NZ Incident Response Bulletin

Standard Edition – August 2020

In this issue:

News **Our Views** **Upcoming Events**

New Zealand	The Insider Threat	Aotea Security - Security Risk Management Seminars
World		2020 New Zealand Cyber Security Summit
		3rd Annual National Cybersecurity Summit

The 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

Auckland pizza shop owner uncovers 'chargeback' fraud

A Domino's Pizza franchise owner noticed unusual items on a recent invoice. Money deducted from their account was being recorded as “chargebacks” at an unusual frequency. The customers confirmed the orders were real; however, further investigation found that they had all placed their orders through a third-party online advertising deal on WeChat, a popular social media platform.

The third-party was a scammer who was keeping the money paid by the legitimate customers and using other stolen bank details to pay Dominos Pizza for the online orders. As victims of the stolen bank details identified the fraudulent transactions, they notified their bank who organised a refund, recorded as a chargeback, from the retailer.

In summary, customers are using online discount offers to order food, which is then paid for by scammers using stolen bank details. Once discovered, the retailer has to absorb the cost of the fraud. The retail industry is warning customers to use legitimate company websites to purchase their products and to avoid third parties.

Should New Zealand internet addresses be for Kiwis only?

Currently, .nz domains are available to be purchased and held by anyone around the world. Globally the stance differs on this issue. For example, in Australia, a company is required to have a local business number before it can register a .com.au address. A recently formed panel is reviewing the InternetNZ policy currently and whether we continue to allow global ownership of .nz domains is one of the issues under review.

Offshore ownership of .nz addresses can make it harder for consumers to resolve legal disputes, and many New Zealanders may also not be aware that businesses with no New Zealand presence may own .nz domains. The other side of the debate, however, is financial. InternetNZ increased monthly domain-name fees by 20 per cent earlier this year. "Falling registrations are threatening our ability to offer the core security and co-ordination services which our market demands"- InternetNZ group chief executive Jordan Carter. InternetNZ may therefore not be able to afford to limit the purchase of .nz domains to New Zealand citizens only. Consultation on this issue is open now, and submissions are invited until 14 August 2020 here.

NZ Incident Response Bulletin

Standard Edition – August 2020

World

Microsoft takes legal action against COVID-19-related cybercrime

Microsoft has taken legal action against COVID-19-related cybercrime resulting in a court order allowing them to seize control of key domains in the criminals' infrastructure to stop them being used for cyberattacks. Cybercriminals have been performing a form of Business Email Compromise (BEC) by attempting to gain access to customer email, sensitive documents and other valuable or personal information using COVID-19 phishing lures in 62 countries.

The FBI has previously reported that BEC crimes are the costliest of all reported cyberattacks with losses of over 1.7 billion dollars reported in 2019 as a result of these schemes. The phishing emails used are sophisticated and designed to look as though they originate from a legitimate source. Business leaders are frequently targeted by these attacks in an attempt to compromise email accounts, steal information or redirect money transfers.

Recent BEC schemes have become even more clever and have been exploiting pandemic financial and health concerns such as including fraudulent links to "COVID-19 Bonus" information. Once clicked upon, the fraudulent links contain web apps that can enable access permissions to accounts such as the victims Microsoft Office 365. This kind of attack can enable unauthorised access to the victim's accounts without them ever explicitly entering their credentials into a fake website.

Microsoft has many measures in place to monitor and block malicious applications; however, when cyber activity scales up as quickly as it has in 2020 and attackers move quickly to evade their defence mechanisms, then legal action becomes a necessary tool. For end-users, protecting against these attacks involves enabling multi-factor authentication and learning how to spot phishing schemes and remediate these attacks.

US charges Chinese Covid-19 research 'cyber-spies.'

Officials in the US justice department have charged two Chinese men for allegedly spying on US companies involved in coronavirus research. They have also accused China of sponsoring the hackers and giving assistance to enable the theft of trade secrets. The US is currently cracking down on International cyber espionage, focusing particularly on China and Russia, who are both accused of spying in an attempt to steal COVID-19 research.

The Chinese men, who reside in China, face charges of trade secret theft and wire fraud conspiracy and are believed to have recently targeted various coronavirus labs and firms globally including targets in Australia, Belgium, Germany, Japan, Lithuania, the Netherlands, Spain, Sweden and the UK. The indictment states that the men "researched vulnerabilities in the networks of biotech and other firms publicly known for work on Covid-19 vaccines, treatments, and testing technology". It is also alleged that since 2009 they have stolen hundreds of millions of dollars worth of intellectual property, business information and trade secrets.

Twitter says about 130 accounts were targeted in cyber-attack

Twitter Inc has disclosed that hackers targeted about 130 accounts during a cyber-attack in July which led to the profiles of many prominent personalities and organisations being compromised. Impacted personalities included U.S. presidential candidate Joe Biden, reality TV star Kim Kardashian, former U.S. President Barack Obama, and billionaire Elon Musk. The corporate accounts of Uber Technologies Inc and Apple Inc were also impacted.

The attack aimed to use the accounts to solicit digital currency and publicly available blockchain records show the attackers may have received $100,000 or more of cryptocurrency as a result of the fraud. The FBI is leading a federal inquiry into the attack and subsequent information indicates that internal employees may have aided the attackers.

NZ Incident Response Bulletin

Standard Edition – August 2020

More than 1,000 staff and contractors at Twitter had the ability to help hackers hijack accounts, two former employees reveal

A further news article reports that more than a thousand employees of Twitter may have had access to internal tools that could enable the hacking attack perpetrated on Twitter. The tools enable a user to change user account settings and assign account control to others. Twitter has subsequently reported that the perpetrators of the attack "manipulated a small number of employees and used their credentials" to log into these tools and give the attackers access to 45 accounts.

Britain back-tracks on Huawei role in 5G high-speed network

Britain has decided to prohibit Chinese telecommunications company Huawei from working on the UK's new 5G high-speed mobile phone network citing security concerns after US sanctions made it impossible to verify the security of any equipment made by Huawei.

The US had also previously threatened to end an intelligence-sharing agreement with Britain as they were concerned that the use of Huawei technology may allow the Chinese government to infiltrate Britain's telecommunications networks. The US claims that the Chinese government could force Huawei to give it access to any foreign networks it has helped build under Chinese law. Huawei denies this claim and states that there are already oversight procedures in place in countries such as Britain to avoid this scenario and ensure no security breaches occur.

The decision not to allow Huawei any involvement in the 5G project will delay the technology rollout and may increase costs by up to two billion pounds however the culture secretary, Oliver Dowden has informed Parliament that it was necessary. "This has not been an easy decision, but it is the right one," he said.

British companies must stop purchasing Huawei equipment by the end of the year and remove all previously installed Huawei equipment from the network by 2027.

Our Views:

This month's theme is "The Insider Threat".

It is a reality that many crimes are perpetrated by someone known to the victim. Homicide detectives have stated that "Familiarity breeds contempt." Looking at recent studies, it appears that when talking about cybercrime and data theft in 2020, the same may apply.

The 2020 Cost of the Insider Threats Global Report released by the Ponemon Institute reveals that the number of insider threats has increased by 47% in two years. The cost of these incidents has also soared from $8.76 million in 2018 to $11.45 million US dollars in 2020. The threat report also finds that 68% of organisations feel vulnerable to insider attacks. This comes as no surprise considering recent news such as the Twitter leak where it appears that employees were manipulated into helping an attacker gain access to accounts, the case of the Yahoo veteran who narrowly escaped jail time after hacking into private accounts, and the misconfiguration of AWS S3 buckets that led to the exposure of victim information.

The events outlined above highlight both the serious and the varied threat that insiders pose. The name "insider threat" is also a misnomer as it refers to many different crimes, issues, situations, tactics, targets, industries and motivations which cannot all be handled under a one-size-fits-all policy or solution.

NZ Incident Response Bulletin

Standard Edition – August 2020

What is the Insider Threat?

Generally, the insider threat can be categorised in three main types:

1. Malicious insiders
   Malicious insiders are often employees, contractors or trusted partners who have legitimate access to the network but abuse this access for profit, revenge, or fun. Frequently they steal data and trade secrets either for profit or to leak to a competitor, another country or the media.

   Recent predictions suggest the tough economic environment being experienced globally as a result of COVID-19 will drive an increase in this type of threat as employees suffer pay cuts and employment uncertainty. A report into the impact of an economic recession on New Zealand policing in the next 6 to 12 months states that middle-class workers and small to medium-size business owners are now vulnerable. There are concerns that many who are unaccustomed to financial hardship may turn to crime or be exploited by criminal gangs. Large redundancies, such as those seen at a number of New Zealand companies, could provide an opportunity for organised crime groups to exploit vulnerable employees who have inside knowledge of an industry. The report predicts that online fraud may increase by as much as 30-100% and highlights businesses that "reprioritise their resource" and cut back on cybersecurity as being of concern.

2. Unwilling participants
   Unwilling participants are pawns who fall for a phishing scheme or execute a malicious macro or script. They may make a mistake such as losing a laptop or mistakenly sending an email to the wrong recipient that results in data loss, theft or financial and reputational harm to the business.

   Recent research from one security firm revealed that 43% of employees admitted making mistakes that led to cybersecurity incidents and 52% of employees said stress was the leading cause for these mistakes. Around 58% of employees have sent a work email to the wrong person. Distraction was cited as the primary reason for falling for a phishing scam.

3. System misconfigurations
   System misconfigurations or negligence are IT mistakes that lead to incidents such as leaving a web server unpatched. The COVID-19 pandemic has led to the rapid adoption of cloud collaboration tools for many businesses and increased the risk of configuration mistakes such as not setting appropriate access control on cloud storage or environments such as Slack. In 2018 researchers found that up to 80% of all AWS S3 buckets they inspected contained readable files.

Detection and Prevention

Defending against insider threats can be challenging as insiders often require an elevated level of trust and access to do their jobs, and may have the capabilities, privileges, knowledge and motivation required for a successful attack. Detecting an insider attack is also challenging, with many insider attacks remaining undetected for an average of 207 days in 2019. One security analyst recently reported forum references to "Twitter plugs" or "Twitter reps" – the terms used to describe cooperative Twitter employees appearing for several years before their recent hack. This highlights that the insider threat risk to Twitter was evident but undetected some time ago.

Several techniques, however, can help including:

Conducting Threat Assessments

A threat assessment can help you determine which type of insider threat is most applicable to your business environment and therefore, where to target your efforts. For example, combatting malicious insider threats require the implementation of strict security controls whereas the threats faced by unwilling participants may be mitigated with awareness campaigns and wellbeing programmes. This stage may also include establishing clear visibility of privileged users and accounts for easier monitoring.

Instituting Cyber Security Governance

Ensuring cybersecurity is governed from a clear vision and consistently managed throughout all levels of an organisation reduces the cyber risk in a business and helps builds a strong cybersecurity culture.

NZ Incident Response Bulletin

Standard Edition – August 2020

Monitoring Data, Activity and Network Traffic

Monitoring email, files and activity including using data protection systems to detect the exfiltration of sensitive data may assist in identifying and mitigating data loss.

Common signs of possible insider threat activity may include:

- The downloading or obtaining of large amounts of business or sensitive data
- Accessing data outside of job function or searching for sensitive data
- Requests or attempts to access resources outside of normal job function
- Using unauthorised devices such as unapproved laptops or USB storage
- Copying sensitive files
- Emailing sensitive data outside of the business
- Increased file activity in privileged folders
- Attempts to alter logs or delete large amounts of data

Security analytics can also alert on unusual behaviours such as those listed above.

Creating Least Privilege Policies

Limiting the access to sensitive resources and information such as Personally Identifiable Information, trade secrets, financial data, or intellectual property and allow people access to only what they need. Local administration rights can be locked down, and application whitelisting and blacklisting policies can help to block malicious software.

Implementing User Training, Awareness and Support

Ensuring all users (including IT) have appropriate training to undertake their roles and recognise security threats is key to avoiding unwilling participants and misconfiguration threats. Additionally, wellness programs and employee mental health support may help prevent workplace stress rising to levels where risk is increased.

Response and Recovery

Following an Incident Response Plan

Following a tailored Incident Response Plan that covers playbooks for specific insider threat scenarios will assist in a faster and more efficient response. Ensuring you have a communications plan in place to handle an event such as a data breach where you may be required to update customers, organisations such as the privacy commission and the media, is also vital.

Conducting an Investigation

If a breach is suspected, conducting a formal forensic investigation can determine the possible cause, breadth and impact of the incident. The use of advanced forensic tools can identify potential evidence relating to any incident for legal or employment proceedings. The potential recovery of sensitive data and evidence such as deleted social media posts can also be achieved with careful investigation. Contact us for further information about investigating insider incidents where protecting the assets, reputation and brand of your business is vital.

Insider threats are an increasing risk for businesses in 2020. They are difficult to prevent and detect and often cause significant financial and reputational harm. Responding to these threats in a timely and efficient manner is therefore critical to protect your business. Planning for the insider threat by ensuring your business understands its risk profile and has good cyber governance and incident response policies and procedures defined and tested are the most effective ways to increase resilience to insider threats.

NZ Incident Response Bulletin

Standard Edition – August 2020

Upcoming Events:

Date	Event	Location
September – October 2020	Aotea Security - Security Risk Management Seminars	Hamilton, Wellington, Auckland
14 October 2020	2020 NZ Cyber Security Summit	Te Papa, Wellington
September – October 2020	3rd Annual National Cybersecurity Summit	Online

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

Visit us at:
incidentresponse.co.nz

Also, visit our Microsites for detailed information:
forensictech.co.nz
whistleblowers.co.nz

Share our Bulletin: