NZ Incident Response Bulletin

Standard Edition – September 2022 – Issue #44

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. Each Bulletin also includes a section of our own content, based on a trending theme. We'll give you a brief summary of each article, and a link to more information. Why do we publish this bulletin? Because we want to keep you up to date with the latest Forensic and Cyber Security news, so that you aren't caught by surprise – and you'll know about risks and changes before they become problems.

Not subscribed to our Premium Bulletin? Click here to join.

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

Cybercrime rampant in New Zealand and cases not investigated until there's multiple victims

A police media spokesperson told Open Justice that online fraud was running rampant in New Zealand and police needed to wait for the victims to stockpile before taking action. "Police receive many more complaints than we can reasonably investigate. Police must assess each complaint against certain criteria to help prioritise offences for investigation, which includes targeting prolific offenders. As part of this process, police assess the available information and whether offender details, bank accounts or phone numbers are linked to other offences." the spokesperson said in a statement.

New Zealand to Adopt New Ecommerce Security Requirement to Counter Cybercrime

With more than half of retail businesses across the country now selling online, merchants are facing a growing threat of enumeration attacks, a criminal practice where fraudsters use automation to test and guess payment credentials such as Primary Account Number (PAN), card verification value (CVV2) and expiration dates, which can then be used in fraudulent transactions. It is the increasing use of botnets – which are networks of hijacked computer devices – that are being used to carry out and scale these attacks.

To help businesses counter the threat, Visa has introduced a requirement for ecommerce payment providers to invest in capabilities that identify and prevent enumeration attacks. By October 2023, providers must ensure they have advanced controls in place. These tools can range from scanning features that look for anomalies in shopping cart data; account blocking after a certain number of login attempts; restricting the number of transactions that can be processed by the merchant from a single card per minute; and CAPTCHAs, which are tasks that are designed to be easy for humans and difficult for bots.

Aotearoa's new Privacy Commissioner shares focus moving forward

In early June 2022, Justice Minister Kris Faafoi announced the appointment of the new Privacy Commissioner. Michael Webster, former Secretary of the Cabinet, replaced previous Commissioner John Edwards, who took on a post as the United Kingdom Information Commissioner.

The role of the Privacy Commissioner is one of the most important public service roles in Aotearoa. They are responsible for upholding and overseeing principles relating to the collection, security, use and disclosure of personal information, as well as access to and correction of personal information and the assignment and use of unique identifiers.

In recent years, data privacy has been an extremely relevant topic in Aotearoa. With changes to the Privacy Act in 2020, businesses and citizens alike are thinking more carefully about their data safety, and how they can be assured the correct protocols are in place. The rise of digitisation and cybersecurity processes in the age of hybrid work has also brought privacy back into the spotlight, with organisations now having to take extra precautions and navigate different technologies.

Breaches to our health system, along with a variety of other high-profile enterprise breaches, have prompted a significant shift in the perception of data security and how it is addressed. In these cases, the Privacy Commissioner is often at the forefront of the decision-making process at a government level, analysing issues and responding to public and enterprise concerns.

"My role is to lead a modern regulator focused on making privacy a core focus for agencies, in order to better protect the privacy of individuals, to enable those agencies to achieve their own objectives, and to safeguard a free and democratic society" - Webster.

World

Court criticises leading City firm for major e-disclosure failure

A High Court judge has criticised City law firm Fieldfisher for its failings in overseeing a disclosure exercise where 800,000 documents were missed, leading to a trial being adjourned for two years. Mrs Justice Joanna Smith ordered that its client, global toy maker MGA, should pay nearly £580,000 on account of wasted costs. UK toy start-up Cabo Concepts alleges a secret anti-competitive campaign on the part of MGA which is said to have caused the failure of Cabo's business. The claim is worth £170m. A four-week trial was due to start on 27 June, but three weeks earlier MGA informed the court that it had missed many thousands of documents during the data collection process underlying the disclosure.

World's Most Popular Password Manager Says It Was Hacked

LastPass, a password manager used by more than 33 million people around the world, said a hacker recently stole source code and proprietary information after breaking into its systems. The company doesn't believe any passwords were taken as part of the breach and users shouldn't have to take action to secure their accounts, according to a blog post on Thursday.

An investigation determined that an "unauthorized party" cracked into its developer environment, which is the software that employees use to build and maintain LastPass's product. The perpetrators were able to gain access through a single compromised developer's account, the company said.

UK NHS suffers outage after cyberattack on managed service provider

United Kingdom's National Health Service (NHS) 111 emergency services were affected by a significant and ongoing outage triggered by a cyberattack that hit the systems of British managed service provider (MSP) Advanced. Advanced's Adastra client patient management solution, which is used by 85% of NHS 111 services, was hit by a major outage, together with several other services provided by the MSP, according to a status page. "There is a major outage of a computer system that is used to refer patients from NHS 111 Wales to out-of-hours GP providers," the Welsh Ambulance Services said today. "This system is used by Local Health Boards to coordinate these services for patients. The ongoing outage is significant and has been far-reaching, impacting each of the four nations in the UK."

Nitrokod Crypto Miner Infected Over 111,000 Users with Copies of Popular Software

A Turkish-speaking entity called Nitrokod has been attributed to an active cryptocurrency mining campaign that involves impersonating a desktop application for Google Translate to infect over 111,000 victims in 11 countries since 2019.

"The malicious tools can be used by anyone," Maya Horowitz, vice president of research at Check Point, said in a statement shared with The Hacker News. "They can be found by a simple web search, downloaded from a link, and installation is a simple double-click." The list of countries with victims includes the U.K., the U.S., Sri Lanka, Greece, Israel, Germany, Turkey, Cyprus, Australia, Mongolia, and Poland.

Lloyd's state-backed cyber mandate spurs "grey area" fears

Lloyd's of London's latest cyber mandate, which will force its managing agents to exclude state-backed cyberattacks and war from standalone cyber policies from the end of next march, could lead the wider insurance market to adopt similar exclusions, and potentially lead to a stream of litigation, sources told Insurance Business. The Lloyd's mandate comes as Russia's Ukraine war has further thrust cyber risk into the public consciousness.

"Cyberattack risks involving state actors, however, have additional features that require consideration," Lloyd's set out in its August 16 market bulletin. "In particular, when writing cyberattack risks, underwriters need to take account of the possibility that state backed attacks may occur outside of a war involving physical force. The damage that these attacks can cause and their ability to spread creates a similar systemic risk to insurers."

Summary of last month's Cyber Alerts and News Clips:

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.

Our Views:

Forensic Readiness

"The art of warfare teaches us to rely not on the likelihood of the enemy's not coming, but on our own readiness to receive him; not on the chance of his not attacking, but rather on the fact that we have made our position unassailable" – Sun Tzu (The Art of War)

This somewhat overused but salient quote highlights the reason for spending time and effort assessing and improving your forensic readiness. Becoming forensically ready or "ready to receive the enemy" allows a business to move incident response and forensics from a purely reactive to a proactive activity.

The primary goals of forensic readiness are to:

1. Maximise the ability to collect evidence, and
2. Minimise the cost of incident response and forensic investigation

Forensic Readiness involves the establishment of administrative, technical and physical foundations to effectively support activities in the forensic process and resolve questions such as:

- Do we have the right information, systems, process, and skills to thoroughly and efficiently investigate a cyber incident?
- Do we know where all potential evidence is?
- Do we have the systems/logs/credentials/skills to obtain the evidence?
- Do we fully understand the backup procedures and how to retrieve backup data?
- Is the information in a usable format?
- Can we trust the information? (Is it authentic/reliable/has integrity been maintained?)
- How long will evidence retrieval take?
- How much is this going to cost?

How do I start?

Conduct a thorough a forensic readiness review and then embed it into your organisation's information security policies. This document should outline:

1. Applicable laws and regulatory requirements that apply to the business where the collection of digital evidence may be required.
2. The available resources your organisation will use in the digital forensic process, such as roles, evidence storage facilities, and suitable workspaces.
3. All assets and possible sources of digital evidence.
4. Who can collect each type of evidence (who has the access, authorisation and forensic skills.)
5. How this evidence can be collected (processes) and what supporting technology is required.

A more advanced readiness plan could also define tailored business risk scenarios (such as BEC) that may require evidence collection.

One example of an advantage gained from completing forensic readiness is identifying whether current security and event log collection is sufficient. For example, enabling detailed logging on an email account can help determine exactly what information an attacker may have viewed during a compromise. This evidence is invaluable when assessing an incident's scope and potential seriousness, but only if it exists and can be accessed and interpreted in a timely fashion. Completing the readiness process ensures you are fully aware of this capability.

In contrast, your response to any incident can be delayed and incur greater costs if you do not understand and document forensic readiness. For example, should a forensic expert require access to a potentially compromised laptop, a delay in obtaining any bitlocker keys necessary to access this laptop will slow down the ability to copy the evidence and start the investigation. Documenting which assets require keys, where the keys are stored, and who can access these can avoid this delay.

A business can take many proactive steps to ensure incident response and investigation run smoothly. Conducting a forensic readiness assessment and implementing forensic readiness is one we highly recommend.

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.

Subscribers to the premium edition also obtain access to the following additional information:

- Cyber Governance
- Cyber Incident Landscape
- Cyber Incident Response Resources
- Cyber Framework and Control Updates, Surveys and Research

Click here if you wish to subscribe to our Premium Edition of the Bulletin.

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

Further Resources:

Alerts	Data Breach Response	Forensic Technology
Cyber Incident Simulations	Social Media Investigations	Guide for NZ Law Firms

Share our Bulletin: