NZ Incident Response Bulletin

Standard Edition - June 2019

In this issue:

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

Unauthorised access to Budget information

On 28 May 2019, the Treasury reported that it had gathered evidence to indicate that its systems had been deliberately and systematically hacked in relation to Budget information.

The Treasury referred the matter to the Police on the advice of the National Cyber Security Centre (NCSC). The Treasury and the NCSC reported it had established the following facts of this incident:

- As part of its preparation for Budget 2019, the Treasury developed a clone of its website.
- Budget information was added to the clone website as and when each Budget document was finalised.
- On Budget Day, the Treasury intended to swap the clone website to the live website so that the Budget 2019 information was available online.
- The clone website was not publicly accessible.
- As part of the search function on the website, content is indexed to make the search faster. Search results can be presented with the text in the document that surrounds the search phrase.
- The clone also copies all settings for the website including where the index resides. This led to the index on the live site also containing entries for content that was published only on the clone site.
- As a result, a specifically worded search would be able to surface small amounts of content from the 2019/20 estimates documents.

NZ Incident Response Bulletin

Standard Edition - June 2019

- A large number (approx. 2,000) of search terms were placed into the search bar looking for specific information on the 2019 Budget.
- The searches used phrases from the 2018 Budget that were followed by the "Summary" of each Vote.
- This would return a few sentences – that included the headlines for each Vote paper – but the search would not return the whole document.
- At no point were any full 2019/20 documents accessible outside of the Treasury network.

On 30 May 2019, the Police advised the Treasury that, on the available information, an unknown person or persons appear to have exploited a feature in the website search tool, but that this does not appear to be unlawful and that they are not planning further action.

Cryptopia liquidators seek advice from courts as to how to pay back customers

Liquidators for hacked cryptocurrency exchange Cryptopia are seeking legal advice as to how to repay out-of-pocket customers.

Cryptopia closed the exchange for trading when a hack was discovered in January. It was reopened to trade in certain crypto assets in March and then continued to trade through to May. Liquidators were appointed due to low trade volumes.

In their first report, the Liquidators said Cryptopia's liabilities totalled $4.2 million with assets totalling $1.7 million. They obtained a court order this week to use Bitcoin held by the company to fund the liquidation.

As there is no legal precedent on crypto assets, the distribution of Cryptopia's assets would require significant direction from the courts, including the Bankruptcy Court in New York in order to preserve the Cryptopia information stored on servers in the United States.

World

Moody's downgrades Equifax's rating outlook due to cyberattack

On 10 May 2019, Equifax acknowledged a first-quarter financial hit of $690 million (USD). The loss is related to a class-action lawsuit and regulatory fines following a data breach which exposed the Personally Identifiable Information of about 148 million customers. The breach has so far cost Equifax around $1.4 billion (USD).

Credit ratings agency Moody's has subsequently revised its rating outlook for Equifax, downgrading it from stable. This is the first time Moody's has taken such an action from a cyberattack. According to Moody's, Equifax's business performance and reputation suffered from the breach. Further, the company's cash flow has decreased because of legal and IT expenditures stemming from the incident.

It's 2019 and a WhatsApp call can hack a phone

A security flaw was discovered in WhatsApp where spyware was injected into victims' smartphones. The hack is activated by calling the target's number, allowing them to hijack the application and run malicious code to access chats, calls, photos, contacts, turn on the microphone and camera as well as altering the call logs to hide the method of infection.

The vulnerability is present in the Google Android, Apple iOS, and Microsoft Windows Phone builds of the app, which is used by 1.5 billion people globally.

Engineers at WhatsApp parent company Facebook moved quickly to patch the hole, designated CVE-2019-3568, with new versions of WhatsApp being rolled out over a matter of days. Security researchers recommend updating your WhatsApp software.

NZ Incident Response Bulletin

Standard Edition - June 2019

Our Views:

A selection of issues relevant to Forensic and Cyber Security matters during the last month. This month's theme is "Computer Crimes and the Law".

Crimes Act 1961

For all its benefits, technology does have a dark side - electronic crime. As traditional means of committing theft and fraud has waned, incidents of electronic crime has continued to rise.

In 2003, the Crimes Amendment Act introduced four new sections relating to "Crimes involving computers". Since then, New Zealand Courts have heard numerous cases involving crimes being prosecuted under these sections. Notably, one high profile case was heard in the Supreme Court.

While a lot of media attention is focused on cyber threats posed by hackers, it is often employees or third parties who dishonestly access, copy or damage data. Organisations who believe they have suffered from a computer crime may pursue one of the following courses of action under the Crimes Act, we have included a summary of the relevant sections below:

Section 249 - Accessing computer system for dishonest purpose

Everyone is liable to imprisonment who accesses any computer system and obtains any property or advantage; or causes loss to any other person.

Section 250 - Damaging or interfering with computer system

Everyone is liable to imprisonment who intentionally or recklessly destroys, damages, or alters any computer system if they know or ought to know that danger to life is likely to result. This extends to any person who damages or modifies any data or software in any computer system.

Section 251 - Making, selling, or distributing or possessing software for committing crime

Everyone is liable to imprisonment who sells or supplies any software or other information that would enable another person to access a computer system without authorisation, knowing that it could be used to commit an offence.

Section 252 - Accessing computer system without authorisation

Everyone is liable to imprisonment who intentionally accesses any computer system without authorisation, knowing that they are not authorised to access that computer system, or being reckless as to whether or not they are authorised to access that computer system.

Search and Surveillance Act 2012

Evidence of offending under the above sections of the Crimes Act may in certain circumstances, be only located in remote locations, commonly referred to as 'the Cloud'.

Remote access is administered under the Search and Surveillance Act, which governs search warrants and surveillance device warrants. Specifically, every person executing a search warrant authorising a remote access search may use reasonable measures to gain access to the thing to be searched and if any intangible material in the thing is the subject of the search or may otherwise be lawfully seized, copy that material (including by means of previewing, cloning, or other forensic methods).

Expert Witnesses

In New Zealand Courts, Computer Crime matters will often require an expert witness to give evidence. Such experts are bound by Schedule 4 of the High Court Rules, 'Code of Conduct for Expert Witnesses'. An expert has a duty to assist the court impartially on relevant matters within the expert's area of expertise and is not an advocate for the party who engages the witness.

NZ Incident Response Bulletin

Standard Edition - June 2019

Upcoming Events:

Date	Event	Location
19 June 2019	NZ Lawyer - Legal Tech Summit	Auckland
19-20 August 2019	Gartner Security & Risk Management Summit 2019	Sydney, Australia
11-13 September 2019	ISACA 2019 Oceania CACS Conference	Auckland
16 October 2019	2019 NZ Cyber Security Summit	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
+64 9 363 7910
+64 21 779 310
campbell@incidentresponse.co.nz

Share our Bulletin: