certnz

# Quarterly Report: Highlights Q4 2020

1 October - 31 December, 2020

New Zealand Government

Rob Pope, Director

# Director's message

**At CERT NZ, helping people is at the heart of what we do. We work across the board in both incident response and recovery as well as acting as the fence at the top of the cliff helping New Zealanders to prevent cyber incidents.**

One of the things we all love about technology is the speed at which we can do things – whether that's paying bills in a few clicks or catching up on the cricket score at the touch of an app. But of course where there's good there's always a bit of bad, and unfortunately malicious online activity can be carried out at equal pace.

Quarter four was no exception. We continued to see how quickly attackers can evolve their techniques to try and access personal and financial information. Although incident reports were down from quarter three, the numbers are still among the highest quarterly figures to date with over 2,000 reports and close to $3 million in direct financial loss.

These are significant numbers and that's just the tip of the iceberg. There are other equally harmful impacts that are more difficult to measure, like loss of confidence online. Understandably it's easy to want to turn away from technology after experiencing a cyber security incident, however doing so can make simple everyday tasks suddenly difficult. That's why it's important that New Zealanders know who to turn to for help.

At CERT NZ, helping people is at the heart of what we do. We work across the board in both incident response and recovery as well as acting as the fence at the top of the cliff helping New Zealanders to prevent cyber incidents. It's these preventative measures that are key in building a cyber-resilient New Zealand.

We do this through the likes of our website guides, alerts and advisories as well as working with international and local partners to gain insights and share information. For example our national awareness campaign, Cyber Smart Week, which took place in quarter four of 2020 brought together 170 partner organisations and shared easy-to-follow cyber security tips with over a million New Zealanders.

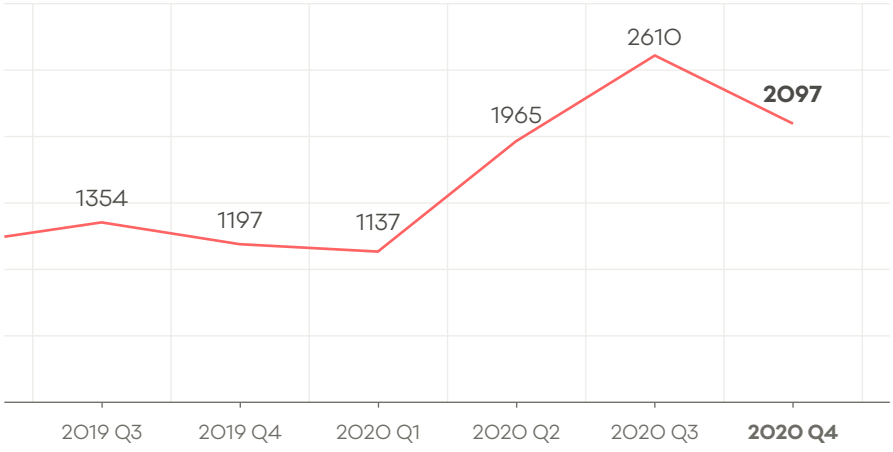
Another example where we help New Zealanders to prevent attacks is through our increasing data sources, which allow us to identify specific cyber security threats and reach out to those who are potentially vulnerable.

These measures are just some of the ways CERT NZ is empowering all New Zealanders to step up their cyber defences and make the most of the good that technology has on offer.

## Incidents reported to CERT NZ

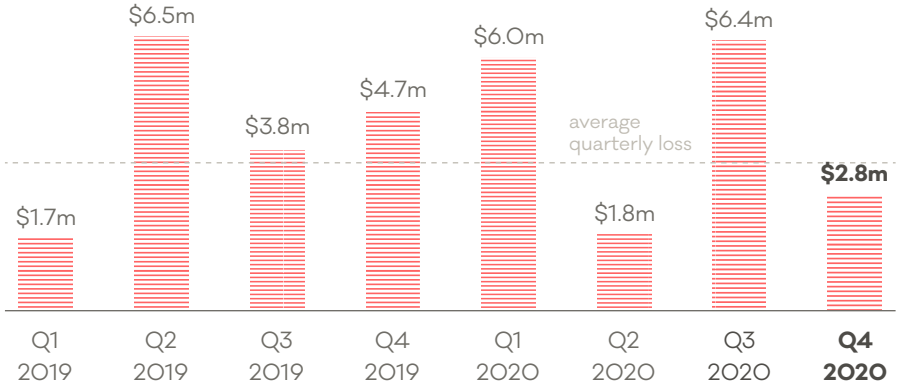
**2,097**
incidents were reported to CERT NZ in Q4 2020.

**▼ 20% decrease**
from Q3 2020.




## Direct financial loss

**$2.8m**
in direct financial loss was reported in Q4, 2020, with 14% of incidents reporting financial loss.




# Putting data in perspective

### Averages per quarter

**1,473***
incident reports

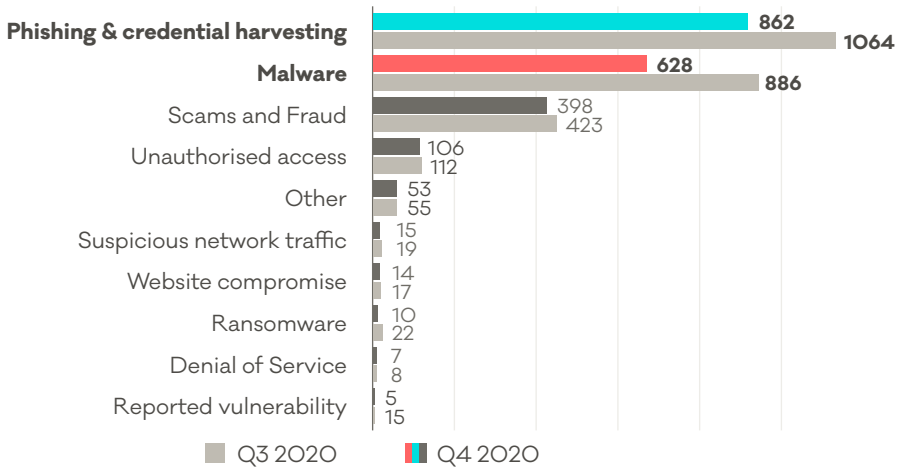
**$4.6m**
in direct financial loss

with a total of $53m in direct financial losses reported to CERT NZ.

*based on the previous eight quarters.

For more on the New Zealand threat landscape in Q4 2020, see the CERT NZ Quarterly Report: Data Landscape. If you have experienced a cyber security issue, report it to CERT NZ at www.cert.govt.nz/report.

## Breakdown by incident category




**Phishing and credential harvesting made up 41%** of all reports in Q4.

**26% increase in reports about vulnerable databases** from Q3, 2020[1].

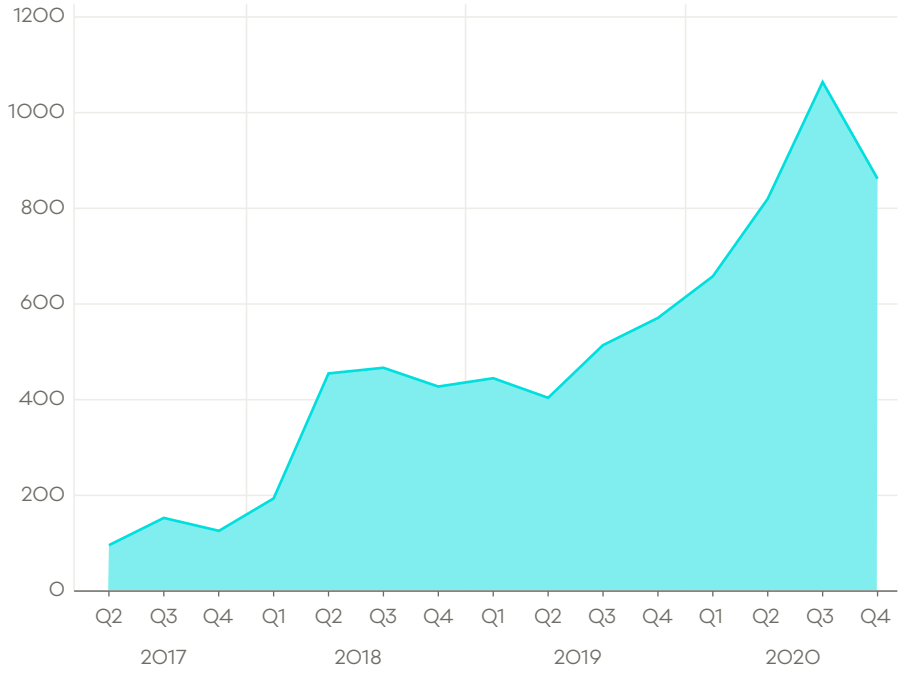
**30% of all reports were about malware**, making it the second highest incident category.

1. Data from cyber threat intelligence provider The Shadowserver Foundation www.shadowserver.org

# Phishing incidents

Phishing is consistently one of the highest incident categories reported to CERT NZ – making up 41% of all incidents reported in Q4, 2020.

**Phishing and credential harvesting reports**




Since CERT NZ launched in 2017, we've received more than 7,200 phishing reports and worked with thousands of organisations and individuals across the country to help them recover.

Phishing campaigns can have a big impact on individuals, businesses and large organisations, and result in financial, data, operational and reputational losses. Often phishing is a precursor to other attacks and scams, like unauthorised access and data breaches.

## What CERT NZ does

In Q4, 44% of phishing incidents reported were about individuals, and 19% about businesses and organisations. Where possible, our incident response team worked with the recipient to determine the impact, and provided relevant guidance to help them recover, and resecure their accounts.

The other 37% includes reports from local and international partners alerting us to phishing campaigns and harvested credentials. CERT NZ takes this information, analyses the data and reaches out to the appropriate person, agency or organisation who may have been affected.

**CERT NZ also uses the information from these reports to:**

- take down phishing websites
- disrupt phishing campaigns
- investigate the techniques attackers use to distribute phishing campaigns and take the findings to develop preventions and mitigations to help protect against them.

# Phishing trends

Attackers use a variety of phishing techniques to try and trick recipients into sharing their private information, making financial transactions, or opening malicious attachments or files.

A common type of phishing reported to CERT NZ is email phishing – where attackers target large contact lists in order to reach as many people as possible. Phishing emails can be hard to spot as attackers often make them look like they're from a well-known organisation. The emails usually replicate the organisation's branding, use similar language and URLs, and spoof the email address to appear legitimate.

Attackers are opportunistic and often evolve campaigns in response to current events and trends in global behaviours.

For example, in Q4 we saw a spike in courier delivery phishing emails. With the festive season and increase in gift giving around the globe, CERT NZ received reports of email and text message scams claiming the recipient had a pending parcel delivery that required a small payment for release. However, there isn't any parcel, and it's a trick to get recipients to click on a URL, visit the phishing website and enter their credentials.

Another example in Q4 was a Zoom-branded phishing campaign. With more people working from home, attackers are targeting software that virtually connects people, like the online conference platform Zoom. Attackers sent emails replicating a Zoom meeting invitation in an attempt to get the recipient to view the invite details by clicking the link provided and entering their Microsoft Suite credentials.

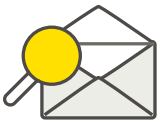

With New Zealand's upcoming COVID-19 vaccination programme, CERT NZ anticipates a rise in Covid-19-related scams.

For more information go to **www.cert.govt.nz/covidscam**

# Protect yourself from phishing


**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 impacted. You'll only need to update the password for the compromised account[2].


**Use two-factor authentication** (2FA) on accounts where possible. It provides an extra layer of security on your account in case your password is compromised[3].



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

**Just ask.** There are no silly questions, especially when it comes to your online security. If you're unsure about an email 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.


**Report it.** If you've received a phishing email or think you've responded to one, get help quickly by reporting it confidentially to CERT NZ[4]. We'll help you work out the steps you need to secure your accounts, and your report means we can get the message out to help protect others.

See CERT NZ's website for more information about phishing[5].

2. www.cert.govt.nz/individuals/guides/how-to-create-a-good-password/
3. www.cert.govt.nz/individuals/guides/two-factor-authentication/
4. www.cert.govt.nz/individuals/report-an-issue/
5. www.cert.govt.nz/business/common-threats/phishing-scams-and-your-business/

# Malware targeting network attached storage devices

Attackers use a variety of techniques to spread malware and get their hands on private information.

In some cases they send malicious software through email attachments or links to infect recipient's computers, in other cases, they target specific internet-exposed services.

Alongside incident reports, CERT NZ monitors data provided by other sources. In Q4, CERT NZ became aware of around 2,000 New Zealand devices infected by malware variant, QSnatch[6]. This malware variant, which first spiked in 2018, specifically targets a widely-used brand of network attached storage (NAS) devices called QNAP.

QSnatch accesses the QNAP device from the internet by exploiting vulnerabilities to bypass the device's password protection.

Once QSnatch has access to the device, it establishes backdoor capabilities allowing the attackers to take control of the device. It then steals passwords and credentials using keylogging and credential scraping. It also stops some software from updating, which prevents the infections from being fully removed.

While QSnatch infections are persistent, our data shows that international agencies have sinkholed the command and control infrastructure's IPs.

This means the attackers are blocked from the infected devices and are unable to send new instructions and harvest user credentials.

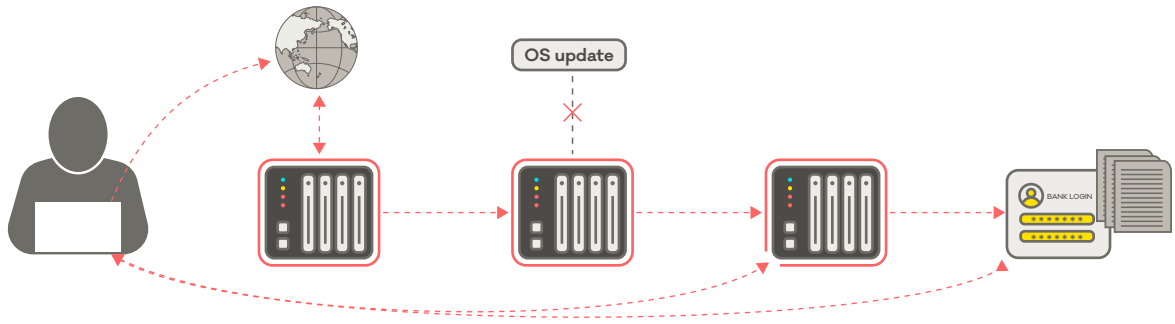
Although the attackers are blocked from communicating with the devices, the devices are still vulnerable to new infections. The attackers can either exploit unpatched vulnerabilities or use previously harvested credentials.

If you use QNAP or another NAS device, CERT NZ recommends:

- keeping firmware and anti-virus software up-to-date
- enabling multi-factor authentication
- configuring logging and alerting to identify suspicious activity
- securing internet-exposed services[7]

If you think your device has been affected, please report to CERT NZ **www.cert.govt.nz/report**

For more information on QSnatch, QNAP published an advisory[8] with detailed recovery steps.




6. Data supplied by cyber threat intelligence provider The Shadowserver Foundation www.shadowserver.org
7. www.cert.govt.nz/it-specialists/critical-controls/securing-internet-exposed-services/
8. www.qnap.com/en/security-advisory/nas-201911-01

Update

# Risk of data breaches continue to rise

In Q3, we highlighted the changes to the Privacy Act 2020[9], including the notifying of data breaches to the Office of the Privacy Commissioner. We also introduced information about potentially vulnerable databases in New Zealand, and the importance of securing them to prevent a data breach and protect customer information.

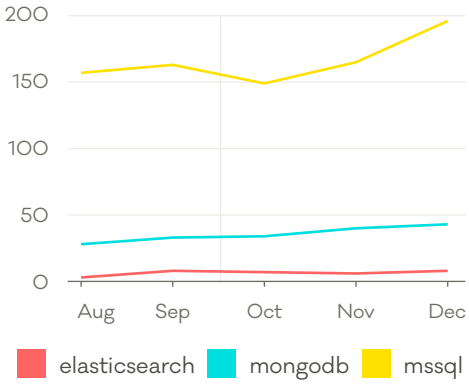
In Q4, the number of vulnerable databases continued to rise, up 26% from Q3.

Databases are a target for attackers because they often hold all sorts of private information. If a database is openly accessible from the internet, attackers can easily access the information it holds, and use it for financial gain. For example, the attacker may threaten to leak the data unless a ransom is paid or sell it to other attackers.

Not only does this lead to a potential data breach of customer information, it can also mean reputational and financial loss for the affected organisation.

From CERT NZ data sources, the top three types of vulnerable databases in New Zealand are Microsoft SQL, MongoDB and Elastic Search, with the largest rise in Microsoft SQL databases.

**Most common vulnerable databases in New Zealand, 2020**




**This data does not include New Zealand organisations using overseas-based cloud providers[10].**

CERT NZ takes an active role in analysing this information. We reach out to the organisations operating the databases to notify them of the possible vulnerabilities, and offer guidance to help secure the databases and protect their customer information.

## Protecting from a data breach

While you may need to engage your IT provider to secure your database, reducing the risk of a data breach is easier than fixing one. CERT NZ recommends the following steps:

- Make sure your databases are not exposed to the internet.
- Make sure your systems have the latest security updates.
- Use long, strong and unique passwords.
- Develop an incident response plan[11] for what to do if your business is affected by a data breach.
- Only collect information that you actually need from your customers and be clear about why you need it, as stated in the Privacy Act 2020.

Case study

# CERT NZ helps New Zealand business secure databases

In Q4, the CERT NZ team identified that 23 seemingly individual Microsoft SQL servers were all linked to one nationally-franchised retail business. All servers were running a variety of versions and were served by a number of ISPs. These potentially vulnerable systems appeared to include back office and point of sale systems.

With this information, we reached out to a central technical contact for the business to advise them of the vulnerabilities and the risk this posed to them and their customers. The business wasn't aware of the issue and are now following CERT NZ's recommended steps to secure their databases.

CERT NZ strongly recommends all businesses and organisations work with their IT provider to check if any databases are internet-exposed and to make sure customer information is secure.

For more information, follow the CERT NZ Critical Controls on patching[12] and securing internet-exposed services[13].

9. www.privacy.org.nz/privacy-act-2020/
10. www.cert.govt.nz/it-specialists/guides/cloud-based-identity-providers-and-authentication/
11. www.cert.govt.nz/business/guides/incident-response-plan/
12. www.cert.govt.nz/it-specialists/critical-controls/patching/
13. www.cert.govt.nz/it-specialists/critical-controls/securing-internet-exposed-services/

Insight



# Partnering for positive outcomes

CERT NZ operates as a central front door for New Zealanders to report cyber security incidents, handling some incidents on our own and working alongside partner and referral agencies for incidents where they may be better placed to help.

Our partner and referral agencies include:

- Commerce Commission
- Consumer Protection
- Department of Internal Affairs
- Domain Name Commission
- National Cyber Security Centre
- New Zealand Telecommunications Forum
- NZ Police
- Office of the Privacy Commissioner

Every quarter, we work with these partners and in Q4, CERT NZ referred 368 incidents.

In the following case study, we highlight an example of how the CERT NZ incident response team worked with NZ Police to resolve a cyber security incident.

Case study

## Working together to recover half a million dollars following invoice scam

In Q4, an owner/operator business reported a scam to CERT NZ. They had received what they thought was a legitimate email from an overseas supplier with details of a new bank account, requesting the business make invoice payments to the new account number.

The business updated the account details and paid the supplier's invoice. It wasn't until after the payment had been made that the business became concerned it was a scam, and reported to CERT NZ.

CERT NZ worked with the business and discovered an attacker had likely accessed the supplier's email account and sent the scam email in an attempt to redirect any payments to their account instead[14].

CERT NZ quickly referred the incident and reported financial loss to NZ Police's Cyber Crimes Unit. Through their network of international partners, NZ Police helped track the transaction and recover the large payment, before it had reached the attacker's account.

This positive outcome highlights the importance of reporting cyber security incidents as soon as possible and the value of CERT NZ's strong partner network.


If you've been affected by a cyber security incident, report it confidentially to CERT NZ at **www.cert.govt.nz/report**. We're here to help.



14. www.cert.govt.nz/business/common-threats/business-email-compromise/