NZ Incident Response Bulletin

Standard Edition – January 2022

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.

Refer to our Premium Edition for additional information on Threat Alerts, Security Frameworks, Information Security Surveys, Forensic News and Research.

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

Health Ministry data deal aims to protect hospitals from cyber attacks

The Health Ministry has made a $45 million-a-year data deal to help protect hospitals from cyber-attacks. At the same time, it has launched a strategy to improve the way health data is collected, managed and shared. The ministry said the three-year deal with Microsoft delivered $27m in savings. It should lead to increased deployment of cyber security technology across health agencies "which will improve protection and resilience to cyberattacks". The deal draws the ministry, the incoming national health agencies and DHBs under a single national contract for the first time. "Technology is a key enabler for the reforms and these arrangements give Health New Zealand and the Māori Health Authority the tools they need right from the start," the ministry said.

Police urge public to be vigilant this summer amid cybercrime and theft rise

A woman unknowingly ending up with $100,000 worth of debt is just one example of the cybercrime a Taranaki police officer is dealing with on a weekly basis. "She had no idea. The scammer had got two personal loans using her identity, had opened up a telephone account, and bought three iPhones," New Plymouth sergeant Terry Johnson said.

He said people are more likely to suffer a cyberattack than any other type of crime, with New Plymouth officers receiving an average of 10 cybercrime reports each week. Nationally, 7,809 incidents were reported to CERT NZ, New Zealand's cybersecurity response network, in 2020, which was a 65 per cent increase on 2019.

Review prompts police to halt plans to use facial recognition technology

Police are pressing pause for now on using facial recognition technology to identify people off live camera feeds, but will still use it on stored footage. They have spent multi-millions increasing their high-tech powers in the last two years, but have agreed with the first-ever independent review of their use of facial recognition that they should now take a breath. "Police will not use live automated FRT [facial recognition technology] until the impact from a security, privacy, legal, and ethical perspective is fully understood," said deputy chief executive Mark Evans.

The police-commissioned review by two leading critics of this country's lax laws around digital surveillance, Nessa Lynch and Andrew Chen, found "no evidence" police had been using the technology live. However the pair warned it would impact Māori the most if they do, and perhaps constitute an unwarranted search in a public place - and police should consult lawyers before taking that path. "Monitoring of protests or community events with live automated FRT [as has happened in the UK] could have a chilling effect on rights to freedom of expression and peaceful assembly," Lynch and Chen wrote.

NZ Incident Response Bulletin

Standard Edition – January 2022

World

New cyber vulnerability poses 'severe risk,' DHS says

Late Saturday, the Department of Homeland Security Cybersecurity and Infrastructure Security Agency (CISA) issued an urgent statement about a new cyber vulnerability that could touch a wide swath of the internet. "This vulnerability, which is being widely exploited by a growing set of threat actors, presents an urgent challenge to network defenders given its broad use," CISA Director Jen Easterly said in a statement.

"To be clear, this vulnerability poses a severe risk," Easterly said. The vulnerability is linked to a commonly used piece of software called Log4j, a utility that runs in the background of many commonly used software applications. "It's probably one of the most ubiquitous software components on the internet today," Tony Turner, VP of Security Solutions for the cyber-security company Fortress, told ABC News. Turner said the vulnerability impacts everything from gaming systems and consumer platforms to critical infrastructure and the Department of Defense. "Why this is so important is it is trivial to exploit," Turner said. "Anyone can do this, like teenagers and kids are playing around with this [vulnerability] like it's a game."

Dozens of Norwegian newspapers go unprinted after cyber attack on systems

Operations at a Norwegian local news publisher came to a halt this week after a major attack was launched on its computer systems. The 78 newspapers owned by Amedia could not be printed on Tuesday after its network was taken offline by the breach. The company said most of its titles were finally published on Friday, after several days of delays. Amedia said that its online news operations were unaffected, but that personal data belonging to employees may have been accessed during the attack. The firm said it was not clear whether any data has actually been extracted, but that police were investigating. “The question of the hackers' identity and other questions related to the investigation is handled by the police,” the firm said in a statement on its website.

As Ukraine crisis heats up, so will cyberattacks, experts warn

Biden administration says it's prepared to send weapons and increase military training efforts in Ukraine. Western nations, including Canada, should brace themselves for the possibility of more cyber and ransomware attacks if current tensions between Ukraine and Russia become worse — or even explode into open warfare early in the new year.

While Moscow likely would not sanction direct, attributable attacks on NATO members, experts say it would almost certainly use its vast cyber and disinformation capabilities to sow confusion and disaccord among Ukraine's closest supporters and allies during a crisis. "I think they could expect high-level cyberattacks just short of Article 5, just short of war, whether or not Putin goes into Ukraine," said Matthew Schmidt, an associate professor and national security expert at the University of New Haven, Connecticut. "That has become a constant background fixture of modern warfare. It's going on now."

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

10 December 2021 – Log4j RCE 0-day actively exploited

News Clips

14 December 2021 - New cybersecurity flaw shows vulnerability in 'LOG4J,' which poses risk to thousands of products

NZ Incident Response Bulletin

Standard Edition – January 2022

Our Views

Looking back on 2021

In 2021, we saw a range of high-profile cyber-attacks impact some of New Zealand's most significant organisations. Cyber threats continued to increase, and the risks and impacts of cyber-related crime continued to escalate. The NCSC reported a 15% increase in incidents impacting nationally significant organisations and highlighted ransomware, DDoS, data theft, and supplier vulnerabilities as problematic areas. The attack technique observed most was vulnerability scanning, with adversaries most commonly gaining unauthorised access to networks by exploiting public-facing applications.

2021 saw small businesses and individuals most impacted by phishing and credential harvesting, which increased in frequency by 73% in the third quarter of 2021, no doubt fuelled by COVID lockdown challenges. Malware incidents, however, also more than tripled for this sector, according to CERT NZ.

Our experiences on the ground echoed those reported above and notably highlighted the importance of credible threat intelligence and remaining vigilant with vulnerability scanning, patching and updates. Gaining clear visibility over where critical data is held and who can access it remains vital, along with preparing for the potential impacts of supply chain vulnerabilities by reviewing your supplier relationships and strengthening your incident response capabilities.

Overall, a greater focus on privacy legislation in 2021 required businesses impacted by a potential cyber incident to ensure they minimised the potential harm to customers of any data breach. This necessitated more use of tools such as dark web credential monitoring and professional public relations advice.

Our Response

In response to the increasing threat landscape, we introduced several new tools last year to better support New Zealand businesses navigate and lower their cyber risk. Each of our team members has nominated one initiative from 2021 they felt will most help combat these increasing threats:

Benoit Lagae: Dark Web Data Leak and Credential Monitoring

When Auckland went into lockdown, we used this as an opportunity to expand our Dark Web tools and capabilities. One area we identified as significant was the rate at which ransomware gangs were posting stolen data onto dark web data leak sites. In response to the growing threat these sites pose, we developed an automated software solution and accompanying procedure to monitor these sites for the presence of client data. We continue to grow and adapt this solution as the threat landscape changes, ensuring our clients are promptly notified if any of their data is found, so that the risk of any compromised data being used for crime is reduced.

Conor Clancy: Electronic Cyber Incident Control Room

Launching our cloud-based electronic incident control room has been a highlight of 2021. It has proved its usefulness in concurrently managing a vast number of cyber incidents, including the Microsoft Exchange compromises earlier in the year. Our retainer clients have instant, pre-configured access to incident response plans and playbooks for immediate use, which has greatly increased the efficiency with which cyber incidents can be managed within the context of their organisation.

Ash Payne: NIST and CIS Controls Assessment

Assessing cyber maturity against the NIST cyber security framework and the CIS controls enabled many of our clients in 2021 to create and act on plans to improve and strengthen their cyber and forensic postures. We have simplified this process, creating a tool that is easy to understand, making improvement initiatives more accessible to all organisations. If our clients can make small, continuous improvements using these tools as a guide, then ultimately, they will all be safer.

NZ Incident Response Bulletin

Standard Edition – January 2022

Campbell McKenzie: Data and Privacy Breach Reviews

For 20 years, I have been involved in many of New Zealand's most complex legal matters where we have utilised leading forensic and e-Discovery software. With the rapid rise in data and privacy breaches, along with the change in the regulatory landscape, we have expanded our review tool offering. We are now proud to offer a full suite of specialist data and privacy breach tools, including 'Nuix Discover', 'RelativityOne', 'Magnet Review', 'Reveal' and most recently, 'Canopy'. Read more at our forensic tech microsite here.

Nicole Girvan: Expanded Cyber Incident Simulations

Many valuable learnings came out of our cyber incident simulations in 2021. These exercises test decision making in highly ambiguous situations and are great for preparing to respond to cyber incidents. They help identify gaps in your current plans and strategies. To enhance the outcomes of these events, we have recently streamlined the planning and delivery processes and introduced some quantitative metrics to the assessment portion of the event. As a result of undertaking a simulation, organisations can now gain further insights into how well they are responding against recognised frameworks.

Predictions for the new year ahead

2022 is looking to be another year of uncertainty, with the global pandemic still disrupting markets, supply chains and daily working life. It is challenging to predict how cybercriminals will respond; however, it is reasonable to expect cybercrime to continue increasing. Where and how? Some crystal ball thoughts are below:

Ransomware: US law enforcement has started to come down heavily on ransomware gangs. While some commentators believe this will drive the big gangs underground and reduce this issue, we think ransomware will remain a core issue in 2022. Ransomware gangs will look further afield from their usual hunting grounds to places such as New Zealand (considered by some as a "soft" target) to continue gleaning profits from well-tried and tested business models.

Possibilities for how ransomware may present in 2022 include:

- Ransomware gangs potentially targeting more cloud environments (cloud platforms and software-as-a-service environments). Vulnerabilities in the cloud (e.g. Azurescape and OMIGOD) create an opportunity for the development of exploits beyond Windows, instead using Linux and cluster-based ransomware to target the cloud.
- Ransomware gangs targeting IoT devices and networks.
- Further use of tactics such as data leak, reputation and the direct targeting of customers to ensure ransom payment.

Supply chain attacks: After the success of the SolarWinds attack and the Kaseya breach, attackers may leverage similar successful strategies (for example, DeadRinger) to extend the reach of supply chain attacks in 2022.

Attacks on Operational Technology: Whilst the operational systems were not impacted by the Colonial Pipeline Attack in 2021; it certainly highlighted the vulnerability of interconnected OT and IT environments. As it is unlikely that OT systems will catch up with IT regarding modern infrastructure, cybersecurity protections, and monitoring, they will continue to remain vulnerable to cyber threats and require strong oversight in 2022.

Business Email Compromise, Fraud, Malware: With 2022 likely bringing another year of increased remote working requirements, pandemic scares, and economic uncertainty, we expect the "same-old" attack methods to continue to pester users. Malware will continue to become more sophisticated, and individuals will continue to be targeted by social engineering schemes and credential theft.

Regulation and Industry: We believe both government and industry bodies will continue to increase pressure on organisations to lift their cyber security resilience and prove they are protecting their clients to the best of their ability in 2022. This may be seen by way of enforcing privacy act regulation or specifying new requirements for professional practices such as performing yearly cybersecurity simulations or adopting a recognised cybersecurity framework.

NZ Incident Response Bulletin

Standard Edition – January 2022

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.

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: