NZ Incident Response Bulletin

Standard Edition - September 2019

In this issue:

News	Our Views	Upcoming Events	Premium Content
Ministry of Culture and Heritage reports serious digital privacy breach	Dealing with the rise in Ransomware	ISACA 2019 Oceania CACS Conference	Threat Alerts
NZ Institute of Directors' website defaced by hacker; passwords at risk	Ransomware Outbreak	SSS Cyber Security Day 2019 - Security - The Human Element	Security Frameworks
US House lawmakers ask regulators to scrutinise bank cloud providers	Economics of Ransomware - To Pay or Not to Pay?	2019 NZ Cyber Security Summit	Information Security Surveys
Texas Pummelled by Coordinated Ransomware Attack	The Ransomware Incident Response Process	Kawaiicon 2019	Forensic News
			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

Ministry of Culture and Heritage reports serious digital privacy breach

The Ministry of Culture and Heritage has suffered a website privacy breach. They were alerted of the potential breach by one of their customers on 22 August 2019 and shut down the impacted website on 23 August 2019. The information leaked consisted of 228 passports, 36 birth certificates, 6 secondary school ID's and 5 New Zealand residential visas. It impacted up to 302 young people who supplied this information as part of an application process to participate in Tuia 250 commemorations.

"This is very disappointing, and Manatū Taonga will be commissioning an external review to determine how this occurred" said Prime Minister Jacinda Adern.

The Ministry is offering support details for those impacted via their website and additional information on identity theft can also be found at CERT NZ.

NZ Institute of Directors' website defaced by hacker; passwords at risk

The New Zealand Institute of Directors recently took its website offline and warned all members to change their passwords after it suffered a cyber-attack defacing its website. The attack was part of a series of global attacks by the same individual or group that targeted mainly government institutions and left generic anti-authoritarian messages on their websites.

Educating its members about cyber risk has been a key focus for the NZ Institute of Directors. The Chief Executive says that the incident proves that online threats are very real.

NZ Incident Response Bulletin

Standard Edition - September 2019

World

US House lawmakers ask regulators to scrutinise bank cloud providers

After the large data breach suffered by Capital One last month, questions are being raised about the risks posed by the banking industries reliance on third-party cloud providers.

Citing the critical nature that cloud services now play in the global financial system, two US lawmakers have called for federal regulators to consider designating Amazon Web Services, Microsoft Azure, and Alphabet Inc's Google Cloud as "systematically important financial utilities".

They highlight that any large disruption to these services may compromise the overall stability of the market and that providing direct oversight of these cloud services should now be considered by policymakers.

Texas Pummelled by Coordinated Ransomware Attack

On the morning of August 16, 2019, more than 20 government entities in Texas reported a ransomware attack. The majority of these entities were smaller local governments. Evidence gathered to date indicates a single threat actor.

Incident response and recovery are the sole focus currently. The Texas Department of Information Resources are leading the response with the Texas Military Department, and Texas Cyber Response and Security Operations Centre teams deploying resources to the most critically impacted areas. It is unclear if the ransomware strain has been identified as yet or what the response effort entails, such as whether restoration of systems is possible from secure off-site backups. Restoration from a ransomware incident, however, can be time-consuming and laborious.

This coordinated ransomware attack follows a similar campaign in July which led to the state of Louisiana declaring a state of emergency after schools in its area suffered multiple malware infections. Local governments remain a frequent target for cybercriminals and coordinated attacks against cities appear to be on the rise.

Lake City, Florida's Fired IT Manager is Suing the City in Aftermath of Ransomware Attack

After Lake City in Florida was hit with a ransomware attack in June, it fired its IT manager. The IT manager is now suing as he maintains that he warned the city about the vulnerability and recommended a solution that the city officials ultimately deemed too expensive.

This event is raising questions and debate around who is ultimately responsible for a cyber-attack and whether laws are fair and available to prosecute those deemed responsible. The outcome of this lawsuit is yet to be determined.

NZ Incident Response Bulletin

Standard Edition - September 2019

Our Views:

A selection of issues relevant to Forensic and Cyber Security matters during the last month. This month's theme is "Dealing with the rise in Ransomware".

Ransomware Outbreak

Ransomware is a type of malware that threatens to publish the victim's data or perpetually block access to it unless a ransom is paid.

Ransomware continues to plague businesses worldwide. The Cybersecurity and Infrastructure Security Agency (CISA) has observed an increase in ransomware attacks across the world and consider it a leading risk to private and public organisations today. CISA has published some specific advice in response to the recent ransomware threats here.

Our experience also suggests that New Zealand organisations continue to be vulnerable to ransomware and need to utilise good planning in order to respond and recover effectively from these events. Sound preparation is the best way to combat or minimise the impact of a ransomware incident. You should consider steps such as:

- Conducting a tabletop exercise centred on ransomware to fully investigate the various threats, defences and required response plans
- Establishing a sound formal incident response plan for ransomware that includes a decision tree, covering each possible threat scenario identified and actions for response
- Conducting a risk analysis to determine appropriate financial responses to a ransomware incident
- Undertaking staff awareness and training
- Testing your business continuity plan and procedures

Economics of Ransomware - To Pay or Not to Pay?

Generally, the payment of a ransom is discouraged as it may further encourage this type of criminal activity. Further, recovery of locked files is not guaranteed. Recent studies highlight that while more organisations are paying ransoms, up to 40% of those that paid still lost their data.

Recovering from a ransomware attack can be a time-consuming and costly exercise. Paying the ransom may therefore be a cheaper (and only) option to recover data. A thorough cost v benefit analysis should be undertaken with a clear understanding of all risks involved to assist in this decision.

The Ransomware Incident Response Process

In the unfortunate incident of being affected by ransomware, the following process can be used as a general guideline.

Ransomware response involves four key stages:

- Stage 1: Incident Assessment and Specific Response Plan
- Stage 2: Risk Assessment and Negotiation
- Stage 3: Payment of the Ransom
- Stage 4: Recovery

NZ Incident Response Bulletin

Standard Edition - September 2019

1. Incident Assessment and Specific Response Plan

Firstly, follow your Cyber Incident Response Plan or similar process to analyse your data, the urgency of your response effort, your budget, the ransomware variant and the threat actor (cyber-attacker). Cyber insurance providers may also require this information.

Your response team should be formed, including identifying authorised representatives. If required, external experts can assist you through the process. Recent variants of ransomware require additional technical steps to be undertaken by the victim, before the decryption keys are provided on payment of the demand. These steps further complicate the recovery process, which may increase the risk of not recovering data.

Activities undertaken by your experts will involve discovering the scope of the cyber-attack by collecting all ransomware ID's and notes and samples of encrypted files. Where required, forensic copies of affected computers will be created. Additionally, the state of your backups should be assessed, and mitigations completed to prevent further spread of the malware. If you can successfully restore from backup, you should conduct a post incident review. Stages two, three and four below may not be required.

2. Risk Assessment and Negotiation

If you are unable to fully recover from backup, then you may need to pay the ransom.

When conducting negotiations for ransomware payment, it is useful to have an expert who has dealt with this type of incident assist you. There are organisations who specialise solely in handling ransomware negotiations. They will work with you in this process to attempt to achieve the best outcome.

During this stage any known information about the threat actor will be reviewed including whether they have been involved in prior negotiations and whether any information about them can be obtained from their wallet address or other sources.

A risk assessment would be undertaken based on any insight found (e.g. how likely is settlement to be successful, is the technical likelihood of decryption high or low etc.). You will set a ransom budget. Negotiations may take time but can also lower the ransom demand.

You will then supply a sample of encrypted files to the threat actor who will then provide proof of decryption. It is preferable not to provide them with confidential information for this process, however bear in mind that the threat actors may have viewed or copied your data during the cyber-attack.

3. Payment of the Ransom

Payment of the ransom to the threat actor may be in cryptocurrency or multiple payment forms. This is another reason why using an intermediary specialised in negotiation and ransom payment who maintains cryptocurrency accounts may be advised.

If professional negotiators are engaged, an Anti-Money Laundering (AML) check is used before any money is transferred to ensure none of the parties involved in the transaction (including the threat actor's wallet address) are on an OFAC Sanctions list.

The negotiating entity then manages the financial exchange.

4. Recovery

Once the decryption tool is received and run, troubleshooting of any failed files is undertaken and occasionally further communication with the threat actor is required. Any clean data is moved to clean environments and standard restoration services performed.

A post-incident review should always be undertaken, and any lesson learned adopted into your incident response plan.

NZ Incident Response Bulletin

Standard Edition - September 2019

Upcoming Events:

Date	Event	Location
11-13 September 2019	ISACA 2019 Oceania CACS Conference	Auckland
16, 18, 20 September 2019	SSS Cyber Security Day 2019	Christchurch, Auckland, Wellington
16 October 2019	2019 NZ Cyber Security Summit	Wellington
17, 18 October 2019	Kawaiicon 2019	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

Share our Bulletin: