certnz

# Quarterly Report: Highlights Q3 2020

1 July - 30 September, 2020

New Zealand Government

Rob Pope, Director

# Director's message

**"Helping all New Zealanders keep secure online and build their cyber resilience is at the heart of what we do at CERT NZ. "**

Our data shows there's no let-up in the number of cyber security incidents affecting New Zealanders. Targeting everyone from intermittent internet users to those navigating the IT sector, attackers don't discriminate. They're constantly evolving their techniques and seeking out opportunities to disrupt services, and access private information and finances.

From July to September 2020, CERT NZ received over 2,600 reports of cyber security incidents; the highest number of reports to date. In this quarter's report we unpack the rise in attacks on email users and their contacts, including the distribution of malicious software and unauthorised access of business accounts. We look at the impacts these attacks can have on everyday New Zealanders and offer simple steps to help secure this vital communication tool.

When the online platforms we rely on every day – whether it's to carry out business transactions or stay in touch with friends and family – are at risk of a cyber attack, it's crucial that New Zealanders have a trusted source to turn to for help and advice.

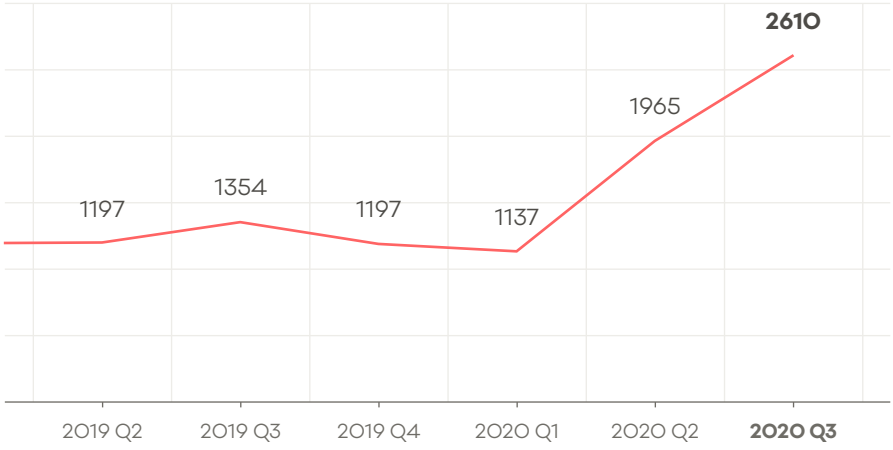
Helping all New Zealanders keep secure online and build their cyber resilience is at the heart of what we do at CERT NZ. That's why we're committed to the continuous improvement in the way we collect and structure data, and the information we share.

We've recently introduced more data sources from local organisations and international partners. This further improves our understanding of the cyber security risks people and organisations are facing here in New Zealand and around the globe.

Alongside the introduction of new data, we've also increased CERT NZ's incident response capacity. Not only is this core function key in assisting people recover from cyber attacks, it also provides unique insights into the types of incidents impacting New Zealanders at home and at work.

It's through combining and analysing these sources that we're armed with the right information to alert New Zealanders to current cyber security risks, and share actionable advice and guidance to help safeguard against and recover from an attack.

## Incidents reported to CERT NZ

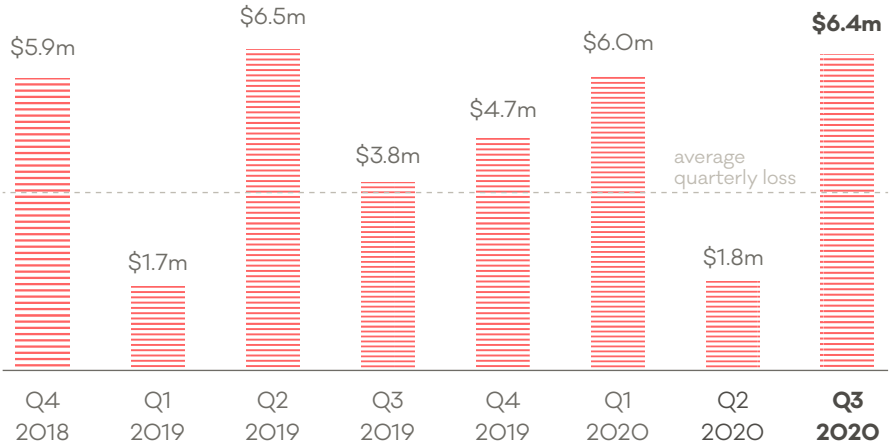



# 2,610

incidents were reported to CERT NZ in Q3 2020.

▲ **33% increase**
from Q2 2020.

## Direct financial loss

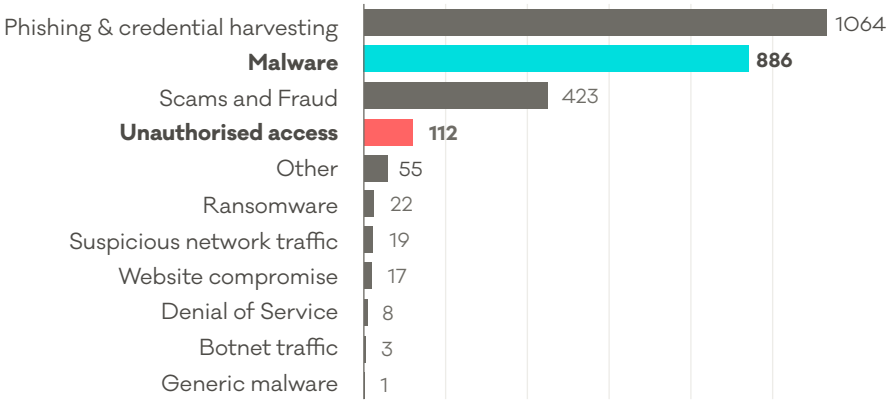



# $6.4m

in direct financial loss was reported in Q3.

▲ **255% increase**
from Q2 2020.

## Breakdown by incident category




**34% (886)** of all incident reports were about **malware**, compared to 1.4% (27) of reports in Q2.

**101% increase** in **business email compromise** in Q3. Business email compromise is a type of **unauthorised access.**

**8 DDoS** incidents were directly reported to CERT NZ in Q3 and **4,473 reports were received from cyber threat intelligence provider The Shadowserver Foundation**[1].

# Putting data in perspective

**Averages per quarter**

Incident reports
**1,295**[2]

Quarterly loss
**$3.6m**

with a total of $50.3m in direct financial losses reported to CERT NZ.



1. www.shadowserver.org
2. Based on 14 quarters, CERT NZ launched in Q2 2017.

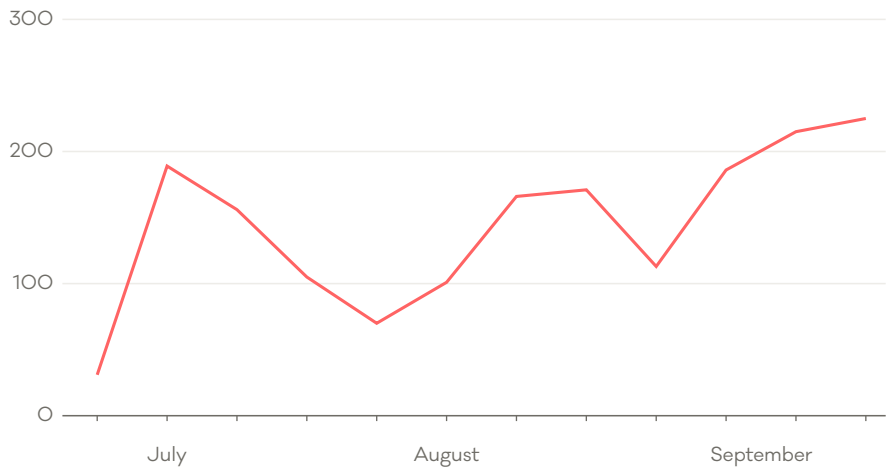
# Distributed Denial of Service (DDoS) attacks impact kiwi businesses

This year a number of DDoS attacks have impacted both high profile organisations and small businesses around the country. These attacks are malicious attempts to overload an organisation's online systems and take their operations offline.

In Q3, CERT NZ's data shows a high volume of attacks on New Zealand networks. Alongside incidents reported to CERT NZ, further data from The Shadowserver Foundation[3] has provided richer insights into the extent of the attacks.

The data shows a series of DDoS attacks throughout the quarter, with numbers peaking at 87 attacks on unique New Zealand IP addresses in one day.

**DDoS attacks on NZ networks – Q3 2020**



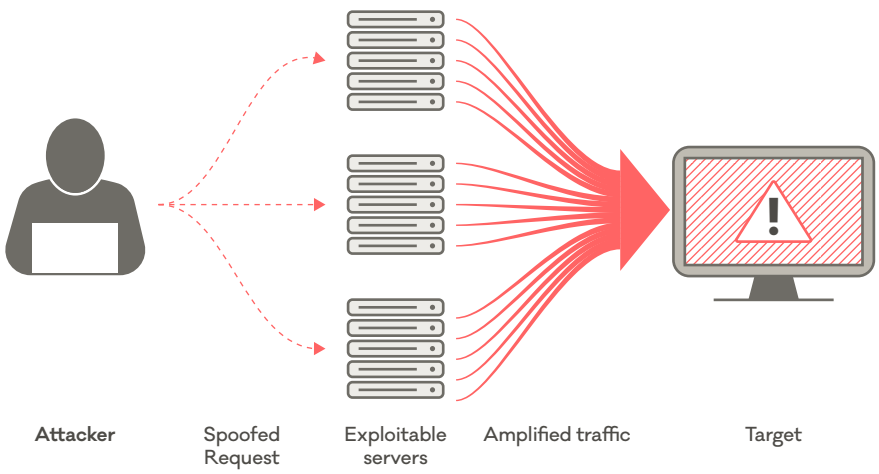

Data source: The Shadowserver Foundation

## Type of attack and outcomes

Of the 4,473 DDoS attacks tracked by CERT NZ, 96% were volumetric attacks. This DDoS technique is where attackers exploit vulnerabilities in networking protocols in order to generate high volumes of traffic. This traffic is directed at the target, either the server or network, to try to overload it and make it inaccessible to users.

In some of these cases the DDoS attacks resulted in the targeted organisation's websites and services being taken offline. Alongside the organisation's online services being disrupted, these attacks can result reputational damage and loss of revenue.

**Volumetric DDoS Attack**




3. The Shadowserver Foundation is a not-for-profit cyber threat intelligence foundation which supplies free public good information to network operators and national CERTs. Organisations which operate their own networks can subscribe to free daily threat reports from Shadowserver about threats in their IP space. For more information visit https://www.shadowserver.org/.

# Defending your organisation

Like many cyber incidents, there isn't a one-size fits all approach to defending against a DDoS attack. That's why it's important to have the right defences in place.

We've recently published advice and guidance for IT specialists on best practices to defend against a DDoS attack.

**https://www.cert.govt.nz/it-specialists/guides/preparing-for-denial-of-service-incidents**

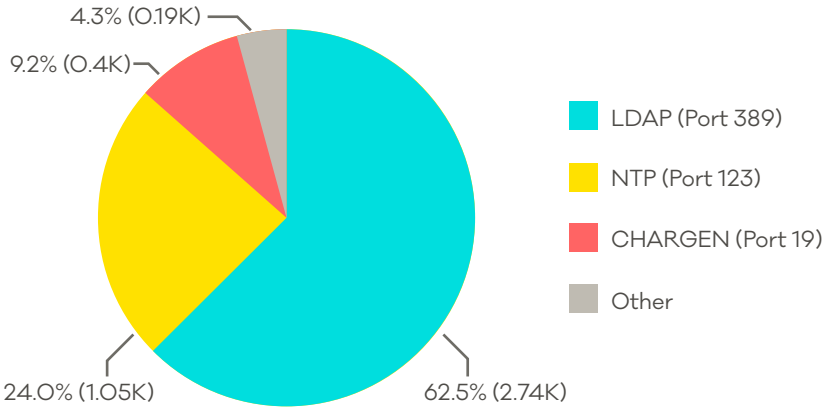
# Protecting New Zealand

As part of CERT NZ's role in building New Zealand's cyber resilience, we're working to help reduce the amount of insecure systems in the country. That's why we're reaching out to ISPs to alert network owners of systems that can potentially be exploited by an attacker to cause a DDoS.

There are many different protocols attackers can exploit. In the campaigns we observed in September and October, attackers exploited three protocols in particular to carry out volumetric DDoS attacks. (see Protocols of DDoS attacks graph)

This quarter, there were 342 unique IP addresses in New Zealand identified with one of these three protocols that could be exploited to carry out DDoS attacks. If your organisation is running these servers, CERT NZ recommends talking to your IT service provider to make sure the servers are inaccessible from the internet and configured so they can't be exploited. Carrying out these checks will help reduce New Zealand's exposure to DDoS attacks.

**Protocols of DDoS attacks – Q3 2020**





If you are concerned that you or your business or organisation has been the target of a DDoS attack, please report to CERT NZ **www.cert.govt.nz/report**. We're here to help and provide advice and guidance to assist in recovery.

# Changes to our data

From 1 July this year, CERT NZ has made some changes to the way we collect and structure data. These changes will improve the level of detail and reporting we produce. These changes also allow CERT NZ to introduce new data sources, as included in this quarter's Focus Area on DDoS attacks.

With these changes, a small amount of historic data has been recategorised and minor amendments made to make sure the data sets remain as accurate and consistent as possible.

More information on how we gather and report data can be found in 'About our information' in the Quarterly Report Data Landscape document.

# Email users affected by Emotet

In Q3, malware reports increased by 34% making it the second highest incident category.

Malware is malicious software often spread through email attachments or links with the goal of infecting the recipient's computer systems.

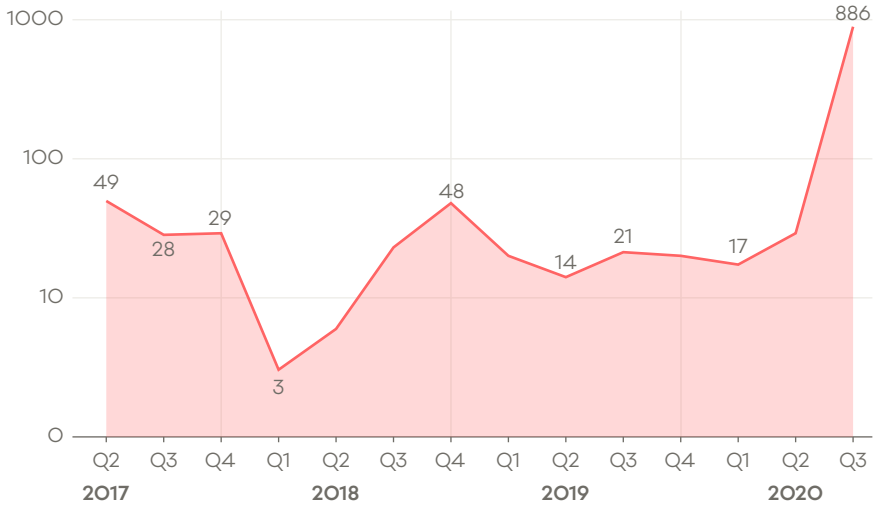
In last quarter's Highlights Report, we explored the rise of multi-stage malware attacks. In this quarter, through direct reports from New Zealanders, and data provided by information sharing partners, these numbers have sharply increased. Of the total malware incidents reported, 96% were attributed to the multi-stage malware variant, Emotet.

Emotet is constantly being developed and is self-replicating. It spreads via emails containing a malicious attachment or link that the recipient is prompted to open. If the recipient opens the attachment, Emotet is installed onto the computer, which has modules to steal data, passwords and other sensitive information. Once installed, it compromises the recipient's email account and sends copies of the email to the recipient's contact list to further spread Emotet. It also allows other malware and ransomware variants to be installed, like Ryuk.

In response to this spike, CERT NZ is reaching out to ISPs where reports of compromised IP addresses have been received. This enables the ISPs to alert their customers to the infection and help them respond and recover.

CERT NZ also received a large number of reports from an international partner about New Zealand email addresses that had been infected. With this information, we contacted the affected account holders directly to provide advice on how to remove the malware and resecure their accounts.

**Malware attacks**




## Protect from Emotet

To help prevent an Emotet infection, CERT NZ recommends:

- Keeping anti-virus software up-to-date.
- If you are unsure that an attachment is legitimate, contact the sender via phone or text to confirm.
- Reporting any suspicious emails to CERT NZ **www.cert.govt.nz/report**.

In September, CERT NZ issued an advisory about Emotet[4]. It includes information on protections as well as steps to take if you or your organisation has been infected.

For more information on multi-stage malware, see our Quarter One and Quarter Two Highlights Report

**www.cert.govt.nz/about/quarterly-report/quarter-one-and-two-report-2020/**

4. https://www.cert.govt.nz/it-specialists/advisories/emotet-malware-being-spread-via-email/

# Increase in business email compromise

## New Zealanders report close to a million dollars in losses

Business email compromise is one of the most common types of unauthorised access reported to CERT NZ. Our Q3 data shows this type of attack is increasing, with 27 reports of business email compromise, up 101% from Q2, and $944,000 in direct financial loss.

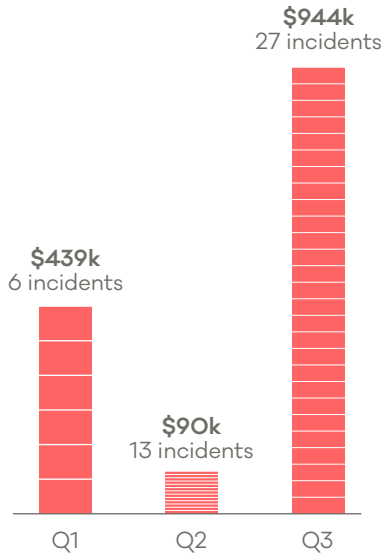
Business email compromise is when an attacker gains access to a business's email account and carries out a range of attacks or scams, usually for financial gain.

There are multiple ways attackers gain can get access to business email accounts, including through weak passwords, credential dumps, malicious software, and phishing campaigns.

Unfortunately, attackers are increasingly sophisticated in their techniques and the compromise isn't often detected until the attacker has successfully carried out the scam.

In the following case study, we share a recent business email compromise report, and provide preventions and mitigations to help keep your email secure.

**Business email compromise incidents – 2020**




46 reports of business email compromise were received in 2020, with over $1.4 million in direct financial loss reported.

## Case study: compromise leads to redirected payments

This quarter CERT NZ received a report from a business in the wholesale trade sector after an email account had been compromised.

The CEO's email account was previously a target of a phishing campaign, where they had unknowingly entered their login credentials. Using these credentials, the attacker was able to access the CEO's email account.

Once the attacker had the CEO's login credentials, they accessed the CEO's email account and set up auto-forwarding rules so that all incoming and outgoing emails were automatically sent to the attacker's account. The attacker monitored the communications for a number of weeks, the attacker became aware that the business was implementing new management software. The attacker waited for the vendor to submit their invoice, and the CEO to authorise the payment, the attacker then swapped the vendor's bank account number to direct payment to their nominated account.

Initially the scam went unnoticed, and the invoice of $180,000 was paid into the overseas account nominated by the attacker.

Unfortunately, it wasn't until the vendor confirmed the payment hadn't been received that the business realised the scam. They immediately reported it to their bank and CERT NZ.

CERT NZ helped establish the cause of the attack and provided steps to secure the email account and help prevent any further attacks.

We reported the incident and financial loss to NZ Police. Due to the amount of time that the scam went undetected, the payment wasn't recovered.

### Protect from business email compromise

- Use long, strong and unique passwords on all accounts. Encourage staff to do the same.
- Apply two-factor authentication (2FA) to cloud and email accounts[5].
- Verify payments to new accounts by phone or SMS.

### If you're affected

- Check auto-forwarding rules on business email accounts, and immediately remove any you're not familiar with.
- Change the account password, making sure it's long, strong and unique.
- Implement 2FA.
- Ask your IT provider to check your system for any installed malware.
- Report to your bank and to CERT NZ **www.cert.govt.nz/report**. In some cases early reporting can result in the recovery of redirected payments.

5. https://www.cert.govt.nz/individuals/guides/getting-started-with-cyber-security/two-factor-authentication/

# Changes to the Privacy Act 2020

The new Privacy Act 2020 comes into effect on 1 December 2020.

## What this means for businesses and organisations.

These changes include the introduction of a privacy breach notification regime. If a business or an organisation experiences a data breach where private information is lost or stolen, and believes this could result in serious harm, it is required to notify the Office of the Privacy Commissioner (OPC) and affected individuals as soon as possible. To help businesses and organisations, the OPC has an online privacy breach notification tool on its website called NotifyUs[6]. This and other Privacy Act 2020 resources can be found on the OPC website[7].

## Vulnerable databases and keeping your customer information safe.

Unfortunately data breaches do happen, but the good news is there are measures you can take to help prevent an incident and keep your customers' information and data secure.

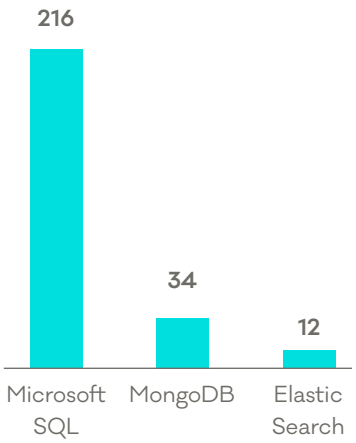
The upcoming changes are a timely reminder to check your business or organisation's databases and make sure you're doing all you can to secure customer information

We receive regular reports about vulnerable databases in New Zealand. In Q3, the top three types of databases reported to CERT NZ were Microsoft SQL, Mongo DB and Elastic Search.

Alongside databases, we received 6,800 reports about other technologies that are openly accessible to the internet, including File Transfer Protocol (FTP) servers.

Whether you operate these systems, or others, CERT NZ recommends considering whether they need to be hosted on the internet, and regularly maintaining databases to make sure information stored is secure. More information on how to implement these measures are included in our critical controls on patching[8] and securing internet-exposed services[9].

**Top three New Zealand databases with vulnerabilities reported to CERT NZ in Q3 2020**




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

For more on the New Zealand threat landscape in Q3 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.**

6. https://www.privacy.org.nz/privacy-for-agencies/privacy-breaches/notify-us/
7. https://www.privacy.org.nz/privacy-act-2020/resources/
8. https://www.cert.govt.nz/it-specialists/critical-controls/patching/
9. https://www.cert.govt.nz/it-specialists/critical-controls/securing-internet-exposed-services/
10. https://www.cert.govt.nz/it-specialists/guides/cloud-based-identity-providers-and-authentication/