certnz

Quarterly Report: Highlights Q1 & Q2 2020

1 January - 30 June, 2020

New Zealand Government

Rob Pope, Director

Director's message

"The increase in reporting is a welcome sign that New Zealanders are becoming more cyber smart and more vigilant online. However, cyber attackers are also increasingly sophisticated, and the need for effective cyber security measures has never been more pressing."

COVID-19 disrupted the activities of all New Zealand businesses and organisations this year. For CERT NZ, it meant the production of the 2020 Q1 report was interrupted. That's why this publication provides a half year picture of the data and trends in 2020, rather than the usual quarterly focus.

CERT NZ received a greater number of incident reports between January and June, compared with the same period in 2019. Although some incidents were clearly the result of opportunistic cyber attackers taking advantage of the COVID-19 environment, the bulk of the reports were not specifically COVID-19 themed.

The increase in reporting is a welcome sign that New Zealanders are becoming more cyber smart and more vigilant online. However, cyber attackers are also increasingly sophisticated, and the need for effective cyber security measures has never been more pressing.

We're all vulnerable to cyber security threats and the best way to stay safe is to take preventative measures. Being cyber smart includes putting in place safeguards that can protect us against attacks. A good example of where prevention is the best approach, is with malware compromise, which is the focus of this report. Although relatively few in number, reports relating to malware are among the most serious we deal with, and can have devastating effects on individuals and online businesses.

More businesses are moving to online trading – a trend that has accelerated over lockdown. In response to this, CERT NZ teamed up with Consumer Protection to run the joint 'Protect it' campaign running both online and on television until the end of August, and then picking up again for the pre-Christmas period through November and December.

CERT NZ's campaign encourages businesses to Trade Smart Online and offers practical steps to help keep their websites secure. Consumer Protection's campaign encourages consumers to Shop Smart Online by pausing before they pay, and checking a few simple things about the website.

Collaboration with other agencies is critical to our efforts to combat cyber threats. Likewise, the businesses and everyday New Zealanders who report incidents to us are vitally important contributors to the cyber security ecosystem.

Every report received through our online reporting tool helps us build a clearer picture of New Zealand's cyber security landscape. They help guide CERT NZ to where our efforts are best directed, and take us closer to the goal of a more cyber resilient New Zealand.

Incident reports

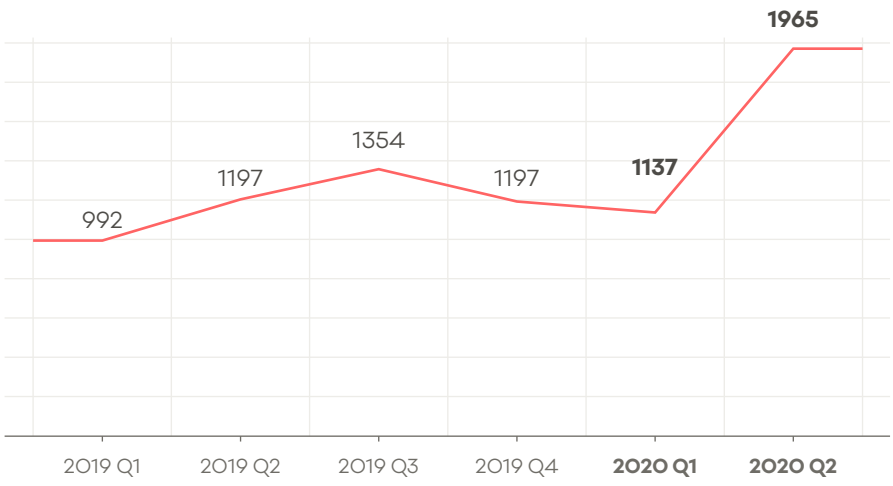
Q1 reports

1,137

Q2 reports

1,965

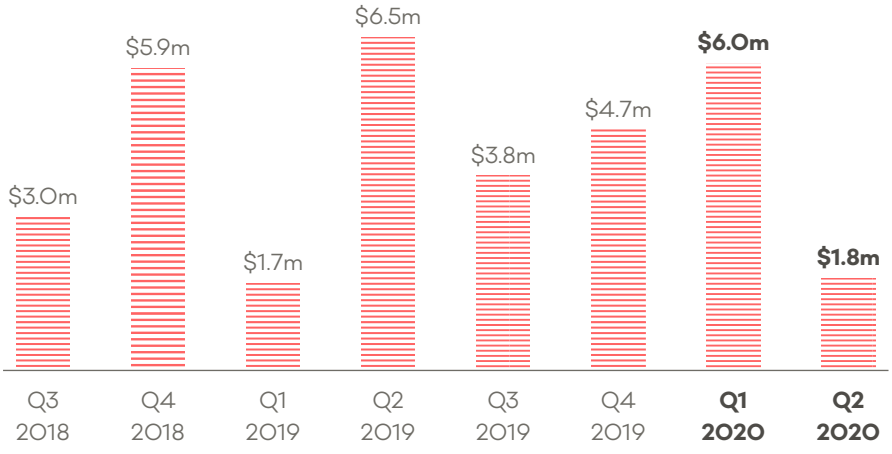
CERT NZ received a total of 3,102 incident reports in Q1 and Q2 2020



Financial loss

$7.8 million

Total financial losses were $7.8m for Q1 and Q2 collectively. Fortunately, there was significantly less financial loss reported in Q2 - just $1.8m, compared with $6m in Q1. This may be attributed to a heightened vigilance among New Zealanders during lockdown.



▲ 73% increase

in incident reports from Q1 to Q2. (72.82%)

April was busy!

820

incident reports were received by CERT NZ in April – the greatest number of reports received in any month since our launch in April 2017.

Higher than normal reporting numbers continued throughout May (539) and June (606).

If this trend continues, we could expect to receive more than 6,000 incident reports in 2020.

This would be significantly more than the previous two years, with a total of 4,470 reports received in 2019 and 3,445 received in 2018.

The overall increase continues to be driven largely by increases in reports about phishing and credential harvesting, and scams and fraud.

Increases and decreases compared to Q4 2019

Phishing & credential harvesting

▲ 15% increase

in Q1 2020

▲ 25% increase

in Q2 2020

Scams & fraud

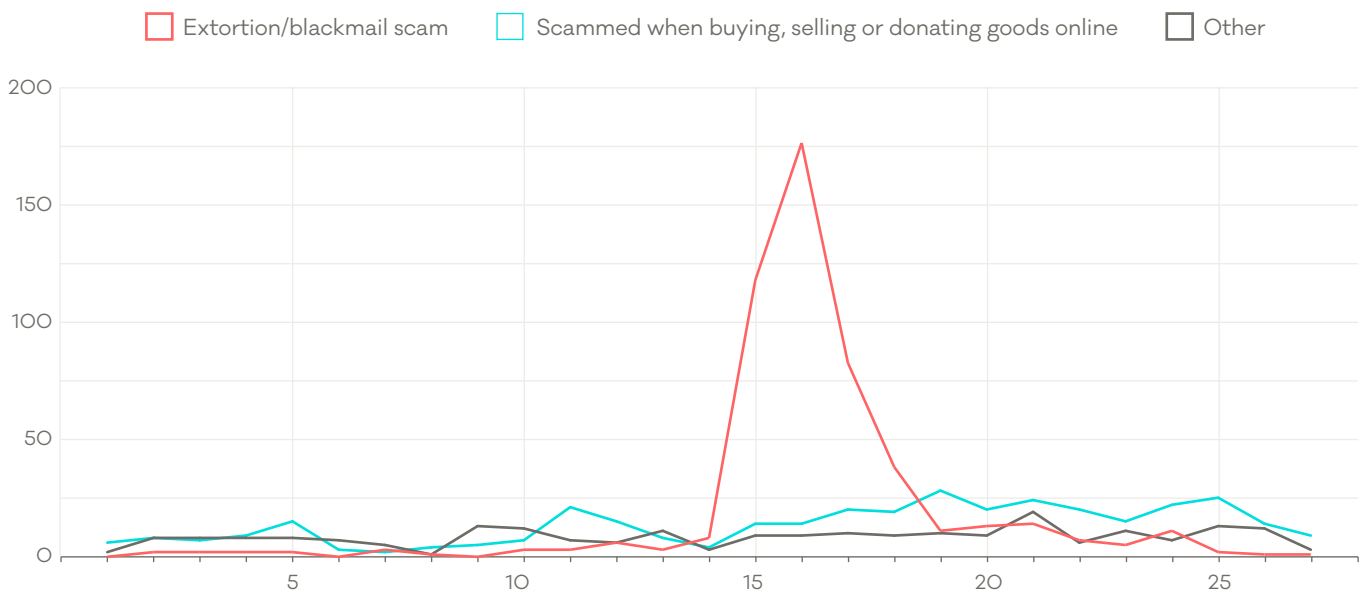
▼ 33% decrease

in Q1 2020

▲ 229% increase

in Q2 2020

Scam and fraud reports



Reports of extortion and blackmail scams increased significantly during April, rising from less than 10 to over 170 per week. The campaign passed quickly, with levels more or less returning to normal within four weeks. Fortunately, the increase in reports did not produce a corresponding increase in financial loss, suggesting New Zealanders are more alert to this type of scam. Campaigns such as CERT NZ's Cyber Smart Week, may also have contributed to this heightened awareness.

A second interesting trend observed during Q2, was the gradual and sustained increase in reports from people who were scammed when buying or selling goods online. Taking precautions to trade safely online will continue to be of increasing importance as more and more economic activity moves online as a result of the COVID-19 pandemic.

Web cam extortion

478 reports

Reports of the familiar webcam extortion email campaigns increased significantly in Q2 - with 478 reports in that quarter, up from just 34 in Q1.

The trend was also observed across the Tasman, with the Australian Cyber Security Centre (ACSC) issuing an advisory about the campaign at the same time[1].

Online trading scams

▲ 119% increase

There was also an increase in reports of scams involving buying and selling online during Q2 – from 112 in Q1 to 246 in Q2 – an increase of 119%.

For more on the New Zealand threat landscape in Q1 and Q2 2020, see the CERT NZ Quarterly Report: Data Landscape. If you have experienced a cyber security issue, report it to CERT NZ at **www.cert.govt.nz/report**.

1. https://www.cyber.gov.au/acsc/view-all-content/alerts/sextortion-email-campaign-impacting-australians

Increased activity during lockdown

CERT NZ received significantly more reports in Q2 compared with Q1, particularly during lockdown. This may have been due to an increase in cyber-criminal activity, with attackers exploiting the increased uptake of digital services, or that people were more aware of cyber threats in a time of greater dependence on digital services.

We received 26 reports directly relating to COVID-19 themed scams during Q2, accounting for just 3% of the total increase in scam & fraud incidents reported from Q1 to Q2.

These reports mainly centred around scammers' use of 'COVID-19' as a key word to get people's interest in their phishing emails. Other examples included:

- 'Covid survival guide' emails, containing a malware payload if users opened the attachment
- Credit card harvesting email scams masquerading as a 'Covid benefit payments', promising money if people entered their card details
- Email extortion scams threatening users families with Covid-19 infection unless a cryptocurrency payment was made.

Multi-stage malware threats

Malware compromises are some of the most serious cyber security threats we deal with at CERT NZ.

By its very nature, most malware aims to go unnoticed, which is why we often speak with people who have discovered all too late that they've been compromised. Many people only become aware of an attack after they've experienced harm from data loss, breached privacy, files held for ransom and credential thefts (leading to money being stolen).

In some cases we receive information from our partners with evidence of malware compromises before they have been detected by the end user. In these cases, CERT NZ immediately contacts the affected parties to inform them of the compromise. We then help them secure their accounts, remove the infection and put systems in place to safeguard against future threats.

We received 46 reports of malware incidents in Q1 and Q2 2020 - a 20% increase on the 41 received in Q3 and Q4 2019.

Here's a look at two cases we've handled so far in 2020.

Qakbot

A malware variant known as Qakbot (also known as Qbot) has been observed globally since around 2007[2]. It's used for cybercrime campaigns that steal sensitive information, like banking credentials, from infected users. Typically circulated via malicious email attachments, Qakbot is designed to evade anti-virus detection, infect computers and steal sensitive credentials stored in the systems they inhabit.

A common scenario is where businesses report to CERT NZ that their email account has been compromised, with further investigations revealing that the root of the compromise is linked to a Qakbot infection.

We also receive reports from New Zealand and internationally-based security partners about the Qakbot activity they're observing.

Whenever CERT NZ receives reports of Qakbot activity affecting New Zealand IP addresses or email accounts, we reach out to the compromised businesses and help them get rid of the malware and restore their system.

Ryuk

Trickbot/Ryuk is an interesting ransomware variant. According to security firm CrowdStrike, "Ryuk is specifically used to target enterprise environments"[2]. It is often installed on systems that have already been compromised with other criminal malware like Trickbot. Once the attackers have stolen their desired information (such as data and credentials), they use the malware to download and install Ryuk to encrypt the system files for ransom, as a nasty way of 'double monetising' the compromise.

In January 2019 CrowdStrike also commented, "since Ryuk's appearance in August (2018), the threat actors operating it have netted over 705.80 BTC across 52 transactions for a total current value of $3,701,893.98 USD".

The reports of Ryuk seen by CERT NZ came via one of our partners, who shared a number of IP addresses that had previously been compromised by another malware (such as Trickbot or Emotet). The attackers were now using that compromise to deploy the Ryuk ransomware.

CERT NZ proactively worked with the ISPs to identify the infected parties and provide them with advice on recovering from the compromise.

Preventions and mitigations

Malware is easier to avoid than to fix. Implementing CERT NZ's critical controls will help organisations protect themselves from much of the malware circulating.

The following controls are particularly relevant to preventing malware attacks:

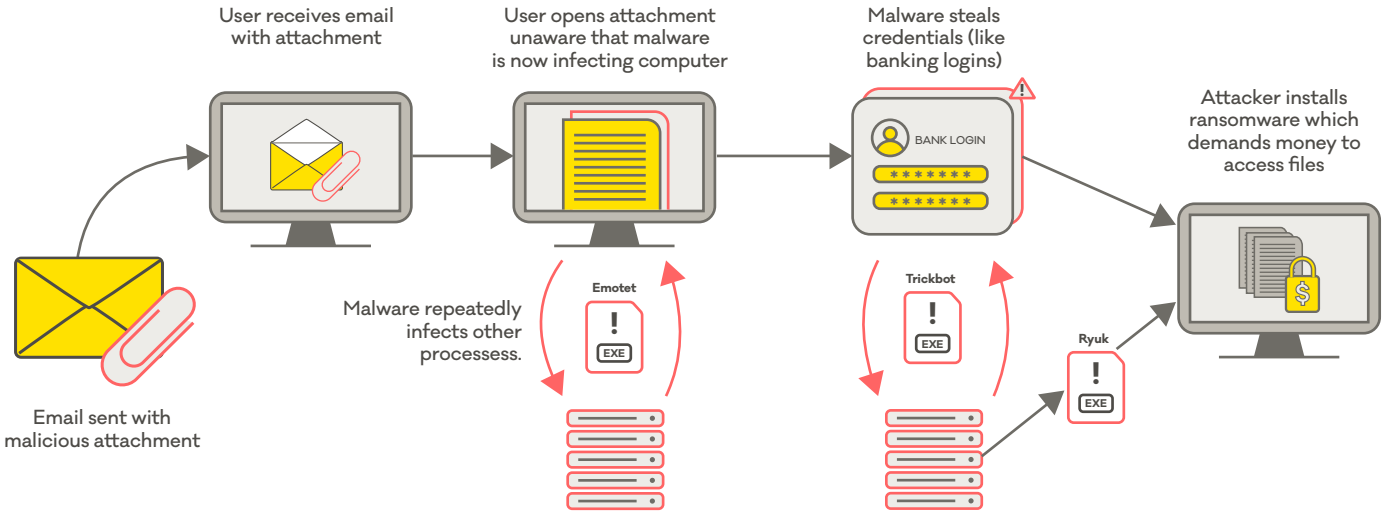
- Patching (updating) your software and system
- Implementing and testing backups
- Enforcing the principle of least privilege
- Implementing network segmentation

See the full list of controls here:

https://www.cert.govt.nz/it-specialists/critical-controls/

2. https://securityintelligence.com/qakbot-banking-trojan-causes-massive-active-directory-lockouts/ and https://threatpost.com/prolock-ransomware-qakbot-trojan/155828/

This is how a multi-stage malware infection, such as Ryuk, works



Some key malware terms

Malware can be complicated! Particularly when talking about variants, families, stages and types. Here are some of the key things you need to know when talking about malware:

Malware – is short for "malicious software". Malware is designed to infiltrate, damage or obtain information from a computer system without the owner's consent.

Virus – is malicious software or code designed to infect and spread throughout a computer after a user is tricked in to running it.

Worm – a worm is malicious software that self-replicates and is designed to infect other connected computers or networks without any interaction from a user.

Ransomware – a common malware variant with a specific purpose. If installed (usually by tricking a user into doing so, or by exploiting a vulnerability) ransomware encrypts the contents of the hard drive of the computer it is installed on, and demands the user pay a ransom to recover the files.

Trojan – malicious software that attempts to hide its malicious code by masquerading as an legitimate program or file – such as a document or excel attachment to an email that actually is actually executable malware.

Variants – over time, malware types have been added to by their original developers and others, resulting in different types of malware evolving from a common base. The new 'variants' might be closely related to other malware and are often grouped into 'families'. An example would be the Andromeda malware, which shares some features of earlier malwares like Dridex and Dorkbot[3].

Module/Stages – as a method of avoiding detection, malware authors have started breaking up malware into modules and stages. Typically, a smaller-sized initial stage is used to conduct the initial compromise which, once established, pulls down additional tools at different stages as required for the attacker's particular objectives.

Persistence – a lot of malware is designed to establish itself on systems and networks in a way that makes it very hard to remove, even if detected. Establishing persistence is one of the very first goals malware seeks to achieve when it is first executed on a system.

Remote Access Trojan (RAT) – a type of malware that, once executed, allows an attacker remote access to the infected computer or system.

A full list of terms is included in the glossary section of the Q1 & Q2 2020 Data Landscape Report

Sources for definitions:[4]

3. https://blog.avast.com/andromeda-under-the-microscope
4. https://blog.malwarebytes.com/glossary/
https://csrc.nist.gov/glossary
https://www.csoonline.com/article/2123316/a-layman-s-glossary-of-malware-terms

Insecure computers used for bruteforcing attacks

CERT NZ received 21 reports of bruteforcing from New Zealand IP addresses in Q1 & Q2. Bruteforcing is where attackers try to gain access to systems by trying multiple passwords or passphrases in the hope of eventually landing on the correct one. They usually use automated tools or scripts to do this at a large scale, often using sets of common passwords obtained from data breaches.

Insecure computers connected to the internet are frequently targets of bruteforcing attacks. They can also be used to conduct bruteforcing attacks on other systems, enabling attackers to cover their tracks. Unpatched systems are particularly vulnerable to this type of misuse, and the use of multi-factor authentication is one of the best practical defences.

CERT NZ recently received alerts about bruteforce activity from an overseas CERT and from threat intelligence provided by AbuseIPDB.[5] The alerts advised that a significant number of the bruteforcing attacks observed had come from New Zealand-based networks. CERT NZ contacted the ISPs who owned the IP addresses, who in turn began an internal investigation with their customers.

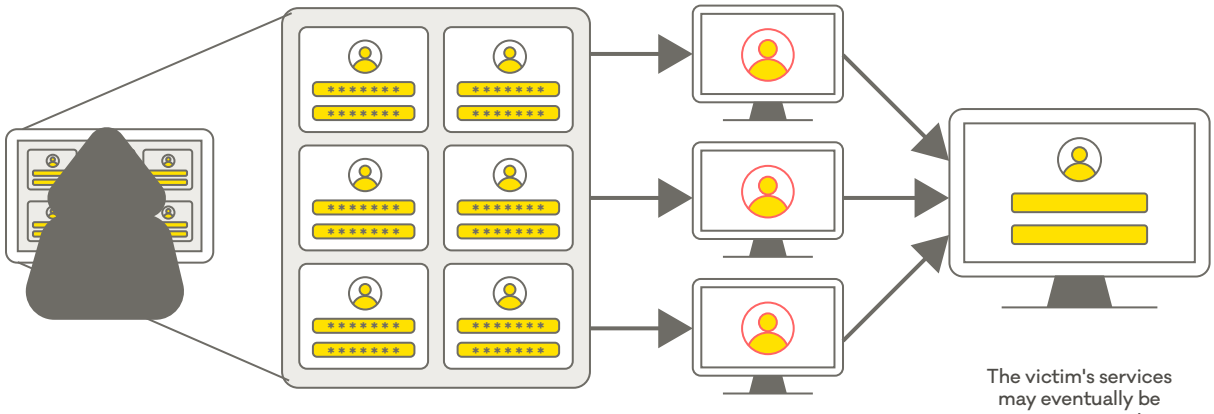
It is likely that the IP addresses were linked to previously compromised servers now being used as automated bots to conduct large scale bruteforce attacks.

AbuseIPDB is a project dedicated to helping combat the spread of hackers, spammers and abusive activity on the internet. Their mission is to help make the web safer by providing a central blacklist for webmasters, system administrators, and other interested parties to report and find IP addresses that have been associated with malicious activity online. Anyone can report suspicious IP addresses to their website.

Guides to both patching and multi-factor authentication can be found on the CERT NZ website:

https://www.cert.govt.nz/it-specialists/critical-controls/patching/

https://www.cert.govt.nz/it-specialists/guides/multi-factor-authentication/



5. https://www.abuseipdb.com/

Case study

NZTA vehicle license email scam

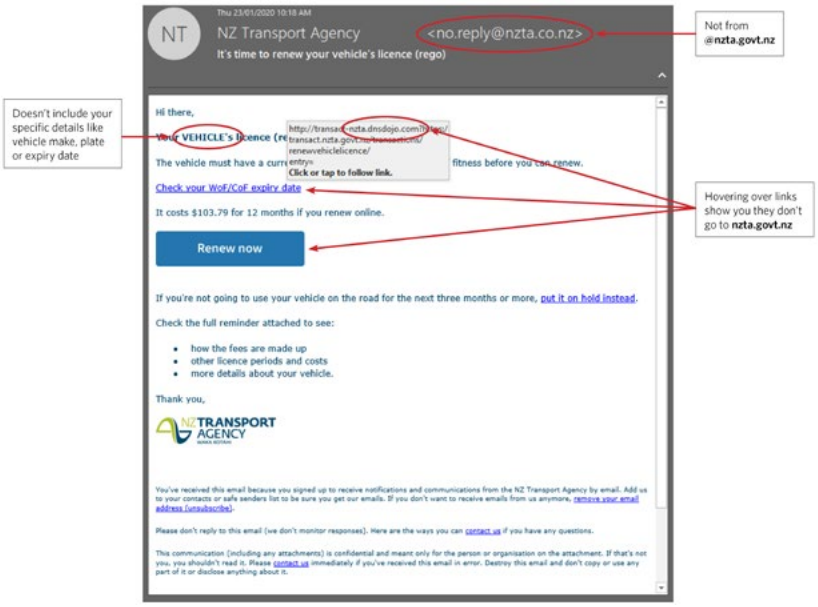
A sustained phishing campaign by scammers pretending to be the New Zealand Transport Agency (NZTA) has been seen throughout the first half of 2020.

In this campaign, waves of emails were sent to thousands of New Zealanders telling them to renew their vehicle registrations. Taking this action meant the person was directed to a fake NZTA website, from where the attacker could steal their credit card details. Perhaps even more concerning, is that the driver license details obtained by the attacker can be used to commit not only financial fraud, but also identity fraud. Driver license holders may not be aware of this until months or years down the track when they are denied credit.

It's a good idea to check your credit status every year. That way, you can see if any accounts have been opened in your name.

Instructions on obtaining a free credit report can be found here:

https://www.govt.nz/browse/consumer-rights-and-complaints/debt-and-credit-records/check-your-own-credit-report/



CERT NZ received 119 reports of NZTA-themed phishing emails in Q1 and Q2, and collaborated with NZTA to have the websites taken down and limit New Zealanders' exposure to the scam.

An alert with further details on how to spot the scam is on the NZTA website: **https://www.nzta.govt.nz/online-services/report-a-phishing-scam/latest-phishing-scams/**

Phishing website disruption

A further 54 incidents involving phishing sites impersonating well-known New Zealand brands were pro-actively identified from our threat intelligence data.

This enabled CERT NZ to flag the problem with network operators, website hosting providers and major internet browsers, thereby limiting everyday New Zealanders' exposure to the attacks.

Phishing & credential harvesting

▲ 37% increase

A total of 1,484 reports of phishing & credential harvesting incidents were received in Q1 and Q2 2020, a 37% increase on the 1,085 received in Q3 and Q4 2019.