NZ Incident Response Bulletin

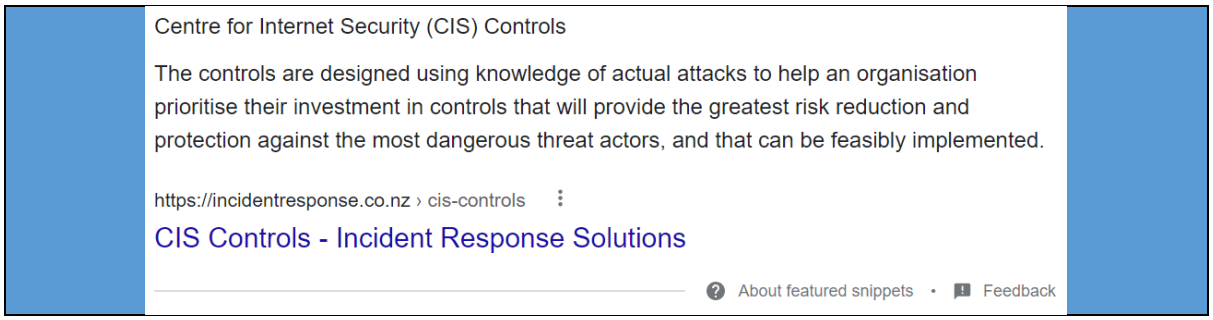
Premium Edition – February 2022 – Issue #37

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.

Bulletin Update:

For the last 36 months, we have published the Incident Response Bulletin to inform our readers about cyber risk, incident response preparation, and forensic technology considerations. We appreciate hearing from you about the insights and value you gain from our ongoing research.

We were also delighted to receive recognition this month from the Google Search Engine, following our recent Bulletin series about the 'CIS Controls'. Google has allocated the following 'Snippet' from our website page on CIS Controls:



One final update, starting this month; we have included a new section in our Premium Bulletin on the "Cyber Incident Landscape" which summarises the incidents we have responded to over the past month, trends to be aware of, and mitigations you can employ. We trust you will find this addition informative. 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

NZ business warns about cybersecurity after Facebook hackers lock owner out

An Auckland woman is warning other business owners to secure their social media accounts after her Facebook account was hacked. Sarah Chant's personal Facebook account was targeted, and Isis propaganda was posted on it, causing her page to be immediately banned because it breached Facebook's guidelines. As a result she lost access to her business Facebook pages, which she had run for more than 13 years, and feared her reputation, and her children's face-painting business Fab Faces, had been tarnished. She was unable to contact clients through the page, and the page sat inactive over the summer holiday period, which was a busy time for the business.

The account was restored after Stuff asked Meta about the scam. She has now set up Google Authenticator, a two-factor authentication service which requires a code sent to her mobile phone to be entered to access the account.

Ukraine might be far away, but a security crisis in Europe can still threaten Aotearoa

A geopolitical earthquake could begin within weeks. As a string of bilateral crisis talks predictably falter, further military aggression by Russia against Ukraine seems all too probable. If this comes to pass, the shock waves will likely be fast, wide and highly disruptive, potentially activating "tripwires" in the global security environment far beyond the edge of Europe. Aotearoa New Zealand's geographical distance will be no defence against the rolling consequences of a protracted crisis involving great powers and their allies. Yet there has been relatively little discussion in New Zealand about these threats. While this risk may seem remote, it is not a paranoid projection: Kremlin think tanks, such as Russtrat, have boasted of Sino-Russian capacity for overwhelming Washington and its allies through multiple-front confrontation. And there is evidence already of concerted cyber and information operations from Moscow and Beijing against Western targets, ranging from cyber-attacks to information warfare aimed at undermining democratic societies' trust in their institutions and leaders.

World

Cyber and Critical Technology Partnership with Australia: Foreign Secretary's statement

Foreign Secretary Liz Truss has agreed a new Cyber and Critical Technology Partnership with Australia's Foreign Minister Marise Payne, to strengthen global technology supply chains, ensure the UK's positive technology vision and tackle malign actors who disrupt cyber-space. The new agreement includes provisions to build greater resilience to ransomware amongst Indo-Pacific nations and sharpen legal sanctions against cyber attackers. It will also deepen practical co-operation on ensuring technology standards reflect our shared values. Foreign Secretary, Liz Truss said:

- As champions of freedom and democracy, the UK and Australia are hard-headed in defending our values and challenging unfair practices and malign acts.
- In the battlegrounds of the future, cutting edge technologies will be crucial in the fight against malign cyber actors who threaten our peace and security.
- That's why today, the UK and Australia have agreed a new cyber and technology partnership to ensure that liberal democracies shape the technology rules of tomorrow.

Cybersecurity labels for consumer products could be on the way

The National Institute of Standards and Technology (NIST) has revealed a certificate program that verifies Internet-connected devices, to ensure they meet a set of basic cyber standards such as accepting software patches and allowing users to control what information the devices collect and share about them. NIST isn't creating the labels itself, but has put together a lengthy set of recommendations for what they should look like. The ultimate goal is a virtuous cycle in which consumers prize the certificates, so companies try to earn them, stores and e-commerce sites prefer to stock products with certifications, and insurers use the certificates to assess product companies' liability. The effort, which sprang from President Biden's big cybersecurity executive order in May, marks one of the rare instances in which the government is trying to move beyond hiking cyber defences in critical industries to actually changing how the broader nation thinks about cybersecurity.

UK warned to bolster defences against cyber-attacks as Russia threatens Ukraine

The UK National Cyber Security Centre (NCSC) has issued new guidance, saying it is vital companies stay ahead of a potential threat. The centre said it was unaware of any specific threats to UK organisations. It follows a series of cyber-attacks in Ukraine which are suspected to have involved Russia, which Moscow denies.

Crypto.com confirms 483 users hit in attack that saw over $31m in coins withdrawn

After issuing hints at final numbers during the week, Crypto.com has made an official statement on the incident that saw it pause its users' ability to withdraw funds. The company said that 483 users were impacted by unauthorised cryptocurrency withdrawals on their accounts. "In the majority of cases we prevented the unauthorized withdrawal, and in all other cases customers were fully reimbursed," the company said. "Unauthorised withdrawals totalled 4,836.26 ETH, 443.93 BTC, and approximately US$66,200 in other cryptocurrencies."

FlexBooker discloses data breach, over 3.7 million accounts impacted

Accounts of more than three million users of the U.S.-based FlexBooker appointment scheduling service have been stolen in an attack before the holidays and are now being traded on hacker forums. The same intruders are offering databases claiming to be from two other entities: racing media organization Racing.com and Redbourne Group's rediCASE case management software, both from Australia.

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.

Alerts

9 January 2022 - Zoho Releases Security Advisory for ManageEngine Desktop Central and Desktop Central MSP

News Clips

15 January 2022 - Massive cyber-attack warns Ukraine to "expect the worst" amid tensions with Russia

Our Views:

Cyber Incident Detection

In 2020, the New Zealand National Cyber Security Centre (NCSC) part of the Government Communications Security Bureau (GCSB), published guidance in Cyber Incident Management. Incident response involves tactical practices to detect, respond to, and recover from cyber incidents.

Cyber incident risks cannot be solely managed through preventative measures. Accepting that a cyber incident could occur, we recommend adopting and adhering to a cyber incident framework that recognises the importance of 'detection' and 'response' functions. These functions require you to have the right data at the right time.

First up, you need a capability to collect and manage logs, events, alerts, and incidents. Identify these sources of data and then determine how this will help you inform your first steps in an incident in order to expedite the processes of containment, eradication and recovery.

So, you received a security alert; what now?

The cyberattack surface is constantly expanding, and attackers are continually adapting and escalating the threat landscape, making it almost inevitable that you will experience malicious activity inside your network at some stage. As we know, detecting this activity quickly and enabling a fast response is key to minimising damage. There are many tools designed for this purpose, such as Security Information and Event Monitoring (SEIM), Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), Data Loss Prevention Systems (DPL) and Network Behaviour Anomaly Detection (NBAD). Each of these tools are intended to act as an early warning system to alert you and initiate a suitable response.

So…how do you respond effectively to a security alert?

Threat Intelligence that comes from reliable and reputable sources is essential to understanding the steps to take after receiving a security alert. In addition, timely intelligence can help you clearly identify which alerts indicate genuine malicious activity and which may be false positives.

Obtaining up to date indicators of compromise and recent typical attack profiles can assist you to stay ahead of new threats as they emerge and take fast preventative action. For example, Cobalt Strike (a legitimate penetration testing framework) is often used as a command-and-control mechanism during an attack. However, it is an early step in the attack kill chain. Therefore, if you know to search for this tool and subsequently find it residing illegitimately on your network, you may be able to act and stop an attack before further damage is done.

If you are wondering what to do next, the NCSC pose a number of questions to ask yourself and then act:

- How would our organisation detect an incident?
- Are we responding to all the alerts we are receiving?
- Are we receiving too many alerts because we aren't tuning them correctly?
- If something happened, would we be able to go back and find the information in our logs?
- How far back can we go? Is it one week, one month, one year, or might we need longer?
- Have we produced reports for our security incidents?

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: