NZ Incident Response Bulletin

Standard Edition – February 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:

Securing NZ's Borders, Facilities & Public Spaces	New Zealand Cyber Security Summit	AppSec New Zealand 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

Global Regulators Taking A Hard-line Approach to Data Protection, Finds Law Firm DLA Piper

Although New Zealand's new Privacy Act 2020 does not give the Privacy Commissioner here the power to issue fines as significant as those available to European and UK regulators, New Zealand's introduction of mandatory data breach reporting means businesses are on notice. They should be watching keenly how breach notifications are dealt with in jurisdictions with more established data breach reporting regimes.

Kiwi identity theft: How much is your identity worth on the dark web?

The hacked credit card of details of New Zealanders sell for just US$7 (NZ$9.75) on the dark web, a report from technology research company Comparitech claims. That price rises to about US$20 when the bare card details are accompanied by full personal information including the name, address, email address, date of birth, the card's expiry date and security number. The most common ways data was stolen for sale was through email phishing, hacking of organisations and card skimming on ATMs.

World

Europe, American cyber cops disrupt possibly world's largest cybercrime network

European and North American cyber cops have joined forces to disrupt what may be the world's largest network for seeding malware infections. The operation appears to strike a major blow against criminal gangs that have used that network for years to install ransomware for extortion schemes and to steal data and money.

World's largest dark web marketplace shuttered after Euro cybercops cuff Aussie

Europol has taken down dark web marketplace "DarkMarket", after arresting an Australian citizen living in Germany who they claim was operating the world's biggest online bazaar of its kind.

Europol announced that DarkMarket had nearly 500,000 users and more than 2,400 sellers, calling it the "world's largest illegal marketplace on the dark web." The site sold a range of illegal goods including drugs, counterfeit money and credit cards, cloned SIM cards and malware.

NZ Incident Response Bulletin

Standard Edition – February 2021

Hackers bypassed MFA to access cloud service accounts

The US Cybersecurity and Infrastructure Security Agency (CISA) has reported that threat actors bypassed multi-factor authentication (MFA) protocols to compromise cloud service accounts. CISA is aware of several recent successful cyberattacks against various organisations' cloud services. The cyber threat actors involved in these attacks used a variety of tactics and techniques - including phishing, brute force login attempts and possibly a 'pass-the-cookie' attack - to attempt to exploit weaknesses in the victim organisations' cloud security practices.

Anti-Secrecy Activists Publish a Trove of Ransomware Victims' Data

For years, radical transparency-focused activists like WikiLeaks have blurred the line between whistle-blowing and hacking. Often they have published any data they consider to be of public interest, no matter how questionable the source; but now one leak-focused group is mining a controversial new vein of secrets: the massive caches of data stolen by ransomware crews and dumped online when victims refuse to pay.

Today the transparency collective of data activists known as Distributed Denial of Secrets (DDoSecrets) published a massive new set of data on its website, all collected from dark web sites, where the information was originally leaked online by ransomware hackers. DDoSecrets has made available about 1 terabyte of that data, including more than 750,000 emails, photos and documents from five companies. The group is also offering to privately share an additional 1.9 terabytes of data from more than a dozen other firms with selected journalists or academic researchers. In total, the giant data collection spans industries including pharmaceuticals, manufacturing, finance, software, retail, real estate and oil and gas.

Attacks targeting healthcare organizations spike globally as COVID-19 cases rise again

At the end of October 2020, Check Point reported that hospitals and healthcare organisations had been targeted by a rising wave of ransomware attacks, with the majority of attacks using the infamous Ryuk ransomware. Unfortunately, that cybercrime threat has worsened over the past two months. Since the start of November, there has been a further 45% increase in attacks targeting healthcare organisations globally. This is more than double the overall increase in cyber-attacks across all industry sectors worldwide seen during the same time. The rise in attacks involves a range of vectors, including ransomware, botnets, remote code execution and DDoS attacks. Ransomware attacks against hospitals and related organisations are particularly damaging, because any disruption to their systems could affect their ability to deliver care and endanger life.

Judiciary Addresses Cybersecurity Breach: Extra Safeguards to Protect Sensitive Court Records

After the recent disclosure of widespread cybersecurity breaches of both private sector and government computer systems, federal courts are immediately adding new security procedures to protect highly sensitive confidential documents filed with the courts. Under the new procedures announced today, highly sensitive court documents (HSDs) filed with federal courts will be accepted for filing in paper form or via a secure electronic device, such as a thumb drive and stored in a secure stand-alone computer system. This new practice will not change current policies regarding public access to court records, since sealed records are confidential and currently are not available to the public.

Hackers 'manipulated' stolen COVID-19 vaccine data before leaking it online

Hackers who stole information about COVID-19 vaccines in a cyberattack against the European Union's medical agency and then published it online also manipulated what they found in order to spread disinformation designed to undermine trust in vaccines. In the latest update on the cyberattack that was first disclosed last month, the European Medicines Agency has revealed how hackers accessed confidential internal emails from November about evaluation processes for COVID-19 vaccines.

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.

6 January 2021 – Mitigate SolarWinds Orion Code Compromise – Supplemental Guidance v3

28 January 2021 – CISA guidance: reducing the risk of ransomware

NZ Incident Response Bulletin

Standard Edition – February 2021

Our Views:

This month's theme is "Staying calm in a cyber crisis".

It is hard to remain calm when a crisis descends. Physically your body responds with hormonal and physiological changes as if it is under threat. These changes are designed to help you act quickly by increasing your heart rate and oxygen flow to your muscles, sharpening your hearing, making you sweat and dropping your perception of pain. All actions that are intended to support a "fight or flight" response.

Whilst the stress hormones released under pressure are great if you need to run fast from a dangerous situation, they are not so relevant when facing a modern-day cyber incident. Cortisol and Adrenaline slow our thought processes and hinder our ability to analyse complex information. Making the critical decisions required to respond effectively to a cyber incident becomes more challenging and it is important to understand that fight, flight, and sometimes freeze are automatic responses to perceived danger and controlling these is extremely difficult. A fox and a cat discuss their strategies for evading hunting dogs in a well-known Aesop's fable. The fox boasts of many techniques, whereas the cat confesses to only having one option. When the hunting dogs arrive, the cat runs up a tree whereas the fox is overcome by choice and freezes before being caught. This tale highlights that when responding to a crisis having a plan works. The cat clearly knows what to do when disaster hits, follows the plan and responds quickly and without hesitation for a successful outcome.

In a cyber incident, having a tested Cyber Incident Response (IR) plan is vital. An IR plan outlines clear overarching measures an organisation should take to reduce the impact of any breach. Having a documented plan prevents "knee-jerk" actions, protects a business's assets in order of criticality and expedites detection, mitigation, remediation and recovery actions. It also reduces the number of decisions a responder must make ensuring that "analysis paralysis" or the fate of the fox in Aesop's fable is avoided. Another key tool that supports an overarching IR Plan is the development of specific playbooks. Being prepared to respond to a cyber incident involves thinking through the potential cyber threats specific to your business and developing a detailed game plan for each of these. We recommend that New Zealand organisations should adopt playbooks (either templated or tailored) for Business Email Compromise, Ransomware, and Privacy Breach threats, as a minimum.

Effective teamwork and communication are also critical factors for a successful response strategy. All team members should be aware of their individual responsibilities during a crisis and everyone must work together towards a common goal. Events move fast during a cyber crisis and often a response to a large incident may run over days and weeks. The members that make up the crisis team may change to allow rest and recuperation, noting that changes to team members poses its own unique challenges when maintaining clear communication and ensuring everyone is up to date.

To maintain consistency, we recommend setting up an electronic IR control room well before it is needed, to facilitate any crisis. A Kanban board can be used that follows the IR plan and playbooks, capturing updates, actions and blockers from all participants in real-time, therefore improving situational awareness and facilitating the coordination of effort. With some preparation, electronic tools such as Microsoft Teams can be used to set this up and provide a common operating picture for all major cyber incidents. When everyone feels informed and can see active progress on actions, a greater sense of control is enabled and panic is less likely to set in.

To quote Captain Sullenberger who landed his stricken aircraft on the Hudson river, "a sense of calm is rooted in confidence". Preparation is the primary way in which to gain the confidence to maintain this calm. In addition to preparing and testing your IR plan, playbooks and control room; you should also identify any skills gaps and gain the required knowledge, which will reduce the risk of making the wrong decisions whilst under pressure. It is important to strongly prioritise actions, break down any problem into manageable chunks and concentrate on the most critical tasks first. Once the first steps are taken, subsequent ones become a little easier. Additionally, use near-misses and small incidents as learning opportunities. Think about what you did well, what you could have done better and whether you reacted fast enough and had the necessary skills. Participating in cyber tabletop exercises is another structured way to test yourself and allow your skills to be sharpened in a safe environment.

You can maintain realistic optimism during a cyber crisis by being fully aware of the risks posed by a cyber incident and simultaneously confident that your skills, knowledge and the team around you will be able to address these risks. Delegate tasks appropriately, ask for help and take care of yourself to ensure you are optimally prepared to act. Maintaining calm during a cyber incident can be achieved with preparation, practice, and support.

NZ Incident Response Bulletin

Standard Edition – February 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: