NZ Incident Response Bulletin

Standard Edition – March 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	ICS Security Summit & Training 2021 - Live Online	

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

New Zealand To Join The Council Of Europe Convention On Cybercrime

The Government is joining the Council of Europe Convention on Cybercrime (the Budapest Convention), Justice Minister Kris Faafoi and Minister for the Digital Economy and Communications Dr David Clark recently announced. The decision progresses a recommendation by the Royal Commission of Inquiry into the Christchurch terror attack to accede to the Convention. By creating a common framework for tackling computer crimes and with common powers for obtaining electronic evidence, the Convention strengthens international cooperation on a wide range of criminal investigations, underpinned by international and domestic human rights laws.

Cyber security to be ramped up ahead of Covid-19 vaccine rollout

Government agencies are gearing up to combat a barrage of vaccine-related scams expected to hit during the Covid-19 immunisation campaign. Covid-19 Response Minister Chris Hipkins said if people received emails out of the blue asking for personal details related to Covid-19 - it was likely to be a scam, even if it appeared to be from a legitimate health agency. Hipkins said both Facebook and Google had contacted the government to explain that they would be taking action to fight this during the immunisation campaigns. The government would be running its own campaign to make sure people had easy access to the correct information, he said.

Increased online gaming poses cyber-security risks for homes, businesses

A sharp increase in the number of people playing games online poses significant security risks for households and businesses, a cyber safety company says. The personal information tied to gaming accounts had become a lucrative target for cyber criminals and players would need to become more vigilant to protect their data, he said. A typical gaming account could include the gamer's name, birth year, mailing address, email, mobile number, payment information and other personal information that could be used by an identity thief.

World

Breach of Trust: How Threat Actors Leverage Confidential Information Against Law Firms

One of the primary tasks of a law firm is managing and protecting a client's private legal information. Knowing this, threat actors seek out this information when penetrating a law firm's network, steal it and offer it for sale on DarkWeb forums &

marketplaces. To protect against these threats, law firms must upgrade their incident response capabilities, ensure that qualified people are in place, bridge the gap in employee knowledge on basic cybersecurity practices and stay vigilant regarding continuing and emerging threats.

Phishing: These are the most common techniques used to attack your PC

Creating malicious Office macros is still the most common attack technique deployed by cyber criminals looking to compromise PCs after they have tricked victims into opening phishing emails. Phishing emails are the first stage in the attack for the majority of cyber intrusions, with cyber criminals using psychological tricks to convince potential victims to open and interact with malicious messages.

Clop targets execs, ransomware tactics get another new twist

Ransomware peddlers have come up with yet another devious twist on the recent trend for data exfiltration. After interviewing several victims of the Clop ransomware, ZDNet discovered that its operators appear to be systematically targeting the workstations of executives. After all, the top managers are more likely to have sensitive information on their machines.

The Egregor takedown: New tactics to battle ransomware groups show promise

Law enforcement officials from Ukraine, France and the U.S. this month cracked down on the Egregor ransomware gang, shutting down its leak website, seizing computers and arresting individuals who are allegedly linked to ransomware attacks that netted $80 million in illicit profits from more than 150 victimised companies. While landing the main culprits behind Egregor would constitute a major coup, often times malware ringleaders are cloistered away in countries where they cannot be touched or extradited and cooperation is scarce.

Why Threat Actors Continue to Rely on Cyber Fraud

While 2020 has come and gone, many of last year's cyber fraud problems will continue into at least mid-2021. Cybercriminals will focus on maximizing their profits, using a traditional cost-benefit analysis to decide on the best attack vector. Pandemic-related emotions will run high, and remote workforces will continue as companies embrace the "new normal." From the cybercriminal perspective, these prevailing trends only increase the return on investment for scams and fraud. With this in mind, organizations must remain vigilant to protect themselves and their sensitive data from these attack methodologies.

CISOs report that ransomware is now the biggest cybersecurity concern in 2021

As the number of remote working arrangements rose substantially in the last year, cybercriminals were quick to take advantage of these new opportunities. Spam and phishing emails increased in number even more rapidly than telecommuting and company cybersecurity officers found themselves struggling to keep up. Phishing emails often came with a sinister sidekick - a ransomware attack. It is not surprising then that a recent survey of IT and cybersecurity officers revealed that ransomware attacks are the primary security concern for these professionals in 2021. This article provides an overview of the rise of ransomware attacks and discusses how security professionals can prepare for and prevent attacks.

Ransomware attacks increasingly destroy victims' data by mistake

More and more ransomware victims are resisting the extortionists and refuse to pay when they can recover from backups, despite hackers' threats to leak the data stolen before encryption. This stance resulted in Q4 of 2020 seeing a significant decline in the average ransom payments compared to the previous quarter, says ransomware remediation firm Coveware. However a more insidious phenomenon is prefiguring, where data is destroyed in the attack leaving companies no option to recover it, even if they pay the ransom.

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.

26 February 2021 - NSA - Embracing a Zero Trust Security Model

NZ Incident Response Bulletin

Standard Edition – March 2021

Our Views:

This month's theme is "Social Media Forensics".

It is believed that, on average, each person now has around eight social media accounts and that there are at least 1.9 billion active users on Facebook alone each month. With millions of people globally posting and chatting on social networking sites, it is not surprising that these social networks have become a rich source of digital evidence. In some cases, social media may be the primary source of data available to unravel and understand an event. The importance of social media evidence was demonstrated recently in the "GameStop" trading controversy. Reddit posts played a crucial role in uncovering the exact nature of how this event unfolded.

Social Media Forensics involves the identification and collection of digital evidence from social media platforms and the devices used to create or access such content, followed by the analysis of this data for use in civil or criminal investigations. Accordingly, your social media policy should include procedures for collecting digital evidence. You should also consult with your legal experts before attempting to collect any data that is associated with an individual's personal network.

Why collect evidence from social media sources

Content and the associated log data posted to social media may:

- Support evidence gathered from other sources such as text messages or emails
- Identify employee misconduct
- Help explain what has happened in any incident
- Show who did what, when, and where
- Indicate intent or state of mind
- Establish connections between people
- Assist in the construction of an event timeline

Challenges with social media forensics

Despite being a rich source of data, obtaining evidence from social media is not without challenges.

- Social media companies often require a warrant to be issued that compels their cooperation when gathering evidence. A private company may submit a request for information; however, the social media company may not be obligated to provide this data. If the user has complied with the site's "terms of use", the social media company may also find themselves exposed should they hand over private data. Therefore, a lack of a warrant may hinder an investigation into matters where law enforcement involvement is not appropriate or desirable, such as an employment dispute.
- Social media content is volatile, and users may delete and modify previously posted content.
- Social media content may synchronise between various physical devices, obscuring the original source.
- The devices used to access social media sites are frequently updated, meaning evidence can be lost quickly.
- All social media platforms publish terms and conditions, defining what information may be collected and used. Not complying with these in an investigation may lead to the evidence being inadmissible in court.
- Social Media accounts may be falsified or taken over and used by an imposter, leading to authenticity concerns. The current state of the law around the admissibility of social media evidence is in flux, and Australasia has limited case law in this area. In the United States, current case law is divided between examples such as *United States v. Vayner* that impose a stringent approach to admissibility requiring unchallengeable proof of authenticity; and other decisions whereby social media evidence is admissible based upon reasonable facts.

Understanding these challenges and ensuring the social media evidence is handled with these in mind is crucial.

NZ Incident Response Bulletin

Standard Edition – March 2021

The Practicalities of Social Media Forensics

The most basic technique for collecting social media evidence is manual collection. This involves simple activities such as visiting a website and taking screenshots of content or scrolling through a phone to view content. Whilst simple, manual evidence collection is not the most reliable or time-efficient method. Care must be taken that there is no opportunity for evidence to be changed or lost in the process of undertaking manual inspection. However, manual collection may be suitable under certain circumstances, such as when access to the device in question is fleeting or there are no other practical ways to retrieve the evidence based on security limitations or other similar challenges.

Advanced commercial forensic tools such as Nuix and Magnet Axiom allows the profiles and information from social networks to be collected and preserved in a forensically sound manner. Analysis of this data can answer many of the questions an investigator or lawyer will have relating to the use of social media accounts.

As more than 90% of social media users use their mobile device to access social networking platforms, smartphones are a vital source of potential evidence. Social media forensic tools offer the ability for the logical acquisition of social media evidence from smartphones. This process involves capturing a logical image of all the files on the phone and then analysing these for evidence of activities such as logging in, browsing, searching, and posting on social media networks. Data artefacts such as activity logs, archives, profile information, geo locations, friends and family, interests, active chat session participants, chat subjects and timestamps of activities may all be visible.

Many social media sites also have a method for users to obtain a copy of their account and activity, such as "Google Takeout'. These records can be downloaded and saved in an unalterable manner for use in an investigation.

Further Guidance

An inexperienced investigator may make mistakes when collecting critical evidence. We recommend seeking a forensic expert and legal counsel's advice in the gathering of social media evidence to ensure this is avoided.

Social media sites such as LinkedIn and Facebook will often truncate the display of comments and posts, whereas specialised forensic software is more likely to capture all of the available content.

We recommend businesses have a comprehensive Acceptable Use Policy outlining how an employee may use the company devices and network, including procedures relating to its collection.

We also recommend that employees are educated on the safe and sensible use of social media. This education should include advice on privacy settings, acceptable content for sharing, password protection and some real examples of the impact that social media evidence can have in legal proceedings.

In conclusion, whilst gathering social media evidence can be challenging, there are techniques available to identify and collect this data to support an investigation. Forensic experts have the skills, expertise, and experience to navigate the complications associated with social media evidence. We advise seeking advice on what may be possible and lawful to obtain and use in any investigation for the best outcome and preparing suitable policies and procedures for forensic readiness to ensure social media evidence is obtainable in the event of an investigation.

NZ Incident Response Bulletin

Standard Edition – March 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: