NZ Incident Response Bulletin

Standard Edition – October 2024 – Issue #69

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

Cyber threats: SMEs don't know where to start

Small and medium enterprises (SMEs) face significant cyber risks, with a one in three chance of experiencing a cyberattack, according to research from New Zealand's National Cyber Security Centre (NCSC). Despite these risks, many SMEs lack essential cybersecurity measures, such as regular data backups and software updates. The NCSC's Cyber Security Behaviour Tracker shows that 36% of SMEs have experienced attacks, but only a small portion take proactive steps before incidents occur.

The study highlights that while more than half of SMEs recognize the importance of cybersecurity, many struggle to prioritize it among other business concerns. The NCSC has developed tools like the "Own Your Online" website to assist SMEs in improving their cybersecurity posture, but many continue to react only after incidents occur, focusing on mitigation rather than prevention. The NCSC encourages SMEs to adopt more forward-thinking cybersecurity strategies.

Kiwi businesses hijacked by scammers: Facebook 'needs to have some responsibility'

New Zealand businesses are increasingly falling victim to a scam targeting Facebook pages, where scammers hijack accounts by posing as advertisers. Hawke's Bay farmer Sally Newall, who runs the "Kiwi Country Kids" Facebook page, had her account stolen after clicking a link from scammers, who now post inappropriate content on her page. Despite numerous reports, Facebook has not taken action, leaving Newall and other victims struggling to regain control.

Social media experts and Netsafe confirm that such scams are becoming more common, urging affected users to persist in reporting the issue to Facebook. However, many victims, like Newall, express frustration with the lack of response from Facebook, calling for the platform to take more responsibility in protecting users and their businesses.

Privacy complaint lodged over IRD's data-sharing with social media companies

A privacy complaint has been lodged against New Zealand's Inland Revenue Department (IRD) for sharing anonymized taxpayer data with social media platforms like Facebook for targeted marketing. David Buckingham, a Queenstown consultant, argues that the anonymization process used by IRD is inadequate and could allow companies to access financial information, violating individuals' privacy. Buckingham has called on the Privacy Commissioner to investigate whether this practice is legal.

In response, IRD acknowledged concerns raised by international regulators and stated it would reassess its data-sharing practices to ensure the ongoing safety of using anonymization techniques.

Security threats facing New Zealand detailed in just-released NZSIS report

The New Zealand Security Intelligence Service (NZSIS) report highlights increasing internal threats to national security, including espionage, unauthorized information disclosure, and terrorism. It emphasizes that foreign interference and espionage are ongoing risks, especially with New Zealand's strategic location in the Pacific. Violent extremism, particularly lone-wolf attacks, remains a significant concern, along with individuals motivated by mixed, unstable ideologies. The report also underscores the growing complexity of security threats, driven by global geopolitical tensions, with insider threats from trusted individuals being a notable risk. The NZSIS calls for greater vigilance and cooperation to mitigate these evolving dangers.

Kiwis lost $6.8 million to cybercrime last quarter

Kiwis lost $6.8 million to cybercrime in the second quarter of 2024, a significant amount largely driven by a few high-value incidents. Most of this loss came from just 11 reports, totalling $5.5 million, with $3.6 million resulting from unauthorized access to systems. The National Cyber Security Centre (NCSC) emphasized the seriousness of unauthorized access, as it allows attackers to potentially commit crimes unnoticed within compromised systems.

Australia

Facebook admits to scraping every Australian adult user's public photos and posts

Facebook has admitted to scraping all public photos and posts of Australian adult users to train its artificial intelligence models without offering an opt-out option, unlike in the European Union. Meta's global privacy director acknowledged that since 2007, unless users explicitly set their posts to private, their data was collected. Despite mounting concerns over privacy, Australian users remain without the legal protections that are available in Europe. Critics urge Australia to update its privacy laws to prevent such data exploitation.

World

LinkedIn scraped user data for training before updating its terms of service

LinkedIn reportedly scraped user data to train its AI models before updating its terms of service to reflect this practice. The company collected public profile information, including posts and images, to improve machine learning capabilities. This data usage occurred before LinkedIn formally communicated the policy change to its users, raising privacy concerns. The move has sparked criticism over transparency and user consent, with privacy advocates urging LinkedIn to offer clearer opt-out options and greater transparency in data handling practices.

Meta fed its AI on almost everything you've posted publicly since 2007

Meta has admitted to using publicly available data from Facebook and Instagram, including photos and posts, to train its artificial intelligence models. This data collection raises concerns about user privacy, as it includes large-scale data scraping without explicit consent. Meta's use of personal content for AI training, while mentioned in its policies, has sparked debate over transparency and user control, with calls for clearer communication and opt-out options for users who do not wish to have their data used in this way.

China-linked APT group Salt Typhoon compromised some U.S. internet service providers (ISPs)

China-linked threat actors, identified as Salt Typhoon, breached a U.S. internet service provider (ISP), as reported by security researchers. The group exploited vulnerabilities to gain access, potentially for espionage or intellectual property theft. Salt Typhoon has a history of targeting telecommunications and critical infrastructure. This incident highlights growing concerns about the cybersecurity of ISPs and the potential for national security risks. The breach underscores the importance of stronger defenses against advanced persistent threats (APTs) from state-sponsored actors.

AT&T pays $13 million FCC settlement over 2023 data breach

AT&T agreed to pay a $13 million settlement to the FCC over a 2023 data breach that exposed customer information. The breach affected 9 million customers and involved sensitive data, such as names and phone numbers. The FCC's investigation revealed that AT&T failed to protect its customers' privacy adequately, leading to unauthorized access. The settlement includes both fines and commitments to improve data security measures, highlighting the importance of protecting customer information in the telecommunications industry.

Germany seizes leak site of 'Vanir' ransomware operation

German authorities seized servers belonging to the Vanir ransomware group, which had been used for leaking stolen data. The seizure is part of a broader crackdown on ransomware operators, disrupting their ability to publish and extort victims. Vanir had been involved in high-profile attacks, and this operation marks a significant blow to their activities. The takedown follows international cooperation, highlighting ongoing efforts to combat ransomware and hold cybercriminals accountable.

Record $65m Settlement for Hacked Patient Photos

A healthcare provider agreed to a record $68 million settlement following a 2023 data breach that exposed sensitive patient information. The breach impacted over a million patients, leaking personal and medical data. This settlement highlights the severe legal and financial consequences of failing to secure patient information under healthcare privacy laws. The case underscores the importance of robust cybersecurity measures in protecting sensitive data within the healthcare sector.

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.

18/09/2024 – People's Republic of China-Linked Actors Compromise Routers and IoT Devices for Botnet Operations

26/09/2024 – International Partners Release Guidance on Detecting and Mitigating Active Directory Compromises

Our Views:

Dark Web Monitoring – Data Leak v Forums

Introduction

Both data leak sites and dark web forums play significant roles in the cybercriminal ecosystem, but they serve different purposes and present unique challenges for organisations trying to defend against cyberattacks. Understanding their differences is crucial for crafting a comprehensive dark web monitoring strategy.

Data Leak Sites

Data leak sites are platforms where cybercriminals, especially ransomware groups, post stolen data as leverage to pressure victims into paying ransom. These sites are typically maintained by organised criminal groups and are used to publish sensitive information if a ransom is not paid. The primary function of these sites is extortion and showcasing proof of a breach, offering a threat to further release confidential or sensitive data.

Monitoring data leak sites is relatively straightforward in comparison to forums. These sites are often public or semi-public, designed to attract the attention of the victim or external parties. However, they can still present challenges, such as requiring manual interventions when CAPTCHA or anti-scraping tools are used to block automated monitoring systems. Additionally, attackers often remove data after negotiations, limiting the window for organisations to respond. Organisations need to act swiftly when their data appears on these sites to minimise damage and take appropriate action, including breach notification and legal responses.

These sites have become central to modern ransomware operations, where cybercriminals publish small portions of data to prove they have sensitive information. If the victim does not comply with ransom, the rest of the data is leaked. This tactic, known as "double extortion," is a growing trend where not only is a ransom demanded to decrypt files but also to prevent the exposure of stolen data.

Dark Web Forums

Dark web forums, on the other hand, serve as broader discussion and marketplace environments where cybercriminals communicate, share techniques, and buy or sell illegal goods, including stolen data, malware, and hacking tools. These forums are not solely dedicated to leaking stolen data but are also places where criminal networks organise, collaborate, and trade resources. Membership in some forums can be exclusive or require invitations, which makes access more difficult for monitoring.

Forums are often harder to monitor due to their hidden nature. Many forums require invitations or vetting processes for new members, meaning even security researchers can face difficulties gaining access. Forums frequently use encryption and anonymity tools like Tor, making it challenging to trace conversations or individuals. They are also temporary in nature, with some forums disappearing or rebranding frequently to avoid law enforcement detection, further complicating monitoring efforts.

Dark web forums are more versatile and act as the breeding grounds for cybercrime. Criminals use them to share tactics, techniques, and procedures (TTPs) to launch ransomware attacks. These forums allow actors to collaborate, obtain initial access tools, malware, and zero-day exploits, and even recruit insiders from targeted organisations. They also help cybercriminals find buyers for stolen data or credentials, enabling broader criminal activities beyond extortion.

Monitoring dark web forums requires more sophisticated techniques. Automated scrapers are used but often need to be tailored to work in these highly anonymous and encrypted environments. Human analysts play a critical role in manually navigating and interpreting conversations, identifying emerging threats, and extracting useful intelligence. The broad volume of data in these forums makes it difficult to distinguish between real and exaggerated threats, adding complexity to the monitoring process.

Conclusion

Both data leak sites and dark web forums are essential elements of the cybercriminal infrastructure, but they serve distinct functions. Data leak sites are primarily used for extortion following ransomware attacks, whereas dark web forums are used for broader criminal collaboration, planning, and trade. Effective monitoring of both requires a combination of automated tools and human expertise to overcome the challenges presented by encryption, anonymity, and the sheer volume of data.

By incorporating strategies for monitoring both types of platforms, organisations can stay ahead of cybercriminals, respond to emerging threats more efficiently, and protect their sensitive data from being exploited.

Feel free to contact us to discuss your Dark Web monitoring requirements.

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

Further Resources:

Alerts	Data Breach Response	Forensic Technology
Cyber Incident Simulations	Social Media Investigations	Guide for NZ Law Firms

Share our Bulletin: