NZ Incident Response Bulletin

Standard Edition – April 2020

In this issue:

News **Our Views** **Upcoming Events**

New Zealand	Cyber security tips when working from home	Free Microsoft Certification and Exams
World		Ministry of Education - Helping children and young people while they are learning at home
		For the Kids - Free Minecraft Educational Games

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

CERT NZ 2019 Report Summary

In March 2020, CERT NZ published its 2019 report which includes key figures, incident types, financial loss and vulnerabilities. Some highlights include:

- 15% of reports to CERT NZ had some form of financial loss with a total value of $16.7 million.
- Scams and fraud accounted for $14.5m of loss.

Also in its Q4 2019 report, CERT NZ reported on an increased number of SIM card swapping attacks where the attacker manipulates a mobile phone provider into porting the genuine customer's SIM card to the attacker's SIM card. The attacker then tries to access accounts or use the two-factor authentication code to work around the security control. CERT NZ recommends the following:

- Be careful where you share identity information.
- When there's a choice, don't use SMS two factor authentication, use an App or a USB device.
- Be creative with account recovery questions.
- Get notifications about suspicious activity.

Coronavirus: Spy agencies warn of cyberattack surge, risks of working from home

New Zealand's spy agencies say criminals and "hostile actors" are exploiting coronavirus concerns and could target employees working remotely.

The National Cyber Security Centre has issued new guidance on remote working, advising companies to secure remote access systems and workers to be security conscious, especially when working at home or in public places.

NZ Incident Response Bulletin

Standard Edition – April 2020

World

FBI warns of COVID-19 phishing scams promising stimulus checks, vaccines

The FBI's Internet Crime Complaint Centre (IC3) has issued a public service announcement warning citizens to watch out for email-based fraud and malware schemes that take advantage of the coronavirus pandemic.

Among the scams to look out for are emails purporting to contain helpful information from the Centres for Disease Control and Prevention (CDC) and other medical sources, and phishing emails that ask recipients to provide their personal information in order to supposedly receive an economic stimulus check.

"While talk of economic stimulus checks has been in the news cycle, government agencies are not sending unsolicited emails seeking your private information in order to send you money," states the announcement, which also says to look out for phishing schemes related to charitable contributions, financial relief, airline refunds, and fake vaccines, cures and testing kits.

Hackers Hijack Routers' DNS to Spread Malicious COVID-19 Apps

A new cyber-attack is hijacking router's DNS settings so that web browsers display alerts for a fake COVID-19 information app from the World Health Organisation that is the Oski information-stealing malware. Over recent days, people have been reporting their web browser would open on its own and display a message prompting them to download a 'COVID-19 Inform App' that was allegedly from the World Health Organisation.

After further research, it was determined that these alerts were being caused by an attack that changed the DNS servers configured on their home D-Link or Linksys routers to use DNS servers operated by the attackers. If your browser is randomly opening to a page promoting a COVID-19 information app, then you need to login to your router and make sure you configure it to automatically receive its DNS servers from your ISP.

UK Government Uses Zoom Despite MoD Security Concerns

The British government is using popular conferencing platform Zoom to conduct Cabinet meetings, despite reported Ministry of Defence (MoD) warnings about the security implications. The government appears to be heeding its own COVID-19 advice in forcing ministers to adhere to social distancing and work from home rules. However, a photo circulated by Boris Johnson showed the Prime Minister using Zoom to host a Cabinet meeting.

The same US-produced platform, which reportedly has a large China-based engineering team, was banned by MoD officials on security concerns, with staff at the department told to stop using it until further notice. A government spokesperson told Sky News that, according to guidance from the National Cyber Security Centre (NCSC) "there is no security reason for Zoom not to be used for conversations below a certain classification."

India committed to fight Cybercrime through I4C

In order to tackle cybersecurity breaches, India is closely monitoring the development of the global cyber norms. The Union government has launched the Indian Cyber Crime Coordination Centre (I4C) along with National Cyber Crime Reporting Portal. The system promises to allow access to people to report cybercrimes online. So far, the initiative has connected to over 700 police districts and more than 3,900 police stations.

NZ Incident Response Bulletin

Standard Edition – April 2020

Our Views:

This month's theme is "Cyber security tips when working from home".

Moving with little notice from a trusted office environment to working from home or a remote location has the potential to create cybersecurity risks. In a rush to comply with the unprecedented Level 4 lockdown New Zealand currently faces, many organisations and staff may not yet have had the opportunity to think about, or implement, basic cybersecurity hygiene in their home office set up.

In addition, there are widespread reports of an increase in cybersecurity risk due to opportunistic criminals seeking to profit from the current coronavirus pandemic. In particular, phishing scams that prey on scared or distracted individuals appear to be prolific.

Working from Home - Cyber Risks
While the home network can present many vulnerabilities, the top cybersecurity risks faced by users working at home usually fall into the following categories:

- Social engineering attacks
  Social engineering attackers target victims in times of uncertainty or stress (such as the current climate) and attempt to trick users into performing an action that ultimately causes harm. They may encourage you to click an email link that directs you to a phoney website or fool you into transferring funds to a fraudulent account.

- Weak passwords
  Weak passwords and poor authentication practices continue to be a leading cause of system and data breaches today. Home PC's that may have once only been used for personal browsing may now be used to access or store sensitive company information. While company policies often force strong password policies, the same may not be in place at home. Vigilance is required to keep these home systems secure.

- Out of date systems
  Not updating applications, anti-virus tools and operating systems to the latest version leaves them exposed to known vulnerabilities.

Considerations for Employers
If your business has employees working from home, we recommend you consider the following:

1. UPDATE YOUR INCIDENT RESPONSE PLAN: Along with your Business Continuity plans, you should review and update your Incident Response Plan to ensure your Incident Response Team can expertly manage any cyber event from home. Consider what your primary communication and online collaboration tools might be, update your phone trees and procedures to accommodate employees working remotely.

2. PROMOTE AWARENESS: Now is a great time to lift the knowledge and awareness of your team. Information on the cyber risks they may face when working from home is an excellent place to start. Additionally, let your team know whom to contact should they think they have been targeted by a scam or are suspicious of any online activity.

3. COMMUNICATE EXPECTATIONS: Ensure your team are aware of their responsibilities to protect sensitive data and that the use of insecure systems is not acceptable. Educate everyone on the types of information that must be protected. Consider activities such as conducting a password audit if applicable.

4. HARDEN YOUR DEFENCES: Ensure Multifactor authentication is a requirement for all remote login or cloud-based applications. Concentrate on securing your VPN, firewalls and endpoint protection by applying the latest patches and checking the configuration.

5. CONDUCT A FORMAL SECURITY ASSESSMENT: When possible, ensure your newly configured information systems are secure in line with best practices.

NZ Incident Response Bulletin

Standard Edition – April 2020

10 Cyber Security Tips for Working from Home
Below are out tips for IT professionals, and the staff who will be using IT systems while working from home. We outline ways to secure your home network and stay safe online while working-from-home.

1. BE AWARE: Use common sense and increase your knowledge of currently active scams. If an email or other communication seems suspicious, assume it could be fraudulent and proceed with caution. Key signs include the message appearing to be urgent, poorly constructed, or too good to be true. Regularly check the NCSC, CERTNZ and our Alerts for cyber threat information.

2. UPDATE YOUR SYSTEMS: Make sure your operating system and all applications are up to date with the latest version and patches installed. Turn on automatic updates wherever available. Don't forget to update firmware (router) and other equipment on your home networks such as your smart tv, or baby monitor if possible. Updating may require rebooting your PC at times – try to regularly find time for this or schedule it to occur overnight.

3. RETHINK YOUR PASSWORDS: Create secure and unique passwords for each account. Change these regularly. Try using passphrases rather than creating longer passwords that are hard to remember or start to use a password manager such as KeePass or LastPass. Password managers create, remember and autofill passwords for you.

4. ENABLE MULTIFACTOR AUTHENTICATION: Multifactor or 2-step authentication requires that you use both a password and a code to access your account. Services such as Dropbox, Twitter, and Gmail all support this. Your workplace may also require you to enable this to access Office 365 and other business systems. Multifactor authentication ensures that your account is still secure even if your password has been compromised.

5. BACKUP YOUR DATA: Ensure all critical files are backed up regularly.

6. SECURE YOUR HOME NETWORK: This includes securing your router by changing the default router/admin password and ensuring WPA2 or WPA3 encryption is enabled. Turn off WPS if your router still supports this as it is no longer secure. Make sure your WiFi password is strong.

7. USE ANTI-VIRUS SOFTWARE: Make sure you have effective anti-virus software in place, and that is up to date.

8. ENABLE FIREWALLS: Firewalls can defend your home device from external threats by creating a barrier between your PC and the Internet. Your operating system will usually have a firewall built-in, so it should be just a case of ensuring it is enabled.

9. USE A VPN: Consider using a Virtual Private Network (VPN). A VPN will encrypt all of your internet traffic, ensuring no one else can read it.

10. ONLY USE REPUTABLE APPLICATIONS AND COLLABORATION TOOLS: It is tempting to download and install new software or collaboration applications when trying to replicate the functionalities you usually have in the office, at home. Be cautious and install only trusted apps and those approved by your organisation for use. Additionally, ensure file sharing is performed securely. Be wary of remote access applications.

NZ Incident Response Bulletin

Standard Edition – April 2020

Free Advice and Resources
Many organisations are uniting to ensure businesses and individuals have the information they need to safely and securely work from home. The following links are reputable free resources that you can use and share with your team to promote safe home working practices.

- **The NZ National Cyber Security Centre - Working Remotely: Advice for Organisations and Staff**
  This resource is a simple, sensible bullet point list for both employers and employees working remotely.

- **CERT NZ - COVID-19: supporting people to work from home webpage**
  CERT's page offers links to various advice for individuals and businesses and includes a printable checklist guide for setting up remote working.

- **SANS Security Awareness Work-from-Home Deployment Kit**
  This kit contains advice for businesses and individuals now working predominately from home. It provides further links to information on several relevant topics such as securely working from home, social engineering scams and hardening the home network. It also contains a cyber-secure video and a communications template you can distribute and use to talk to employees about working from home securely.

- **NIST – User's Guide to Telework and Bring Your Own Device (BYOD) Security**
  The NIST guide covers a broader area than just at-home working and includes teleworking and BYOD advice for employers and employees.

- **CIS Controls – Telework and Small Office Network Security Guide**
  This is a slightly more technical guide focussed on the purchase and secure setup of network devices created for the small office or home office situation.

While we find ourselves forced to operate our businesses in a new, and for some, unfamiliar way; practising basic security hygiene such as the steps outlined above will assist in addressing any new cyber risks.

Follow these steps to increase your home security and ensure that you remain extra vigilant in your daily online interactions.

NZ Incident Response Bulletin

Standard Edition – April 2020

Upcoming Events:

Date	Event	Location
Lockdown	Free Microsoft Certification and Exams	Home
Lockdown	Ministry of Education - Helping children and young people while they are learning at home	Home
Lockdown	For the Kids - Free Minecraft Educational Games	Home

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

Share our Bulletin: