NZ Incident Response Bulletin

Standard Edition - December 2019

In this issue:

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

Cyber Threat Report for 2018/19 released

The National Cyber Security Centre (NCSC) has released its Cyber Threat Report for the 2018/19 reporting year. Director of the NCSC, Lisa Fong, says while the number of incidents recorded by the NCSC in 2018-19 is similar to the previous year, the impact of those incidents has been greater. The NCSC recorded 339 incidents in the 12 months to 30 June 2019, compared with 347 incidents in the previous year.

"The NCSC was able to identify indicators linking state-sponsored cyber actors to 38 percent of total incidents recorded in 2018-19. In 2018-19 more incidents were detected at a later (post compromise) stage in the threat cycle, when actors have been able to establish their presence on a network and potentially have an effect on it. State-sponsored cyber activity is generally more sophisticated than criminal or non-state activity, a reflection of the greater resources state-based actors usually have," Ms Fong says.

"The incidents recorded by the NCSC represent a small proportion of the total cyber security incidents impacting New Zealand, as the NCSC's focus is on potentially high impact events and nationally significant organisations", Ms Fong says.

Wishing you a happy and safe Christmas holiday.
We'd like to thank you for your support during 2019 and look forward to 2020!

Campbell *Nicole* *Yair* *Bryan* *Ash*

NZ Incident Response Bulletin

Standard Edition - December 2019

[New Zealanders lose $23 Million to Scams]

Netsafe has released its latest figures as part of Fraud Awareness Week, indicating that New Zealanders lost almost $23 million as a result of scams and fraud this year. Further, the sophistication level of the scams seen in New Zealand continues to grow.

“It is clear from the reports we receive that scammers are taking the time to set people up often by using personal data available online…the simple message of 'if it seems too good to be true, it probably is' no longer reflects the reality of the online scam and fraud landscape.” says Martin Cocker, Netsafe’s CEO.

Product and services fraud was the biggest category of reported scam, with fraudsters using well-known brands in text or emails suggesting the recipient has won a prize or asking them to complete a survey.

World

[Labour Party hit by two DDoS attacks]

The UK Labour Party has confirmed that it has been hit by two cyber-attacks on consecutive days. Being this close to the general election, the labour leader Jeremy Corbyn says the incidents are “suspicious”.

It is believed the two attacks were distributed denial of service (DDoS) attacks. A DDoS attack aims to overwhelm servers, causing them to crash by directing large amounts of internet traffic to them. Criminal hackers use a network of compromised computers (via a botnet) to perform the attacks which are designed to interrupt an organisations ability to operate.

Whilst DDoS attacks are often used as a diversion to carry out a more serious attack, no sensitive information was breached in the attack. Additional security processes required to protect the systems were however slowing down campaign activity.

[Millions of accounts - including Kiwis' - compromised in huge internet registry breach; tips to keep safe]

Registrar.com, one of the largest companies that sell and manage internet domains has notified their customers of a breach involving both Register.com and a sister company Network Solutions. It is believed the intruders were potentially inside the systems for six weeks and information stolen included customer contact details such as names, addresses, phone numbers and email addresses.

To remain safe, the company is warning customers to monitor their credit card account for any suspicious activity and immediately change their passwords.

[Hackers Demand US$14M in Ransom to Unlock Systems in U.S. Nursing Homes]

Hackers have demanded US$14 million dollars from Virtual Care Provider, a technology services provider for nursing homes. The demand comes after a successful attack which infected their systems with the Ransomware strain known as “Ryuk”.

Over 80,000 systems including access to email, patient records, billing, payroll and phone systems have been affected by the ransomware, leaving 110 nursing homes unable to pay employees or order urgent medications.

Ransomware attacks targeting healthcare services is a growing concern. This attack comes after multiple ransomware attacks on hospitals and healthcare providers from both the US and Australia in recent months. Affected hospitals have cancelled surgeries and turned away new patients as a result of the attacks with some forced to shut down some operations.

NZ Incident Response Bulletin

Standard Edition - December 2019

Our Views:

A selection of issues relevant to Forensic and Cyber Security matters during the last month. This month's theme is "Enfuse Forensic and Cyber Conference 2019".

The Enfuse Conference was held at the Venetian Resort across four days in November 2019. Two members of Incident Response Solutions attended the event, which included a keynote from James Clapper, the Former U.S. Director of National Intelligence. Below is a selection of take-aways from the conference.

The effects of Emerging Technologies on Digital Forensics and Incident Response

This session provided forensic examiners and incident responders with an insight into 'MITRE ATT&CK™', a knowledge base of adversary tactics and techniques based on real-world observations. The focus of this resource isn't on the tools and malware that adversaries use, but on how they interact with systems during an operation. ATT&CK organises these techniques into a set of tactics to help explain to provide context for the technique. Each technique includes information that assists in understanding the nature of how a technique works and also to a defender for understanding the context surrounding events or artifacts generated by a technique in use.

Why the Legal Profession Must Rethink and Change its Approach to Data Security

Law Firms are not only subject to external attacks, but also insider threats through either careless or malicious actions by employees.

According to the 'ABA TECHREPORT 2019' from the American Bar Association, 26% of law firms experienced a data breach.

Law firms hold sensitive data which is valuable to cyber criminals, including information about corporate deals and strategic plans, intellectual property, litigation documents, and financial information such as trusts or conveyancing.

Research cites a lack of documented policy, inferior technology, no formal training programs, poor management and a failure to monitor and detect threats as reasons why law firms may fall victim to a cyber-attack. The ABA has introduced new model rules and opinions on how to combat this threat.

Keynote – James Clapper, Former U.S. Director of National Intelligence

Six years ago, at the same event, General Michael Hayden, a former Director of the National Security Agency and Central Intelligence Agency discussed the threats associated with leaking confidential information in the age of the Cyber War. One week later, Edward Snowden leaked information about the Prism program.

James Clapper detailed the emerging threat of weaponisation through social media. Such actions can lead to the influencing of elections and the general the decline of trust. He referred to the response to such threats as a 'global whack a mole game'.

Clapper advocated the need to thoroughly investigate any cyber-attack, learn from the intel gained, which should lead to a better defence the next time your organisation is attacked.

He also discussed his concerns around taking too much of a wide reaching response to insider threats, where systems are setup to try and 'catch' staff. He cited this type of action may reduce the loyalty of your staff.

Clapper concluded by saying that the US will be financially be paying the price of the Snowden leaks for many generations to come.

NZ Incident Response Bulletin

Standard Edition - December 2019

Upcoming Events:

Date	Event	Location
21 February 2020	OWASP New Zealand Day	Auckland
28 February 2020	CybersecCon	Auckland
3 – 4 February 2020	International Conference on Forensic Sciences and Law Enforcement	Melbourne, Australia

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

Share our Bulletin: