

CYBER THREAT REPORT

2023/2024

The National Cyber Security
Centre is part of the Government
Communications Security Bureau




Te Tira Tiaki
Government Communications
Security Bureau



**National Cyber
Security Centre**

Contents

Ngā kaupapa

- 3 Foreword
Whakapuakitanga
 - 4 By the numbers
Mā ngā tau
 - 6 Aotearoa New Zealand threat landscape
Te āhuatanga o ngā tuma i Aotearoa
 - 8 Incidents usually affecting individuals or small to medium businesses
Ngā whakaeke ā-ipurangi ka pā ki te tangata, ki ngā pakihi iti ki te waenga rānei
 - 12 Incidents of potential national significance
Ngā mōreareatanga ka tūpono whaipānga ki te motu
 - 16 The impact of ransomware
Te pānga o ngā pūmanawa tonono utu
 - 18 Analysing trends in tactics and techniques
Te tātari i ngā ia rauhanga, tikanga hoki
 - 20 High-impact techniques and mitigations
Ngā tikanga me ngā whakamaurutanga pānga nui
 - 25 Loss and harm
Ngā ngaronga me te tūkinotanga
 - 26 International threat landscape
Te āhuatanga i te ao
 - 29 Conclusion
Whakakapi
 - 29 Getting in touch with the NCSC
Te whakapā atu ki te NCSC
 - 30 Glossary
Rarangi kupu
- 

Foreword

Whakapuakitanga

The National Cyber Security Centre (NCSC), a part of the Government Communications Security Bureau (GCSB), is Aotearoa New Zealand's lead operational cyber security agency. An important organisational milestone was reached in the past financial year, when New Zealand's Computer Emergency Response Team was transferred from the Ministry of Business, Innovation and Employment (MBIE) to the NCSC. This integration process, when completed, will result in an agency that provides cyber security services to all New Zealanders – from individuals and small to medium enterprises, through to nationally significant organisations.

This Cyber Threat Report outlines the NCSC's view of the domestic threat landscape for the year from 01 July 2023 to 30 June 2024. The report provides insight into the scope and nature of cyber threats targeting the information and systems of New Zealand organisations and individuals. The report identifies and analyses some of the common, recurring techniques that malicious cyber actors have used in cyber incidents.

The information in this report is primarily intended to support the work of cyber security practitioners and researchers, as well as cyber security decision makers. However, anyone with an interest in cyber security may find the report informative, and I encourage all New Zealanders to build their understanding of cyber security.

This is the first reporting year in which the NCSC has compiled a whole-of-economy overview of cyber threats. While still drawn from separate data sets, in this report readers can begin to see the extent to which our country's entire economy is being impacted by malicious cyber activity.

This year's report illustrates how malicious cyber activity affects every part of New Zealand society. Good cyber security awareness and practices help to protect against the harm this malicious activity can cause. This report encourages familiarity with the cyber landscape and better understanding of the techniques and tactics used by malicious cyber actors, and recommends steps to mitigate them. Through good decisions and action, New Zealand can become a place where good cyber security happens everywhere, all the time, by everyone.

Lisa Fong (she/her)

Deputy Director-General Cyber Security.

By the numbers

Mā ngā tau

The NCSC in 2023/24

The NCSC receives and handles incident reports through two distinct triage processes. Most incident reports are handled through the NCSC's general triage process because they do not require specialist technical attention. Often these incidents affect either individual New Zealanders or small to medium businesses. The NCSC acknowledges that while these incidents did not require specialist attention, they remain highly impactful for the people or organisations they affect.

A much smaller proportion of incidents are triaged for more 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 are incidents affecting organisations such as operators of critical infrastructure, and those that have the potential to impact large groups of New Zealanders. This report examines both categories of incident and provides analysis of key statistics and trends within them.

7122

Total incident reports recorded by the NCSC

DISRUPTIONS AND INDICATORS

10.3m

In 2023/2024, the NCSC disrupted over 10.3 million malicious cyber events via Malware Free Networks® (compared to 250,000 in 2022/2023).

This exponential growth has continued since the reporting period closed.



28,804

Indicators of malicious activity published in 2023/24 via Malware Free Networks.



11,386

Phishing indicators published in 2023/24 via the Phishing Disruption Service.

343

Incidents triaged for specialist technical support because of potential national significance

Compared to 316 incidents in 2022/2023 - an increase of 8.5%



110

or 32% of 343 incidents of potential national significance indicated links to suspected state-sponsored actors

Compared to 28% in 2022/2023

65

out of 343 incidents of potential national significance, or 19%, were likely criminal or financially motivated

Compared to 28% in 2022/2023



6779

Incidents handled through the NCSC's general triage process, often affecting individual New Zealanders or small to medium businesses

Compared to 7744 in 2022/2023, a decrease of 12.5%

HARM REDUCTION AND FINANCIAL LOSS

\$38.8m

\$38.8 million worth of harm prevented in 2023/2024. Since June 2016, the NCSC has prevented an estimated \$421.2 million worth of harm to Aotearoa New Zealand's nationally significant organisations.

\$21.6m

Total financial loss reported to the NCSC in incidents handled through the NCSC's general triage process

Compared to \$22.4 million in 2022/2023

Since 2017, the estimated total financial loss reported through the CERT function is \$121 million.



THE NCSC IN A TYPICAL MONTH THIS YEAR:

Detected **7** cyber incidents affecting one or more nationally significant organisations through the NCSC's cyber defence capabilities.

Received **22** new incident reports or requests for assistance for incidents of potential national significance. Of the new incident reports received each month, 15 came from international or domestic partners while 7 came from self-reporting by victim organisations.

Recorded **565** incidents handled through the NCSC's general triage process, often affecting individual New Zealanders and small to medium businesses and organisations.



IN THE 2023/2024 YEAR THE NCSC AND GCSB:

Received **143** notifications of network change proposals under the Telecommunications (Inception Capability and Security) Act 2023 (TICSA).

Conducted **21** assessments of regulated space activities under the Outer Space and High-altitude Activities Act 2017 (OSHAA).

Conducted **74** assessments of regulated radio spectrum activities under the Radiocommunications Act 1989.

Provided advice on **39** assessments under the Overseas Investment Amendment Act 2021 (OIAA).



THE NCSC INCREASED AOTEAROA NEW ZEALAND'S COLLECTIVE CYBER RESILIENCE:

Delivered **82** incident reports to customers.

Published **19** advisories for customers, including 16 co-authored with domestic and international partners.

Published **30** critical vulnerability alerts.

Co-chaired **24** sector-based Security Information Exchanges.

Aotearoa New Zealand threat landscape

Te āhuatanga o ngā tuma i Aotearoa

The cyber threat landscape is constantly changing, so it is vital to understand key cyber security threats in order to inform responses to the challenges. Malicious cyber activity is likely to continue to impact a larger range of systems and victims as New Zealand's dependence on technology grows in size and complexity.

Aotearoa New Zealand's growing connectivity of devices and networks, alongside the adoption of emerging technologies (such as artificial intelligence and machine learning), has made our domestic cyber landscape more complex, and our nation continues to experience cyber threats from an increasing number of sources. A rising dependence on digital technology within New Zealand's economy and day-to-day life is also providing more opportunities for malicious cyber activity to affect more victims.

State-sponsored malicious cyber activity and hacktivism

State-sponsored malicious cyber activity endures and primarily poses an espionage threat to New Zealand organisations. This year, the NCSC has observed a wider range of state-sponsored malicious cyber activity and some heightened activity from traditional adversaries.

While the number of incidents that can be linked to state-sponsored actors (110 incidents, or 32% of incidents of national significance) is up 8.5% on the previous year, it is broadly consistent with the proportion of recorded state-sponsored incidents over the previous five years. These have ranged from 33% in 2019/20, 28% in 2020/21, and 34% in 2021/22. An exception was a decrease to 23% in 2022/23.

New Zealand's international relations, involvement in global organisations, technological innovations, and research, means our nation holds information that is likely of high intelligence value, and state-sponsored cyber actors continue to demonstrate the intent and capability to target us for its acquisition.

The tense geopolitical environment – including the rise of hacktivism, fallout from the Russia-Ukraine conflict, and acceleration of disruptive cyber capabilities – has almost certainly increased the cyber threat to New Zealand organisations. The NCSC has seen this reflected in cyber incidents in a number of ways, including an increase in Russian state-linked malicious cyber activity and pro-Russian hacktivists targeting multiple New Zealand government organisations.

Hacktivism refers to the act of using digital techniques to gain unauthorised access to computer files or networks for politically or socially motivated purposes.

As more cyber threat actors enter this environment, it is becoming increasingly difficult to disassociate or attribute state and criminal cyber activity. A proportion of unattributed cyber incidents this year was likely also state-sponsored activity that could not be linked. Additionally, there is the potential that some criminal groups are being directed by states, or at least have tacit approval to conduct malicious cyber activity that aligns with state interests.

Cyber-dependent and cyber-enabled crime

New Zealand is increasingly experiencing incidents in which sophisticated cyber criminals are using their capabilities and wider resources to scale their operations.

Ransomware has remained a persistent threat to New Zealand's nationally significant organisations, smaller businesses and even schools. Disruption efforts, such as arresting actors and taking down infrastructure, have resulted in a decrease in financially motivated cyber incidents this year. However, it is expected that this will only be temporary as groups diversify and rebuild. Ransomware actors continue to take advantage of exfiltrated data to extort payment from their victims, increasing the potential for reputational and economic harm, and impact to critical services. Dominant ransomware players continue to successfully target high-profile victims. Extortion activity in New Zealand was not only limited to ransomware; victims also experienced disruptive distributed denial-of-service (DDoS) activity in lieu of encryption or data leaks.

The scale and impact of online scams and cyber-enabled fraud is rising in New Zealand, enabled through the growing use of social media and cryptocurrency. The compromise of business or corporate email accounts is of growing concern and is becoming increasingly profitable for criminals. This is because it enables cyber criminals to pretend to be trusted organisations, making it more likely for people to provide personal information. Victims are experiencing significant personal, reputational and financial harm as a consequence of this activity.

Tradecraft and technology

The proliferation of cyber capabilities has lowered the barrier of entry for malicious cyber actors, providing access to more sophisticated skills and techniques. Offensive cyber tools and services (including spyware), once only available to well-resourced countries who could develop them internally, are now widely accessible to both states and cyber criminals. This growing availability of effective malicious cyber tools, compromised credentials, and vulnerabilities in public-facing infrastructure, has made it

easier for malicious cyber actors to work at scale and with the ability to cause national-level harm in New Zealand.

Advancements in and adoption of these technologies is enabling the propagation of scams and other forms of cybercrime. In particular, the scale and sophistication of this enabling activity is likely to test the resilience of financial and identity systems as malicious cyber actors improve their ability to bypass security controls. Whilst controls such as multi-factor authentication (MFA) can mitigate against some of this activity, malicious cyber actors continue to develop tactics, techniques and procedures (TTP) that challenge these cyber security defences.

The use of large-scale data and credential breaches to enable malicious cyber activity is an ongoing trend. This year, the NCSC saw significant data breaches occur worldwide, some of which included New Zealanders' personal information. An example this year was a publicly reported incident in which a finance company experienced a breach of customers' personal identity and contact information. These breaches can subsequently allow actors to identify targets for phishing activity, or to directly compromise accounts: two of the most prolific and impactful forms of malicious activity experienced by New Zealanders.

Cyber threat actors' success from social engineering use is increasing. This year social engineering was used across the sophistication spectrum: from scams against individual victims, to state-sponsored cyber actors using it to gain accesses for cyber espionage. What makes social engineering effective is its reliance on the human element, rather than technical vulnerabilities in software and systems. A wide range of malicious cyber and scam actors rely on social engineering and behavioural manipulation to convince a victim to act against their interests.

Cyber threat actors will likely continue to experiment with new tradecraft and technologies, but success does not necessarily rely on these. The threat to victims from simpler, long-standing methods – such as phishing to deploy malware or vulnerability exploitation – is still prevalent across New Zealand's domestic cyber threat landscape, from individuals to our nationally significant organisations.

The next section of this report illustrates how this cyber threat landscape translates into incidents recorded by the NCSC. First, the report outlines the key trends related to the 6779 incidents handled through the NCSC's general triage process and the most common incident types. Then the report focuses on the 343 incidents of potential national significance and provides insight into the types of measures that could prevent these incidents from occurring.

Incidents usually affecting individuals or small to medium businesses

Ngā whakaeke ā-ipurangi ka pā ki te tangata, ki ngā pakihi iti ki te waenga rānei



The majority of the incidents recorded by the NCSC affect individuals and small to medium businesses and organisations. Cyber criminals continue to prey on people's increasing reliance on technology in their daily lives, as well as an absence of fundamental cyber security protections. Scams and fraud, phishing and credential harvesting, and unauthorised access were the most common types of incidents this year.

In total, NCSC recorded 7122 incidents in 2023/2024. The majority of these incidents, 6779, were handled through the NCSC's general incident triage process because they did not require specialist technical attention. Often, these incidents impacted individual New Zealanders or small to medium businesses. While these incidents did not require specialist or intensive technical attention, they may be highly impactful for the people or organisations they affected.

6779

Incidents handled through the NCSC's general triage process.

565

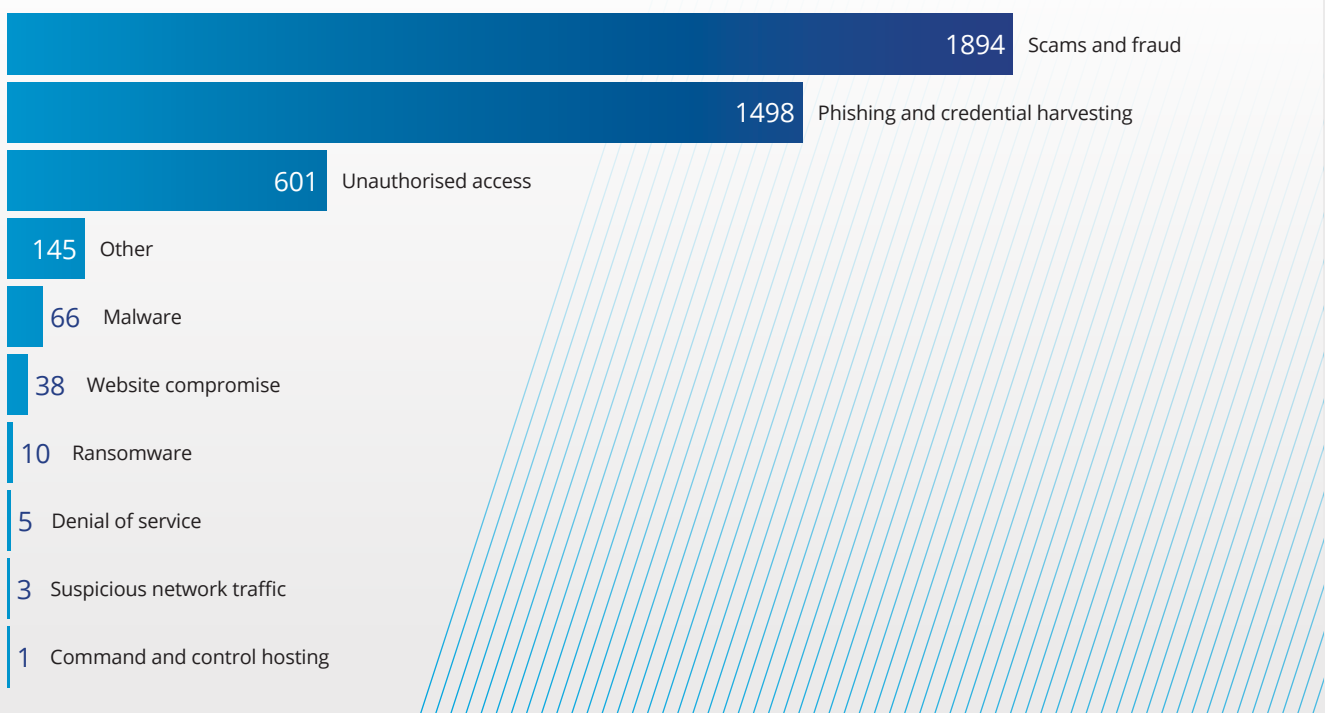
Average incidents per month.

The 6779 incidents handled through the NCSC's general triage process was 12.5% lower than the previous year. For these incidents, scams and fraud, and phishing and credential-harvesting were the most common types of incident in this year. Both incident types generally rely on a person inadvertently taking actions that are part of malicious cyber activity. Most categories of incident experienced an overall decline from 2022/2023 figures, except website compromise and denial-of-service.

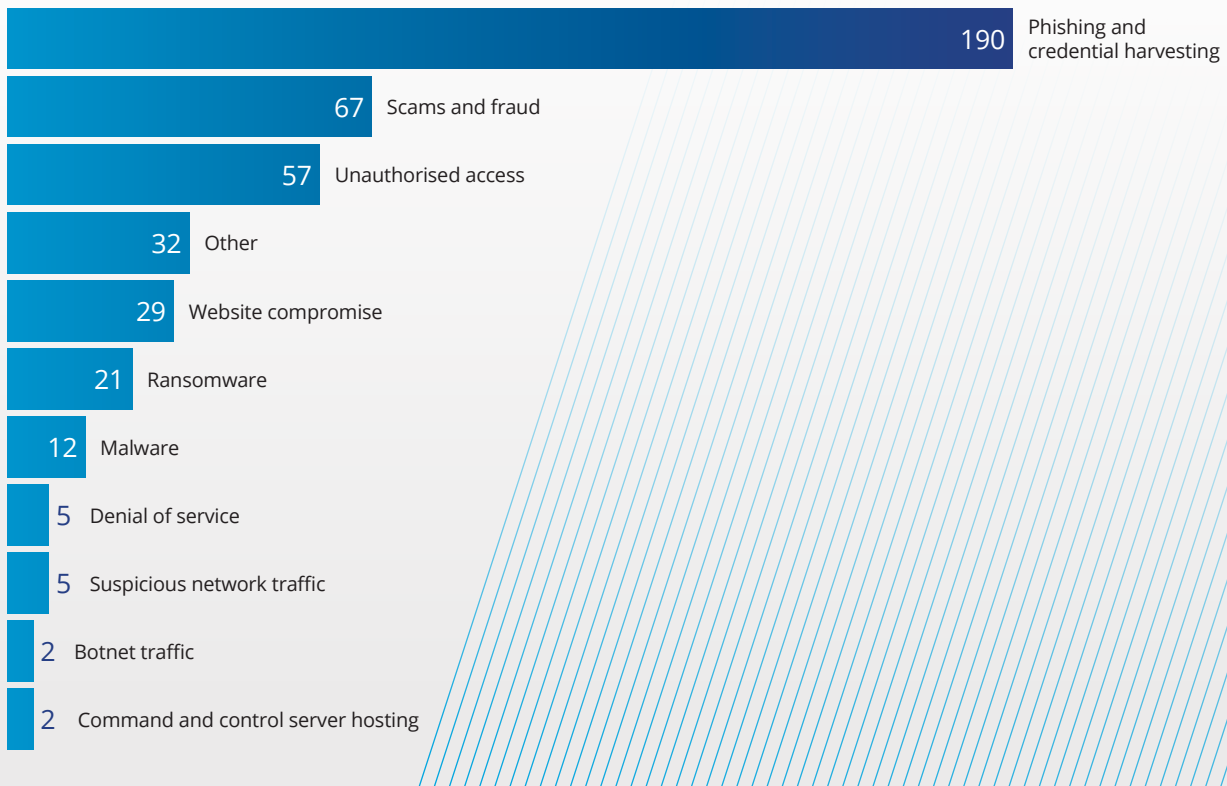
All 2023/2024 incidents handled through general triage process, by category



2023/2024 incidents handled through general triage process affecting individuals, by category



2023/2024 incidents handled through general triage process affecting organisations, primarily small to medium, by category



Scams and fraud incidents

Of the 6779 incidents handled through NCSC's general triage process in 2023/2024, 30% related to scams and fraud. Scams and fraud incidents rely on deceiving a legitimate user into doing something, rather than gaining unauthorised access to an account or system. Although the scams and fraud incidents included here are cyber-enabled, they can often only be prevented through the individual identifying them as illegitimate, as opposed to other cyber incidents which are cyber-dependent and can be prevented through cyber security controls. Incidents of scams and fraud includes fake investment 'opportunities' that are propagated over email, or online deals that are too good to be true.

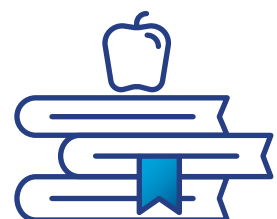
Cyber-enabled crimes are assisted, facilitated or escalated in scale by the use of technology.

Cyber-dependent crimes can only happen on a computer, where the computer or the system is the target.

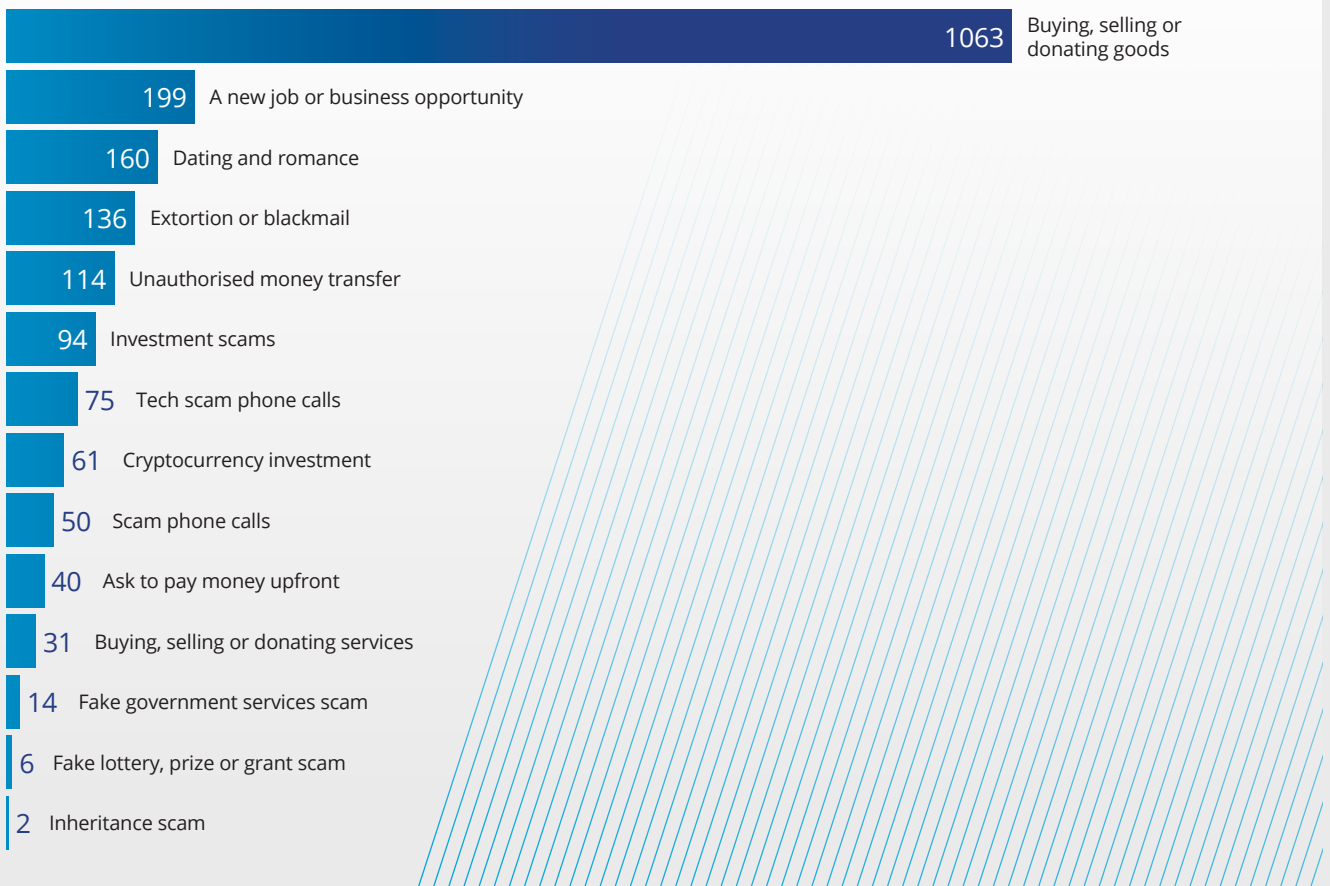
This incident type consistently features in the top three incident types reported. During 2023/2024, investment scams saw a 176% increase from the previous financial year (34 to 94 incidents). Extortion/blackmail scams increased from 119 to 136, although the reported financial loss decreased.

Case study: education sector incident

In August 2023, the NCSC became aware of reports of phishing coming from an organisation in the education sector. The NCSC let the organisation know they likely had a compromised email account. The organisation was then able to remove the malicious access to the compromised account. The NCSC also used the Phishing Disruption Service (PDS) to help organisations block the malicious website domain.



Breakdown of incidents in the scams and fraud category



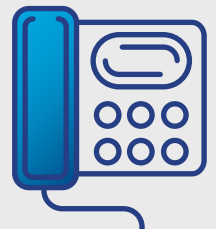
Cyber security incidents targeting individuals remain a concern, despite lower numbers of reported incidents. With technology use pervasive within day-to-day life, whether people are buying and selling goods or pursuing career opportunities, threat actors are willing to identify and exploit opportunities to prey on people’s trust.

The NCSC provides general technical advice regarding scam and fraud incidents. Incidents that have potential financial or legal consequences, or where further action is required, are referred to New Zealand Police or other relevant agencies, with consent from the individual or organisation reporting.

Phishing and credential-harvesting incidents

Phishing and credential-harvesting continue to be the most common incidents reported by organisations, despite a 31% decrease from the previous year. This category was the second-most common incident reported by individuals (after scams and fraud) despite decreasing by 19%. The prevalence of this incident type is largely due to its use ranging from unauthorised money transfer to ransomware. The most common phishing impersonation theme was mail or package delivery, making up the vast majority of phishing

emails and links. Other impersonation themes include government services, banks, and online shopping.



Unauthorised access incidents

In 2023/2024, the NCSC handled 658 reports of unauthorised access through its general triage process. 601 reports impacted individual New Zealanders, and 57 reports impacted organisations - a 23% and 27% decrease from the previous year, respectively. A significant portion of these reports involve cyber threat actors gaining unauthorised access to social media accounts. For individuals, this frequently results in malicious messages being sent to their friends and family, spreading malware and furthering the distribution of scams. For organisations, this may include messaging customers as well as purchasing fraudulent ads to spread the same malware and scam messaging. The best ways to prevent unauthorised access include using long, strong and unique passwords, along with multi-factor authentication (MFA) to improve cyber security and reduce opportunities for malicious cyber actors to bypass security controls.

Incidents of potential national significance

Ngā mōreareatanga
ka tūpono whaipānga
ki te motu



A subset of incidents the NCSC responds to are triaged for more intensive technical support based on the nature of victim or incident. These incidents could cause high impact at the national level, and are referred to as incidents of potential national significance. This year there was an increase in the number of state-sponsored incidents. This increase is consistent with global experience of an increasingly adversarial cyber threat landscape.

An incident of potential national significance can include those that affect the systems and data of organisations in key sectors such as government, key economic generators, niche exporters, research institutions, or institutions that are important for New Zealand's health and safety, economic wellbeing, international reputation, and democracy. Whether an incident is potentially nationally significant can also be determined by the NCSC's understanding of the nature of the malicious actor responsible for the incident.

In 2023/2024, NCSC recorded 343 incidents of potential national significance.

While this figure is 8.5% higher than the previous year's incidents, it is close to the yearly average of 353 recorded by the NCSC in the past five years. The proportion of incidents attributed to suspected state-sponsored actors and criminal or financially motivated actors has also remained relatively consistent over this five-year period.

65

of the 343 incidents were likely criminal or financially motivated (19%).

110

of the 343 incidents that indicated links to suspected state-sponsored actors (32%).

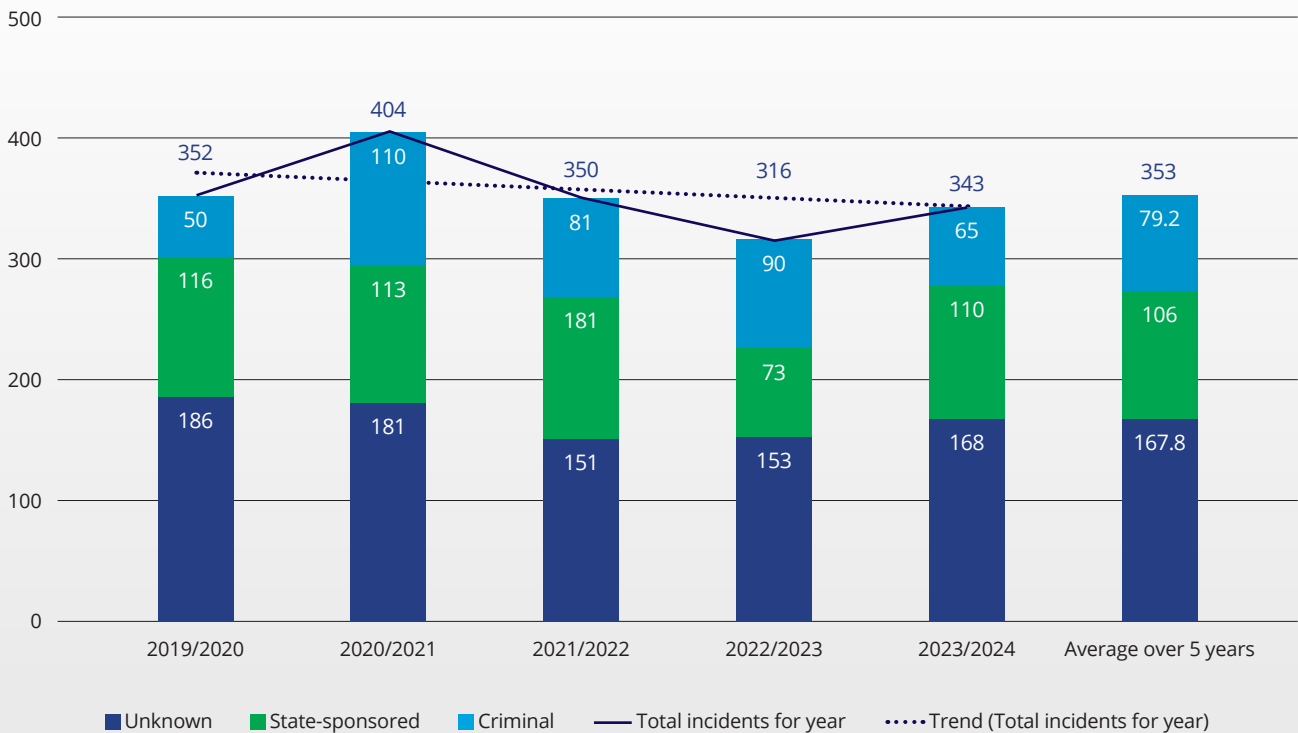
29

Average incidents of potential national significance per month.

861,204

Average MFN disruptions per month.

Incidents of potential national significance for the financial years 2019/20 to 2023/24



In 2023/2024, multiple organisations experienced similar malicious cyber activity around the same time. These incidents significantly increased the volume of total incident figures and were considered likely to be part of the same malicious cyber campaign. The groups of incidents were typically phishing campaigns or mass-exploitation of the same vulnerability. For example, in June 2024 the NCSC recorded six incidents of advanced, multi-stage adversary-in-the-middle (AiTM) phishing attacks targeting the health, education and government sectors. One of these incidents resulted in a breach where malicious actors were able to send 450 further phishing emails to contacts of the breached account. Sending phishing emails from a known individual or organisation can make it more likely for users to trust the email.

This financial year there was also an increase in the number of suspected state-sponsored incidents. An increase in state-sponsored malicious cyber activity is consistent with global experience of an increasingly adversarial cyber threat landscape and escalation in targeting of critical infrastructure. The NCSC assesses it is possible that a proportion of the 49% of unattributed cyber incidents may also have been conducted by state-sponsored actors but owing to technical or other constraints cannot be linked. This proportion is approximately consistent with previous years.

The technical attribution process

The NCSC undertakes a technical attribution process to identify the actors responsible for malicious cyber activity, and the intent behind their actions. This process can inform and direct the NCSC’s own incident response and network defence efforts, as well as the advice the NCSC provides to affected organisations.

Technical attribution can also inform decision and policy makers, enabling them to understand the malicious cyber activity affecting New Zealand, including those responsible for the impacts. This technical attribution process can subsequently enable further response actions, including in the most significant cases using the attribution to contribute to the Government’s decision to publicly ‘call out’ the activity. The NCSC’s contribution to this process ensures that New Zealand has an independent, sovereign technical assessment that supports confidence in calling out malicious activity.

Top 10 sectors affected by incidents of potential national significance



The NCSC categorises organisations into sectors following the Australian and New Zealand Standard Industrial Classification (ANZSIC) divisions from the Australian Bureau of Statistics. The public administration and safety division includes central government agencies, local councils, public order and safety services, and Defence.

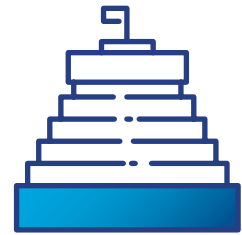
Of the 343 incidents of potential national significance that the NCSC responded to, the 10 sectors affected by malicious cyber activity in 2023/2024 remained consistent with the previous fiscal year. The sector with the highest percentage of recorded cyber security incidents was again public administration and safety. Aotearoa New Zealand government organisations are commonly targeted for their access to sensitive information and data, which is reflected in this year's increase in suspected state-sponsored cyber incidents, alongside the increasing global threat of the

targeting of democratic institutions. Government sectors and regulated critical infrastructure also have reporting obligations, which means there is a higher rate of incidents reported for these sectors compared to others.

Incidents arising from the actions of financially motivated malicious cyber actors predominately involved organisations in the health care, information media and telecommunications sectors. The health care sector is a common target in financially motivated cyber activity, as disruption to critical services is more likely to increase the possibility of a ransom payment. Growing global connectivity and software supply chains also make it more likely that financially motivated ransomware incidents overseas could have indirect downstream effects for New Zealand organisations or critical services.

Case study: networks compromised

In August 2021, the NCSC provided support to the compromise of computer networks associated with New Zealand’s Parliamentary Counsel Office and the Parliamentary Service by malicious cyber actors attributed to the People’s Republic of China (PRC), known as APT40. During the last three years, the PRC has demonstrated ongoing targeting of democratic institutions globally, and the targeting of critical infrastructure networks in the United States.



Following the March 2024 public announcement of the APT40 activity against Parliament, in July 2024 the NCSC joined partners to highlight evolving tactics, techniques and procedures of APT40. The actors had been observed using compromised small-office/home-office (SOHO) devices as operational infrastructure, and exploiting newly public vulnerabilities in applications and devices such as Microsoft Exchange, Atlassian Confluence, and Apache Log4j. Many of these SOHO devices, including in New Zealand, are unpatched or end-of-life devices left vulnerable to exploitation. Once compromised, SOHO devices can be used for attacks whilst blending in with legitimate traffic, subsequently presenting challenges for network defenders. APT40 continues to make use of compromised infrastructure and use available exploits within hours or days of public release.

This joint advisory served to raise awareness of and resilience to the tactics associated with a significant cyber threat to New Zealand and likeminded nations.

To help understand the impact of any one incident, NCSC triages incidents affecting nationally significant organisations into categories, which consider the severity of the compromise and the size of the organisation impacted.

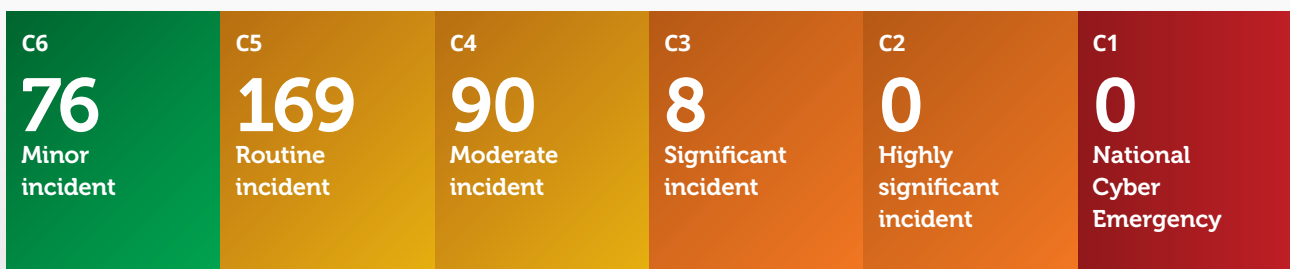
This year’s most severe cyber incidents were categorised C3. These C3 incidents were predominately associated with disruptive ransomware or other extortion activity. Other incident types within this category included the exploitation of public-facing applications and compromised networks or infrastructure. Organisations affected by these C3 incidents were in the education, government, media and telecommunications, transport, and energy sectors.

Another C3 incident included the targeting of a central government organisation by a sophisticated state-sponsored malicious cyber actor. Analysis revealed that a vulnerable perimeter device was exploited to gain initial access to the network. The NCSC assisted the

victim organisation and its managed service provider to understand the scope of the intrusion, remove the intruder, and prevent further attempts to compromise the network. Prompt response efforts and work to identify the full path of the intrusion contained the compromise and reduced its impact.

Moderate (C4) and routine incidents (C5) increased in volume this year, consistent with the overall downward trend in the severity of impact experienced in New Zealand’s cyber incidents of potential national significance. Moreover, several incidents relating to the same vulnerability being exploited could be grouped as the same activity. For instance, in April 2024, the NCSC responded to a series of 10 incidents connected to a then zero-day vulnerability that could allow malicious cyber actors root access to systems using Palo Alto’s PAN-OS software. The NCSC observed attempted use of this vulnerability early and supported organisations’ remediation.

Impact of incidents of potential national significance



The impact of ransomware

Te pānga o ngā pūmanawa tonono utu

This year, Aotearoa New Zealand's reported ransomware incidents declined significantly, despite global trends of ransomware being a pervasive and damaging cyber security threat. Even with a smaller number of incidents, it was still disruptive to those impacted, with ransomware actors incorporating a range of techniques intended to extort ransoms from victims including individuals, organisations, and government agencies.

A year in ransomware incidents

Of the 7122 total incidents recorded during the 2023/2024 financial year, the NCSC responded to 46 ransomware incidents, approximately half the number of incidents compared to 2022/2023. Overall, the total number of ransomware incidents in 2023/2024 dropped considerably from previous years.

While the number of ransomware incidents has declined, the severity of impact from ransomware this year was still proportionally more than other cyber security incidents. In 2023/2024, 5 out of the 8 C3 incidents of potential national significance involved ransomware, or extortion/exfiltration which is often associated with ransomware events.

37 of the 46 ransomware incidents (80%) were not likely to cause nationally significant harm as they impacted smaller organisations or individuals. Ransomware actors likely select smaller enterprises and individuals alongside 'big game' targets, since these victims likely have less-mature cyber security capabilities. Emerging players enabled by ransomware-as-a-service are also capitalising on smaller organisations' vulnerabilities to test their capabilities.

In many ransomware incidents where impact was less severe, this was mainly due to effective cyber security measures, including robust backups, automated cyber threat detection, and timely incident response. This is reflected in the following case studies about four ransomware incidents experienced by Aotearoa New Zealand organisations this year:

- In September 2023, the NCSC was made aware of a ransomware event affecting a New Zealand transport organisation's card service for public transport services. The ransomware affected the system responsible for reconciling account balances with credit card data that facilitates users' ability to top up their accounts. The NCSC provided the transport organisation with support and guidance to assist with the containment of this incident.
- In November 2023, the NCSC was made aware of malicious cyber activity that indicated ransomware on the network of a New Zealand organisation in the media and telecommunications sector. Subsequent investigation supported by the NCSC indicated the intrusion occurred via a vulnerable remote services tool with weak administration credentials. Due to robust backups (which were not affected) the organisation had the ability to restore the impacted file systems and data.
- In March 2024, the NCSC was notified of possible ransomware activity on the network of an organisation in the manufacturing sector. Access was likely via the exploitation of a known vulnerability in a remote service tool. After gaining access to the network, the actor was observed making attempts to copy sensitive credential databases. Early identification of the activity by a cyber threat detection tool on the network allowed the organisation to remediate the server before the ransomware was deployed.



The NCSC recommends never paying cyber ransoms

Governments worldwide are increasingly concerned about appropriate protection of sensitive data, including personal information, and are discouraging the payment of a ransom.

In 2021, the New Zealand Government agreed that government agencies should not pay cyber ransoms.

Paying ransoms encourages illegal activity and may fund other illicit activities. Payment of a ransom could also be in violation of the Russia Sanctions Act 2022 or the United Nations Act 1946.

Payment of ransom does not guarantee that an organisation gets their data or systems back, and can result in the same organisation being targeted again, due to their willingness to pay.

The New Zealand Government encourages all victims to report any cyber ransom incidents to the relevant agencies, regardless of whether a ransom is paid. The Privacy Act 2020 requires reporting of privacy breaches that have caused serious harm or are likely to do so.

For more information see:
ncsc.govt.nz/news/ransomware-advice

Analysing trends in tactics and techniques

Te tātari i ngā ia rauhanga, tikanga hoki

Mapping recorded incidents to the MITRE ATT&CK® framework provides insight into common or emerging trends and can help defenders focus their security efforts. This section provides an overview of the three most used techniques in the 343 incidents of potential national significance. Security leaders should ensure their organisation has a process for managing risks associated with these commonly used techniques.

Malicious cyber actors use a variety of tactics, techniques and procedures (TTPs) to conduct malicious activity. TTPs are the behaviours or methods an actor uses to compromise or conduct activity on a network. Understanding TTPs of malicious actors can inform how organisations best defend their networks. While the NCSC observes a wide variety of TTPs in recorded cyber incidents, malicious actors continue to have success using commonly used techniques that can be prevented.

Initial access – exploiting public-facing applications

The exploitation of public-facing applications, such as websites or webservers, for initial access was the top technique in 2023/2024. It was also the top technique observed within ransomware incidents, but is similarly utilised by malicious cyber actors with a wide range of motivations, including state-sponsored actors. Malicious cyber actors have increasingly been observed leveraging weaknesses, known vulnerabilities or bugs to exploit internet-facing software for initial access into a network. The existence of these vulnerabilities is typically public knowledge, and as a result, there may be several active exploits associated with them.

The exploitation of public-facing applications is typically due to weaknesses or misconfigurations within the underlying code of an internet-facing application or system. Targets usually include websites, databases or network services (such as File Transfer Protocol (FTP) or Secure Shell (SSH)). A frequently recorded technique in 2023/2024 was cyber criminals exploiting public-facing application vulnerabilities through SQL injection and cross-site scripting for manipulating or stealing data from internet-facing applications.

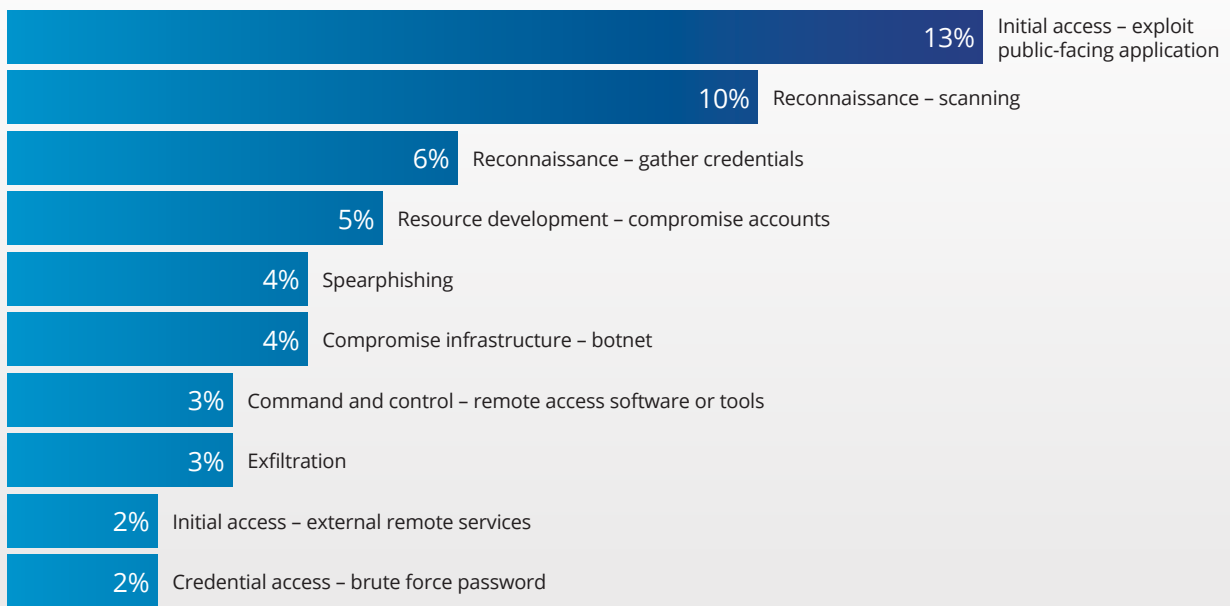
Reconnaissance – scanning

Consistent with past years, vulnerability scanning remains a top-recorded technique, likely enabled by tools facilitating automation. During 2023/2024, vulnerabilities were observed frequently being leveraged for initial access. Publicly accessible vulnerabilities within networking devices and security infrastructure have become some of the most common initial access vectors for malicious cyber actors, including for ransomware.

Reconnaissance – gather credentials

Compromised credentials persist as a key vector for enabling network-wide compromise. During 2023/2024, the NCSC continued to record incidents for identified compromised credentials, consistent with the increase observed in 2022/2023. The NCSC also observed an increase in the use of valid account credentials in both routine and significant incidents in 2023/2024, including cloud user account logins. Adversaries may obtain and abuse the credentials of existing accounts as a means of gaining initial access, maintaining persistence or evading defences. In many cases, gaining initial access through valid accounts is made possible via insecure software development practices. Credentials used in these situations are typically gained either through phishing, when passwords are leaked in credential dumps, or when cyber actors make use of default passwords or attempt brute-forcing.

Most-recorded MITRE ATT&CK techniques used in incidents of potential national significance in 2023/24



High-impact techniques and mitigations

Ngā tikanga me ngā whakamaurutanga pānga nui

In addition to the three most common techniques, through investigations the NCSC has identified a number of other recurring techniques that malicious cyber actors have used effectively in high-impact incidents. A selection of techniques is paired here with steps organisations can take to mitigate the threats. The mitigations that follow below are aligned to the functions of the NCSC Cyber Security Framework.¹ Many of these mitigations are technical, and they are predominately designed to inform the efforts of security practitioners.

Adversary-in-the-middle (AITM) phishing attacks used to bypass security controls like multi-factor authentication (MFA)

During 2023/2024, several attempts at adversary-in-the-middle (AITM) phishing attacks were reported to the NCSC. AITM phishing attacks are an advanced way to steal sensitive credentials and bypass security controls, such as MFA. In AITM phishing attacks, a server is used as a proxy to intercept the network communication between a victim's computer and the real web server. Additionally, the malicious cyber actor creates their own website security certificate to remove encryption from data in secure internet connections, subsequently enabling sensitive information such as credentials and MFA session cookies to be captured. Engaging with a legitimate website through a proxy also ensures that MFA session cookies last longer, giving attackers more time to perform malicious activities.

Managing the threat

- **Prevent and Protect:** Although AITM attacks have been used to bypass some MFA implementations, phishing resistant MFA methods using the Fast Identity Online 2 standard (FIDO2) can be utilised to protect against these attacks. FIDO2 uses a combination of origin checking, token binding, and public key cryptography, preventing attackers from using intercepted authentication and session information.
- **Detect and Contain:** Use endpoint security products that include rules to detect phishing attempts alongside correlation rules from third-party log sources, which may be provided by endpoint security products or security information and event management (SIEM) systems, to identify and disrupt clicked phishing links and related network activity. Some products may include specific AITM monitoring rules, which should be enabled wherever possible.

¹ <https://www.ncsc.govt.nz/resources/ncsc-cyber-security-framework>

Historical common vulnerabilities and exposures (CVEs) used by state and criminal actors

While conscientious organisations may work to address new vulnerabilities, some of the biggest CVE threats have been used for a long time. Historical CVEs, including those from 2019 or earlier, are still frequently seen exploited in New Zealand cyber incidents, even though solutions are known and readily available. These unpatched vulnerabilities are still threats to the security of systems domestically. In many cases, individuals or organisations are not selected as specific targets, but the fact that they rely on a product or service with unaddressed vulnerabilities exposes them to risk.

Managing the threat

- **Guide and Govern:** Maintain clear expectations with technology owners and external support partners regarding patching requirements, through policies, standards, and reporting mechanisms.
- **Identify and Understand:** Systems should be catalogued and regularly scanned to ensure the latest available patches are implemented, with compensating controls applied where assets can't be patched in a timely manner. Reports for patch compliance should be provided regularly.
- **Prevent and Protect:** Patch all systems as soon as possible, following a ringed release model that allows the pause of patch updates in the unlikely event that updates impact service availability.
- **Detect and Contain:** Monitor for indicators of compromise related to high-scoring CVEs. It is not safe to assume that because patches have been installed in a timely manner, that they have not been exploited prior to the installation of a patch.

SQL injection and cross-site scripting used for exploitation of public-facing applications

Several incidents in 2023/2024 where public-facing applications or websites were targeted for exploitation involved the use of SQL injection or cross-site scripting (XSS). The NCSC observed these techniques were being used in instances where the malicious cyber actors attempted or gained unauthorised access to data for subsequent exfiltration. The NCSC has observed both state-sponsored and criminal cyber actors using this technique, including in some of the most damaging ransomware incidents reported to the NCSC. SQL injection is a security vulnerability that targets the underlying database of a web application. It occurs when a malicious cyber actor manipulates the application's database into running malicious SQL queries. XSS is another prevalent server-based web vulnerability that targets the trust a user has in a particular website. In XSS attacks, malicious scripts are injected into web pages that other users subsequently view.

Managing the threat

- **Guide and Govern:** Organisations should provide strong guidance to application developers through secure development training, which incorporates recognised risks and related mitigations, such as the Open Web Application Security Project Top 10 Web Application Security Risks 2021 (OWASP Top 10:2021).
- **Identify and Understand:** Early detection and remediation of application security issues are important steps to minimise the risk of web application compromise. Organisations should conduct threat modelling consistently to understand how injection attacks (including SQL injection and XSS) could impact their applications before they are built.
- **Prevent and Protect:** Implementing application security tools and checks within CI/CD pipelines (a method of automatically testing and delivering new software) is a good way to check for common security issues. Such tools can be configured to fail build tasks where issues are identified, preventing the introduction of potentially risky issues into live, internet-facing systems.

BADCANDY malware implant used to compromise Cisco IOS devices

In February 2024, exploitation of a previously unknown vulnerability in the Web User Interface feature of Cisco IOS software led to 11 of New Zealand's nationally significant organisations experiencing targeted reconnaissance activity. Unauthorised users exploited vulnerabilities in order to maintain and elevate access to victims' systems. Once a local user account was created, a malware implant known as BADCANDY was deployed. This allowed the user to attempt privilege escalation, where modifications grant access to additional roles, permissions or higher-privileged valid accounts.

Managing the threat

- **Guide and Govern:** Organisations should maintain a vulnerability management strategy that encompasses networks, cloud platforms, and locally installed devices. Organisations should also subscribe to vendor notifications for security issues. These alerts highlight security issues, mitigating actions, and notify the availability of security updates to address identified vulnerabilities.
- **Identify and Understand:** Organisations should make use of technology capabilities such as attack surface management to understand their web-facing assets and what the risks of exposure to the internet may be.
- **Prevent and Protect:** Disable HTTP/HTTPS server components of management interfaces and restrict configuration access to trusted locations.
- **Detect and Contain:** Implement processes to monitor network appliances and security gateways for unauthorised changes. Regular revalidation of access requirements, alongside auditing of network device configuration is a good hygiene step, which can be supported by administrative log ingestion by SIEM services.

Cloud storage providers targeted, but not just for data exfiltration

In 2023/2024, the NCSC responded to several incidents in New Zealand associated with possible compromised accounts held by cloud-managed service providers.

The NCSC frequently observes legitimate cloud providers being targeted for data exfiltration. However, the abuse of cloud service providers is frequently a vector for other forms of intrusion. This includes unauthorised access to cloud data gained for the purpose of espionage, cloud infrastructure being used to propagate email spam campaigns, DDoS attacks to disrupt legitimate users from accessing IT resources, and the hosting of malicious content such as bots and phishing pages. Hosting of malicious content on the cloud is difficult to block, as malicious cyber actors are able to hide in legitimate content from trusted cloud brands.

Managing the threat

- **Guide and Govern:** Organisations should emphasise training requirements around security best practices and identifying phishing attempts.
- **Identify and Understand:** Cloud security posture management (CPSM) capabilities continuously check cloud settings and configurations to find risks and misconfigurations. Ensure that all cloud storage platforms are integrated with CPSM solutions, and that recommendations from such tools are acted on in a timely manner.
- **Prevent and Protect:** Organisations should consider adoption of cloud services following a zero trust architectural approach, which requires continuous evaluation and enforcement of policies, prior to granting access. Following principles of least-privilege, which restrict users and services to only the resources required for their role, can minimise the impact of a malicious user gaining access to services through phishing or exploitation of other vulnerabilities. Implementing access policies that require a number of sign-in conditions to be satisfied before access is granted may be an effective way to prevent many attacks from occurring.
- **Detect and Contain:** If a successful account compromise is detected, revoke active sessions, reset MFA registration and user account passwords, and isolate end-user compute devices where suspicious activity is occurring from (if this is within the control of the organisation).

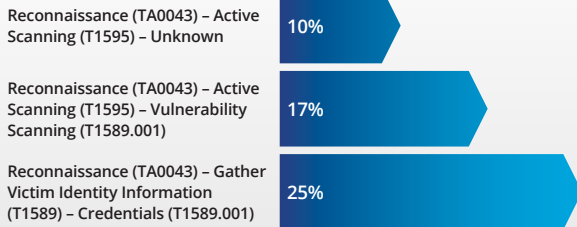
Most-recorded MITRE ATT&CK techniques within each tactic recorded by the NCSC in 2023/24

For each of the 343 incidents of potential national significance in 2023/24, the NCSC analysed the tactics and techniques used at the various stages of the exploitation lifecycle. The chart below displays the top 3 techniques used at each stage of the lifecycle, known in MITRE ATT&CK as Tactics. For example, the exploitation of a public-facing application was the technique used during the initial access stage in 54% of incidents.

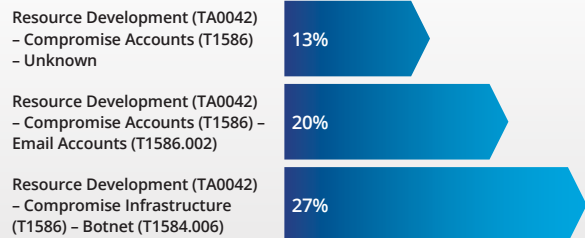
A common observation is that across the MITRE categories, many organisations remain vulnerable to the same activity. Accordingly, malicious cyber actors with intent and capability may be successful in their compromise of many organisations across multiple sectors. The benefit of this trend is that mitigation techniques remain applicable to a broad range of organisations.

Security practitioners can use this information to identify whether they have the ability to detect and respond to these techniques.

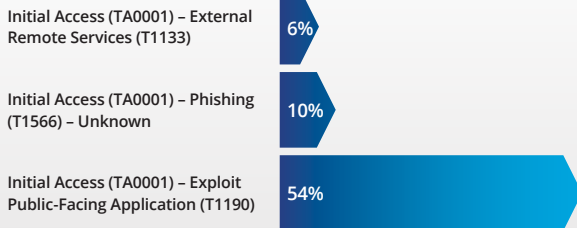
Reconnaissance



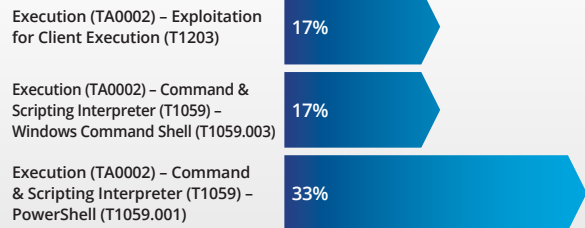
Resource Development



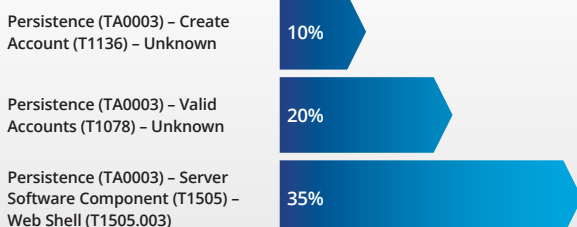
Initial Access



Execution



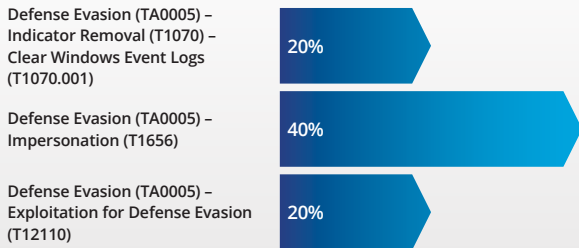
Persistence



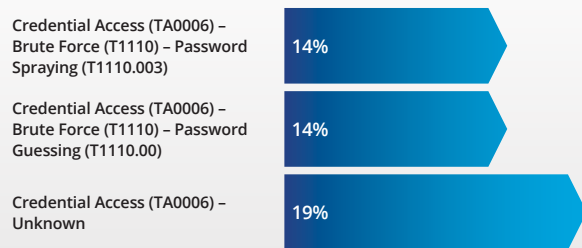
Privilege Escalation



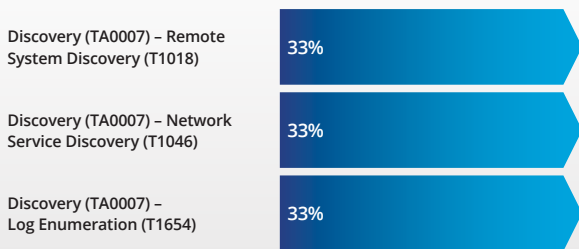
Defense Evasion



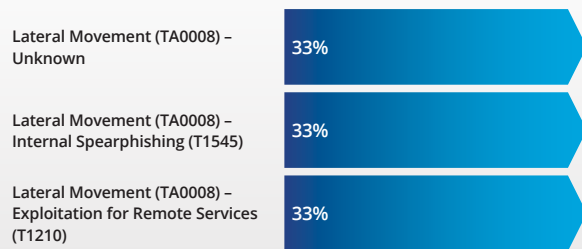
Credential Access



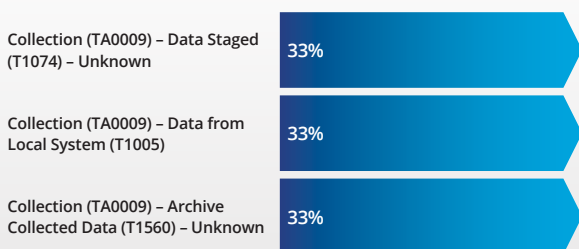
Discovery



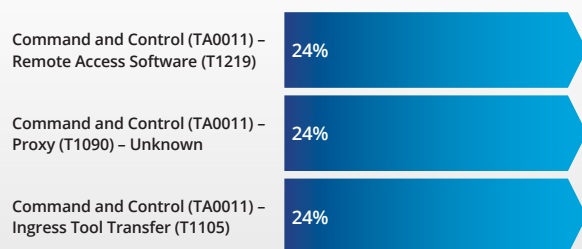
Lateral Movement



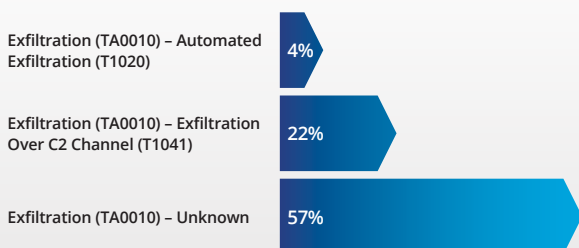
Collection



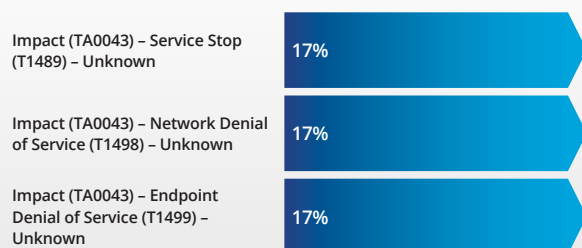
Command and Control



Exfiltration



Impact



Loss and harm

Ngā ngaronga me te tūkinotanga

The total impact of cyber security threats is difficult to quantify. This year the NCSC prevented loss of an estimated \$38.8 million while also receiving reports of \$21.6 million of direct loss. Due to under-reporting of cyber incidents, the NCSC recognises this is only a small proportion of the overall harm.

Harm prevention through response to incidents of potential national significance

In 2023/2024, the detection, disruption and threat intelligence services the NCSC provides prevented an estimated \$38.8 million of harm to Aotearoa New Zealand's nationally significant organisations. 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 \$421 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.

There are a number of potential factors affecting the difference in the value of estimated harm prevention compared with 2022/2023's \$65.4 million figure. In 23/24, the NCSC recorded fewer significant incidents. Equally, many organisations were able to respond to incidents with less intervention from the NCSC. Another potential contributing factor is the year-to-year variations in victim organisations, and the differing criticality of their roles and services.

Direct financial loss reported through incidents handled through general triage process

The NCSC records the direct financial loss reported by victims, whether lost to scams or the cost of recovery (including IT contractors). Across the 6779 incidents handled through NCSC's general triage process, the direct financial loss reported in 2023/2024 totalled \$21.6 million, decreasing from \$22.4 million in 2022/2023.

Of the incidents reporting a loss value, 63% were below \$500. Of the 40 incidents involving losses of \$100,000 or more, 17 related to a scam concerning an offer of a job, business or investment opportunity, 8 related to cryptocurrency scams, 4 related to dating or romance scams, 4 related to unauthorised access, 3 related to buying, selling, or donating goods online, 1 related to denial-of-service, and 1 related to inheritance scams.

Although the number of incidents handled through the NCSC's general triage process in 2023/2024 decreased by 12.5%, the total direct financial loss across all incidents was comparable to 2022/2023. This meant that the average direct financial loss per incident increased significantly, from \$14,000 to \$25,500. In 2023/2024, individuals reported a total direct financial loss of \$20.1 million, compared to organisations reporting a total of \$1.2 million.

Another trend was an 81% increase in the total financial loss reported for incidents where there was unauthorised access to systems and/or network – an increase from \$2.7 million to \$4.9 million. The total loss from investment scams increased from \$1.6 million in 2022/2023 to a total of \$4 million in 2023/2024. In demographic terms, the total amount of financial loss reported in the age 65+ band doubled from \$2 million in 2022/2023 to \$4 million in 2023/2024.

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

- 1674 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.
- 245 data loss incidents: loss or unauthorised copying of data, business records, and intellectual property.
- 66 reputational loss incidents: damage to the reputation of an individual or organisation as a result of the incident.
- 42 operational impact incidents: the time, staff and resources spent on recovering from an incident, taking people away from normal business operations.
- 11 technical damage incidents: impacts on services like email, phone systems or websites, resulting in disruption to a business or organisation.
- 62 other loss incidents: includes types of loss not covered in other categories.

International threat landscape

Te āhuatanga i te ao

As malicious cyber activity takes little notice of borders, international trends are usually reflected at the domestic level, whether directly or indirectly. Geopolitical tensions, conflict and an economic downturn have resulted in a more adversarial global cyber environment. Collaboration and enablers within the cyber ecosystem continue to swell the resources of malicious cyber actors. The scale of malicious cyber activity has escalated, and disruptive cyber activity has been felt worldwide.

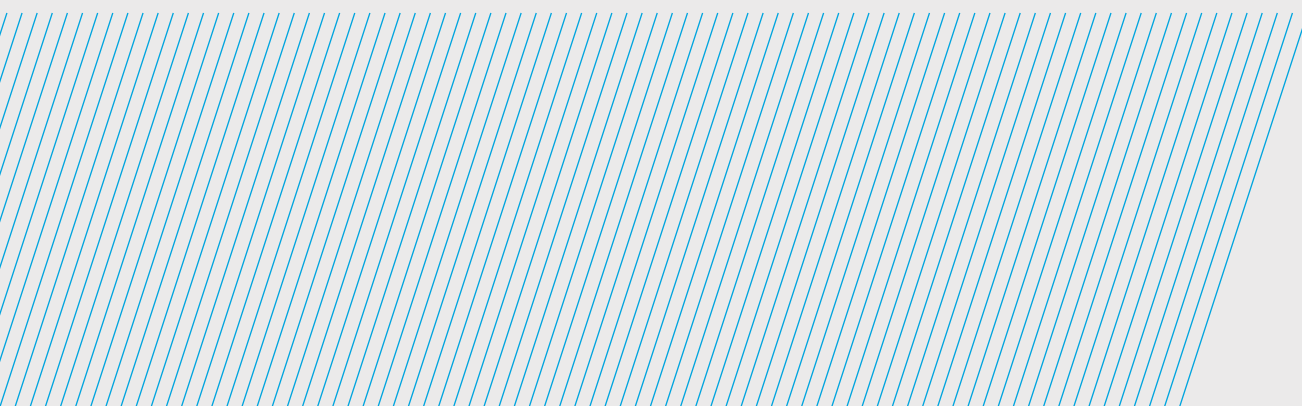
Global tensions intensify the cyber environment

Heightened tensions within the international landscape have driven cyber threat actors to break further away from rules-based international systems. State-sponsored cyber actors are increasingly demonstrating a disregard for the norms of responsible state behaviour online. The number of malicious cyber actors aspiring to target systems supporting Western critical infrastructure is also increasing. It is possible that disruptive malicious cyber activity linked to conflict could escalate and impact Aotearoa New Zealand.

Ongoing global tensions, including Russia's invasion of Ukraine, have almost certainly generated a significant amount of targeted intrusion and hacktivist cyber activity globally in 2023/2024, including against New Zealand organisations. Likely emboldened by the invasion, Russia-aligned cyber actors have continued targeting Russia's neighbours and New Zealand's like-minded partners. While not to the extent many expected, malicious cyber activity in support of Russia and Ukraine has persisted into 2024.

Attempts to undermine the integrity of democratic institutions was a rising trend in this financial year's international cyber landscape. In December 2023, the Minister Responsible for the GCSB, on behalf of the New Zealand Government, publicly condemned malicious cyber activity affecting the United Kingdom's domestic democratic institutions and processes, including civil society organisations. This activity was attributed to Russia's Federal Security Service (FSB).

In March 2024, New Zealand's Government again joined with the UK in its condemnation of People's Republic of China (PRC) state-backed malicious cyber activity impacting the UK's Electoral Commission and targeting UK Members of Parliament. As part of this announcement, the NCSC publicly shared its attribution of a PRC state-sponsored compromise of New Zealand's Parliamentary Counsel Office and Parliamentary Service in 2021. The NCSC remains concerned that challenges to democracy may become more common in cyberspace.



Living-off-the-land tradecraft

Malicious actors continue to use living-off-the-land (LOTL) tradecraft for avoiding detection and maintaining persistence on networks. This technique is used by both state and non-state actors, though it is likely favoured by state-sponsored actors who are attempting to maintain access for espionage and data exfiltration over long periods of time.

Living-off-the-land is a technique in which actors use legitimate or pre-existing software on a victim network to maintain access. Use of legitimate software and accounts is less likely to raise alerts for defenders. This is in contrast 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.

In the financial year, the NCSC joined international partners in publishing two joint guidance advisories. The first of these reports provided information on common LOTL techniques and gaps in cyber defence capabilities. It also provided guidance for network defenders to mitigate identified gaps and to detect and hunt for LOTL activity.

The second advisory detailed the risks and indicators of PRC actors on systems of critical infrastructure. It urged critical infrastructure organisations to apply the recommended mitigations and hunt for similar malicious activity using the guidance within the advisory to reduce the risk and impact of compromise.

Cloud service exploitation

Targeting of cloud services has been a persistent feature of the international landscape in 2023/2024. The growing reliance on the cloud is bringing new security challenges to an already complex problem. While understanding and confidence in implementing cloud services has improved, so has the sophistication of cyber threat actors taking advantage of cloud complexity for malicious activity. Malicious cyber actors likely target these services for extracting large volumes of data quickly and undetected.

In June 2023, a wave of cyber incidents targeting cloud-based data storage supplier Snowflake affected over 100 customers. This breach was not caused through a vulnerability, misconfiguration, or a breach of its systems. Instead, initial access was gained using stolen credentials that were obtained through multiple malware infections.

Cyber criminals are increasingly targeting the providers of managed information and communications technology (ICT) infrastructure suppliers to widen their impact and extort payment. State-sponsored cyber actors have similarly compromised major international infrastructure and software-as-a-service providers for espionage. In 2024, the US Cyber Security Review Board published its findings on the compromise of several Microsoft Exchange-hosted government email accounts compromised by PRC-linked cyber actors.

Additionally, the targeting of cloud-service providers for disruptive activity can also be ideologically motivated. In June 2023, a series of distributed denial-of-service (DDoS) attacks against Microsoft led to disruptions across multiple services. The cyber attacks were linked to a pro-Russia hacktivist group likely using multiple virtual private servers, alongside rented cloud infrastructure, open proxies and DDoS tools.

Collaboration in the cybercrime ecosystem

The success rates of financially motivated malicious cyber actors in 2023/2024 were likely enabled through collaborative relationships in the cybercrime ecosystem. Malicious cyber actors' resources have grown as a result of access to crime-as-a-service models and connection to an ecosystem of cyber enablers. It is likely both state-sponsored and criminal cyber actors will continue forging ties with enablers such as access brokers to reduce overheads for their cyber operations.

Russian-language criminals operating ransomware or ransomware-as-a service (RaaS) play a pivotal role in the cybercrime ecosystem. These syndicates continue to be responsible for the most impactful cyber incidents responded to by the NCSC. Several of these syndicates have links to the Russian state and are likely emboldened by its tacit tolerance of their malicious activities.

During the 2023/2024 financial year, global law enforcement cybercrime disruption efforts impacted dominant ransomware groups. Despite these disruption efforts likely leading to a dent in ransomware activity, it is almost certain that groups will reorganise and diversify, enabling them to bounce back. Effective and long-term disruption of the cyber criminal ecosystem will require sustained collaboration between government, law enforcement, and industry. This should focus on disruptive efforts, including infrastructure takedowns, seizure of illicit proceeds, arrest of cyber criminals and cryptocurrency regulation.

Use of artificial intelligence for malicious cyber activity

The increasing accessibility and proliferation of AI technologies lowers the barrier for some criminals to commit malicious cyber activity at a scale and level of sophistication previously outside their capabilities. At present, the use of AI mainly amplifies existing risks from cyber-dependant and cyber-enabled crime, rather than creating new ones.

Along with the general population, many criminals use AI primarily when it is embedded in easily accessible services. The frequency and sophistication of fraud will likely increase with developments in AI applications such as voice cloning, and data harvesting and impersonation. Large language models are likewise being used in a range of ways including writing credible phishing messages and writing code for creating information-stealer malware to obtain victims' personal details for use in fraud. Equally, the large-scale data processing abilities of AI will be progressively exploited by criminals to identify and profile victims as it is used for the consolidation of images and data.

Commoditisation of identity

Online, identities are increasingly commoditised to facilitate data exfiltration, and the sophistication of identity-related attacks is rising. The advent of smartphones and use of internet of things (IoT) technologies have increased the surface of the threat environment.



Cyber criminals can obtain digital images, voice feeds and confidential information about people with ease for use in social engineering. With the growth of social media, identity theft is rife. Personal information, including that concerning jobs, hobbies, and friends, saturates the digital environment and is visible to everyone. Collection of this information is consequently able to be conducted with anonymity, and collected data can be used for phishing, scams, or even deepfake deceptions.

A new generation of cyber threat actors

Some cyber criminal syndicates are no longer hesitant to target individuals or organisations where there may be retribution, or where cyber attacks were perceived by some as unethical, for example against hospitals. Victim harassment, including threat to life, is also being increasingly leveraged against employees of organisations to exert pressure to release payment.

This new generation of cyber threat actors is challenging these accepted rules in pursuit of profits, regardless of potential risk to innocent lives or possible consequences from attacking critical infrastructure. Combined with this less-restricted approach to victim selection, these actors regularly alter the type of cyber criminal activity they conduct. This makes their behaviour unpredictable and therefore more difficult to respond to.

Conclusion

Whakakapi

In 2023/24, cyber incidents impacted all parts of Aotearoa New Zealand's economy and society. For individual New Zealanders, these incidents have the potential to cause significant harm. Common attacks take millions of dollars from New Zealanders every year, in addition to the emotional toll they inflict on their victims. For New Zealand organisations, the impact of cyber incidents can range from temporary inconvenience through to significant disruption of critical public services. Organisations that experience cyber incidents can lose important data or the use of systems, sometimes irretrievably, as well as experiencing diminished public or customer trust.

Good cyber security practices are a responsibility for all New Zealanders, as cyber security challenges are increasingly interconnected. Individuals, small-to-medium enterprises, the public sector, and critical national infrastructure are all potential targets of malicious cyber activity, as are their supply chains, and the impact can be felt beyond the original target.

Sophisticated cyber actors have continued to demonstrate the intent and capability to target Aotearoa New Zealand. A wider range of state-sponsored malicious cyber activity, and increased activity from some traditional cyber adversaries, was observed this year.

Advanced cyber tools and techniques are more readily available to malicious actors than ever before, lowering barriers to entry and making it easier for them to work at scale and cause serious harm. Rapid developments in enabling technologies such as artificial intelligence are also helping attackers to identify and exploit vulnerabilities more quickly and efficiently than ever.

Despite this growing sophistication, however, common techniques continue to be used by threat actors across Aotearoa New Zealand's domestic cyber threat landscape. This means there are also well-known cyber security controls that could prevent these incidents from occurring.

The NCSC encourages readers to familiarise themselves with the techniques described in this report, and, most importantly, take action.

The NCSC's work to improve the nation's cyber resilience continues, but it cannot do this alone. The majority of the country's cyber security capabilities exist outside of government, so everyone must take a proactive approach to protecting their data and infrastructure, and, where relevant, their customers.

Getting in touch with the NCSC

Te whakapā atu ki te NCSC

For general enquiries please email: info@ncsc.govt.nz

To read the latest NCSC news, updates and the resources and guides mentioned in this report, visit our website and follow us on LinkedIn:

— <https://www.ncsc.govt.nz>

— <https://nz.linkedin.com/company/ncsc-nz>

Individuals and small businesses looking for simple, straightforward cyber security advice are encouraged to visit the NCSC's Own Your Online website: <http://www.ownyouronline.govt.nz>

If your organisation of national significance requires assistance, you can complete the NCSC's Cyber Security Incident Request for Assistance form: <https://www.ncsc.govt.nz/incidents>

You can speak with us directly by calling (04) 498 7654. You can also contact us via email at: ncscincidents@ncsc.govt.nz

Individuals and small to medium organisations can report a cyber security incident on the CERT NZ website: <https://www.cert.govt.nz/report>

Glossary

Rarangī kupu

TERM / KUPU

DEFINITION / WHAKAMĀRAMATANGA

**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.

**Botnet /
Whatunga Pūwerewere**

Normally 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.

**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 /
Whakahaumarū ā ipurangi**

Measures to protect systems, data, and devices from unauthorised access, and ensuring the confidentiality, integrity, and availability of information.

**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 avoid network defenders 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.

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.

**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.

TERM / KUPU	DEFINITION / WHAKAMĀRAMATANGA
Hypervisor / Kaiwhakahaere pūrere mariko	Software enabling the creation, management, and running of discretely hosted virtual machines (VMs) on the same hardware.
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.
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.
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.
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.
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.
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.
Ransomware / Pūmanawa utu uruhi	A type of malware designed to disrupt the use of computer systems and files until a ransom is paid.
Supply chain compromise / Poke ara ratonga	A form of attack that targets software, hardware, or an IT service provider, where the ultimate aim is exploit downstream customers.
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.
Virtual private server (VPS) / Tūmau tūmataiti mariko	A portion of a large physical server divided into virtual spaces available for temporary use.
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



**National Cyber
Security Centre**