Incident Response
FORENSIC & CYBER

NZ Incident Response Bulletin

Standard Edition - May 2019

In this issue:

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

Alfred Keating trial: CCTV shows man planting hidden Washington toilet embassy camera

During April in the Auckland District Court, senior police digital forensic analyst Kerry Baker gave evidence in the trial of a high-ranking military officer relating to charges of planting a hidden camera at the New Zealand embassy in Washington.

Mr Baker examined the camera and said 736 files were deleted from the camera's memory card. A further 21 video files were still on the micro SD card, all dated the same day the camera was discovered.

Most of the still images recovered were associated with the video files, the court heard. Baker also said software from 'BrickHouse Security' was installed on the officer's computer, but later uninstalled at 6.47pm on the day the device was found.

The internet history on the officer's computer showed Google searches for "Brickhouse camscura modes" and "Brickhouse camscura switch positions". The file cleaning software CCleaner was also searched and seemingly installed on the officer's computer, the court heard.

For readers wishing to receive additional Forensic and Cyber Security information, the Premium Edition of the NZ Incident Response Bulletin is now available to clients who are subscribed to our Incident Response Retainer. The Premium Edition contains recent publications on Threat Alerts, Security Frameworks, Information Security Surveys, Forensic News and Research. Please contact us at support@incidentresponse.co.nz for further information or to request a one-off complimentary copy.

NZ Incident Response Bulletin

Standard Edition - May 2019

World

Cyber expert credited with stopping 'WannaCry' attack admits malware charges

According to Reuters, a British cyber security researcher who was credited with neutralising the "WannaCry" ransomware attack has pleaded guilty to U.S. charges of writing malware.

In May 2017, Marcus Hutchins helped halt the attack which infected hundreds of thousands of computers and caused widespread disruption across more than 150 countries.

He was arrested later that year in Las Vegas on charges relating to malicious code which could steal banking credentials. U.S. prosecutors claimed that he and a co-defendant advertised, distributed and profited from a malware code known as "Kronos" between July 2014 and 2015. Hutchins pleaded guilty to two charges.

Intelligence agencies seek fast cyber threat dissemination

The annual CyberUK conference was recently hosted by the U.K.'s National Cyber Security Centre, a division of the Government Communications Headquarters (GCHQ). For the first time, representatives from all the "Five Eyes" (Australia, Canada, New Zealand, the U.K. and U.S.) appeared on stage together.

GCHQ Director Jeremy Fleming said his agency continues to put more essential threat intelligence into the hands of U.K. businesses and government agencies. *"Specifically, in the last year we have made it simple for our analysts to share time-critical, secret information in a matter of seconds."*

Fleming also committed to more rapidly disseminating more data. *"In the coming year, we will continue to scale this capability so - whether it's indicators of a nation-state cyber actor, details of malware used by cybercriminals or credit cards being sold on the dark web - we will declassify this information and get it back to those who can act on it,"* he said.

Intelligence officials said getting the right information into the right hands as quickly as possible is mandatory for battling online attacks.

Rob Joyce, senior adviser for cybersecurity strategy to the director of the U.S. National Security Agency (NSA), said less classification - or declassifying information altogether - can make information more useful. *"Getting it ... unclassified at actionable levels and down to actionable levels is really the area that's going to pay the most dividends,"* Joyce said. *"Exquisite intelligence that's not used is completely worthless."*

More than half of British firms 'report cyber-attacks in 2019'

According to recent research from the insurance company Hiscox, the proportion of UK firms reporting a cyber-attack has jumped from 40% to 55% in 2019. Most businesses admitted they were not adequately prepared for a data breach with around 75% of respondents ranked as "novices". Hiscox said a lot of businesses incorrectly felt that they weren't at risk.

Average losses from breaches increased 61% from £176,000 to over £280,000. British firms were reported as having low cyber security budgets compared to other countries. They were also joint-least likely to have a defined role for cyber security on their staff (e.g. Security Manager). Hiscox reports that the low UK spending could be driven by the large number of small businesses in Britain. *"They may feel like they won't be targeted, as we tend to only read about large breaches in the press. If they incorrectly feel that they won't be targeted, they may be less likely to spend on cyber security."*

Since the introduction of new European data protection rules, eight in ten UK firms reported they have made changes to their cyber security.

NZ Incident Response Bulletin

Standard Edition - May 2019

Our Views:

A selection of issues relevant to Forensic and Cyber Security matters during the last month. This month's theme is "Managing Business Email Compromise Risk".

Configure

Many New Zealand organisations are either anticipating, or have recently migrated, to a cloud-based email system. On deployment, the email system should be configured to protect against security risks. This guidance is targeted at small to medium sized organisations, who are on a Microsoft business plan. Further references will be published in future for other email vendors such as Google. Microsoft recommends that you complete the tasks listed below that apply to your service plan.

- Set up multi-factor authentication
- Train your users
- Use dedicated admin accounts
- Raise the level of protection against malware in mail
- Protect against ransomware
- Stop auto-forwarding for email
- Use Office Message Encryption
- Protect your email from phishing attacks
- Protect against malicious attachments and files with ATP Safe Attachments

Review

Once you have completed configuring the security in your email environment, review how secure you are by checking your Office 365 Secure Score. This tool assigns a score based on your regular activities and security settings. While you may not necessarily obtain the maximum score, Secure Score continually helps you to keep abreast of the changing threat landscape by protecting your environment. See "Introducing the Office 365 Secure Score".

Another important area to review is Audit Log settings. If you suffer a business email compromise, audit logs are a critical source of evidence during a forensic examination. For Microsoft environments, mailbox audit logging must be turned on for each user before activity will be recorded, see Enable mailbox auditing.

Respond

If you suspect that an email account has been compromised, act quickly as a live cyber-attack may be underway. Common attack examples include email accounts being used to send Phishing attacks or SPAM. "Man in the Middle" is another common type of email attack, where a fraudster attempts to divert a payment into their own account.

Microsoft recommends the following response procedure.

- Step 1 Reset the user's password
- Step 2 Remove suspicious email forwarding addresses
- Step 3 Disable any suspicious inbox rules
- Step 4 Unblock the user from sending mail
- Step 5 Optional: Block the user account from signing-in
- Step 6 Optional: Remove the suspected compromised account from all administrative role groups

A forensic examination will heavily rely on mailbox audit data to determine the extent of any compromise. This data records which emails were accessed by the attacker, which enables you to inform affected parties that their information may have been breached.

NZ Incident Response Bulletin

Standard Edition - May 2019

Upcoming Events:

Date	Event	Location
3-5 July 2019	Australasian Conference on Information Security and Privacy (ACISP)	Christchurch
19-20 August 2019	Gartner Security & Risk Management Summit 2019	Sydney, Australia
11-13 September 2019	ISACA 2019 Oceania CACS Conference	Auckland
16 October 2019	2019 NZ Cyber Security Summit	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
+64 9 363 7910
+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: