certnz

Quarterly Report: Highlights Q3 2021

1 July - 30 September

New Zealand Government

Director's message

Rob Pope, Director

The busy holiday season is almost upon us, bringing all the sharing and goodwill we associate with it. However, more so than ever, we need to be careful that our generosity isn't exploited.

Attackers are always looking for opportunities to exploit our online behaviours and catch us off guard with time-specific techniques that aren't always easy to spot. As we highlight in this report, attacks can come in many forms, like a seemingly legitimate text message or through malicious software on your IoT device.

This increasing sophistication in attacks paired with our increasingly busy lives, means that sometimes we can get caught out. So it's really important New Zealanders know where to turn to for support. If you are impacted by a cyber security incident, report it to CERT NZ as soon as possible. The quicker you report, the faster we can work with you and our partner organisations to minimise impact, help recover any funds lost and get you back up and running online –we share an example in this quarter's case study.

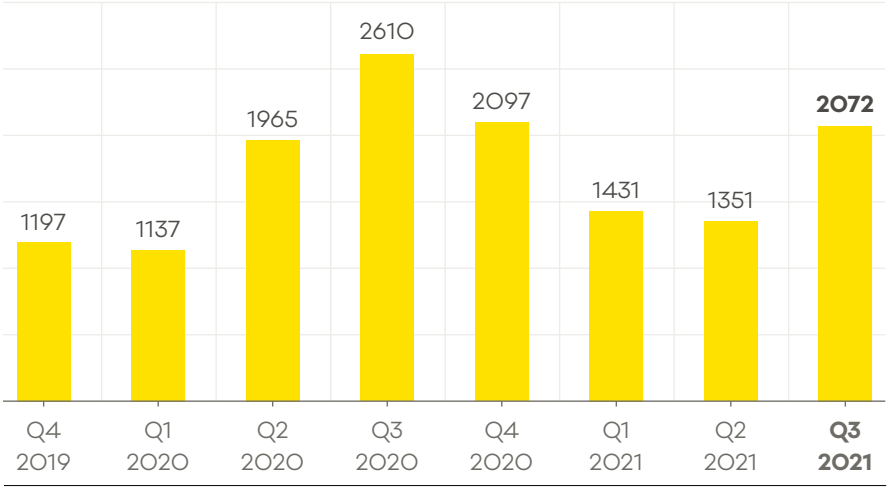
The bottom line is, CERT NZ is here to help. We do this by providing support to those impacted by a cyber security incident, as well as sharing actionable and relevant security steps to help protect against one. You can find these in the likes of this report, our Get Cyber Smart campaigns, in our security advisories, and on our website. And we encourage all New Zealanders, at work and at home, to put them in place.

So whether you're doing last-minute shopping, paying the final invoices for the year, or jumping online to make plans with friends and family, don't let good cyber security practices fall by the wayside. Let's keep our online defences up and risk of cyber security threats down, and enjoy a cyber secure holiday season.

Incidents responded to by CERT NZ

2,072
incidents were responded to by CERT NZ in Q3 2021.

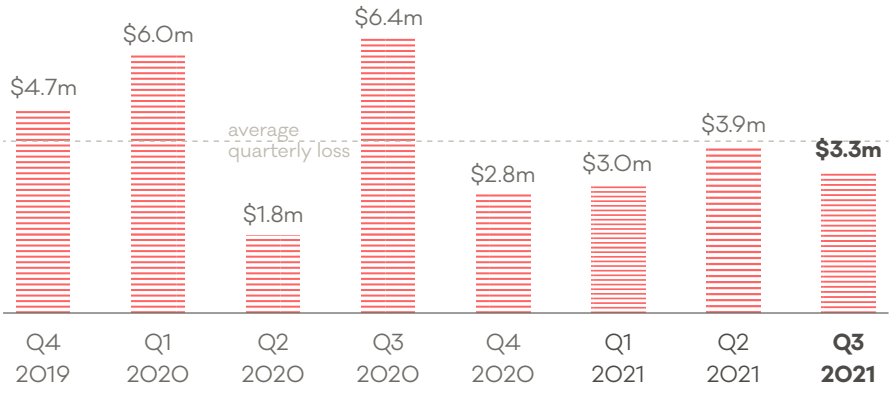
▲ **53% increase**
from Q2 2021.



Direct financial loss

$3.3m
in direct financial loss was reported in Q3 2021.

16% of incidents reported direct financial loss.



Putting data in perspective

Average incidents reported per quarter*
1,643

Average loss reported per quarter*
$4.1m

Total losses reported to CERT NZ
$63.2m
since Q2 2017

*figures based on previous eight quarters

For more on the New Zealand threat landscape in Q3 2021, see the CERT NZ Quarterly Report: Data Landscape. **www.cert.govt.nz/about/quarterly-report/quarter-three-report-2021**

Breakdown by incident category

		From previous quarter
Phishing and credential harvesting	**1,071**	▲ **73%**
Scams and fraud	**488**	▲ **25%**
Unauthorised access	225	▲ 32%
Malware	**151**	▲ **372%**
Website compromise	30	▲ 58%
Ransomware	18	▼ 40%
Suspicous network traffic	10	▲ 11%
Denial of service	5	● 0%
Botnet traffic	4	▲ 100%
C and C server hosting	4	▲ –%
Other	66	▼ 12%

73% increase in phishing and credential harvesting reports from Q2 2021

25% increase in scams and fraud from Q2 2021

Malware reports increased from 32 in Q2 to 151 in Q3 2021.

Malware reports increase

In Q3, malware reports more than tripled from the previous quarter. Malware is malicious software designed to go unnoticed and damage or compromise a computer system.

In most cases it can enter your computer system or device through a malicious download or attachment, a local network or an infected portable media device like a USB drive.

Attackers use different types of malware to get access and control of a computer system usually with the aim of stealing data and money.

There have been a number of malware variants reported to CERT NZ, many of which are one or more of these common types of malware:

Worms are a self-propagating malware. This means once they're in your system they can move quickly and easily spread through systems and networks. Worms can also damage your files and programs, leaving you vulnerable to other forms of attack.

An example of a worm is the self-propagating function of the FluBot malware, which we cover in more detail on page 5.

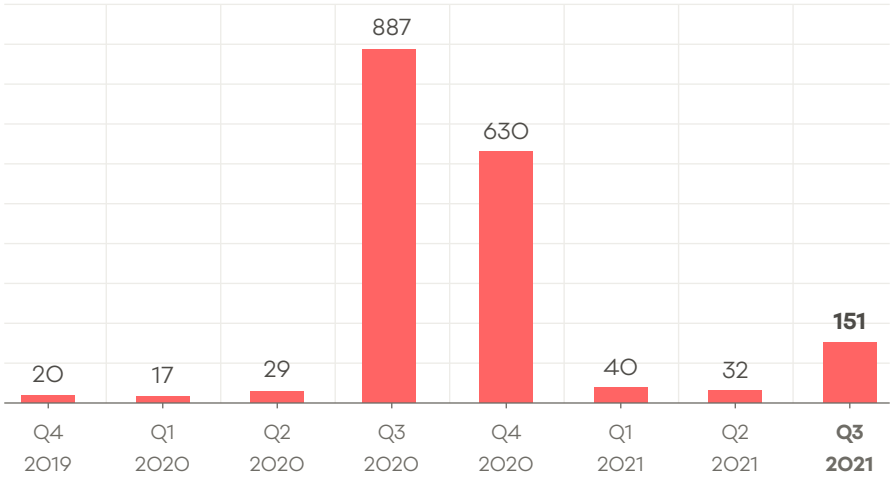
Trojans function by hiding malware inside legitimate files, like Word documents or PDFs. When someone opens an infected file, the malware gets into the system. The malware can often go undetected because the file has a legitimate purpose. Once infected, it can give attackers access to your computer without your knowledge. Attackers can then use this access to carry out other malicious activity.

An example of a trojan is a downloadable document on a legitimate website, like a PDF menu on a restaurant website.

Ransomware is a type of malware that attackers use to encrypt and steal data from an infected system, and then demand the recipient to make a payment to have the data recovered[2].

Spyware works by tracking online behaviour and information entered into websites and within an infected system. This information can include web browsing habits, information about installed software, personal information and even logging keystrokes that are typed on the device. This means if you are infected by spyware and log into your internet banking, the spyware can record your login credentials and access your accounts without your knowledge.

Number of malware reports to CERT NZ



The high reports numbers in Q3 and Q4 2020 were due to the malware variant Emotet[1]

Protecting from malware

As with most cyber security threats, having protections in place to reduce the risk of an attack is much easier than recovery. CERT NZ recommends that you:

- update operating system and apps when new versions are available and turn on automatic updates where possible.
- enable two-factor authentication on your important accounts like banking or your business's website to add another layer of security.

For more information on how to protect against malware go to **https://www.cert.govt.nz/individuals/common-threats/malware/**

1. https://www.cert.govt.nz/about/quarterly-report/quarter-three-report-2020/
2. https://www.cert.govt.nz/business/guides/protecting-from-ransomware/

Worm-like malware affecting Android phones

In the last week of Q3, we saw the global malware variant FluBot begin large-scale targeting of New Zealand mobile phones. These incidents contributed to this quarter's spike in malware reports.

FluBot is a self-propagating malicious application which uses text messages to target mobile phones and spread across devices quickly. The texts can be received by all types of phones, however FluBot can only infect Android phones.

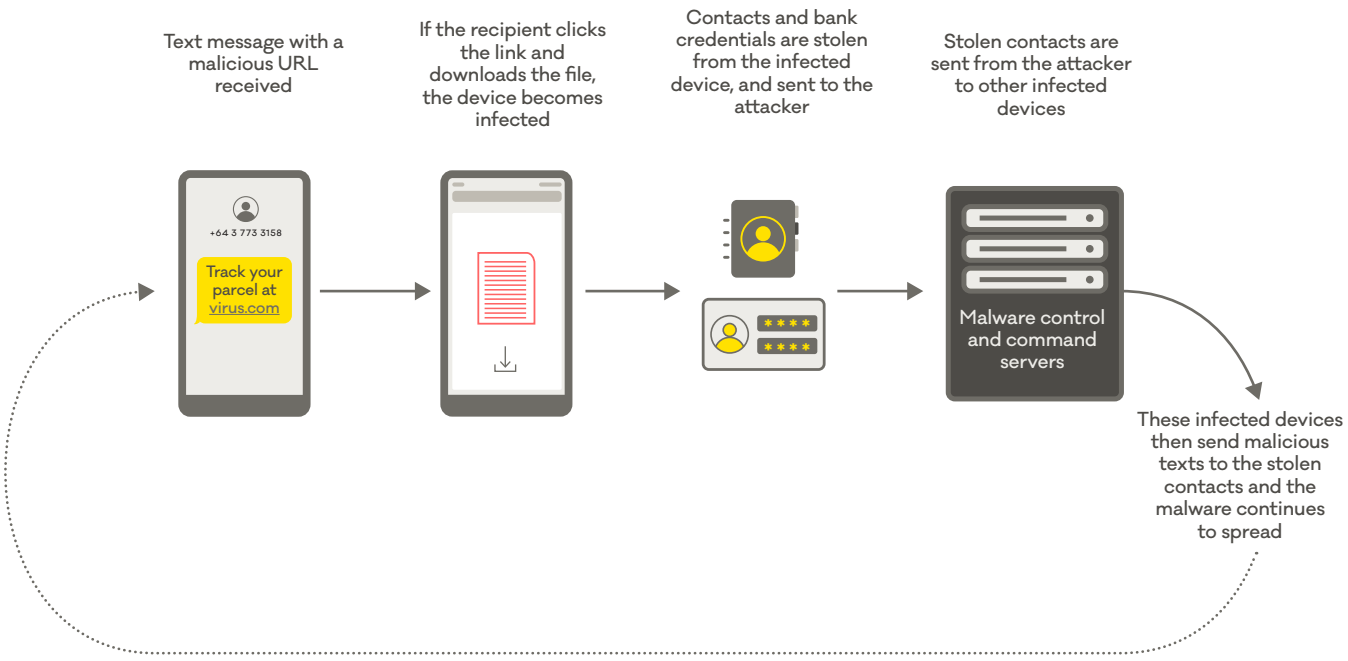
The text message attempts to appear as a legitimate message and contains a URL. For example, it may look like a pending parcel delivery and prompt the recipient to click the URL to download a delivery app. However, the link is not to a legitimate delivery app and if downloaded, it infects the device.

Once the malicious application is installed it can extract data from the phone, like credit card and banking details. It also automatically redistributes the text message to contacts it has stolen from other infected devices.

Once the message is sent, the phone blocks the number so the recipient cannot respond to avoid raising any suspicion with the sender.

Like many cyber security threats, FluBot is constantly changing to try and trick more people into downloading it. The attackers operating this malware evolve it by changing the subject matter of the text and what the URL links to. Recent examples include texts about parcel deliveries, shared photo albums and voicemail.

How FluBot works



Responding to FluBot

What did CERT NZ do?

CERT NZ partnered with the Digital Safety team at The Department of Internal Affairs (DIA) to lead the government response to the incident.

We worked collaboratively with New Zealand ISPs to protect as many people as possible from the malware. This included close to 1,200 requests to take down malicious websites linked to FluBot. Our response also included supporting more than 700 New Zealanders who called CERT NZ with concerns about being affected.

CERT NZ released an advisory on FluBot, and regularly updated New Zealanders on the incident as the campaign evolved[3].

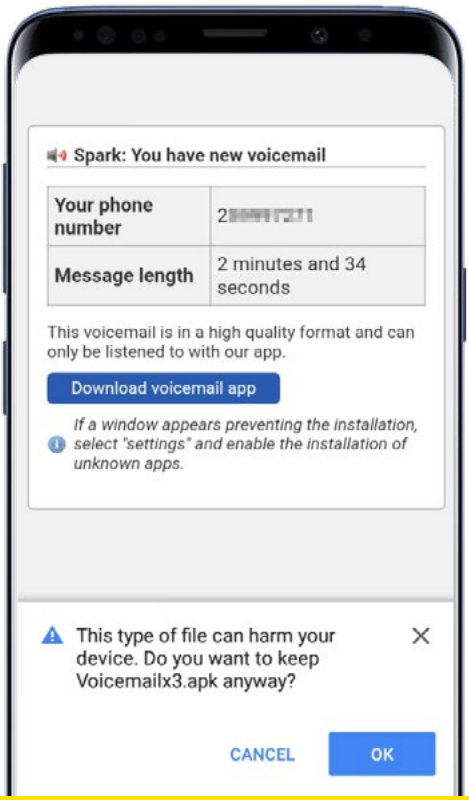
As this incident crosses quarter three and quarter four, we'll include updated data on FluBot in the next report.

If you have clicked a link and downloaded FluBot

- CERT NZ recommends doing a factory reset on your device as soon as possible. This will delete any data on your phone, including personal data.
- Do not restore from backups created after installing the app. Seek the services of a qualified IT professional if you require assistance.
- Change the passwords to all of your online accounts. As FluBot is designed to steal banking details, immediately change the passwords to your online bank accounts. If you have concerns that your accounts may have been accessed by unauthorised people, contact your bank immediately.

Protecting from FluBot

- If you receive a suspicious text message, do not click on the link and do not follow any prompts to install an app or security update. Report the text by sending it, free-of-charge, to DIA on 7726.
- If you are expecting a delivery, don't click on any links—it's best to track the delivery by going directly to the courier's website.



Example of FluBot text message

3. https://www.cert.govt.nz/individuals/alerts/FluBot-malware-infecting-android-phones/

Online services disrupted by denial-of-service attacks

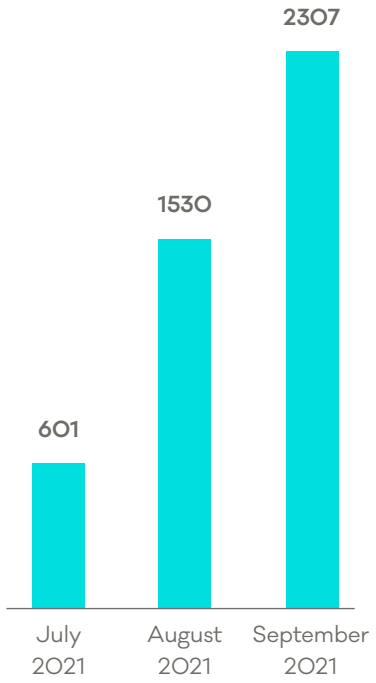
A denial-of-service (DoS) attack is when an attacker sends malicious internet traffic with the aim of restricting or disrupting user access to a computer system or network. These attacks typically target servers to make websites and payment services unavailable — preventing legitimate users from accessing them.

DoS attacks frequently use multiple sources to send internet traffic to the target. This is referred to as a distributed-denial-of-service (DDoS) attack.

DDoS attacks can result in the targeted organisation's website and services being taken offline. Alongside these impacts, the attacks can cause reputational damage and loss of revenue. Although the targeted system is disrupted or inaccessible, there isn't any risk to the system data or threat to users trying to access the service.

In Q3, these attacks continued to affect New Zealand organisations. Data shared by The Shadowserver Foundation[4] shows a total of 4,438 DDoS attacks, varying in size and impact, targeting New Zealand networks.

Number of DDoS attacks in Q3 2021



How CERT NZ helps

Where possible, CERT NZ works with the affected organisation to provide guidance and support to mitigate an attack. The first step when responding to a DoS report is to determine how the organisation's systems are being impacted. This helps our Incident Response team to understand the internet traffic the affected organisation is seeing and the impacts that traffic is having on their services.

With these insights, CERT NZ's incident response team can determine what kind of DoS attack is occurring, what mitigations the organisation has in place that could be activated, as well as any gaps in their current response plan.

As part of the response, CERT NZ analyses the incident information and identifies other organisations and stakeholders that could also be at risk. Once notified, the Incident Response team advises them of the possible cyber security threat and works to provide relevant information and advice so they're prepared for, and can protect against a possible attack.

How organisations can protect from DoS attacks

As there isn't a one-step approach to protecting from a DoS attack, CERT NZ recommends making sure your organisation has defences and mitigations in place, and an incident response plan prepared.

On our website, we have covered the steps to best protect and mitigate a DoS attack. Check with your IT team or service provider that you have these in place.

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

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

4. www.shadowserver.org

How IoT devices can be used in DDoS attacks

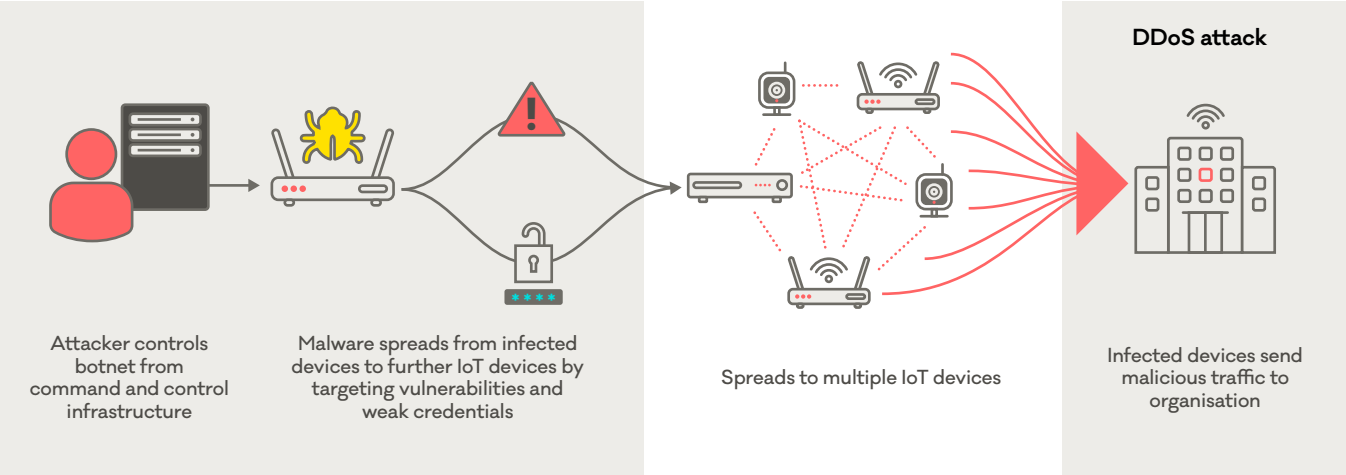
This quarter we continued to see networks of IoT (Internet of Things) devices being used in DDoS attacks. This happens when insecure internet-connected devices, like routers and WiFi-connected cameras, become infected with malware.

Once an IoT device is infected, it can become part of a large interconnected network of devices called an IoT botnet ('robot network') which is under the control of an attacker—often without the owner's knowledge. Because botnets work by spreading the malware from device to device, it can rapidly grow its network while remaining hidden.

With control of the devices within the botnet, an attacker can carry out a DDoS attack by commanding the botnet to send traffic to a target or online services. This large network creates a simultaneous high volume of traffic to the target in an attempt to overwhelm it and try to disrupt its services or take it offline.

Outlined in the diagram below is a common way botnets operate to infect devices to carry out a DDoS attack.

How IoT devices can be used in DDoS attacks



Prevent your devices from being part of an IoT botnet

There are some simple steps you can take to prevent your IoT devices from being used for malicious activity like a DDoS attack.

- Install updates as soon as they are available.
- Make sure you change default passwords or weak passwords wherever possible.

CERT NZ recommends considering whether you need the device connected to the internet. If not, disconnect it.

Botnets can also target non-IoT devices like computer networks. To protect computer networks from becoming part of a botnet please follow malware protection tips on page 4.

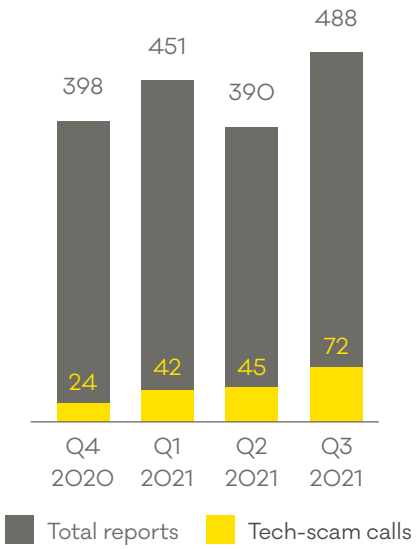
CERT NZ helps recover funds following tech-scam call

Scams and fraud is consistently one of the highest-reported incident categories to CERT NZ. In Q3, there were 488 scam reports, and 15% were about tech-scam calls.

This is a common scam reported to CERT NZ and happens when scammers call people at home pretending to be from a well-known tech company like Microsoft. They often request remote access to a PC or device claiming they need to repair an issue or install a software update. They do this to try and gain access to your private and financial information.

In Q3, an individual reported to CERT NZ that they had received a call about a potential technical issue with their computer. Believing the caller was legitimate, they gave them remote access to their computer. However, the caller was instead an attacker who was attempting to trick the recipient into sharing access to their computer.

Scam and fraud reports in Q3 2021



Once the attacker had remote access, they opened the recipient's bank account and transferred large sums of money.

The recipient quickly became aware that funds had been taken from their account and reported to CERT NZ. In response, CERT NZ provided advice on how the attack had happened and what to do next. This included alerting the recipient's bank about the scam and stolen money as soon as possible so the attacker's account could be traced.

Because the recipient had reported the incident quickly, most of the funds were recovered and their bank account was secured with a new password and a new credit card issued. The recipient also stated that they felt better placed to identify any future scam calls.

NZ Police were also advised of the scam for their investigation into the malicious actors.

Protecting from a tech-scam call

- If you receive a call about a technical issue with your PC or device, do not provide any information over the phone or allow the caller to have remote access.
- If you are concerned that there is an issue with your PC or device, contact the store you purchased it from or seek help from a trusted IT professional.

For advice and support, or if you think you have been affected by a scam, please report to **www.cert.govt.nz/report**