NZ Incident Response Bulletin

February 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

Security Breach at New Zealand Crypto-Currency Firm Cryptopia

On 14th January 2019, the Cryptopia Exchange suffered a security breach which resulted in significant losses. Once identified, the exchange was put into maintenance while they assessed damages.

On January 16, police began an investigation into the unauthorised transfer of a "significant amount" of digital currencies, thought to be worth tens of millions of dollars.

Police have now been investigating for two weeks, occupying Cryptopia's Sydenham offices and calling on overseas experts and law enforcement authorities.

In a statement, police said good progress was being made and positive lines of enquiry developed to identify the source of the transfer, and where the crypto-currencies have been sent.

NZ Incident Response Bulletin

February 2019

World

Airbus Discloses Data Breach

Airbus detected a cyber incident on Airbus "Commercial Aircraft business" information systems, which resulted in unauthorised access to data. There is no impact on Airbus' commercial operations.

This incident is being thoroughly investigated by Airbus' experts who have taken immediate and appropriate actions to reinforce existing security measures and to mitigate its potential impact, as well as determining its origins.

Investigations are ongoing to understand if any specific data was targeted, however we do know some personal data was accessed. This is mostly professional contact and IT identification details of some Airbus employees in Europe.

The company is in contact with the relevant regulatory authorities and the data protection authorities pursuant to the GDPR (General Data Protection Regulation). Airbus employees are being advised to take all necessary precautions going forward.

Popular WordPress Plugin Hacked by Angry Former Employee

A very popular WordPress plugin was hacked after a hacker defaced its website and sent a mass message to all its customers revealing the existence of supposed unpatched security holes. In a follow-up mass email, the plugin's developers blamed the hack on a former employee, who also defaced their website.

Wordpress is an open source content management system used by more than 60 million websites.

The plugin in question is WPML (or WP MultiLingual), the most popular WordPress plugin for translating and serving WordPress sites in multiple languages. WPML has over 600,000 paying customers.

The WPML team said the hacker is a former employee who left a backdoor on its official website and used it to gain access to its server and its customer database. WPML claims the hacker used the email addresses and customer names he took from the website's database to send the mass email, but he also used the backdoor to deface its website, leaving the email's text as a blog post on its site.

The company says it's now rebuilding its server from scratch to remove the backdoor and resetting all customer account passwords as a precaution.

World Economic Forum Report: Data Breaches and Cyber Attacks in Global Risks List Top Five

Technology continues to play a profound role in shaping the global risks landscape. Concerns about data fraud and cyber-attacks were prominent again in the GRPS, which also highlighted a number of other technological vulnerabilities: around two-thirds of respondents expect the risks associated with fake news and identity theft to increase in 2019, while three-fifths said the same about loss of privacy to companies and governments.

There were further massive data breaches in 2018, new hardware weaknesses were revealed, and research pointed to the potential uses of artificial intelligence to engineer more potent cyberattacks. Last year also provided further evidence that cyber-attacks pose risks to critical infrastructure, prompting countries to strengthen their screening of cross-border partnerships on national security grounds.

NZ Incident Response Bulletin

February 2019

Our Views:

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

Compromised Passwords

In 2012, around 164 million Linkedin passwords were compromised. The critical risks to the many Linkedin users wasn't that their online 'CV' would be altered, rather whether they had used the same login and password on other accounts such as webmail. Linkedin sent an email shortly afterwards to affected users urging them to change any shared passwords. Passwords from such breaches continue to appear in fake emails, such as the recent 'webcam' scam where the subject line contains a password that was probably used by the recipient at some point. The sender says they have used that password to hack the recipient's computer, install malware, and record video of the recipient through the webcam. The attackers say they will reveal adult-website habits and send video to contacts unless they are sent around $1,000 NZD of bitcoin.

More recently in January, media reported that at least nine New Zealand websites were caught up in one of the biggest password security breaches of all-time. The breach known as 'Collection #1' contains 772,904,991 compromised accounts. We recommend checking whether any of your organisations email addresses have been compromised in either this or any other compromise, by running a search on this website https://haveibeenpwned.com.

Password Managers

Passwords should be protected against compromise using appropriate tools and policies. One tool is a password manager, which is a secure storage location for all your different passwords. A password manager protects its contents by using a "master" password which should obviously be very strong. A good password manager can also generate secure passwords for you.

A password manager can either be installed locally on your computer or you can access the information from a cloud-based manager. Locally stored password managers should be backed up regularly in case of corruption. Cloud based password managers have the added advantage of being able to access passwords from multiple devices. Accounts can be further strengthened using Two/Multi Factor Authentication (or 2FA/MFA), where the method used can also be stored in the Password Manager.

Cloud Identity

With the proliferation of cloud services, it is not surprising the cloud vendors are providing password manager services built into their offerings. According to a recent media article citing Google, *"Users expect agile, mobile work environments across multiple devices, and it's reshaping how we think about security, access, and control. Admins want to give them this modern, forward-thinking experience, but they don't want security to be compromised. The perimeter has disappeared."*

Faced with an ever-increasing threat of cyber-attack, a Cloud Identity system offers benefits such as screen locks, remote wipe, 2-Step verification, monitoring of password strength, assessments of your domain's overall exposure to a data breach, and reporting on which particular users pose security risks.

Upcoming Events:

Date	Event	Location
15 February 2019	CybersecCon	Auckland
22nd February 2019	OWASP New Zealand Day 2019	Auckland
28th February 2019	(ISC)^2 Auckland Chapter - Cybersecurity Dragons' Den	Auckland
7 March 2019	SFO Fraud and Corruption Conference 2019	Auckland

NZ Incident Response Bulletin

February 2019

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.

Share our Bulletin:

About Incident Response Solutions Limited:

Our mission is to provide speciality forensic, cyber security and crisis management expertise at all stages throughout the incident response lifecycle. We help you to “prepare, respond and recover”. We will assist you in returning to normal operations as quickly as possible, and to the extent possible, minimising reputational harm.

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

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.