NZ Incident Response Bulletin

Standard Edition – October 2021

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.

Refer to our Premium Edition for additional information on Threat Alerts, Security Frameworks, Information Security Surveys, Forensic News and Research.

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

Ransomware incidents continue to rise

CERT NZ's latest report shows that ransomware incidents are on the rise. The Quarter Two (Q2) report, which highlights New Zealand-related cyber security trends between 1 April to June 30, shows there were more than 1,350 cyber security incidents responded to by CERT NZ, with almost $4 million in direct financial loss. Of the reports received, ransomware showed a significant spike (from 12 in Q1 to 30 reports in Q2), followed by unauthorised access. The number of phishing and credential harvesting reports dropped by 5% from the previous quarter, however remains the most reported incident category type.

Crypto heist: Raiders steal safe containing $4m in cryptocurrency from Westmere home

Raiders stole a safe containing $4 million in cryptocurrency in what appears to be a sophisticated "inside job" targeting a wealthy businessman's home. Mark Geor said his home was burgled while it was being renovated. "We have lived there since 2017 and never had an issue. This burglary was executed with surgical precision," he said. Forensic experts were unable to obtain fingerprints or footprints because of the concrete floors. "They won't have any idea of what's inside the safe. If they are able to crack it open, I think they will take out what they can sell. The cryptocurrency is on a USB stick among other USB sticks of family and wedding photos and wills ... If they find it they might think that's just paper and biff it or they could take it to people who do know about cryptocurrency. I am worried they now know more than they set out to know," Geor said.

SMS Scam Targets The NZ Public In Record Numbers

Te Tari Taiwhenua Department of Internal Affairs want to make the public aware of a large-scale malware scam which has generated thousands of complaints over a 24 hour period. The scam involves people being sent a text message indicating you have a parcel that is out for delivery, or that has failed, with a link included. This link is to a website that asks the recipient to download a new application to their phone.

Upon downloading the application, the recipient's phone will become infected with a piece of malware called "Flubot". If installed, it uses malware to steal personal information from your phone including banking details, passwords, and other sensitive information. The app then accesses your contacts and sends their details to the perpetrators of the scam and send additional text messages from your device to other people's contacts, further spreading the scam.

NZ Incident Response Bulletin

Standard Edition – October 2021

World

Port of Houston Quells Cyber-Attack

The Port of Houston Authority (Port Houston) successfully defended itself against a cybersecurity attack in August. Port Houston followed its Facilities Security Plan in doing so, as guided under the Maritime Transportation Security Act (MTSA), and no operational data or systems were impacted as a result. Hackers exploited a previously unknown vulnerability in password management software to break into one of the port's web servers.

The threat actor installed malicious code to expand their access to the system. He then exfiltrated all the log-in credentials for a piece of Microsoft password management software used to control network access. "If the compromise had not been detected, the attacker would have had unrestricted remote access to the [IT] network," the unclassified report by US Coast Guard Cyber Command reportedly reads. "With this unrestricted access, the attacker would have had numerous options to deliver further effects that could impact port operations."

HSE cyber-attack: Irish health service still recovering months after hack

The first time Donna-Marie Cullen heard about a massive cyber-attack on Ireland's health system, it was on the morning news. The 36-year-old mother of two was waiting for her radiation treatment that afternoon for sarcoma, a rare and aggressive form of brain cancer. "I thought this is an awful situation for the HSE [the Irish health system] to be in," she says. "After that, I got a call at lunchtime and was told that my radiation wouldn't be going ahead because of the cyber-attack". The attack in May was unprecedented in the history of the Irish state, affecting almost every part of its healthcare system, already worn down by more than a year of fighting Covid-19.

REvil Affiliates Confirm: Leadership Were Cheating Dirtbags

After news broke that the cybercrime group REvil's was ripping off their affiliates by using backdoors & double chats, those affiliates took to the top Russian-language hacking forum to renew their demands for their share of ransom payments from REvil.

Apple says its security flaw was fixed. Cyber analysts warn zero-click threats will persist.

Cybersecurity analysts are urging Apple users to immediately update the software of their phones, computers and watches after the company issued an emergency security patch on Monday to prevent hackers from gaining access to the devices without the users knowing. In a new report, researchers at the University of Toronto's Citizen Lab said the NSO Group, an Israeli spyware company, used what is known as a "zero-click exploit" to access the phone of an unnamed Saudi activist. Researchers at Citizen Lab called the exploit "Forcedentry" and said it has been in use since February. They also revealed that the NSO Group's flagship "Pegasus" spyware program was used to infect the activist's device.

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

23 September 2021 – CERT - Active scanning for VMware vCenter Vulnerability

7 September 2021 – CISA - Microsoft Releases Mitigations and Workarounds for CVE-2021-40444

3 September 2021 – CISA - Atlassian Releases Security Updates for Confluence Server and Data Center

News Clips

5 September 2021 - Behind the booming ransomware industry: How hackers hold businesses hostage

NZ Incident Response Bulletin

Standard Edition – October 2021

Our Views: CIS Controls 10-12

This month we look at CIS controls 10, 11 and 12, comprising malware defences, data recovery and network infrastructure management.

CIS Control 10: Malware Defences

Prevent or control the installation, spread, and execution of malicious applications, code, or scripts on enterprise assets.

Why is it needed?

Cybercriminals design and deploy malicious software (otherwise known as malware, viruses, worms, trojans etc.) to achieve various goals such as data/credential theft and data encryption. Malware types in circulation are constantly changing, with sophisticated variants using machine learning and artificial intelligence to evolve. Modern malware variants are designed to avoid, disable, or deceive security defences, making it possible for them to enter a network and hide in systems until they have enacted their nefarious purpose.

Malicious software can enter an organisation's network through vulnerabilities in end-user devices, cloud services, webpages, or email attachments. Unfortunately, it is often successfully introduced via end-user behaviour such as clicking on a link, opening a malicious attachment, installing unauthorised software or inserting an infected USB stick. This control describes the necessary deployment and automation of malware defences at all entry points and enterprise assets for malware detection, containment, and control to combat these attacks.

How is it implemented?

The ability to detect and block malware can be achieved using traditional malware prevention and detection solutions. At the basic level, an organisation should ensure anti-malware solutions are deployed and maintained on all enterprise assets and that malware signature files are automatically updated. Enabling automatic vendor updates will allow Indicators of Compromise (IOC's) to remain current in a fast-moving landscape and enhance threat detection capability. Disabling autorun and autoplay options for all removable media is also a basic safeguard to protect against malware, and configuring automatic anti-malware scanning of removable media will help detect its presence.

Beyond the basic steps above, an organisation can consider enabling anti-exploitation features. These are solutions such as Microsoft Data Execution Prevention (DEP), Apple System Integrity Protection (SIP), and Windows Defender Exploit Guard (WDEG). In addition, malware solutions that utilise behaviour-based detection rather than just relying upon known malware signatures should also be considered for more advanced protection. Typically referred to as Next-Generation Antivirus solutions, they use predictive analytics driven by machine learning and artificial intelligence to prevent known and unknown attacks.

Finally, the ability to centrally collect logs is desired to support alerting, identification, and incident response. Enabling logging as outlined in the earlier CIS control 8 will support any investigation into how the malware entered the network and what it may have done while it was present.

CIS Control 11: Data Recovery

Establish and maintain data recovery practices sufficient to restore in-scope enterprise assets to a pre-incident and trusted state.

Why is it needed?

Most organisations rely upon data for making decisions and facilitating daily transactions. The uninterrupted availability of information is therefore crucial for maintaining smooth business operations. However, whilst some organisations can function without some information for a while, others may not be able to operate at all safely. As the unavailability of data can be an outcome of various cyber-attacks or the result of simple human error, all organisations require procedures for data recovery.

When attackers successfully compromise a network, they often make configuration changes to the systems, such as turning off anti-malware systems and alerts, adding or changing registry items, deleting logs, or opening ports to allow further exploitation. This makes the ability to recover data to a known and trusted state (before the compromise) vital to ensure a speedy recovery and minimise business interruption. The exponential rise of ransomware has also driven focus in this area. The ability to recover from a known and trusted state may avoid the necessity for a business to pay a ransom to unlock files. *(It is important to note here that ransomware schemes have evolved to include demanding payments to avoid leaking any stolen confidential data. Restoration (whilst extremely useful) would not help the recovery of data already exfiltrated).*

How is it implemented?

The basic level of this control involves establishing and maintaining a data recovery process. The scope of recovery efforts should be defined along with recovery prioritisation and the security requirements for all backup data. Backups should be automated for all in-scope assets and run at least weekly. Data in backups must be protected with equivalent security mechanisms as the primary data using tools such as encryption and data separation. Finally, an isolated instance of all recovery data should be established and maintained.

Once basic data recovery safeguards are in place, these should be tested. Once per quarter a testing team should evaluate a random sampling of the backups and ensure they can be restored onto a test environment. Verification that the operating system, application and all data are intact should occur.

CIS Control 12: Network Infrastructure Management

Establish, implement, and actively manage (track, report, correct) network devices, in order to prevent attackers from exploiting vulnerable network services and access points.

Why is it needed?

Network infrastructure refers to all of the devices that make up the network, including physical and virtual gateways, firewalls, access points for wireless networks, routers and switches. Network infrastructure can be vulnerable to attack when insecure default configurations are left in place, potentially increasing the attack surface with open services or ports, default accounts and passwords, support for vulnerable (older) protocols, or pre-installed but unneeded software.

As network configurations become outdated and insecure over time, attackers will take advantage of these vulnerabilities in the infrastructure. Maintaining a secure network infrastructure by regularly evaluating architecture diagrams, configurations, and access controls is, therefore, an essential line of defence.

How is it implemented?

CIS Control 12 has only one basic safeguard. This safeguard requires an organisation to ensure its network infrastructure is up to date. This is achieved by ensuring the latest stable software releases are run and/or using the current network as a service (NaaS) offering. In addition, software versions should be reviewed at least monthly to verify they are supported. This basic safeguard is essential for all businesses. For more advanced protection the following actions are desired:

- Establish and Maintain a Security Network Architecture that addresses segmentation, availability and principles of least privilege.
- Securely Manage Network Infrastructure by using tools such as secure protocols (SSH and HTTPS) and version-controlled infrastructure as code.
- Establish and Maintain Architecture and other Network and System Diagrams and Documentation.
- Centralise Network Authentication, Authorisation and Auditing (AAA).
- Use Secure Network Management and Communication Protocols (e.g., WPA2, 802.1X).
- Ensure Remote Devices use a VPN and AAA services prior to accessing the organisations' resources.

A final advanced safeguard encouraged in this control is establishing and maintaining dedicated resources for all administrative work (admin tasks or any task that requires admin access). These resources can be physically or logically separated and segmented from the primary network. They should not have any internet access.

NZ Incident Response Bulletin

Standard Edition – October 2021

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.

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: