NZ Incident Response Bulletin

Standard Edition – July 2020

In this issue:

News	Our Views	Upcoming Events
New Zealand	Threat Actors	DFIR Summit & Training 2020 - Live Online
World		2020 New Zealand Cyber Security Summit

Premium Edition contains additional information on Threat Alerts, Security Frameworks, Information Security Surveys, Forensic News and Research.

News:

A high-level executive summary containing some of the most important news articles that have been published on Forensic and Cyber Security matters during the last month.

New Zealand

Parliament passes modernised Privacy Act

The new Privacy Act 2020 was recently passed with unanimous support in Parliament. Replacing the old Privacy Act of 1993, it reflects many of the recommendations from a comprehensive review by the Law Commission in 2011.

"The new Privacy Act provides a modernised framework to better protect New Zealanders' privacy rights in today's environment," Privacy Commissioner – John Edwards.

The new Act comes into effect on 1 December 2020, and some of the key reforms include:

- **Mandatory notification of harmful privacy breaches.** If a business suffers a breach that poses a risk of serious harm, they are required to notify the Privacy Commissioner and affected parties. This change reflects international best practice in this area.
- **Introduction of compliance orders.** The Privacy Commissioner may issue notices to require compliance with the Privacy Act. Failure to act on a notice could result in fines of up to $10,000.
- **Binding access determinations**. The Privacy Commissioner will now have the power to demand a business make personal information available upon request.
- **Controls on the disclosure of information overseas.** Prior to disclosing New Zealanders' personal information overseas, New Zealand businesses must ensure those overseas entities have similar levels of privacy protection to New Zealand.
- **New criminal offences.** It will be an offence to mislead an organisation in a way that affects someone's personal information or to destroy personal information if a request has been made for it. A maximum fine of $10,000 applies.
- **Explicit application to businesses whether or not they have a legal or physical presence in New Zealand.** International digital platforms undertaking business in New Zealand, with New Zealanders' personal information, will be obliged to comply with New Zealand law regardless of where they or their servers are based.

NZ Incident Response Bulletin

Standard Edition – July 2020

GCSB advised of risks of using Zoom video calls at Cabinet meetings in memo on lockdown eve

On the eve of level 4 lockdown, the Government Communications Security Bureau (GCSB) warned of several security concerns around the use of zoom for activities such as cabinet meetings or classified communications. Memos from the GCSB that were obtained under the Official Information Act (OIA) highlighted to Parliament Zooms prior publicly disclosed security vulnerabilities – including issues identified where hackers could remotely access video conferencing.

Despite this warning, the collaboration tool was used after cabinet officials felt appropriate security measures had been taken. A spokesperson for Zoom said it had "engaged with GCSB on recommended configurations, as well as updates to the security improvement that were subsequently made."

Clicking delete on extreme content: new Bill targets objectionable online material

New legislation has been introduced that aims to combat online terrorism and violent extremism by restricting objectionable online content.

The new Films, Videos and Publications Classification (Urgent Interim Classification of Publication and Prevention of Online Harm) Amendment Bill would make livestreaming of objectionable content a criminal offence. The Bill targets anyone who posts objectionable content as well as internet service providers and online content hosts.

The Bill comes after the 2019 terror attack in Christchurch and aims to align with international efforts to enable better regulation of online content. The Bill has extraterritorial application, which means it will apply to both overseas and New Zealand based online content hosts, "that provide services to the public" in New Zealand. The Bill introduces a new "take-down" regime and makes future provision for the establishment of a government-backed (either mandatory or voluntary) web filter if required.

Whistleblowers' protection bill introduced to replace 20-year-old Act

The Minister of State Services, Chris Hipkins, has just introduced a bill that will strengthen protections for whistleblowers. The Protected Disclosures (Protection of Whistleblowers) Bill will replace the Protected Disclosures Act, which is now 20 years old.

Chris Hipkins said the current laws were not working as well as they should. "Anyone who raises these issues, or 'blows the whistle', needs to have faith that their role, reputation, and career development will not be jeopardised when speaking up." Hipkins said the bill provided assurance that people could make disclosures without fear of punishment or reprisal. "The Bill will ensure New Zealand has a strengthened regime for disclosing serious wrongdoing in the workplace, which is critical to maintaining the country's reputation for high standards of integrity, openness and transparency," he said.

The changes will:

- Allow serious wrongdoing to be reported directly to an external authority, if a discloser wishes to do so
- Strengthen protection for disclosers by outlining what those receiving disclosures should do
- Require public sector organisations to provide more support for disclosers
- Extend the coverage of serious wrongdoing to include misuse of public funds or resources, whether public or private
- Make it clearer for whistleblowers who the appropriate authority is for making a disclosure

Summary of last month's cyber Alerts:

Incident Response Solutions post certain alerts and tips we consider to be in the public interest as it comes to hand.

We publish these alerts and tips on our YouTube Channel and this webpage.

- 30/06/2020 - EINSTEIN Data Trends – 30-day Lookback
- 22/06/2020 - ACSC Releases Advisory on Cyber Campaign using Copy-Paste Compromises
- 16/06/2020 - Active ransomware campaign leveraging remote access technologies
- 05/06/2020 - Cyber Alerts & Tips - CISA Unpatched Microsoft Systems Vulnerable to CVE 2020 0796

NZ Incident Response Bulletin

Standard Edition – July 2020

World

Judge demands Capital One release Mandiant cyberforensic report on data breach

A United States District Court Judge has ruled that Capital One must provide a copy of the forensic report produced by Mandiant following a high-profile data breach suffered by the company in 2018. Capital One faces multiple lawsuits in connection with the data breach that compromised the PII of approximately 100 million US and six million Canadian citizens. Credit card applications containing names, addresses, phone numbers, birth dates and more were stolen after a cyber attacker exploited a “configuration vulnerability” in Capital One systems. Mandiant was engaged after the breach to provide “services and advice concerning computer security incident response; digital forensics, log, and malware analysis; and incident remediation.” Capital One have attempted to keep the result of the forensic report confidential arguing it was protected as a “legal document.” However, the judge has disagreed, and a copy must be supplied.

Cyber spies use LinkedIn to hack European defence firms

Cybercriminals posing as corporate recruiters working for US military contractors on LinkedIn managed to gain access to the systems of two European defence and aerospace companies by sending phoney job offers to employees at the companies. The attackers are believed to have flattered their victims informing them that “they are “elites” who had a spot waiting for them with their purported companies”. “The attackers then used LinkedIn’s private messaging feature to send documents containing malicious code which the employees were tricked into opening” - Jean-Ian Boutin, Head of Threat Research, ESET.

LinkedIn identified and deleted the accounts used to conduct the attack, however ESET believes LinkedIn is a fertile ground for espionage despite their efforts to remove imposters. Hacking groups have reportedly been seen previously using the business-networking site to profile potential targets, demonstrating how criminals are using social engineering for cybercrime and espionage.

This attack is believed to be an example of international espionage. Whilst it has not yet been attributed to a known organised crime group, the attacks had some links to a North Korean group known as “Lazarus” who has previously been accused of high-profile attacks against Sony Pictures and The Central Bank of Bangladesh. Although it is still unclear what data was taken in the attacks, it is believed that the attackers were targeting sensitive technical and business-related documentation.

‘Modern warfare has changed’: Cyber attack threat rising in Australia

An emergency phone call to Scott Morrison was made on Thursday evening, declaring that Australia was under attack. “Based on advice provided to me by our cyber experts, Australian organisations are currently being targeted by a sophisticated state-based cyber actor,” Mr Morrison said from Parliament House. “This activity is targeting organisations across a range of sectors, including all levels of government, industry, political organisations, education, health, essential service providers and operators of other critical infrastructure.”

Treasury Sanctions Nigerian Cyber Actors for Targeting U.S. Businesses and Individuals

In a coordinated action with the U.S. Department of Justice, the Department of the Treasury’s Office of Foreign Assets Control (OFAC) took action against six Nigerian nationals for conducting an elaborate scheme to steal over six million dollars from victims across the United States. The individuals targeted U.S. businesses and individuals through deceptive global threats known as business email compromise (BEC) and romance fraud. American citizens lost over $6,000,000 due to these individuals’ BEC fraud schemes, in which they impersonated business executives and requested and received wire transfers from legitimate business accounts. Money was also stolen from innocent Americans by romance fraud, in which the designees masqueraded as affectionate partners to gain trust from victims.

As a result of today’s action, all property and interests in property of the designated persons that are in the possession or control of U.S. persons or within or transiting the United States are blocked, and U.S. persons generally are prohibited from dealing with them.

NZ Incident Response Bulletin

Standard Edition – July 2020

Our Views:

This month's theme is "Threat Actors".

In June, the Australian prime minister announced that their country was under attack. "Based on advice provided to me by our cyber experts, Australian organisations are currently being targeted by a sophisticated state-based cyber actor," Mr Morrison said from Parliament House.

These attacks on our neighbouring country had the potential to cause widespread damage to Australia, its stability, and its economy; however, for many businesses, the threat of a nationwide cyber-attack and the consequences of this on individual companies is abstract and not well understood. At the same time, albeit further afield, the US Department of Justice and the Treasury took action against a group of Nigerian nationals who are believed to have cost American citizens over USD 6,000,000 by perpetrating Business Email Compromise (BEC) fraud schemes and romance schemes.

In light of these varied scenarios, we thought it was time to investigate who the current cybercrime perpetrators (actors) are, what type of schemes they are specialising in and how this impacts businesses today. While many threat actors exist, many of those currently in the news fit into the following groups:

1. State-Sponsored Actors

It is estimated that at least 30 nations are actively waging cyber warfare on other countries targeting their economic, military, political or commercial infrastructure. Groups that are nation-state sponsored have unparalleled technical, financial, and material resources to create sophisticated attacks and are known for playing a "long-game".

These groups often conduct cyber-espionage to find competitive information, resources, or users to advance their political or military agendas. While mainly focusing on activities that benefit the interests of one nation over another; businesses may negatively feel the impact of this cybercrime too.

Cyberweapons such as Stuxnet and NotPetya severely impacted not only their designated targets but businesses throughout the globe, causing billions of dollars' worth of damage. A nation-state may also want your companies Intellectual Property for its use.

Defending against state-sponsored actors may seem lofty for an individual business; however, actions can be taken, including:

- Ensuring your patch/vulnerability management is up to date
- Employing Advanced Endpoint Protection and Anti-ransomware technology
- Considering which of your business assets may be attractive to a nation-state.

2. Organised Crime

Organised crime groups are motivated by financial gain. They undertake cybercrime to steal PII that can be sold on the dark web, and hijack critical business resources for a ransom. Various tactics are used to achieve their goals, but they are responsible for the significant recent increase in Business Email Compromise and Ransomware attacks. These groups also use Remote Access Trojans seen recently in New Zealand, along with phishing, social media, extortion, cryptominers, exploit kits, and blackmail. One hacking group, Fin7 are suspected of gleaning USD$50 million in profit each month of operation.

Defending against organised crime schemes involves the basics of good security hygiene, including:

- Strong password management and Multi-Factor Authentication
- User Awareness training (Often phishing schemes are the first entry point for an attack)
- Advanced endpoint protection
- Timely patching to encourage the attacker to find an easier target
- An Incident Response Plan to prepare your business to respond to any incident in a timely and coordinated fashion

3. Hacktivists

Hacktivist groups are motivated by a political, social, or religious agenda. They target government entities and corporations to expose what they believe are unjust or unethical business practices. Unlike organised crime groups, they tend to be loosely affiliated individual hackers or smaller groups who band together to highlight a cause or expose a perceived injustice.

Common tactics employed by these groups include the defacing of corporate websites, the hijacking of social media accounts and DDoS attacks on websites. Well-known hacktivist groups Anonymous and LulzSec have previously targeted various high profile victims, including the US presidential campaign, the Islamic State (IS) and certain corporates. Since 2016 however attacks attributed to hacktivist groups have reduced.

Defending against an attack from hacktivists starts with considering whether your business could be a target by understanding the causes that these groups are acting in support of (i.e., environmentalism) and being aware of how your brand is perceived concerning these issues. Create a sound and secure social media management strategy and stay up-to-date with trends.

4. Insider Threat

The insider threat refers to anyone operating inside your business such as employees, contractors, trusted vendors or third parties. Insider threats are challenging to detect as an insider may have valid credentials, inhouse knowledge of systems and security and operate in a trusted position.

Typically, the insider threat comes from two different areas. Firstly, many are disgruntled or ex-employees who may wish revenge or financial gain (a second revenue stream). These insiders have malicious intent. The second category, however, can do just as much damage, and that is insiders who are negligent or commit unintentional errors.

Insider threats appear to be on the rise, and some studies believe they play a role in 50% of security breaches. The insider threat is one that is difficult to manage and we believe is an overlooked area that businesses should focus on as thoroughly as their external threat strategies.

High profile cases where insiders have caused damage include Edward Snowden, who disclosed two million confidential files in 2013 and a South Korean employee who sold 27 million company data files for profit. However, most insider threat cases do not make the news as are considered Human Resource matters for internal resolution.

A business needs to have visibility across their network for tracking user behaviour and identifying anomalous behaviour to protect against the insider threat. This visibility has been made more challenging of late as many businesses have moved to the cloud where access monitoring and granular log detail creation may not be as rigorous. Other actions companies can consider for protection against insider threat include:

- Employing the concept of 'least privilege" when granting system and file access
- Ensuring all devices on the network (including BYOD) are protected via a firewall, media control and protected against Bluetooth and other peripherals
- Instigating Employee Wellness programmes to uncover disgruntled or employees under stress or duress early
- Conducting cybersecurity training frequently to minimise unintentional errors.

While various cyberthreats are highlighted in the media every day, understanding how and whether these threats may apply to your business can be challenging. Defending your business against a known threat may be easier and more effective than defending against the unknown.

Therefore, we recommend staying aware of the key activity happening in the cybercrime world via threat alerts and becoming familiar with the main perpetrators and their motives to ensure your defence strategies are appropriate.

As mentioned by Sun Tzu in The Art of War, "If you know the enemy and know yourself, you need not fear the result of a hundred battles".

NZ Incident Response Bulletin

Standard Edition – July 2020

Upcoming Events:

Date	Event	Location
16 to 25 July 2020	DFIR Summit & Training 2020 - Live Online	Online
14 October 2020	2020 NZ. Cyber Security Summit	Te Papa, Wellington.

About the Bulletin:

The NZ. Incident Response Bulletin is a monthly high-level executive summary containing some of the most important news articles that have been published on Forensic and Cyber Security matters during the last month. Also included are articles written by Incident Response Solutions, covering topical matters. Each article contains a brief summary and if possible, includes a linked reference on the web for detailed information. The purpose of this resource is to assist Executives in keeping up to date from a high-level perspective with a sample of the latest Forensic and Cyber Security news.

To subscribe or to submit a contribution for an upcoming Bulletin, please either visit https://incidentresponse.co.nz/bulletin or send an email to bulletin@incidentresponse.co.nz with the subject line either "Subscribe", "Unsubscribe", or if you think there is something worth reporting, "Contribution", along with the Webpage or URL in the contents. Access our Privacy Policy.

About Incident Response Solutions Limited:

Our Purpose - We help you with specialist forensic, cyber security and crisis management expertise at all stages throughout the incident response lifecycle.

Our Promise - We will provide you with the confidence you require to prepare, respond and recover from forensic and cyber incidents.

Our specialist Forensic Technology expertise includes Computer Forensics, Cybercrime Incident Response, Social Media Analysis and eDiscovery. We have significant experience in providing expert witness reports and in delivering expert witness testimony at trial. Our background includes experience in Law Enforcement (NZ Police) and Big 4 Professional Services.

Campbell McKenzie
Director
Incident Response Solutions Limited
0800 WITNESS
+64 21 779 310
campbell@incidentresponse.co.nz

This Bulletin is prepared for general guidance and does not constitute formal advice. This information should not be relied on without obtaining specific formal advice. We do not make any representation as to the accuracy or completeness of the information contained within this Bulletin. Incident Response Solutions Limited does not accept any liability, responsibility or duty of care for any consequences of you or anyone else acting, or refraining to act, when relying on the information contained in this Bulletin or for any decision based on it.

Share our Bulletin: