NZ Incident Response Bulletin

Standard Edition – December 2024 – Issue #71

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.

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

Kiwis lose $2.3b to digital scams, Government readies three big moves

New Zealanders have suffered losses amounting to $2.3 billion due to digital scams. In response, the government is preparing three significant initiatives to combat this growing threat. These measures aim to enhance cybersecurity infrastructure, improve public awareness, and strengthen legal frameworks to deter cybercriminal activities. The comprehensive approach underscores the government's commitment to safeguarding citizens' financial well-being and digital security.

Govt to ramp up anti-scam efforts, bringing public sector and banking industry together

The New Zealand government plans to enhance anti-scam initiatives by fostering collaboration between public sector agencies and the banking industry. Commerce and Consumer Affairs Minister Andrew Bayly emphasizes the need for improved coordination to effectively address the issue, noting that only about 20% of scams are reported due to victims' reluctance. The strategy includes better information sharing, industry-led solutions, and international cooperation, particularly with Australia and Singapore, to develop a regional approach against scams.

Warning as online scams rise 53% in lead-up to Christmas

As the holiday season approaches, online scams have surged by 53%, with cyber safety experts urging consumers to remain vigilant. A survey by Norton revealed that a quarter of New Zealand adults have been targeted by scams during previous holiday seasons, with an average financial loss of $1,356. The current economic climate may lead consumers to overlook red flags in pursuit of better deals, making them more susceptible to fraudulent activities. Experts recommend avoiding unfamiliar websites, scrutinizing unsolicited communications, and using secure payment methods to mitigate risks.

Is your toaster spying on you? What data do our appliances collect?

Modern appliances, including toasters and air fryers, often come equipped with smart features that collect user data, sometimes without explicit consent. Investigations have found that certain appliances request permissions to record audio and track user behaviour, with data potentially being sent to manufacturers overseas. This raises concerns about privacy and data security, as consumers may be unaware of the extent of data collection and its usage. Experts advise consumers to be cautious about connecting appliances to networks and to understand the data policies of manufacturers.

Two UK nationals to be deported over text phishing scam

Two UK nationals have been convicted and are set to be deported for orchestrating a text phishing scam in New Zealand. The scam involved sending fraudulent messages impersonating reputable organizations, leading to significant financial losses for victims, with some losing between $10,000 and $100,000. The operation was disrupted through a joint effort by the police and the Department of Internal Affairs, marking a significant success in combating complex cybercrimes. Authorities emphasize the importance of vigilance and prompt reporting of suspicious communications to prevent such scams.

Australia

Australia's first Cyber Security Act becomes law

On November 25, 2024, the Australian Parliament enacted the Cyber Security Act 2024, marking a pivotal advancement in the nation's cyber defense strategy. This legislation mandates that organizations report ransomware payments to the government, aiming to improve transparency and coordination in combating cybercrime. The Act also facilitates enhanced information sharing during cyber incidents, bolstering the resilience of critical infrastructure sectors. This move aligns with Australia's Cyber Security Strategy 2023-2030, which aspires to position the country as a global leader in cyber resilience.

Australia: Privacy Act Amendments and Cyber Security Act Become Law

On November 29, 2024, the Australian Senate passed the Privacy and Other Legislation Amendment Bill 2024, introducing significant changes to the Privacy Act 1988. These amendments aim to strengthen data protection and privacy rights for individuals, complementing the recently enacted Cyber Security Act 2024. The legislative reforms collectively enhance Australia's cyber resilience and data security framework, addressing emerging threats and aligning with global best practices.

Spy alliance's dire warning on Aussie kids

The Five Eyes Intelligence Alliance, comprising Australia, New Zealand, Canada, the UK, and the US, issued a rare warning about the online radicalization of young Australians. Since 2020, over 35 Australian minors aged 12-17 have been suspects in counter-terrorism cases, with approximately 57% facing charges. Authorities emphasize the necessity for early intervention, highlighting instances such as a 16-year-old planning extremist acts and a 14-year-old orchestrating a school shooting. The report advocates for a "whole of society" approach, urging vigilance from parents and frontline workers to detect early signs of radicalization. Prime Minister Anthony Albanese called for increased parental awareness regarding children's online activities.

Australia critical infrastructure faces cyber threats, report says

A report by the Australian Signals Directorate revealed that over 11% of cybersecurity incidents in the past year targeted critical infrastructure sectors, including electricity, gas, water, education, and transport services. Common attack methods involved phishing (25%), exploitation of public-facing interfaces (21%), and brute-force activities (15%). Defense Minister Richard Marles expressed concern over the increased focus on critical infrastructure by cybercriminals and state actors, attributing some incidents to activities from China, Russia, and Iran. The report noted China's evolving cyber techniques targeting critical infrastructure, indicating preparations for potential disruptive effects.

World

BlackBasta Ransomware Brand Picks Up Where Conti Left Off

The article discusses the emergence of the BlackBasta ransomware group following the takedown of the Conti group in 2022. BlackBasta has quickly become a significant player in the Russian-language ransomware scene, adapting to law enforcement actions by diversifying its tactics. Initially relying on botnets like Qakbot for ransomware delivery, the group shifted to using Pikabot and developed custom malware tools such as Cogscan and Knotrock to enhance their operations. Their methods include phishing, vishing, social engineering, and purchasing access from initial access brokers. The article highlights concerns about BlackBasta's potential collaboration with the Russian state, especially given the increase in cyberattacks against the healthcare sector in 2024.

Massive Nigerian Cybercrime Bust Sees 130 Arrested

The Nigeria Police Force arrested 130 individuals involved in cybercrime activities, including 113 foreign nationals from China and Malaysia, and 17 Nigerians. The suspects are accused of high-level cybercrimes, hacking, and activities threatening national security. The operation, led by Assistant Inspector-General Benneth Igweh, targeted a store in Abuja, highlighting Nigeria's commitment to combating cybercrime. This significant bust reflects ongoing efforts to address cyber threats and protect national security.

Wanted Russian Hacker Linked to Hive and LockBit Ransomware Arrested

Russian authorities arrested Mikhail Pavlovich Matveev, a cybercriminal linked to ransomware operations like LockBit and Hive. Accused of developing malicious programs for encrypting files and demanding ransoms, Matveev faces charges under Russian law for creating and distributing harmful software. Previously indicted by the U.S. in May 2023 for attacks on thousands of victims worldwide, he operated under aliases such as Wazawaka and m1x. The U.S. Treasury had sanctioned him, offering a $10 million reward for information leading to his arrest. This arrest marks a rare instance of Russian law enforcement acting against a domestic hacker, signalling a potential shift in handling cybercriminals within its borders.

Free Decryptor Released for BitLocker-Based ShrinkLocker Ransomware Victims

Bitdefender released a free decryptor to assist victims of the ShrinkLocker ransomware, which exploits Microsoft's BitLocker utility to encrypt files. The decrypt in-depth analysis of ShrinkLocker's mechanisms, identifying a specific opportunity for data recovery post-removal of BitLocker protectors. ShrinkLocker, first identified in May 2024, targeted sectors in Mexico, Indonesia, and Jordan, notably affecting a healthcare company in the Middle East. The ransomware, written in VBScript—a language Microsoft plans to deprecate—gathers system information and installs BitLocker to encrypt drives. Bitdefender's tool offers victims a means to recover their data without yielding to ransom demands, emphasizing the importance of robust cybersecurity measures and regular data backups.

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.

21/11/2024 - CISA Releases Insights from Red Team Assessment of a U.S. Critical Infrastructure Sector Organization

Our Views:

Preparing for a Secure Holiday Season: A Guide for New Zealand Organisations Heading into 2025

As the festive season approaches, businesses across New Zealand often wind down operations, making it an opportune time for cybercriminals to exploit vulnerabilities. Cybersecurity risks don't take a break, and the rise of sophisticated attacks underscores the importance of being vigilant, even during the holiday season. Here's what New Zealand organisations should prioritise to secure their systems and prepare for 2025.

1. Understand the Threat Landscape

Both the **Australian Signals Directorate (ASD) Cyber Threat Report 2023-24** and **Google's Cybersecurity Forecast 2025** highlight the evolving nature of cyber threats in the following ways:

- **State-Sponsored Attacks**: Advanced Persistent Threats (APTs) from state actors, especially from the "Big Four" (China, Russia, Iran, and North Korea) continue to grow in sophistication driven by geopolitical tensions and strategic objectives. These attacks leverage sophisticated malware to target critical infrastructure, government entities, and key industries.
- **Cybercrime Trends**: Ransomware, phishing, and credential theft are on the rise, with attackers increasingly exploiting AI to craft realistic scams and automate attacks.
- **Living Off the Land (LOTL) Techniques**: Attackers are increasingly using built-in tools and vulnerabilities to avoid detection and maintain access. By exploiting built-in administrative tools and processes already present in the victim's network such as PowerShell or Windows Management Instrumentation (WMI), attackers camouflage their activities to blend seamlessly with legitimate operations. This technique reduces the likelihood of detection by traditional security mechanisms and are increasingly used to compromise critical infrastructure.

For New Zealand, our proximity to Australia and shared geopolitical interests means similar risks, particularly to critical sectors like energy, healthcare, and government services.

2. Prepare for AI-Driven Threats

Artificial Intelligence (AI) is a double-edged sword in cybersecurity:

- **Attackers Using AI**: Expect AI-powered phishing campaigns and deepfake-driven identity theft to surge, creating more sophisticated scams and bypassing traditional defences. For example, AI-generated voice spoofing has been deployed in vishing attacks, while deepfakes are increasingly used for fraud and identity theft. AI also aids adversaries in vulnerability research, code development, and automating reconnaissance, enabling quicker and more targeted exploitation.
- **Defenders Leveraging AI**: Organisations must adopt AI-enabled tools for anomaly detection, threat hunting, and rapid response. These tools can help mitigate human error and improve efficiency.

3. Secure Critical Systems Before the Break

The holiday season is prime time for cyberattacks due to reduced staffing. We recommend the following measures:

- **Implement Multi-Factor Authentication (MFA)**: Protect critical accounts and systems with phishing-resistant MFA to reduce the risk of credential compromise.
- **Patch Known Vulnerabilities**: Ensure all systems, including legacy infrastructure, are updated to address publicly disclosed vulnerabilities.
- **Monitor for Abnormal Activity**: Use AI-driven tools to detect unusual behaviour and respond swiftly, especially in critical sectors like healthcare or utilities.

4. Strengthen Incident Response Planning

Preparation is crucial for mitigating the impact of a cyber incident. Focus on the following activities:

- **Develop and Test Incident Response Plans**: Simulate potential scenarios such as ransomware attacks or phishing campaigns to ensure all team members understand their roles.
- **Backup Critical Data**: Regularly back up important data and ensure backups are offline, tested, and secure.
- **Engage Key Partners**: Collaborate with cybersecurity professionals and government agencies like CERT NZ to stay informed about emerging threats and available resources.

5. Build a Cyber-Resilient Culture

Long-term cybersecurity requires a proactive approach. Consider the following actions to future proof your organisation:

- **Train Staff**: Educate employees about recognising phishing attempts, securing devices, and reporting suspicious activity. Access our learning management system here.
- **Adopt "Zero Trust" Models**: Implement least privilege access and continuously verify users and devices within your network.
- **Plan for Quantum Security**: Begin considering post-quantum cryptography to future-proof systems against evolving threats. NIST has finalised its principal set of encryption algorithms designed to withstand cyberattacks from a quantum computer.

6. Plan for 2025: A Secure Start

Looking ahead, organisations should prioritise:

- **Cyber Governance:** Implement a suitable framework such as the CIS Controls, measure your current security maturity and continually improve.
- **Cloud Security**: With the increasing adoption of cloud services, ensure robust security configurations, regular audits, and identity management protocols are in place.
- **Supply Chain Security**: Vet third-party vendors and implement strategies to mitigate risks arising from their potential vulnerabilities.
- **Regular Updates to Protocols**: As cybercriminals innovate, so must your defences. Regularly review and refine your cybersecurity policies.

Staying Vigilant During the Holidays and Beyond

While the Christmas season is a time to relax, it is also a time to remain vigilant. By understanding the threat landscape, leveraging AI, securing critical systems, and fostering a culture of resilience, New Zealand organisations can enjoy peace of mind during the holidays and start 2025 on solid ground. Cybersecurity is a shared responsibility—stay informed, prepared, and proactive.

For more guidance, visit CERT NZ or connect with cybersecurity partners who can help secure your operations this holiday season and beyond.

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: