certnz

Q4

OCTOBER TO DECEMBER 2022

CYBER SECURITY INSIGHTS

Held to ransom

IN THIS ISSUE

Te Kāwanatanga o Aotearoa
New Zealand Government

Q4 CYBER SECURITY INSIGHTS

Director's message

Rob Pope, Director

We finished out the year with lower-than-expected report numbers, but that doesn't mean there was a lower threat.

Scammers are finding new and inventive ways of getting to our money. While reports were slightly down on 2021, financial losses have jumped a whopping 19% to $20 million. A large chunk of that came from unauthorised money transfers – touched on in our last report.

In quarter 4, a big increase in ransomware attacks reminded us that attackers are still willing to attempt large attacks for potentially large pay outs. This quarter's increase was driven in part by a single attack that had a ripple effect out to other companies.

Third-party providers of software services make enticing targets for criminals because they can hold anything from data to full email or financial systems of multiple companies.

Organisations thinking of using a managed service provider need to vet them carefully by going over certification and accreditation processes, asking to see incident response plans and reviewing their controls. Doing this gives you peace of mind and a clear path to follow if anything should go wrong.

We're also seeing a rise in extortion and blackmail. These sorts of incidents reached a peak in Q2 of 2020, accounting for almost a quarter of all reports. And in 2022 there was a new report roughly every three days.

The scammers will claim they've hacked your email and installed malware on your computer or have footage of you in a compromising position. They may even include a password of yours that was caught up in a data breach as 'proof'.

The messages are designed to be shocking, so you're frightened and act without thinking. The criminals want to pressure you into acting quickly, so, as with most scams, we encourage people to pause and take a moment.

Staying vigilant is crucial to staying secure online. Hopefully we can all work to get that financial loss figure down.

AT A GLANCE...

Average incidents reported per quarter

2,124

Average loss reported per quarter

$4.6m

Losses reported to CERT NZ from previous eight quarters

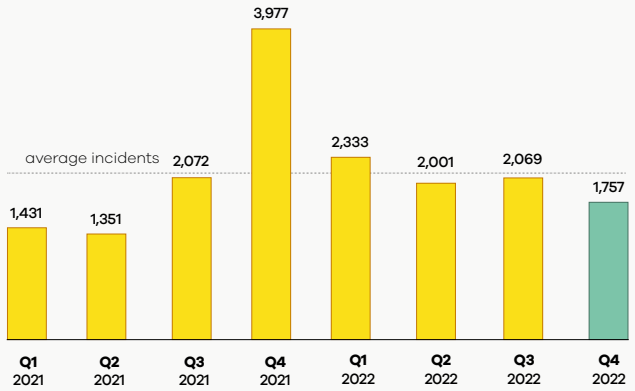
$36.8m

Figures based on previous eight quarters

INCIDENTS RESPONDED TO BY CERT NZ

1,757
incidents were responded to by CERT NZ in Q4 2022.

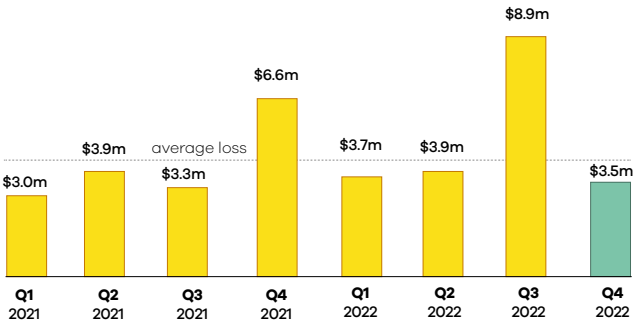
▼15%
decrease from Q3 2022.



DIRECT FINANCIAL LOSS

$3.5m
in direct financial loss was reported in Q4 2022.

▼61%
decrease from Q3 2022, with 26% of incidents reporting financial loss.



BREAKDOWN BY INCIDENT CATEGORY

In Q4, a decrease in reports occurred in most categories. Financial loss has decreased 61% after a record-breaking loss last quarter (Q3 2022).

		From previous quarter
Phishing and credential harvesting	905	▼ 2%
Scams and fraud	510	▼ 27%
Unauthorised access	178	▼ 40%
Malware	43	▲ 10%
Website compromise	15	● 0%
Ransomware	36	▲ 500%
Botnet traffic	5	▲ 25%
Denial of service	0	▼ 100%
C and C server hosting	2	▲ 100%
Suspicious network traffic	1	▼ 86%
Attack on a system	0	● 0%
Other	63	▼ 20%

For more on the New Zealand threat landscape in Q4 2022, see the CERT NZ Quarterly Report: Data Landscape.

Held to ransom

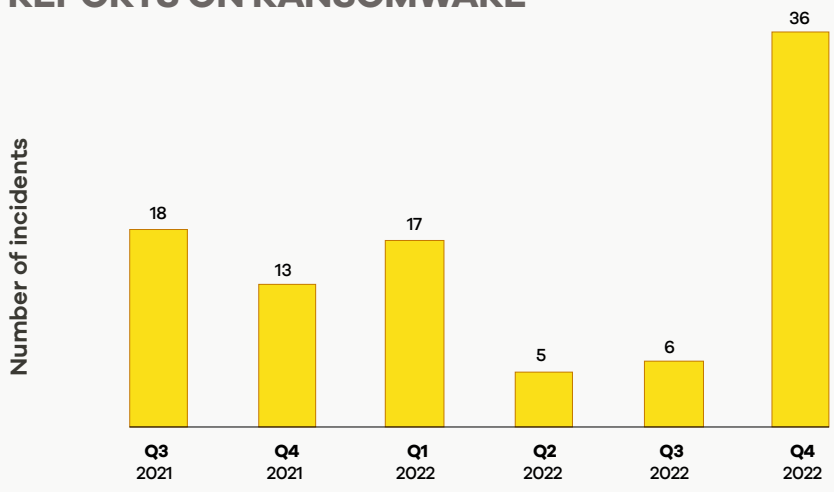
Ransomware is one of the scariest types of attack that an organisation can suffer. No matter how it turns out, it usually means losses and stress.

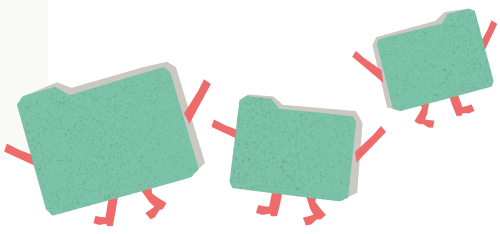
Reports of ransomware attacks over the past two years have tended to wax and wane. However, in Q4 of 2022, the numbers increased suddenly month on month, to the highest numbers CERT NZ has received in a quarter.

In part, this is the result of an attack on one company that had downstream effects on others. This is covered further in the Insight below on page 7.

No one type of business is more susceptible than another to ransomware. Reports to CERT NZ show the attacks are spread across a range of organisations. This could potentially be because attackers are looking for certain systems, legacy devices or exploitable vulnerabilities, rather than targeting specific businesses.

REPORTS ON RANSOMWARE





HOW A RANSOMWARE ATTACK HAPPENS AND WHAT YOU CAN DO TO STOP IT

A typical ransomware attack has three parts: initial access, consolidation and preparation, and impact on target. Understanding how an attacker works can help you know what to do to stop them.[1]

INITIAL ACCESS

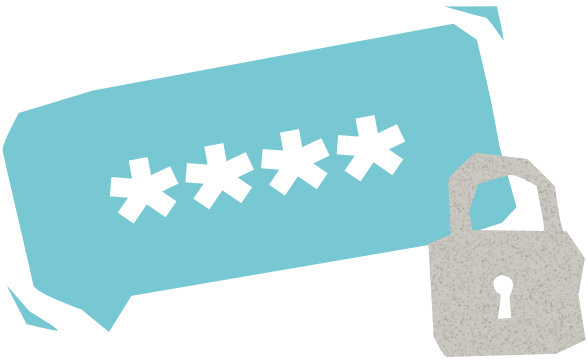
First an attacker needs to get access to your system, so this is also your first line of defence.

Attackers have a few ways to try to get in. The most common ones are phishing for credentials, collecting compromised passwords found in data breaches, using software to 'brute-force' guess passwords, exploiting a software vulnerability or tricking a user into downloading malware.

The first step in defending against these types of attacks is to identify and reduce the number of possible targets. Once you have a complete list of internet-facing systems, enforcing multi-factor authentication on them and ensuring passwords are not reused are two of the easiest and most effective security controls to prevent unauthorised access.

Staff education about phishing and malware can help to mitigate some of the user-initiated access paths. But, remember, even the most tech-savvy users can be fooled from time to time.

> Multi-factor authentication is your friend again, because it's another barrier to the attacker spreading through your system.



CONSOLIDATION AND PREPARATION

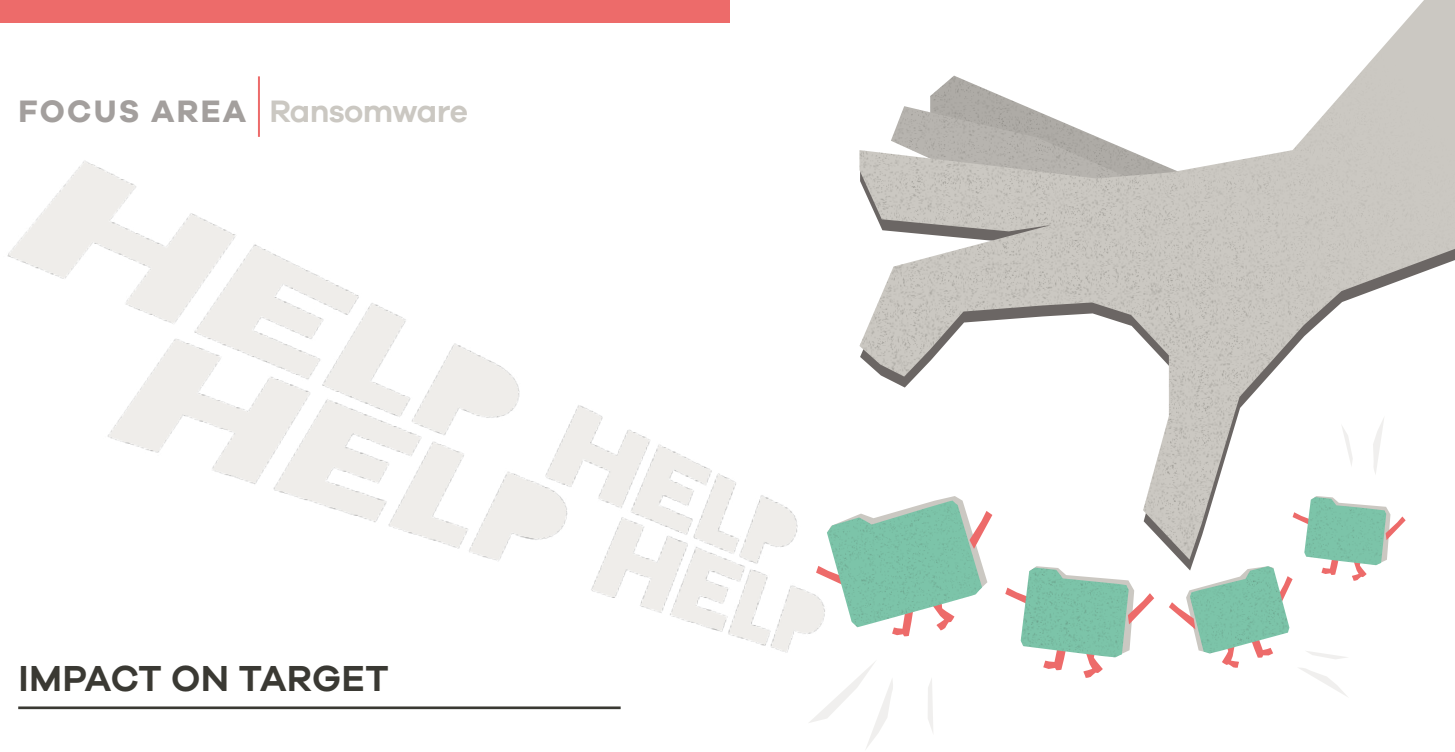
After gaining access, an attacker then deploys tools to take control and spread further through the system. They will attempt to access all devices and parts of your system, including back-up servers. During this stage, the attackers will be trying to hide their activities, by doing things like disabling security controls and working outside of regular office hours.

Application allowlisting supported by **logging** and **alerting** are important defences to mitigate damage at this stage. By using these defences, you can prevent the attacker's tools from running and this can help you to respond rapidly if they are detected in your environment. This is essential to preventing further compromise.

Multi-factor authentication is your friend again, because it's another barrier to the attacker spreading through your system.

Another mitigation is to separate administrative and critical devices from the rest of the environment and **segment the network** to limit the scope of an attacker. If the attacker cannot communicate with their intended targets, then their options will be greatly limited.

[1] Initial access | CERT NZ



IMPACT ON TARGET

Once they are in a system and have their tools running, the attacker can do what they want. This can include stealing (exfiltrating) data to sell or hold to ransom, as well as encrypting your system and destroying backups.

Your best bet at this point is to have an incident response plan[2] and, if possible, a robust and well-tested backup to restore to. Because attackers will attempt to delete your backups, keeping them offline or disconnected from your internet-connected servers is critical.

If you discover an attacker in the early stages, you may need to move carefully because they could trigger a lockdown early to prevent you from removing or disabling their tools.

Communication will be essential in this scenario. There may need to be internal and external communication and potentially disclosures to an agency such as the Office of the Privacy Commissioner. CERT NZ has a communications framework that can be used to create a communications plan for an incident response.[3]

If you are sent a ransom note or any other communication by the attacker, CERT NZ recommends you **do not engage with them or pay the ransom**. There is no guarantee you will get your data or systems back, and the money could be used to fund further attacks and other real-world harm.

IF YOU SUFFER AN ATTACK

In the event of an attack, you will need to implement your incident response plan. If you don't have a plan, CERT NZ has resources to help you create one. Reporting the incident as soon as possible to CERT NZ will mean we can help you in your response.[2]

If you discover an attacker in the early stages, you may need to move carefully because they could trigger a lockdown early to prevent you from removing or disabling their tools.

[2] Creating an incident response plan | CERT NZ
[3] Public communications for cyber security incidents: A framework for organisations | CERT NZ

Crashing the third party

With businesses needing more IT and online services, there has been a rise in third-party software as a service (SaaS) and managed service providers. This can range from server hosting to the running of full IT systems remotely.

This gives organisations the ability to outsource a lot of technical work while keeping costs down. However, that makes these external services a target for attackers because it potentially gives them access to all the connected organisations.

For example, the supplier may hold data or other information from various organisations, giving the attacker a much large payoff for a single attack, not to mention the downstream effects that may create more disruption.

In these types of incidents, the attackers will exfiltrate as much as they can from the system before destroying backups and locking it down. The more organisations involved, the more widespread the damage and the more targets the attackers can ransom.

HOW TO MITIGATE AGAINST THIS

When looking for a supplier, ensure you go over your own certification and accreditation process with them. Ask to see incident response plans and review their controls (such as those mentioned in the Focus Area on ransomware). Large suppliers may be less vulnerable, but no one is 100% protected.

Backups are essential, so ensure they are offsite or disconnected.

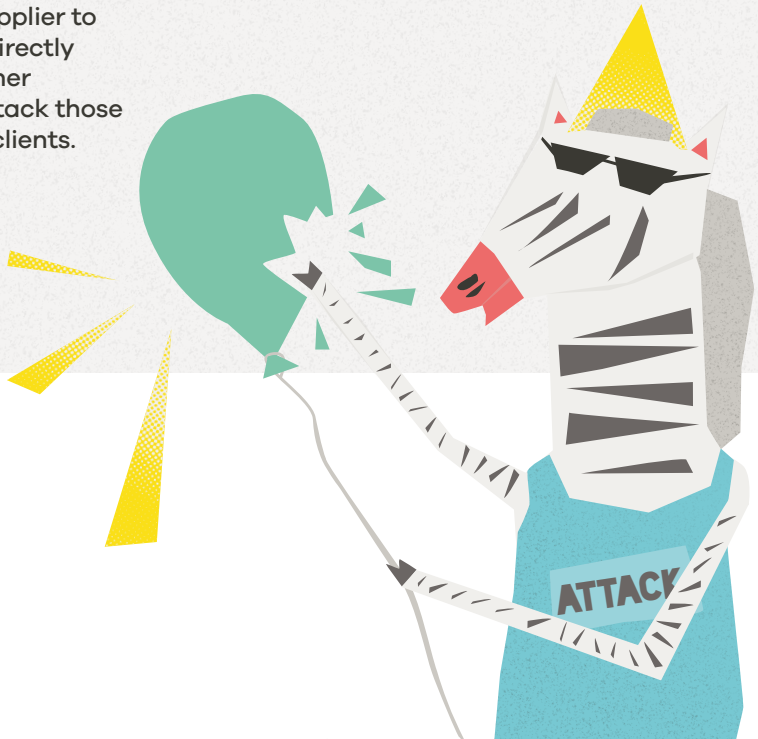
Backups are essential, so ensure that they are offsite or disconnected.

If you are affected

If you use a third-party supplier and they get hit with an attack, such as ransomware, there isn't much you can do.

Contact CERT NZ. We can help work with the supplier. They should be in contact with you as soon as they learn of the attack and report any potential breaches or lost information. You will need to communicate with your stakeholders and possibly the Office of the Privacy Commissioner.

There is also the chance attackers will double down and use the information stolen from the supplier to target its clients directly or move even further downstream to attack those connected to the clients.



Fake extortion leads to real losses

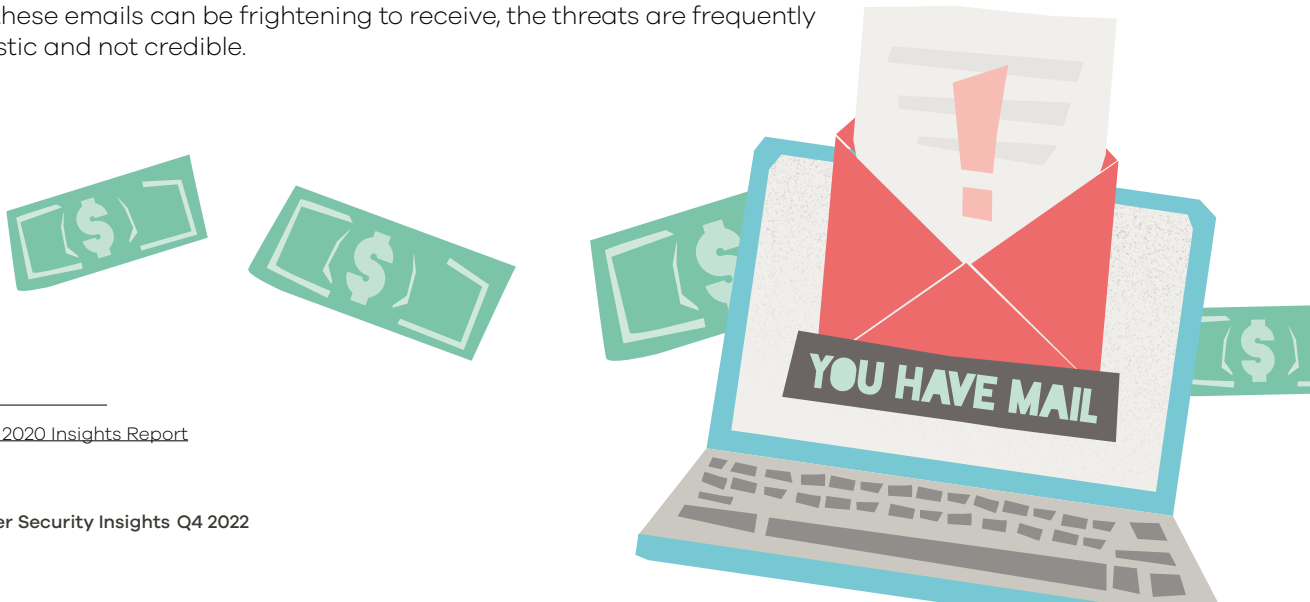
We've seen blackmail and extortion campaigns in Aotearoa before. A peak occurred in Q2 of 2020,[4] with 482 reports, which made up almost a quarter of every report to CERT NZ.

The reports for extortion have tailed off but we're still seeing roughly one every three days (186 reports in 2022).

WHAT IS BLACKMAIL AND EXTORTION?

In a cyber context, extortion scams take the form of an email trying to trick recipients into paying money by threatening to release private information or images.

Although these emails can be frightening to receive, the threats are frequently opportunistic and not credible.



[4] Quarter Two 2020 Insights Report

SCAMMERS USE URGENCY AND AUTHORITY

These sorts of scams are designed to create stress and fear in the targets. The scammers use urgency to push these emotional buttons, for example, a short deadline for payment.

They also pretend to have authority, by using technical language and talking like experts despite their claims not standing up to further scrutiny.

Reports from 2022 have included the following claims from scammers.

They have hacked your email and installed malware on your computer. Possibly controlling your computer's camera or keyboard. To add weight to the scam, the scammers can make it look as though the message has been sent from your own email address.

They have recorded video of you via your computer's webcam. They will usually say this footage is of you in compromising positions or visiting adult websites.

Previously, these sorts of scams included a password you've used for an online service, to make the extortion seem more plausible. The scammer gets this password from data breaches of the different online service.

WHAT TO DO IF YOU RECEIVE AN EXTORTION EMAIL?

If you receive an extortion email:

- **do not respond**
- **do not pay, and**
- **report them to CERT NZ.**

Reports to CERT NZ are completely confidential and are treated with care because we know these threats can be shocking to receive, even if they aren't credible.

If the scammers included a password in the email, make sure to go to any accounts where that password is used, change it and, if possible, enable two-factor authentication.

LASTPASS

At the end of Q4, the password management tool LastPass was compromised leading to an attacker obtaining customer account information and protected (encrypted) vault information. The stolen data includes unencrypted details like company names, usernames, billing and email addresses (amongst other things) and encrypted details like website usernames and passwords.

If you're a LastPass user, it's important to change all your important passwords. By that we mean changing: banking, email, social and medical login accounts and, with time, ideally all passwords.

Two-factor authentication should be enabled wherever possible, for an extra layer of protection.

Using a password manager remains CERT NZ's top recommendation for managing passwords. If you're no longer feeling confident using your existing one, many other great password managers are available both free and paid. Weigh up your options and decide which one might work best for you. For more information on the LastPass breach, you can read about it on our website.[5]

International insights

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

The Canadian Centre for Cyber Security (CCCS) has released its National Cyber threat Assessment 2023–2024. The report notes that ransomware continues to be a persistent threat to Canadian organisations, and it has been judged to be the most disruptive form of cybercrime facing Canadians.[6]

The Australian Cyber Security Centre (ACSC) has also released its Annual Cyber Threat Report, which shows a continuing "increase in the number and sophistication of cyber threats, making crimes like extortion, espionage, and fraud easier to replicate at a greater scale". The ACSC also noted ransomware remained the most destructive cybercrime.[7]

[5] When password managers get hacked

[6] National Cyber Threat Assessment 2023-2024

[7] ACSC Annual Cyber Threat Report July 2021 to June 2022