National Cyber Security Centre

Cyber Threat Report 2025

Pūrongo Tuma ā-Ipurangi 2025

An analysis report by the National Cyber Security Centre

Te Tira Tiaki
Government Communications Security Bureau

www.ncsc.govt.nz

Contents
Ngā kaupapa

Foreword
Whakapuakitanga

Are you prepared for a serious cyber security incident?

If your organisation was targeted by a sophisticated actor today, would you be ready?

New Zealand's remote location at the bottom of the world can isolate us from challenges in other regions, but when it comes to cyber activity, there's nowhere to hide.

Over recent years, the National Cyber Security Centre (NCSC) has dealt with about one incident per day that has the potential to cause harm at the national level. Such incidents don't just involve large corporates or big government agencies – some smaller organisations also play a crucial role in our economy and society and can be affected.

Many New Zealand businesses and organisations make the mistake of assuming they are not big enough, wealthy enough or critical enough to be a target.

As we highlight in this report, there are many reasons why your organisation may be a target.

In cyber security, we talk about the activity of threat actors arising from their capability and intent. Do they have the tools and ability to cause us harm? Do they have a reason to? Around the globe, both capability and intent are on the rise.

Capability is increasing through technological advancement. Business models such as ransomware-as-a-service – in which developers sell or rent ransomware tools and infrastructure to other cybercriminals – are well-established and have enabled a less technically skilled cohort of malicious actors to access effective tools.

In terms of intent, malicious cyber actors target New Zealand organisations for a range of reasons. Financial gain is the obvious one, but actors may also be motivated by espionage (including intellectual property theft), or the desire to cause disruption for political reasons. The current turbulent international environment is more likely to generate motivated actors.

The likelihood of threats being realised also depends on target availability and how well-defended those targets are. Malicious actors' scope for causing harm has been enlarged as the threat surface has also expanded. New systems, technologies and practices that organisations are adopting can open new avenues for attack.

And although you may be doing your best as an organisation to keep your own security practices up to standard, you may be affected by a supplier or third party with links to your network or in custody of your data.

In summary, malicious actors could target you because of what you have, what you know, or what you stand for. You may be a stepping stone to another, more valuable organisation. You may be collateral damage. Or you might just be an easy win.

HOW PREPARED ARE YOU?

While cyber security is an important focus of the Government, most protections in New Zealand exist outside government. Individuals, private organisations, and industry are best-placed to protect data, networked devices, and infrastructure, and most effort in protecting technology and systems needs to come from the owners and operators of these.

This report is designed for leaders making strategic decisions about cyber security risks and investments in medium-to-large organisations in both the public and private sectors. However, the report has relevance for anyone seeking to protect themselves or their organisation from cyber risks. By being equipped with the right context and questions to ask, you can ensure your organisation is thinking about the risks that may affect you. Those who have read our previous Cyber Threat Reports may notice that the format has changed this year. We hope you find value in our new approach.

Bridget White (she/her)
Deputy Director-General Cyber Security (acting)

THE PURPOSE OF THIS REPORT

- This report is written for leaders making decisions about cyber security in medium-to-large organisations.
- It outlines five key judgements about the New Zealand cyber security threat environment.
- We encourage you to use it to consider how prepared your organisation is.
- The report is designed to provide you context, so you can act on informed decisions.

About us
He kupu mō mātou

The National Cyber Security Centre is a part of the GCSB. We make it easy for everyone in New Zealand to play their part in keeping New Zealand cyber-secure. We deliver our work through three primary approaches:

1. We support all New Zealanders to act on informed decisions.
2. We work with key players to build good cyber security basics into New Zealand's cyber ecosystem and essential services.
3. We use our mandate, relationships and specialist capabilities to counter the most serious harms.

Getting in touch
Whakapā mai

Visit **ncsc.govt.nz** for more cyber security advice and information about NCSC programmes. On our website you can:

- report a cyber security incident
- subscribe to receive NCSC news and updates
- subscribe to receive alerts about current cyber security threats and vulnerabilities, and how to mitigate their impact.

General enquiries

For all general enquiries, email us at **info@ncsc.govt.nz**

Follow the NCSC on LinkedIn. **www.linkedin.com/company/ncsc-nz**

Individuals & small businesses

For cyber security advice aimed at everyday New Zealanders and small businesses, visit Own Your Online at **ownyouronline.govt.nz**

www.facebook.com/ownyouronline

www.instagram.com/ownyouronline/

www.youtube.com/@OwnYourOnline

www.linkedin.com/company/ownyouronline/

Key judgements for 2025
Ngā whakataunga matua mō te tau 2025

Cyber security is a critically important consideration for all New Zealand organisations.

In this document we set out five judgements for 2025 regarding cyber security. Each judgement explores a key aspect of the current threat landscape that we think is most relevant for decision-makers.

The judgements are:

1. State-sponsored actors are actively targeting New Zealand
2. The commercialisation of cybercrime means cybercriminals have more tools
3. Hacktivists are targeting New Zealand organisations as global conflicts escalate
4. Threat actors are exploiting supply chains, hidden dependencies and organisational blind spots to cause impact
5. Known weaknesses and unpatched vulnerabilities are providing threat actors with easy access

These are explored further in the following sections.

Our judgements are based on our work both domestically and internationally. This is not an exhaustive list, but they include some of the most prominent, noteworthy and recurrent issues that we observe.

These judgements also reflect the trends in the more severe incidents the NCSC responded to this year. Of the 5995 reports received by the NCSC during the 2024/25 financial year, 331 incidents were triaged as incidents of potential national significance, meaning they received additional analysis and support.

The statistics and case studies used throughout the report are primarily based on our work between 1 July 2024 and 30 June 2025. We recognise that we do not have perfect understanding of the cyber security environment, so these should be regarded as illustrative rather than a complete overview.

This report will give you a picture of how the cyber security environment is evolving and how these changes should be factored into your risk assessments and strategic thinking.

We hope this information will help you consider how well your organisation is prepared for the current cyber threat landscape, and will help to inform the cyber security investment and resourcing decisions you make in your organisation. This information should be considered alongside other sources of information that inform your cyber security decisions.

State-sponsored actors are actively targeting New Zealand

Kei te poke tonu ngā mūrere a kāwanatanga kē i a Aotearoa

State-sponsored actors are among the most sophisticated and persistent threats in cyberspace. They are generally motivated not by financial gain but by national objectives such as gaining strategic advantage.

They may attempt to achieve these objectives through intellectual property theft, espionage, disruption of critical services, and even sabotage.

Globally, there is growing concern and increased awareness of state-sponsored malicious cyber activity, particularly against government organisations, critical infrastructure and sensitive industries.

Tactics and techniques

State-sponsored actors often use techniques such as spear-phishing, zero-day exploitation, and living off the land to blend into legitimate activity on a computer system or network. They may also make use of ephemeral or disposable infrastructure, like botnets. These actors are often referred to as advanced persistent threats (APTs) due to their resourcing and ability to switch between tactics and techniques to achieve and maintain access to their targets.

Spear-phishing sees actors take the time to research victims, to create a customised and convincing message from what appears to be a trusted source. Artificial intelligence (AI) tools make this job much easier and faster. (Read more on the impact of AI on page 15)

EXAMPLES

- In September 2024, US authorities warned that cyber actors affiliated with the Russian General Staff Main Intelligence Directorate (GRU) were responsible for attacks designed to cause espionage, sabotage and reputational harm. (https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-249a)
- Between October 2023 and October 2024, suspected Iranian cyber actors were discovered conducting credential brute-forcing in attempts to access operational technology across the government, information technology, engineering, and energy sectors. (https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-290a)

A zero-day exploitation is a vulnerability that is unknown to the vendor and does not have an available patch. State-sponsored actors are known to utilise zero-day vulnerabilities, often against cyber-mature organisations. The lack of an available security update to address the vulnerability means that malicious cyber actors have more time to compromise computer networks without detection and maintain their unauthorised access.

Living off the land involves the use of legitimate or pre-existing software on a victim network to maintain access. This is less likely to raise alerts for defenders, compared to the installation of malicious software, which may look suspicious in incident response logs and is much more likely to be stopped by antivirus software.

Living off the land techniques have been employed by two prominent threat actor groups referred to as Volt Typhoon and Salt Typhoon.

- **'Salt Typhoon'** activity has been described by our US partner agency, CISA, as a 'broad and significant cyber espionage campaign targeting commercial telecommunications infrastructure'. Salt Typhoon, has been observed in several countries, including New Zealand. New Zealand operates similar systems to partner nations meaning New Zealand organisations need to be aware of this activity and how to defend against it.
- **'Volt Typhoon'** is a PRC state-sponsored actor that has been observed compromising the digital systems of critical infrastructure providers in the United States. The US assesses that Volt Typhoon has compromised multiple critical infrastructure organisations, including telecommunications and energy companies. The actor maintained longstanding access to these organisations using living off the land techniques. The US assesses this is pre-positioning to enable disruptive or destructive attacks against critical infrastructure in the event of a major crisis or conflict. The NCSC assesses that New Zealand's critical infrastructure operators could be vulnerable to similar activity from PRC state-sponsored actors.

Throughout the reporting year, the NCSC published a number of advisories with its international cyber security partners detailing a range of ways in which state-sponsored cyber actors are having success against even cyber-mature organisations worldwide. The NCSC joins its partners in these publications after a robust review process to validate the nature of the threat and the usability of the information to its New Zealand customers. New Zealand organisations should ask themselves, "Could we detect this kind of activity, or what changes do we need to make to do so in future?"

The following are some of the joint publications the NCSC released to help with identifying and mitigating cyber threats linked to state-sponsored actors:

- In July 2024, the NCSC joined the Australian Signals Directorate's Australian Cyber Security Centre and other international partners to release an advisory outlining a PRC state-sponsored cyber group, APT40, and the threat it posed to Australian networks. https://www.ncsc.govt.nz/alerts/prc-mss-tradecraft-in-action/
- In September 2024, the NCSC joined international partners to highlight and help mitigate the threat posed by a botnet created by PRC-linked cyber actors to enable malicious cyber activity. https://www.ncsc.govt.nz/alerts/cyber-security-agencies-call-out-prc-linked-botnet-and-provide-mitigation-advice/
- In April 2025, the NCSC joined its UK counterpart and others in warning of spyware targeting Taiwanese, Tibetan, Uyghur groups and civil society actors. https://www.ncsc.govt.nz/alerts/moonshine-and-badbazaar-spyware-targeting-communities-and-groups/
- In August 2025, the NCSC warned that PRC-linked state-sponsored cyber threat actors were targeting networks globally, including telecommunications, government, transportation, lodging, and military infrastructure networks. https://www.ncsc.govt.nz/alerts/china-state-sponsored-actors-target-networks-globally/

More information can be found at www.ncsc.govt.nz/alerts

The New Zealand landscape

Cyber intrusions and incidents with potential national significance continue to threaten our safety, security and wellbeing.

Incidents linked to state-sponsored actors in the reporting year included:

- compromise of a virtual private network (VPN) appliance in a medium-sized telecommunication company,
- brute-forcing attempts against a central government organisation, and
- spear-phishing of senior public servants.

In the 2024/25 year, nearly a quarter of the incidents of potential national significance the NCSC dealt with had suspected state-sponsored links (82 of 331 incidents). In the previous year, this proportion was 32% (110 of 343 incidents).

The apparent downward trend in reporting numbers does not reflect a softening in the threat landscape. We have continued to observe significant attacks and intrusions, which require effective management and mitigation.

The boundaries between state and criminal activity are blurring as some governments tolerate, enable and sometimes even benefit from criminal groups operating within their jurisdictions.

State-sponsored cyber actors continue to pose a persistent threat to New Zealand. We are aware of some incidents that could have had much more severe impact if they had not been detected at an early stage. An example is presented in Case Study 1.

Additionally, as the modus operandi of some state-sponsored actors is to remain undetected, compromises can come to light much later than they occur. The international exposure of the sophisticated and high-profile cyber campaigns tracked as Salt Typhoon and Volt Typhoon has demonstrated the level of capability and potential impact of state-sponsored actors linked to the PRC Government.

CASE STUDY 1

NETWORK COMPROMISE FOR ESPIONAGE PURPOSES

During 2024/25, an organisation informed the NCSC that unauthorised activity had been detected on its network, and it requested assistance.

The NCSC worked with a commercial cyber security provider to assess the threat and determine how it should be contained. Through analysis undertaken by both teams, it was concluded the activity originated from a resourceful, sophisticated suspected state threat actor that was motivated by espionage.

Investigations found that the suspected state actor had connected to an appliance on the victim's network. The appliance had been running an outdated firmware version which was vulnerable to recently disclosed critical common vulnerabilities and exposures (CVEs). The actor had also attempted to log into staff accounts using a range of techniques including brute-forcing, and had targeted both cloud and cloud-integrated capabilities. Based on post-compromise analysis, the actor was likely seeking to maintain persistence on the victim's network for espionage purposes, consistent with state-sponsored motivations.

A review showed that the organisation's existing cyber security hygiene had been decisive in stopping the actor. This included strong passwords, multi-factor authentication (MFA), and network segmentation.

Through the NCSC's unique capabilities, we verified that no data had been stolen and offered further advice on mitigating any lingering risk.

Implications for organisations

Although critical infrastructure and government agencies are often perceived to be the main targets of state-sponsored activity, no sector is immune.

Any organisation which holds valuable information, contributes to essential services, or holds influence, may be an appealing target.

Organisations that have prepared themselves to defend against cybercriminals should be aware that preventions effective at addressing the easy access points to their systems may not be sufficient to deal with the tactics and techniques of state actors at their most sophisticated – additional measures may be required. State actors are stealthy and play the long game: they often maintain undetected access for months or years, and the impact to your organisation may not be felt immediately. Detecting these actors can require an in-depth understanding of what baseline activity is expected on your network, in order to notice tell-tale variances.

Three questions leaders should be asking

01 Do we have the relationships, systems and processes to provide for early warning and coordinated response?

02 Are we confident in our ability to detect a sophisticated actor using living off the land type techniques?

03 Have we tested our ability to respond to a sophisticated intrusion designed not just to steal, but to remain undetected?

Resources

For further information, refer to the following guidance:

- NCSC | Identifying and mitigating Living Off the Land (LOTL) techniques. https://www.ncsc.govt.nz/protect-your-organisation/identifying-and-mitigating-living-off-the-land-lotl-techniques/
- NZSIS | Countering Espionage and Foreign Interference. https://www.nzsis.govt.nz/our-work/countering-espionage-and-foreign-interference
- NZSIS | Due Diligence Assessments For Espionage and Foreign Interference Threats. https://www.protectivesecurity.govt.nz/assets/psr/due-diligence-assessments.pdf
- New Zealand Information Security Manual: Information Security Monitoring. https://nzism.gcsb.govt.nz/ism-document#Chapter-13001

The commercialisation of cybercrime means cybercriminals have more tools

Nā te tāhoko o te taihara ipurangi kua nui atu ngā utauta ki ngā nanakia ipurangi

Globally, the shift to ransomware-as-a-service (RaaS) has commercialised cybercrime, allowing criminals to 'rent' effective attack tools, and for criminal groups to specialise in different elements of the attack. Meanwhile, new technologies such as AI are accelerating their work and effectiveness.

Cybercriminals are responsible for most of the incidents New Zealanders report to the NCSC. The end goal for cybercriminals is usually financial gain; however, they may carry out activities that are indirectly related, for example by stealing passwords and personal information, in order to stage future attacks.

Ransomware continues to be the most damaging type of criminal attack, causing disruption as well as potential loss of money, data and sensitive information.

Ransomware activities can result not only in data loss and exposure but also disrupted operations, reputational damage, and financial cost – and in extreme cases, threats to life. It is in the interests of criminals to cause as much trouble as possible to increase their chance that an organisation will pay the ransom. Unfortunately, many of those who pay do not get their data back or their systems unlocked, and sometimes they are extorted further with the threat of releasing sensitive data.

EXAMPLES

- In April 2024, MediSecure – a holder of sensitive Australian health data – discovered a database had been encrypted by ransomware actors. Later investigations discovered that over 12 million transactional records across a four-year window had been breached.
- In July 2025, Qantas suffered a customer data breach numbering millions of records, including from New Zealand. Criminals later released data on the dark web.
- Financially motivated cyber attacks in the UK on Marks & Spencer in April 2025 and Jaguar Land Rover in September 2025 crippled operations and are estimated to have cost the firms hundreds of millions of dollars.
- In September 2025, airports across Europe experienced disruption to check-in technology following a ransomware attack.

Tactics and techniques

Ransomware refers to a multi-stage operation by an actor, typically involving the installation of malware to encrypt files, exfiltrate files, and demand payment. Actors seek targets where disruption will have widespread and visible impact, to increase their chances of being paid.

High-value targets include essential services like transportation, where disruption is costly and highly impactful, and organisations with sensitive personal information such as healthcare and government agencies.

For cybercriminals, any opportunity is a good one, however many prepare by conducting research or social engineering to identify valuable targets and increase their chances of success.

Ransomware perpetrators are financially motivated. Of the moderate to significant ransomware incidents reported to the NCSC in 2024/25, all were linked to suspected financially motivated non-state actors.

Cybercriminals use a range of tools to speed up and support their work. For example, vulnerability scanning gives malicious actors a list of potential targets they can attack en masse or target specifically.

With the advent of RaaS, ransomware attacks now require reduced technical expertise to deploy, lowering barriers to entry. The proliferation of RaaS has led to specialisation and corporate-level execution; defenders now find themselves dealing with experienced and professional negotiators.

More than half of the significant incidents the NCSC analysed in 2024/25 were likely to involve use of RaaS.

RaaS continues to evolve, developing new features to assist cyber actors with avoiding detection, victim engagement and money laundering.

The use of AI has only added to the threat (see below).

AI AND CYBER SECURITY RISKS – AMPLIFICATION THROUGH AUTOMATION

Cybercriminals have been early adopters of AI. As a result, attackers no longer need advanced technical skills to launch convincing and scalable attacks. Generative models can create personalised phishing emails in flawless English or te reo Māori, assemble convincing deepfakes for extortion or romance scams, and even write or adapt malicious code. For organisations with thousands of employees and complex supply chains, this means there's a much higher likelihood that at least one employee will fall victim to a convincing scam.

Automation is another major factor. AI can rapidly scan networks for vulnerabilities, test stolen credentials, or exploit misconfigured cloud services. Large New Zealand companies – such as those in finance, energy, health, and telecommunications – may hold valuable data and provide critical services, making them attractive targets. The scale and speed of AI-driven attacks could overwhelm traditional security teams, especially if basic cyber hygiene is lacking. Still, automation benefits both sides: rapid detection and response must outpace automated attacks to remain effective.

AI doesn't reinvent cybercrime, but it supercharges methods and scale. For New Zealand – where a few successful incidents can cause outsized disruption – the implications are that organisations need to close basic security gaps while also carefully leveraging AI for defence.

The New Zealand landscape

Cybercrime continues to have a significant impact on New Zealanders. Of the 331 incidents of potential national significance the NCSC dealt with in the past year, 137 were linked to criminal or financially motivated cyber actors – more than double the year before (65).

The direct financial loss from cyber security incidents reported to the NCSC in 2024/2025 totalled $26.9M, up from $21.6 million in 2023/2024.

These figures are indicative only: the full impact is likely to be much more. A consumer survey commissioned by the NCSC indicated that New Zealanders could be losing as much as $1.6 billion each year to cybercriminals and scammers. In addition, organisations frequently incur operational and reputational losses, and individuals are affected by the associated stress.

Our research also tells us that 53% of New Zealand's small-to-medium enterprises (SMEs) experienced a cyber threat between January and June 2025, a significant increase from the 36% reported in 2024. The impact of these cyber threats on those businesses also increased.

Research indicates that while SMEs understand that cyber security is important, complacency often prevents them from implementing some of the most important security practices.

Ransomware continues to have devastating impacts on New Zealand organisations. In 2024/25, 88 reports of ransomware were recorded by the NCSC, compared to 63 the year before.

These included the following:

- An agriculture producer's IT infrastructure was infected with ransomware, halting production.
- An IT provider's virtual machines were encrypted, causing service disruption, and their backups were deleted, preventing rebuilding.
- A financial service provider was infected with ransomware, compromising documents containing customers' personal information.

Most of the more impactful ransomware incidents the NCSC dealt with in the past year resulted in either suspected or confirmed data exfiltration. The exfiltration of data and the threat of exposing it publicly can provide criminals with additional leverage.

CASE STUDY 2

RANSOMWARE IN THE HEALTH SECTOR

In May 2025, the NCSC received an incident notification from an organisation in the health sector that had been impacted by ransomware. Many of the organisation's servers and endpoint devices had been encrypted, and a large amount of data was stolen.

The organisation's IT provider helped it to take initial remediation steps, which included changing credentials, updating accounts, and deploying extra security measures. The NCSC assisted the organisation by providing technical assistance to help remediate the problem and understand how the ransomware was able to enter its systems.

The NCSC determined that a lack of MFA on an important service had enabled a threat actor to gain access. Fortunately, the organisation had completed system backups just one hour before the ransomware activity occurred. By restoring from these recent backups, it was able to successfully recover its systems and quickly return to normal operations.

This event shows how good security practices – in this case frequent backups – can help mitigate or prevent ransomware incidents. The organisation may have avoided the incident entirely – and prevented data from being stolen – if it had also implemented MFA across its critical systems.

Implications for organisations

Many cyber criminals are skilled, motivated, and well-organised, with a range of effective tools at their disposal. Organisations need to be aware of the way that criminals continue to innovate, whether it's deepfake phishing videos or calls, or deploying information-stealing malware, and how to detect and prevent these.

Through ransomware attacks, cybercriminals can cause significant disruption to business operations, and their extortion activities can damage your reputation with clients and stakeholders. Organisations of all sizes can be targeted. Paying does not guarantee recovery, or that your sensitive data won't be released.

The New Zealand Government recommends not paying a ransom. Payment does not guarantee that you will get your data back, may breach sanctions, and creates harm to others by providing funding for criminal activities.

Three questions leaders should be asking

01 If ransomware impacted our critical systems tomorrow, could we continue operating without paying?

02 Do we understand the personal information we hold and how we store and protect it?

03 Have we tested crisis management, legal, and communications processes for a ransomware event?

The direct financial loss from cyber security incidents reported to the NCSC in 2024/2025 totalled $26.9M, up from $21.6 million in 2023/2024.

Resources

For further information, refer to the following guidance:

- NCSC | Protect your organisation against ransomware. https://www.ncsc.govt.nz/protect-your-organisation/protect-your-organisation-against-ransomware/
- DPMC | Government guidance on cyber ransom payments. https://www.dpmc.govt.nz/our-programmes/national-security/cyber-security-strategy/cyber-ransom-advice
- NCSC | Public communications for cyber security incidents: A framework for organisations. https://www.ncsc.govt.nz/protect-your-organisation/public-communications-for-cyber-security-incidents-a-framework-for-organisations/
- NCSC | Rolls and Responders. https://www.ncsc.govt.nz/protect-your-organisation/rolls-and-responders/
- Information Security Manual: Information Security Incidents. https://nzism.gcsb.govt.nz/ism-document#Chapter-13097

Hacktivists are targeting New Zealand organisations as global conflicts escalate

Kei te whakaeke ngā mūrere i ngā whakahaere o Aotearoa i te nui haere kē atu o ngā whawhai o te ao

Hacktivism usually seeks to cause disruption to business, sector, or state to promote political or social causes. The goal of hacktivist groups is visibility rather than financial gain, but their activities can still undermine trust, damage reputations, and disrupt services.

Unlike state actors or organised cybercriminals, hacktivists often rely on basic but noisy techniques. Issue-motivated cyber actors rarely seek payment or issue demands and frequently claim responsibility for the activity. Their actions may not cause long-term harm, but they can create operational headaches and public embarrassment.

Tactics and techniques

Hacktivists will commonly use distributed denial-of-service (DDoS) attacks and website defacements to cause visible disruption.

DDoS attacks cause an excess of traffic to a network, which can lead to the degradation or inaccessibility of the target network, and sometimes data corruption.

Attack tools are widely available, lowering barriers to entry.

In many cases, actors command sizable botnet infrastructure to orchestrate and sustain DDoS attacks.

Hacktivists will usually target sectors with the highest potential for significant and visible disruption, such as government services, banks and other financial institutions, news media, transport, utilities and retail.

However, the NCSC has observed that hacktivist groups sometimes use opportunistic criteria for target selection, such as existing vulnerabilities and victim availability, rather than a strategic focus on particular organisations.

Large organisations generally engage managed service providers for DDoS mitigation, limiting impact. Smaller businesses, such as those that openly support particular political views or conflict-related activities, could be vulnerable because they often do not have mitigation services in place.

The line between state-sponsored cyber operations and hacktivism has increasingly blurred, with state involvement ranging from direct to indirect. For example:

- Proxies are employed directly to act.
- 'True believer' but independently motivated individuals or organisations conduct attacks aligned with foreign state interests.
- States may turn a blind eye to activity emanating from within their borders.

EXAMPLES

- In the 2024/25 year pro-Ukrainian and pro-Russian hacktivist groups both conducted global distributed denial-of-service (DDoS) campaigns against financial institutions and government sites, including in New Zealand.
- In the same period, environmental and social-justice hacktivists targeted energy companies and public agencies globally to amplify their causes.

The New Zealand landscape

The NCSC is aware of activity associated with hacktivist groups affecting New Zealand organisations during the 2024/25 period. These incidents have often coincided with political activities or statements:

- In October 2024, the NCSC recorded DDoS attacks against a range of financial sector organisations. This occurred at a similar time to multiple pro-Russian campaigns targeting Western governments.
- In June 2025, when the New Zealand Government pledged more financial support to Ukraine, the NCSC recorded DDoS campaigns against organisations in the government, transport, and water sector.

While there has been an increase in the frequency of ideologically motivated cyber incidents in New Zealand, they have had varied success to date.

Nevertheless, disruption can affect customer trust, even if the technical impact is minimal.

There has also been a handful of low-impact New Zealand cyber incidents against operational technology (OT) claimed by hacktivist groups. In situations where OT is less protected, actors setting out to create a nuisance may end up causing significant damage beyond what they expected, escalating tensions and causing unintended consequences.

Although by definition a hacktivist group is motivated by its beliefs, some activity that appears as hacktivism may have other motives.

Hacktivist campaigns may overlap with state or criminal activity, complicating attribution and defence.

At least two known hacktivist groups active against New Zealand were likely created as an unattributable platform for conducting state-sponsored malicious cyber activities.

The actors behind these kinds of cyber incidents probably view DDoS attacks as harder to attribute, plausibly deniable, and unlikely to trigger an escalatory response from the countries affected.

The NCSC anticipates this type of ideologically motivated malicious cyber activity is likely to continue if geostrategic competition trends continue internationally. We assess that the government, financial, news, utilities, IT and retail sectors are most likely to be targeted, due to the potential for noticeable disruption. Cyber actors conducting this kind of activity will target sectors most impacted by digital disruption, as this will help amplify their message.

Implications for organisations

The targets of hacktivism are usually symbolic, for example a media organisation, bank or telecommunications company taking a particular stance on a contentious issue, or associated with a certain country. In such cases, an organisation with a New Zealand connection could inadvertently become a target if hacktivists oppose New Zealand Government policy.

Organisations should consider whether they could be targeted by hacktivists for any reason, and what the impact of a typical hacktivist attack would be on the organisation's business continuity and reputation.

DDoS attacks are much easier to defend against if controls are in place already, rather than trying to mitigate once an attack is underway.

Three questions leaders should be asking

01 Have we assessed our risk profile in relation to hacktivism?

02 Are our websites and online services resilient to denial-of-service attacks?

03 Do we have a plan for communication and reputation management if our organisation becomes a symbolic target?

CASE STUDY 3

HACKTIVISM WITH UNCLEAR MOTIVES

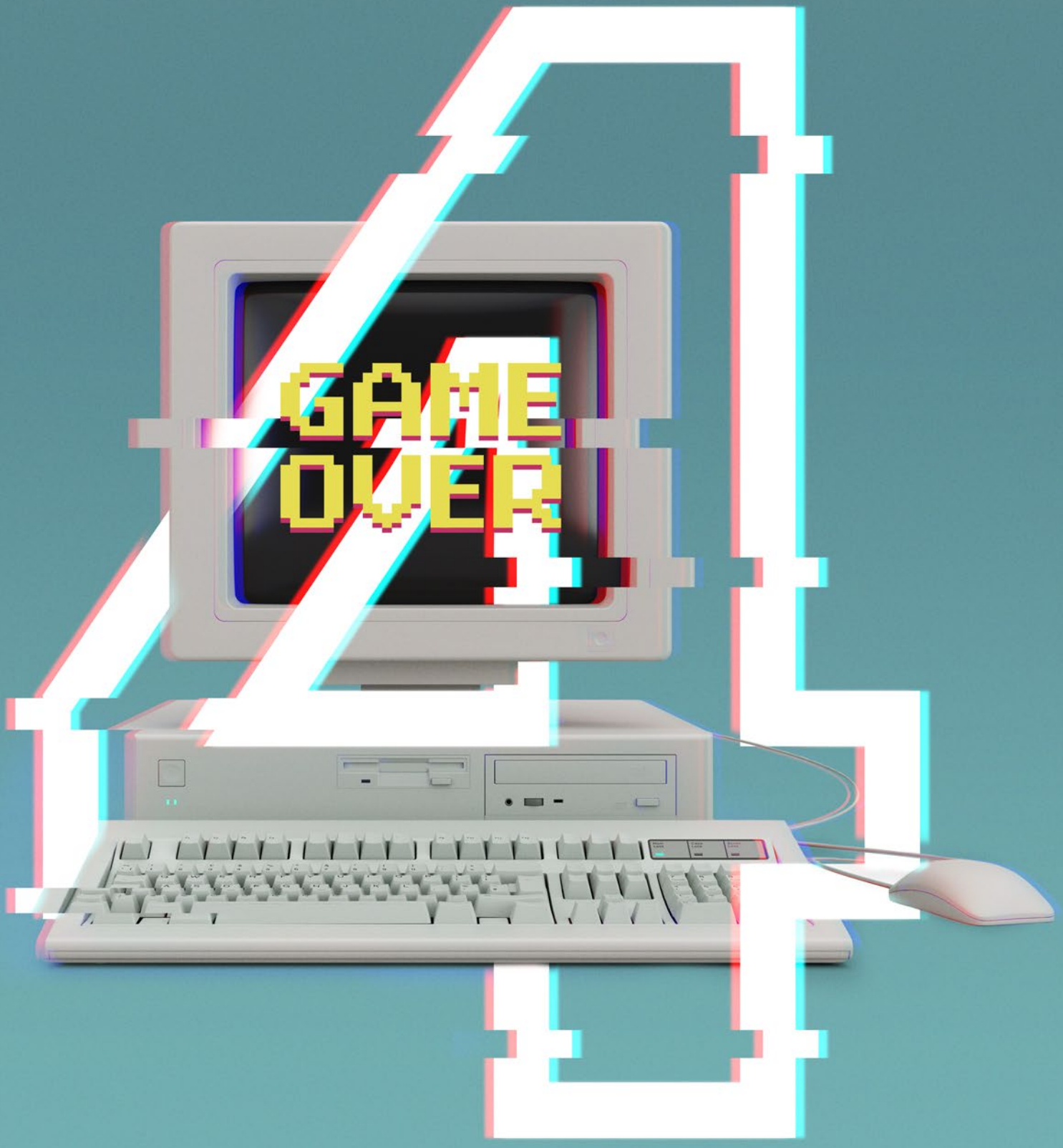
In April 2025, a New Zealand organisation in the health sector began experiencing a high-volume distributed DDoS attack early one morning, causing service outages. Later that same day, the organisation received an extortion email that claimed the attack was being orchestrated by a known hacktivist group. The email threatened to increase the severity of the attack unless a Bitcoin payment was made. However, the email did not specify why this particular organisation had been targeted.

By the evening of the attack, the impacted organisation was able to implement security measures to mitigate the attack and return traffic to normal levels. The following morning, the organisation received another note claiming the attack had been a demonstration, and that the attack would resume with greater severity if the ransom payment was not received. The impacted organisation ensured that adequate security measures had been implemented, and maintained a state of readiness to respond to further attacks. However, no further DDoS activity was observed.

Resources

For further information, refer to the following guidance:

- NCSC | Preparing for and mitigating Denial of service (DoS) incidents https://www.ncsc.govt.nz/protect-your-organisation/preparing-for-and-mitigating-denial-of-service-dos-incidents/
- New Zealand Information Security Manual: Network Security. https://nzism.gcsb.govt.nz/ism-document#Chapter-16188
- New Zealand Information Security Manual: Gateway Security. https://nzism.gcsb.govt.nz/ism-document#Chapter-16567


GAME
OVER

Threat actors are exploiting supply chains, hidden dependencies and organisational blind spots to cause impact

Kei te urutomo ngā kaiwhakatuma i ngā ara tukutuku, ngā tūhononga i waenga wae pūmanawa tē mōhiotia, me ngā wāhi huna o ngā whakahaere kia nui ai te tūkinotia

Malicious actors are increasingly circumventing organisations' defences by targeting blind spots in the form of supply chain vulnerabilities or other dependencies that may be overlooked.

Supply chain (or third-party) attacks occur when actors seek to gain access through vulnerabilities in third-party products and services, vendors and service providers, or software instead of attacking target organisations directly. This approach works where the third party may not adhere to the same security standards as the target organisation, or where actors are prepared to put in the effort to compromise the third party because it is key to unlocking access to one or more valuable targets. Some attackers are successfully using social engineering techniques to achieve this.

Supply chain attacks are conducted by both financially motivated criminals and state-sponsored actors.

Other examples of organisational blind spots include legacy technology, configuration errors, and incomplete closure of accounts at the end of employment.

Organisations can also be indirectly impacted due to the cascading effects of a cyber security incident. A compromise of a single organisation of any size can trigger systemic disruption to the interconnected organisations in that sector, or those who rely on that organisation for business operations.

OT is an area where blind spots can occur. Organisations may not be accustomed to considering cyber security risks for technology that was previously protected by air gaps (i.e. physically separated). The linking of OT to software and digital tools introduces new risks organisations need to manage.

EXAMPLES

- In 2021, a vulnerability affecting Apache's Log4j, a Java-based logging library, was widely exploited by threat actors to gain significant global compromises. Few system administrators or IT professionals knew they were running Log4j as it was frequently bundled inside commercial software. By targeting a weakness in a little-known technical library, cyber actors could take advantage of unseen weaknesses in a wide range of commercially purchased and business-critical software. The Log4j vulnerability has had a long tail in New Zealand and overseas, and continues to provide sophisticated cyber actors with a viable entry route to networks even in 2025.
- In 2025, a hacking group known as Scattered Spider has been responsible for some high-profile supply chain attacks, such as one against Marks & Spencer (M&S) in the UK. The group is known for its use of social engineering techniques, including posing as IT or helpdesk workers to convince staff to hand over credentials, multi-factor authentication codes, or to run remote access tools.
- In 2025, a security researcher discovered a vulnerability in Microsoft's cloud identity manager (Entra ID) that allowed access to every Microsoft tenant. There is no evidence of exploitation prior to Microsoft patching the vulnerability (CVE-2025-55241). If exploited, this vulnerability could have allowed malicious actors to create accounts in any or all Azure tenancies, with widespread impact.
- Also in 2025, threat actors used a critical vulnerability in SAP NetWeaver, a widely used enterprise software platform, to deploy sophisticated backdoor malware. SAP moved quickly to release a patch; however, the damage had already been done for affected organisations that had failed to apply the patch in time. In the case of one exploit, attackers were reportedly able to deploy the malware, establish control, and begin extracting sensitive data within a matter of hours.

Tactics and techniques

Technology evolution means organisations are now more reliant on digital information, outsourcing and cloud platforms – including software-as-a-service. With more platforms, services and providers in the supply chain mix, a typical organisation's attack surface is growing. The increasing use of outsourced systems means that responsibility for security can be shared across both the provider and customer. This can create gaps if organisations are unclear on who is doing what.

Threat actors understand these challenges and exploit them accordingly.

The New Zealand landscape

Although we have not observed high-profile data breaches of New Zealand organisations in the past year, New Zealand customers have been impacted by breaches of other organisations such as Qantas, where thousands of records were stolen by cybercriminals.

In 2025, a cyber actor advertised millions of credentials reportedly associated with a legacy cloud service hosted by Oracle on a dark web forum. By some estimates, over 100,000 customers' key and credential material had been exposed.The NCSC tracked the activity and provided advice to critical sectors about precautions they could take.

Activity similar to that linked to the Scattered Spider group has also been observed in New Zealand. Scattered Spider targets IT helpdesks and uses the access for data extortion and ransomware. Its attacks often involve social engineering techniques to learn how to get password resets from helpdesks, and phone calls to employees to gain the information required to successfully obtain the reset. The group may also search social media sites for the personal information they need.

The NCSC is aware of similar techniques targeting helpdesks that have been used to infiltrate a number of New Zealand organisations.

Government agencies are a valuable target for both state-sponsored and financially motivated actors. Both types of actors have successfully compromised IT service providers with New Zealand Government customers in the last five years. Due to the nature of these businesses, there are significant impacts beyond the single organisation.

As described in Case Study 4, supply chain attacks are occurring in New Zealand where a breach of a subsidiary or vendor is used as a stepping stone to a larger and potentially more lucrative target.

CASE STUDY 4

VENDOR COMPROMISE PREVENTED

In June 2025, an organisation in the energy sector received a malicious email that targeted several of their inboxes. The malicious email originated from a compromised account owned by an external vendor, and it contained a link to a PDF embedded with malware. The PDF was hosted on a Sharepoint account owned by the vendor. This kind of attack is called business email compromise (BEC), which is a type of phishing.

Fortunately, the energy company's existing security policies blocked the link to the external PDF. While one of their users did attempt to interact with the link, no harm was caused due to the security policy, and the user's sessions were quickly revoked. The energy company then contacted the vendor, who confirmed that they had been compromised by a threat actor. The threat actor had highly likely obtained access to a staff email account. The energy company was able to verify that no sensitive information had been shared with the vendor in the past, and they advised all staff to be extremely careful in their communications with the vendor, until it was confirmed that the threat had been fully contained.

In this case, a threat actor gained access to the vendor's systems and then attempted to leverage this access to target other organisations who had relationships with the vendor. Through having good security policies already in place, the energy company avoided any impact when its staff received phishing links.

OPERATIONAL TECHNOLOGY

It's not just IT that's vulnerable to exploitation – OT is also at risk. OT refers to systems that interface with the physical world to automatically control and monitor equipment and processes. Many New Zealand organisations rely on OT systems to deliver services, including those in critical sectors like water, electricity and transport. Common types of OT include industrial control systems (ICS), supervisory control and data acquisition (SCADA) systems, and building management systems.

Historically, OT devices were designed for use in isolated, air-gapped networks without external connectivity. Due to business requirements such as the need for remote control or monitoring of OT equipment, OT devices are increasingly connected to the internet and corporate IT networks. However, many OT devices lack adequate security functionality. They are often legacy devices that are difficult to patch and may be challenging to upgrade or replace due to high costs or operational requirements.

During 2024/25, NCSC analysis of public-facing infrastructure identified numerous OT devices in New Zealand that are connected to the internet. It is highly likely that the asset owners were unaware of the risk posed by this exposure.

OT is increasingly being targeted by malicious cyber activity worldwide. Malicious cyber actors may opportunistically or systematically target OT devices in New Zealand for financial or political gain. The potential impacts of unauthorised access to OT devices include financial loss, loss of asset control, loss or degradation of essential services, environmental impacts or, in serious cases, loss of life.

Resources

For further information, refer to the following guidance:

- NCSC | Supply Chain Cyber Security. https://www.ncsc.govt.nz/protect-your-organisation/supply-chain-cyber-security-in-safe-hands/
- NCSC | Preventing unintentional operational technology (OT) device exposure. https://www.ncsc.govt.nz/protect-your-organisation/preventing-unintentional-operational-technology-device-exposure
- New Zealand Information Security Manual: Product Security / Supply Chain. https://nzism.gcsb.govt.nz/ism-document#Section-14623

Implications for organisations

The interconnected nature of IT infrastructure means organisations need to look beyond what they directly control when considering their cyber security.

Thinking laterally, organisations must consider potential weaknesses in vendors or third-party suppliers that could be used as access points.

Organisations also need to consider the indirect impact of an organisation they rely on being impacted by a cyber security incident, and the flow-on impacts to business operations and customer trust.

This could include a critical system being unavailable due to a ransomware or a denial-of-service event, or an organisation holding your information being subject to a data breach. A supplier or vendor you work with could have its business email system compromised, resulting in your organisation paying fraudulent invoices.

The NCSC strongly recommends that OT asset owners and operators identify internet-connected OT devices in their networks. Where internet connectivity is unintentional or unnecessary, operators should change configurations to prevent or restrict access to, from, or across the internet. Where remote connectivity is necessary, a layered defence should be implemented.

Five questions leaders should be asking

01 How well do we understand and manage cybersecurity risk across our supply chain?

02 What requirements are placed in contracts regarding management of supply chain risk?

03 Do we provide training to staff to recognise social engineering attacks?

04 Have we considered supply chain cyber incidents in our business continuity planning?

05 If our organisation uses OT, are we confident there are no unintentional or nonessential instances of internet connected OT in our network?

Known weaknesses and unpatched vulnerabilities are providing threat actors with easy access

He māmā te uru poka noa a ngā kaiwhakatuma nā ngā ngoikoretanga me ngā whakaraeraetanga kāore i te whakatikahia

Headlines can often give the impression that malicious actors are highly skilled players with the tools to penetrate sophisticated defences. While that is true in some cases, many attacks succeed because organisations fail to address common weaknesses. We regularly observe that poor patching, weak credentials, and misconfigured systems provide threat actors with easy entry points.

Threat actors can move quickly to exploit known vulnerabilities, reducing the time window for patching. Applying a patch may not mean you're protected if the threat actor has already gained access.

Compromised credentials are a common way for malicious actors to gain initial access, yet securing accounts through enforced password policies and MFA is one of the simplest mitigations an organisation can undertake.

This highlights the importance of cyber security fundamentals: resilience often depends less on advanced tools and more on consistently applying basic practices across the entire environment.

EXAMPLES

- A joint advisory published by NCSC and partners in July 2024 highlighted that sophisticated cyber actors possessed the capability to rapidly transform and adapt proof of concept code of new vulnerabilities, enabling them to immediately utilise them against target networks. They also regularly conducted activity to identify vulnerable, end of life, or no longer maintained devices, and continue to find success exploiting vulnerabilities dating back to 2017. https://www.ncsc.govt.nz/alerts/prc-mss-tradecraft-in-action/
- In July 2025 Microsoft advised of APTs and ransomware actors using spoofing and remote code execution vulnerabilities to exploit on-premises SharePoint servers. https://www.microsoft.com/en-us/security/blog/2025/07/22/disrupting-active-exploitation-of-on-premises-sharepoint-vulnerabilities/
- Technical advice published by NCSC and partners in August 2025 highlighted that actors had considerable success exploiting publicly known common vulnerabilities and exposures and other avoidable weaknesses within compromised infrastructure to gain initial access. https://www.ncsc.govt.nz/alerts/china-state-sponsored-actors-target-networks-globally/

Tactics and techniques

Exploiting known vulnerabilities remains a high-use tactic for both criminals and state actors. Common gaps include unpatched software, reused passwords, and unsecured remote access. Threat actors often scan the internet for exposed systems, compromising them at scale.

Common vulnerabilities and exposures (CVEs) often have information about how to exploit them in the public domain, which enables threat actors to quickly use available exploits against unprotected systems. Where this information exists for a particular vulnerability, there is an increased urgency for organisations to patch and review logging for signs of compromise prior to the patch being applied.

Keeping software and systems up to date remains critically important, especially in a fast-evolving environment. The growing rate of software vulnerabilities exposed each year highlights that software updates are not optional or intermittent – patching requires ongoing, proactive attention to keep pace with vulnerability disclosures.

Meanwhile, remote work has expanded the attack surface due to poorly secured endpoints and cloud services.

Compromised credentials is another common avenue for access. Valid credentials are of high value to cyber actors and enable a range of malicious activities across the adversary lifecycle.

ANALYSIS: THE LONG TAIL OF VULNERABILITY EXPLOITATION

In 2025, the NCSC contributed to analysis alongside international partners of CVEs routinely and frequently exploited by malicious cyber actors in 2023.

This analysis found that threat actors continue to have success exploiting vulnerabilities up to two years after public disclosure of the vulnerability.

Although the majority of vulnerabilities were initially exploited as a zero-day, the reality is that many malicious actors can use the same techniques even once a fix has been made available, due to the fact organisations have not taken advantage of updates.

The New Zealand landscape

Failure to patch devices or software in time has been a contributing factor in a significant proportion of the NCSC's recorded high impact incidents over the last five years.

In the past year, the NCSC observed the targeting, scanning and exploitation of historical and recently disclosed CVEs. This included a CVE dating back to 2018.

The exploitation of public-facing applications continues to be a prevalent initial access vector for malicious cyber actors.

We continue to record high numbers of incidents involving public-facing applications, including devices used to provide internet access and security to private networks. These incidents consisted of the targeting, scanning and/or exploitation of both zero-day vulnerabilities, and historical or recently disclosed CVEs in a range of applications. Malicious cyber actors may also exploit end-of-life devices and misconfigured devices – for example, with permissive defaults or poor security settings.

Case study 1 (page 11) illustrated how recently disclosed vulnerabilities enabled cyber actors to compromise an organisation's network during 2024/25.

In the 2024/25 year, the NCSC also recorded a range of activity involving the misuse of credentials. Malicious cyber actors published compromised credentials online, used brute-force techniques (repetitive guessing of passwords) to access accounts, and phished for credentials or to compromise accounts. Some of these incidents involved business email compromise (BEC), in which a cyber actor compromises the legitimate email account of a trusted contact to extract information from another.

Of the moderate to significant credential-based incidents, government organisations were highly impacted, likely due to the targeting of sensitive information.

CASE STUDY 5

DEVICE VULNERABILITY

In August 2025, the NCSC received a report from New Zealand Police with information that devices owned by 19 New Zealand organisations had been compromised by a suspected ransomware group. When the NCSC investigated this report, it was discovered that all the compromised devices were exposed to the same known vulnerability. The NCSC was able to identify the owners of 18 of the devices, which included small businesses, councils and managed services providers (MSPs). The NCSC shared this information with New Zealand Police, who in turn contacted the impacted organisations to inform them of the vulnerability, and provided advice about how to remediate the problem. Two of the notified organisations identified malicious activity on their systems and were able to mitigate this to prevent any further damage.

Resources

For further information, refer to the following guidance:

- NCSC | Patching. https://www.ncsc.govt.nz/protect-your-organisation/patching/
- New Zealand Information Security Manual: Product Security / Product patching & updating. https://nzism.gcsb.govt.nz/ism-document#Section-14530
- New Zealand Information Security Manual: Public Cloud Security / Governance, Risk assessment & Assurance. https://nzism.gcsb.govt.nz/ism-document#Section-17478

Implications for organisations

Threat actors – particularly advanced ones – are quick to exploit the time between vulnerability disclosure and patching. This means that organisations must focus on vulnerability management.

Additionally, organisations should ensure that second-order defences such as network segmentation, principle of least privilege, MFA, and software allow-lists are in place. These measures can reduce the impact of clicking on bad links, or zero-day vulnerabilities being exploited against public-facing applications.

Poor credential practices also offer opportunities to threat actors, especially with the rising adoption of cloud-based services that can be accessed from anywhere in the world.

As New Zealand organisations adopt a cloud-first strategy for storing and processing their sensitive information, malicious cyber actors will almost certainly 'follow the data' and target application programming interface (API) endpoints, mobile endpoints and credentials to gain cloud accesses. Credential and account compromises will continue to be an important part of malicious cyber tradecraft, enabling cyber actors to steal sensitive information.

Three questions leaders should be asking

01 Do we have an ongoing process for understanding the systems within our environment?

02 How effective is our patch management programme, and do we allow downtime to address vulnerabilities?

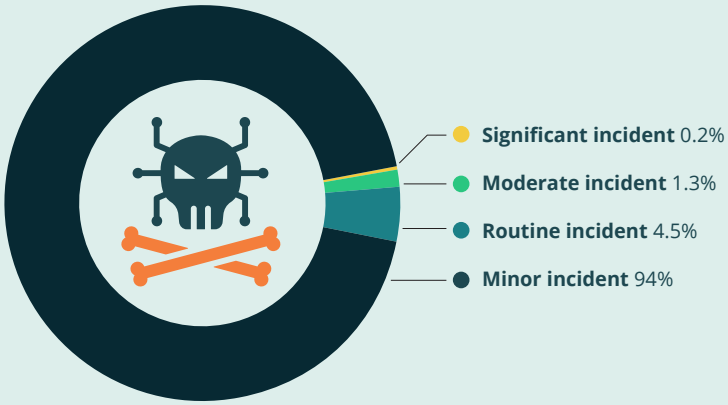
03 Are we confident our systems are not exposed through misconfiguration or unmonitored endpoints?

By the numbers: 2024/25

Total incidents reports recorded for 2024/25

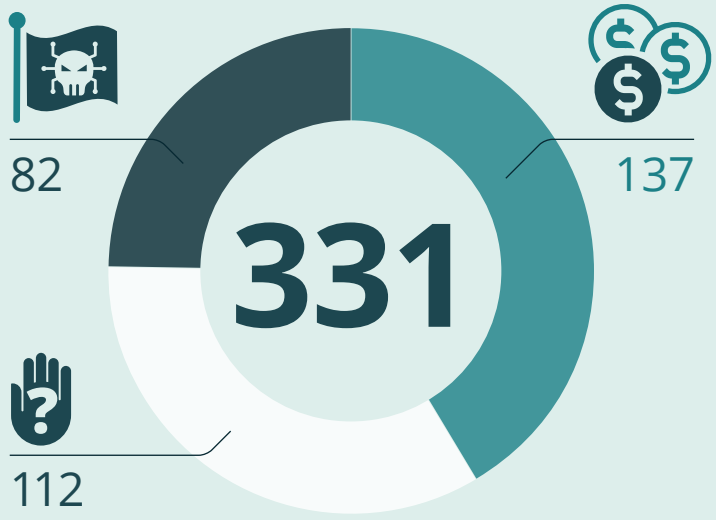
5995

(compared to 7122 in 2023/24)



Total incidents triaged for specialist technical support because of potential national significance

(compared to 343 in 2023/24)



25% incidents linked to **suspected state-sponsored actors** (compared to 32% (110) in 2023/24)

41% incidents were likely **criminal or financially motivated** (compared to 19% (65) in 2023/24)

34% incidents **could not be linked** (compared to 49% (168) in 2023/24)

$26.9m

direct financial loss recorded

(compared to $21.6 million in 2023/24)

$47.9m

estimated harm prevented by NCSC detection services work

(compared to $38.8 million in 2023/24)

Incident reporting analysis 2024/25
Tātaritanga pūrongo maiki mō te tau 2024/25

New Zealanders can report cyber security incidents to the NCSC through an online portal, which enables us to provide relevant advice on recommended next steps to those affected. The NCSC receives incidents of all sizes, from phishing sightings up to major cyber security breaches.

INCIDENT TRIAGE

The NCSC handles incident reports through two distinct triage processes. Most incident reports are managed through the NCSC's general triage process.

A small number of incidents are triaged for specialist technical support because of the nature of the victim, or the nature of the incident. These incidents could cause high impact at the national level and are referred to as incidents of potential national significance. These may be incidents affecting organisations such as operators of critical infrastructure, and incidents that have the potential to impact large groups of New Zealanders.

The following section presents an analysis of incidents reported to us during the period 1 July 2024 to 30 June 2025. Due to the way incidents are dealt with, some analysis is only available for certain subsets of the data.

WHY REPORT?

Any person or organisation in New Zealand can report incidents to the NCSC, to obtain help and guidance. We can help you understand what has happened, stop the incident getting worse, and help you get back on your feet. Reporting also provides us with information about the threat landscape, which we can use to issue advisories and alerts, or take disruptive action.

Severity and sector breakdowns

In 2024/25, the NCSC received a total of 5,995 reports. Individuals made 4,343 reports and organisations were responsible for 1,321 reports. The remaining did not specify the reporter.

INCIDENT SEVERITY

The NCSC triages incidents into six categories ranging from C1 (most significant) to C6 (minor).

In the 2024/25 year, the most severe incidents were categorised as C3. These incidents included several DDoS incidents that were likely linked to ideologically motivated malicious cyber activity, and ransomware incidents that had links to criminal or financially motivated actors. There was also a significant incident involving the network compromise of a New Zealand organisation, which had links to state-sponsored actors.

C6	C5	C4	C3	C2	C1
5635	268	81	11	0	0
Minor incident	Routine incident	Moderate incident	Significant incident	Highly Significant incident	National Cyber Emergency

A national cyber emergency (C1) is defined as an incident that causes severe disruption to a core New Zealand service, and/or affects key sensitive data, and/or undermines the economic or democratic stability of New Zealand. At the other end of the scale, a minor incident (C6) is defined as an incident causing a known or likely impact on an individual/ individuals, or precursor activity against an individual/ individuals or a small or medium enterprise. In the middle, a significant incident (C3) is defined as an incident causing a known or likely impact on a large commercial enterprise, wider government, or supply chain to core New Zealand services.

Highly significant incidents (C2) consume substantial time and resources, but even significant (C3) or moderate incidents (C4) can take weeks to resolve and will generally involve complex responses involving several teams. For minor or routine incidents (C5 or C6), the NCSC might respond by providing general advice or alerts to customers.

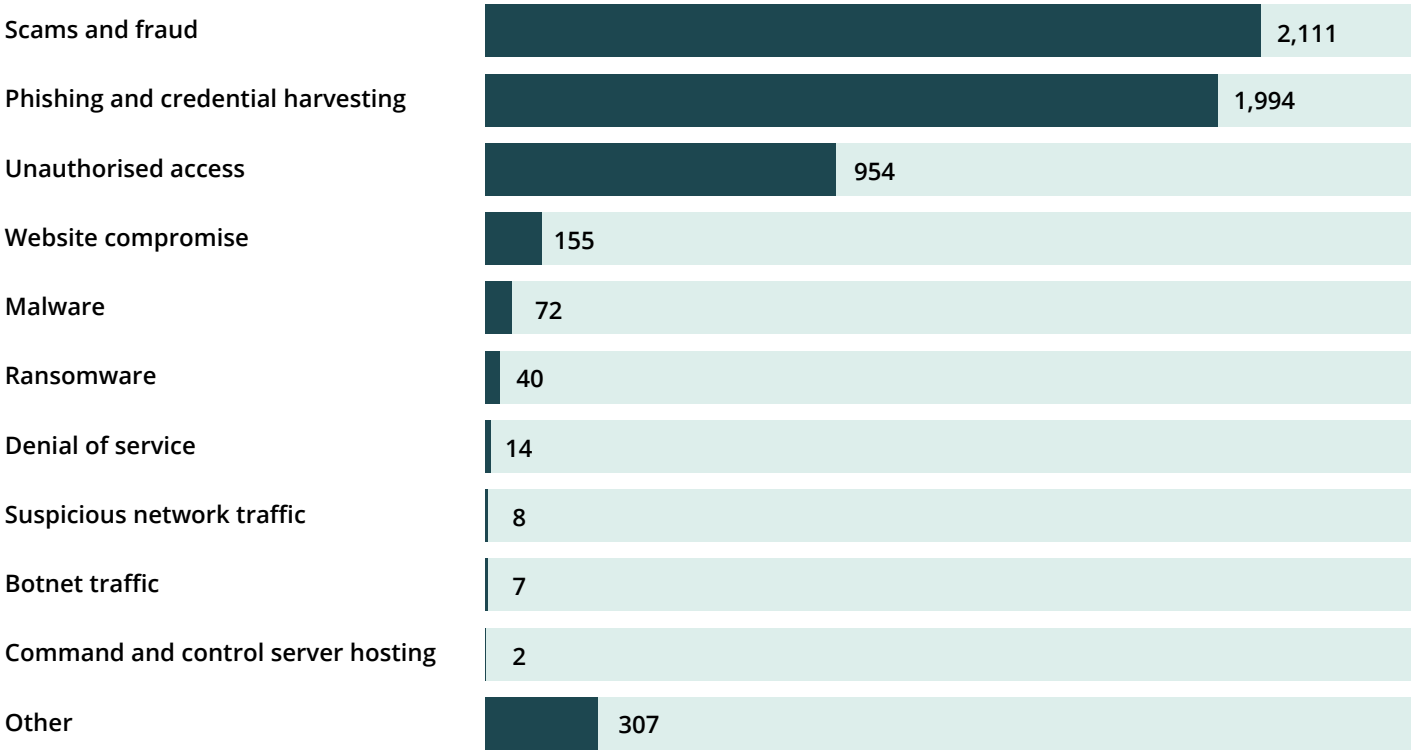
SECTOR BREAKDOWN

The following table shows the sector breakdown of the 5,664 incidents handled through our general triage process

Agriculture, Forestry and Fishing	24	Not Specified	929
Arts, Recreation and Other Services	26	Professional, Scientific, Technical, Administrative and Support Services	49
Construction	40		
Education and Training	21	Public Administration and Safety	11
Electricity, Gas, Water and Waste Services	6	Rental, Hiring and Real Estate Services	8
Financial and Insurance Services	29	Retail Trade and Accommodation	45
Health Care and Social Assistance	34	Technology	23
Individual	4343	Transport, Postal and Warehousing	19
Information Media and Telecommunications	21	Wholesale Trade	17
Manufacturing	19		

SUB-CATEGORY BREAKDOWN

The following table shows a breakdown of the 5,664 incidents handled through our general triage process by sub-category.



FINANCIAL AND OTHER LOSSES

The NCSC records the direct financial loss reported by victims, whether lost to scams or the cost of recovery, where this information is volunteered.

The direct financial loss reported in 2024/2025 totalled $26.9M, increasing from $21.6 million in 2023/2024.

The NCSC has recorded several types of loss amongst the incidents handled through the general triage process:

- 1,697 financial loss incidents: this includes not only money lost as a direct result of an incident, but also the cost of recovery, for example the cost of contracting IT security services.
- 274 data loss incidents: loss or unauthorised copying of data, business records, and intellectual property.
- 114 reputational loss incidents: damage to the reputation of an individual or organisation as a result of the incident.
- 63 operational impact incidents: the time, staff and resources spent on recovering from an incident, taking people away from normal business operations.
- 26 technical damage incidents: impacts on services like email, phone systems or websites, resulting in disruption to a business or organisation.
- 118 other loss incidents: includes types of loss not covered in other categories.

Due to the way incidents are handled, not all financial loss information is reported or recorded.

Analysis of incidents of potential national significance

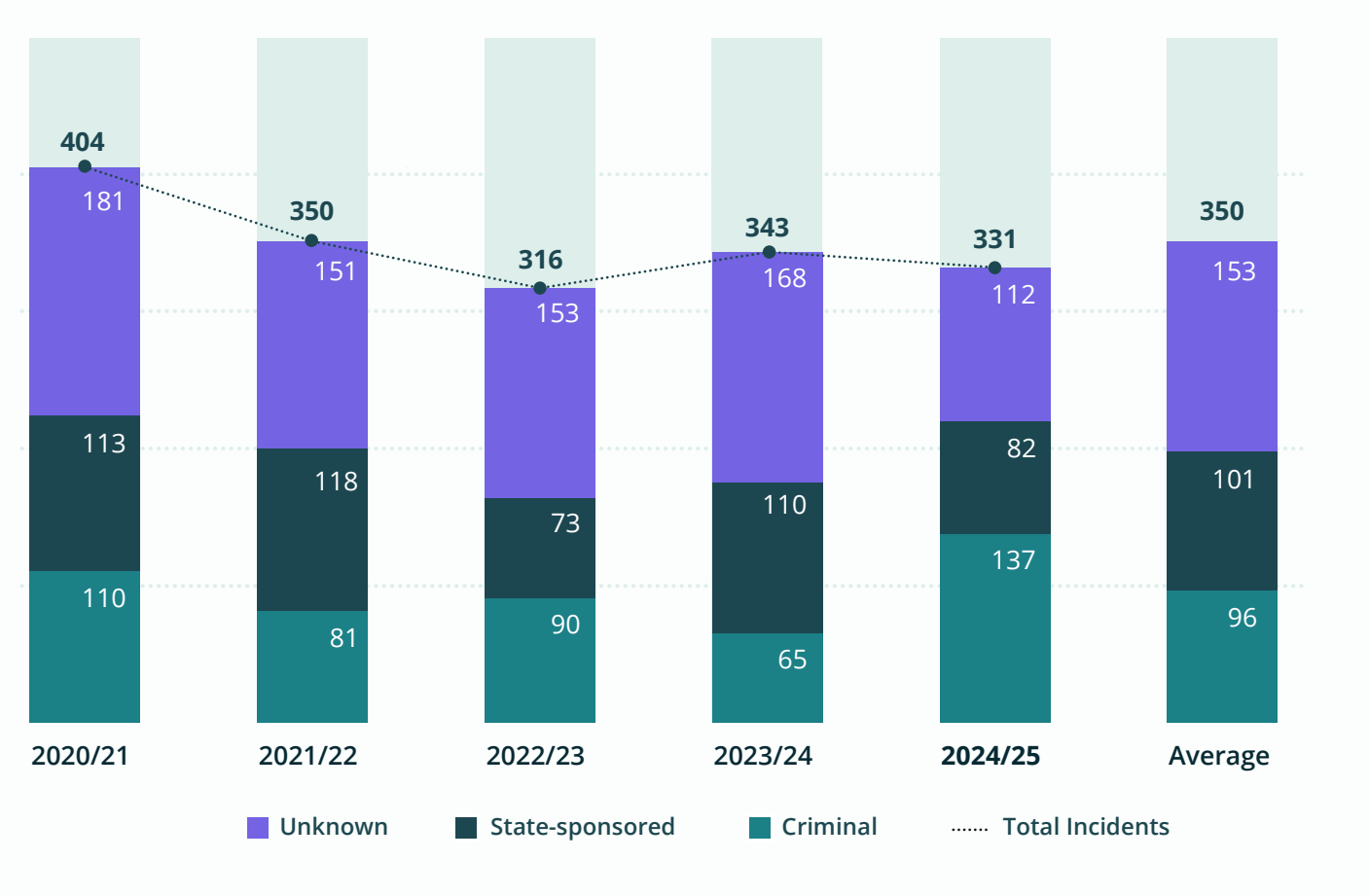
In 2024/25, 331 incidents reported to the NCSC were triaged for specialist support and analysis, and are referred to as incidents of potential national significance.

Actor motivations

Out of the 331 incidents, 82 indicated links to suspected state-sponsored actors, compared to 110 in the 2023/24 year.

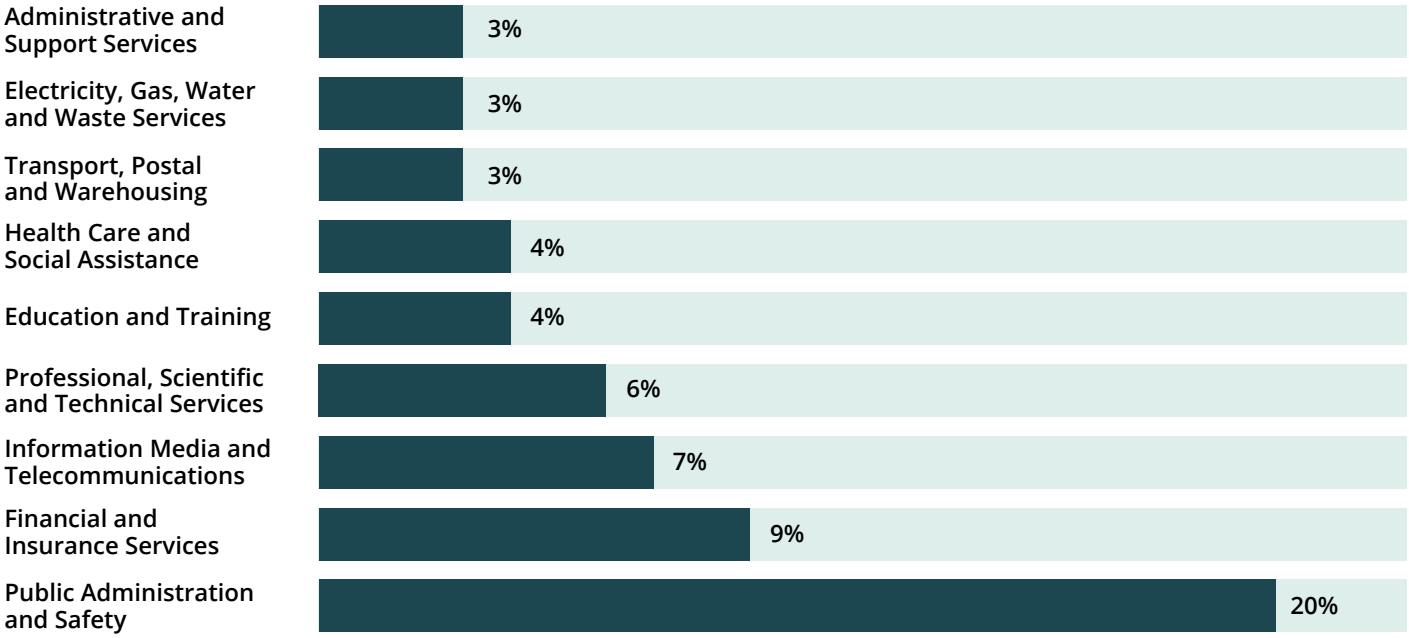
Of the remaining incidents, 137 indicated links to criminal or financially motivated actors, compared to 65 in the 2023/24 year.

Over time, the number of incidents of potential national significance dealt with by the NCSC has remained largely stable.



BREAKDOWN BY SECTOR

The sectors most affected by incidents of potential national significance during 2024/25 were public administration and safety, financial and insurance services, information media and telecommunications, and professional, scientific and technical services. The public administration and safety sector – made up of central government agencies, local councils, public order and safety services, and defence – experienced a fifth of these potentially high-impact incidents. During 2024/25 the NCSC observed a moderate increase in the targeting of the financial sector.



HARM PREVENTION THROUGH RESPONSE TO INCIDENTS OF POTENTIAL NATIONAL SIGNIFICANCE

In 2024/25, through response to the 331 incidents of potential national significance, the NCSC prevented an estimated $47.9 million worth of harm to New Zealand. This figure reflects incidents where the NCSC's detection of malicious cyber activity or engagement with victims likely prevented future harm.

Since 2016, the NCSC has prevented approximately $468.9 million worth of harm to significant organisations across New Zealand.

The model used to estimate harm factors in important impacts such as losses caused by intellectual property theft, including copyright and patent infringement. While assigning a dollar value to harm prevention can provide a useful benchmark, many of the impacts of cyber harm are intangible. Loss of public confidence and trust, reduced health and wellbeing, and hesitance to adopt new technologies can all eventuate when cyber resilience is low.

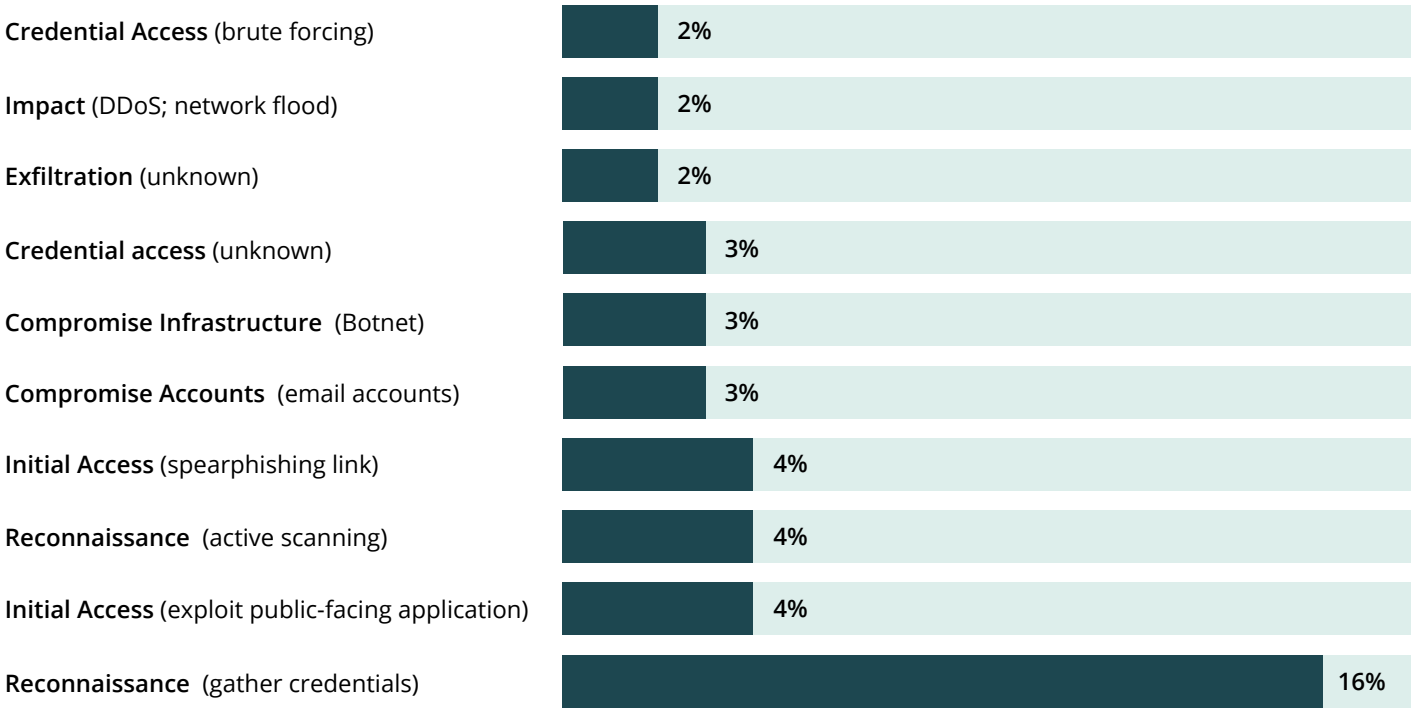
COMMON TACTICS AND TECHNIQUES

The NCSC maps incidents of potential national significance to the MITRE ATT&CK framework to gain insights into common or emerging trends. This framework is an open source knowledge base that shows cyber adversary tactics and associated techniques based on real-world observations.

The following graph show the tactics and techniques observed in incidents of potential national significance the NCSC handled in 2024/25, classified using the MITRE ATT&CK framework.

For more details on the tactics and associated techniques see MITRE ATT&CK® https://attack.mitre.org/

Most-recorded MITRE ATT&CK techniques observed in incidents of potential national significance 2024/25



Glossary
Rarangi kupu

	TERM / KUPU	DEFINITION / WHAKAMĀRAMATANGA
A	**Advanced persistent threat (APT) / Tuma pakepake arā atu anō**	A well-resourced, highly skilled cyber actor or group that has the time, resources, and operational capability for long-term intrusion campaigns. Their goal is typically to covertly compromise a target, and they will persist until they are successful. They are very capable of compromising secured networks using both publicly disclosed and self-discovered vulnerabilities.
	Application Programming Interface (API) / He Tāhono Papatono	A set of rules and tools that allows software applications to communicate, share data, and request services from each other, enabling integration, automation, and functionality across different systems and platforms.
B	**Botnet / Whatunga Pūwerewere**	Networks of compromised personal or office devices such as internet modems, personal computers, or network attached storage. Malicious cyber actors use these as infrastructure to send spam, perform denial-of-service activities, or attempt to obfuscate the origins of a malicious cyber campaign.
	Brute-force attack / He kōkiri takimano	A hacking method that systematically tries all possible passwords or encryption keys until the correct one is found, exploiting weak credentials through automated, repetitive guessing to gain unauthorised access to systems or data.
	Business Email Compromise (BEC) / He Whakamōrea Īmēra Pakihi	A cyber attack where criminals impersonate executives or trusted contacts via email to manipulate employees into transferring money, sharing sensitive data, or taking unauthorised actions, often leading to significant financial and operational consequences. BEC is a type of phishing attack.
C	**Cloud service / Ratonga kapua**	Provides ubiquitous, convenient, on-demand access to shared pools of computing resources such as servers, storage, or online applications.
	Common vulnerabilities and exposures (CVE) / Whakaraeraetanga	A vulnerability is a weakness in software, hardware, or a network that can be exploited by an actor. The Common Vulnerabilities and Exposures (CVE) database is a publicly available register of known vulnerabilities, each assigned a unique identifier in the format of CVE-yyyy-xxxx.
	Credentials / Whakatūturu pārongo	A user's authentication information used to verify identity – typically a password, token or certificate.
	Cryptocurrency miner / Maina moni whitirangi	Malicious software that co-opts computing resources for generating cryptocurrency. Many digital currencies require the solving of computationally intensive mathematical problems in order to generate digital assets.
	Cyberspace / Āteatāurungi	The global network of interdependent information technology infrastructures, telecommunication networks, and computer processing systems in which online communication takes place.
	Cyber security / Whakahaumaru ā ipurangi	Measures to protect systems, data and devices from unauthorised access and ensure the confidentiality, integrity, and availability of information.

	TERM / KUPU	DEFINITION / WHAKAMĀRAMATANGA
D	**Data breach / Raraunga wāwāhi**	The intentional or unintentional release of sensitive or private information into an insecure environment.
	Defence evasion / Karo kaupare	A tactic that describes a series of attempts to prevent network defenders from discovering a malicious actor.
	Denial of service (DoS) / Whakakore ratonga	An attempt to make an online service unavailable by overwhelming the service with more traffic than it can handle.
	Disinformation / Ngā kōrero horihori	The deliberate, intentional spread of false and misleading information designed to achieve a strategic purpose.
E	**Endpoint / Pito Whakamutunga**	A network-connected device that acts as an access point for data and applications, including laptops, desktops, and mobile devices, often requiring security measures to prevent unauthorised access and cyber threats.
	Exfiltration / Tāhae	Where an actor has unauthorised access to private organisational data (for example, legitimate credentials or intellectual property) and copies it from a system.
H	**Hacktivism / Porotū Mūrere**	The use of hacking techniques to promote political, social, or ideological causes, where activists breach or disrupt systems, leak data, or deface websites to draw attention to their message or protest perceived injustices.
	Hybrid threat / Tuma momorua	A mix of military, non-military, covert and overt activities by state- and non-state-sponsored actors that occur below the line of conventional warfare.
	Hypervisor / Kaiwhakahaere pūrere mariko	Software enabling the creation, management, and running of discretely hosted virtual machines (VMs) on the same hardware.
I	**Incident / Maiki**	An occurrence or activity that appears to have degraded the confidentiality, integrity, or availability of a data system or network.
	Indicators of compromise (IoCs) / Paetohu whakamōrearea (ngā IoC)	Usually IP addresses, domain names, or files that may be shared publicly or in confidence. Together they suggest a computer system or network may be compromised.
L	**Living off the land / He ora nō te whenua**	A technique using legitimate and pre-existing software on a victim network, in contrast to the installation of malicious software, to maintain network accesses. Use of legitimate software and accounts is less likely to raise alerts for defenders.
M	**Malicious cyber actor / Nanakia tūkino mōhiohio**	An individual or group of people who seek to exploit computer systems to steal, destroy or degrade an organisation's information. Actors may be individual computer hackers, part of an organised criminal group, or state-sponsored.
	Malware / Pūmanawa kino	Malicious software or code intended to have an adverse impact on organisations' or individuals' data, such as viruses, Trojans, or worms.
	Mitigation / Ārai mōrea	Steps that organisations and individuals can take to minimise and address cyber security risks.

	TERM / KUPU	DEFINITION / WHAKAMĀRAMATANGA
	MITRE ATT&CK framework / **Te Pou Tārawaho MITRE ATT&CK**	A knowledge base of adversary tactics, techniques, and procedures, used by cyber security professionals to understand, detect, and defend against cyber threats through structured analysis of attacker behaviour.
N	**Nationally significant organisation /** **Whakahaere hira ā-Motu**	Organisations such as government agencies, key economic generators, niche exporters, research institutions, and operators of critical national infrastructure. If these organisations were affected by a cyber security incident, the impact could lead to national-level harm.
	Network-attached Storage (NAS) / **Rokiroki Āpiti-Whatunga**	A dedicated device connected to a network that provides centralised file storage and sharing for multiple users or systems.
O	**Operational Technology (OT) /** **He Hangarau Whakahaere**	The systems and equipment used to control, monitor and manage industrial processes and physical operations, such as machinery, power grids, and transport systems, enabling real-time automation and safety in critical infrastructure.
	Opportunistic cyber activity / **Ngohe ā-ipurangi tūpono**	Occurs when malicious cyber actors select their victims based on the availability of a vector of compromise, regardless of victim location, sector or intelligence value.
P	**Personal information /** **Ngā mōhiohio whaiaro**	Information about an individual, including name, date of birth, biometric records, medical, educational, financial, and employment information.
	Phishing / **Hītinihanga**	The use of fake, deceptive or alluring messages to solicit a behaviour from the recipient – such as clicking a link or divulging personal information or credentials.
	Public attribution / **Whakahuatia whānuitia nō hea**	A tool used by governments and private-sector organisations to deliberately release information about the source of a cyber intrusion, primarily to uphold norms about what constitutes acceptable state behaviour in cyberspace.
R	**Ransomware /** **Pūmanawa utu uruhi**	A type of malware designed to disrupt the use of computer systems and files until a ransom is paid.
	Ransomware-as-a-Service (RaaS) / **Ko te taupānga-whawhe-hei-ratonga**	A criminal business model where developers sell or lease ransomware tools to affiliates, who deploy attacks and share profits. It lowers technical barriers, enabling widespread, scalable cyber extortion campaigns.
S	**Small Office/Home Office (SOHO) /** **Tari Iti / Tari Kāinga**	A business setup with few employees operating from a small or home-based workspace, using consumer-grade technology to manage professional tasks, communications, and network operations.
	Spear phishing / **He hītinihanga ā-tao**	A targeted cyber attack where malicious actors craft personalised messages to trick specific individuals into revealing sensitive information, clicking malicious links, or installing malware, often by impersonating trusted contacts or organisations.
	Supply chain compromise / **Poke ara ratonga**	A form of attack that targets software, hardware or an IT service provider, where the ultimate aim is to exploit downstream customers.

	TERM / KUPU	DEFINITION / WHAKAMĀRAMATANGA
T	**Targeted cyber activity / Ngohe ā-ipurangi heipū**	Occurs when malicious cyber actors demonstrate an intent or a tasking to compromise an organisation for its intelligence value, regardless of a specific access vector.
V	**Virtual Private Network (VPN) / Whatunga Tūmataiti Mariko**	A secure connection that encrypts internet traffic and routes it through a remote server, protecting user privacy, hiding IP addresses, and helping to prevent data from being intercepted on public or untrusted networks.
	Virtual private server (VPS) / Tūmau tūmataiti mariko	A portion of a large physical server divided into virtual spaces available for temporary use.
Z	**Zero-day vulnerability / Whakaraeraetanga rā-kore**	A software vulnerability for which there is currently no patch, and for which there is often no CVE number assigned. The term derives from the number of days for which defenders and developers have been aware of the vulnerability.

Te Tira Tiaki
Government Communications
Security Bureau