National Cyber Security Centre

Unclassified

Cyber Threat Report

2016
2017

The National Cyber Security Centre is hosted within the Government Communications Security Bureau

GOVERNMENT COMMUNICATIONS SECURITY BUREAU
TE TIRA TIAKI

newzealand.govt.nz

Contents

Foreword

The National Cyber Security Centre (NCSC) helps protect New Zealand's most important information systems from advanced cyber threats and responds to cyber incidents that have a high impact on New Zealand. This report aims to provide insight into the types of cyber threats and incidents encountered by these systems.

The National Cyber Security Centre passed a major milestone this year. In June 2017, after three years of intensive development, the NCSC completed delivery of new advanced cyber defensive (CORTEX) capabilities and services to a range of New Zealand's nationally significant organisations.

Deploying the NCSC's capabilities to consenting organisations has taken considerable resource and effort. However, as this report will outline, the variety and seriousness of cyber threats from state-sponsored and other malicious actors continues to evolve and the NCSC will continue to adapt to meet them.

In the reporting year from 1 July 2016 to 30 June 2017, the NCSC recorded 396 incidents. Due to the NCSC's focus, this is only a small percentage of the total incidents affecting New Zealand.[1]

A numerical rise from the 2015/16 year reflects the evolving threat landscape, our broadening customer base and our growing capacity of the NCSC to detect, triage and respond to incidents. As our capacity increases, we gain a more accurate picture of the cyber threats facing New Zealand organisations. Some of these are described in more detail in this report.

It is a difficult task to analyse the impact of an incident had it not been detected. However an independent 'cost avoidance' model developed at the NCSC's request estimated that NCSC's advanced cyber defensive (CORTEX) capabilities resulted in a benefit dividend to a subset of nationally significant organisations of nearly NZD$40m in the 12 months to 30 June 2017.

Our activity relies on the consent and cooperation of our customers and the public. For this reason, it is important that we are as transparent as possible and people understand our cyber protection mandate and functions. We hope this report will promote informed discussion of cyber security and contribute to increased resilience across the broad range of New Zealand's networks and systems.

Lisa Fong

Director, National Cyber Security Centre

THE NATIONAL CYBER SECURITY CENTRE

The NCSC is an operational branch of the Government Communications Security Bureau (GCSB) that provides a range of advanced malware detection and disruption services to consenting nationally significant organisations. It also produces threat prevention and mitigation advice, provides incident response capabilities and acts as a point of contact for organisations who are victims of cyber incidents.

1 https://www.cert.govt.nz/it-specialists/quarterly-report/

About the National Cyber Security Centre

The role of the NCSC is to protect the security and integrity of communications and information infrastructures of importance to the Government of New Zealand.

The NCSC provides specialist information security services, advice and support to assist nationally significant organisations. These organisations include government departments, key economic generators, niche exporters, research institutes and operators of critical infrastructure.

An incident at a nationally significant organisation is likely to have a wider impact on the functioning or administration of a key government or economic sector. The threats to these organisations include espionage, theft of intellectual property, damage to IT systems or the disruption of their operations. Such events have the potential to impact the administration of government and the security and prosperity of New Zealanders.

Our focus is on protecting organisations from the type of cyber threat that they, or the commercial security tools they use, are not specifically designed to meet. We also assist with the response to cyber incidents where there is the potential for those incidents to impact on nationally significant organisations or sectors. As a part of the New Zealand Government, we have the resources and mandate to perform activity for the benefit of the whole of New Zealand on a non-commercial basis.

Cyber defence

As part of our cyber security function we work across government and the private sector to implement cyber defence capabilities (developed through our CORTEX initiative) to protect a range of nationally significant organisations from advanced cyber threats.

CORTEX capabilities focus on countering complex and persistent foreign-sourced malware. They use threat information from a range of sources, including our Five Eyes partners, to detect and disrupt this malware.

Operation of these capabilities helps protect against theft of intellectual property, loss of customer data, destruction or dissemination of private communications, holding data for 'ransom' and damage to IT networks and services.

The capabilities operate with the explicit consent of the organisations that are protected, and are subject to independent oversight from the Inspector-General of Intelligence and Security.

While we provide some services directly to nationally significant organisations, the NCSC also engages more broadly with organisations representing key sector and industry groups. This interaction ranges from incident response to information sharing. It includes coordination of a number of sector-based security information exchanges and regional meetings where information security professionals are able to meet and confidentially share information. This wider group also receives cyber threat alerts and advisories produced by the NCSC.

What was the impact of our work?

To help quantify the economic benefits of our advanced cyber threat detection and disruption (CORTEX) capabilities and services, NCSC commissioned an independent evaluation of the potential impact of advanced cyber harm on New Zealand's nationally significant organisations. The resulting analysis indicated the potential cost of these harms - should the full range of organisations be subject to advanced cyber threats - to be in the order of $640m annually.

The analysis also provided a mechanism for assessing the cost avoided by NCSC's cyber defensive capabilities preventing advanced cyber threats from causing harm. Application of this 'cost avoidance' model to threats detected or mitigated through the operation of NCSC's capabilities - operating on a small subset of our nationally significant organisations - (and before CORTEX capabilities were fully deployed) resulted in a conservatively estimated "gross reduced harm benefit" of $39.47m to New Zealand.

TOTAL POTENTIAL HARM

$640m

ANNUALLY

CORTEX REDUCED HARM BENEFIT 2016/17

$39.47m

ESTABLISHING THE BENEFITS OF CYBER DEFENSIVE CAPABILITIES

NCSC commissioned independent research to establish the benefits to nationally significant organisations of its advanced cyber defensive (CORTEX) capabilities in disrupting and preventing cyber harm.

The research focussed on a specific part of the advanced cyber threat problem, namely the impacts of advanced, mostly foreign-sourced, often state-sponsored cyber threats targeting the information assets of nationally significant organisations.

The threats in scope were of the type the organisations receiving cyber threat detection and disruption protection were unlikely to be able to stop or detect themselves using commercially available tools. The intrusions or compromises had to have the potential to cause considerable harm to the integrity and availability of systems or the functioning and viability of the affected organisation, and be highly targeted, as opposed to a random attack.

The types of harm considered were theft of intellectual property, copyright and patent infringement and espionage.

The research sourced respected international studies, took the average cost of cyber harm expressed in those reports, translated that figure into New Zealand equivalents and scaled it to the number of organisations of potential interest. The complexity of events was also factored in. This was supported by additional New Zealand research and sample interviews.

CYBER SECURITY BY CONSENT

The new Intelligence and Security Act 2017 (ISA), which came into effect in September, changes the authorising regime that enables GCSB's information assurance and cyber security activities provided through the NCSC.

Under the previous legal framework, these services were provided under warrant, authorised by Ministers and the Commissioner for Security Warrants, and with the consent of the organisations receiving the services.

The NCSC works with organisations with their willing participation. Recognising this, the new legislation does not require warrants for all activities. The NCSC is directly empowered to provide immediate assistance to organisations who have consented to receiving it, without the additional requirement of a warrant. This facilitates more effective response to potentially significant cyber events.

What we do

NCSC deals with advanced cyber threats that have the potential to affect New Zealand's national security or the economy:

We supply advanced cyber threat detection and disruption (CORTEX) capabilities and services to organisations of national significance.

We coordinate and respond to high-impact cyber incidents and provide advice on mitigation and prevention. We may get involved in other incidents if required.

Our cyber threat analysis is shared with our customers and partners through a range of fora including sector based security information exchanges and a NCSC customer portal.

We foster a mature security culture based on standards set out in the Government's Protective Security Requirements and the New Zealand Information Security Manual.

Customers - the most important partner

The NCSC's most important partnership is with the nationally significant organisation it endeavours to protect. Not only does the NCSC require their consent to provide services, but the measures they implement themselves are equally as important.

Nationally significant organisations are primarily responsible for their own security. Implementing key strategies can protect organisations from up to 85 percent of cyber threats. The NCSC encourages organisations to work towards implementation of these principles and actively works with organisations to provide advice that will enable this.[2]

Who else do we work with?

Most advanced cyber threats originate from outside New Zealand. To respond to these trans-national threats effectively, the NCSC must work with other agencies both internationally and in New Zealand.

Domestically, the NCSC works in close cooperation with other agencies, including NZ Police, NZSIS and the CERT NZ,[3] to protect New Zealand from advanced cyber threats and to help increase the overall resilience of New Zealand's networks and systems.

The NCSC takes the lead in response to potentially significant cyber events, particularly where those events may impact on national security or the availability and integrity of our nationally significant systems and information. CERT NZ has a primary responsibility for cyber threat reporting and a coordination role in threat response. NCSC's relationship with CERT NZ ensures a wider coverage and awareness of the victims of cyber security incidents in New Zealand and enables a "no wrong door" approach to cyber incident reporting.

To build our understanding of cyber threats and cyber adversaries, the NCSC works closely with other cyber security agencies including the Australian Cyber Security Centre, the United Kingdom's National Cyber Security Centre, Canada's Communications Security Establishment and the United States of America's National Security Agency. The NCSC maintains relationships with other international partners, including the global CERT community, which also shares information regarding cyber threats.

These relationships enable the NCSC to provide greater protection to New Zealand entities from a broad range of cyber threats.

2 https://www.asd.gov.au/publications/protect/essential-eight-maturity-model.htm

3 CERT NZ https://www.cert.govt.nz/

The cyber threat landscape

Why do we face cyber threats?

New Zealand is deeply integrated in the global digital economy and internet society. New Zealanders continue to realise the unique and transformational opportunities of cyberspace in new and fascinating ways. Our internationally focused and market driven economy and open and diverse social environment make New Zealand a perfect place to leverage the benefits of cyberspace.

The connectivity and speed of the Internet has brought New Zealand closer to international customers, but it has also brought us closer to the global domain of malicious cyber actors. The trend towards greater adoption and expansion of digital services creates more targets, while the ability to purchase cyber threat capabilities enables greater numbers of actors, with a lower level of technical skill, to threaten systems and create cyber harm.

The interests and activities of a range of actors in cyberspace, both state and non-state, threaten to degrade the cyber security of New Zealand. These threats come in many forms, continually evolving and adapting to new technology or security measures. Their motivation is similarly varied, from economic gain to other commercial goals through to espionage or other political objectives.

New Zealand faces both direct and indirect cyber threats. Direct threats deliberately target New Zealand, such as cyber espionage aimed at government departments or the theft of intellectual property from a New Zealand company. Indirect threats include, for example, indiscriminate cyber operations by irresponsible or low skilled cyber actors that do not target New Zealand but can harm us nonetheless.

Cyber security is now an important part of ensuring New Zealanders continue to enjoy the prosperity and well-being cyberspace has enabled. Maintaining the integrity, availability and confidentiality of information in the networks and systems that make up cyberspace is vital to modern life.

WHAT IS A "CYBER THREAT"?

When the NCSC describes a cyber threat or an advanced cyber threat, it is referring to threats that occur within cyberspace.

Cyberspace is defined in the *2015 New Zealand Cyber Security Strategy* as the global network of interdependent information technology infrastructures, telecommunication networks and computer processing systems in which online communication takes place. These usually require a vulnerability in a system or network that can be exploited to enable an adversary to affect the availability, confidentiality or integrity of information. The harm itself may be felt outside of cyberspace, such as financial loss, but the capability used to produce the harm must be produced using a system or network.

For example, malware is a cyber threat because it exploits a vulnerability in a computer system and has the potential to affect the availability, confidentiality or integrity of information. A digger cutting through a fibre optic cable would not be described as a cyber threat because, although it may impact the availability of information, it was not caused in cyberspace.

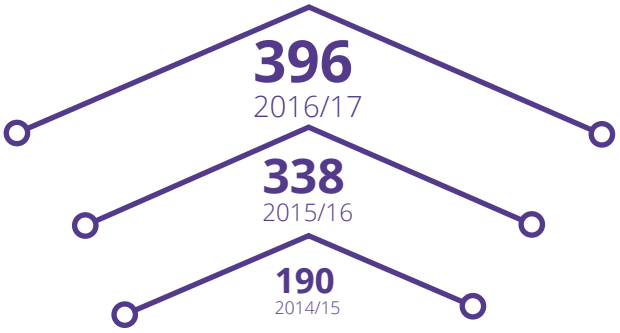
Summary of recorded incidents by sector

NCSC recorded 396 incidents in the 2016/17 year, an increase of 58 over 2015/16. This increase matches NCSC's continued growth in capacity and customer base. The steadier growth of NCSC's capacity now its advanced cyber defensive (CORTEX) capabilities are in place and the emergence of CERT NZ in April 2017 will affect the number of incidents recorded in the next year.

The NCSC remains focused on countering sophisticated cyber threats and protecting New Zealand's networks of national importance. However, at the initial discovery of an incident, there is not always sufficient information to determine its severity or significance. As a result, a number of incidents are recorded and triaged that, upon further investigation, do not reach the threshold for response by NCSC. In such situations, the NCSC will refer the reporting organisation on to the most appropriate organisation for response.

In the most serious cases, the NCSC provided hands-on intensive incident response and has done so on 31 occasions in the past year. On a further 239 occasions, the NCSC provided reports or advisories to alert customers to potential cyber security incidents or risks and to provide mitigation advice to help increase the resilience of customers' networks.

TOTAL RECORDED INCIDENTS



	2014/15	2015/16	2016/17
Public sector entities	114	169	211*
Private sector entities	56	73	146*
Other	20	96	91

The NCSC records incidents from a number of sources. These include self-reporting by the victim, detection by NCSC's advanced cyber defensive (CORTEX) capabilities, and reporting from our domestic and international partners.

The NCSC defines a cyber security incident as "an occurrence or activity that appears to have degraded the confidentiality, integrity or availability of an information infrastructure".

*A change in incident recording allowed more than one victim per incident, therefore the number of public and private entities affected differs this year from the total number of incidents.

What types of threats do we face?

The NCSC records the type of vulnerability or exploit that has affected a victim. The variety in any given category of technical threats makes a precise taxonomy difficult, but it is possible to represent this information at the stage it occurs within the life cycle of a compromise. The adjacent box explains the Cyber Threat Framework and illustrates the stage at which incidents were detected or reported to the NCSC during the 2016/17 year.

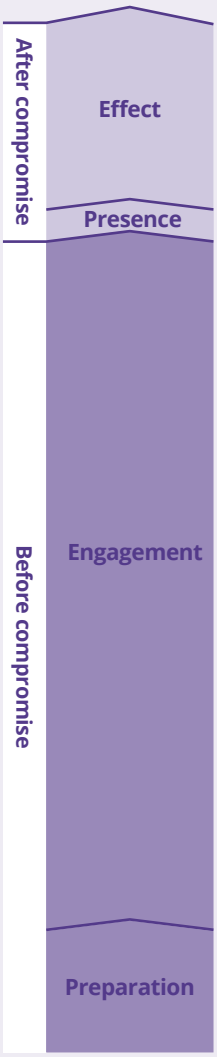
Phishing contributes to the 'engage' category. It remains the most common delivery mechanism because individual users remain vulnerable to deception, frequently clicking on malicious links or opening malicious attachments.

Compromised credentials, either stolen or unintentionally exposed, is a growing category of increasing importance due to the number of online or cloud services that are accessed using credentials. These compromised credentials contribute mostly to the 'presence' category because of the role they play in enabling an adversary to establish access or persistence on a network.

Publicly known vulnerabilities underpin many of the categories of cyber threats in the 'engage' and 'effect' categories. Unlike a zero day (a vulnerability that is not widely known prior to its exploitation) publicly known vulnerabilities often have existing fixes that only need to be applied to remove the vulnerability. If everyone patched operating systems and software or mitigated known vulnerabilities in some other way, adversaries would have to invest far more time and effort discovering ways to exploit computers.

An adversary, endeavouring to reduce the cost of their operations, can also use scanning to scale and automate the discovery of vulnerable systems. An adversary undertaking scanning will set up a tool to work methodically through internet addresses, making requests to routers, devices or webpages to determine the presence of, or exploit a vulnerability. The threat of scanning is often difficult to establish, it is not exclusively undertaken by malicious actors and can appear to be low impact preparation or potentially high impact engagement depending on the context.

The compromise of a computer network or system is not a singular event. While New Zealand's significant organisations regularly encounter cyber threats, not all of them have an impact.



CYBER THREAT FRAMEWORK

The cyber threat framework shows the phases of an incident and reflects that the NCSC is able to disrupt a threat at the engage phase, before harm has occurred.

Tracing the life cycle of a cyber threat takes place through a variety of stages: from preparation of capabilities and targeting to initial engagement with the targets or temporary non-intrusive disruptions by the adversary, to establishing and expanding the presence on target networks, and finally the creation of effects and consequences from theft, manipulation, or disruption.

Life cycle analysis, with slight variation, is used widely in the cyber security industry. The NCSC mostly draws on the Cyber Threat Framework.[4]

Effect
Deny, Extract, Destroy, Enable

Engagement
Deploy, Interact, Exploit

Presence
Hide, Expand, Persist

Preparation
Plan, Research, Develop

The majority of incidents recorded by the NCSC have been detected or reported before an effect occurs, with the largest category being 'engage'.

4 The Cyber Threat Framework was developed by the US Office of the Director of National Intelligence and is available at www.dni.gov/index.php/cyber-threat-framework

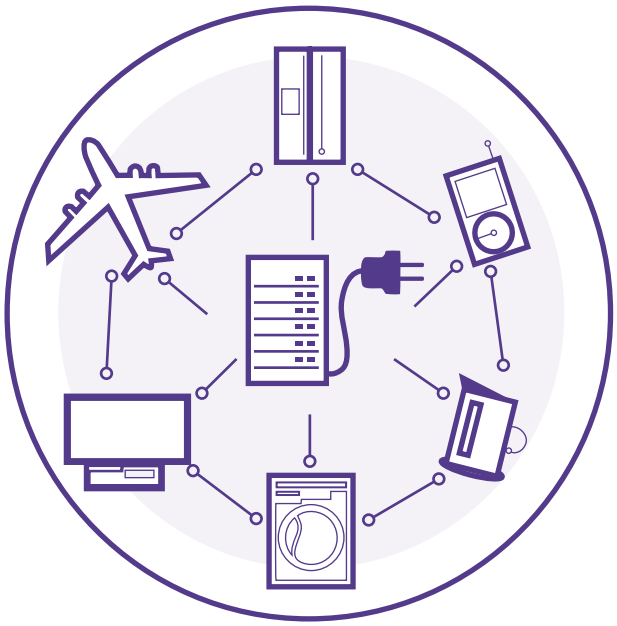
EXAMPLES OF VULNERABILITIES

Publicly released vulnerabilities

In April 2017 a group of cyber actors publicly released a number of exploits for vulnerabilities in several versions of Microsoft Windows operating systems. Patches for the exploited vulnerabilities had been released by Microsoft in March 2017, however many organisations had not applied the patches. A known cyber threat group subsequently used the exploit on 12 May 2017 to create a worm-like ransomware campaign, resulting in a global infection of 200,000 computers in the first 24 hours. Regular patching and updating systems, or ensuring sufficient mitigations where this is not possible, is fundamental to cyber security.

Internet of Things (IoT) and Control Systems

IoT is a real enabler for business (and individuals), as are control systems for industry. These also increase the number of exploitable devices on a network, are often difficult to manage, and pose unique and often high impact threats if compromised. Organisations should be aware of the risks that come with IoT, and demand baked-in security from providers and vendors.

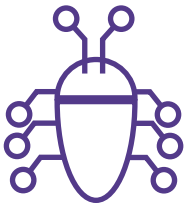


Supply chain

Modern organisations often rely on technology systems that are highly connected and in many cases, allow a range of third parties to access parts of their networks (for example lawyers, accountants, suppliers, customers, and managed ICT and security service providers). As organisations get better at cyber security, our adversaries are increasingly looking for new ways to target victims. Immunity of the herd will be critical to managing cyber risk.

Case studies

New Zealand's relative geographic isolation offers no protection from global cyber harms. Our systems and information are just as likely to be subject to attack as those in any other part of the world. The following case studies are based on real incidents the NCSC responded to in the 2016/17 year.



Infrastructure

The NCSC received information that a New Zealand organisation's network had been used to perform a significant cyber operation against a foreign organisation. The NCSC, along with the New Zealand Police, investigated the compromise and identified a malicious remote access tool (RAT) on a server in the network.

The RAT's functionality allowed the adversary to route the attack against the foreign organisation through the unwitting New Zealand organisation's network. The NCSC determined the New Zealand organisation was not targeted on their own merits and the compromise was likely opportunistic; analysis indicated the cyber actor exploited a weak password to gain access to the server.

In this instance, the NCSC attributed the compromise to a foreign intelligence service. The NCSC worked with the New Zealand organisation to remediate the compromise and provided prevention guidance to enhance its IT security.

Supply Chain

The NCSC became aware of suspicious activity from the New Zealand subsidiary of a global organisation's network. The organisation provided services to a wide range of organisations of national significance. The NCSC worked with the organisation to investigate the activity and identified the presence of two malicious RATs on a server in New Zealand.

The NCSC also recovered evidence the adversary had used a password dumping utility and lateral movement tool. The presence of these tools indicated the scope of the compromise was likely wider than a single server.

In this instance, the NCSC attributed the compromise to a foreign intelligence service. In response, the victim organisation launched a large global investigation and made significant changes to improve its network security posture.

Network Compromise

The NCSC became aware of historical malware activity on a New Zealand organisation's network. On investigation, the NCSC identified the presence of RAT malware on a number of core servers in the network. The NCSC determined the adversary had compromised the network a number of years earlier and had gained domain administrator credentials, enabling them full access to all parts of the network.

The NCSC also identified a file collector utility that automated the searching for and copying of certain document types. It is likely the adversary stole an unknown quantity of documents from the network.

In this instance, the NCSC attributed the compromise to a foreign intelligence service. The NCSC worked with the New Zealand organisation to identify the full nature of the compromise and remove the actors from their network.

Who did it?

The way the internet operates, including its physical distribution across numerous countries, makes it difficult to assign responsibility for an act to an individual. The NCSC performs attribution in various cases, usually in the classified space, to help it assess the intent of an actor or the potential impact of an incident.

The NCSC's most common form of attribution occurs when an incident is detected or discovered that contains indicators or technical artefacts previously associated with a state-sponsored actor. These indicators and artefacts come from numerous sources including the NCSC's own analysis and partner and open source reporting. In the past year, 122 incidents involved indicators that had been linked to state-sponsored computer network exploitation (CNE) groups.

The process of attribution can be costly and is only performed in its full extent in the most serious incidents. The confidence with which attribution can be performed will depend on the resources available to the agency undertaking the attribution and will include a combination of technical artefacts and analytical tradecraft.

Publicly reporting attribution is a significant decision and is not made by the NCSC alone. Public attribution is one way to reduce the efficacy of malicious cyber actors by revealing their tools or increasing the reputational costs of illegitimate activity. However, it also carries risk for New Zealand and is considered alongside our other national objectives including the need to maintain our ability to protect the networks that are of importance to New Zealand.

IN THE PAST YEAR

122

INCIDENTS

involved indicators that had been linked to state-sponsored computer network exploitation (CNE) groups.

Conclusion

Cyberspace is increasingly becoming a domain where all manner of cyber actors pursue their objectives, causing incidents of startling scale or impact. As the world and New Zealand becomes increasingly reliant on cyberspace, the incentives for malicious actors and the consequences for victims also increase.

Highlighting this trend in the past year were a number of high profile incidents illustrating the ends malicious cyber actors will use their cyber operations to achieve. The cyber attack against Ukraine using NotPetya malware,[5] the global WannaCry ransomware campaign, and the compromise of the US Democratic National Committee are all cyber operations with different purposes ranging from disruption to financial gain.

These cyber threats made it into the headlines but many of the most pervasive threats do not. The impact of cyber harm on New Zealand is far more significant and widespread than the incidents described above, but occurs with less intensity and visibility. Avoiding attention is also a guiding principle of most advanced or state-sponsored cyber actors that have a very real interest in New Zealand.

Underpinning insecurity in cyberspace are many non-technical economic, social and strategic factors. For example, a consumer who places price ahead of security diminishes the economic incentive of businesses to improve the security of their products. Social conventions like trust affect whether an individual will click a link or whether a victim reports an incident. International strategic factors can equally have a bearing on how many states are intending to conduct cyber operations.

The driving forces of insecurity remain and the level of security maturity amongst New Zealand's organisations of national significance varies. Organisations with mature cyber security arrangements are making it more difficult for adversaries, but malicious actors still possess the intent and capabilities to target most organisations. The ongoing success of common techniques, such as phishing and publically known vulnerabilities, demonstrates that adversaries are able to stay ahead without much effort.

To counter this, the NCSC aspires to a strategic goal of "impenetrable infrastructure" by 2020. Our drive towards this is based around working with nationally significant organisations and partners across the public and private sector, to help increase the cyber resilience of our important networks and systems.

GETTING IN TOUCH WITH US

If you have encountered a cyber incident, please visit our website for further information: www.ncsc.govt.nz

5 Cyber Attack Hits Ukraine Then Spreads Internationally, https://www.nytimes.com/2017/06/27/technology/ransomware-hackers.html