NZ Incident Response Bulletin

Standard Edition – May 2022 – Issue #40

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

Official Visit of the Right Honourable Jacinda Ardern, Prime Minister of New Zealand, 18 to 20 April

President Halimah and Prime Minister Ardern reaffirmed the strong and multifaceted relations between Singapore and New Zealand. The Prime Ministers noted that there have been frequent exchanges between Singapore and New Zealand cyber security experts since a Cyber Security Memorandum of Arrangement was signed in 2019.

Wide-ranging discussions have covered the resilience of critical infrastructure and SMEs to cyber incidents, cyber security workforce development, Internet of Things security, ransomware and cooperation with the private sector for stronger cyber outcomes.

The Prime Ministers directed their respective cyber security leads (Chief Executive of Cyber Security Agency of Singapore and the New Zealand Prime Minister's Special Representative for Cyber and Digital) to meet virtually to discuss opportunities to further deepen the cyber security partnership between the two countries.

Foreign Minister Nanaia Mahuta says Pacific leaders may need to meet as Solomon Islands prepares to ink China security deal

Foreign Minister Nanaia Mahuta says Pacific leaders want "greater clarity" from the Solomon Islands about their contentious China security deal and may need to bring forward a crucial regional meeting.

Among provisions, the agreement promises an "expanded development programme" to build economic resilience, to strengthen Fiji's disaster response, and to support "capability to uphold sovereign authority over our land and maritime territories", and expand cooperation in policing, cyber-security and intelligence. "Cyber-security is a really new area, so the more we can strategically cooperate on cyber issues, then, I guess the more resilient what we do across the Pacific can become," Mahuta said.

FluBot: Nasty phone virus sends spam messages that can cost you thousands

Hundreds of thousands of spam text messages are pouring into inboxes all around the country every day and it is largely due to FluBot - the malware that arrived in New Zealand late last year. Your mobile phone company filters out most of the spam messages coming into the country, but FluBot is a bit different because it is actually a virus rather than traditional spam.

Mobile phone companies and CERT, the Government's Cyber-Security Response Team, have been working with the Department of Internal Affairs (DIA) to tackle the problem, but it largely comes down to the phone's owner having to reset it to its original factory state. For some, that might just be a step too far as they haven't backed up anything from their phones and don't want to lose all that content (always back up your phone, and computer).

An infected phone is constantly blasting out these text messages – on average around 5,000 a day for the duration of the infection. That's a huge risk to the rest of us who are being bombarded with spam, but also to the person sending those messages as some get sent internationally - and that comes at a cost. If you send 3,000 international text messages a day for five days - the average duration most phones are infected for – that would be an enormous phone bill.

The good news is it's relatively easy to remove FluBot from your phone. Resetting your phone to factory settings is all it takes - unfortunately you will lose whatever is on your phone when you do that, so you need to have everything you want to keep backed up first.

World

[The Perils and Promise of America's Older Cyber Regulatory Regime]

In October 2021, Josh Renaud exposed two dangerous flaws: one in the code of a website and another in the American cyber regulatory regime. As a reporter for a Missouri newspaper, Renaud located a vulnerability on a state agency's website which endangered the Social Security numbers of more than one hundred thousand educators. He disclosed the flaw to the state and ensured it was patched before he published a story about the incident. While many private companies pay handsome rewards to those who uncover and report vulnerabilities in their code, Renaud received little thanks from the Missouri state government. Instead, Gov. Mike Parson (R) accused the paper of violating a state anti-hacking law and ordered the State Highway Patrol's digital forensic unit to look into the incident, although a prosecutor later declined to bring charges.

In the wake of the controversy, Renaud has been declared the "poster child for overboard hacking laws." His ordeal highlights how decades-old laws fail to account for the realities of rapid digital development. The law referenced by Gov. Parson, the Computer Fraud and Abuse Act, makes it illegal to access personal information online without permission. It states that someone illegally tampers with data if they "knowingly and without authorization" access "a computer, a computer system or a computer network, and intentionally examines information about another person." The prosecutor who declined to press charges asserted, "the law does appear to be so vague that it basically describes someone using a computer to look up someone's information."

[Latest Attacks Target Entities Handling Sensitive Data]

Recent incidents affecting the sensitive information of tens of thousands of individuals underscore the ongoing threats and risks facing organizations - including medical care providers and social services agencies - that handle health and other delicate personal information. Augusta, Arkansas-based ARcare, a community health center that provides services including chronic disease management, behavioral health and HIV treatment, on Monday reported to the U.S. Department of Health and Human Services a hacking incident involving a network server and affecting more than 345,000 individuals.

A statement ARcare posted on its website Monday says that it experienced a data security incident that affected its computer systems and caused a temporary disruption to services. ARcare immediately worked to secure its systems and commenced an investigation to confirm the nature and scope of the incident, the statement says. ARcare concluded a review of affected data and determined that personal information relating to individuals was in affected files, the statement says.

[Over 30 Countries Take Part in NATO's 'Locked Shields 2022' Cyber Exercise]

NATO's Cooperative Cyber Defence Centre of Excellence (CCDCOE) on Tuesday kicked off the thirteenth instalment of Locked Shields, its annual live-fire cyber defence exercise. With more than 2,000 participants from over 32 countries, this complex international cyber exercise is meant to facilitate cooperation and coordination between nations, industries, and public and private organizations in preparing against state-sponsored cyberattacks.

Since 2010, the exercise has been testing the readiness of national, military, and civilian IT systems against attacks targeting vital services and critical infrastructure by simulating a realistic, large-scale assault against an entire nation. This year's scenario involves Berylia, a fictional island country in the northern Atlantic Ocean, victim of a series of crippling coordinated cyberattacks that disrupted the operation of government and military networks, communications, electric power grid, and water purification systems.

A Red Team vs. Blue Team exercise, this year's event will involve roughly 5,500 virtualized systems that will face more than 8,000 cyberattacks. Locked Shields 2022 has 24 participating Blue Teams – with an average of 50 experts each – that will take the role of national cyber Rapid Reaction Teams, scrambling not only to secure complex IT systems, but also to effectively report incidents and solve forensic, legal, media operations and information warfare challenges.

[Google Blows Lid Off Conti, Diavol Ransomware Access-Broker Ops]

Google's Threat Analysis Group (TAG) has provided a rare look inside the operations of a cybercriminal dubbed "Exotic Lily," that appears to serve as an initial-access broker for both Conti and Diavol ransomware gangs. Researchers' analysis exposes the business-like approach the group takes to brokering initial access into organizations' networks through a range of tactics so its partners can engage in further malicious activity.

While ransomware actors tend to get most of the attention, they can't do their dirty work without first gaining access to an organization's network. This is often the job of what are called initial-access brokers (IABs), or "the opportunistic locksmiths of the security world," as Google TAG calls them. "It's a full-time job," Google TAG researchers Vlad Stolyarov and Benoit Sevens wrote in the post. "These groups specialize in breaching a target in order to open the doors — or the Windows — to the malicious actor with the highest bid."

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

28 April 2022 – Joint Cyber Security Advisory: Top 15 routinely exploited vulnerabilities of 2021

News Clips

17 April 2022 - Former NSA Director on cybersecurity risks from Russia

Our Views:

Multi-Factor Authentication – Prompt spamming and Fatigue Attacks

MFA 101

Multifactor Authentication (MFA) for authentication has become an essential component of many cybersecurity strategies. It is the process of using two or more factors to validate a user's identity. The three common factors used in MFA are:

a) something you know, like a password or PIN;
b) something you have, like a mobile device; and
c) something you are, like a fingerprint, optics or voice.

For those coming to the MFA party a bit late, enabling MFA strengthens your security by ensuring an attacker must have access to more than one of these authentication factors to breach your systems successfully.

Passwords and PINs can be susceptible to leaks, successful guesses, or brute-force and phishing attacks. Therefore MFA supplements these fundamental measures with other factors, such as something you are (fingerprint) or something you have (unique mobile device) for additional protection. Current tools for enabling MFA include SMS, One Time Passwords (OTP), and push notifications from an Authenticator App.

MFA is one of the best cybersecurity controls an organisation can implement and is therefore strongly recommended; however, it suffers from both human and technical weaknesses, which means that it is not a silver bullet. Increasingly we see attacks that target and successfully bypass MFA protections.

Attacks against MFA

On a daily basis (particularly in large organisations or those with multiple systems), users are now bombarded with notifications, emails, alerts and pop-ups asking them to accept authentication requests. As a result of this overload, users experience "acceptance fatigue", which increases the risk of users clicking, swiping, or accepting notifications without genuinely looking at what they are.

Cybercriminals are taking advantage of this acceptance fatigue by conducting attacks that flood a user's authentication app with push notifications, hoping they will accept and enable entry to an account or device. Sometimes called MFA Prompt spamming or MFA Fatigue Attacks, these relatively simple techniques are effective as they target the human factor using social engineering.

In an MFA prompt spamming attack:

1. The adversary uses previously stolen valid username/password credentials to log in to an account protected by push MFA and does this multiple times in succession;
2. The victim then receives valid push notifications (generally to a mobile app of some sort) over and over;
3. Eventually, the user (or a child using their parents work mobile device for gaming) tires of this notification flood and taps "yes" instead of "no."

Often, users will accept the notification because they are distracted or overwhelmed by the notifications. However, in some sophisticated cases, the attack can be misinterpreted as a bug or a legitimate request. For example, a child on their parent's phone swiping yes to rid the screen of a pop-up that stands in their way of watching YouTube.

The cyber security company Mandiant recently reported on the ongoing activity of UNC2452 (a Russian-state-sponsored APT group) that use these techniques to successfully bypass Multi-Factor Authentication (MFA) and compromise their targets. This highlighted that MFA fatigue is proving troublesome globally even though it is not a sophisticated technical attack.

Prevention

MFA is an effective tool if configured well and used appropriately. Some suggestions for preventing MFA fatigue and combatting attacks on MFA are to:

- Consider using adaptive authentication methods. These methods leverage tools to minimise the number of login events and avoid users becoming bombarded by them. For example, they may only challenge using MFA when there is a known level of risk. Reducing the number of alerts keeps users from being de-sensitised to them.
- Protect against credential compromise. As these attacks usually rely on previously compromised credentials protecting identity is critical. To achieve this, some basic steps such as enabling MFA for all users in all locations and blocking easily guessed passwords should be used.
- Be strict in the period in which users must enrol themselves when introducing MFA to your organisation.
- Track alerts for new MFA and MDM device enrolments.
- Move away from legacy authentication protocols such as SMTP, IMAP, and POP. Many legacy authentication protocols cannot support MFA, and if these still exist within your organisation, they leave a possible hole in your defences, regardless of MFA use elsewhere. Microsoft provides a list of legacy authentication mechanisms that you should consider deprecating.
- Regularly review and test your organisation's MFA implementation and consider a review against an industry-accepted benchmark such as the CIS control benchmarks.
- Specific configurations to enhance MFA security in Microsoft environments and reduce MFA fatigue include:
  - Enabling Azure MFA number matching/ MFA codes. These present a number to the user that they must type into the app to complete approval.
  - Implementing impossible travel detections
  - Implementing advanced authentication features using geography.
  - Implementing Identity Protection (Azure ID protection detects events such as atypical travel, malicious IP addresses, leaked credentials and more.)
  - Enabling the Additional Context in Notifications. These show the end-user which application is performing the MFA request.
  - Regularly review your enterprise app/OAuth consents in your Microsoft 365 tenancy. Check the name of the applications being granted, the permissions the applications have been granted, and the application author's validity.

Finally, improve user awareness of MFA spamming and social engineering attacks. Raising and enhancing understanding of MFA spamming and other new tactics is vital to ensure user vigilance. Ensure that users are aware that not all MFA requests are correct and educate them on how to detect and report malicious attempts.

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: