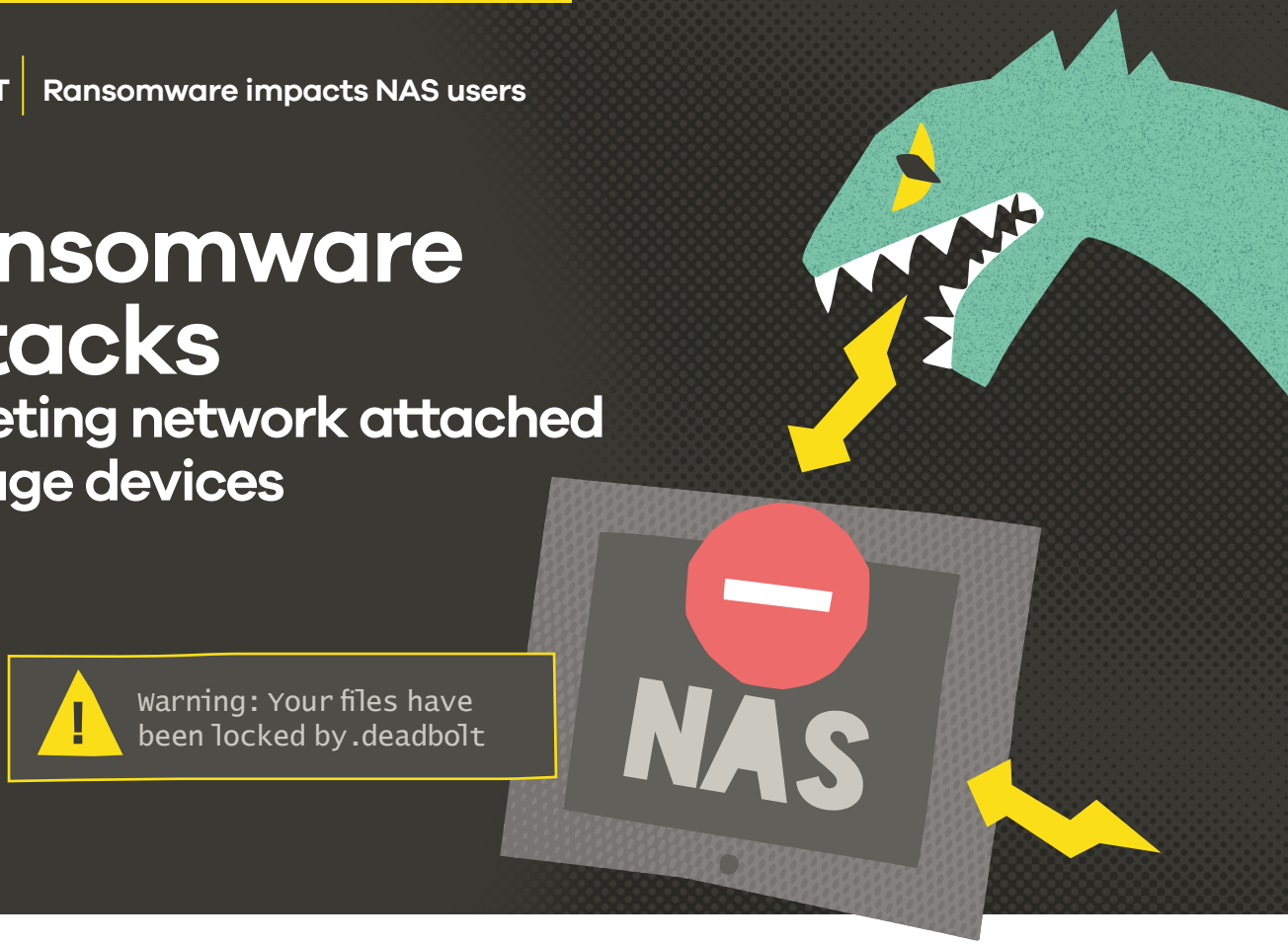


The Financial Markets Authority highlights three risks regarding cryptocurrencies.[2]

- Cryptocurrencies are high risk and highly volatile, the price can go up and down very quickly.
- Cryptocurrencies are not regulated in New Zealand.
- Cryptocurrencies, crypto-exchanges and the people using them are often the targets of hacking, online fraud and scams.

[1] www.cert.govt.nz/individuals/guides/two-factor-authentication/
[2] fma.govt.nz/investors/ways-to-invest/cryptocurrencies/.

Ransomware attacks
targeting network attached storage devices



CERT NZ received 17 reports about ransomware this quarter, five of which specifically targeted network attached storage (NAS) devices. These NAS-targeted ransomware attacks locked files on the device preventing the owners from accessing their information, like business files, family photos and more.

NAS devices are computers designed to store large amounts of files, or to provide access to the files from multiple devices. NAS devices are set up for a variety of personal and business uses.

Attackers target NAS devices with ransomware because the data stored is often of high personal or business value. This can force those targeted to have to choose between losing their data permanently or paying a ransom and hoping the attacker will keep their word.

CERT NZ recommends not paying the ransom, because it doesn't guarantee data will be recovered and attackers may target you again.

If a NAS device is exposed to the internet, attackers can use several different attacks to gain access and deploy ransomware. The most common attacks include exploiting vulnerabilities in the operating system and targeting of weak or default passwords. Once the attacker has access to the device, they can begin locking the files. The attacker then demands a payment or 'ransom' to have the files unlocked.

This quarter, CERT NZ received reports from small businesses that had their files encrypted with a '.deadbolt' file extension. CERT NZ identified this as being part of a larger campaign actively targeting QNAP and Asustor NAS vulnerabilities.

Following this, CERT NZ published an advisory detailing the affected versions and mitigations to help protect from the attack.[1]

HOW TO PROTECT YOUR NAS

- **Prevent attackers gaining access by not exposing your NAS to the internet. If internet access is necessary, restrict it by IP/CIDR or geolocation.[2]**
- **Change default or weak passwords to long, strong and unique passphrases.[3]**
- **Apply updates as soon as they are available.[4]**
- **Turn on two-factor authentication.[5]**

[1] www.cert.govt.nz/it-specialists/advisories/qnap-and-asustor-nas-vulnerabilities-exploited-to-deploy-ransomware/
[2] www.cert.govt.nz/it-specialists/critical-controls/network-segmentation-and-separation
[3] www.cert.govt.nz/individuals/guides/how-to-create-a-good-password
[4] www.cert.govt.nz/it-specialists/critical-controls/patching/
[5] www.cert.govt.nz/individuals/guides/two-factor-authentication/