National Cyber Security Centre

Unclassified Cyber Threat Report – 2015/16

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

Internationally and in New Zealand cyber threats are continuing to increase. This National Cyber Security Centre Cyber Threat Report aims to provide context around New Zealand cyber incidents and guidance to mitigate such attacks.

The insights in this report reflect the perspective and understanding gained from helping protect New Zealand's organisations of national significance from advanced cyber threats. Information has been drawn from a broad range of sources to provide better awareness and understanding of cyber threats.

While this represents a significant increase from previous years it is likely to represent only a small proportion of total incidents impacting New Zealand and New Zealanders. This is in part because the NCSC's focus is typically on more advanced threats and those affecting nationally significant organisations and systems.

In summary, the NCSC recorded 338 cyber incidents during the reporting period from 1 July 2015 to 30 June 2016.

The increase reflects both the increased detection of threats by our defensive capabilities and an increase in organisations' self-reporting.

The NCSC recognises the role that informed and constructive discussion has in improving awareness of cyber threats and the depth of our cyber security response in New Zealand. This report is intended to support public awareness and mitigation of cyber threats.

The report highlights the range of threats that the NCSC has identified and responded to. The threats targeting New Zealand organisations are consistent with those identified by other cyber security service providers domestically and internationally.

Lisa Fong
Director, National Cyber Security Centre
Government Communications Security Bureau

The National Cyber Security Centre

The NCSC is an operational unit 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.

About the National Cyber Security Centre

What do we do?

The role of the NCSC is to protect New Zealand's most significant information systems from cyber borne threats. The NCSC's focus is on providing specialist information security advice and support to New Zealand's most significant organisations. This includes government departments, key economic generators, niche exporters, research institutions and operators of critical national infrastructure.

We assist these entities to protect their networks from the types of threats that are typically beyond the capability of commercially available tools, and from threats that could potentially impact on the effective functioning of a government, or the administration of a key economic sector.

In July 2014, Cabinet approved a project (CORTEX) for the GCSB to supply malware detection and disruption services to a cross-section of nationally significant organisations. These services are currently provided under warrant, authorised by Ministers and the Commissioner for Security Warrants. All services are provided with the express consent of the organisations being protected.

The NCSC delivers these services to a growing range of public and private sector customers. The threats to these organisations include espionage, theft of intellectual property, damage to IT systems or the disruption of their operations.

The NCSC also engages with a broader group of nationally significant stakeholders and organisations representing key sector and industry groups. This interaction ranges from incident response to improving information sharing. It includes coordination of a number of sector information exchanges where information security professionals from organisations within a sector are able to meet and confidentially share information relating to threats and response to threats that could potentially impact on that sector. This wider group also receives cyber threat alerts and advisories produced by the NCSC.

We are regularly able to proactively assist nationally significant organisations to respond to and mitigate threats based on what we see through our operational activity, including under CORTEX, and reporting we receive from our partners.

The NCSC's work delivering CORTEX services and our engagement across a broad range of nationally significant organisations are part of the Government's strategic approach to increasing New Zealand's cyber resilience as set out in the National Cyber Security Strategy.

Who do we work with?

As most cyber threats to New Zealand are foreign-sourced, the NCSC works with international and domestic partners, including government organisations, internet service providers (ISPs) and network operators to both help mitigate cyber threats, and increase New Zealand organisations' resilience to cyber threats. Domestically, the NCSC works in close cooperation with other agencies in order to determine the appropriate agency to respond to individual cybercrime or cyber security incidents.

This cooperation will continue with the development of New Zealand's Computer Emergency Response Team (CERT NZ), which will commence operations in the first half of 2017. Staff from the NCSC are working closely with officials from a range of organisations providing input into the establishment of CERT NZ. Once CERT NZ is operating, the NCSC will continue to play a key role in response to significant cyber events, particularly those which may impact on our nationally significant systems and information. CERT NZ's focus will be on helping NZ individuals, businesses and organisations to report cyber security incidents for action or referral to the right organisation.

The NCSC works closely with the international CERT community and shares information regarding cyber threats and threat actors with the Australian Signals Directorate (Australia), Communications Security Establishment (Canada), Government Communications Headquarters (United Kingdom) and National Security Agency (United States), all of whom have a similar cyber-security mandate. The information shared with partners is limited to only that necessary to counter cyber threats.

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

What is cyberspace?

The use of the word 'cyberspace', or sometimes just 'cyber,' is often criticised for being vague or simplistic. Yet it remains one of the easiest and quickest ways to communicate a complex idea to a broad audience.

A definition can be found in the 2015 New Zealand Cyber Security Strategy: cyberspace is the global network of interdependent information technology infrastructures, telecommunication networks and computer processing systems in which online communication takes place.

However, most readers will have their own intuitive understanding of what cyberspace means. How it is expressed will often differ, but it typically involves a person's relationship with information technology and the relationship between various different information technologies.

Summary of Activity

Incidents Recorded

	2014/15	2015/16
Total Recorded Incidents	190	338
Public Sector	114	169
Private Sector	56	73
Other	20	96

NCSC records incidents from a number of sources. These include self-reporting of incidents by the victim, detection of incidents by 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".

The NCSC recorded 338 incidents during the 2015/16 Financial Year, 148 more than in the 2014/2015 period. This increase is primarily due to the expanding capacity of the NCSC to detect and respond to more incidents. Cyber threats are proliferating along with the diverse range of internet-connected technologies and the increasing range of malicious actors. The NCSC remains focused on countering sophisticated, foreign sourced cyber threats and protecting New Zealand's networks of national importance.

Of the 338 incidents, 169 were associated with public sector entities and at least 73 involved the private sector; the remainder involved individuals, small businesses and some instances in partner reporting where the victim is not readily identifiable. This distribution of recorded incidents is a reflection of detection and reporting rather than an indicator of greater vulnerability of public over private sector systems.

In the most serious cases, where we have seen the potential for significant compromise or indicators of a particularly sophisticated threat, the NCSC provides hands-on, intensive incident response. In 2015/16 this support was provided on 28 occasions, to 18 different organisations, including nine private sector companies. Where the NCSC is unable to assist, or judges the victim to have sufficient capability to respond themselves, it will issue an advisory or provide advice to the victim.

Who did it?

Attribution is difficult for incidents and events that occur in cyberspace. The way the internet operates, and its physical distribution across numerous countries, makes it very difficult to assign responsibility for an act to an individual. Our methods and tools are constantly evolving to meet the developing tradecraft of our adversaries.

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

From time to time the NCSC undertakes various

levels of attribution in the classified space to help us assess the intent of an actor and the potential impact of a cyber threat. Official attribution increases the risk for malicious cyber actors for whom remaining undetected is important. Where attribution includes technical details, it can also enhance the security of others by providing technical leads. Public attribution can however pose risk to future detection of attacks, and in many instances entities are reluctant to publicly disclose that they have been the subject of compromise. The decision to release information publicly is taken after careful consideration and consultation where appropriate.

What type of cyber threats do we face?

New Zealand private and public sector entities continue to be an attractive target for cyber espionage. Cyber threats to New Zealand's interests do not respect national borders. The threats discussed below are those most commonly detected or reported to the NCSC.

Our important information is at risk from a wide range of actors including nation states – many of whom have developed advanced cyber capabilities, and from criminals and organised crime groups who use readily available, highly effective tools and techniques to achieve their aims.

In the 2015/16 financial year the NCSC has seen targeting of critical networks by malicious cyber actors. The success of these actors could result in the loss of identity information, credentials or intellectual property, cause economic harm, or the loss of valuable government information.

The NCSC typically focuses on operations that target networks of significant national importance where the type of threat is advanced and typically beyond the capability of commercially available tools, or where the threat could potentially impact the effective functioning of a government, or the administration of a key economic sector.

Activity, for instance, that requests some form of payment, or targets banking credentials is typically criminally motivated and is more appropriatly handled by other New Zealand agencies. However, the NCSC does receive a wide range of reported incidents and some of the more common ones are described below.

Phishing

A common cyber threat seen by the NCSC is phishing, and it is assessed that most New Zealand companies and individuals receive phishing emails. Phishing is a technique that relies on the deceptive use of email to exploit a victim, and is used by both state-sponsored and criminal cyber actors.

The prevalence of phishing demonstrates the ongoing value and success malicious actors are able to achieve using this method. The dependence on email for online communication ensures a captive pool of readily accessible targets. Many larger organisations have the capacity to mitigate some of this threat at a corporate level, however small to medium size enterprises and individuals will remain the most vulnerable.

Only as strong as the weakest link

Malicious cyber actors rely on vulnerabilities in people and technology in order to gain unauthorised access to systems or networks.

The process of discovering new vulnerabilities is time consuming. Most major software vendors offer regular updates and patches for their products that fix vulnerabilities as they are discovered. Fortunately for malicious cyber actors, many people do not install updates and known vulnerabilities can be used for extended periods of time.

Other cyber actors find it simpler to target vulnerabilities in people than technology itself. By exploiting trust or employing deception, network users can be tricked into handing over their passwords, running malicious software and bypassing security systems.

Education and awareness can reduce the likelihood of individuals being deceived. Updating and patching software limits the potential vulnerabilities cyber actors can use.

Case Study of Incident types in 2015/16

Phishing emails

A number of New Zealand Government entities continually receive phishing emails from state-sponsored actors. The actors target employees who are or who have travelled abroad. The phishing emails are often themed around the areas of interest to the employee or topical news events. These phishing emails contain malicious attachments or links to malicious files. The links, when clicked on, typically direct the user to a website that attempts to run malicious software on the user's computer. Likewise, the attachment (which may take the form of a PDF, Word document or similar legitimate looking file), when opened, attempts to run malicious software on the user's computer. This malicious software can perform a number of functions, including opening a backdoor to the user's computer, downloading additional software, or stealing sensitive information. The NCSC works with these entities to ensure that their security continues to prevent these attacks from being successful.

A phishing email is only effective if a user interacts with it, either downloading a malicious attachment, following a link to a compromised webpage or responding to the sender. The craft of phishing is to appear convincing by pretending to be a friend, a familiar online service, or by appearing really interesting, to get a user to interact with the email.

The phishing techniques reported to the NCSC demonstrate social engineering that would often be effective against New Zealand recipients. In some cases, the actors mimic email addresses of local organisations to improve credibility. These campaigns do not typically demonstrate much concern for detection and are the delivery mechanism for malware or to elicit users to provide credentials.

Despite increasing awareness, phishing remains a low-cost and effective distribution mechanism for cyber actors, and its ongoing use is cause for concern. When it is not possible to detect or block all phishing emails, the last line of defence against phishing is the recipient. The continued use of phishing suggests that adversaries remain optimistic about their ability to avoid detection and can rely on end users downloading malicious attachments or clicking on malicious links.

A successful phishing campaign can result in the collection (using deception or misdirection) of usernames, passwords or other details required to access a computer, network or digital service. The use of credential harvesting increased in the past year and the NCSC received reports or responded to several incidents involving compromised credentials.

Malware

Malware is malicious software designed to facilitate unauthorised access to a computer system, or cause damage or disruption to a system. Malware can be delivered to victim computers in a range of ways. In 2015/16 global information security providers reported they were identifying new malware variants of a rate of more than 200,000 new samples every day. The most common methods are by the use of phishing (by directing users to click on a malware attachment or link to a website hosting the malware), by the use of watering holes (by compromising a legitimate website known to be visited by the victim), and by the use of removable media (such as infected USB sticks).

The form of malware most commonly reported to the NCSC is ransomware. Whereas other malware may go unnoticed for a long periods, ransomware differs significantly in that it has a visible effect by denying access to files. The victim must pay the malicious actor in order to regain access and provides an easy way to monetise vulnerabilities found in a wide range of systems.

Ransomware is commonly delivered via phishing email but can also be the result of visiting a compromised web page. It is highly successful and likely to continue in 2017, with the potential for greater innovation in delivery mechanisms.

Ransomware has been a significant cause of financial harm for many New Zealand businesses and individuals. The NCSC has received reports of ransomware across a large number of victims from New Zealand's private sector as well as individual

New Zealanders. The NCSC also detects ransomware attempts against networks of national importance but their higher level of network security is typically enough to prevent infection or quickly remediate, and does not typically require a response.

Other forms of malware seen include Remote Access Tools (RATs). A RAT is a form of software that has both legitimate and illegitimate uses. When used illegitimately, it allows an adversary to remotely access a computer system and take control of it as if they were sitting at the keyboard. The RAT can allow a user to copy or delete files, steal passwords and record key strokes.

During the past year, the NCSC has also responded to incidents involving web shells. A web shell is a piece of malicious code injected into a vulnerable but otherwise legitimate web server, giving an unauthorised actor some degree of control. The owner of the webserver may not realise that they have been compromised but malicious actors could be using that access to attack other organisations, more seriously, to compromise visitors to their web site.

Malicious actors use tools to scour the internet for vulnerable servers. When a vulnerable server is detected it can be compromised, often with little or no effort by the adversary. Typical vulnerabilities the NCSC identify being exploited include weak remote access passwords, and vulnerabilities in unpatched software or systems such as Content Management Systems (CMS).

In most cases, this activity could have been prevented by owners of web servers implementing a good process to ensure that they are regularly patching Content Management System software (including all plugins and themes) they are running on their servers.

Denial of Service

Another common incident affecting New Zealand entities is Distributed Denial of Service (DDoS), or the threat of DDoS. A DDoS attack overwhelms a web service with such a high volume of traffic that the service is unable to cope, and becomes unresponsive.

Case Studies of Incident types in 2015/16

Web site compromise #1

In late December 2015, the NCSC became aware that a website of a New Zealand business was compromised and invisibly redirecting visitors' web-browsers so that malware was automatically downloaded. This malicious code forms the first step in a process to compromise visitors to the website. Subsequent analysis by the NCSC indicated that the malicious code was part of a widely available, open source, exploit kit. The attacker used a known vulnerability in the website's unpatched content management system to insert the malicious code into the website. The NCSC provided the owners of the website remediation and prevention guidance to remove the threat and enhance their security.

Web site compromise #2

In late 2015, the NCSC received information that a New Zealand business had potentially been targeted by state-sponsored foreign cyber actors, using a technique commonly known as a "wateringhole attack". The NCSC worked with the business and identified that the company's webserver had a number of web shells that were known to be used by the same actors. The web shells would have allowed a malicious actor to search for, access and change files or web pages, as well as giving them the ability to execute arbitrary commands on the webserver.

The NCSC worked with the business to identify the full nature of the compromise and enable remediation advice and assistance to remove the actors from their network.

This can have significant effect on businesses that rely on their online presence. A common use of this attack vector is as a form of blackmail for a payment (typically of bitcoins). Only some DDoS blackmail actors actually follow through on their threats. Distributed Denial of Service operations have also been used by issue-motivated groups to try and achieve media attention. These have resulted in limited success.

Why does New Zealand 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. With an internationally focused and market driven economy, as well as an open and diverse social environment, New Zealand is a perfect place to leverage the benefits of cyberspace.

The same factors that have enabled New Zealand's success in cyberspace make it vulnerable to malicious cyber actors. The connectivity and speed of the Internet, which has brought New Zealand closer to a vast number of international customers, has also brought it closer to vastly more cyber actors.

The ability to easily encrypt files has made online communications more secure enabling greater online commerce, but it also enables malicious actors to conduct their business undetected. The trust that underpins our online interactions and enables vibrant communities can be exploited to deceive people into clicking malicious links or downloading malware.

The malicious cyber activity does not have to be specifically directed against New Zealand for it to be a risk. The indiscriminate or transient cyber operations of malicious cyber actors are equally capable of causing significant personal or financial damage as specific, targeted, cyber operations.

New Zealanders can also be collateral victims of a cyber-intrusion against a third-party such as an online service provider, where that intrusion results in the compromise of account details or private information.

The trend towards greater adoption and expansion of digital services creates more targets for malicious cyber actors, who are in turn focusing on cyberspace in greater numbers and with increasing skill. Cyber security is now an important part of ensuring New Zealanders continue to enjoy the prosperity and well-being that cyberspace has enabled.

Mitigating Cyber Threats

Organisations can protect themselves from up to 85 percent of cyber threats by implementing key strategies:

- Patching - ensuring software and operating systems are up to date with the latest vendor released security patches;
- Application white listing - restricting the applications which are able to operate on your network to those that are really necessary; and
- Minimising administrative privileges - limiting the numbers of staff who have access to system controls and the areas of the system they can access.

There are a range of sources of support and advice to help organisations address the risks from cyber threats. These include business consultancy and information assurance providers (see the Department of Internal Affairs panel of IT security providers). In the case of more serious threats the NCSC's incident response team may assist. There are also a range of sector based information exchanges. In the first half of 2017 CERT NZ will be available for New Zealand individuals, businesses and organisations to report cyber security incidents for action or referral.

For more information and resources to assist response to cyber threats please visit www.ncsc.govt.nz/resources