certnz

Quarterly Report: Highlights.

Q4 1 October – 31 December 2018

New Zealand Government

/// Director's message

Online threats and vulnerabilities have a big impact on business operations and the day-to-day lives of New Zealanders.

The reports we've received this quarter show that these incidents are not only causing financial impact, they're also affecting people's confidence online.

For instance, scam reports have spiked in quarter four, with a significant increase in email extortion scams. This is where attackers email a seemingly legitimate threat and demand urgent payment to revoke it – examples we've seen include bomb threat emails sent to businesses through to threats of sharing embarrassing images. Whether you're an employee in a large company or checking your personal emails at home, receiving an extortion email can be a frightening experience. Even though it's highly unlikely these threats would be realised, they can discourage people from participating in the online environment.

Scammers continually evolve their approach and employ new tactics to try and trick people into meeting their payment demands. This means it's more important than ever that New Zealanders have a trusted source they can turn to for reliable information and actionable advice to protect themselves online.

> "It's more important than ever that New Zealanders have a trusted source they can turn to for reliable information and actionable advice to protect themselves online."

As a central front door for recovering from cyber security incidents, we're here to help people mitigate these complex campaigns and stay safe online. We do this by analysing reports, gathering up-to-the-minute information, and working with partners in New Zealand and across the globe to develop and share straightforward measures. We understand first-hand how these email scams and other cyber security incidents can affect people, and it's our job to enable New Zealanders to act with confidence online and defeat them, because it is possible.

Rob Pope
Director, CERT NZ

/// Q4 highlights

1333 incident reports

were received in Q4, up 53% from Q3.

$5.9 million

in reported losses, up $3m from Q3.

783 reports

were about individuals, up 130% from Q3.

Malware reports continued to increase

with 48 reports, more than double the amount in Q3.

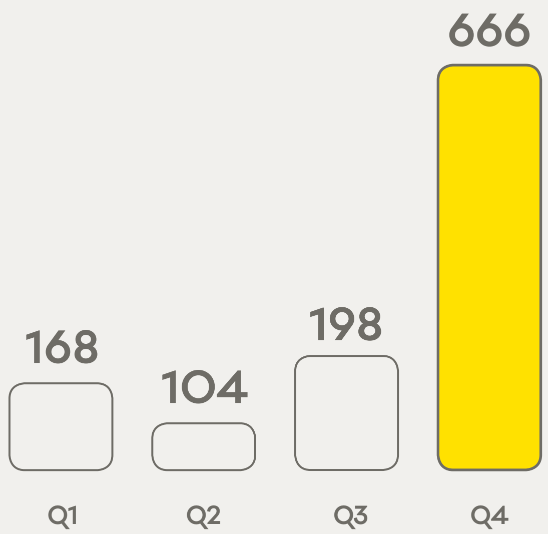
Significant spike in scams

Reports of scams and fraud increased this quarter, making up half the total number of reports received, with a total loss of $4.9 million. In total, 666 scam and fraud reports were received in Q4, up 236% from Q3.

91% of the scam and fraud reports were about individuals across all age groups and regions in New Zealand. More than a third of all reports related to a particular type of scam – email extortion.

We explore email extortion campaigns, their variants and how to mitigate them in this quarter's focus area.

Scam and fraud reports in 2018



For more insights into what CERT NZ has seen in the New Zealand threat landscape in quarter four 2018, 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**

/// Focus area – email extortion scams

In Q4, CERT NZ received a record number of incidents –36% of these related to email extortion scams.

Email extortion scams are threat-based emails that try and trick recipients into paying money to make the threat go away. Criminals behind these scams use a range of extortion tactics which have been refined over time.

The campaigns CERT NZ has seen this quarter show scammers have moved beyond just emailing large numbers of people with threats and payment demands. They now include personal information, like passwords, to make their threats seem more real.

How do they target individuals and businesses?

Like most cyber attacks, email extortion scams don't target any particular individual or business. The scammers are looking for the easiest way to make money. They gather information from public sources, like data breaches, into large sets of user credentials and passwords, and target those users.

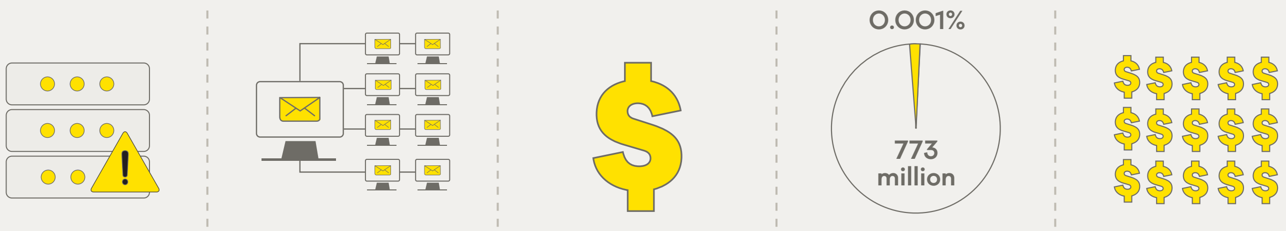
In many of the incidents reported, scammers sent an email that included a password they claimed belonged to the recipient. Some recipients reported that the password sent in the email was an old password they no longer used. This shows the scammers were likely using information they sourced from old data breaches, rather than 'hacking' the recipient's computer as the email claimed.

How do the scams work?

Scammers collect customer records from data breaches that are available online. Some of these collections contain millions of entries that include information like email addresses, passwords and other account details.

They then send extortion emails to all of the addresses on their list, sometimes including other account information made available in the data breaches. Because of the volumes of emails sent out, even if only a small percentage of people pay, the scammers can still make a considerable amount of money with little effort.

Email extortion scam example based on recent 'Collection #1' data breach



773 million users details are exposed in a data breach

Scammers target the database with extortion emails

If the average payment demand is $100

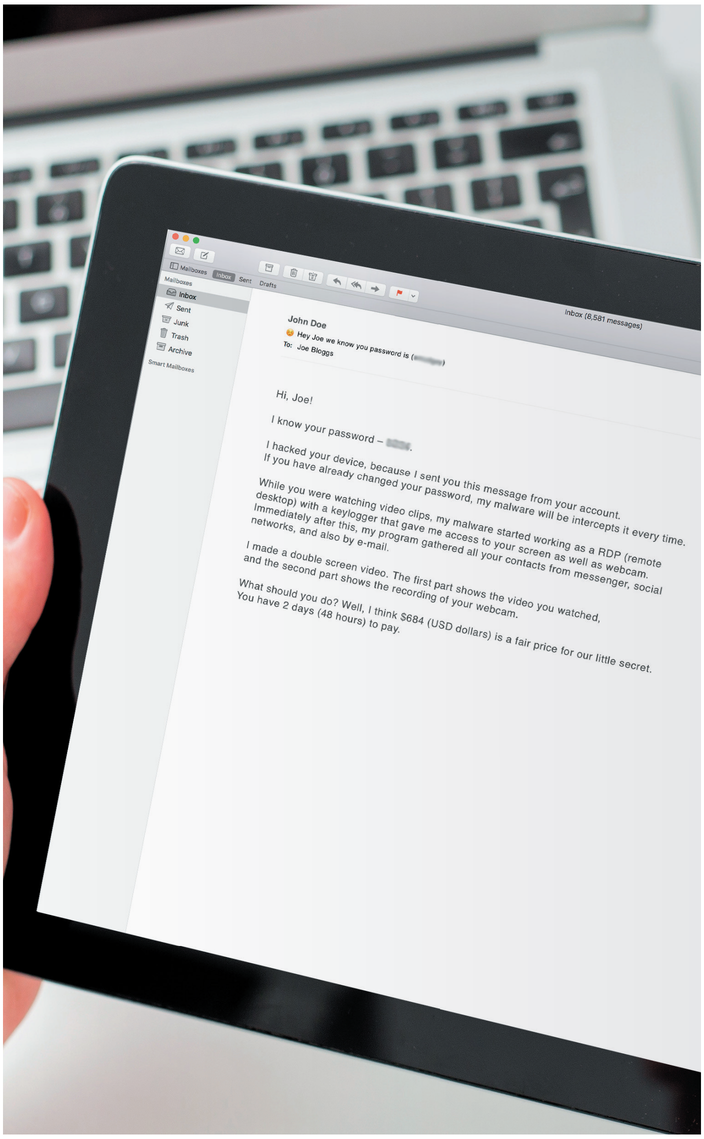
And 0.001% of recipients pay

The scammers could potentially extort $773,000

How do these scams change over time?

Scammers modify their approach to avoid being caught, or when scams become well-known and have less impact. In Q4, CERT NZ saw this happen in rapid succession.

- In October, scammers sent email threats saying they had compromised the recipient's computer, recorded them using their webcam and monitored their browsing activity. The scammers then threatened to publish embarrassing content about the recipient if they were not paid. CERT NZ issued an advisory to New Zealanders following a high volume of reports[1].
- In November, new email threats claimed that the recipient's home router had been compromised, revealing sensitive or embarrassing information about them. Attackers used technical language to make the threat more convincing.
- In December, scammers sent bomb threat blackmail emails to businesses. The emails threatened to detonate a bomb within the business' building if the payment demand wasn't met. CERT NZ worked quickly with national and international partners and issued an advisory on 14 December.[2]



John Doe
Hey Joe we know you password is ([redacted])
To: Joe Bloggs

Hi, Joe!

I know your password – [redacted].

I hacked your device, because I sent you this message from your account. If you have already changed your password, my malware will be intercepts it every time.

While you were watching video clips, my malware started working as a RDP (remote desktop) with a keylogger that gave me access to your screen as well as webcam. Immediately after this, my program gathered all your contacts from messenger, social networks, and also by e-mail.

I made a double screen video. The first part shows the video you watched, and the second part shows the recording of your webcam.

What should you do? Well, I think $684 (USD dollars) is a fair price for our little secret. You have 2 days (48 hours) to pay.

What to do if you receive an extortion email

Although these emails can be frightening to receive, it's important to report them to CERT NZ, and not contact the sender or respond to any threats made. If the scam email includes a password, make sure you change the password on any account where that password is used. You can also check if your information has been leaked in well-known data breaches with tools like 'Have I been pwned?[3]'

Report to CERT NZ online at **www.cert.govt.nz/report** or phone 0800 CERT NZ (0800 2378 69).

[1] https://www.cert.govt.nz/businesses-and-individuals/recent-threats/webcam-and-password-blackmail-scam/

[2] https://www.cert.govt.nz/businesses-and-individuals/recent-threats/bomb-threat-emails-affecting-new-zealanders/

[3] https://haveibeenpwned.com/

Case study – CERT NZ helps business resolve malware infection

In Q4, a New Zealand business with more than 20 regional offices was disrupted by a malware infection.

The compromise happened after an employee received a phishing email that looked like an invoice from a standard accounting software service.

Clicking the link loaded a webpage, where malware downloaded in the background without the employee knowing, and infected their computer.

This type of malware detects when a user accesses their business' online banking, and redirects them to an identical looking phishing page.

The phishing page collected the employee's login and two-factor authentication information. The attacker used the information to access the real banking login page, while the employee was redirected to a 'site under temporary maintenance' page.

The business' bank noticed the account was being accessed from an overseas IP address and notified the business. Both the business and the bank reported the incident to CERT NZ.

The business was concerned that removing the malware from their systems would impact their day-to-day operations. CERT NZ helped the business resolve the incident while maintaining their operations.

CERT NZ analysed the detail of this report and others, and worked with New Zealand banks and overseas partners to gather information, share advice, and help minimise the impacts on the affected business. This information was then published in an advisory[4] to alert other businesses to this threat.

> " CERT NZ helped the business resolve the incident while maintaining their operations "

[4] https://www.cert.govt.nz/businesses-and-individuals/recent-threats/malware-targeting-business-customers-of-new-zealand-banks/