Incident Response
FORENSIC & CYBER

NZ Incident Response Bulletin

Standard Edition – March 2025 – Issue #74

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

Government unit moves focus from natural disasters to cyber security

The New Zealand government's Department of Prime Minister and Cabinet (DPMC) is shifting its primary focus from natural disaster resilience to cybersecurity and broader national security risks. This unexpected shift surprised local authorities and industry stakeholders, given the recent severe storm impacts. Although specific reasons remain unclear, the government emphasizes that prior infrastructure resilience efforts will inform future programs. Meanwhile, public surveys indicate ongoing concerns about critical infrastructure failures and insufficient governmental communication regarding hazards.

Waikato couple narrowly avoid $270k scam after lawyer's email hacked

In December 2024, a Waikato couple narrowly avoided a $270,000 loss due to a sophisticated email scam involving their law firm's compromised email account. Cybercriminals, believed to be based in the UK, infiltrated the email system of a law firm and sent fraudulent payment instructions to the couple, who were in the process of purchasing a property. The scam was thwarted when a vigilant bank teller questioned the legitimacy of the transaction, prompting the couple to verify the request directly with their lawyer. Subsequent investigations revealed that the same fraudulent bank account had successfully defrauded other victims of at least $250,000.

Google's AI has been breaching New Zealand court name suppressions

Google's AI has been breaching New Zealand court-ordered name suppressions by revealing the identities of individuals involved in legal cases. The issue arises from AI-generated overviews and Google's search suggestions, which have exposed suppressed names despite legal protections. The breaches raise concerns about AI's ability to access and disseminate legally restricted information, though Google has yet to respond to inquiries about how this is occurring.

Legal experts warn that this development challenges New Zealand's name suppression laws, which are already difficult to enforce in the digital age. Media law specialist Steven Price noted that suppression orders for high-profile individuals often spark online speculation, undermining their effectiveness. He emphasized that while most suppressions protect victims rather than accused individuals, AI's ability to reveal sensitive information poses a significant risk. If Google's AI were to expose the names of protected victims, it would be far more alarming. The company's policies state that its AI relies on publicly available data, but concerns remain over how it processes and presents sensitive legal information.

Netsafe's tech ties spark calls for independent regulator

Netsafe, a New Zealand charity responsible for investigating online abuse under the Harmful Digital Communications Act (HDCA), has come under scrutiny due to its financial ties with major tech companies like Meta, X (formerly Twitter), and TikTok. Chief Executive Brent Carey acknowledged that these platforms contribute between $100,000 and $200,000 to Netsafe's funding, though he emphasized that approximately 90% of their $7 million budget comes from government contracts. Critics argue that accepting funding from tech giants compromises Netsafe's independence, leading to calls for the establishment of an independent regulator to oversee online safety.

The controversy intensified when RNZ reported that Netsafe and NZ Tech, the administrator of the Code of Practice for Online Safety and Harms—which is signed by companies like Meta, Google, TikTok, Twitch, and X—took legal action against the Human Rights Commission (HRC). This action followed the HRC's criticism of social media platforms for failing to protect former Prime Minister Dame Jacinda Ardern from online abuse and labelling the online safety code as inadequate. These developments have led to increased calls for a dedicated, independent regulator with enforcement powers to ensure accountability in managing online safety issues.

State-linked Russian spies increasingly targeting NZ organisations - National Cyber Security Centre

The NCSC reports increasing Russian state-linked cyberattacks targeting New Zealand's government and defence sectors. Over 7,100 incidents were recorded in a year, with 100+ attributed to state actors, intensified by the Russia-Ukraine conflict. Attacks include exploiting weak security, stealing credentials, and impersonation via business email compromise. The NCSC emphasizes adopting "zero trust" practices, urging stronger defences and improved awareness against evolving threats.

Australia

Further cyber sanctions in response to Medibank Private cyberattack

The Australian government has imposed further cyber sanctions in response to the 2022 Medibank Private cyberattack, targeting Russian entity ZServers and five individuals—Aleksandr Bolshakov (owner) and employees Aleksandr Mishin, Ilya Sidorov, Dmitriy Bolshakov, and Igor Odintsov—who facilitated the breach. These sanctions, a first for Australia against both an entity and its enablers, criminalize financial dealings with them, enforce travel bans, and carry penalties of up to 10 years' imprisonment. This move follows previous sanctions against Russian hacker Aleksandr Ermakov and aligns with Australia's broader cybersecurity strategy, reinforcing international collaboration with partners like the UK and US to combat cybercrime.

Patient information posted on dark web after cyber attack on IVF company Genea

In February 2025, Genea, a leading Australian IVF provider, experienced a cyberattack by an international ransomware group. The attackers claimed to have exfiltrated 700GB of sensitive patient data spanning six years and posted samples on dark web forums. This compromised information includes personal and medical details of patients. Genea responded by obtaining an interim injunction from the NSW Supreme Court to prevent further dissemination of the stolen data. Despite this legal action, the leaked information remained accessible on the dark web. The company faced criticism for delayed communication with affected patients, many of whom struggled to contact their clinics for urgent medical inquiries. Patients expressed frustration over the breach, highlighting the profound sensitivity of the compromised data and concerns about personal safety. Genea advised clients to remain vigilant against identity theft or fraud and to be cautious of unsolicited communications. The company is collaborating with cybersecurity experts and authorities to investigate the incident and has notified the Office of the Australian Information Commissioner.

World

North Korean hackers linked to $1.5 billion ByBit crypto heist

In February 2025, North Korea's Lazarus Group executed the largest cryptocurrency heist to date, stealing over $1.5 billion in Ethereum from the Dubai-based exchange Bybit. The hackers exploited a vulnerability during a routine transfer from Bybit's cold wallet to its hot wallet, redirecting approximately 400,000 ETH to an address under their control. This incident underscores the persistent threat posed by state-sponsored cybercriminals to the cryptocurrency industry.

RansomHub Becomes 2024's Top Ransomware Group, Hitting 600+ Organizations Globally

In 2024, RansomHub emerged as the most active ransomware group, targeting over 600 organizations globally across sectors such as healthcare, finance, government, and critical infrastructure. First identified in February 2024, RansomHub operates as a Ransomware-as-a-Service (RaaS) platform, recruiting affiliates from defunct groups like Knight and leveraging known vulnerabilities in Microsoft Active Directory and the Netlogon protocol to escalate privileges and infiltrate networks. Their tactics include brute-force attacks on VPN services and exploiting default credentials in backup solutions, with a rapid attack progression leading to data encryption and exfiltration within 24 hours of initial compromise.

DeepSeek AI Fails Multiple Security Tests, Raising Red Flag for Businesses

Security researchers have identified significant vulnerabilities in DeepSeek's AI models, particularly its R1 large language model (LLM). The model failed numerous security evaluations, including susceptibility to prompt injection attacks, where malicious inputs can manipulate the AI's responses. Additionally, concerns have been raised about DeepSeek's data handling practices, with reports indicating that user data may be transmitted to servers affiliated with Chinese state-owned entities, posing potential privacy risks. These findings suggest that DeepSeek's AI models lack robust security measures, raising concerns about their suitability for business applications.

Home Office contractor collected data on UK citizens while checking migrants' finances

In February 2025, it was reported that the UK's Home Office, through its contractor Equifax, collected personal data on numerous British citizens during financial assessments of migrants seeking fee waivers for visa applications. A document mistakenly sent to a charity revealed information on over 260 individuals, including names, dates of birth, and electoral roll data, some dating back to 1986. This incident has raised significant concerns about privacy and data protection practices within government operations.

Russian cybercrime network targeted for sanctions across US, UK and Australia

The US, UK, and Australia jointly imposed sanctions on the Russian web-hosting service Zservers and two Russian nationals connected to it, due to their role in facilitating LockBit ransomware attacks. LockBit, supported by Zservers' "bulletproof" hosting, has targeted critical institutions globally, extorting over $120 million. High-profile victims include Boeing, ICBC, the UK's Royal Mail, and NHS. These sanctions highlight international collaboration aimed at disrupting sophisticated cybercriminal networks and their infrastructure, reinforcing collective cybersecurity efforts.

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 this webpage.

12/02/2025 – CISA and FBI Warn of Malicious Cyber Actors Using Buffer Overflow Vulnerabilities to Compromise Software

Our Views:

The Rising Threat: MFA Token Theft and Email-Based Remote Access Tool Infections

As organisations continue to strengthen their security postures, attackers are evolving their methods to bypass traditional defenses. Two growing trends we have seen in this space include firstly, the theft of multifactor authentication (MFA) tokens and secondly, the distribution of remote access tools (RATs) via email. These sophisticated tactics enable attackers to silently gain persistent access to corporate networks, often evading standard detection mechanisms.

Understanding the Threat Landscape

1. MFA Token Theft

Multifactor authentication has been a cornerstone of modern cybersecurity, but threat actors have developed methods to intercept and hijack session tokens, effectively bypassing MFA protections.

How it happens:

- **Session Hijacking:** Attackers use phishing emails or malicious links to trick users into logging into fake portals. Once credentials and MFA tokens are entered, attackers harvest session cookies, allowing them to impersonate the user.
- **Malware & Info Stealers:** Keyloggers and advanced malware can exfiltrate authentication tokens stored in browsers or memory.
- **Reverse Proxy Tools (e.g., Evilginx2):** These mimic legitimate login pages and relay authentication requests in real-time, capturing both credentials and tokens.

Preventing MFA Token Theft

- **Use FIDO2/WebAuthn Authentication:** Replace SMS or TOTP-based MFA with phishing-resistant methods like hardware tokens (e.g., YubiKey) or biometric-enabled security keys.
- **Implement Conditional Access Policies:** Require re-authentication for sensitive applications or sessions and monitor for anomalies like impossible travel.
- **Session Management Controls:** Limit token lifespan, implement revocation policies, and monitor for concurrent logins from different geographies.
- **Advanced Email Filtering:** Block phishing emails that host fake login portals or redirect to credential harvesting sites.

2. Email-Distributed Remote Access Tools (RATs)

Cybercriminals are increasingly using email as a vector to distribute stealthy RATs, which grant full control over compromised systems.

How it happens:

- **Malicious Attachments:** Attackers embed RATs in office documents with macros or scripts that run upon opening.
- **Embedded Links:** Emails lure users into clicking links that download and install RAT payloads.
- **Trusted Spoofs:** Messages appear to come from legitimate vendors, internal departments, or known contacts, increasing the success rate.

Once installed, RATs allow adversaries to obtain login credentials, access or exfiltrate sensitive data, move about within the technology systems and install additional malware (e.g., ransomware or info stealers).

Defending Against RAT Infections via Email

- **Email Security Gateways & Sandboxing:** Scan attachments and links in a secure environment before delivery.
- **Endpoint Detection and Response (EDR):** Detect and isolate suspicious behaviours, such as unauthorised remote access or unusual process execution.
- **User Awareness Training:** Equip users with the ability to spot suspicious attachments and phishing attempts.
- **Application Whitelisting:** Block unapproved executable files from running on endpoints.

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: