NZ Incident Response Bulletin

Standard Edition – August 2023 – Issue #55

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

Government strengthens cyber security

A lead operational agency will be established to strengthen cyber security readiness and response as well as make it easier for people and organisations to get help, Minister for the Public Service Andrew Little says. "The cyber security threats New Zealand faces are growing in scale and sophistication. We're committed to staying ahead of the hackers, to protect communities, businesses and our public services. "That's why we're acting on the recommendation of the Cyber Security Advisory Committee to bring New Zealand's Computer Emergency Response Team (CERT NZ) into the National Cyber Security Centre (NCSC). Having a single agency to provide authoritative advice and respond to incidents across every threat level is international best practice, and will ensure New Zealand is well placed to take advantage of the opportunities in the digital economy and provide secure government services to our citizens," Andrew Little said.

"Since 2018 this government has invested $94 million in improved cyber security capability. We've delivered world-leading protection products, such as Malware Free Networks to protect internet service providers and private networks, and we've rolled out baseline security templates that make it easier for organisations to take advantage of innovative cloud services while better protecting their information," Minister for the Digital Economy Ginny Andersen said. "But we know there's more to do. $5.8 million of direct financial losses from cyber incidents were reported to CERT NZ in the first quarter of the year. The NCSC prevented $33 million of harm to our economy over the whole of last year. We know the true scale of harm to our economy is underreported."

"Creating a dedicated new lead operational agency ensures New Zealand is best positioned to fight back against the hackers we know cause real harm to individuals and to our economy," Ginny Andersen said. Operational integration of CERT NZ into the NCSC will begin on 31 August and will be phased over several years. All current services will be maintained in the interim.

Police admit it's impossible to ID offshore scammers, investigators 'not focused' on solving crimes

A senior police boss says investigators have all but shelved attempts to solve international scam crimes due to complexities in identifying offshore offenders and their use of "money mules" to mask the trail of stolen cash. Offshore scammers are estimated to be draining hundreds of millions of dollars from Kiwi victims every year, with cases surging in recent months.

Detective Inspector Chris Barry oversees Auckland City CIB investigations and the police district's 19-man financial crime unit. In a blunt admission, Barry said while scams were becoming more innovative and victims were suffering significant financial harm, it was nearly impossible for police to trace funds sent offshore or identify the criminal masterminds due to their remote locations and ability to hide identities online. Rather than trying to solve these cases and bring international criminals to justice, police were instead focused on identifying local people who helped facilitate the crimes through the use of domestic bank accounts, and educating the public to raise awareness about scams.

Parliament hit by cyber attack, Russian hacker group claims responsibility

A Russian hacker group claims to have temporarily taken down a number of New Zealand websites - including Parliament's - in retaliation for the Government supporting Ukraine. The 'NoName057(16)' hacker group claims on Telegram to have caused the New Zealand Parliament, Parliamentary Counsel Office (PCO) and Legislation websites to temporarily crash this week as a result of a denial-of-service (DDoS) attack.

Clerk of the House of Representatives David Wilson confirmed to Newshub the Parliament website was impacted by a "cyber security-related event on Monday night". "The situation was resolved quickly thanks to the hard work of the Parliamentary Service's IST website technical team," Wilson said. "The security of the website was not compromised during the attack and no communication was received by Parliament from the attackers. For cyber-security reasons we will not be sharing the technical details of the situation."

World

Letchworth IT worker blackmailed bosses at Oxford company during cyber attack and demanded money

A 28-year-old man from Letchworth has been jailed for three years and seven months after he attempted to extort money from the company he worked for. Ashley Liles, 28, of Fleetwood in Letchworth Garden City, was sentenced for blackmail and unauthorised access to a computer with intent to commit other offences at Reading Crown Court. He admitted the offences earlier this year following the incident that took place five years ago.

WormGPT: New AI Tool Allows Cybercriminals to Launch Sophisticated Cyber Attacks

With generative artificial intelligence (AI) becoming all the rage these days, it's perhaps not surprising that the technology has been repurposed by malicious actors to their own advantage, enabling avenues for accelerated cybercrime. According to findings from SlashNext, a new generative AI cybercrime tool called WormGPT has been advertised on underground forums as a way for adversaries to launch sophisticated phishing and business email compromise (BEC) attacks. "This tool presents itself as a blackhat alternative to GPT models, designed specifically for malicious activities," security researcher Daniel Kelley said. "Cybercriminals can use such technology to automate the creation of highly convincing fake emails, personalized to the recipient, thus increasing the chances of success for the attack."

'FraudGPT' Malicious Chatbot Now for Sale on Dark Web

Threat actors riding on the popularity of ChatGPT have launched yet another copycat hacker tool that offers similar chatbot services to the real generative AI-based app but is aimed specifically at promoting malicious activity. Researchers have found ads posted on the Dark Web for an AI-driven hacker tool dubbed "FraudGPT," which is sold on a subscription basis and has been circulating on Telegram. FraudGPT starts at $200 per month and goes up to $1,700 per year, and it's aimed at helping hackers conduct their nefarious business with the help of AI. The actor claims to have more than 3,000 confirmed sales and reviews so far for FraudGPT.

Google exposes intelligence and defense employee names in VirusTotal leak

Hundreds of individuals working for defense and intelligence agencies globally have had their names and email addresses accidentally exposed by an employee at Google's malware scanning platform VirusTotal. The online service lets organizations upload suspected malware to be checked against a range of anti-virus tools. VirusTotal then shares these files with the security community, creating a library of malware signatures to help cybersecurity professionals detect attempted attacks and develop threat intelligence. But a list of 5,600 of the repository's customers also was uploaded, accidentally, to the platform itself. The list, which has been seen by Recorded Future News, identifies individuals affiliated with U.S. Cyber Command and the National Security Agency, as well as with the Pentagon, the FBI, and a number of U.S. military service branches.

New tool exploits Microsoft Teams bug to send malware to users

A member of U.S. Navy's red team has published a tool called TeamsPhisher that leverages an unresolved security issue in Microsoft Teams to bypass restrictions for incoming files from users outside of a targeted organization, the so-called external tenants. The tool exploits a problem highlighted last month by Max Corbridge and Tom Ellson of UK-based security services company Jumpsec, who explained how an attacker could easily go around Microsoft Teams' file-sending restraints to deliver malware from an external account.

The feat is possible because the application has client-side protections that can be tricked into treating an external user as an internal one just by changing the ID in the POST request of a message.

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.

12/07/2023 – Enhanced Monitoring to Detect APT Activity Targeting Outlook Online

Our Views:

Using Government-issued Cyber Security Advisories

Reliable threat intelligence and mitigation advice is a critical tool for all organisations looking to stay across the latest cyber threats in the landscape and take effective actions to protect their information systems and data. Government agencies use their access to elite technical capabilities and far-reaching networks to develop advisories and cybersecurity guidance papers and alert on important cybersecurity threats.

Threat intelligence covers both existing and emerging threats and includes detailed information on threat actors, TTP's, and Indicators of Compromise that are specific to the threat described. Alerts are issued to provide timely information about the most relevant threats in the landscape and cybersecurity advisories also provide step by step guidance on how to identify a specific type of attack, and how best respond and recover from it. Additional information is also available in the form of information sheets, technical reports and research based white papers that support businesses to protect themselves against cyberthreats.

We recommend following reputable government-issued alerts and advisories for multiple purposes including:

- Incident Response Planning: The advice in government issued advisories that outlines how threats work, how the threats are typically applied and how to identify them can be used to craft effective playbooks and plans to respond in a cyber incident. Include this information in your playbooks and business continuity plans and ensure these are regularly updated in accordance with the latest advisories.
- Incident Response: If your business suffers an unforeseen cyber incident, the actions included in recent alerts and advisories should be used to pivot and guide your actions in all phases of your response lifecycle including identification, containment, and recovery.
- Proactive Threat Hunting: Businesses can search their networks for the specific IOC's included in threat intelligence alerts and advisories helping to identify any potential threats and take actions to mitigate them before they have an impact.
- Cyber Security Improvement Planning: Threat advisories offer guidance around the general attack landscape that can be used to shape and guide the creation of your cybersecurity improvement plans by helping to identify gaps in defences and prioritise mitigations and improvement.
- Training and Awareness: External alerts and advisories can provide situational context for generating internal security advisories and cyber training and awareness content.

The cybersecurity landscape moves quickly, and organisations need to constantly monitor and review the issued alerts and advisories from agencies such as the following:

- National Cyber Security Centre
- CERT NZ
- CISA
- National Cyber Security Centre - UK
- Australian Cyber Security Centre

Keeping abreast of these advisories and taking the recommended steps above to incorporate the advice into your cybersecurity practice will assist in lifting cyber security posture and allow more effective response and recovery from cyber incidents.

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: