NZ Incident Response Bulletin

Standard Edition – May 2021

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.

Upcoming Events:

Techweek	ITx - Tech Conference	

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

Reserve Bank Publishes Cyber Resilience Guidance

The Reserve Bank of New Zealand (RBNZ) has released the finalised version of its guidance on cyber resilience for its regulated entities. The guidance contains the regulator's expectations regarding cyber resilience, drawing from national and international standards and best practices on cybersecurity. This applies to all financial institutions under the purview of the Reserve Bank, including banks, insurers, non-bank deposit takers, and designated financial market infrastructures.

'It's an arms race': The Kiwi cyber firm that shielded Biden's home state during 2020 election

The 2020 US Presidential Election had the highest voter turnout in 120 years. Widespread fear of foreign interference coupled with Donald Trump's war against the news media had created a storm of suspicion and conspiracy theories that would eventually result in an attempted insurrection at the US Capitol. RedShield – a Kiwi cybersecurity firm based in Wellington – stepped straight into this maelstrom. Redshield was charged with protecting the security of the online infrastructure of Delaware, the home state of Democratic challenger and now-President Joe Biden. Screens constantly monitored for spikes in malicious activity and attempted hacks, but his team was on the lookout for molehills rather than mountains. The real threat was small attacks hidden among the noise.

NZ Government accelerates move to SaaS with TechnologyOne

The Ministry of Business Innovation and Employment has announced a new procurement framework with TechnologyOne that will pave the way for 23 New Zealand government agencies to transition to modern and secure Software-as-a-Service environments. The new streamlined procurement arrangements will offer stronger cybersecurity options and improve services to citizens by allowing agencies to be more flexible and innovate more quickly.

Security guards photographing public becoming increasingly common

The security industry says security guards are increasingly using smartphones to photograph incidents while on patrol. Security Association chief executive Gary Morrison said photographs were helpful for providing supporting evidence for incidents. "The security industry more and more frequently uses smart technology to take photos as evidential backup to the reports that they provide". Smartphone technology had improved rapidly, and firms should get legal advice about taking and storing photographs to make sure they were acting within the law." Wellington lawyer Amanda Hill, who specialises in privacy issues, said the incident in Auckland possibly breached the Privacy Act.

NZ Incident Response Bulletin

Standard Edition – May 2021

World

Cyber-attack hackers threaten to share US police informant data

Washington DC's Metropolitan Police Department has said its computer network has been breached in a targeted cyber-attack. A ransomware group called Babuk is reportedly threatening to release sensitive data on police informants if it is not contacted within three days. According to the Washington DC police department, the FBI is investigating the extent of the breach. Ransomware is used to scramble computer networks and steal information. Attackers target companies or organisations and can lock their systems, then demand large sums of money in return for ending the hack.

Should firms be more worried about firmware cyber-attacks?

Computing giant Microsoft recently put out a report claiming that businesses globally are neglecting a key aspect of their cyber-security - the need to protect computers, servers and other devices from firmware attacks. Its survey of 1,000 cyber-security decision makers at enterprises across multiple industries in the UK, US, Germany, Japan and China has revealed that 80% of firms have experienced at least one firmware attack in the past two years. Yet only 29% of security budgets have been allocated to protect firmware. However, the new report comes on the back of a recent significant security vulnerability affecting Microsoft's widely-used Exchange email system. The computing giant launched a range of extra-secure Windows 10 computers last year that it says will prevent firmware from being tampered with.

New cyber security laws to protect smart devices amid pandemic sales surge

The UK's Department for Culture, Media and Sport (DCMS) has added smartphones to its Secure by Design plan. Makers of Internet of Things, including smartphones, tablets, and other gadgets will be required to disclose to its customers, when they plan to stop providing security support for its devices. Makers of smart devices will also be prohibited from publishing default admin passwords for those devices. They will also have to offer a single point of contact for reporting vulnerabilities and obtaining updates. DCMS is pushing for Secure by Design to become law.

A Ransomware Gang is Now Shorting Stock Price of its Victims

Darkside ransomware operators have changed their extortion tactics and are now targeting organisations listed on stock markets. They believe that the negative impact of having a Listed organisation's name listed on their website would cause its stock price to fall, and the attackers are trying to make a profit out of this.

Expert cyber cohort call out on ransomware

Aggressive nationally and internationally coordinated strategies are needed to tackle the growing threat of ransomware, according to an expert taskforce that included the US, UK and Canadian government cyber agencies. A coalition of global experts assembled by business group, the Institute for Security and Technology (IST), on Thursday released a strategic framework for combating ransomware, which has quickly grown into a "serious national security threat and a public health and safety concern". "This global challenge demands an 'all hands on deck' approach, with support from the highest levels of government," the IST report said.

Summary of last month's Cyber Alerts:

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.

2 April 2021 – FBI-CISA Joint Advisory on Exploitation of Fortinet FortiOS Vulnerabilities

NZ Incident Response Bulletin

Standard Edition – May 2021

Our Views:

This month's theme is "Mobile Device Forensics".

Research suggests that there are now more active mobile devices on Earth than people. Mobile devices such as smart phones and tablets are commonly used to save personal information such as contacts, photos, notes, messages, video, and email. They are also increasingly used for work purposes, to store and transmit corporate information and facilitate online transactions.

This usage results in a rich source of data that may be used as forensic evidence when investigating incidents such as intellectual property theft, harassment and inappropriate social media activity. Collecting data from these devices in a defensible manner is critical when later examining the data to establish activities, timelines, and the intent of the user for forensic purposes. Mobile device forensics is a field aimed at recovering digital evidence in a forensically sound manner. This field has evolved quickly in line with the growing proliferation of mobile devices.

Mobile device evidence can be extremely detailed and the amount and types of different data that can be found is increasing. Evidence may come from various sources such as the local handset memory, attached memory cards or the SIM card. A non-exhaustive list of data that can be recovered from a mobile device and used as evidence includes:

SMS and MMS messages
Instant Messaging
Call logs (incoming, outgoing, missed)
Contact Lists
IMEI/ESN information
Web Browsing artefacts
Wireless Network settings
Geolocation information
Images and video
Emails and attachments
Documents
Stored payment data
Online portals
Social Networking Posts and Contacts

We have found that the examination of mobile devices in an investigation often provides crucial information pertinent to the inquiry and should never be overlooked. These devices can also present unique technical challenges when trying to obtain digital evidence. Examples of the opportunities and challenges that exist when examining a mobile device include:

Fast pace of technology change - Manufacturers are updating their systems at an astounding pace. This creates new streams of evidence, but makes that collection and examination more complex, including the operating system and mobile application data. Ensuring all data sources are identified and located is critical for successful retrieval.

Data Synchronisation – Mobile devices store a lot of data, but also connect with data located in the 'cloud'. Again, this additional data can create a new source of evidence, but care is required to obtain this, both legally and technically. For example, social media information that may have been created on a mobile but since deleted, may still reside in the cloud service. Also, a similar situation can arise when a social media post has been deleted from the cloud, but may be still recoverable from the mobile device.

Large volumes of data - Mobile devices commonly have around 64 Gigabytes or more of data storage, which is equivalent to 33,500 reams of paper. This volume of data potentially offers more detailed evidence.

Constant connectivity and activity - Mobile devices and tablets use an "always-connected" operandi. They hibernate, suspending services when idle whilst remaining active, however a significant number of activities may still be creating data in the background even when they are seemingly inert.

Advanced security features - Security functions on mobile devices are evolving and many contain features such as remote wiping. Care must be taken not to trigger these security features and destroy any potential data and evidence the device holds.

Specialised Tools - No single forensic tool can be relied on to guarantee that all data is collected from any given mobile device. We recommend using specialised commercial tools to assist in the mobile forensic process. Certain tools enhance the ability to obtain a robust set of data and offer significant advantages to obtain critical information on many device models. Advanced automated tools can also recover artifacts that may be unknown to the investigator or typically difficult to find.

As mobile devices have become a common business tool, the data they hold can be crucial to uncovering the facts surrounding any given incident. Careful handling of these devices in each stage of the process is required to ensure any possible evidence is forensically maintained. Whilst challenges exist when retrieving data from mobile devices, our experience confirms that when approached correctly, results derived from mobile forensics can be invaluable to any investigation.

NZ Incident Response Bulletin

Standard Edition – May 2021

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

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: