certnz
newzealand.govt.nz

CERT NZ QUARTERLY REPORT
April - June 2017

Since our launch on **11 April 2017,** we have analysed trends in local cyber security data.

Results

These results reflect data collected in the period 11 April – 30 June 2017.

Incidents reported to CERT NZ

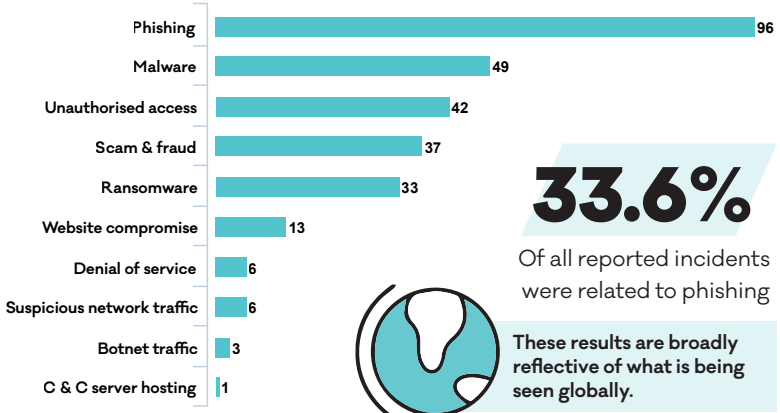
364
incident reports received for the **11 April – 30 June 2017** period.

286
were responded to by **CERT NZ**

70
involved cyber crime and were referred to **NZ Police**

8
involved cyberbullying and were referred to **Netsafe**

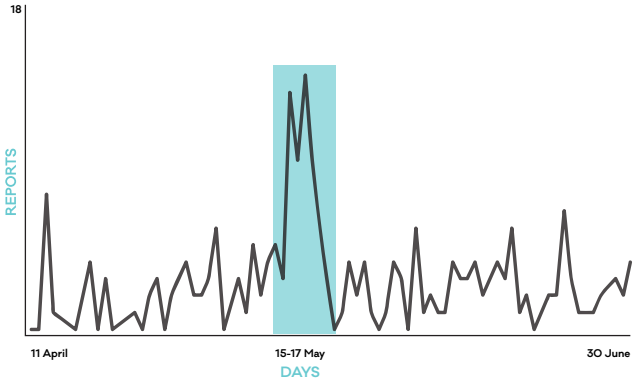
Incident reports by type



33.6%
Of all reported incidents were related to phishing

These results are broadly reflective of what is being seen globally.

Reporting spike in May



MAY

A reporting spike occurred immediately following the WannaCry ransomware event in **May 2017**

6
CERT NZ received only 6 WannaCry incident reports

Impacts

Cyber security incidents are inflicting significant losses on New Zealanders.

Losses caused by cyber crime

Over $730,000
in direct financial loss as a result of cyber crime, have been reported.

28%
of people who reported incidents suffered some form of loss.

Case Study: Phishing

Recently we received an incident report about a phishing campaign that claimed to be from a well-known New Zealand company. The phishing emails were sent from a .nz email address, and had links in them directing victims to fake websites that tricked users into providing financial details. The sites were very convincing and well made, making it difficult to tell they were fakes at a glance.

We identified the ISP that the email address used, and working with them we blocked the email address from sending any further phishing emails.

We also contacted some of our international CERT partners in countries that the fake websites were hosted in, to ask them to take action and block the fake websites.

With both of these measures, the phishing campaign was effectively stopped. New Zealanders were no longer getting the emails, and those that did couldn't fall victim to the fake website as it had been taken down.

Thanks to the connections established with the international CERT community, we were able to rapidly assist the take down of the phishing campaign and contain the incident.

certnz
newzealand.govt.nz

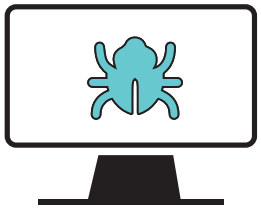
CERT NZ QUARTERLY REPORT
April - June 2017

Since our launch on **11 April 2017,** we have analysed trends in local cyber security data.

Focus on ransomware

Ransomware attacks are causing losses to New Zealanders. Here's a quick guide to ransomware.

What is ransomware?

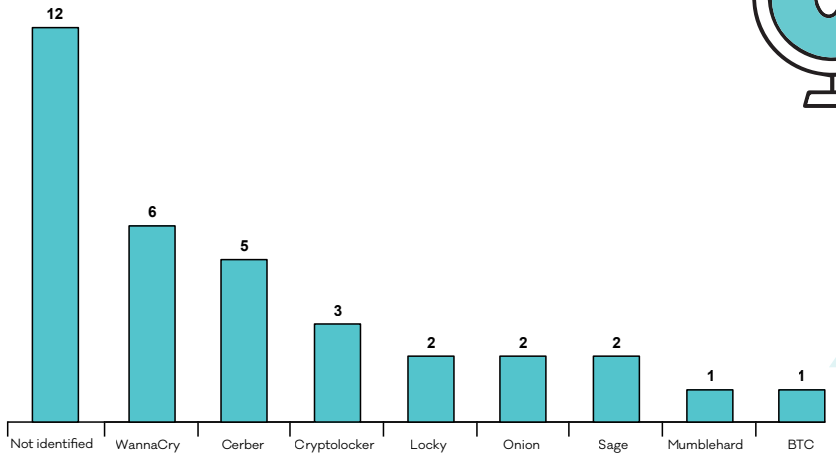


RANSOMWARE
is a type of malicious software (or malware) that tricks users into installing it onto their systems.

It then encrypts their system files and demands a ransom payment to decrypt them.

BE CAREFUL
when visiting unsafe or suspicious websites, opening emails or files from someone you don't know, clicking on malicious links in social media.

Ransomware reported in NZ



Two variants received major global attention: **WannaCry** and **NotPetya.**

CERT NZ only received 6 reports of **WannaCry** affecting New Zealanders

Protect yourself against ransomware

Always update your operating system and your apps when new versions are available. You can set this up to happen automatically with Windows and a lot of other applications like Office.

Make sure you back up your files regularly. This includes the files on your computers, phones and any other devices you have.

WannaCry

WannaCry was a newly discovered ransomware variant, which made headlines globally in May 2017 after it compromised a number of networks around the world. The ransomware blocked access to computers and demanded approximately $430 (NZD) to unlock it. Even if the victim paid the ransom, it was highly unlikely they would recover their files.

The ransomware spread rapidly via a vulnerability in computers running unmatched versions of Windows by exploiting flaws in Microsoft Windows SMB Server.

Once a single computer in a network was infected with WannaCry, the ransomware looked for other vulnerable computers on the network and infected them too.

CERT NZ published an advisory in response to the event which contained preventative measures and mitigations to protect networks. In the days following the attack, CERT NZ received 6 incident reports of WannaCry infections from small businesses.

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