NZ Incident Response Bulletin

Standard Edition – April 2022 – Issue #39

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

[$6.6 million lost to cybercrime in the December quarter]

A record $6.6 million was lost to online financial crime during the quarter ending December, the largest amount lost to digital fraud in a quarter since records began, Cert NZ says in its latest quarterly report. There has been a 28 per cent increase in phishing and credential harvesting, where a fake email or text message was used to take a victim's personal information. New types of scams were on the rise, with reports of the Flubot text scam, which encouraged victims to pay for a non-existent courier package, with 1,707 instances reported.

However Cert NZ chief executive, Rob Pope, said a rise in reported scams was not entirely a bad thing. "On the one hand, more reports means that more incidents are occurring, but it also means New Zealanders are aware of the steps to take when they encounter cybercrime," Pope said.

[Police warn New Zealanders over WhatsApp impersonation scam]

Police are warning New Zealanders to be wary of a scam circulating in the community via WhatsApp. The scammers are impersonating family members or friends, saying they are in difficulty and in need of money. "Victims of this scam have received a message from an unknown number, claiming to be a loved one who has just lost their phone and got a replacement," police said in a statement. "The scammer then attempts to obtain the victim's credit card information."

Police said, while these types of scams are virtually ever-present, some people are more vulnerable than others. "We urge people to have conversations with vulnerable or elderly family members, to help ensure they are aware of the tactics often used by scammers and don't become victims," police said. "Police's message on scams like this is simple - do not engage with anyone on the phone and if you think you are being scammed, report the incident immediately." If you suspect someone might be impersonating a loved one, ask if you can call them back, police said. If possible, ask them a personal question too, like their date of birth, name of a sibling, pet name or maiden name. Anyone who believes they are a victim of a scam should immediately report it to their bank and then to their local police. Online scams should be reported to the Government online security agency, CERT NZ.

[GCSB collaboration with cloud service providers wins industry award]

Collaboration between the Government Communications Security Bureau (GCSB) and two major cloud service providers has been judged the best security project in the annual information security industry iSANZ awards. The GCSB worked with Microsoft and Amazon Web Services to have its government information security standards (NZISM) built into product templates for the deployment of cloud products.

The GCSB's Director-General, Andrew Hampton, said the collaboration with Microsoft and Amazon Web Services recognises the importance of government working closely with private-sector providers to ensure information security is built into the development and deployment of systems across all phases of their lifecycle. "In recent years, we have seen malicious actors increasingly exploit vulnerabilities in supply chains. It is more important than ever that cyber security is seen as an end-to-end consideration. By incorporating the NZISM standards into their cloud products, Microsoft and Amazon Web Services are making it easier for government and private-sector customers to ensure the security of their cloud deployments."

World

The Largest Online Marketplace of Stolen Login Credentials Seized by Law Enforcement

On March 16, 2022, a federal grand jury put on trial Igor Dekhtyarchuk, a citizen of the Russian Federation (Russia), with charges for running a cyber-criminal marketplace that sold thousands of stolen login credentials, personally identifiable information and authentication tools. Dekhtyarchuk ran Marketplace A, which allegedly sold credentials of over 48,000 hacked email accounts, 39,000 internet accounts and had an average visitor count of 5,000 people every day. Marketplace A specializes in the selling of illegally obtained access devices for compromised online payment platforms, retailers, and credit cards, and also provides data associated with such accounts, such as users' names, names and addresses, account credentials, and credit card data. This operation is known as a "carding shop."

Anonymous hacked Nestlè and leaked 10 GB of sensitive data

The popular Anonymous hacktivist collective announced to have hacked Nestlè and leaked 10 GB of sensitive data because the food and beverage giant continued to operate in Russia. The popular Anonymous hacktivist collective recently declared war on all companies that decided to continue to operate in Russia by paying taxes to the Russian government. Nestlè is one of the companies that is still operating in Russia after the invasion and Anonymous first threatened the company then hacked it. Today the group of hacktivists announced to have hacked Nestlè and leaked 10 GB of sensitive data, including company emails, passwords, and data related to business customers.

Marshall Islands telecom service hit by cyber attack

When internet systems in the Marshall Islands went on the blink in mid-March, it wasn't immediately clear what was causing the rolling outages. Home, business and government DSL and dedicated lines as well as mobile 4G services became intermittent or non-functional, forcing the National Telecommunications Authority (NTA) to repeatedly issue messages updating customers about "intermittent disruptions" and "urgent maintenance" needed to restore service. Information technology and security staff at NTA responded by working long nights to fix and reboot the systems. "But then in the morning, we were getting the same error messages," said NTA CEO Tommy Kijiner, Jr. Friday. "After several days, it became apparent that NTA systems were shutting down as the result of a large-scale "distributed denial of service" (DDoS) attack, he said.

Lapsus$ Infiltrates High Profile Victims Through Employee Accounts

Since its discovery in December 2021, the Lapsus$ ransomware gang has been incessantly adding high profile victims to its list. After NVIDIA and Samsung last month, the threat actor has now attacked Microsoft and Okta. It is time to take a glance into the group's attack vectors. Microsoft has published an analysis of Lapsus$, also referred to as DEV-0537. The analysis has detailed the attack vectors used by the group to gain initial access. The TTPs are diverse, indicating that the actor is motivated by destruction and theft.

- The group deploys the RedLine password stealer to get access to session tokens and passwords.
- It buys session tokens and credentials from underground forums.
- Lapsus$, furthermore, pays employees at targeted firms for access to credentials and MFA approval.
- The gang sifts through public repositories for exposed credentials.

Lapsus$ leverages these credentials and session tokens to access internet-facing systems and apps. These systems are VPN, RDP, and VDI solutions.

"It's coming": President Biden warns of "evolving" Russian cyber threat to U.S.

President Biden warned Monday that "evolving intelligence" suggests Russia is exploring options for potential cyberattacks targeting U.S. critical infrastructure. "The magnitude of Russia's cyber capacity is fairly consequential," Mr. Biden said, addressing the Business Roundtable, an association of some of the nation's largest corporations. "And it's coming." While there's no evidence of any specific cyberattack threat, Anne Neuberger, Mr. Biden's deputy national security adviser for cyber and emerging technology, told reporters Monday afternoon that U.S. officials have observed "preparatory work" linked to nation-state actors. Such activity could indicate increased levels of scanning websites and hunting for vulnerabilities among U.S. companies.

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 our YouTube Channel and this webpage.

Alerts

1 March 2022 – Network Infrastructure Security Guidance

News Clips

23 March 2022 - Russia preparing to launch cyberattacks in U.S., FBI says

Our Views:

Forensic Technology in Employment Investigations

Over the last 12 months, we have seen an increasing number of cases involving employees stealing intellectual property. In this month's bulletin, we provide an overview as to how best to manage your forensic investigation.

Firstly, there are a number of complicating factors that need to be considered, such as the security on devices, particularly when they are owned by the employee but used for work purposes. Secondly, it is important to act quickly and preserve volatile evidence such as audit log data. Thirdly, all of the actions taken need to comply with the relevant laws so that the evidence can withstand legal proceedings.

A forensic technology expert can assist in securing electronic data and maintaining its evidential value throughout the investigation. The forensic expert will uncover the "who, what, when, where and how" relating to the evidence at issue. This work must be underpinned by robust methodologies, evidentially sound processes and suite of forensic tools that are fit for purpose and have been accepted by the courts.

The following is a list of considerations when engaging a forensic expert to assist you with an employment investigation:

- brief the expert appropriately on the background and purpose of the case
- be satisfied your expert has the necessary resources including a well-equipped laboratory
- provide the expert with the terms of reference which sets out objectives, timeframes and limitations
- confirm what data is required to be collected and examined
- confirm whether the investigation needs to be covert and that your expert can work within these requirements.

We recommend that all physical devices be preserved for potential forensic examination at the outset of your investigation. This includes copying the hard drive from a laptop, the contents of a mobile device, cloud data, and any other removable devices such as USB keys.

In particular, if you are seeking to examine deleted data, there are a number of considerations that may impact on the success or otherwise of recovering this information, including:

- how long ago the files were deleted
- where the files were deleted from (such as a USB device or a laptop)
- whether a record of deleted files is available, particular for cloud storage accounts
- what the format of the deleted file is (documents are easier to recover than emails).

As internet users post their personal details online, social media has become a potential goldmine of evidence for employment investigations. Evidence from social media activities can be collected either directly from the cloud provider or extracted from the device which was used by the employee to post the content, including content which has long since been deleted from the cloud version.

Mobile devices contain a rich source of evidence including "to-do" lists, photos and GPS coordinates. They store a considerable amount of data and the technology employed on such devices is rapidly evolving. Success factors for examining mobile devices depend on the make and model, the software version installed on that device, and the nature of the data being sought. Always remember that data transmitted from a mobile device may also exist in the cloud. However, you may not be permitted to access the cloud data from your work owned device. Check with a lawyer first.

Finally, it is important to note the difficulties associated with cloud computing. Over recent years organisations have moved a significant amount of data into the cloud, with varying degrees of traceability in relation to employee activity. If you suspect your employee has taken your confidential information, you should immediately instruct your IT providers to preserve as much data as possible that is in the cloud. Your success of recovering relevant data will be dependent on the cloud systems licensing, audit retention policies, and whether it records files that have been copied or deleted.

Please do talk to us if you have a requirement to conduct a forensic technology investigation.

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: