certnz

Quarterly Report: Highlights Q1 2021

1 January - 31 March

New Zealand Government

Director’s message

Rob Pope, Director

We all have a role to play in helping build a cyber-resilient New Zealand.

We often talk about the impacts cyber security incidents have on New Zealanders and the work we do to help in response and recovery – and with more than 1,400 incidents reported with an associated $3 million in financial loss this quarter, there’s a lot to cover.

However, our focus isn’t all big numbers and bad news. Our efforts are also aimed at arming New Zealanders with relevant advice and support to combat cyber security risks and minimise impact. That’s why at CERT NZ we’re always working to improve our services and continuing to develop ways to identify and disrupt malicious cyber activity before its impacts are widely felt.

In this report, we highlight some of the proactive work we are doing behind-the-scenes to halt phishing and scam attacks, and help keep New Zealanders secure online. We don’t do this work alone. Like we’ve seen with the country’s COVID-19 response, we know that a collaborative approach brings the best results. We work alongside our national and international partners to share high-confidence insights and communicate risks. The results show the more we do this, the better our shared understanding of the cyber security threat landscape is – and the better equipped we are to identify and disrupt cyber security risks, and reduce the impacts on New Zealanders.

This proactive work doesn’t stop with us, the responsibility to keep secure online extends to all New Zealanders. Whether it’s following the internal security controls in our workplaces or keeping checks on how we share our personal information and who we share it with – we all have a role to play in helping build a cyber-resilient New Zealand.

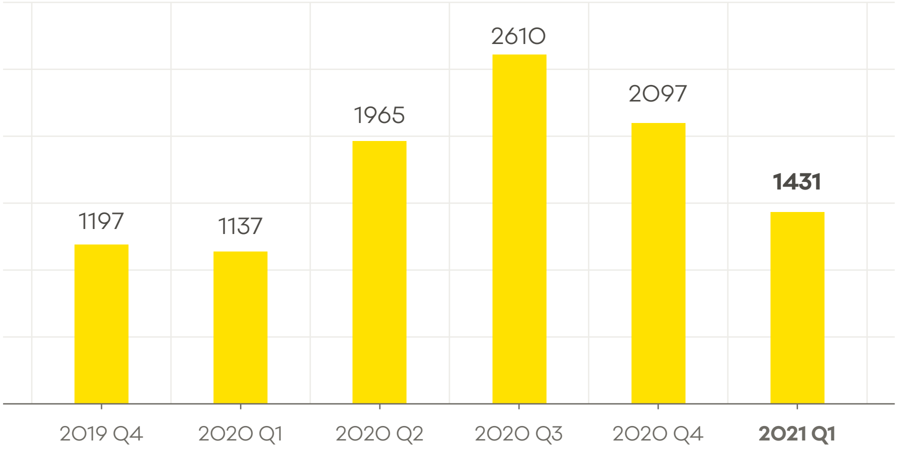
Incidents responded to by CERT NZ

1,431

incidents were responded to by CERT NZ in Q1 2021.

▼ **32% decrease**

from Q4 2020.



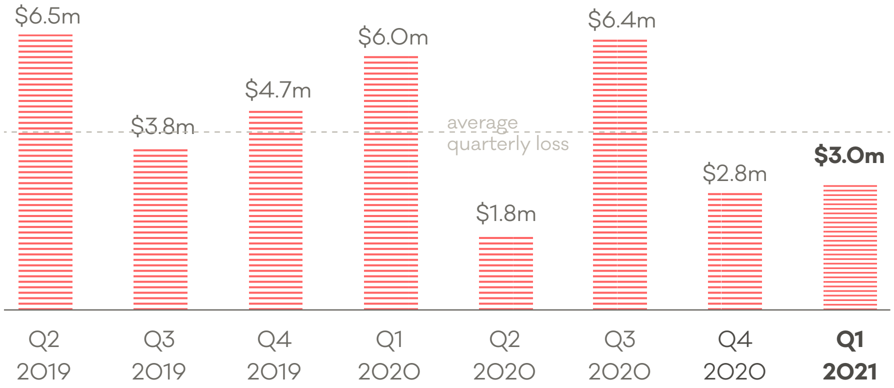
Direct financial loss

$3.0m

in direct financial loss was reported in Q1 2021

▲ **7% increase**

from Q4 2020 with 23% of incidents reporting financial loss.



Putting data in perspective

Average incidents*

1,569

Average loss*

$4.2m

Total losses reported to CERT NZ

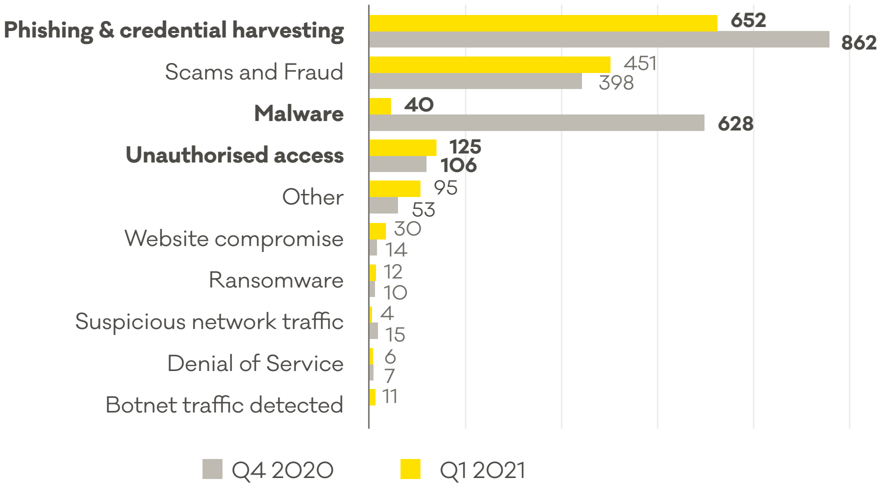
$56.0m

since Q2 2017

*figures based on previous eight quarters

For more on the New Zealand threat landscape in Q1 2021, see the CERT NZ Quarterly Report: Data Landscape. www.cert.govt.nz/about/quarterly-report/

Breakdown by incident category



18% increase in reports about unauthorised access from Q4 2020.

24% decrease in phishing and credential harvesting from Q4 2020.

94% decrease in malware from Q4 2020, due to international agencies successfully dismantling the Emotet malware infrastructure.

Cutting the line on phishing campaigns

Phishing and credential harvesting is one of the most reported incident types to CERT NZ, making up 46% of all incident reports in quarter one. In last quarter's Highlights Report[1], we covered trends in phishing and credential harvesting and shared tips on how to protect against it. In this quarter's focus area, we dive a little deeper into CERT NZ's proactive work in disrupting these types of attacks.

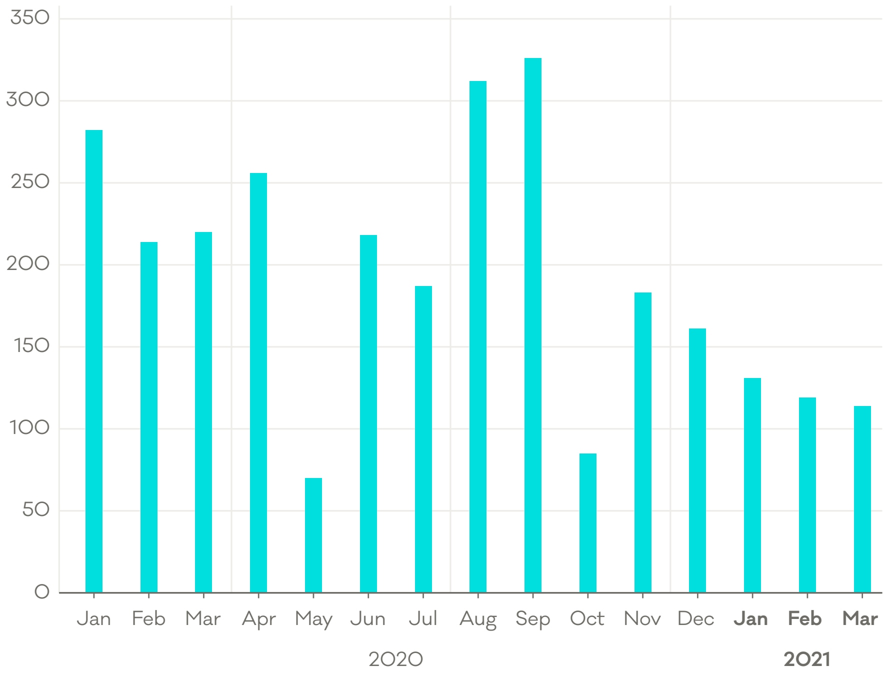
Phishing campaigns can have a big impact on individuals through to large organisations, and can result in financial, data, operational and reputational losses. Often phishing is a precursor to other attacks and scams, like email compromise and data leaks.

Attackers are constantly evolving phishing campaigns and their attempts to gather financial and personal information can vary, meaning phishing campaigns can be tricky to spot and easy to fall for.

To help reduce the impacts of phishing on New Zealanders, CERT NZ has been working with partners to share high-confidence and actionable information about phishing incidents specifically affecting New Zealanders, and misrepresenting New Zealand brands.

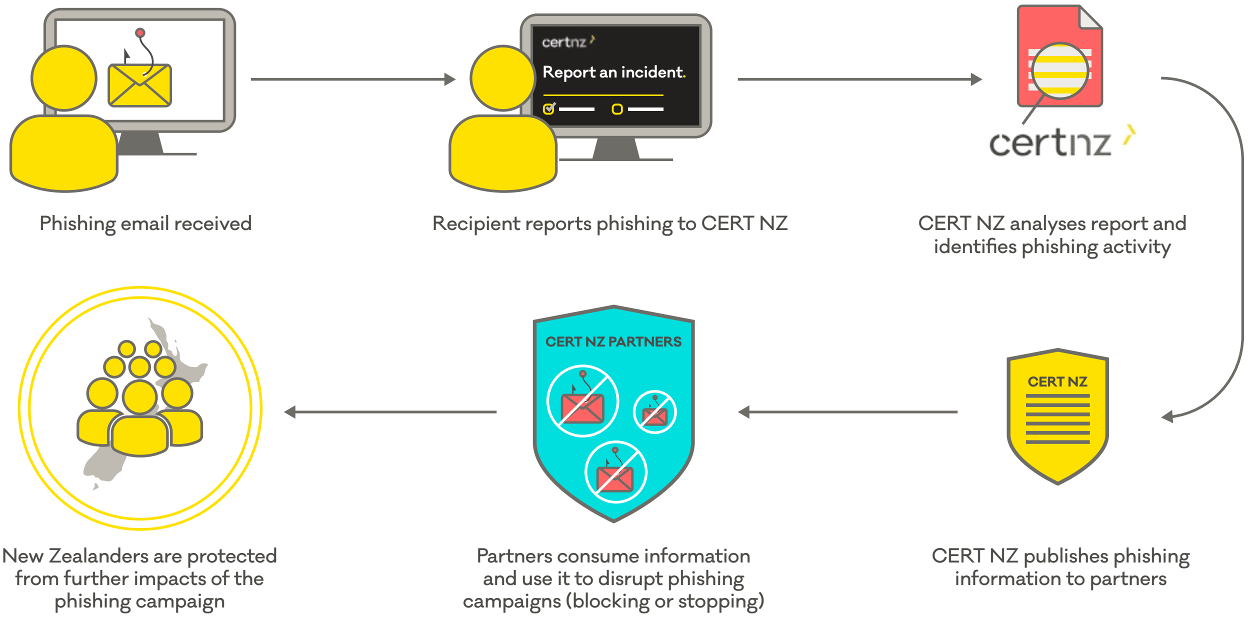
The information comes from third parties and reports made to CERT NZ. CERT NZ's team then collates and analyses the phishing data and identifies indicators of malicious activity. CERT NZ then publishes the indicators for New Zealand internet service providers, email providers and security providers. With this information, the providers can automatically protect their customers and disrupt the identified phishing campaigns. This may include stopping phishing emails before they reach people's inboxes or blocking user access to a phishing website.

Number of phishing indicators identified by CERT NZ



[1] https://www.cert.govt.nz/about/quarterly-report/quarter-four-report-2020/

How CERT NZ is working to disrupt campaigns and protect New Zealanders


certnz
Report an incident.
certnz
CERT NZ PARTNERS
CERT NZ
Phishing email received
Recipient reports phishing to CERT NZ
CERT NZ analyses report and identifies phishing activity
CERT NZ publishes phishing information to partners
Partners consume information and use it to disrupt phishing campaigns (blocking or stopping)
New Zealanders are protected from further impacts of the phishing campaign

What this means to New Zealanders

This process aims to stop phishing campaigns before they cause wide-spread harm. This means the more phishing information we can provide partners, the more phishing campaigns we can disrupt – and the better protected New Zealanders are.

What you can do

If you think you've received a phishing email, report it to www.cert.govt.nz/report.

1. We'll provide guidance to make sure you and your accounts are not at risk.
2. We'll analyse the report for phishing indicators and use the findings to alert partners and notify other New Zealanders before they're impacted.

CERT NZ working to reduce the impacts of COVID-19 vaccine scams

Alongside incident response, CERT NZ works to identify, understand and alert New Zealanders to possible cyber security threats, and provide actionable advice to help protect against them. The COVID-19 vaccination roll out is one example of this.

In Q1, CERT NZ began working as part of an inter-agency approach in preparation for New Zealand's COVID-19 vaccine roll out. The Ministry of Health appointed CERT NZ as the central coordination agency for COVID-19 vaccine-related scams and misinformation. We began reaching out to international partners in countries that were already in the vaccination phase to gain a better understanding of the cyber security risks they'd encountered. Findings showed a range of attacks from phishing campaigns to more targeted attacks on the key operational organisations.

Taking this information and pairing it with findings from other NZ agencies, we've gained a wider understanding of possible cyber security risks around the roll out. We've used this information to develop an evidence-based approach to detect and resolve anticipated cyber incidents here in New Zealand.

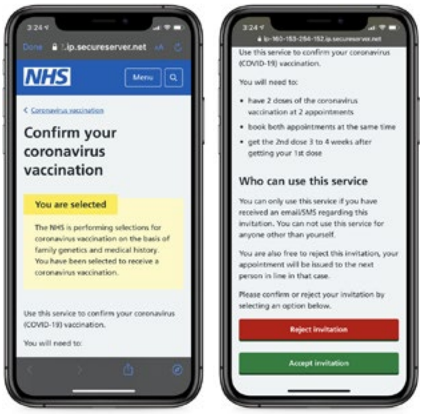
From here, CERT NZ has been alerting both the organisations involved in the vaccine roll-out and New Zealanders awaiting the vaccination to the possible COVID-19 vaccine-related scams and what to look out for.

What to look out for

Attackers are opportunistic and are constantly evolving their campaigns to try and trick people into sharing their financial and personal information. The COVID-19 vaccine-related scams are no exception.

Others are an attempt to collect login credentials asking recipients to enter personal information like usernames and passwords – this information is then often used to carry out attacks like email compromise.

In Q1, CERT NZ responded to less than ten reports about COVID-19 vaccine-related scams. We anticipate the volume of the scams will increase, and vary in look and messaging. **The easiest thing to remember is the COVID-19 vaccine is free. At no point will you be asked to pay for the vaccine, or pay for your place in the queue. If you are, it's likely a scam.**



Confirm your coronavirus vaccination

You are selected

The NHS is performing selections for coronavirus vaccination on the basis of family genetics and medical history. You have been selected to receive a coronavirus vaccination.

Use this service to confirm your coronavirus (COVID-19) vaccination.

You will need to:

Use this service to confirm your coronavirus (COVID-19) vaccination.

You will need to:

- have 2 doses of the coronavirus vaccination at 2 appointments
- book both appointments at the same time
- get the 2nd dose 3 to 4 weeks after getting your 1st dose

Who can use this service

You can only use this service if you have received an email/SMS regarding this invitation. You can not use this service for anyone other than yourself.

You are also free to reject this invitation, your appointment will be issued to the next person in line in that case.

Please confirm or reject your invitation by selecting an option below.

Scam email example pretending to be from UK's National Health Service.

If you think you've received a COVID-19-related scam, please report it to us www.cert.govt.nz/covid-scams

Attackers target widely-used email servers

In Q1, CERT NZ received reports about attackers exploiting vulnerabilities on New Zealand servers running Microsoft Exchange – a widely-used email and calendar service.

During the quarter, CERT NZ identified almost 500 vulnerable Microsoft Exchange email servers and over 100 compromised email servers. The majority of the compromised mail servers belonged to small businesses, with a number of large organisations also affected.

The attackers exploited four newly-discovered Microsoft Exchange vulnerabilities to gain access to the Microsoft Exchange Server.

The attackers begin by scanning for vulnerable targets on the internet. They then send a malicious request to the server to gain unauthenticated access. Once they have access, they deploy a web shell (backdoor) that allows the attackers to steal data, view emails on the server as well as send emails and carry out further malicious activity like ransomware, phishing and invoice scams.

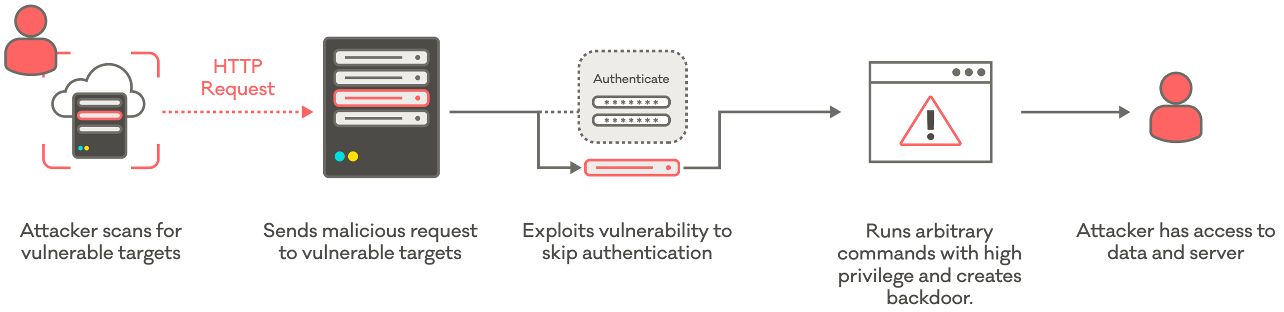
In response, CERT NZ quickly issued an advisory alerting New Zealanders to the issue and included steps to prevent and mitigate possible attacks[2]. CERT NZ also contacted ISPs with information on vulnerable and compromised IP addresses, and provided resources they can forward to the affected individuals and businesses.

If you use Microsoft Exchange, CERT NZ strongly recommends the following steps.

- Immediately apply the latest security updates for your version of Microsoft Exchange and Antimalware if possible, including Microsoft's One-click Microsoft Exchange On-premises mitigation tool and scanning tool[3]
- Change any passwords related to your Microsoft Exchange servers. Attackers can try to use stolen passwords to compromise other systems or regain access.

If you think your server may have been affected, please report to CERT NZ www.cert.govt.nz/report.

How attackers gain access to Microsoft Exchange servers


HTTP Request
Authenticate
Attacker scans for vulnerable targets
Sends malicious request to vulnerable targets
Exploits vulnerability to skip authentication
Runs arbitrary commands with high privilege and creates backdoor.
Attacker has access to data and server

[2] https://www.cert.govt.nz/it-specialists/advisories/updates-released-for-new-critical-vulnerabilities-in-microsoft-exchange/

[3] https://www.microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange-servers/

Simple steps can help New Zealand businesses keep cyber attackers out

In Q1, reports to CERT NZ about unauthorised access increased 18% from the previous quarter, with a direct financial loss of close to $1 million. Unauthorised access is when an attacker gains access to accounts without the account holder's knowledge. In some cases the attackers gain access to an account because it has a weak or reused password, or the attacker has sourced login credentials from a data breach or phishing campaign.

Once an attacker has access they can use this to carry out a range of attacks usually for financial gain. This can include compromising an email account to distribute phishing campaigns, stealing sensitive data and intercepting bill payments and invoices.

Often businesses are targets of this malicious activity, with more and more financial transactions carried out online. One example of this in quarter one, was an incident reported by a New Zealand business. They noticed a reliable customer had missed an invoice payment for tens of thousands of dollars. They called the customer who informed them they had made the payment, and paid the money to the new bank account number the business had sent them a couple of days earlier. However, the business had not sent the email to update the payment details, an attacker had accessed the business's account and been monitoring emails for some time. Knowing when an invoice was due, the attacker sent an email pretending to be from the business to the customer to get the payment redirected to the attacker's account.

The business quickly reported the incident to CERT NZ, where we helped the business resecure accounts. We also referred the loss to NZ Police who were able to freeze the attacker's bank account and recover the money.

Although unauthorised access is a constant threat to businesses, there are simple steps staff can take to help protect your accounts.

- Encourage staff to use long strong and unique passwords across all accounts by implementing a password policy[4]
- Add an extra layer of security to the login process by turning on two-factor authentication (2FA)[5]

For more actionable information to make sure you've got your business covered, check out CERT NZ's top 11 cyber security tips for business[6].

If you think you may have been affected, please report to CERT NZ www.cert.govt.nz/report.

[4] https://www.cert.govt.nz/business/guides/password-policy-for-business/
[5] https://www.cert.govt.nz/individuals/guides/two-factor-authentication/
[6] https://www.cert.govt.nz/business/guides/top-11-cyber-security-tips-for-your-business/