certnz

Quarterly Report: Highlights Q4 2021

1 October - 31 December

New Zealand Government

Director's message

Rob Pope, Director

The numbers in this report are some of the highest we've seen in the four years CERT NZ has been operating. However, big numbers aren't all bad news.

The increase in reports demonstrates that New Zealanders are becoming more aware and better skilled at recognising cyber security incidents. It also shows that New Zealanders know where to turn for guidance when they need to get back up and running – which is a good thing, and something we want to see more of. We're here to help people and businesses at the time when they need it most.

On the downside, this quarter New Zealanders reported more than $6 million in direct financial loss to cyber security incidents, and that doesn't cover the impacts of data and operational losses. While we work with partner organisations to recover some of these funds, the best course of action is always prevention.

That's the reason CERT NZ promotes steps like using long, strong and unique passwords, turning on two-factor authentication and keeping software up to date. They're simple actions, but they do make a big difference. Taking these steps significantly reduce the chance of 'cyber baddies' getting a toehold into your online accounts and systems.

While we encourage New Zealanders to take action, the CERT NZ team are also scanning the threat landscape for new risks.

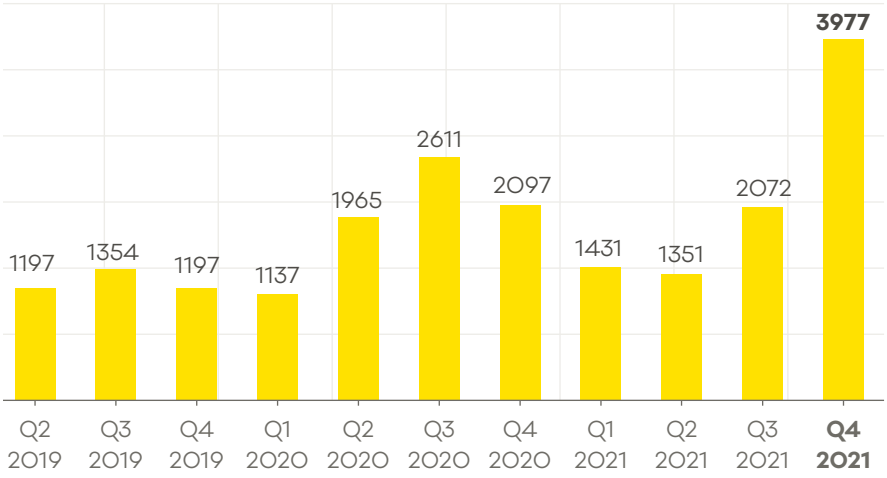
Incidents, like the Log4j vulnerability discussed in this report, have shown that, as new threats arrive, vigilance is the best defence. I'm proud to say that CERT NZ was the first government agency in the world to send out an advisory on Log4j. And while no harm has yet been reported, we remain on alert and ready to respond.

It goes to show, having a 'fence at the top of the cliff' like CERT NZ, is beneficial to all New Zealanders.

Incidents responded to by CERT NZ

3,977
incidents were responded to by CERT NZ in Q4 2021.

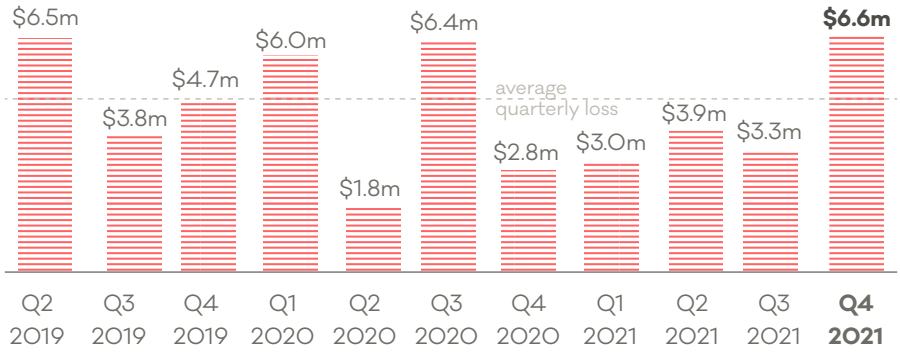
▲ **92% increase**
from Q3 2021.



Direct financial loss

$6.6m
in direct financial loss was reported in Q4 2021.

▲ **100% increase**
from Q3 2021, with 11% of incidents reporting financial loss



Putting data in perspective

Average incidents reported per quarter*
1,733

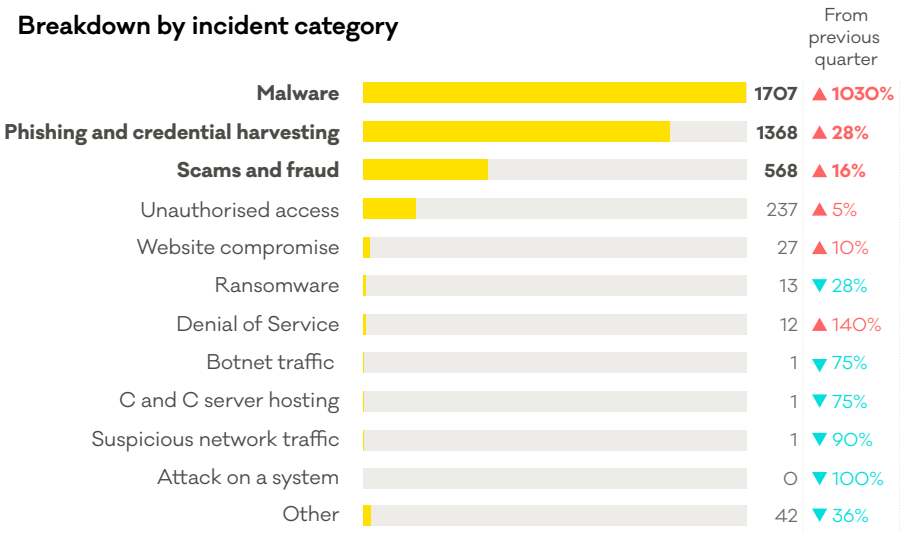
Average loss reported per quarter*
$4.0m

Total losses reported to CERT NZ
$69.8m
since Q2 2017

*figures based on previous eight quarters

For more on the New Zealand threat landscape in Q4 2021, see the CERT NZ Quarterly Report: Data Landscape. **www.cert.govt.nz/about/quarterly-report/**

Breakdown by incident category



Reports about malware increased 1,030% from Q3 2021.

Phishing and credential harvesting reports increased 28% from Q3 2021.

Scams and fraud reports increased 16% from Q3 2021.

Log4j vulnerability

In December a critical security vulnerability in an open-source software component called Log4j was made public.

Log4j is widely used in software applications, which means the vulnerability immediately put thousands of businesses and organisations in New Zealand at risk. An update was quickly made available, however any lag in discovering the software's use on systems and applying the update provided a window for attackers to seek access to systems.

What is Log4j?

Log4j is a Java-based logging software component used to carry out numerous tasks, including recording and communicating warning or error messages. Common examples include recording what types of devices are accessing your website or when someone tries to access a missing file on your website resulting in a "404 error" message.

Log4j is part of a software supply chain which means it is used in many software applications.

> **A software supply chain is similar in function to a physical supply chain. For example, Log4j is like a component in car manufacturing, such as an airbag. The car manufacturer buys the airbags from another supplier and installs them into every car across various models. In day-to-day use you won't notice it's there, but if there's a critical fault with the airbag, the manufacturer may need to do a mass recall. If you don't hear about the recall, or take appropriate action, you could be at risk.**

With so many software applications and services using Log4j, many companies still may not know it's bundled together into the software they use.

How does the vulnerability affect systems?

The Log4j vulnerability, known as Log4Shell, allows attackers to run their own malicious code on a system. The results of this attack can vary and could include a system being controlled remotely, data being stolen, or the system being locked down with ransomware. Once the system is infiltrated, other systems within the organisation can be targeted.

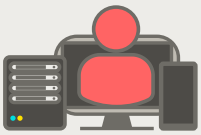
Log4Shell is relatively easy for attackers to exploit, for example some of the first public activity noticed was the malicious code executed in the chat functions of the video game Minecraft.

Any applications that use Log4j could be affected. The vulnerability works by running code logged to the system. This means attackers can send lines of code and instead of logging the text, the system will execute it. This is also known as code injection or execution vulnerability.

Attackers may access systems but don't always take advantage of the access immediately, meaning the compromise may not be discovered until they decide to carry out an attack.

Exploitation of the Log4j vulnerability may be difficult to detect because it allows attackers to carry out various types of compromise, making it more difficult to identify the root cause.

How the Log4j vulnerability works



Attacker prepares malicious code

Attacker pastes malicious code into a logged field, like a chat box

Log4j allows the malicious code to process

The vulnerability allows the malicious code to run and gives the attacker access to the system

The attacker can control the system remotely.

CERT NZ response

CERT NZ was the first government organisation internationally to release advice on the Log4j vulnerability[1]. This information was quickly picked up and circulated by international agencies and media, helping raise awareness of the risk and share advice to help protect against compromise.

Our Incident Response team worked with local and international agencies, to establish an incident coordination and response function, and shared information about how the incident was progressing.

How to protect your systems

As Log4j is widely used, you may not know if it's part of your system. CERT NZ recommends that you talk to your IT team or IT service provider to make sure they're taking the right security steps to help reduce risk.

- Contact your software vendors to find out if they use Log4j, and implement the fixes they provide. This may include updating software to the latest version.
- If solutions aren't available from the vendor, manually updating or applying mitigations for Log4j may be an option.
- Otherwise, isolate the affected devices as much as possible or restrict outbound traffic from the device.
- Keep all software up-to-date.
- Catalogue software you use.

If you know Log4j is in your systems but haven't been affected, it's still important to follow these recommendations. There is a possibility that attackers are quietly monitoring compromised systems.

Because of these factors, CERT NZ anticipates that impacts from this vulnerability will continue and encourages all businesses and organisations to implement and maintain good cyber security practices.

Key Takeaways

- Log4j is a software component used by millions of systems around the globe.
- Attackers are actively scanning for the vulnerability.
- Larger organisations are likely to be targeted first. Due to ease of exploitation, attackers will likely target smaller businesses once larger organisations have patched all systems and are no longer easy to exploit.
- The extensive use of Log4j means some vulnerable software may still be undiscovered, leading to a potential "long-tail" of attacks.
- It may be difficult to determine if a compromise originated through exploitation of the Log4j vulnerability, because:
  - attackers can hide on systems for long periods of time before being discovered
  - the exploit allows attackers to carry out other malicious activity.

For more information go to:

Top tips for businesses - **Top 11 cyber security tips for your business | CERT NZ**[2]

Critical controls - **Critical controls | CERT NZ**[3]

New Zealand's National Cyber Security Council (NCSC) comprehensive guidance on supply chain cyber security **https://www.ncsc.govt.nz/assets/NCSC-Documents/NCSC-Supply-Chain-Cyber-Security.pdf**[4]

1. https://www.cert.govt.nz/it-specialists/advisories/log4j-rce-0-day-actively-exploited/
2. https://www.cert.govt.nz/business/guides/top-11-cyber-security-tips-for-your-business/
3. https://www.cert.govt.nz/it-specialists/critical-controls/
4. https://www.ncsc.govt.nz/assets/NCSC-Documents/NCSC-Supply-Chain-Cyber-Security.pdf

Flubot fallout continues

In Q4, Flubot made up two-thirds of the 1,707 malware incidents reported to CERT NZ. Flubot (which we covered in Q3 2021[5]) began affecting New Zealanders in September. It was sent through text messages containing a malicious website link that if clicked on, downloaded malware to the recipient's phone. Reports of Flubot spiked in the first part of Q4, with a total of 1,107 reports across the quarter.

During that time, CERT NZ updated the Flubot advisory[6] as the content of the text message used to spread the malware varied. We also continued to work with the Department of Internal Affairs (DIA) responding to reports and supplying ISPs with information on the affected URLS.

Across both Q3 and Q4, no direct financial loss was reported as a result of the Flubot campaign. However, those who received the text messages, even if they didn't download the malware, had their phone number logged by the attackers and many are now the targets of further text-scam campaigns.

These subsequent text scams use similar content to the initial Flubot messages, for example parcel deliveries that prompt the recipient to click on a link to confirm delivery.

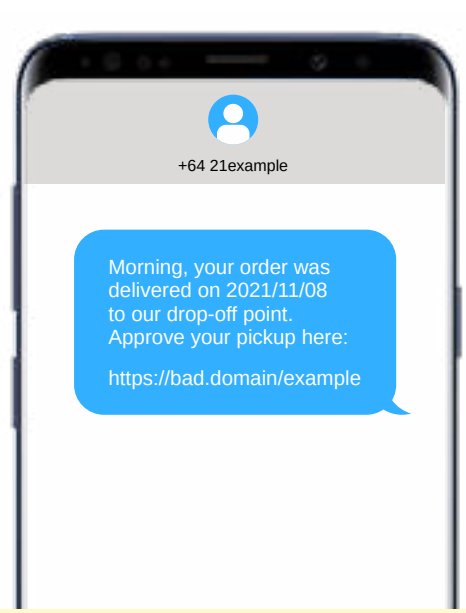
During Q4, CERT NZ received over 150 reports of follow-on text scams. The key difference in the new text scam is the website link goes to a phishing page instead of a page that attempts to trick the recipient into downloading malware.

The phishing page prompts the recipient to enter their personal details and a credit card number in to pay to have the parcel released (typically less than $5). If the recipient pays the fee, they are unknowingly signed up to a subscription that will charge them a higher amount (approximately $85) usually within three days.

How to spot a text scam

- Text scams usually contain a website link and the message will try to convince the recipient to click the link.
- In most cases, legitimate businesses and organisation won't send direct links and ask you to click on them.
- The text contains a website link and is from a number you don't recognise.
- If you suspect a legitimate business has sent you a genuine website link, make sure it matches the business's own website. You can also check with the business's contact centre to confirm the legitimacy of a text message and its contents.

Text-scam example



If you think you've received a text scam

- don't click on any website links or follow any instructions
- block the sender's numbers, either through your phone or with the assistance of your telecommunications company,
- report the text message by forwarding it free-of-charge to 7726. This is a service from the DIA that allows them to investigate the messages further.

If you think you've been affected, please report to **www.cert.govt.nz/report**

5. https://www.cert.govt.nz/about/quarterly-report/quarter-three-report-2021/
6. https://www.cert.govt.nz/individuals/alerts/flubot-malware-infecting-android-phones/

Financial losses from scams and fraud increase

This quarter, CERT NZ received 568 reports about scams and fraud with an associated direct financial loss of $5.9 million, an increase of 269% from last quarter. It is the highest direct financial loss from scams and fraud in a single quarter to date.

Of the scam and fraud incidents reported, the three scam categories with the highest direct financial loss in Q4 were 'buying, selling or donating goods online' ($2.3m), followed by 'investment scams' ($1.8m) and 'a new job or business opportunity' ($1.1m).

Buying, selling or donating goods online

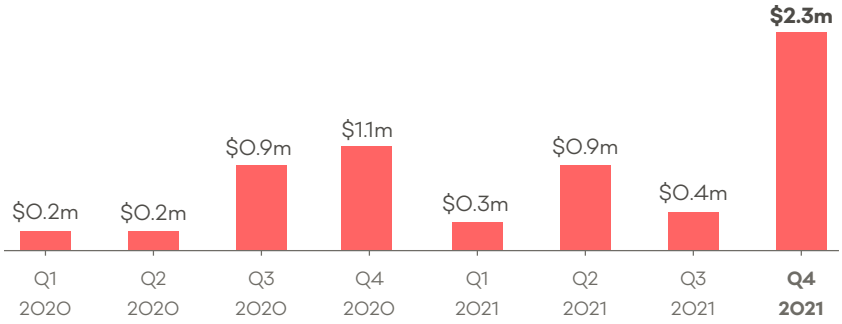
Scammers are opportunistic and always looking for ways to exploit New Zealanders' uptake in online shopping, and this was reflected in the busy holiday season.

This quarter, CERT NZ continued to see many reports of scams about websites operating from overseas that pretend to be legitimate New Zealand-based businesses.

A common example involves scammers outside of New Zealand setting up an e-commerce website using a .nz website address and advertising well-known or expensive products at reduced prices, like popular shoe brands. When people make purchases from the website, they end up receiving a lesser product, a different product or in some cases, nothing at all.

When a .nz website is identified as a scam site, CERT NZ contacts the Domain Name Commission and the hosting provider, with a request for it to be taken down. In some cases, CERT NZ also reports the website to the Financial Markets Authority to issue a warning.

Direct financial loss from 'buying, selling or donating goods' online per quarter



What to look out for

To help work out if an online store is genuine, check

- the domain name owners' address is registered in New Zealand[7]
- the store is a registered New Zealand company[8].

Be wary of websites that do the following.

- Don't list a physical address or have unusual contact information
- Don't display terms of trade (including return policies) or fully disclose costs (such as shipping and delivery).
- Have significantly lower-priced goods. This should raise your suspicion that you might not get what you expect. If a deal is too good to be true it, probably is.
- The URL doesn't seem to match what they're selling. For example, if Bob's Sporting Goods (bobssportinggoods.co.nz) is selling luxury handbags.
- Negative online consumer feedback and reviews.

If you think you have been affected by a scam, please report it confidentially to CERT NZ **www.cert.govt.nz/report**, and immediately notify your bank if you've made a payment or shared payment information.

7. https://www.dnc.org.nz/
8. https://companies-register.companiesoffice.govt.nz/