NZ Incident Response Bulletin

Standard Edition – October 2020

In this issue:

News	Our Views	Upcoming Events
New Zealand	Hacktivists	2020 New Zealand Cyber Security Summit
World	Establishing Roles and Responsibilities	Christchurch Hacker Conference 2020
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

Police disclosing Covid-19 patient info through vetting process was 'inappropriate' - report

Police use and disclosure of Covid-19 patient information was "inappropriate", says Privacy Commissioner John Edwards. The latest inquiry into the Ministry of Health's disclosure of Covid-19 patient information to emergency services was released today.

Edwards also said Government agencies should review the way they handle and share highly sensitive Covid-19 patient health information. "Police should never have disclosed patients' Covid-19 statuses to prospective employers as part of their vetting process." Police had access to alerts related to Covid-19 to help carry out pandemic management and general policing duties.

New Zealand businesses unaware of online security laws - CERT NZ

Many companies rushing to set up e-commerce and online trading have failed to comply with rules protecting customers' data, according to a new survey.

The cyber security advisor - CERT NZ - found that 39 percent of businesses with an online store have never heard of the Payment Card Industry Data Security Standard (PCI DSS).

This is a set of international standards businesses should follow to protect customers information through the use of firewalls, proper password protections, and the encryption of customer's data.

The level of ignorance was even higher for firms with a website or operating a website for a small business.

Less than two-thirds of businesses with online stores had heard of the standards, with only 17 percent reporting "a reasonably good understanding of PCI DSS compliance".

NZ Incident Response Bulletin

Standard Edition – October 2020

World

Prosecutors open homicide case after hacker attack on German hospital

German prosecutors opened a homicide investigation on Friday into the case of a patient who died after a hospital in the western city of Duesseldorf was unable to admit her because its systems had been knocked out by a cyber-attack. The female patient, suffering from a life-threatening illness, had to be turned away on the night of Sept. 11 by the city's University Clinic and died after the ambulance carrying her was diverted to Wuppertal, 30 km (20 miles) away.

Prosecutor Christoph Hebbecker, head of the cybercrime unit in Cologne, said he had opened an investigation into negligent homicide against unknown persons. If the investigation leads to a prosecution, it would be the first confirmed case in which a person has died as the direct consequence of a cyber-attack.

Microsoft report shows increasing sophistication of cyber threats

Microsoft is releasing a new annual report, called the Digital Defense Report, covering cybersecurity trends from the past year. This report makes it clear that threat actors have rapidly increased in sophistication over the past year, using techniques that make them harder to spot and that threaten even the savviest targets. For example, nation-state actors are engaging in new reconnaissance techniques that increase their chances of compromising high-value targets; criminal groups targeting businesses have moved their infrastructure to the cloud to hide amongst legitimate services and attackers have developed new ways to scour the internet for systems vulnerable to ransomware.

In addition to attacks becoming more sophisticated, threat actors are showing clear preferences for certain techniques, with notable shifts towards credential harvesting and ransomware, as well as an increasing focus on Internet of Things (IoT) devices.

NAB sets up 'bug bounty' cyber program

National Australia Bank (NAB) has announced the launch of a bug bounty program through its partnership with Bugcrowd, a crowdsourced security company. Said to be the first program of its kind in Australian banking, NAB will reward vetted security researchers who uncover previously undisclosed vulnerabilities in NAB's cyber environment.

Cyber threat to disrupt start of university term

Universities and colleges are being warned by the UK's cyber-security agency that rising numbers of cyber-attacks are threatening to disrupt the start of term. The National Cyber Security Centre has issued an alert after a recent spike in attacks on educational institutions. These have been "ransomware" incidents which block access to computer systems.

Tyler Technologies says it was hacked with ransomware, election programs safe

Tyler Technologies TYL.N said the hacking attack against it, disclosed Wednesday, used ransomware which encrypts company files and demands payment to decrypt them again. In a statement to Reuters, the vendor of software to counties and municipalities said the hacker only reached internal networks. Tyler said the attack had no impact on the software it hosts for clients and the software it sells that displays election results is hosted by Amazon and so was not at risk.

Summary of last month's Cyber Alerts:

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.

17 September 2020 – Critical Vulnerability in Microsoft Windows Netlogon Remote Protocol

7 September 2020 – Malware being spread via email attachments

4 September 2020 – DoS and DDoS Attacks against Multiple Sectors

NZ Incident Response Bulletin

Standard Edition – October 2020

Our Views:

This month's theme is "Hacktivism".

What is Hacktivism?

The Merriam-Webster dictionary defines hacktivism as "computer hacking done to further the goals of political or social activism". Hacktivists are those engaging in hacktivism and historically have been decentralised groups of individuals acting together out of a sense of common purpose.

Hacktivists differ from other cybercriminal groups in that they are driven and united by an ideology, principle or cause. These can be political, religious, or regional issues.

Hacktivist groups came to the attention of the general public and the security community around ten years ago when they launched high-profile campaigns against targets such as the Church of Scientology, Visa, Mastercard, and Amazon. They also became heavily affiliated in political struggles such as the "Arab Spring" at that time. Some of the more well-known groups include Anonymous, Lulzsec, and the Syrian Electronic Army.

Methods Used

Hacktivists have traditionally used Distributed Denial of Service attacks (DDoS), website defacement and customer data theft as their primary methods of attack.

In the last two years, hacktivist activity has primarily focussed on the defence of civil rights and operations against child abuse, terrorism, and hate crimes. Whilst these causes seem worthy, the techniques used to achieve hacktivists' goals are often criminal and can cause significant harm to businesses and individuals. Business disruption as a result of large-scale DDoS attacks and data leaks can lead to substantial financial loss. Even short-term website defacement can cause reputational damage to a business.

Hacktivists are known to directly attack businesses whom they believe are engaging in morally corrupt activities, such as Visa refusing to process donations made for Julian Assange or the Ashley Madison website promoting extramarital affairs. In the case of Ashley Madison, the impacts of the 2015 data breach and release of thousands of customers confidential data are still being felt today with victims still being subject to bribery attempts and the attack costing Ashley Madison over $30 million in fines and recovery costs.

During the current Covid-19 crisis some cybercriminals eased off on targeting healthcare facilities, however hacktivist groups were very vocal about maintaining their campaigns against large pharmaceutical companies whom they believe are profiting from the pandemic. This is of concern to some as it has the potential to delay the development of a vaccine.

Whilst it is generally thought that businesses who are closely linked to a nation (such as a national bank) are more likely to be targeted by hacktivists, companies from a diverse range of industries have been attacked. Sometimes for seemingly innocuous business dealings such as heavy machinery maker Caterpillar Inc. who has suffered multiple attacks related to the sale of bulldozers to Israel. Businesses can also suffer collateral damage from hacktivism due to general disruptions (like nationwide internet service outages) or supply chain disruptions.

Learning from hacktivist attacks

Verizon's Data Breach Investigation Reports (DBIR) show that in previous years, hacktivists have been responsible for leaking more personal data records than cyber-criminals. With the NZ Privacy Act 2020 strengthening the obligations New Zealand businesses have around protecting sensitive data it is an appropriate time to review what lessons can be gleaned from previous hacktivist breaches and how companies should mitigate against this threat in 2020.

NZ Incident Response Bulletin

Standard Edition – October 2020

Remain Wary

Large scale hacktivist attacks are not random. The Ashley Madison website was targeted because it was seen as immoral or profiting “off the pain of others”. If you suspect your business may be at risk from hacktivism, it is a good idea to add this scenario to your Incident Response plan and playbooks. Ensure you also include a thorough Public Relations and communications plan. However, you do not have to be in an “obviously” controversial industry (such as oil) to be wary, as any organisation has the potential of being a target, by someone willing to try to embarrass or damage your reputation. As such, if your organisation would suffer from the release of personal customer information, you should remain vigilant.

Monitor not only the threat landscape, but the social climate

Despite hacktivism dropping from the major headlines for several years, Crowdstrike intelligence has recently seen an overall increase in hacktivism and groups, who had previously been quiet, once again beginning active operations. Anonymous claimed responsibility recently for convincing Korean pop music fans to hijack white supremacist Twitter hashtags in support of Black Lives Matter. Shortly after the assassination of Iran’s Major General Qasem Soleimani in early 2020, Digital Shadows also identified an increase in activity from pro-Iran hacktivists, the first such activity since campaigns in 2015 and 2016.

Accenture’s 2019 Cyber Threatscape Report predicts that events with global reach such as the Olympics may become a setting for hacktivist cyber threat activity. Threat actors have previously carried out hacktivism campaigns against the World Doping Agency (WDA), and the 2018 PyeongChang Winter Olympics.

Continuously Improve your Cybersecurity Maturity

Despite Ashley Madison encrypting most of their stored passwords, a subset (15 million) were able to be compromised using a brute force attack. Inconsistently applied security measures can occur as networks evolve, and it is a reminder that reviewing, upgrading and working to improve your cybersecurity posture continuously is vital. While you can never be entirely secure, constant improvement can help ensure you are continuing to meet obligations in regard to securing data as technology changes.

Ensure Robust Management of the Full Data Lifecycle – Including Deleting

In the Ashley Madison example, the hacktivists exposed a large amount of data which supposedly had been previously deleted. Ensure you have a robust method for the permanent and irretrievable deletion of all copies of data that are no longer required to be held by your business. This requires that you are aware of where all possible copies of data are held, including any mailboxes, third party cloud-based storage, or related applications.

Have Sufficient DDoS Mitigation

As many hacktivists use DDoS attacks, you should understand your DDoS mitigation service-level agreements to ensure you are protected in the event of a widespread attack. Your response plan and procedures should reflect your current protections and your team should be fully aware of how to engage and use these services if required.

Validate that Your Data is Secure

Finally, consider hiring an external company to test your security measures via Penetration Testing and Vulnerability Assessments.

NZ Incident Response Bulletin

Standard Edition – October 2020

Upcoming Events:

Date	Event	Location
24 February 2021	2020 NZ Cyber Security Summit	Te Papa, Wellington.
29 - 31 October 2020	Christchurch Hacker Conference 2020	The Arts Centre Te Matatiki Toi Ora,Christchurch

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.

Share our Bulletin: