NZ Incident Response Bulletin

Standard Edition – April 2021

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. Each Bulletin also includes a section of our own content, based on a trending theme. We'll give you a brief summary of each article, and a link to more information. Why do we publish this bulletin? Because we want to keep you up to date with the latest Forensic and Cyber Security news, so that you aren't caught by surprise – and you'll know about risks and changes before they become problems.

Refer to our Premium Edition for additional information on Threat Alerts, Security Frameworks, Information Security Surveys, Forensic News and Research.

Upcoming Events:

Securing NZ's Borders, Facilities & Public Spaces	Fireside chat with Rob Pope (CERT NZ)	

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 - Quarter Four Report 2020

This quarter, CERT NZ received 2,097 incident reports about individuals and businesses from all over New Zealand. This report shares examples of the incidents and advice on how to best protect against them. Highlights include:

- 2,097 incidents were reported in Q4, down 20% from Q3.
- 41% of all reports were about phishing and credential harvesting.
- $2.8 million in direct financial loss was reported in Q3, with 14% of incidents reporting associated financial loss.
- 30% of all reports were about malware, making it the second highest incident category.

Two years, 120 different profiles: Relentless online attacks from cyber stalker teen worst Judge has seen

Two years of incessant and vicious online harassment by a Milton teenager was the worst such case a judge had seen, a court has heard. The stalker used more than 120 online profiles to target their victim. The case was heard in the Dunedin District Court. Every time the victim blocked an account from which she received abuse, another one would pop up and the vitriol would continue. "On and on and on," Judge Kevin Phillips said. "Since the Harmful Digital Communications Act 2015 came into place, I've dealt with a number of people who have offended against those provisions, but the case against you is the worst in my recall of any of those cases." The offender pleaded guilty to two charges under the Act — relating to conduct on Instagram, Facebook, Snapchat, TikTok and Trade Me — and was on bail awaiting sentencing when she struck again.

New Zealand spy agency NZSIS intercepted multiple potential threats to 2020 general election

As New Zealanders prepared to vote last year for who they thought should form the next Government, potential threats to the integrity of October's general election were being intercepted. The Government Communications Security Bureau (GCSB) said, in a letter released to Newshub, that the National Cyber Security Centre engaged directly with the Electoral Commission to provide cyber security advice and support to reinforce their cyber security resilience.

"This included investigation of potentially anomalous activity identified through operation of our cyber security capabilities and information provided by Electoral Commission Security staff," the GCSB said. "We are unable to provide further details of this work as to do so might disclose aspects of our capabilities which could be of benefit to malicious actors (section 6(a) of the OIA applies: the release of the information would be likely to prejudice the security or defence of New Zealand)."

NZ Incident Response Bulletin

Standard Edition – April 2021

World

At Least 30,000 U.S. Organizations Newly Hacked Via Holes in Microsoft's Email Software

At least 30,000 organizations across the United States — including a significant number of small businesses, towns, cities and local governments — have over the past few days been hacked by an unusually aggressive Chinese cyber espionage unit that's focused on stealing email from victim organizations, multiple sources tell KrebsOnSecurity. The espionage group is exploiting four newly discovered flaws in Microsoft Exchange Server email software and has seeded hundreds of thousands of victim organizations worldwide with tools that give the attackers total remote control over affected systems.

FBI Releases the Internet Crime Complaint Center 2020 Internet Crime Report, Including COVID-19 Scam Statistics

The FBI's Internet Crime Complaint Center has released its annual report. The 2020 Internet Crime Report includes information from 791,790 complaints of suspected internet crime—an increase of more than 300,000 complaints from 2019—and reported losses exceeding $4.2 billion. State-specific statistics have also been released and can be found within the 2020 Internet Crime Report and in the accompanying 2020 State Reports.

The top three crimes reported by victims in 2020 were phishing scams, non-payment/non-delivery scams, and extortion. Victims lost the most money to business email compromise scams, romance and confidence schemes, and investment fraud. Notably, 2020 saw the emergence of scams exploiting the COVID-19 pandemic. The IC3 received over 28,500 complaints related to COVID-19, with fraudsters targeting both businesses and individuals.

Australia cyber attacks hit television channel and parliament

A cyber-attack disrupted Channel Nine's live broadcasts from Sydney, the TV company has confirmed, at the same time as an attack led to Parliament House's email system being taken offline. As a result of the attack, the channel's Sunday morning news programme, Weekend Today, was not aired, nor was its 5pm news show, although future programming is expected to transmit as normal.

Although the nature of the attack has not yet been confirmed, Channel Nine said it was investigating whether it was a matter of "criminal sabotage or the work of a foreign nation".

Cyber security complacency puts UK at risk, says NCSC head

The UK has made good progress on overall cyber security, but a sense of complacency risks upsetting the apple cart and too many people are still not taking cyber security issues as seriously as they should, according to Lindy Cameron, recently appointed CEO of the UK's National Cyber Security Centre (NCSC). "The pace of change is no excuse – in boardrooms, digital literacy is as non-negotiable as financial or legal literacy. Our CEOs should be as close to their CISO as their finance director and general counsel."

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.

8 March 2021 – CISA – Remediating Microsoft Exchange Vulnerabilities

3 March 2021 – CERT NZ – Urgent Microsoft Exchange security update released

NZ Incident Response Bulletin

Standard Edition – April 2021

Our Views:

This month's theme is "Electronic Incident Control Rooms".

Successfully managing a cyber incident is crucial to minimising the impact of any compromise. When asking what 'Good' looks like, it is reducing recovery costs, avoiding potential liabilities, and recovering to business as usual quickly. In our day-to-day jobs as incident responders and forensic examiners, we cannot stress the importance of having a structured plan to achieve this and manage any crisis effectively. However, we have also witnessed first-hand, both during active events and through our cyber simulations, the collaboration challenges involved when managing a cyber incident. Challenges that we have seen repeatedly rearing their heads for organisations during this process include:

- **Selecting appropriate communication and collaboration tools:** *Do all Cyber Incident Response Team (CIRT) members have access to the chosen tools? Does everyone know we are using X tool? What happens if our systems are down due to a cyber-attack? What happens if we are all working from home or in multiple locations? How do we add all the relevant people to the communication group when time is of the essence?*
- **Difficulties in securely sharing critical information**: *How can we ensure everyone has access to the information they need during an incident? How can we review what has already been done? Where can we post files so that partners and third parties can view these? How can we keep track of material up to date?*
- **Challenges with keeping track of progress through the Incident Management Plan**: *Do all key stakeholders hold a printed copy of the Incident Response plan? What page are we on now? Where do I find this information?*
- **Difficulties with managing actions and decisions and providing visibility of information:** *Who is doing what right now? Was that decision made? When and why did we decide this?*
- **Lengthy update meetings and stand-ups:** *How do we spend less time keeping everyone up to date and more time responding?*
- **Plan updates and playbooks:** *When was the plan last updated? What actions do we take for this new type of attack?*
- **Reporting and post-incident review**: *Did anyone save the whiteboard notes? Who knows when the first notification came through?*

Whilst much of the magic involved with a smooth response comes down to knowledge, experience, and strong incident responder skills, we know and endorse the benefits of a pre-prepared cloud-based incident response control room.

Advantages also include:

- **The ability to quickly add new playbooks based on new threats:** *An electronic control room grants the ability to dynamically change and update information in real-time and add new playbooks when required. For example, we recently developed a Microsoft Exchange Server playbook in response to the developing threat. This playbook was invaluable in saving time in responding to these compromises.*
- **Provides a single source of truth:** *The electronic control room becomes the location for the plan, playbooks, actions, meetings, minutes, documents and any other information related to the active incident. The whole team can see immediately what actions are assigned to them, what has been completed and what is yet to be done.*
- **Allows secure collaboration:** *Secure access can be easily granted to all parties needing to collaborate in an incident regardless of where everyone is located. Various areas can also be locked down where necessary to smaller groups. Hosted out of your network, the electronic control is always available even should your systems be impacted.*
- **Post-Incident Review:** *All information captured within the control room can be archived, providing an auditable record of all actions taken throughout the incident.*

As managing a complex cyber incident can be daunting, we recommend setting up a pre-configured control room ready to go should the worst happen. With a small amount of preparation, this will aid a smooth and successful response to any cyber incident your business may face.

NZ Incident Response Bulletin

Standard Edition – April 2021

Critical Advisory:

Overview

Beginning the week of 1st March 2021, Microsoft and others in the security industry have seen an unprecedented number of cyber-attacks on on-premises Microsoft Exchange servers. In the attacks observed, the threat actor used multiple, previously unknown vulnerabilities to access email data allowing the installation of additional malware to facilitate long-term access to victims' environments. Presently, the vulnerabilities are limited to Microsoft Exchange email servers that are 'on-premise', Exchange Online (MS365) is not known to be vulnerable to these attacks.

While researchers initially suggested that this cyber-attack began as a nation-state attack, over recent days there is increasing evidence to suggest that the same vulnerabilities are being exploited by multiple cybercrime groups, including the threat of ransomware attacks along with the potential of other malicious activities. Microsoft consider this to be a "broad attack and the severity of these exploits means protecting your systems is critical". Such protection includes the use of traditional tools to update software, but with a heightened approach. Accordingly, Microsoft are providing specific updates for older and out-of-support software so you can update your systems more easily and quickly protect your business.

Read more and stay up to date by visiting our Cyber Security and Incident Response Advisory here.

On 25 March, the Microsoft 365 Defender Threat Intelligence Team published detailed guidance on their threat intelligence to help detect and evict threat actors from affected environments. Microsoft note that many of the compromised systems have not yet received a secondary action, such as human-operated ransomware attacks or data exfiltration, indicating attackers could be establishing and keeping their access for potential later actions. These actions might involve performing follow-on attacks via persistence on Exchange servers they have already compromised, or using credentials and data stolen during these attacks to compromise networks through other entry vectors. Specific examples of post-exploitation activity include DoejoCrypt ransomware, Lemon Duck botnet and Pydomer ransomware.

Credential theft, reconnaissance and persistence (For Technical Staff)

- Exchange servers potentially contain highly privileged credentials making them an attractive target
- Built in Windows functionality can be used to harvest credentials such as using the comsvcs.dll to dump the LSASS process
- Built-in Exchange commandlets and dsquery can be used to exfiltrate information about network configurations, users and email assets
- Attackers are using 'malwareless' persistence mechanisms such as enabling RDP, installing shadow IT tools and creating local administrator accounts

Defending against exploits and post-exploitation activity (For Technical Staff)

- Investigate internet facing Exchange servers for any evidence of malicious activity regardless of whether or not they have been patched
- Look for the presence of web shells by following Microsoft's guidance and running the Microsoft Safety Scanner tool to detect and remove malicious applications
- Review Active Directory and local user/group configurations for new account creation and privilege escalation activities. New user creations are represented by Windows Event ID 4720.
- Reset domain user passwords including service accounts and Kerberos
- Reset local administrator passwords and consider using a tool such as LAPS to manage these
- Review RDP, firewall, WMI subscriptions, and Windows Remote Management (WinRM) configuration for changes that may allow an attacker to maintain persistence
- Review the Windows Event log for Event ID 1102 which indicates that logs have been cleared
- Review services, scheduled tasks and startup items for suspicious entries that may serve as persistence mechanisms
- Look for the installation of Shadow IT tools that may be used for persistence such as non-Microsoft remote access tools, e.g. Teamviewer, Anydesk, VNC clients etc
- Review mailbox forwarding, inbox rules and Exchange Transport rules for any suspicious entries

NZ Incident Response Bulletin

Standard Edition – April 2021

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

Further Resources:

Alerts	Data Breach Response	Forensic Technology
Cyber Incident Simulations	Social Media Investigations	Guide for NZ Law Firms

Share our Bulletin: