NZ Incident Response Bulletin

Standard Edition – June 2020

In this issue:

Premium Edition contains 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

The Detail: Questions surround the NZ Covid Tracer app

Over 100,000 New Zealanders have downloaded the NZ Covid Tracer application so far; however, questions remain about its use and ongoing role in New Zealand. While researchers believe the app seems safe, there are inconsistencies with its functionality including QR code variances that mean the app will not read all QR codes, and the issue of accessibility and technical knowledge for its use.

The current version of the app collects two different types of data which is then stored in two separate locations. On joining, users are asked for information including full name, address and phone number. This data is collected by the Ministry of Health and stored on secure Australian servers. The second type of data the app collects is data associated with any QR code you scan when entering a store. This data is stored locally on the phone and not shared without user action enabling it to be.

The primary outstanding question, however, is what happens once the Covid-19 situation is deemed over?

The companies and governments involved with developing tracing apps have said that the data they are collecting can only be used for the purposes of managing the COVID-19 pandemic and that the systems will be shut down once the crisis is over. This indicates that constant remote surveillance should not be normalised through the introduction of tracing apps for Covid-19.

FMA's Cybersecurity Concerns

The Financial Markets Authority (FMA) report that several cybersecurity incidents have recently come to its attention and is reminding financial services firms to review their IT security.

"In particular, firms need to proactively monitor IT systems and electronic mailboxes to identify any unusual activity and ensure they have not been compromised. We'd also note the importance of maintaining internal risk controls to protect customer information and money." – FMA Industry regulator

The FMA recommends that businesses use their cyber resilience guidance document and the New Zealand National Cyber Security Centres cybersecurity guide for identifying areas of improvement.

NZ Incident Response Bulletin

Standard Edition – June 2020

World

Data Stolen from The Toll Group Published on Dark Web

In an update on the ransomware attack they suffered in April this year; Toll Group has revealed that data stolen during this compromise has been subsequently published to the dark web. Toll did not pay the ransom and chose to shut down its systems to contain the malware infection.

The April ransomware attack is believed to be the result of Nefilim ransomware. Toll was also a victim of the Mailto ransomware variant in January this year which led to them reverting to manual processes for operations. The Australian Cyber Security Centre has provided technical experts to identify the nature of the compromises and give mitigation advice.

Toll is in the process of assessing the nature of the stolen data that has been published online but believes it could take several weeks to determine any further attack details. Impacted customers are currently being notified.

British airline EasyJet breached, data of 9 million customers compromised

Easy-Jet UK has disclosed a breach involving the information of 9 million customers. The compromised data includes email addresses, travel details and payment card information.

Easy-jet notified the appropriate authorities and engaged forensic experts to investigate the incident immediately on becoming aware of the breach; however, they have not released any further details on the investigation outcome. The lack of additional information has led to speculation that the compromise may have been avoided. Some also believe that hackers will seek to take advantage of customer uncertainty and instigate further campaigns to exploit them.

It is thought that Easy-Jet will face financial penalties under the GDPR, however the fine may either be nominal or punitive dependant on any negligence involved.

Scammers Use Contact Tracing as Bait to Target Users

Cybercriminals are using Covid-19 "Contact Tracing" to fool victims by posing as contact tracers to gather details for identity theft and fraud. In this scam, phoney SMS messages are sent to trick a recipient into visiting a fraudulent website and sharing their personal information. Often the text message will imply the victim has already come into contact with someone who has tested positive for COVID-19.

The US federal government has issued guidelines for protection against these COVID-9 contact tracing scams including highlighting that:

- Official health department messages will never include links and
- Real contact tracers will never ask for any financial identity information from you – such as a tax number.

ARCHER Supercomputer Offline

The main supercomputing service for academic research in the UK was offline for days after a recent incident. The ARCHER computing service is primarily used for data modelling events such as the recent COVID-19 outbreak and climate change.

It is thought that hackers have specifically targeted scientific research resources as several computers involved in these kinds of activities have been compromised across Europe in recent weeks. The UK National Cyber Security Centre has provided support in the recovery efforts; however, as yet the attack has not been attributed to any cybercriminal or group.

NZ Incident Response Bulletin

Standard Edition – June 2020

Our Views:

This month's theme is "COVID-19's impact on cybercrime and cybercriminals".

The COVID-19 pandemic has impacted businesses worldwide. Some companies have suffered sizeable financial loss due to an inability to operate under strict quarantine conditions. In contrast, some businesses have adapted and are thriving in the new environment. Many are searching for ways to maintain a profit despite the challenges that social distancing and reduced consumer spending brings.

Cybercrime is a business, albeit an illegal one. Successful cybercriminals operate their scams and attacks with organised processes that have been polished to maximise ill-gotten gains. It stands to reason that cybercrime and the way cybercriminals operate amid the global pandemic must also be impacted. Whether the current conditions favour an increase in cybercrime opportunities or by contrast, hinder its profitability, is a complicated question.

Challenges faced by Cybercriminals as a result of the COVID-19 pandemic

The COVID-19 pandemic and the resulting lock-downs seen internationally has interrupted supply chains globally. For example, "reshipping fraud" has not been immune to the delays and cost increases as a result of supply chain disruption.

Online retailers carefully manage their risk when shipping products to regions where credit card fraud is prolific. Our research suggests a vast underground "reshipping" market, in places such as North Africa, Russia and Eastern Europe. Criminals buy expensive products online using stolen credit card details and enlist "mules" to receive and relay the goods to embargoed areas. Mules may be willing or unwitting participants in these crimes, and it is a term used to describe anyone hired or used to enact part of the illegal process.

According to the report of one cyber intelligence company, many criminal reshipping services are struggling during COVID-19 as long FedEx or UPS shipping delays are causing their product to be rerouted to the original credit card holders address instead of to the mules.

Money Mules (people hired to help launder cybercrime proceeds) are also reportedly being hindered in their activities. Many are unable to withdraw funds due to not wanting to leave their homes and reshipping mules are unable to pick up goods directly from stores anymore due to widespread lock-downs.

Cybercriminals have also reported difficulties in executing social-engineering fraud. Bank support phone lines are overloaded. Along with legitimate customers, criminals are therefore struggling to get through to support desks to conduct account changes. It has also been predicted that the black-market price of stolen credit card data used to create physical counterfeit credit cards may fall due to physical store closures, making this endeavour no longer as profitable as what it once was.

Finally, according to Digital Shadows, the scale of the global crisis appears to have some cybercriminals rethinking their moral standpoints. Reportedly, this is making it harder for them to undertake scams without considering the resulting karmic consequences of profiting from their activities.

Opportunities granted Cybercriminals as a result of the COVID-19 pandemic

While an environment of physical distancing and business interruption presents challenges to cybercrime, there also appears to be opportunity. The quick move to remote working for large sections of the global population presents a significant new pond for criminals to conduct phishing scams and release malware.

Fear is a traditional social-engineering technique used by criminals, and COVID-19 health uncertainties present new ways to frighten potential victims into revealing more information than they might otherwise. As seen in recent news and alerts, COVID-19 tracing schemes and fraud are rife.

NZ Incident Response Bulletin

Standard Edition – June 2020

Unemployment caused by the predicted global economic recession is also an area where cybercriminals can find opportunities. For example, Intel 471 report that cybercriminals are looking forward to the glut of available and desperate possible mules that high unemployment levels will create.

Cybercriminals are also taking advantage of unemployment programs across the United States by filing unemployment claims in multiple states using information obtained via identity theft. Sadly as described by KrebsOnSecurity, much of the fraudulent PII used to obtain these benefits is from those on the front line of the pandemic such as first responders and government personnel.

Due to the current pandemic and scale of people in need, it is thought that many states have dramatically reduced the amount of information required to request an unemployment filing successfully. The result being that cybercriminals have seized the opportunity and the scale of this operation has led to warnings that false filings may cost the government hundreds of millions of dollars in losses.

Predictions for 2020 and beyond

It is clear that although cybercrime enterprises may be impacted and inconvenienced by COVID-19 restrictions, they are continuing to evolve and look for financial advantages in the crisis. While some criminal schemes may diminish due to a lack of profitability, such as credit card dumps, other types of fraud such as unemployment fraud are quickly rising to take their place.

The British government are already highlighting a surge in cyberattacks so far this year compared to previous years, and that may continue throughout 2020. Large scale unemployment may create a new pool of vulnerable people willing to accept offers of shady employment, and fear may drive ordinarily sensible individuals into taking bigger risks with their data.

In summary, the cybercriminals appear to be weathering the coronavirus storm. Ongoing vigilance against cybercrime must remain high amongst New Zealand individuals and businesses.

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.

- 20/05/2020 – Summary of Tradecraft Trends for 2019-20 (ACSC)
- 12/05/2020 – Top 10 Routinely Exploited Vulnerabilities
- 05/05/2020 – APT Groups Target Healthcare and Essential Services

NZ Incident Response Bulletin

Standard Edition – June 2020

Upcoming Events:

Date	Event	Location
Jul 16 - Jul 25, 2020	DFIR Summit & Training 2020 - Live Online	Online
14 Oct 2020	2020 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: