NZ Incident Response Bulletin

Standard Edition – March 2022 – Issue #38

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

January 2022 New Zealand Information Security Manual v3.5 Release

The New Zealand Information Security Manual (NZISM) has released an update (v3.5), which includes updates to Chapter 2 – Information Security Services within Government, Chapter 3 – Roles & Responsibilities, Chapter 5 – Security Documentation, Chapter 13 – Media and IT Equipment Management, Decommissioning and Disposal and Chapter 17 – Cryptography:

Businesses should prepare for increased regulatory, enforcement action in 2022

Law firm MinterEllisonRuddWatts' annual litigation forecast says businesses should expect more court action for unintentional regulatory breaches as regulators have increased funding to carry out that type of work. The firm's disputes resolution team said legal action was likely even where breaches were self-reported and corrected. "There is increasing regulatory intervention, climate change pressures, class actions and swift legislative change for some sectors. We can expect this trend to continue with a higher level of enforcement action by the Financial Markets Authority, Commerce Commission and the Reserve Bank." Business leaders should also expect increased risk, particularly around compliance, cyber threats and climate-related financial disclosure.

Ministers confirm new initiative to combat cyber threats

GCSB Minister Andrew Little and Digital Economy Minister David Clark have convened a committee of senior business leaders to provide advice on cyber-threats, Clark has confirmed. It is understood that the committee is receiving administrative support from the Department of Prime Minister and Cabinet and that the leaders of the businesses involved have been required to sign non-disclosure agreements. Clark did not comment on whether there was a specific change that prompted the ministers to establish the committee, such as an increase in the threat environment, but he said the group would advise the Government on how New Zealand could be more resilient to cyber threats and how government agencies could work more effectively with the private sector.

Innovation necessary for sustainable financial future - Reserve Bank governor

Innovation will be key to building a sustainable future for money and the cash system. In a speech to a conference of Angel Investors in Wellington today, Reserve Bank Governor Adrian Orr said the future of money and cash was at a "crossroad" and innovation was necessary to build a sustainable future. "We must decide how best to use digital technology to modernise central bank money, while we continue to ensure cash remains an option for those who need it," he said. While no decisions had yet been made, he said work was underway to design a Central Bank Digital Currency (CBDC).

New cybersecurity programme to tackle skills shortage

With about 10 billion devices connected to the internet worldwide and high-profile data breaches becoming all too common, there is a growing need for New Zealand organisations to invest in protecting and storing data. UCOL is responding to this need by offering the New Zealand diploma in cybersecurity from mid February. UCOL will deliver the one-year full-time level 6 diploma at its Manawatū campus together with Unitec Institute of Technology in Auckland, using their established programme and resources.

World

Regulators Move to Combat Cybercrime

In December, news surfaced of cybercriminals exploiting a new network vulnerability in a piece of Java-based, open-source software called Log4j. The widely used software performs the perfunctory task of logging data to help other programmes function. By mid-December, cybersecurity experts estimated that Log4j was the target of over 100 hacking attempts per minute, leading some to call it the most serious network vulnerability they had ever seen.

As serious as the Log4j vulnerability is, it will likely be eclipsed soon by a new one, and then another. The risk of cybercrime is steadily growing at a disturbing rate, both in terms of the sophistication of the attacks and the potential damage they can do. In response, the U.S. government has been reappraising cybersecurity risk. This will have important implications for private businesses, particularly contractors and subcontractors to the federal government.

The FBI is launching a cryptocurrency crime unit

Following the rise in cryptocurrency crime and ransomware attacks, the US Federal Bureau of Investigation (FBI) has revealed its plans to launch a new unit dedicated to stopping cybercriminals that abuse digital currencies. At this year's Munich Cyber Security Conference, US Deputy Attorney General Lisa Monaco announced the formation of the Virtual Asset Exploitation Unit (VAXU). According to Monaco, the new team will prevent the US government from falling behind “threat actors who exploit innovations as fast as the marketplace produces them”.

UK firms most likely to pay ransomware hackers

Some 82% of British firms, which have been victims of ransomware attacks, paid the hackers in order to get back their data, a new report suggests. The global average was 58%, making the UK the most likely country to pay cyber-criminals. Security firm Proofpoint's research also found that more than three-quarters of UK businesses were affected by ransomware in 2021. Phishing attacks remain the key way criminals access networks, it found.

US accuses couple of laundering $4.5bn in Bitcoin tied to currency exchange hack

The US Justice Department said it had unravelled its biggest-ever cryptocurrency theft, seizing a record-shattering $US3.6 billion in Bitcoin tied to the 2016 hack of digital currency exchange Bitfinex. A husband-and-wife team of alleged money launderers was arrested in Manhattan on Tuesday morning, it added. It was the Justice Department's biggest financial seizure, Deputy Attorney General Lisa Monaco said, adding in a statement that it shows cryptocurrency is "not a safe haven for criminals."

NSO Group: Israel launches inquiry into police hacking claims

Israel's government will set up a commission of inquiry to examine allegations that the police used spyware to hack the phones of Israeli public figures without authorisation. Officials, protesters, journalists, a son of former Prime Minister Benjamin Netanyahu and two aides were targeted, the newspaper Calcalist said. A witness in Mr Netanyahu's corruption trial was also allegedly monitored. Prime Minister Naftali Bennett said the reports, if true, were "very serious".

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

26 February 2022 - Cyber attacks against Ukraine that may have consequences on New Zealand organisations

News Clips

26 February 2022 - The U.S. Has Cyberattack Options, But What Would Retaliation Look Like?

Our Views:

The Ongoing Threat Posed by Phishing

Phishing remains the number one vector for malware to enter an organisation's network, and despite greater awareness of these scams, Business Email Compromise is still causing significant financial loss for businesses globally.

Typical phishing (spear-phishing and whaling) attacks often attempt to spoof a sender and use a forged email address. The subject lines or messages are frequently meaningless or contain poor spelling and grammatical errors that immediately raise suspicion. These types of campaigns rely on an end-user being either uneducated, distracted, busy or stressed. Whilst there are still plenty of these basic phishing campaigns around, we would like to highlight that phishing has and will continue to become more sophisticated and more targeted.

An example of a phishing attack method that is becoming more common and is harder to spot are email reply chain attacks. In an email reply chain attack, the attacker first takes over an email account. Email account takeover is achieved either via an earlier compromise and credential dump or through credential stuffing and password-spraying techniques. Once the attacker has access to one or more email accounts, they monitor ongoing conversation threads for any opportunity to send malware (e.g. Emotet, Qakbot etc) to the conversation's participants. Attackers will often utilise VBScript or PowerShell through Office Macros to deliver this malware.

Email reply chain attacks are more difficult to detect and much more successful than traditional phishing as the attacker does not need to spoof someone else's email address (as the email is commonly sent from a genuine email account). In addition, trust is already established between the email participants as a conversation has been ongoing. As the attacker has observed the preceeding conversation, they can also insert a malicious thread that fits the context of the discussion and does not appear out of place. This scenario means the likelihood of the attack being successful increases.

To avoid detection, attackers will do one or more of the following:

- Set up and use an alternate inbox to receive messages by configuring email account rules to route particular messages away from the usual inbox and into a folder that the genuine account holder may overlook or not suspect (such as Trash)
- Configure email forwarding rules to forward mail from specific recipients to another account

How to prevent falling victim to an email reply-chain phishing attack:

- Enable Multifactor Authentication
- Ensure strong password policies are enforced
- Encourage users to regularly check their email account setting for unusual rules or settings
- Disable macros use wherever possible
- Continue to educate end-users about these types of attacks

Microsoft recently outlined an extended version of this threat whereby the attackers compromise email accounts, extend their foothold within a business using lateral phishing and outbound spam, and finally connect an unauthorised device to the network to propagate the attack further. This attack version takes advantage of the current environment where BYOD and remote working has become business as usual. However, to thwart the second stage of this attack, an organisation merely has to ensure that MFA is enabled.

We believe these more evolved and multi-stage attacks involving reply chain phishing attacks will continue to rise.

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

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.

Further Resources:

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

Share our Bulletin: