NZ Incident Response Bulletin

Standard Edition – December 2020

In this issue:

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

New Zealand	Ransomware and Data Leak Sites	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

Healthcare sector suffering surge in cyber attacks

Hospitals and other healthcare organisations have recently been under heavy attack by cyber criminals, according to information from both Microsoft and US Federal agencies. The attacks put lives at risk during what is already a challenging time due to the current COVID-19 pandemic.

Worryingly, pharmaceutical companies working on vaccines and treatments for COVID-19 have been included in the attacks. Gorilla Technology CEO and Futurist Paul Spain indicates that, whilst every organisation is at risk from random cyber-attacks, it is likely that those leading the way with developing vaccines for COVID-19 were directly targeted by state sponsored attackers.

Cert NZ tracks big rise in cyber attacks during pandemic

The Government's Computer Emergency Response Team (Cert NZ) fielded a record 2610 reports of cyberattacks in the September quarter, which included the second lockdown for Aucklanders. It continued a trend of escalating online fraud, phishing and ransomware attacks during the pandemic.

Reported financial loss for the three months to September 30 jumped to $6.4 million from $3.8m in the year-ago quarter - but Cert NZ says a lot of offending is likely going unreported. Business email compromise has been on the increase since quarter two and has led to significant financial loss to businesses and organisations throughout July, August and September.

New Zealand's new Privacy Act 2020, came into force on 1 December 2020, creating new responsibilities for organisations in New Zealand. The new Act introduces a number of changes concerning how the privacy principles are enforced and regulated including mandatory notifications for privacy breaches where serious harm may result.

For more information, read our special publication here.
https://incidentresponse.co.nz/data-breach-response

NZ Incident Response Bulletin

Standard Edition – December 2020

World

Ragnar Locker gang uses Facebook ads to pressure ransomware victim into paying

The Ragnar Locker ransomware gang has been making regular headlines for its ransomware attacks on multiple companies in recent months, but in a new twist, the group has taken to advertising on social media to pressure one of its victims into paying.

The victim in this case is Italian drinks maker Davide Campari-Milano S.p.A., best known simply as Campari, which was targeted in a Ragnar Locker ransomware attack on 2 November 2020.

First reported by Krebs on Security, the Ragnar Locker gang has started using Facebook accounts to run ads to pressure Campari publicly into paying its demanded ransom.

Campari had said in a statement on 6 November 2020 that "at this stage, we cannot completely exclude that some personal and business data has been taken," a claim directly addressed in the Facebook ads.

Hacker posts exploits for over 49,000 vulnerable Fortinet VPNs

A hacker has posted a list of one-line exploits to steal VPN credentials from almost 50,000 Fortinet VPN devices. Present on the list of vulnerable targets are domains belonging to high street banks and government organisations from around the world.

The vulnerability can impact a large number of unpatched Fortinet devices. By exploiting this vulnerability, unauthenticated remote attackers can access system files.

The exploit posted by the hacker lets attackers access files from Fortinet VPNs to steal login credentials. These stolen credentials could then be used to compromise a network and deploy ransomware. Although the 2018 bug was publicly disclosed over a year ago, researchers have spotted around 50,000 targets that can still be targeted by attackers.

GoDaddy Employees Used in Attacks on Multiple Cryptocurrency Services

Fraudsters redirected email and web traffic destined for several cryptocurrency trading platforms over the past week. The attacks were facilitated by scams targeting employees at GoDaddy, the world's largest domain name registrar.

The incident is the latest incursion at GoDaddy that relied on tricking employees into transferring ownership and control over targeted domains to fraudsters. In March, a voice phishing scam targeting GoDaddy support employees allowed attackers to assume control over at least a half-dozen domain names, including transaction brokering site escrow.com.

In May of this year, GoDaddy disclosed that 28,000 of its customers' web hosting accounts were compromised following a security incident in October 2019 that wasn't discovered until April 2020.

This latest campaign appears to have begun on or around 13 November 2020, with an attack on cryptocurrency trading platform liquid.com.

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.

20 November 2020 - Nitro PDF users' email addresses and hashed passwords leaked.

NZ Incident Response Bulletin

Standard Edition – December 2020

Our Views:

This month's them is "Ransomware and Data Leak Sites".

In the course of our day to day work as Cyber Incident Responders we have noticed a concerning rise in Ransomware attacks which now extend to the threat of leaking compromised data. Our observations are backed by similar warnings from organisations such as the Australian Cyber Security Centre (ACSC), The United Kingdom's National Cyber Security Centre (NCSC) and The United States Department of Homeland Security (CISA), all of whom have recently issued general Ransomware advisory notices. Not only is the increase in attacks concerning, but the nature of Ransomware attacks has also evolved making them a significant threat to all organisations in New Zealand.

Ransomware typically encrypts data on devices rendering them inaccessible. A ransom is generally demanded in the form of crypto currency in order to obtain a decryption key. It is currently one of the most profitable forms of malware for the cybercriminals as they are successful in using ransomware to disrupt operations and cause reputational harm. Ransomware is not only costly to mitigate but the impact of this kind of attack has now stretched beyond financial and reputational damage to include threats on life. A German hospital recorded the first reported death as a direct result of Ransomware in September this year.

Research indicates that any business that stores electronic information is a target and the size and sensitivity of this data is largely irrelevant. This means you do not have to be storing national security secrets or traditional Personally Identifiable Information (PII) to be a target and attacked.

Ransomware Innovations and Data Leak Sites

The potential damage ransomware can inflict has recently increased. Cybercriminals are now tailoring attacks to ensure they are more successful and profitable than ever by using techniques that incentivise victims to pay.

One worrying trend is the combining of encryption with the exfiltration of confidential data. In these instances, the ransomware gang compromise the network and steal data before encrypting the systems and sending a ransom note. The cybercriminals then threaten to release the information publicly if the ransom is not paid, providing a sample to prove they have the data. This means that even if an organisation has great backups, they are still under pressure to pay the ransom or else sensitive data may be released online.

Many ransomware gangs have created dedicated websites called "data leak sites" where they publish the data stolen from organisations who do not pay the ransom. While not all gangs work this way, it is known that Maze, Ako, Avaddon, CLOP, Darkside, DoppelPaymer, Mesipinoza, neflim, netwalker, ragnarLocker, REvil and Sekhmet all operate data leak sites and publish confidential data to these portals. Coveware report that up to 50% of the ransomware incidents investigated recently involved the theft of data before encryption occurred and that this percentage is rising.

Typically to date, if a ransom is paid to decrypt locked data, the decryption key is provided. This is because ransomware gangs operate as businesses that rely on reputation. Unfortunately, when it comes to the double extortion schemes where data is stolen prior to encryption, more incidents are being reported where the cybercriminals are not keeping their promises. Instead of deleting the stolen data once the ransom is paid, some groups are asking for second payments weeks later using data that the victim thought had been deleted after the first ransom payment. Sensitive data has also been seen published on data leak sites even after a ransom was paid and falsified evidence has been sent to victims indicating it was deleted when it was not.

"Unlike negotiating for a decryption key, negotiating for the suppression of stolen data has no finite end. Once a victim receives a decryption key it cannot be taken away and does not degrade with time. With stolen data, a threat actor can return for a second payment at any point in the future" - Coveware

In light of this research, we recommend caution when considering such demands. Instead, focus on identifying and notifying any impacted parties in order to mitigate any potential harm. Under the new Privacy Act, notification in the event of potential serious harm is mandatory in New Zealand.

NZ Incident Response Bulletin

Standard Edition – December 2020

Other tactics cybercriminals use to increase their success of ransomware attacks are to:

- Publicly advertise that an organisation has been compromised (to the attention of their customers and partners) to put additional pressure on the organisation to resolve the problem and pay the ransom.
- Perform significant reconnaissance on a target to understand their vulnerabilities and potential to pay a ransom including investigating a business's net income to establish ransom amounts.
- Increase the ransom demand amount after a specific time period placing pressure on the victim to pay quickly and before receiving expert advice.
- Offer to partially decrypt some of the victim's network for a reduced percentage of the ransom. While this offer is sometimes posed under the guise of compassion it actually benefits the cybercriminal by indicating to them what parts of the business network are the most valuable to the victim which they then may on sell.
- Target critical service sectors such as hospitals who cannot afford any loss of system operations.

Mitigation and Incident Response

Like other malware, ransomware can infect a device in a variety of ways including via:

- Opening emails or files from unknown or unsafe sources.
- Clicking on malicious email links.
- Insecure remote desktop protocol sessions.
- Clicking on malicious links in social media and peer to peer networks.
- Visiting compromised or unsafe websites.

Mitigation strategies involve various steps to ensure your business can prevent malware delivery, recover data and systems, and contain any damage. Prior to an attack happening steps such as conducting user education, implementing allow listing, ensuring principle of least privilege, maintaining adequate offline backups, regularly patching systems, disabling macros and configuring endpoint detection and response are essential.

If an attack has occurred however it is vital to understand approaches for uncovering, mitigating, and remediating malicious activity. The Department of Homeland Security recently published Alert (AA20-245A) which we consider to be critical advice to assist in addressing potential incidents. This advisory combined research from five nations including New Zealand and can serve as a playbook for incident investigation. Details on general mitigation are also included in this advisory such as:

- Restricting use of FTP and Telnet services
- Restricting use of non – approved VPN services
- Shutting down unused services and systems
- Quarantining and reimaging compromised hosts
- Disabling unnecessary ports, protocols, and services
- Restricting interactive logins for service accounts
- Disabling unnecessary remote network administration tools
- Managing unsecure remote desktop services
- Resetting credentials and reviewing access control
- Patching vulnerabilities

The threat of extortion via elaborate ransomware and data exfiltration schemes is growing. If sensitive data is released publicly it can have devastating effects on organisations and individuals. Should you fall victim to a ransomware attack we suggest you consider the possibility that your data has been compromised and immediately seek help from a cyber security and incident response service.

NZ Incident Response Bulletin

Standard Edition – December 2020

Upcoming Events:

Date	Event	Location
November December 2020	AWS: re:Invent 2020	Virtual
10 - 13 February 2021	AppSec New Zealand Conference 2021	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: