certnz

Q2

APRIL TO JUNE 2023

CYBER SECURITY INSIGHTS

Patch work

IN THIS ISSUE

Te Kāwanatanga o Aotearoa
New Zealand Government

Q2 CYBER SECURITY INSIGHTS

Director's message

Rob Pope, Director

We've all seen them: those text messages saying we need to pay road tolls, that a courier package is waiting for us or there's unusual activity on our bank account. Many of us dismiss them, but all the scammers need is to get you on a day when you're busy or stressed and may not be thinking clearly.

The rise in SMS text-based phishing (smishing) is a worrying development. The number of phishing reports (including smishing) to CERT NZ is up 26% from the last quarter and doesn't seem to be slowing down.

Phishing – both email and SMS – has become one of the main paths for cybercrime, because, for the bad guys, it's the fastest and most cost-effective way of targeting New Zealanders.

But let's not dwell on the bad stuff and, rather, look at how you can keep yourself secure from these sorts of incidents. One way we can all defend ourselves is through awareness.

If there's a vulnerability in a piece of software you use, you'd want to know. Vulnerability disclosure is a vital part of cyber security; knowing there's an issue gives the software vendors a chance to fix it before malicious actors can get in.

CERT NZ is a strong believer in security by default and design, so we encourage anyone who creates software to have a vulnerability disclosure policy in place. This is a system where vulnerability disclosures can be sent through to your organisation, you acknowledge it with the discloser and potentially gain clarity on the vulnerability and coordinate further action or publication.

Doing this keeps all of us more secure online. Of course, it's then on us, as users, to make sure we update with any patches when they come out. It has been one of our main messages at CERT NZ for years: keep all your devices and software up to date.

It's all part of our ongoing fight against cybercriminals and keeping New Zealand secure and cyber resilient.

AT A GLANCE...

Average incidents reported per quarter

2,266

Average loss reported per quarter

$5m

Losses reported to CERT NZ

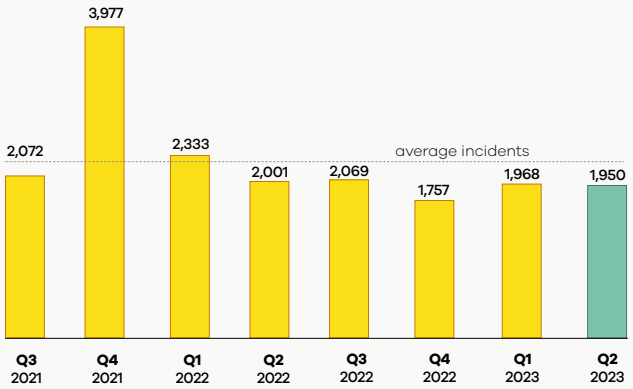
$39.9m

Figures based on previous eight quarters

INCIDENTS RESPONDED TO BY CERT NZ

1,950
incidents were responded to by CERT NZ in Q2 2023

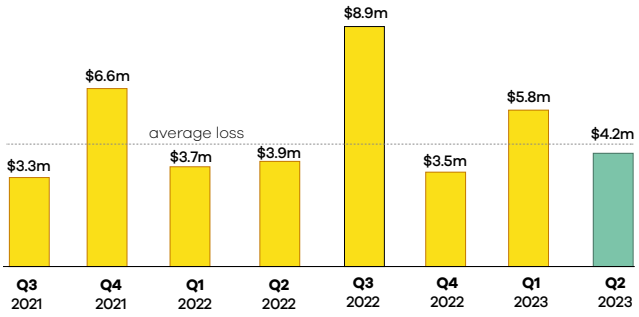
▼1%
decrease from Q2 2023



DIRECT FINANCIAL LOSS

$4.2m
in direct financial loss was reported in Q2 2023

▼27%
decrease from Q1 2023, with 21% of incidents reporting financial loss



BREAKDOWN BY INCIDENT CATEGORY

Despite an overall decrease in both reports and financial loss in Q2, many incident categories saw increases compared with the last quarter.

		From previous quarter
Phishing and credential harvesting	1189	▲ 26%
Scams and fraud	474	▼ 24%
Unauthorised access	173	▼ 28%
Malware	38	▲ 36%
Website compromise	18	▲ 38%
Ransomware	13	▲ 8%
Suspicious network traffic	2	● 0%
C and C server hosting	2	●
Botnet traffic	1	▼ 67%
Denial of service	0	▼ 100%
Attack on a system	0	●
Other	39	▼ 60%

For more on the New Zealand threat landscape in Q2 2023, see the CERT NZ Quarterly Report: Data Landscape.

Patch work

Online vulnerabilities are constantly being discovered as cyber security actors, both malicious and non-malicious, search for potential 'holes'. This is often when software doesn't run as expected under certain circumstances.

Vulnerabilities can be found in software, hardware, firmware, or online services. Once discovered, they can be exploited to potentially gain access to devices and use that access to do anything from intercepting communications to deploying malware across a network.

PATCH EVERY HOLE

When a vulnerability is uncovered, just like a hole in the fence, you need to patch it up.

Software owners often release patches intended to reduce or remove the vulnerability. Applying these patches in a timely manner is the number one way to keep your devices and software secure.

Where possible, CERT NZ recommends setting updates to automatic; this includes on your mobile devices. Most vulnerabilities are exploited in the first two weeks, so update as soon as possible.

There is sometimes a reluctance to apply patches immediately as they may cause unexpected issues within your current systems. While this can happen, it rarely outweighs the risk of continuing to operate with a known vulnerability.

CERT NZ recommends organisations take the following steps:

- Know what you have running in your system.
- Have a patch-management process.
- Update regularly and, where possible, have automatic updates on.

FULL DISCLOSURE

A lot of information about vulnerabilities comes from voluntary and anonymous disclosures. Disclosures allow the affected organisation to work out a solution to the vulnerability before it becomes public and a risk to users.

CERT NZ stresses that disclosure is a good thing, and organisations that supply software or services should have a vulnerability disclosure policy in place.

Without disclosure policies, organisations must rely on their own teams to catch all the holes. If your organisation receives a disclosure, it's good practice to respond to the discloser, where possible, letting them know you have received the notification. This can help you gain clarity on the vulnerability and coordinate further action or publication.

> **Disclosures allow the affected organisation to work out a solution to the vulnerability before it becomes public and a risk to users.**

A few avenues for disclosure exist, and CERT NZ runs a system where it acts as an in-between for those wanting to disclose vulnerabilities. In 2022, 41 vulnerabilities were reported to CERT NZ, 26 were done through our coordinated vulnerability disclosure (CVD) system that allows for anonymous disclosure.[1]

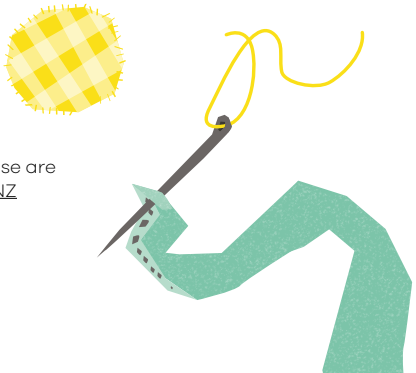
ON ALERT

CERT NZ monitors emerging vulnerabilities that may affect New Zealand businesses and individuals.

If we see one that is widespread or being actively exploited that broadly affects New Zealanders, we put out an advisory.[2] Advisories describe exactly which systems the vulnerability affects, the steps needed to identify if you are at risk and how to mitigate or prevent exploitation.

The best way to stay informed is to subscribe to CERT NZ's alerts and advisories.[3]

CERT NZ also sends proactive notifications to organisations if the vulnerability affects only a small number of organisations. In Q2 2023, we sent out 184 proactive notifications, informing organisations that they were affected by a vulnerability.



[1] Getting a vulnerability report - CERT NZ

[2] For incidents affecting individuals, such as an active phishing or malware campaign, we put out alerts. These are usually less technical. Advisories for IT specialists - CERT NZ. Alerts for businesses and individuals - CERT NZ

[3] Subscribe to CERT NZ - CERT NZ

ANATOMY OF AN ADVISORY

A

1:00pm, 12 June 2023

TLP Rating: Clear

Company ABC Remote Code Execution vulnerability

Update: 26/06/23

A vulnerability has been discovered that affects Company ABC devices with Software X enabled. B

This heap-based buffer overflow vulnerability allows for an attacker to run unauthorised code or commands remotely on the affected system.

C The vulnerability is tracked as CVE-2023-xxxxx.

What to look for/What to do

D How to tell if you're at risk: All devices running X versions
Mitigation: Disable support on inspection profiles. Update to latest version.

A Date of publication and date of latest update. Updates may not be sent out to subscribers – though they will be noted on social media – unless the scope of the vulnerability has widened significantly or the vulnerability is in active use by malicious actors.

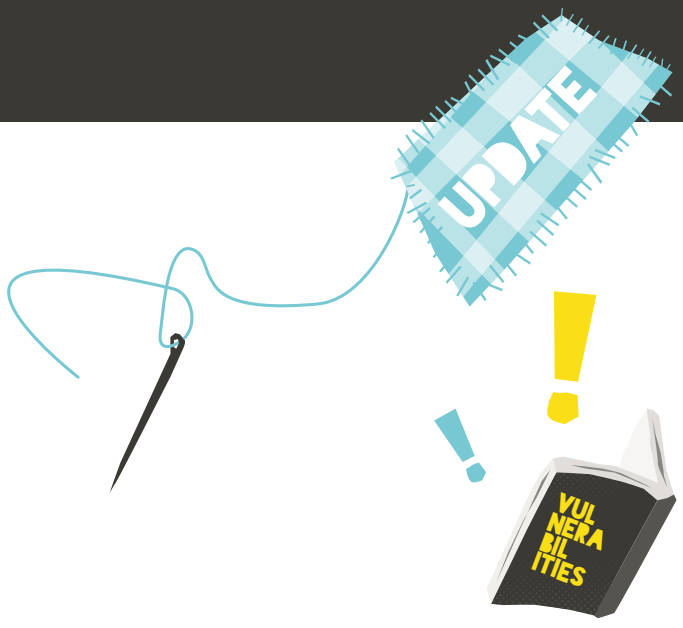
B The affected systems will be listed in the introduction with more detail.

C The Common Vulnerability and Exploit (CVE) code for the vulnerability. This means the vulnerability has been added to the CVE database. CERT NZ will sometimes send out advisories on 'zero-day' vulnerabilities that are too new for a CVE code.

D The 'What to look for' and 'What to do' sections provide details to help you work out if you're at risk, along with providing prevention and mitigation advice.

The advisory will have a list of affected software and firmware versions or, if the vulnerability requires a combination of factors, it will outline these.

A section is included on mitigation and, where possible, prevention. The last section includes further information and links to any available patches or updates.



Case study:

The following is an example of CERT NZ's proactive outreach, which occurs when we discover a vulnerability that directly affects a small number of organisations.

CERT NZ identified a newly discovered vulnerability that was high risk because of the level of impact a breach could have.

CERT NZ identified that only a handful of New Zealand services would be vulnerable.

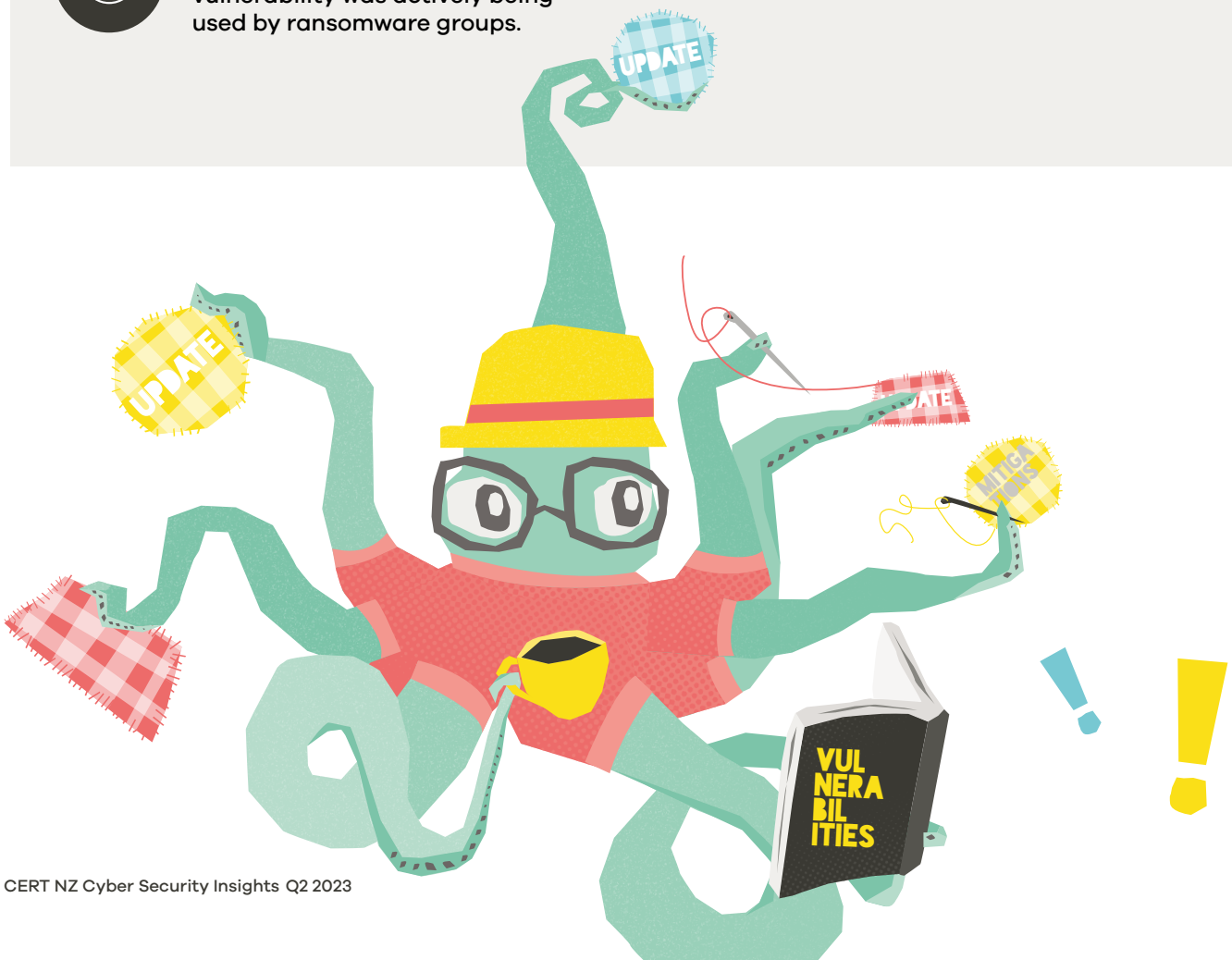
CERT NZ contacted the organisations and provided advice on mitigation.

The organisations applied the mitigation and continued to monitor the situation.

Over the next few days reports began circulating that the vulnerability was actively being used by ransomware groups.

> The advisory will have a list of affected software and firmware versions or, if the vulnerability requires a combination of factors, it will outline these.

In some instances, the vulnerability may change over time to include more affected systems than originally reported. When this happens, we work quickly to put out an advisory (or update) and make sure any organisations at risk put mitigations in place as soon as possible.



Gone smishin'

It's something many people consider an annoyance, however, phishing remains the largest reporting category to CERT NZ and one of the biggest paths for other types of attacks.

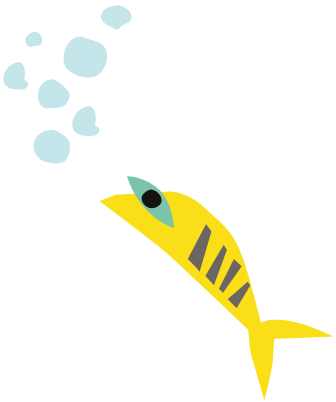
Historically, most phishing was delivered by email. However, this year, CERT NZ has seen many more phishing text messages (also known as 'smishing') than phishing emails.

The risks to people are increased with smishing, because most people have their phones on them all the time and see text messages as soon as they arrive. This means messages can come through at times when you are on auto pilot. Links sent via text messages are also easy to disguise using URL shorteners (for example, bit.ly) and can be sent from 'spoofed' phone numbers.[4]

While the exact wording will change, typically smishing messages pretend to be from a reputable organisation: banks, Inland Revenue, New Zealand Post, Waka Kotahi and other government departments. They usually claim there is an issue and ask you to click on a link to resolve it. A sense of urgency is often included around the action.

Recently, some smishing texts have come with a phone number as well as or instead of a link. Calling the number gives the scammers direct access to you and can make their scam seem more legitimate.

[4] See Q1 2022 Cyber Security Insights report

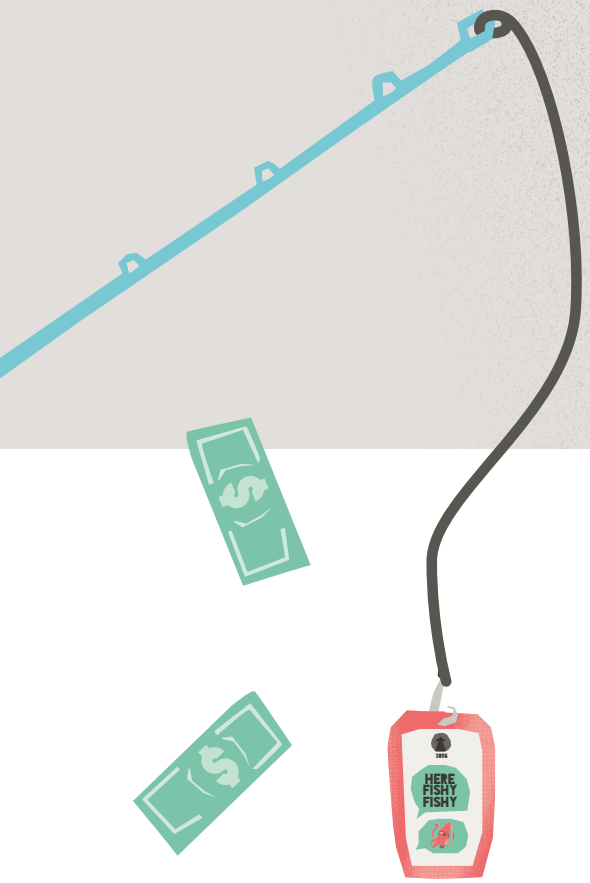


EXAMPLES:

"You have unpaid road tolls. Visit the link to pay..."

"You have successfully paired a new device to your online banking. If you don't recognise this, visit..."

"You have unclaimed tax refunds available. Add bank details before refund expires..."



ADVICE

The best way to keep yourself safe from these scam messages is to avoid clicking links in text messages and emails. Even if you think the text might be legitimate, it's better to navigate to the organisation's website using another method.

Ghosted in the marketplace

Everyone loves a good online marketplace. Unfortunately, they are also a great place for scammers to find potential targets.

In the last quarter, CERT NZ received reports of specific tactics scammers use in these marketplaces.

REVERSE PICKUP SCAM

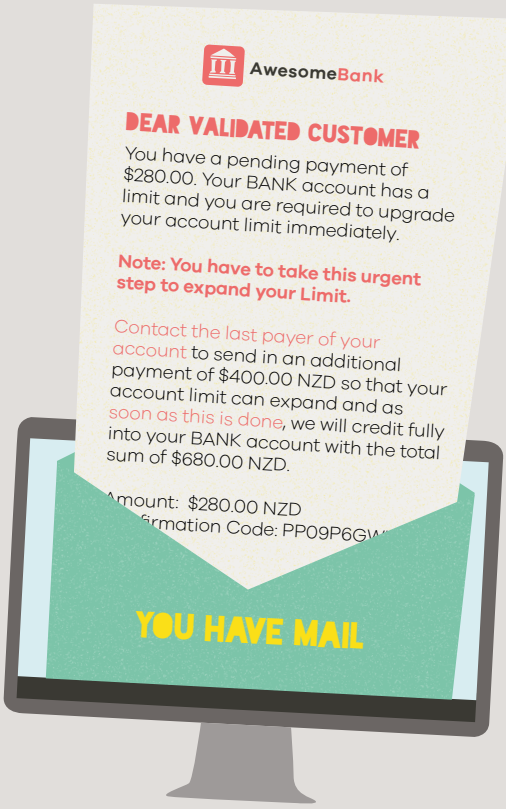
In this situation, the scammer poses as a buyer and pretends to purchase an item from a genuine seller. The scammer says they have prepaid for a courier to pick up the item and asks the seller to send them an 'insurance fee' they will refund when the item arrives. The fee is what the scammer wants.

The scammer may threaten to report the target, to get them to pay. After they receive the fee, they will break off all contact with the seller and cancel any purchase they may have agreed to. It can be hard to recover any funds from this type of scam simply because it requires a lot of work and back-and-forth between banks and the marketplace.

BANK ACCOUNT LIMIT SCAMS

This is a sneakier scam. Again, the scammer claims to be interested in purchasing an item from a genuine seller. They request bank account details from the seller to make the payment. The scammer then asks the seller to check their email for confirmation of payment.

The email looks to be from the seller's own bank and claims that a transaction was attempted but couldn't be processed due to a limit on their bank account. The scammer is the one who sent the email, and it states your 'bank account limit' can be increased by transferring your last buyer (the scammer in this case) a certain amount of money, which will be refunded to you once your limit has been increased.



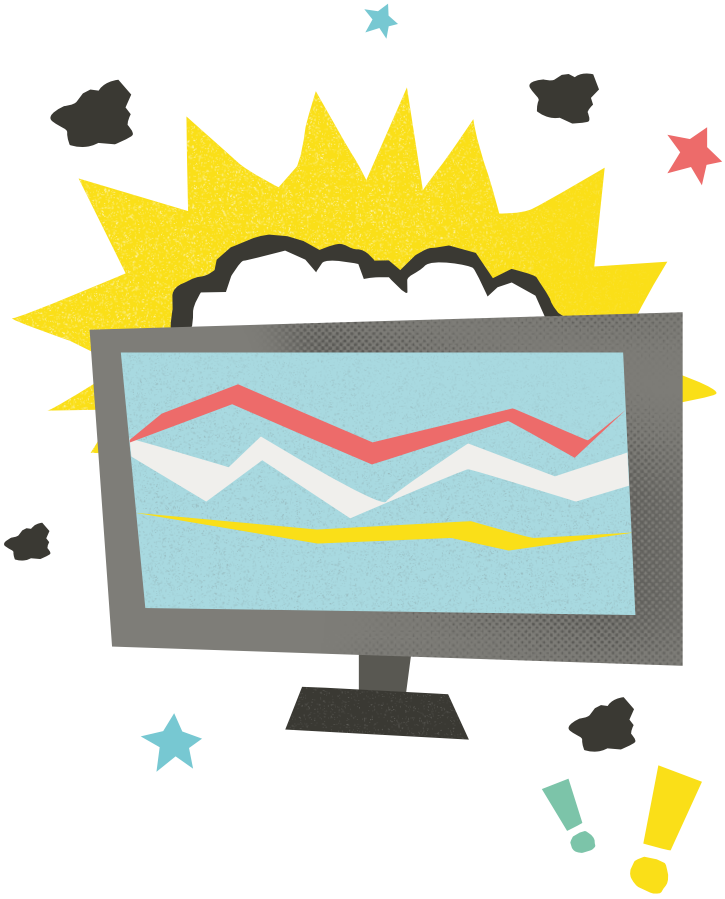
Again, when the target sends through the money, the scammer immediately breaks off all communications and leaves the legitimate seller out of pocket and with a long fight to recover any of the funds.

> The scammer is the one who sent the email, and it states your 'bank account limit' can be increased by transferring your last buyer (the scammer in this case) a certain amount of money, which will be refunded to you once your limit has been increased.

CERT NZ WORK

CERT NZ has published two new guidance pages and a video for small businesses on what to do if caught in a distributed denial-of-service (DDoS) attack.[5]

A DDoS attack is aimed at stopping your online tools and websites from working by overloading them. These pages talk about how DDoS works, what a DDoS attack looks like, how to mitigate against an attack and how to protect your business.



> A DDoS attack is aimed at stopping your online tools and websites from working by overloading them.

International insights

In this section, we cover news from our international partners.

CERT NZ, along with international partners, published a comprehensive cyber advisory on LockBit Ransomware in June. This was released to help organisations around the world better understand and protect against this global ransomware threat.[6]

CERT NZ also worked alongside international partners to publish information outlining the most commonly exploited vulnerabilities in 2022.[7]

[5] Distributed denial-of-services (DDoS) attack - CERT NZ and Protect your business form DDoS attacks - CERT NZ

[6] New Zealand and International Partners Release Comprehensive Cyber Advisory on LockBit Ransomware - CERT NZ

[7] Cybersecurity and Infrastructure Security Agency, 2022 Top Routinely Exploited Vulnerabilities