NZ Incident Response Bulletin

Standard Edition – June 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

In May 2021, New Zealand forensic and cyber related news was dominated by a high-profile ransomware attack on a Government Agency. Given the significant coverage to date in the media, instead of listing the numerous articles, we are providing guidance to assist you in improving your cyber resilience and Incident Response preparedness, focusing on the threat of Data Leak Sites.

New Zealand Data Breach Response Guide

Understanding Ransomware and Data Leak Sites

CISA and MS-ISAC - Ransomware Guide

CISA - Technical Approaches to Uncovering and Remediating Malicious Activity

On 1 December 2020, the Privacy Act was updated to include mandatory notification requirements if serious harm could be caused to individuals whose data had been compromised. On 26 May 2021, the Privacy Commissioner John Edwards warned DHBs to address security failings identified in a Ministry of Health stocktake of health IT systems in 2020. The Privacy Commissioner also stated the need to:

1. *notify and offer support to the individuals identified in that information without delay.*

We recommend that notifications be conducted using specialist tools, which will also track and record which custodians have received your communications.

2. *actively monitor potential host sites on the Dark Web or elsewhere.*

As published in recent copies of this bulletin, we have seen an increasing number of New Zealand organisations being targeted and impacted with Ransomware, often resulting in data theft and publication. Our forensic examination over recent months of numerous ransomware notes, the associated malware and associated data leak sites has identified the following three data leak sources:

- Credential Monitoring. This is a cost-effective option to monitor known Dark Web sites for your compromised logins and passwords.
- Dark Web sites referenced in ransomware notes. Cyber criminals operating as part of organised crime groups are motivated for direct financial gain. Accordingly, they are increasingly publishing the Dark Web sites where they will publish compromised data. The monitoring of these sites requires a degree of technical knowledge and therefore carries a slightly higher price tag.
- Data Leakage Detection. If you do not know which Data Leak Site your compromised data may be published to, then you may need to conduct a more thorough monitoring exercise requiring specialist software and expertise, at a considerably higher cost.

NZ Incident Response Bulletin

Standard Edition – June 2021

World

Britain's ex-GCHQ chief has urged the government to ban ransomware payments to stop criminals profiteering from attacks.

Ciaran Martin, the founding chief executive of GCHQ's Cyber Security Centre (NCSC), spoke after the Irish health service was targeted by international criminals yesterday. The Prime Minister of Ireland refused to pay a ransom demand after the Health Service Executive (HSE) was plunged into chaos by the 'most significant cybercrime in the history of the State' which threatened the care of thousands of patients. Mr Martin said making these payments illegal would help stop the funding of organised criminals who forced businesses into helping pay for further attacks.

Colonial Pipeline boss confirms $4.4m ransom payment

Colonial Pipeline has confirmed it paid a $4.4m (£3.1m) ransom to the cyber-criminal gang responsible for taking the US fuel pipeline offline. The Wall Street Journal reported that Colonial Pipeline authorised the payment on 7 May because of uncertainty over how long the shutdown would continue. "I know that's a highly controversial decision," Joseph Blount said in his first interview since the hack.

This is how the Cobalt Strike penetration testing tool is being abused by cybercriminals

New research shows how Cobalt Strike is being weaponized in campaigns deploying malware ranging from the Trickbot banking Trojan to Bazar. The popular penetration testing kit, of which source code for version 4.0 was allegedly leaked online in 2020, has been abused by threat actors for years and has become a go-to tool for advanced persistent threat (APT) groups including Carbanak and Cozy Bear. The researchers say that the existing abuse of Cobalt Strike has been linked to campaigns ranging from ransomware deployment to surveillance and data exfiltration, but as the tool allows users to create malleable Command and Control (C2), it can be complicated to trace C2 owners.

Microsoft says group behind SolarWinds hack now targeting government agencies, NGOs

The group behind the SolarWinds (SWI.N) cyber attack identified late last year is now targeting government agencies, think tanks, consultants and non-governmental organizations, Microsoft Corp (MSFT.O) said on Thursday.

"This week we observed cyberattacks by the threat actor Nobelium targeting government agencies, think tanks, consultants, and non-governmental organizations", Microsoft said in a blog. Nobelium, originating from Russia, is the same actor behind the attacks on SolarWinds customers in 2020, according to Microsoft.

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

18 May 2021 – Incident Response Solutions – Ransomware (Updated 18 May 2021)

16 May 2021 – Ransomware Attack on Health Sector

14 May 2021 – CISA Publishes Eviction Guidance for Networks Affected by SolarWinds and AD/M365 Compromise

News Clips

11 May 2021 - Biggest US fuel pipeline shut down in cyber attack that “may originate in Russia”, BBC News

NZ Incident Response Bulletin

Standard Edition – June 2021

Our Views:

This month's theme is "Implementing Cyber Controls".

In previous bulletins we have discussed the importance of adopting a mature and trusted cybersecurity framework for guiding your cybersecurity improvement programme. We recommend the NIST cybersecurity framework for this purpose.

Additionally, we believe organisations will benefit from using an appropriate set of Cyber Controls that align with the cybersecurity framework to support their journey to cybersecurity maturity. The CIS controls provide clear, actionable items for immediate gains in cybersecurity posture.

The SANS Institute developed the CIS critical security controls in early 2008 due to an alarming number of US defence industrial base organisations suffering significant data losses. The controls were intended to act as best practice guidelines for computer security. They have since evolved to become a prioritised set of specific actions a business can implement for protection from known cyber-attack vectors.

The Controls at a glance

CIS controls version 8 were released in May 2021 consisting of 18 top-level controls and 153 safeguards (sub controls) that can guide you through the process of creating a layered or defence-in-depth cybersecurity strategy. This latest version focuses more heavily on cloud-based computing (full and hybrid environments), virtualisation, outsourcing, work-from-home and mobility. It also recognises changing attacker tactics. The list of top-level controls below displays the scope of the framework:

1: Inventory and Control of Enterprise Assets	7: Continuous Vulnerability Management	13: Network Monitoring and Defense
2: Inventory and Control of Software Assets	8: Audit Log Management	14: Security Awareness and Skills Training
3: Data Protection	9: Email Web Browser and Protections	15: Service Provider Management
4: Secure Configuration of Enterprise Assets and Software	10: Malware Defenses	16: Application Software Security
5: Account Management	11: Data Recovery	17: Incident Response Management
6: Access Control Management	12: Network Infrastructure Management	18: Penetration Testing

Each of the 18 controls have multiple safeguards (formally called sub-controls). We will be undertaking a deep dive of these over the coming months to describe what each one means practically and how it can be assessed and implemented.

Benefits of Implementation

The CIS Controls recognise that most organisations have limited resources which must be prioritised. The controls are tiered by way of Implementation Groups (IG), whereby organisations can continually assess their resource availability to determine whether they can increase their cyber improvements.

IG1 is for small businesses and start-ups with limited resources and is considered "basic security hygiene".

IG2 is for medium enterprises with moderate resources, therefore comprising a more extensive control set.

IG3 is for large organisations with significant resources, capable of implementing all the CIS controls and sub-controls.

The ability to prioritise and categorise the controls is what makes the CIS control set so effective in practice. It allows you to focus on a small number of actions that can significantly reduce cybersecurity risk and provide the most "bang for your buck".

The recently released 2021 Verizon Data Breach Investigations Report identifies a core set of CIS controls that they believe all businesses should implement regardless of size to protect against the most common attack vectors seen in the report.

Combining the NIST cybersecurity framework and the CIS Controls

As the CIS controls align to the NIST cybersecurity framework, we recommend these be used together to gain control of your cybersecurity maturity in a methodical, organised way.

NZ Incident Response Bulletin

Standard Edition – June 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: