NZ Incident Response Bulletin

Standard Edition – April 2024 – Issue #63

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.

Not subscribed to our Premium Bulletin? Click here to join.

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

NZ MPs and Parliament systems targeted by China-based hackers

New Zealand's Parliament faced a significant cybersecurity breach in 2021, attributed to Chinese state-sponsored cyber espionage. While data theft occurred, it was deemed non-strategic. Despite condemnation of China's malicious cyber activities targeting democratic processes, New Zealand refrained from imposing sanctions. The breach underscored the importance of robust cybersecurity measures, with officials urging China to cease future intrusions. Identified as Advanced Persistent Threat 40 (APT 40), linked to China's Ministry of State Security, the incident highlighted the need to safeguard governmental operations and sensitive information.

New Zealand central bank to implement cyber reporting rules through 2024

The Reserve Bank of New Zealand plans to implement cyber reporting rules until 2024 to enhance cybersecurity in the financial sector. These regulations aim to improve resilience against cyber threats and ensure prompt responses to potential breaches. The move underscores the central bank's commitment to bolstering the country's financial system's cybersecurity posture amid evolving digital risks.

Bank expert explains money mules

Banks are stepping up efforts to combat 'mule' accounts used in illegal fund transfers, employing measures like matching account names and numbers. Money mules, recruited through job scams promising easy money, are often unaware of their involvement in criminal activities. Detection and prevention remain challenging for banks, especially with transactions appearing legitimate and funds often transferred internationally. Initiatives such as proposed national anti-scam centers aim to enhance information sharing to tackle these schemes. ANZ utilizes fraud detection algorithms and teams to identify suspicious activities, implementing measures like two-factor authentication to protect against scams. These efforts highlight the importance of ongoing vigilance in combating financial fraud.

Spark to introduce barriers to help stamp out objectionable material, cyber risks and scams

Internet service and telecommunications provider Spark is taking proactive steps to enhance online safety for its customers. These measures include the introduction of multiple barriers such as an automated text message scam firewall and two filters aimed at reducing exposure to malware, phishing attempts, and objectionable material, including child sexual abuse content. The move aligns with Spark's commitment to making the internet a safer space for its users, particularly concerning the dissemination of illegal content. Spark is set to roll out additional features, including a firewall capable of automatically detecting fraudulent SMS content, and collaboration with the GCSB National Cyber Security Centre to implement the Malware Free Networks service. Despite these advancements, Spark urges customers to remain vigilant against evolving scam tactics, emphasising the ongoing need for online safety awareness and protection measures.

Australia

Australian Government Doubles Down On Cybersecurity in Wake of Major Attacks

The Australian government is actively reforming its cybersecurity policies and laws in response to recent high-profile cyberattacks. This includes updating the Security of Critical Infrastructure (SOCI) Act 2018 to better prevent threats, share information, and respond to incidents. The reforms are part of a broader strategy aimed at making Australia a global leader in cybersecurity by 2030. Following attacks on Optus, Medibank, and critical port infrastructures, the need for stronger cybersecurity measures has become apparent, with incidents exposing significant vulnerabilities and affecting millions. The government's proposed changes advocate for secure design standards, ransomware reporting, and improved incident sharing among key infrastructure sectors. Despite these advancements, gaps remain, particularly in software supply chain security. However, with substantial investments in cybersecurity, amounting to a projected 11.5% increase in spending for 2024, Australia is on a path towards significant improvement in its cyber defences, aligning with global standards and leveraging its innovative capabilities to enhance national security.

World

Hackers Behind the Change Healthcare Ransomware Attack Just Received a $22 Million Payment

The ransomware attack on Change Healthcare by the hacker group AlphV, also known as BlackCat, caused widespread disruption across US pharmacies for over 10 days. A significant development has emerged from a dispute within the criminal underworld, revealing that AlphV received a $22 million ransom payment. This was discovered when an affiliate of AlphV accused the group of withholding their share of the ransom, citing a $22 million Bitcoin transaction as evidence. Security researchers have linked this transaction to AlphV, suggesting that Change Healthcare likely paid the ransom. This incident highlights a dangerous precedent for the healthcare industry, as it could encourage more ransomware attacks on vital services. Despite the payment, there's concern that the affiliate hacker still has access to sensitive medical data from Change Healthcare's network. This case underscores the profitability of ransomware and the risks of trusting criminals, as even paid ransoms don't guarantee safety from further exploitation or data leakage.

Microsoft warns Russian hackers still trying to break into its systems

Microsoft reported that Russian hackers linked to the country's foreign intelligence, identified as Midnight Blizzard or Nobelium, have been attempting to infiltrate its systems using data from a previous breach of corporate emails in January. This ongoing cyber intrusion campaign has raised significant concerns among analysts about the safety and national security implications, given Microsoft's extensive involvement in providing digital services to the U.S. government. The hackers initially gained access through a method known as a "password spray" attack and have continued their efforts, indicating a high level of resource commitment and targeting sophistication. Microsoft, known for its vast cybersecurity research and intelligence capabilities, revealed that among the stolen data were access credentials to source code repositories and internal systems. This breach not only demonstrates the persistent threat posed by Midnight Blizzard but also underscores the critical cybersecurity challenges facing major software providers and their government clients.

Former telecom manager admits to doing SIM swaps for $1,000

Jonathan Katz, a former telecommunications company manager in New Jersey, pleaded guilty to conspiracy charges related to performing unauthorized SIM swaps, a cyberattack method. These swaps enabled an accomplice to hijack customer accounts by transferring a target's phone number to a SIM card controlled by the attacker, bypassing two-factor authentication to access online accounts. Katz executed these swaps between May 10 and 20, 2021, exploiting his managerial position and privileged access. He received $1,000 in Bitcoin for each swap, contributing to the hijacking of victims' accounts across multiple states. Katz now faces a potential five-year prison sentence and significant fines, with sentencing scheduled for July 16, 2024.

Bankman-Fried sentenced to 25 years for multi-billion dollar FTX fraud

Sam Bankman-Fried, the founder of the now-bankrupt FTX cryptocurrency exchange, was sentenced to 25 years in prison by U.S. District Judge Lewis Kaplan for stealing $8 billion from customers. The sentence follows his conviction on seven fraud and conspiracy counts related to FTX's collapse, considered one of the largest financial frauds in U.S. history. Despite his apology to FTX colleagues and acknowledgment of customer suffering, Bankman-Fried did not admit to criminal wrongdoing and plans to appeal his conviction and sentence. The sentencing reflects Bankman-Fried's dramatic fall from being a billionaire and political donor to a significant figure in the U.S. crackdown on cryptocurrency market malfeasance. The court also imposed an $11 billion forfeiture order to repay victims, with Bankman-Fried's parents expressing heartbreak and vowing to continue fighting for their son.

ICO publishes new fining guidance

The Information Commissioner's Office has published new data protection fining guidance setting out how it decides to issue penalties and calculate fines. The guidance provides greater transparency for organisations about how the ICO goes about using its fining power.

Tim Capel, ICO Director of Legal Service, said "We believe the guidance will provide certainty and clarity for organisations. It shows how we reach one of our most important decisions as a regulator by explaining when, how and why we would issue a fine for a breach of the UK General Data Protection Regulation or Data Protection Act 2018." Publication of the guidance follows a consultation last year, where views were gathered on a draft version. The new guidance replaces the sections about penalty notices in the ICO Regulatory Action Policy published in November 2018. Among other things, the guidance explains:

- the legal framework that gives the ICO the power to impose fines –helping people more easily navigate the complexity of the legislation;
- how the ICO will approach key questions, such as identifying the wider 'undertaking' or economic entity of which the controller or processor forms part; and
- the methodology the ICO will use to calculate the appropriate amount of the fine.

Summary of last month's Cyber Alerts and News Clips:

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 this webpage.

21/03/2024 - CISA, FBI, and MS-ISAC Release Update to Joint Guidance on Distributed Denial-of-Service Techniques

Our Views:

Changes to the Cyber Landscape - Generative Artificial Intelligence

In response to the changing cyber landscape, Lloyds (the global insurance and reinsurance market) published "Generative AI: Transforming the Cyber Landscape". The report represents collective insights and research from experts within the Lloyd's market.

The report outlines significant shifts in the cybersecurity landscape due to advancements in Generative AI (GenAI) and Large Language Models (LLMs). The report covers the relatively short history of GenAI, and then deep dives into the implications for businesses and insurance.

We are increasingly being asked about the role insurance plays in managing cyber risk, so we have summarised the key takeaways in this month's bulletin and will return to the topic in future months to explore some of the key issues.

Brief History of AI and LLM's

Generative AI and LLMs have made significant advancements, particularly in the last 18 months, potentially altering cybersecurity dynamics. Recent efficiencies in the processing of data have made it easier to run models on commodity hardware, which in turn have raised concerns about unrestricted model access and the creation of harmful content by cyber attackers.

About six years ago, Google Research published a pivotal paper introducing the 'Transformer' algorithm, revolutionizing the way sequential data with complex structures is encoded, represented, and accessed. This innovation laid the foundation for the majority of generative machine learning approaches in language, vision, and audio by 2023, by transforming sequential processing into parallel processing. This allowed for handling significantly larger datasets within the same computational budget, drastically reducing costs and enhancing the model's ability to understand and generate long-range data structures.

This breakthrough spurred rapid advancements in AI capabilities, evidenced by the development and release of models like ChatGPT and GPT-4, which demonstrated human-like proficiency across various tasks. The pace of these advancements has posed challenges for establishing effective AI governance policies among enterprises and regulatory bodies, highlighting a need for balanced approaches to ensure the technology's safe evolution. The EU, UK, and US have each adopted different regulatory strategies, ranging from strict legislative frameworks to more principle-based or soft-law approaches, reflecting the global diversity in managing AI's growth while safeguarding against its risks.

Transformation of Cyber Risk

Lloyds outlines a framework of how Gen AI tools may be used by attackers (or cyber security professionals). These factors will influence cyber threats in predictable ways and assess the potential impact that LLM technology has on each of them.

Vulnerability Discovery

Automated tools, especially those utilising LLMs, could significantly increase threat actors' ability to discover vulnerabilities, potentially outpacing defensive tools due to asymmetric incentives.

Finding such vulnerabilities is traditionally time-consuming and requires deep technical expertise. However, the advent of Large Language Models (LLMs) has the potential to revolutionise this process by enabling the automated discovery of exploitable vulnerabilities across various challenging domains like embedded firmware, proprietary software binaries, and hardware device drivers. This automation could significantly reduce the cost and time associated with identifying vulnerabilities, making cyber attacks easier, cheaper, and more effective.

LLMs can perform at-scale scans of open-source repositories, identifying vulnerabilities that would be difficult or impossible for humans to find. This creates a larger pool of vulnerabilities, offering threat actors greater flexibility in their attack strategies. AI-enhanced tools could also be used by security professionals for defensive purposes, such as threat intelligence and incident response, but the asymmetry in incentives and flexibility means that threat actors might derive more benefit from these technologies.

The potential impacts of this evolution are substantial, with the automated discovery of vulnerabilities likely to increase the frequency and severity of cyber incidents significantly. This includes the potential for cyber-physical risks, as vulnerabilities in industrial control systems are uncovered. While security teams within organisations face various constraints that may limit their ability to defend against these evolving threats, threat actors have the motivation and flexibility to exploit this new technology fully.

Campaign Planning and Execution

The automation and fine-tuning capabilities of GenAI could enable more efficient, targeted cyber campaigns, lowering costs and expanding the scope of potential attacks.

Traditional cyber campaigns, including phishing and data breaches, require considerable human effort for tasks such as target identification, data collection, and the creation of attack materials. These requirements have historically limited the scalability and cost-effectiveness of cyber attacks.

Gen AI technologies, particularly Large Language Models (LLMs), introduce the potential to automate several aspects of campaign planning and execution. This includes the automated collection and analysis of data on potential targets, the generation of customised attack materials (such as phishing emails or fake communications), and even engaging with targets in real-time without direct human intervention. The use of LLMs can significantly reduce the resource constraints faced by threat actors, enabling them to conduct broader, more sophisticated campaigns with less effort and potentially greater effectiveness.

This automation also poses risks of impersonation and misinformation, as Gen AI can produce highly convincing fake content that can be used to manipulate individuals and breach organisational networks. The National Security Agency (NSA) has highlighted these risks, indicating the serious implications of Gen AI's capabilities for cyber security.

Risk-Reward Analysis

Enhanced capabilities may embolden threat actors by improving their ability to evade detection and successfully execute their objectives.

For threat actors, the utility derived from their activities—be it financial, informational, reputational, or political—is paramount. However, achieving these goals without drawing undue attention from powerful entities like state intelligence agencies is crucial to avoid detection and countermeasures. Threat actors commonly employ techniques to obscure their digital "fingerprints," obfuscate attack components, or safely move stolen assets, minimising the risk of attribution.

The advent of Large Language Models (LLMs) offers new tools for enhancing these obfuscation efforts. LLMs have the potential to automate the process of removing or altering identifiable characteristics from malware and cyber campaign materials, as well as to misdirect forensic analysis through sophisticated manipulation of digital traces. This capability could significantly improve the ability of threat actors to conduct operations covertly, complicating the efforts of cybersecurity professionals to track and mitigate cyber threats effectively.

Single Points of Failure

The centralisation of LLMs as a service could introduce new vulnerabilities and potential for widespread impact from cyber attacks.

As LLMs become embedded in critical services and infrastructure, their centralised nature and the concentration of service providers like OpenAI, Google, and Microsoft introduce significant vulnerabilities. This centralisation could lead to disruptions across multiple domains if these key providers are compromised. Furthermore, the widespread use of LLMs raises concerns about dataset poisoning, embedded vulnerabilities, unpredictable AI behavior, and potential biases in AI-generated outputs. These factors combined could result in substantial risks, including large-scale outages, cyber-physical incidents, and market disruptions, highlighting the need for comprehensive risk management and mitigation strategies in the face of increasing reliance on LLM technologies.

Discussion points for your organisation

AI technologies lower the entry barrier for cybercrime, leading to an increase in vulnerabilities and potential cyber losses. This scenario necessitates more nuanced risk assessments and adjustments in insurance policies to cover emerging threats such as deepfakes.

As cyber attacks become more automated and sophisticated, there's a growing risk of cyber catastrophes, especially those linked to large-scale, systemic failures involving new LLM service providers. The insurance sector is likely to evolve its products to address these broader risks, including disruptions and data breaches stemming from AI-enhanced attacks.

Your organisation needs to consider how insurance may address these risks which might have been previously underserved. We encourage you to adopt comprehensive cyber defense and continuity plans to mitigate AI-related vulnerabilities, with cyber insurance playing a crucial role in supporting resilience and recovery. Moreover, fostering a collaborative effort between insurers, governments, and society is essential for creating a secure cyber environment, emphasising the importance of information sharing, enhancing supply chain resilience, and promoting public awareness on cyber hygiene.

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.

Subscribers to the premium edition also obtain access to the following additional information:

- Cyber Governance
- Cyber Incident Landscape
- Cyber Incident Response Resources
- Cyber Framework and Control Updates, Surveys and Research

Click here if you wish to subscribe to our Premium Edition of the Bulletin.

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: