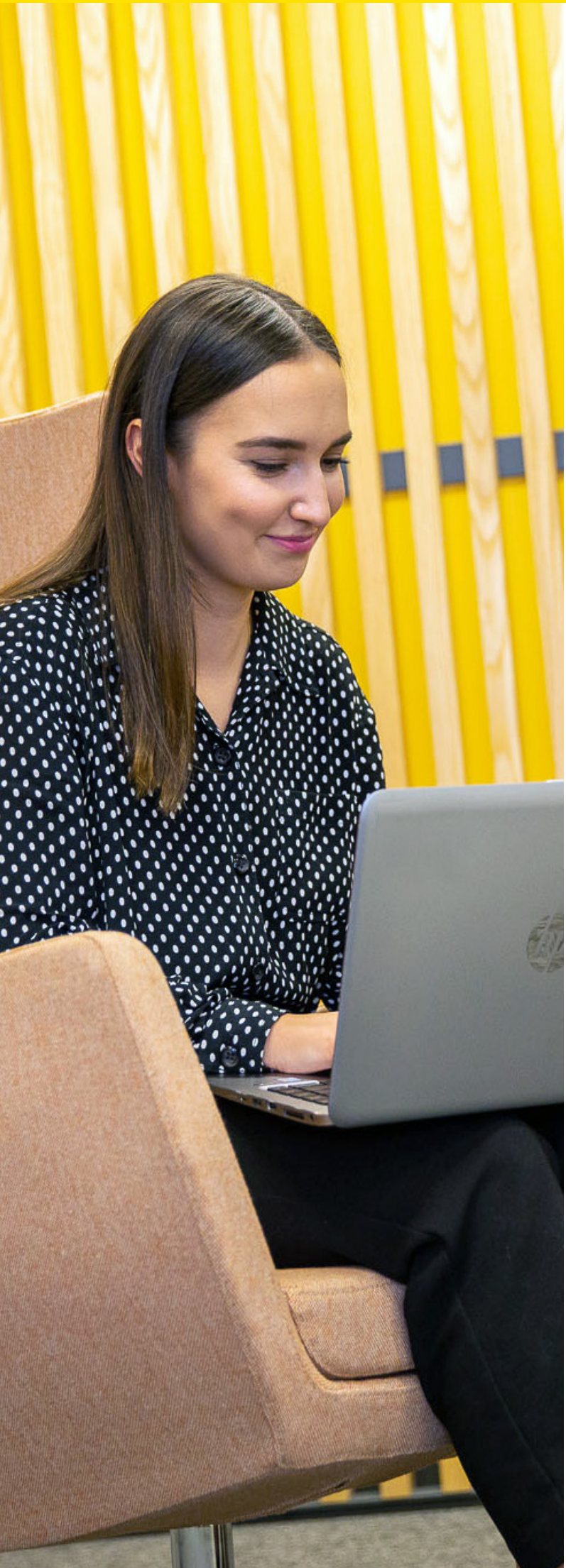


certnz

Quarterly Report: Highlights.

Q1 1 January – 31 March 2018

New Zealand Government

/// Director's message

With our first year under our belt we've thought about the best way to share the data we collect and what it means about the cyber security landscape in New Zealand.

> "We make the most difference when we're working as a fence at the top of the cliff"

We know that reporting every quarter works for you, and we're going to keep it up. From this quarter we'll produce two new reporting documents:

- **Quarterly Report: Highlights** document which summarises key observations and focus areas that our data is demonstrating, and
- **Quarterly Report: Data Landscape**, which provides graphs and information about the reports we receive, and the impact this has on New Zealand.

Things are changing in our data too. For the first time we have received more than 500 reports in a quarter. With this increase comes more information about the impact on New Zealanders; financial losses continue to be high, with almost $3 million in direct financial loss reported. We're also sharing some new analysis, including insights on the age distribution of people making reports to CERT NZ, and information on how we respond to the prevalence of phishing reports.

We help Kiwis improve their cyber security using the data we collect and collate. We make the most difference when we're working as a fence at the top of the cliff, rather than focusing just on being the best ambulance at the bottom of it. We're doing this by working on new ways to disrupt models of attack and building outreach activities that help people take simple actions to protect themselves online.

While we will always have a response role to play, CERT NZ doesn't only support the people reporting to us. We use the information we receive to identify other New Zealanders who are vulnerable to being impacted and reach out to them to help stop incidents before they happen. We do this either directly or publically, via our alerts and advisories process, through the army of partners that we work with, or through our outreach programmes such as Cyber Smart Week.

Rob Pope
Director, CERT NZ

/// Q1 highlights

506 incident reports

were made in Q1, the highest number received in a quarter since CERT NZ was established.

$3 million in losses

Significant losses continue to be reported, with almost $3 million in losses in Q1. 45% of incidents reports show some form of loss.

Increased vulnerability reports

Vulnerability reports increased considerably, with twice as many received in Q1 2018 as in Q4 2017.

New ransomware variants

We received reports of two new ransomware variants – Rapid and David.

Over 55s report 87% of financial loss

For the first time , we can share insights about the age of individuals reporting to CERT NZ.

In Q1 we received 180 incident reports that provided a date of birth, out of a total of 297 reports about individuals[1].

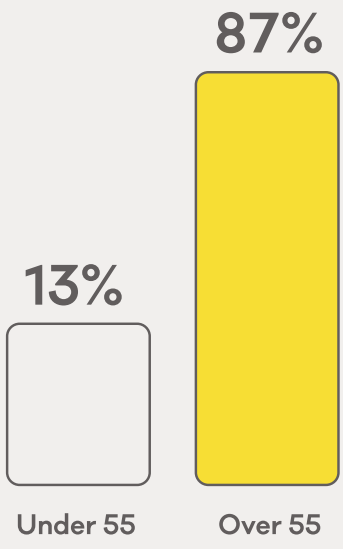
Of these 180 reports, the largest age bracket reporting to CERT NZ was people over 65 years, although New Zealanders of all ages were targeted and vulnerable to cyber security threats: the average number of reports per age bracket was 26.

When we look at reported financial loss by age, 87% of the value of financial loss impacts people over 55[2].

This data helps us develop specific outreach programmes that work for the communities that we are targeting.

Read more about the data in section 6 of CERT NZ's Quarterly Report: Data Landscape[3].

Financial loss by age



1. This figure also excludes reported vulnerabilities, as those are from individuals proactively reporting issues, rather than having been affected by them.
2. For the reports that provide date of birth
3. https://www.cert.govt.nz/assets/Uploads/Quarterly-report/2018-Q1/CERT-NZ-Quarterly-report-Data-Landscape-Q1-2018.pdf [PDF 954KB]

Highest ever number of vulnerabilities reported

CERT NZ received 35 vulnerability reports this quarter, the highest number in a quarter since reporting began and more than twice as many as in Q4 2017.

A vulnerability is a weakness in software, hardware, or an online service that can be exploited to access information or damage a system[4]. The reports received ranged in complexity from small web application bugs through to large network device vulnerabilities. In each case, CERT NZ worked with the vendor to help them understand the vulnerability and resolve it.

A small number of expert security researchers made almost 50% of vulnerability reports. Their contribution helps improve cyber security for all New Zealanders.

Phishing takedowns on the up

Taking down phishing websites is one way to reduce the impact of phishing on New Zealanders. This quarter we can report the number of takedowns CERT NZ has been involved in.

102 takedown requests were received, either for specific action by CERT NZ or to support reports made by impacted banks and financial services organisations.

This quarter, phishing is the top category of incident reports (39%), after being overtaken by scams and fraud in Q4 2017. Part of this increase is due to the increase in the number of phishing website takedowns CERT NZ has been involved in as we ramp up our efforts to try and address this problem.

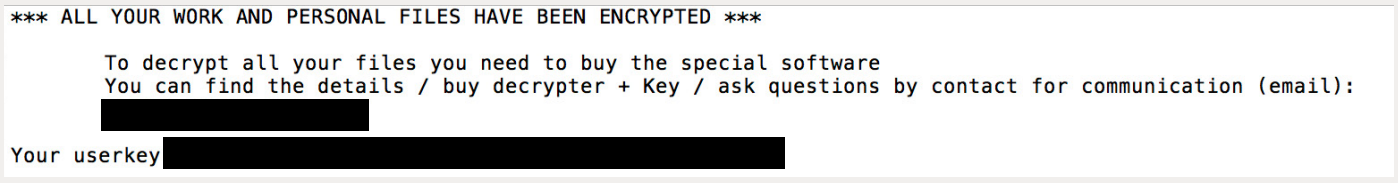
102
takedown requests were received.

Case study: Backups minimise impact from David ransomware

A transport operator reported a ransomware infection to CERT NZ. The attackers gained access by brute-forcing passwords for local administrator accounts through remote access. The ransomware was a new variant, David. All files on the computer were encrypted and the ransom demand was shown in a simple text screen.

Because the organisation runs backups daily, there was minimal impact to the business: the user's computer was replaced and the data was restored from backups. All local administrator credentials were also changed.

Security has been improved since the breach by implementing additional security controls where remote access is required. CERT NZ recommends keeping remote access software patched, disabling any unused remote services and enforcing multi-factor authentication where possible. More information on these controls can be found in the CERT NZ Critical Controls 2018[5].



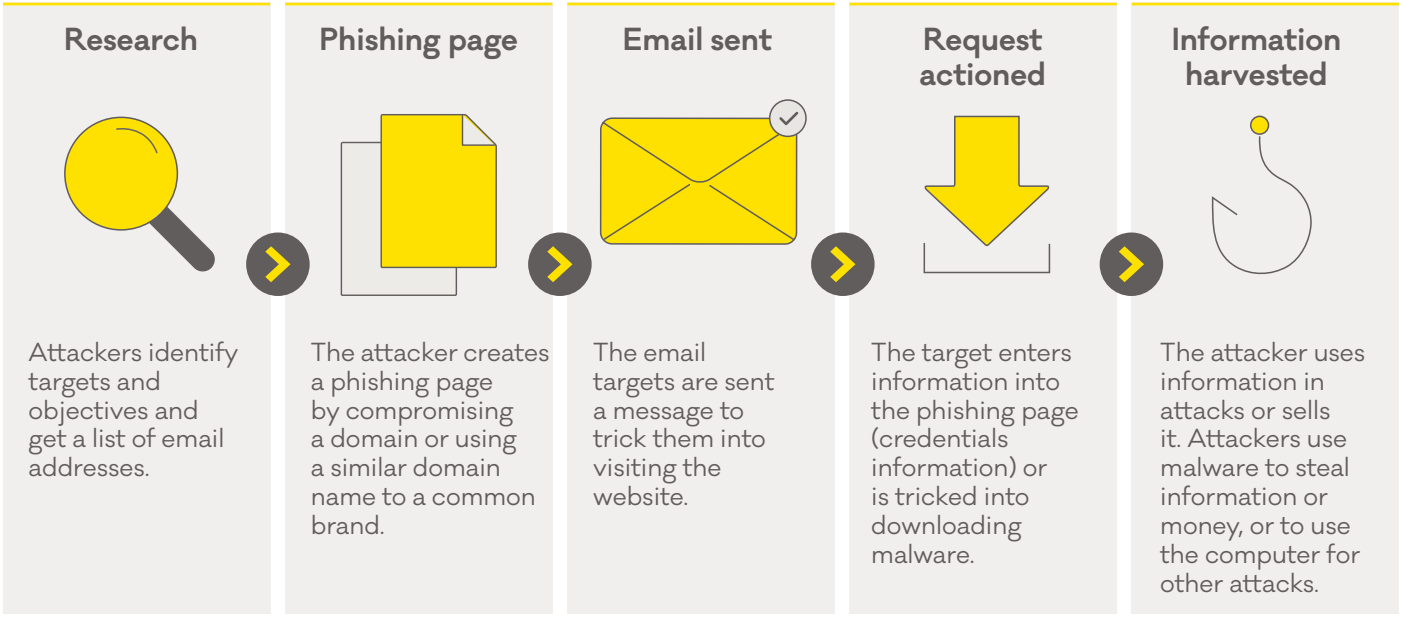
4. Read about CERT NZ's coordinated vulnerability service: https://www.cert.govt.nz/it-specialists/guides/reporting-a-vulnerability/
5 https://www.cert.govt.nz/it-specialists/critical-controls/10-critical-controls/

/// Focus area – phishing campaigns

Phishing email campaigns are one of the most common, prolific and successful cyber threats that we see.

They are repeated because they're effective, play on a numbers approach, and are low cost to run. Attackers can easily send phishing emails to 10,000 people and even if only 5% respond by clicking a link, they've had success with 500 people.

One of the challenges with phishing is that it exploits normal everyday behaviour of users. For example, customers are regularly sent emails from businesses that ask them to click website links for further information, and many of them require the customer to log in. Whether it's legitimate or a phishing attack, a user is likely to expect to have to do this. By using this process, attackers masquerade as legitimate, trusted brands and use these normal processes to trick users into giving up information, or credentials, or installing malicious applications. **The process works as follows:**



One way to disrupt these campaigns is to prevent step two. Attackers seek out unpatched or insecure websites local to the target brand and take them over to run their campaign. They target local brands and websites to make the phishing emails appear more trustworthy.

Attackers will also register for domains that are similar to their target brand, by either misspelling the brand name (e.g. using a 1 instead of an l) or using a different top level domain (e.g. using .org instead of .co.nz).

When CERT NZ triages phishing incidents, we investigate the phishing page to understand where the web server is hosted, where the domain is registered, and if the website appears to be a legitimate one that was compromised. We work with hosting providers, the Domain Name Commission, and other domain registrars to try and make contact with the domain owner. We also work with other international CERTs if the web server or domain is in another jurisdiction.

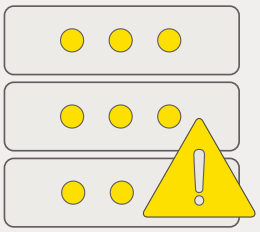
Disrupting phishing campaigns is a critical part of addressing cyber threats in New Zealand. We are looking at how can do this with our government and private sector partners.

/// Focus area – CERT NZ uses vulnerability information to protect memcached servers

This quarter CERT NZ was notified of a traffic increase to memcached servers. These servers are widely used to speed up popular websites.

Unprotected memcached servers can be used for denial of service amplification attacks where an attacker can trigger traffic amplification at rates of 50,000 requests or more. This is far in excess of earlier amplification attacks and would have considerable impacts on anyone targeted.

In February 2018, JP-CERT (Japan) notified its partners, including CERT NZ, of an increase in traffic to specific ports, indicating scanning of the internet for unprotected memcached servers may be underway. In response to this alert, CERT NZ checked reports for active attacks either aimed at New Zealanders or which used local unprotected memcached servers.



The number of vulnerable servers was reduced by 80% within a week.

CERT NZ worked to identify unprotected memcached servers in New Zealand, finding almost 50 overall. After issuing an advisory and contacting the server owners to alert them of the risks, the number of vulnerable servers was reduced by 80% within a week of the first alert being posted by JP-CERT. The number has since been further reduced by issuing a public advisory[6] working through internet service providers to contact the remaining customers running exposed servers and alert them to the risk.

While we can't stop denial of service attacks targeting New Zealand organisations, in this case we can prevent local resources from being used by identifying vulnerable servers and ensuring they are updated with correct configurations and access controls. CERT NZ has a number of partners including other international CERTs that we share information with. We use this threat and vulnerability information to take proactive steps in protecting New Zealand, applying international context to the New Zealand threat landscape.

For more insights into what CERT NZ has seen in the New Zealand threat landscape in Quarter One 2018, see the CERT NZ Quarterly Report: Data Landscape[7]. If you have experienced a cyber security issue, report it to CERT NZ at **www.cert.govt.nz**

6. https://www.cert.govt.nz/it-specialists/advisories/advisory/memcache/
7. https://www.cert.govt.nz/about/quarterly-report/q1-report-2018