# NZ Incident Response Bulletin

Standard Edition – September 2020

## In this issue:

| News | Our Views | Upcoming Events |
|---|---|---|
| New Zealand | State-Sponsored or Nation-State Cybercrime Actors | Aotea Security - Security Risk Management Seminars |
| World | | 2020 New Zealand Cyber Security Summit |
| *Refer to our Premium Edition for additional information on:*<br>*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

Concerns over how Māori data will be looked at as New Zealand plans to join international cybercrime treaty

The New Zealand Government is currently looking at joining the “Budapest Convention on Cybercrime”, an international treaty that aims to target cybercrime. The Budapest Convention fosters international collaboration to prevent and investigate cybercrime.

International cooperation is something University of Waikato Associate Professor Dr Te Taka Keegan believes is essential for New Zealand to control and manage cybercrime effectively. Concerns have been raised however about how Māori data will be looked at under this agreement. The treaty may mandate that participating countries store specific data for a given time frame and for given purposes, which may not recognise Māori sovereignty over Māori data.

Moving NZ into cyber space

Auckland has won the right to host the International Privacy, Security and Trust Conference in 2021. This conference will draw the tech world’s attention and some of its most prominent experts in cybersecurity to our shores.

The conference will allow New Zealand the opportunity to be seen as a tech hub. Global security expert Professor Hossein Sarrafzadeh believes that New Zealand’s most significant selling point when it comes to technology is that it’s trusted. New Zealanders are also trusting however, which can make us a soft target for attack as demonstrated by CERT NZ who recently reported a 38 per cent increase in cyber incidents from 2018. There are opportunities for New Zealand to leverage the trust other countries have in us, by creating data centres in New Zealand run by New Zealand companies.

CERT NZ provides threat intelligence for InternetNZ’s DNS Firewall

InternetNZ has revealed that it is now using CERT NZ’s localised cyber threat feeds as part of its Defenz DNS Firewall which protects users of the Internet from online security risks.

“A DNS firewall kicks in when a device tries to resolve a domain name to an IP address. If that site is on the blacklist of malicious sites, the firewall prevents your customer from connecting to it.” – InternetNZ.

Defenz DNS firewall stops threats at the DNS layer. It can also maintain a blacklist of malicious sites, prevent connection to those sites, prevent phishing attacks and prevent malware accessing the Internet from a network.

# NZ Incident Response Bulletin

Standard Edition – September 2020

## World

### CISA Releases 5G Security Strategy

The US Cybersecurity and Infrastructure Security Agency (CISA) recently released a strategy for defending 5G networks against security threats. The strategy "establishes five strategic initiatives that seek to advance the deployment of a secure and resilient 5G infrastructure." - Christopher Krebs Director, CISA.

Each of the five strategic initiatives addresses critical risks to secure 5G deployment. These risks include physical security concerns, weaknesses within the 5G supply chain, attempts to influence the design and architecture of the network, and the increased attack surface 5G creates that malicious actors may use to exploit vulnerabilities.

### IOOF hit with lawsuit alleging cybersecurity failure

RI Advice Group, a subsidiary of IOOF, has been named as the defendant in a civil litigation suit filed in the Federal Court by the Australian Securities and Investments Commission (ASIC) this month.

ASIC has alleged that RI Advice "failed to have adequate cybersecurity systems" in place for approximately 300 financial planners, thereby breaching provisions of the Corporations Act. They seek a court-imposed penalty and "compliance orders" to implement better systems. The legal action comes after RI Advice Group suffered several cybersecurity incidents from 2016 to 2018 but failed to properly review the effectiveness of cybersecurity controls across their network, leaving them exposed to an unacceptable level of risk.

### Uber ex-security boss accused of covering up hack attack

Uber's former chief security officer Joseph Sullivan has been charged in the US with obstruction of justice. He is accused of attempting to cover up a data breach in 2016 that impacted 57 million Uber drivers and passengers.

The charges state Mr Sullivan had taken "deliberate steps" to stop the Federal Trade Commission (FTC) from discovering the hack. He is accused of approving a $100,000 bitcoin payment to the hackers, and then disguising this as a "bug bounty" reward. The charges also allege that Mr Sullivan requested that the hackers sign non-disclosure agreements, falsely stating they had not stolen any Uber data.

### University CISOs say zero trust is the best defence against the existential threat of Phishing

Universities and their service providers have been a prime target of hackers over the last few years. In a recent interview, CISOs at Stanford, Ohio State and the University of Chicago Medicine all agreed that Phishing is the top cybersecurity threat to students, professors, and researchers. They also believed a security approach of zero trust is the most effective; however, not an easy concept to sell.

Each university has seen an increase in scamming and phishing emails this year that are getting more sophisticated. Each of the universities run regular phishing campaigns to educate employees and students and lift awareness levels of these schemes.

As well as moving to digital certificates for authentication, Stanford is also trying a zero trust model of security. A zero trust model was supported by all three CISO's; however, they agreed it goes against many of the existing cultural tenants of educational institutes that prioritize openness, sharing, and collaboration.

# NZ Incident Response Bulletin

Standard Edition – September 2020

## Our Views:

*This month's theme is "State-Sponsored or Nation-State Actors".*

Organisations are increasingly at risk of state-sponsored cyber-attacks. Whether the goal is espionage, theft, disruption or sabotage, there is growing evidence that attackers supported and funded by countries are targeting a wide range of enterprises.

Who are they?

State-sponsored cybercriminals usually work for or on behalf of a government to compromise organisations, other nations governments, or individuals, to steal information or cause disruption and harm. They are well-funded, can operate without fear of retribution from their home country, and usually have a high level of technical expertise. They are the group most associated with or described as Advanced Persistent Threats (APT's).

A critical difference between state-sponsored cybercrime and other actors such as insiders or organised crime gangs is their determination and persistence to succeed. This determination is often motivated by nationalism, and they will go to great lengths to cover their tracks. Unlike other cybercriminal actors, such as hacktivists, state-sponsored cybercriminals will never own their actions.

Recent research suggests that state-sponsored hackers and cybercriminal gangs are also increasingly impersonating each other to hide their tracks. State-sponsored actors from different nations have also started to work together; for example, Russia and Iran and China and North Korea are believed to collaborate in attacks. Another technique used by foreign entities is to engage cybercriminal groups to increase their capabilities and launch attacks.

What is the risk?

The traditional targets of state-sponsored cyber-attacks have been military, government and critical infrastructure organisations. Increasingly, however, businesses across a diverse spectrum such as healthcare, education, finance and entertainment are being targeted. Economic gain is a motivator, and companies with valuable intellectual property are at risk. For example, laptops stolen from a wave power company Pelamis are believed by some to be directly linked to remarkably similar products appearing in China soon after the theft. Other motivating factors are gaining political leverage and espionage, highlighted by the recent global concerns around Huawei's telecommunication technology possibly spying on other nations or having the possibility to disrupt critical infrastructure.

The trend for state-sponsored actors to target businesses also seems to be growing. Last year Microsoft warned 10,000 of their customers (84% enterprises) that they were targeted or compromised by a state-sponsored attack, and Google issued 40,000 notifications of nation-state hacking attacks. Verizon's Data Breach Investigations Report indicated that the number of data breaches caused by nation-states had risen from just 12% in 2018 to 23% in 2019.

Methods Used

The methods used by state-sponsored actors vary and include crypto-jacking, ransomware, Denial-of-Service (DDOS), and malware. Traditional methods, such as phishing attacks are also still highly effective. A recent analysis of nation-state sponsored phishing attacks by Google's threat analysis group indicates that impersonating journalists is popular and highlights the lengths nation-state actors will go to for success.

The attackers start by setting up accounts purporting to belong to a reporter and use these to spread disinformation through false stories that eventually get used by mainstream news outlets. They then use a fake journalist account to build email and social media relationships with other legitimate journalists. This groundwork can occur over several years until sufficient trust has been built so that when they drop a malicious link or attachment into correspondence, it will likely be opened. The UK National Cyber Security Centre (NCSC) issued an advisory this year, noting that "advanced persistent threat" actors (APTs) were also exploiting the COVID-19 pandemic in this way to launch campaigns.

Along with traditional methods, state-sponsored actors have the resources to undertake more technically advanced attacks. APT actors are increasingly utilising "fileless attacks" which leverage applications already on the victim's network. Once inside the organisation, data can then be exfiltrated using cloud-based storage technologies.

Additionally, more zero-day (i.e. yet to be discovered or protected against) vulnerabilities are also being used. The US and Israeli state-sponsored attack on the Iranian Natanz nuclear plant in 2010 (Stuxnet), utilised four zero-days which was unprecedented at the time. Recently, however, a single state-sponsored actor was found to be hoarding five zero-days.

A further risk posed by Nation-State cyber activity was highlighted at the 2020 RSA Security conference by a former hacker for the NSA. He demonstrated how sophisticated attacks developed by government-sponsored actors are being reused and repurposed by hackers previously limited in the skills and resources needed to create such advanced threats. Examples of repurposing exist already with several state-sponsored attack tools such as EternalBlue, Vault7, and ShadowBrokers having been released into the wild and weaponised by cybercrime gangs. The risk here lies in the fact that the attackers may not have the intelligence to use or tailor these tools appropriately, which could lead to more attacks that have unintended consequences, such as the Wannacry attack where Operational networks were impacted severely by malware never intended for them.

### Mitigation

Defending against sophisticated APT's designed by highly skilled and resourced nation-state actors must be a joint effort between the government and the private sector; however, individual businesses can implement effective mitigation strategies.

Recommended techniques include:

1. *Identifying any assets you hold that may be attractive to a nation-state:*

For commercial businesses, this may be intellectual property, research outputs, political influence, individuals with a high profile, or critical infrastructure services.

2. *Assuming you have already been compromised:*

We recommend that businesses assume that they have already been compromised and focus on the data they hold. Are you aware of where sensitive information resides in your network? Who has access to this data? What is in place to limit data exfiltration? Do you have tested response and recovery procedures? Is it encrypted?

3. *Running Employee Security Awareness Programmes:*

As many of these attacks still use traditional methods such as Phishing as a primary attack vector, educating employees on recognising social engineering attempts is vital.

4. *Investing in Advanced Endpoint Protection and Anti-Ransomware technology:*

Advanced endpoint detection allows greater visibility of your network and works to defend against a broader range of malware.

5. *Consider avoiding acquiring technology from companies based in nations that pose a threat:*

The National Institute of Standards and Technology's (NIST), Special Publication 800-53 Revision 4, includes a security control to restrict purchases from specific suppliers or countries.

6. *Isolating internal networks from the Internet:*

Where possible use demilitarised zones (DMZ) that isolate the internal network (or at least sensitive part of it) from the Internet.

7. *Ensuring patch/vulnerability management is up to date:*

Aim for a process that allows critical security updates to be applied immediately.

Although many businesses may believe that state-sponsored actors only target critical infrastructure or companies with significant intellectual property, it is apparent that the growing threat from these attacks is potentially harmful to all businesses. Organizations may suffer as a result of collateral damage from a newly developed malware strain, or by not yet recognising the value their business assets may present to another nation-state and preparing accordingly.

# NZ Incident Response Bulletin

Standard Edition – September 2020

## Upcoming Events:

| Date | Event | Location |
|---|---|---|
| 24 September 2020 | Aotea Security - Security Risk Management Seminars | Wellington |
| 14 October 2020 | 2020 NZ. Cyber Security Summit | Te Papa, Wellington. |

## 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: