NZ Incident Response Bulletin

Standard Edition – November 2020

In this issue:

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

New Zealand		AWS: re:Invent 2020
World		2021 New Zealand Cyber Security Summit
		AppSec New Zealand Conference 2021
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

Banks need stronger cyber security - RBNZ

The Reserve Bank is taking steps to ensure banks and other regulated financial services improve their cyber security. Reserve Bank deputy governor Geoff Bascand - responsible for financial stability - said improving cyber resilience had become a key priority for regulators around the world. The central bank's draft guidance on the topic would apply to all the entities it regulated and draws heavily from international and national cybersecurity standards and guidelines.

Complacency makes Kiwis more vulnerable to cyber attacks

The country needs to be serious about cyber protection as the volume and sophistication of financially-motivated cyber attacks has increased over the past six months, according to CERT NZ. The government agency helping organisations and individuals affected by cyber attacks said people need to become much more aware of the risks and take steps to protect their data and personal information.

Recent research by CERT found 87 percent of those surveyed thought safety and security of their personal information online was something important to them, however, 40 percent thought the precautions to protect online personal information were inconvenient.

Fives Eyes alliance calls for access to encrypted data

New Zealand and its Five Eyes security partners have made another plea for social media companies like Facebook to allow governments to access their encrypted data. Justice Minister Andrew Little issued the statement alongside Five Eyes partners Britain, the United States, Canada and Australia, as well as India and Japan. They say they support strong encryption that protects privacy, trade secrets and cyber security, but this technology also poses major risks to public safety.

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.

16 October 2020 – Microsoft Releases Security Updates to Address Remote Code Execution Vulnerabilities

NZ Incident Response Bulletin

Standard Edition – November 2020

World

[Patients in Finland blackmailed after therapy records were stolen by hackers]

The confidential records of thousands of psychotherapy patients in Finland have been hacked and some are now facing the threat of blackmail.

Attackers were able to steal records related to therapy sessions, as well as patients' personal information including social security numbers and addresses, according to Vastaamo, the country's largest private psychotherapy centre. The stolen records do not spell out specific discussions with patients, but they do include care plans and narrower professional entries.

Authorities are working to track down patients who received emails threatening to disclose personal information unless the recipient pays the blackmailer. Some of the records have already been leaked online.

[Cyberattack strikes media-monitoring company used by Australian government]

A media-monitoring and analytics firm used by the federal government has been hit by a cyberattack, prompting the involvement of the nation's leading cybersecurity agency.

Isentia, which boasts it has "most government departments and large corporations" as clients in Australia, told the Australian Stock Exchange on Tuesday it is "urgently investigating a cybersecurity incident" that was "disrupting services" involving its media portal – a service customers use to see media reporting on them, or issues of interest to them, and find journalists.

The company said it had engaged external cybersecurity specialists and informed the Australian Cyber Security Centre about the attack.

[Officials Warn of Cyberattacks on Hospitals as Virus Cases Spike]

Hundreds of American hospitals are being targeted in cyber attacks by the same Russian hackers who American officials and researchers fear could sow mayhem around next week's election.

The attacks on American hospitals, clinics and medical complexes are intended to take those facilities offline and hold their data hostage in exchange for multimillion-dollar ransom payments, just as coronavirus cases spike across the United States.

Some hospitals in New York State and on the West Coast reported cyberattacks in recent days, though it was not clear whether they were part of the attacks, and hospital officials emphasized that critical patient care was not affected.

[New action to combat ransomware ahead of U.S. elections]

"Today we took action to disrupt a botnet called Trickbot, one of the world's most infamous botnets and prolific distributors of ransomware. As the United States government and independent experts have warned, ransomware is one of the largest threats to the upcoming elections. Adversaries can use ransomware to infect a computer system used to maintain voter rolls or report on election-night results, seizing those systems at a prescribed hour optimized to sow chaos and distrust.

We disrupted Trickbot through a court order we obtained as well as technical action we executed in partnership with telecommunications providers around the world. We have now cut off key infrastructure so those operating Trickbot will no longer be able to initiate new infections or activate ransomware already dropped into computer systems." - Tom Burt - Corporate Vice President, Customer Security & Trust

NZ Incident Response Bulletin

Standard Edition – November 2020

Our Views:

This month's theme is "Organised Crime".

In the cybercrime landscape, Organised Crime Groups arguably cause the most harm to organisations by perpetrating crimes such as ransomware attacks, business email compromise, online fraud and data theft. They are the cybercrime actors with the capability and expertise to target big businesses, banks, and law firms.

Organised crime groups are motivated by profit. Online gambling is believed to have been the catalyst for organised crime groups developing an interest in cybercrime, which subsequently proved to be very profitable. They follow the "Willie Sutton Rule" by targeting "…where the money is" which in today's landscape means focusing on online business activity. Researchers recently estimated that organised crime groups and networks globally cause around $445-600 billion US dollars of harm each year. Verizon's 2020 Data Breach Investigation Report also indicated organised criminal groups were responsible for 55% of all data breaches in the last year.

Organised cybercrime groups form after connecting online and often consist of a core group of skilled actors who then develop an ancillary network of people to perform additional roles. They look to niche markets for specific expertise; for example, Dubai purportedly offers the best talent for laundering money. Their structure often closely resembles a corporate business consisting of partner networks, resellers, associates, and vendors. Sophisticated groups may even have dedicated call centres to handle ransomware victims' requests. Roles are varied and include:

- Team Leaders to coordinate and communicate with the broader team
- Coders who have the expertise to develop hacking tools and vulnerabilities
- Network Administrators to manage Botnets and DDOS attack packets
- Intrusion Specialists to carry out an attack
- Data Analysts to clean and format stolen data for resale
- Money Specialists and Mules to launder the attack proceeds

Methods Used

Organised crime groups have taken traditional crime online. Illegal gambling groups, drug cartels, and prostitution and trafficking rings all sell their services online and launder their profits digitally. However, in addition to these traditional pursuits, they have also branched out into technical cybercrime primarily using malware such as ransomware, business email compromises including phishing and invoice fraud, and social engineering attacks to extort organisations for profit.

Ransomware serves multiple purposes for organised crime groups. Firstly, it poses a significant threat to organisations both directly and indirectly, such as when third party service providers and supply chains are impacted. Increasingly it is also being used as a smokescreen for stealing Personally Identifiable Information (PII) and confidential data which the organised crime groups then threaten to auction off unless payment is made. 2020 has seen a change in tactic away from scatter-gun campaigns to performing targeted ransomware attacks as well as adding new attack layers such as crypto mining.

In addition to conducting cybercrime attacks themselves, organised crime groups will also provide services to facilitate cybercrime (crime as a service) such as providing data and identity documents, made to order malware, botnet services and training on how to use vulnerabilities and exploits. Products sold by these groups on the deep web include: Zero-day exploits for between US$30,000 and $250,000, and malware exploit kits for around US$200-$600 per exploit.

One way organised crime groups benefit from ransomware attacks, while limiting their risk or need for a specialised resource, is to only conduct the network intrusion themselves (using multiple attack vectors and malware to gain entry). They then sell this access to different actors to perform privilege escalation, lateral movement, and ransomware deployment. Emotet malware is currently omnipresent and is setting the benchmark for modern malware with over 200,000 unique versions seen in the wild. Emotet deployed by organised crime groups can provide Access-as-a-Service (AaaS) functionality to other cybercriminals who then monetise the opportunity by deploying a second attack.

NZ Incident Response Bulletin

Standard Edition – November 2020

Organised crime groups rapidly change their tactics and techniques to evade security controls and recent developments in the sophistication of malware is an example of this in action. The Europol Internet Organised Crime Threat Assessment 2020 describes how these groups have recently converted some traditional banking trojans into more advanced, highly adaptive, modular malware with a broader set of capabilities that are increasingly difficult to combat. Each known malware strand can have a code that is distributed and operated differently in different areas of the world, and the more frequent use of polymorphic and fileless malware is also limiting the effectiveness of traditional signature-based antivirus products. The malware used by organised crime groups typically includes remote access tools (RATS) and trojans to gain control over infected computers.

Business Email Compromise also continues to increase as a threat. This growth is driven by organised crime groups who have sufficient resources to investigate an organisation thoroughly and target companies using knowledge of their internal business processes and system vulnerabilities. More sophisticated measures are being used by these groups to conduct complex man-in-the-middle attacks or even using Artificial Intelligence (AI) to mimic the voice of a CEO. Social engineering and phishing remain the primary methods of initial ingress into an employee's email account, highlighting the constant need for user awareness training. Often a compromise of Office 365 is also possible due to a lack of security measures such as multi factor authentication.

Fighting Back

Prevention and awareness, as well as being prepared to manage an incident, are vital to combatting attacks from organised crime groups. Steps an organisation can take are:

Intelligence Sharing:

Organisations can help the global effort to thwart organised crime groups by reporting and sharing their knowledge and experiences. Incident reporting to national bodies such as CERTNZ or the NCSC allows a better picture of organised crime groups activity to be available to authorities. Additionally, sharing information with industry partners may assist in higher levels of awareness and preparedness to face emerging threats.

Deploying Advanced Endpoint Protection:

Traditional endpoint security tools such as firewalls and signature-based antivirus solutions depend on known threat information to detect possible attacks. In contrast, advanced solutions now use machine learning and behavioural analytics to protect endpoints from contemporary threats such as fileless and zero-day exploits.

Using Multi-Factor Authentication (MFA/2FA) and Strong Password Management Systems

All accounts should use application or hardware-based multi-factor authentication.

Conducting Regular User Awareness Training

Phishing schemes and social engineering attacks are still primary entry points for attacks leading to business email compromise, invoice fraud, ransomware and data exfiltration. Regularly reminding users of the possible risks and what to be mindful of will promote vigilance.

Timely Patching

Unpatched vulnerabilities are open doors for organised crime groups. Applying all security patches in a timely fashion will discourage any attackers looking for the low hanging fruit.

Developing Incident Response Capabilities

Develop a tested Incident Response Plan that contains specific playbooks for typical threats to your industry, such as Ransomware and Business Email Compromise. This will help ensure that your organisation has the resources, knowledge, and tools to quickly respond, contain, mitigate and recover from a cyber-attack.

NZ Incident Response Bulletin

Standard Edition – November 2020

Upcoming Events:

Date	Event	Location
November December 2020	AWS: re:Invent 2020	Virtual
10 - 13 February 2021	AppSec New Zealand Conference 2021	Owen G. Glenn Building, University of Auckland
24 February 2021	2021 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

Share our Bulletin: