(NCSC, 2023: 2)

Cyber Threat Report 2022/2023

National Cyber Security Centre

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

Te Tira Tiaki
Government Communications Security Bureau

5th

BY THE NUMBERS

Mā ngā tau

316

incidents affecting nationally significant organisations

(COMPARED TO 350 INCIDENTS RECORDED IN 2021/2022)

73

of those, or 23%, indicated links to suspected state-sponsored actors

(COMPARED TO 34% IN 2021/2022)

THE NCSC IN A TYPICAL MONTH*

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

Receives 20 new incident reports or requests for assistance. Of the new incident reports received each month, 12 come from international and domestic partners while 8 come from victim organisations self-reporting.

$382m

Since June 2016, the NCSC has prevented an estimated $382.4 million worth of harm to Aotearoa New Zealand's nationally significant organisations. $65.4 million worth of harm prevented in 2022/2023.

THE NCSC INCREASED AOTEAROA NEW ZEALAND'S COLLECTIVE CYBER RESILIENCE

Delivered **79** incident reports to customers

Published **7** advisories for customers, including 5 co-authored with domestic or international partners

Triaged **105** common vulnerabilities and exposures (CVEs), leading to 20 critical vulnerability alerts

Co-chaired **22** sector-based Security Information Exchanges

90

incidents, or 28%, were likely criminal or financially motivated

(COMPARED TO 23% IN 2021/2022)

250,000

In 2022/2023, the NCSC disrupted over 250,000 malicious cyber events as part of Malware Free Networks.®

IN THE 2022/2023 YEAR THE NCSC AND GCSB

Received 159 notifications of network change proposals under the Telecommunications (Interception Capability and Security) Act 2013 (TICSA).

Conducted 20 assessments of regulated space activities under the Outer Space and High-altitude Activities Act 2017 (OSHAA). Conducted 45 assessments of regulated radio spectrum activities under the Radiocommunications Act 1989.

Conducted 42 assessments under the Overseas Investment Amendment Act 2021 (OIAA).

* These numbers represent the incidents that meet the threshold for an NCSC response. Our focus is on incidents with a possible high national impact, or incidents that may affect Aotearoa New Zealand's nationally significant organisations. For incident reports that do not meet the threshold for an NCSC response, the NCSC engages with other domestic partners better placed to support the victim organisation.

OVERVIEW

Tirohanga whānui

The 2022/2023 Cyber Threat Report provides the NCSC's perspective on domestic and international cyber threat landscapes for the year beginning 1 July 2022 and ending 30 June 2023 (the fiscal year). The NCSC's understanding of the Aotearoa New Zealand cyber threat landscape is shaped by its focus on significant cyber threats leading to possible national-level harms, together with its unique capabilities and partnerships.

The 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 sophistication required to cause national-level harm. It is likely more politically or ideologically motivated groups and individuals have access to the cyber tools they require to cause real-world impacts, and they are further galvanised by domestic and global events. The effects of Russia's invasion of Ukraine in February 2022 continue to be felt in cyberspace, too. While the direct cyber threat to Aotearoa New Zealand has not changed as a result of the invasion, the number and frequency of destructive or disruptive malicious cyber incidents globally has likely increased.

The first section of this report provides the NCSC's view of cyber threats affecting Aotearoa New Zealand. Based on our observations of the domestic cyber threat landscape, the report also provides advice on the steps organisations can take to mitigate the most significant threats seen this year. We work every day to protect Aotearoa New Zealand's prosperity and security through the provision of trusted cyber security services. However, all organisations play a part in protecting New Zealanders' privacy and security by adopting good cyber security practices.

Some of the key themes we explore include the continued effects of cyber criminal activity and extortion. We see ransomware imposing significant costs and requiring substantial recovery efforts. We increasingly see malicious cyber activity with downstream impacts, as Aotearoa New Zealand's digital supply chain is only growing in depth and interconnectedness. Phishing and other forms of social engineering are ubiquitous and effective. However, new techniques and emerging technology such as generative AI will almost certainly enable more convincing and targeted lures, potentially leading to a heightened pace of compromise.

> "We increasingly see malicious cyber activity with downstream impacts, as Aotearoa New Zealand's digital supply chain is only growing in depth and interconnectedness."

During the 2022/2023 year, the NCSC contributed to several cyber security advisories, publicly identifying sophisticated malicious cyber activity and providing steps to detect and mitigate its impact.

In May 2023, we joined international cyber security partners in disclosing technical information about malicious software (malware) associated with Russia's Federal Security Service (FSB). In the same month, the NCSC joined its like-minded partners to identify techniques associated with the stealthy compromise of critical infrastructure. By 'living off the land', sophisticated cyber actors from the People's Republic of China (PRC) were able to use legitimate tools existing on victim networks to maintain access to significant targets overseas, without detection.