Incident Response
FORENSIC & CYBER

NZ Incident Response Bulletin

Premium Edition – May 2024 – Issue #64

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

GCSB centre considers US finding that Microsoft 'cascade' of errors allowed Chinese hack

Microsoft, which holds the data of millions of New Zealanders given to it by the government, has been castigated in the United States for slack cybersecurity which it says let in Chinese hackers. Health New Zealand Te Whatu Ora said it was seeking "assurances" from the tech giant and, with other public agencies, was "monitoring these developments". The US Department of Homeland Security in a new investigation said Microsoft had a lax overall security culture, leading to "a cascade of avoidable errors" in last year's hack of US and United Kingdom government emails.

Microsoft's attitude to security was "at odds with the company's centrality in the technology ecosystem and the level of trust customers place in it", the DHS's Cyber Safety Review board said. "Microsoft still doesn't know how the hackers got in", though it had pretended for months that it did, it said. This comes on top of alarm at an ongoing successful hack of Microsoft corporate email by the Russia-backed Midnight Blizzard group linked to successful attacks which targeted the US presidential elections in 2016.

Companies and organisations underprepared and overconfident, says cyber security firm

A global cyber security firm says New Zealand companies and organisations are underprepared and overconfident and need to narrow their focus to combat cyber threats. Cisco's second annual Cybersecurity Readiness Index indicates cyber threats were much bigger than ransomware and phishing, with criminals increasingly exploiting vulnerabilities in older, common software applications.

The threat extended to such things as credential stuffing (using stolen username and passwords to gain access to a service), supply chain attacks, social engineering (conning victims) and cryptojacking (fraudulently using computer power to mine cryptocurrency). The report says advancements in artificial intelligence (AI) and the mainstream availability of capabilities like generative AI were further empowering malicious criminals to deploy more sophisticated targeted attacks, but was also providing smarter, defensive tools.

Police search Auckland properties in relation to major global cybercrime scheme that's targeted thousands

New Zealand Police have joined international authorities to tackle a major cybercrime operation which targeted thousands of people worldwide. Working alongside Europol, police have executed three search warrants at Auckland properties relating to a multi-national operation. The scheme targeted the phishing as a service platform, LabHost.

In a statement from police, Cybercrime Investigator Detective Sergeant Richard Briscoe said police allege the platform enabled users to operate "phishing kit" websites. These imitated websites of real online services trick people, through text messages, into providing their banking, bank card or other online account credentials.

Public warned about new phone scammers who pose as police officers

Kiwis are being warned to be alert for phone scammers who have been posing as police officers. The scam involves a fake officer, claiming to be from a special department, telling the person they've been a victim of a fraud or scam - to then secretly get their private financial details. Det Snr Sgt Craig Bolton said more than a dozen reports of the scam have emerged since the start of the month, largely to landlines.

Bolton said scammers are opportunistic and target victims on a range of platforms. Officers will never contact people about banking details, card numbers, PINs or passwords, he stressed. Bolton also said a previous email scam claiming to be authorities from police, justice, and the courts is also doing the rounds again. The public is encouraged to report all scams to police by calling 105.

World

After ChatGPT, US Congress bans use of Microsoft's AI tool Copilot for staff members

After OpenAI's ChatGPT, the US Congress has restricted its employees from using Microsoft's Copilot AI. As per a report by Axios, this decision is taken due to major security concerns. The staff members will not be able to use Copilot on their government-issued devices. The directive came through a memo from House Chief Administrative Officer Catherine Szpindor. The memo stated concerns regarding potential risk of data leak to unauthorised cloud services. These concerns were raised by the Office of Cybersecurity. Notably, the employees can still use Copilot AI on their personal devices.

Initial access brokers are the latest cybercriminals targeting Australians. Here's how they work

In some ways, the newest cybercriminals attacking Australia are a lot like real estate agents. It's all about location, location, location. Marketing is key, of course, and so is plenty of stock. And, like the housing market, there's plenty of money to be made. A big difference is that when real estate agents hand over the keys, it's not a crime. Known as initial access brokers, this emerging class of hackers use their specialist skills to break into businesses and then sell usernames and passwords — the keys, so to speak — to ransomware gangs on the dark web. They've become an integral part of the cybercrime economy and the cost to Australians is clear. The federal government now estimates digital crime is costing the economy $29 billion a year. The Australian Cyber Security Centre last year revealed that, on average, a cybercrime report is made every six minutes — a frequency that's been steadily increasing over the past two years.

LastPass Warns of Deepfake Phishing Attempt

Password Manager software developer LastPass warned that one of its employees was targeted by a social engineering attack that used an audio deepfake which impersonated the company's CEO. Fortunately, the (trained) employee grew suspicious and avoided falling for the attack. You can count on the fact that other password manager software companies are attacked as well. LastPass warns that the technology to create deepfakes is now widely available, so these types of attacks will likely continue to increase. Increasing awareness of these techniques is a crucial defense against these attacks.

Microsoft Warns: North Korean Hackers Turn to AI-Fueled Cyber Espionage

Microsoft has revealed that North Korea-linked state-sponsored cyber actors have begun to use artificial intelligence (AI) to make their operations more effective and efficient. The company specifically highlighted a group named Emerald Sleet (aka Kimusky or TA427), which has been observed using LLMs to bolster spear-phishing efforts aimed at Korean Peninsula experts. The adversary is also said to have relied on the latest advancements in AI to research vulnerabilities and conduct reconnaissance on organizations and experts focused on North Korea, joining hacking crews from China, who have turned to AI-generated content for influence operations.

Five people arrested in Australia over global cybercrime, phishing attacks

Five Australians were arrested as part of a global operation against a cybercrime platform called LabHost, which criminals used to steal personal information like banking logins and credit card details through phishing attacks. This platform was instrumental in tricking victims into providing their personal data, affecting over 94,000 Australians among other global targets. The Australian Federal Police's operation involved 22 raids across five jurisdictions, leading to these arrests and the dismantling of LabHost's domain along with 207 criminal servers. These servers hosted fraudulent phishing websites mimicking legitimate banks and government portals, such as the myGov online portal, presenting a potential harm of $28 million to Australians. The operation was part of a larger effort that saw additional arrests in other countries, highlighting the international scope of cybercrime enforcement.

Australian digital ID bill finally passes the Senate

The Australian Senate recently passed the Digital ID Bill, setting the foundation for Australia's first comprehensive digital identity scheme, which aims to extend to the private sector as well as state and territorial governments. The legislation, supported by various parties including the Greens and the Jacqui Lambie Party, aims to enhance the existing digital ID accreditation system by boosting privacy, consumer protection, and governance. A key feature of the scheme, highlighted by the Greens, is its voluntary nature and the requirement for service providers to offer non-digital alternatives. The bill's passage is seen as a crucial step in strengthening the framework for digital identities in Australia, allowing for more streamlined interactions with businesses and government entities without the need to repeatedly share personal identification documents.

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.

15/04/2024 - CISA - Joint Guidance on Deploying AI Systems Securely

Our Views:

Business Email Compromise - Threat actors leveraging MFA bypass

Over the last nine months, we have seen a notable increase in large-scale Adversary in the Middle (AiTM) phishing and Business Email Compromise (BEC) attacks targeting organisations. In many cases, Multi-Factor Authentication (MFA) was in place and it appears that attackers were able to bypass these defences.

A Brief Overview of Adversary-in-the-Middle (AitM) Attacks

AitM attacks are characterised by their active engagement, going beyond passive eavesdropping to actively manipulate data and communications. This makes them a potent threat in the cybersecurity landscape. The concept of AitM attacks is rooted in the historical development of Man-in-the-Middle (MitM) attacks, which originally emerged as a means of intercepting communications between two parties. Today, AitM attacks have evolved to become highly sophisticated and malicious. They can manifest in various forms, including: Credential Harvesting, Data Manipulation, Phishing and Malware Delivery.

Phishing

Social engineering plays a crucial role in the effectiveness of phishing attacks. For instance, cybercriminals often use legitimate credentials and personally identifiable information (PII) from previous breaches to impersonate employees convincingly. They deploy various social engineering tactics to manipulate IT service desk personnel into resetting passwords, disabling multi-factor authentication (MFA), or registering new devices to specific accounts. This strategy is particularly effective against employees with privileged access, who are often identified through basic searches on platforms like LinkedIn. These techniques significantly increase the likelihood of the initial phishing email being clicked on, leading to successful breaches. There are a number of phishing-as-a-service toolkits that have become prominent (e.g. Evilginx2). These are the tools used to create phishing pages that mimic reputable services to capture the credentials, tokens, and cookies.

How AiTM phishing works

AiTM (Adversary in The Middle) phishing is a type of cyberattack where a hacker tricks a user into thinking they are logging into a legitimate website, but they are actually interacting with a fake site controlled by the hacker. Here's a simpler breakdown of how it happens:

- Why Session Cookies Matter: Imagine logging into a website and getting a special pass that tells the website you are already logged in, so you don't have to enter your password on every page. This "pass" is what we call a session cookie.
- Creating a Convincing Fake Site: The hacker sets up a fake website that looks just like the real one you intend to visit. This fake site is a trick; it's set up to intercept and pass along all the information you try to send to the real site.
- How the Trick Works: When you enter your login details on the fake site, the hacker's site sends your information to the real site behind the scenes. This makes everything look normal to you, as you can still see your account and do things as if nothing is wrong.
- Stealing the "Pass": As you log in, the fake site steals the session cookie—the "pass" that proves you are logged in. With this cookie, the hacker can get into your account on the real site without needing your password.
- Taking Control: Once the hacker has your session cookie, they can access your account, read your messages, make purchases, or do anything that you could do, even if you have extra security like two-factor authentication.

This attack is particularly sneaky because it's hard to notice and can bypass extra security measures. It highlights why it's important to check the URL in your browser's address bar before logging into any site to make sure it's the legitimate one.

Defending against AiTM phishing and BEC

The rise of AiTM (Adversary in The Middle) phishing campaigns underscores the adaptive nature of cyber threats in response to security defenses organisations put in place. Despite AiTM's ability to sidestep Multi-Factor Authentication (MFA), it's important to recognise that MFA remains a critical component of identity security. MFA's effectiveness is so notable that it has prompted the evolution of sophisticated phishing techniques like AiTM. To bolster defenses against such advanced threats, organisations can adopt several strategies:

- Implement Phishing-Resistant MFA: Utilising solutions that support Fast ID Online (FIDO) v2.0 and certificate-based authentication can create a more secure authentication environment that is resistant to phishing.
- Enable Conditional Access Policies: These policies are crucial as they are evaluated each time an attacker tries to use a stolen session cookie. By enforcing policies that recognise only compliant devices or trusted IP addresses, organisations can mitigate the risk posed by stolen credentials.
- Deploy Advanced Anti-Phishing Solutions: Investing in technologies that monitor and evaluate the security of incoming emails and the websites users visit can help prevent phishing attacks. Enhanced browser security features that identify and block malicious websites are particularly effective.
- Continuous Monitoring for Suspicious Activities: Vigilance is key in cybersecurity. Monitoring for signs of unusual activities, such as odd sign-in attempts (from unexpected locations or devices) or strange mailbox activities (like creating suspicious inbox rules), can help identify and mitigate potential breaches early.

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: