# Q3 CERT NZ Quarterly Report /// July – September 2017

certnz

## Results ///

### **Incidents reported** to CERT NZ

**390** incident reports received

**297** were responded to by **CERT NZ**

**78** involved cyber crime and were referred to **NZ Police**

**15** involved cyber bullying and were referred to **Netsafe**

### **Incidents reported** by sector

The four sectors that reported the most incidents were:

**8%** Technology

**6%** Retail trade & accommodation

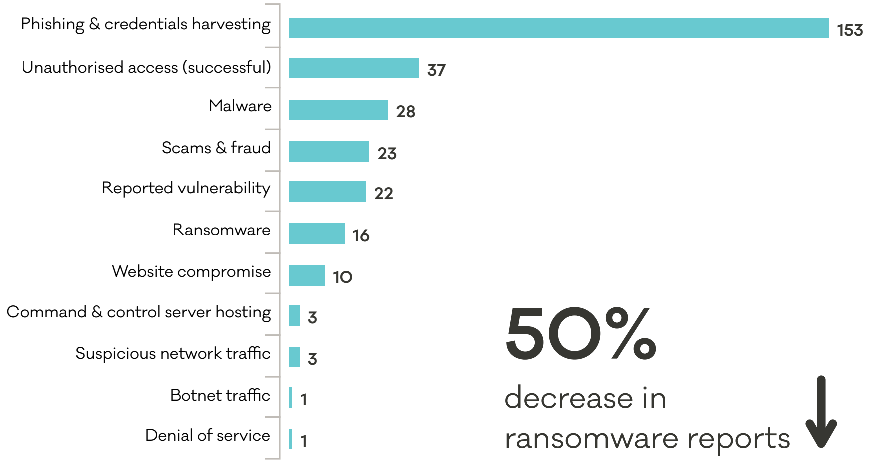
**6%** Public administration & safety

**4%** Financial & insurance services

**57%** of incidents reported were about individuals

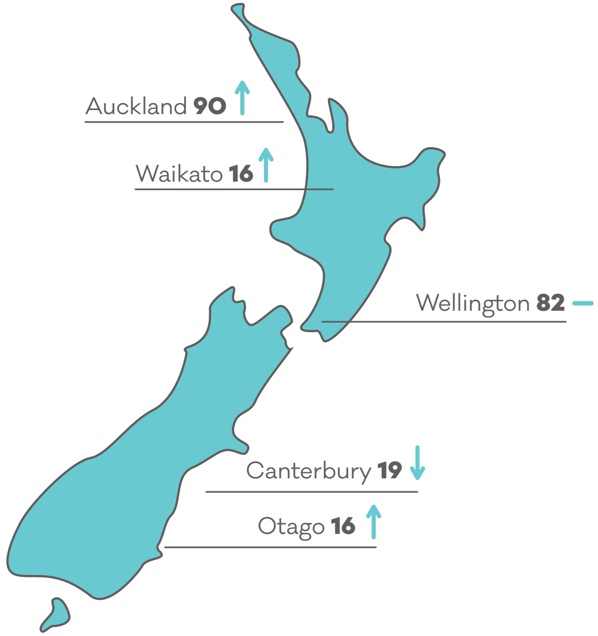
Reporting period: 1 July - 30 September 2017

### **Incidents reported** by type



**50%** decrease in ransomware reports ↓

### **Highest reporting** regions



## Impacts ///

Over **$1.1 million** in direct financial loss was reported.

**29%** of people who reported incidents suffered some form of loss.

### **Case study** - Avalanche clean-up underway

CERT-BUND (Germany) alerted us to New Zealand hosts that were infected by the Avalanche botnet. CERT-BUND was part of a joint operation with international law enforcement agencies to take down the Avalanche botnet server infrastructure in 2016 .

The Avalanche botnet was used as a delivery platform to launch and manage mass global malware attacks and money mule recruitment campaigns. The takedown operation involved law enforcement agencies seizing the command and control servers for the network, disrupting their operations.

As part of the on-going clean-up operation, a number of infected hosts in New Zealand were identified. We have been contacting the relevant ISPs to notify them of the affected computers on their networks to help them clean up the infection.

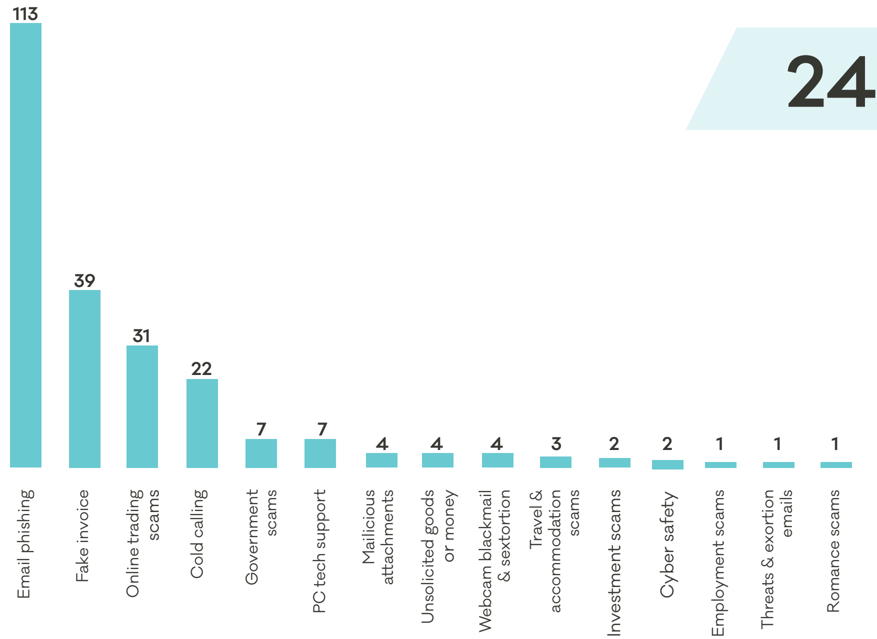
# Q3 CERT NZ Quarterly Report /// July – September 2017

## Focus on scams & fraud ///

Scams & fraud can be categorised as a single incident in itself or part of a wider attack. CERT NZ and Netsafe are working together to align reporting to create a better picture of the scams & fraud landscape.

**2619** scams & fraud reports received by CERT NZ and Netsafe

**$2.1 million** financial loss reported as a result of scams & fraud



**242** scams & fraud reports were received by CERT NZ

**47%** of scams & fraud reports involved email phishing campaigns

## Invoice Scams

Invoice scams were identified in 39 (16%) of scams & fraud reports.

**A basic invoice scam involves scammers sending out fake invoices disguised as invoices for well-known services.**

If recipients pay the bill, they lose their money.

If they enter into contact with the scammers, the scammers will usually use a variety of social engineering tactics ranging from persuasion through to bullying to try and convince them to pay the fake invoice.

There are also more sophisticated campaigns, where scammers send emails to businesses and organisations that appear to be from a senior executive (such as a Chief Financial Officer) asking the recipient to pay an urgent bill.

These emails can come from fake email addresses intended to look legitimate. Scammers also try to use phishing techniques to gain access to businesses email addresses, making the fake invoices much harder to detect.

Businesses with overseas suppliers have received fake copies of the suppliers invoices. In some cases these suppliers were compromised by attackers, who altered invoices from them in order to steal money from legitimate transactions.

Reporting period: 1 July - 30 September 2017

## Case Study – Invoice scam costs company over $300k

CERT NZ received a report from a small company in the retail, trade and accommodation sector, who had lost a lot of money to an invoice scam. The NZ company had a supplier in China they used regularly. Scammers had managed to get enough information about the Chinese supplier to imitate their emails, including using a very similar email address, and even copying the signature in the email.

The scammers then sent fake invoices to the NZ company, at a time they were expecting to pay and as a result, paid the fake invoices, resulting in losses of over $300,000. The case was referred to the NZ Police for investigation.

More tips for staying safe online can be found at **www.cert.govt.nz**