NZ Incident Response Bulletin

Standard Edition – May 2020

In this issue:

News	Our Views	Upcoming Events
New Zealand	Remote Forensic Investigations	IBM - Think Digital
World		2020 NZ Cyber Security Summit

Premium Edition contains 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

Scam warning for online shoppers before move to Level 3

New Zealanders are being urged to remain vigilant when shopping online at Covid Alert Level 3. While under level 4 restrictions, online shopping was limited; however, scammers are poised to take advantage of the increase in online purchasing expected under level 3.

Fake or cloned websites of well-known brands exist that take shoppers personal details and credit card numbers and use them for performing identity theft. Large amounts can be charged to a shoppers card without any supply of goods. New Zealanders should keep an eye out for discrepancies in the company name or brand logo on a site and if suspicious, check if the company is registered with the New Zealand Companies Office. Registration of the website domain name can also be verified.

"Fake shopping websites and phishing emails set up to steal personal information and credit card details can look convincing" – Bronwyn Groot (Commission for Financial Capability).

In addition to keeping all shopping receipts, consumers should be wary of purchasing through sites of companies located overseas, as once money leaves New Zealand, it is almost impossible to retrieve. Google is reportedly blocking an additional 20 million coronavirus phishing scams per day, and the UK National Fraud and Security Centre has reported a 400% increase in cyber scams exploiting Covid-19.

We recommend visiting the 'Domain Name Commission – Detecting Fake Websites' for Security Awareness.

Coronavirus: New Zealand contact tracing app due within two weeks

In response to an audit that found New Zealand's contact tracing capabilities needed to be significantly increased, the Ministry of Health intends to launch a voluntary app to track the movements of people with Covid-19.

The Privacy Commissioner believes the government has followed robust processes to ensure any data collected by the app is used appropriately. The success of the app, however, will depend primarily on its level of trustworthiness and as yet clarification is still required from the government around how it will use the data it collects, who will be able to access this data and how long it will be retained.

Seven out of ten people surveyed support authorities using their mobile data for Covid-19 contact tracing; however, similar apps launched recently in Singapore and Australia, have had a mixed response from the public.

NZ Incident Response Bulletin

Standard Edition – May 2020

World

Shade Ransomware shuts down, releases 750k decryption keys

The operators of a significant ransomware strain (Shade Ransomware) have apologised for the harm they have caused their victims, handed over 750,000 decryption keys and shut down their business. Shade Ransomware has not been distributed since late 2019, which is good news for citizens of Russia and Ukraine, who were predominantly targeted by the strain. The team that created the ransomware trojan also claim to have destroyed all of the source code to prevent it from further use.

While the decryption process has not proved simple, it does work. Security Researchers have announced they plan to include the released master keys in their ransomware decryption tool to help ease the decryption process for impacted victims.

Department of Justice Announces Disruption of Hundreds of Online COVID-19 Related Scams

Federal authorities announced that an ongoing cooperative effort between law enforcement and a number of private-sector companies, including multiple internet domain providers and registrars, has disrupted hundreds of internet domains used to exploit the COVID-19 pandemic to commit fraud and other crimes.

As of April 21, 2020, the FBI's Internet Crime Complaint Center (IC3) has received and reviewed more than 3,600 complaints related to COVID-19 scams, many of which operated from websites that advertised fake vaccines and cures, operated fraudulent charity drives, delivered malware, or hosted various other types of scams. To attract traffic, these websites often utilised domain names that contained words such as “covid19,” or “coronavirus.” In some cases, the fraudulent sites purported to be run by, or affiliated with, public health organisations or agencies. For example, the cooperative effort has disrupted:

- An illicit website pretending to solicit and collect donations to the American Red Cross for COVID-19 relief efforts.
- Fraudulent websites that spoofed government programs and organisations to trick American citizens into entering personally identifiable information, including banking details.
- Websites of legitimate companies and services that were used to facilitate the distribution or control of malicious software.

Defence puts week between Citrix security notice and assessing recruitment network

The Australian Defence Force Restricted Network was taken offline and placed in quarantine for ten days in February amidst fears it had been hacked. The military database contains the personal details of tens of thousands of Australian Defence Force members.

The Australian Department of Defence started investigating this network, including monitoring for external reconnaissance and scanning attempts, one week after Citrix released an announcement that warned of a vulnerability. Several patches released by Citrix were all subsequently applied to Defence Application Delivery Controllers.

Australian Signals Directorate Penny Wong reports that she is not concerned by the one-week delay stating that organisations will often take a week or so to understand what is happening on their network. The Australian Defence Force also reports that extensive forensic analysis undertaken by the Australian Cyber Security Centre found no evidence that data was taken.

Cybercriminals increasingly using SSL certificates to spread malware

A recent report released by Menlo Security highlights the importance of decrypting Secure Sockets Layer (SSL) certificates and performing adequate SSL inspections. SSL certificates alone do not guarantee security. This is because SSL is now commonly used by cybercriminals. Malware sites, phishing domains, and command and control sites all utilise https. On-premise appliances usually undertake SSL decryption; however, many companies choose not to perform SSL decryption due to concerns over employee privacy or performance, thereby increasing their risk of suffering a breach.

The current working from home climate has also complicated security in this area, making the inspection of SSL certificates at times impossible. The report shows that many VPN infrastructures are currently stretched as they were only ever designed to cope with 1-5% of employees working remotely. This situation is leading to employees operating online without VPN security protection and companies losing all visibility of the traffic.

NZ Incident Response Bulletin

Standard Edition – May 2020

Our Views:

This month's theme is "Remote Forensic Investigations".

Remote working is now, and will be for some time, business as usual. This recent change to the way we operate has increased certain risks, whilst also posing new challenges when needing to conduct an investigation.

These risks should prompt businesses to think about how they would respond to any incidents requiring a forensic investigation.

Finding a balance between dependable investigative techniques and innovative new technology

Traditional forensic investigative techniques ensure the robustness of any case, and are critical to preserving evidence so that it can be presented in a court of law. However, new tools and technologies are required to remotely investigate incidents while ensuring compliance with "social distancing" and satisfying the greater need to search and collect evidence from remote devices. Visibility of the corporate network, which has now thoroughly expanded into employee's homes, has become critical.

Some of the specific challenges posed by the current environment include:

1. How can appropriate evidential standards for withstanding legal proceedings be maintained?
2. How will you obtain sufficient evidence of who committed an offence?
3. How can you balance a "thorough" investigation with the constraints imposed by remote working and lockdown?
4. How can you securely share data with lawyers, investigators and subject matter experts while maintaining physical distance?
5. How can you expedite investigations to save money?

We recommend a combination of a web based review platform that offers the latest document prioritisation tools. We summarise these below, and please feel free to contact us if you require further information.

Web based review platforms

There are number of reasons to shift your investigations into a web based review platform.

Not only does it provide physical and financial flexibility, but it also offers the latest review technologies.

Where possible, data can be neatly transferred from the source, e.g. web based email systems, into the review platform. This avoids the need to physically hand over electronic devices, whilst still maintaining the necessary chain of custody requirements.

Access to the review dataset (and subsets thereof) can be centrally managed allowing timely access to the appropriate people.

Certain tools also offer access via mobile devices, reducing the requirement to extract documents from the review platform when needing to share.

Continuous Active Learning

An investigation often begins with a small set of filters comprising keywords, individual and date ranges. This task becomes more difficult when there is a large dataset.

Consider the use of the latest review technology, 'Continuous Active Learning' (CAL).

CAL constantly reprioritises your review queue within the dataset based on your ongoing review decisions, therefore presenting you with documents that are most likely to be relevant within the context of your investigation. With CAL you can potentially identify 90% of the most relevant documents, by reviewing only 20% of them.

When considering current physical and financial constraints, it is possible that investigations may be comparatively scaled back. We therefore recommend that consideration be given to adopting advanced technologies that can help you focus on what is important, whilst still applying the principles of natural justice.

NZ Incident Response Bulletin

Standard Edition – May 2020

Upcoming Events:

Date	Event	Location
6, 7 May 2020	IBM - Think Digital	Online
14 Oct 2020	2020 NZ Cyber Security Summit	Te Papa, Wellington

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.

Share our Bulletin: