certnz

Quarterly Report: Data Landscape

Q1 & Q2 2020

1 January – 30 June, 2020

New Zealand Government

Contents

1. Introduction

The CERT NZ Data Landscape report for Q1 and Q2 2020 provides a standardised set of results and graphs for the first half of 2020, and an analysis of the latest trends. Analytical comment is provided where meaningful or interesting trends are identified.

The report covers quarters one and two (1 January – 30 June) 2020, and supplements the:

- CERT NZ Quarterly Report: Highlights Q1 & Q2 2020, providing an overview of the cyber security incidents reported during the first two quarters of 2020.
- CERT NZ 2020 Half Year Summary, providing and overview of what we have seen and done so far this year.

All three documents can be found on our website at: https://www.cert.govt.nz/about/quarterly-report/

2. Incidents and referrals

Incident summary

Between 1 January and 30 June 2020, 3,102 incidents were reported to CERT NZ.

Of the 3,102 incidents reported:

- 2,528 (81%) were responded to directly by CERT NZ
- 562 (18%) were referred to New Zealand Police
- 10 (0.3%) were referred to the Department of Internal Affairs (DIA).
- 2 (0.06%) were referred to the National Cyber Security Centre

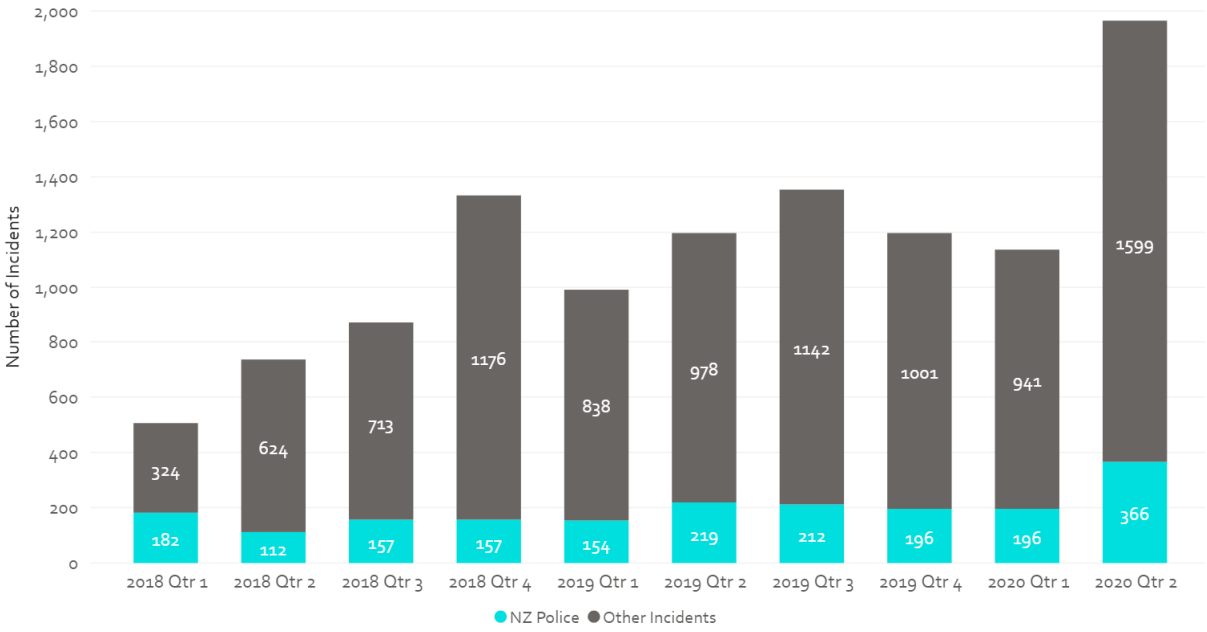
This is broadly consistent with the trends throughout 2019, with just a slight rise in the proportion of incidents referred to New Zealand Police, up 2% from 16% in 2019.

Table 1: Incident partner referrals

Q1	Q2	
933	1,595	responded to directly by CERT NZ
196	366	referred to NZ Police
0	0	referred to Netsafe
2	0	referred to National Cyber Security Centre
6	4	referred to Department of Internal Affairs
1,137	**1,965**	**Total**

Incidents per quarter

Figure 1: Number of incidents reported by quarter



3. Reporting by incident category

Breakdown by category

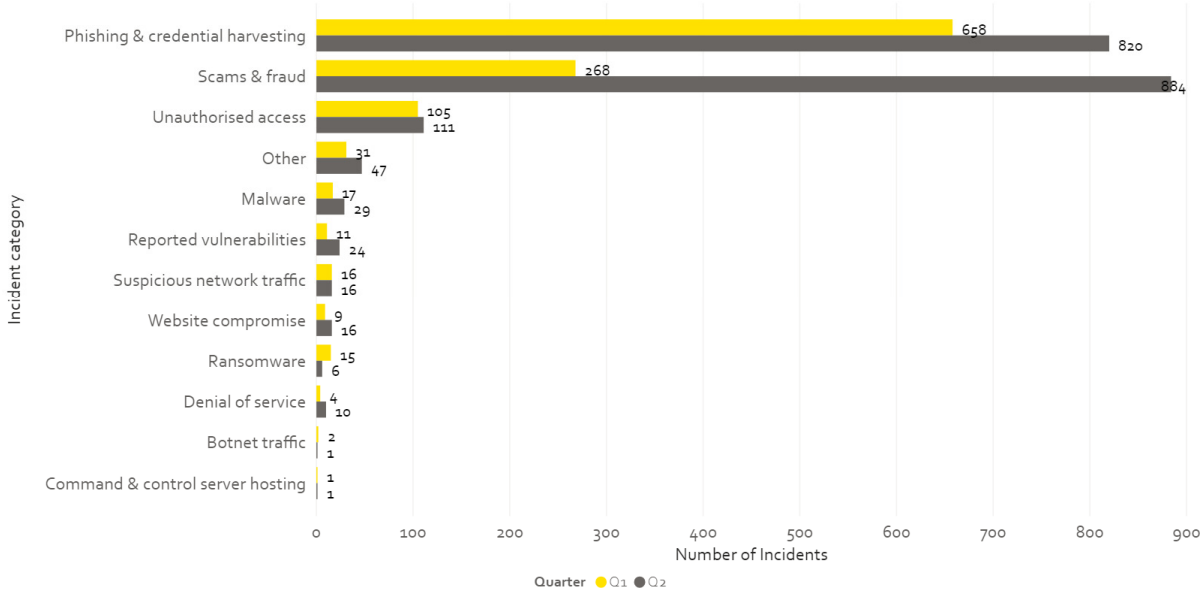
We received 884 reports of scam and fraud incidents during Q2 2020, a 230% increase on Q1. Reports of phishing and credential harvesting have shown consistent growth with a quarter-on-quarter increase of 15% in Q1, and 25% in Q2

Notable incident category trends include:

- a drop in reported incidents of ransomware quarter-on-quarter, down from 17 reports in Q4 2019 to six in Q2 2020
- a 52% increase in reports of malware during Q2, with 29 reports, from a rolling quarterly average of 19 over the previous three quarters
- significant increases in vulnerability reports – up to 24 in Q2 compared to just five in Q4 2019

For more information about the incident reports received, read the CERT NZ Quarterly Report: Highlights Q1 & Q2 2020 on https://www.cert.govt.nz/about/quarterly-report/

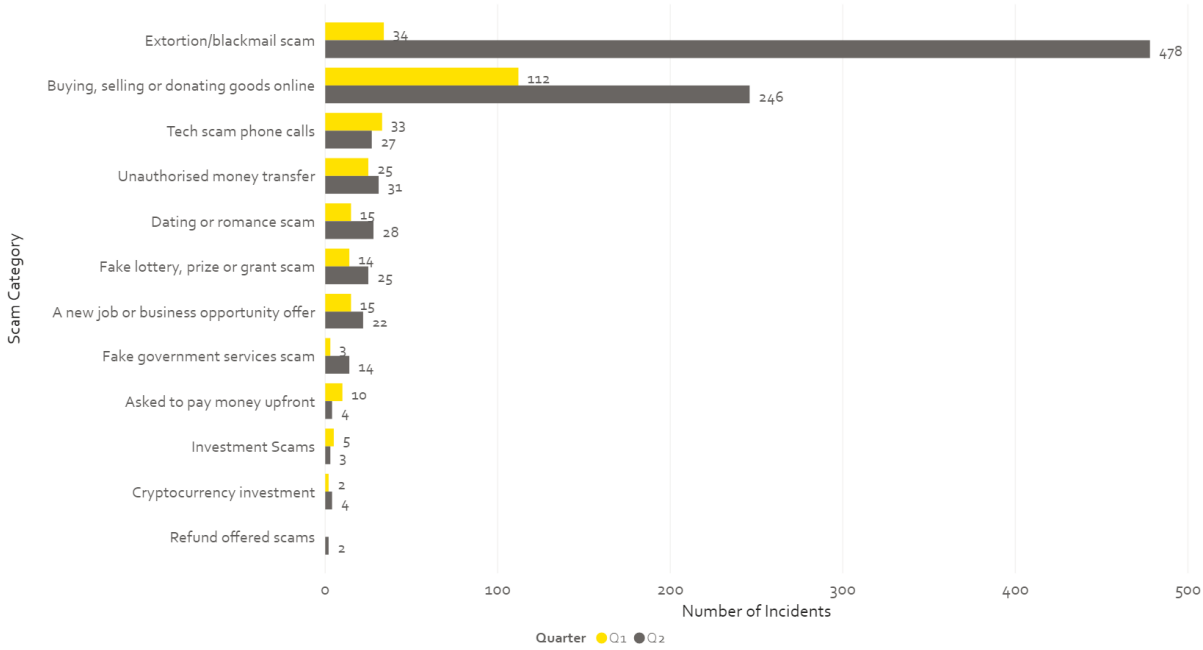
Figure 2: Breakdown by incident category



Breakdown of scam and fraud incidents

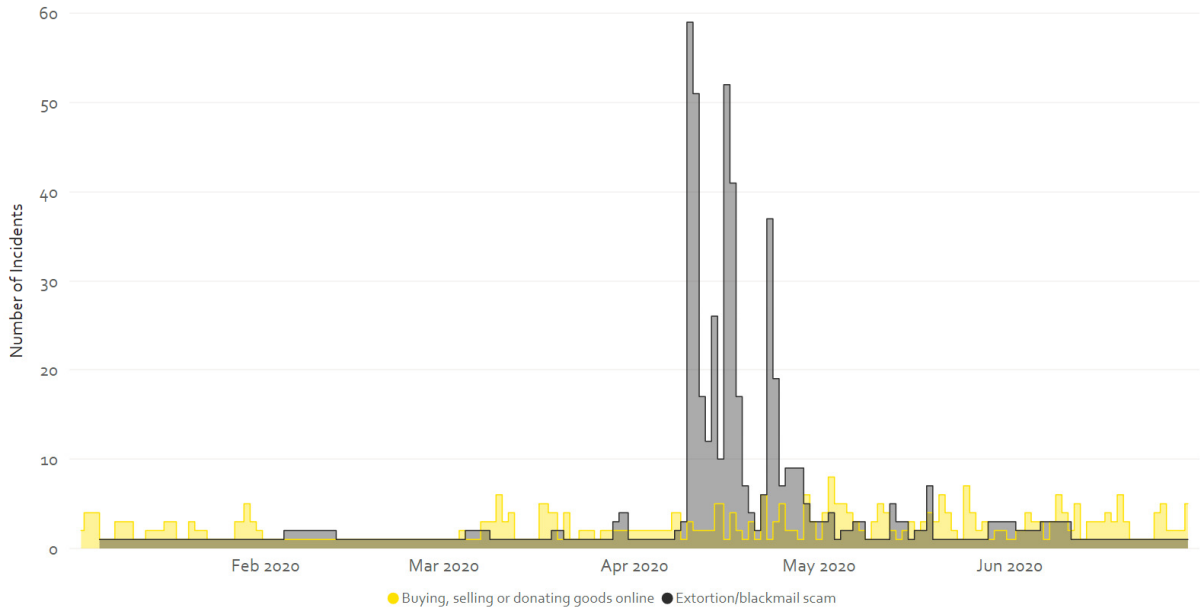
Of the incidents reported during Q1 and Q2, 1,152 (37%) were about scams and fraud. The scam and fraud category consistently features in the top three categories of incidents reported to CERT NZ. In 2019, CERT NZ began breaking down scam reports in to sub-categories, to gain further insights into the types of online scams and fraud affecting New Zealanders. The graph below shows the number of reports per sub-category.

Figure 3: Breakdown of scam and fraud categories



Of particular note during Q2 is the sharp spike in extortion/ blackmails scams over a four week period, with volumes then dropping back down to historical averages by the end of the quarter. In contrast, we noted a consistent increase in volume of scams relating to buying, selling or donating online throughout the quarter.

Figure 3a: Top two scam and fraud categories by day

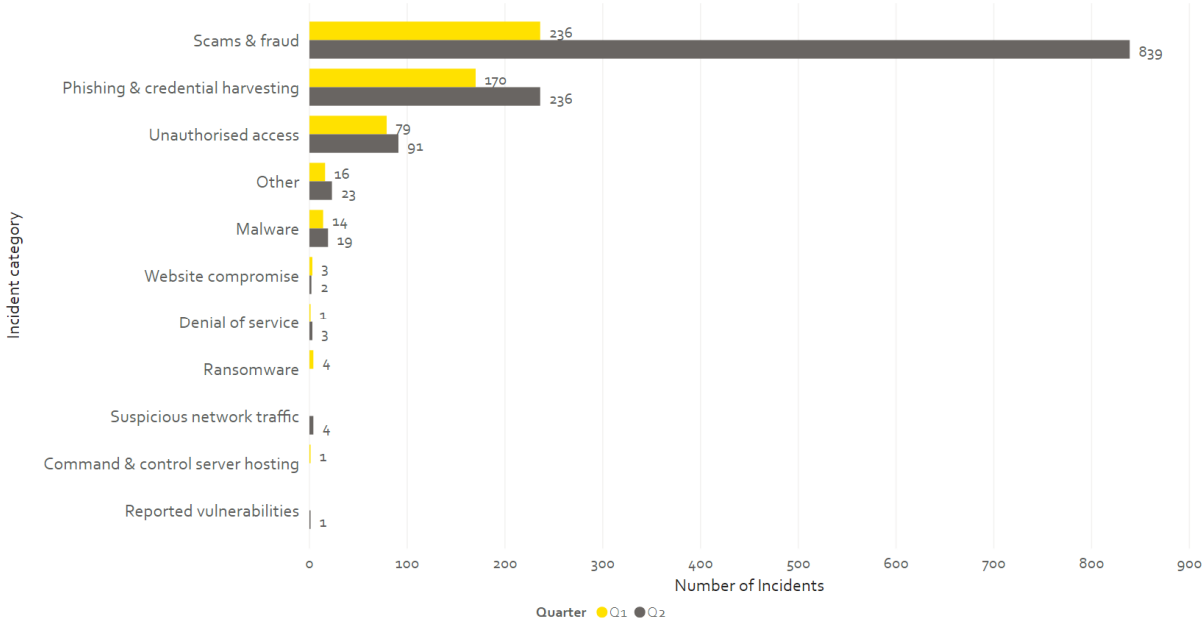


Breakdown of incidents affecting individuals

In Q1 and Q2, 1,742 reports (56%) were about incidents affecting individuals, a slight increase in proportion from Q4 2019 (50%).

Of particular note, is the significant increase in scams and fraud affecting individuals during Q2 (839), up 256% from Q1 (236). This increase is primarily driven by the increase in blackmail and extortion scams detailed above.

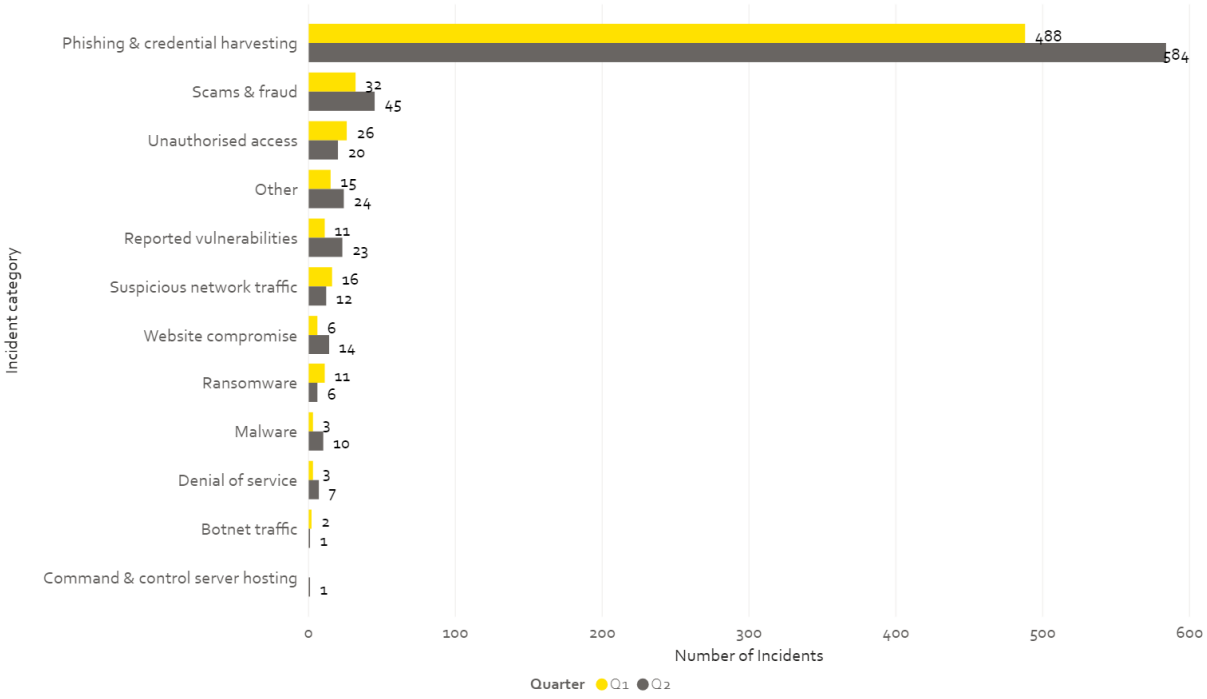
Figure 4: Breakdown of incidents affecting individuals



Breakdown of incidents affecting organisations

44% of reports (1,360) received in Q1 and Q2 were about incidents affecting organisations, compared with 50% (562) in Q4 2019. Phishing and credential harvesting continues to be the largest category of incidents reported to us by organisations – accounting for 79% of reports by organisations. This rose significantly in Q2, with a 20% increase in reports on Q1.

Figure 5: Breakdown of incidents affecting organisations

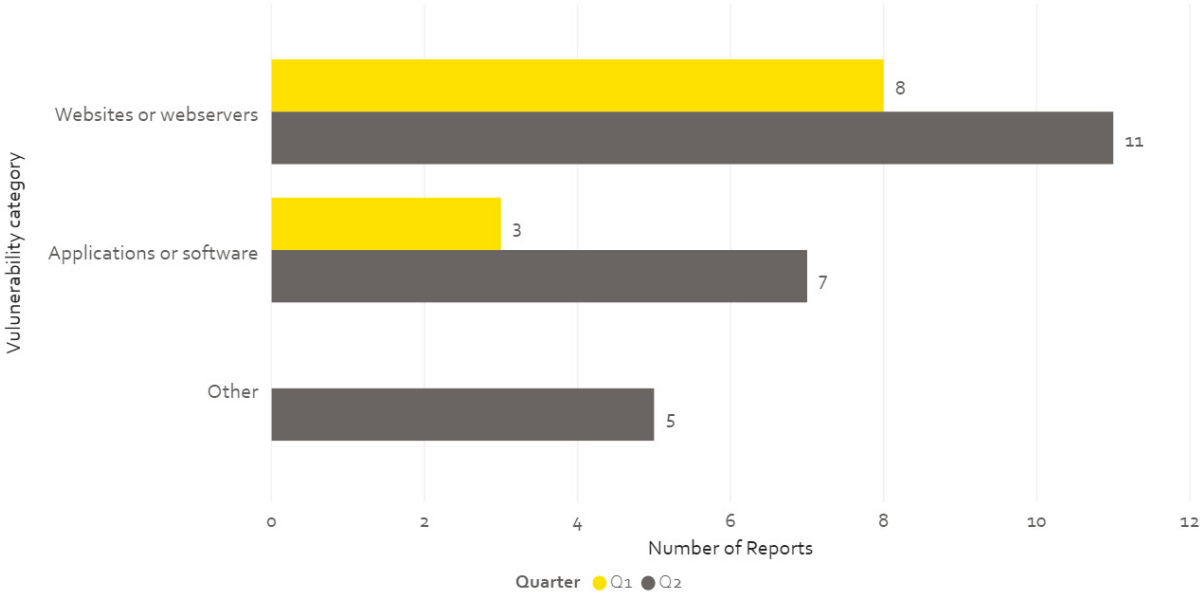


Breakdown of reported vulnerabilities

A vulnerability is a weakness in software, hardware or an online service that can be exploited to allow access to information or damage a system. Early discovery of vulnerabilities means they can be addressed to prevent future incidents.

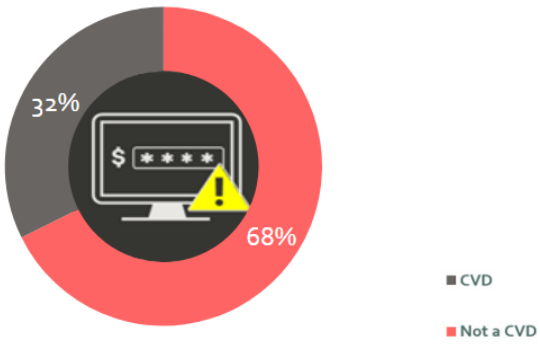
CERT NZ received 23 vulnerability reports in Q2, up from 11 in Q1.

Figure 6: Breakdown of reported vulnerabilities



Some vulnerability reports come under CERT NZ's Coordinated Vulnerability Disclosure (CVD) policy. This is used when the person reporting the vulnerability doesn't want, or has been unable, to contact the vendor directly themselves. CERT NZ received 11 vulnerability reports using the CVD policy1, making up 32% of the vulnerability reports received in Q1 and Q2 2020.

Figure 7: Proportion of coordinated vulnerability disclosures



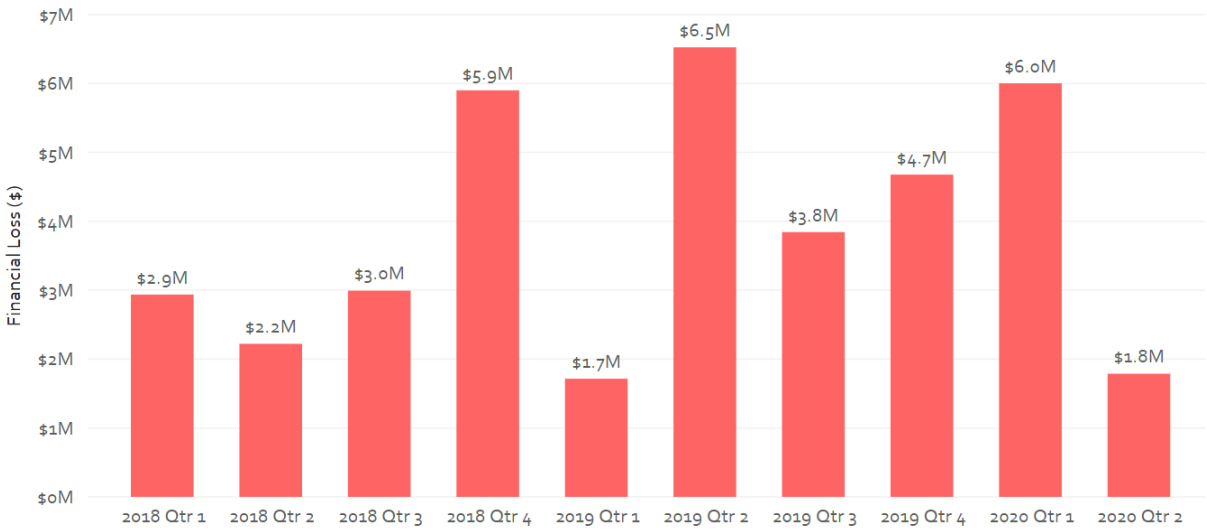
https://www.cert.govt.nz/it-specialists/guides/reporting-a-vulnerability/

4. Impacts

Direct financial loss

Direct financial losses totalled $7,791,174 during Q1 and Q2 2020. However, while incident volumes rose 73% in Q2, direct financial losses decreased 70%.

Figure 8: Direct financial losses per quarter



Distribution of direct financial losses

The difference in financial loss between reports affecting individuals and those affecting organisations was:

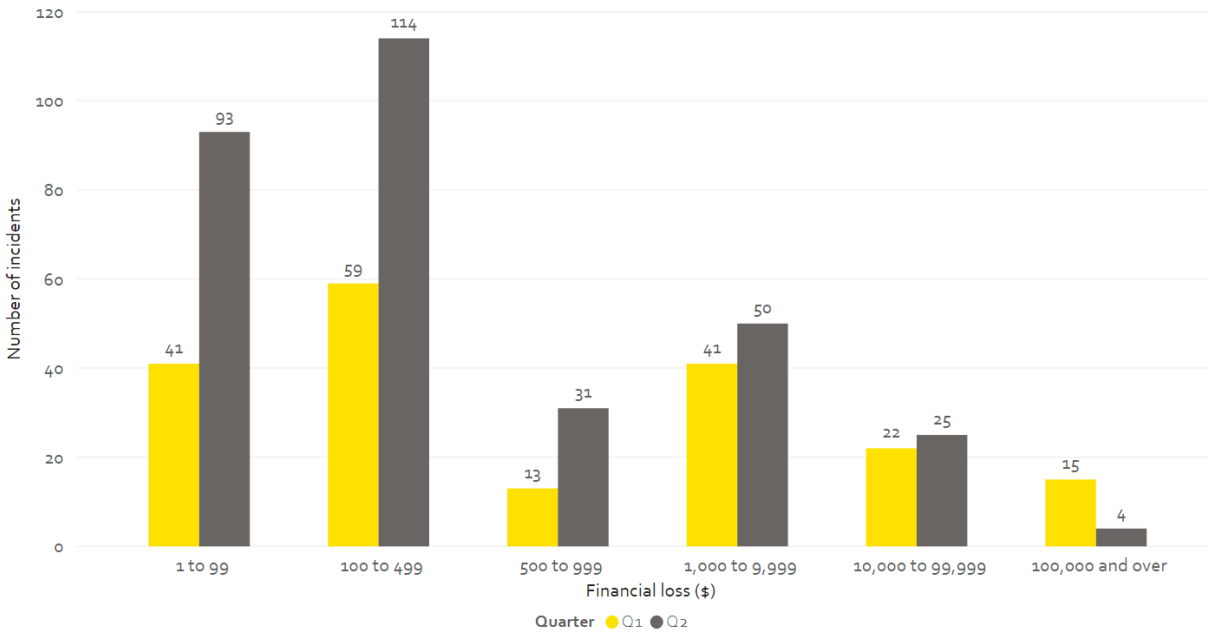
- 63 organisations reported financial losses during Q1 and Q2 2020
- 445 individuals reported financial losses during Q1 & Q2 2020.

19 incidents reported during Q1 and Q2 involved losses of $100,000 or more. Of these:

- 10 involved the unauthorised transfer of money, with each incident relating to the compromise of business email accounts
- 4 involved unauthorised access to accounts, including from 'sim swap' attacks detailed in Quarterly Report: Highlights Q4 2019.

The remaining five incidents resulting in significant financial loss concerned range of scam types, including cryptocurrency, investment, business opportunities and romance scams.

Figure 9: Distribution of direct financial losses



Types of loss

627 (20%) reports received in Q1 and Q2 2020 involved incidents where some type of loss (not only financial) occurred.

Of the 1,742 reports of incidents affecting individuals, 507 (29%) involved some type of loss. Of the 1,360 reports of incidents affecting organisations, 120 (9%) involved some type of loss.

Reported losses are broken down by type, as follows:

Table 2: Types of loss in Q1 and Q2 2020

16% **Financial loss**

This not only includes money lost as a direct result of the incident, but also includes the cost of recovery, like the cost of contracting IT security services or investing in new security systems following an incident

(Q4 2019: 15%).

1% **Reputational loss**

Damage to the reputation of an individual or organisation as a result of the incident

(Q4 2019: 1%).

3% **Data loss**

Loss or unauthorised copying of data, business records, personal records and intellectual property

(Q4 2019: 3%).

0% **Technical damage**

Impacts on services like email, phone systems or websites, resulting in disruption to a business or organisation

(Q4 2019: 0%).

1% **Operational impacts**

The time, staff and resources spent on recovering from an incident, taking people away from normal business operations

(Q4 2019: 1%).

1% **Other**

Includes types of loss not covered in the other categories

(Q4 2019: 3%).

5. Demographics

Reporting by sector

Reports from the finance and insurance sector accounted for 53% of the 1,360 reports about incidents affecting organisations. Of particular note, is the increased reporting from the technology sector, up 256% between Q1 (41) and Q2 (146). The increase was primarily made up of reports of phishing and credential harvesting incidents.

Figure 10: Reports by sector

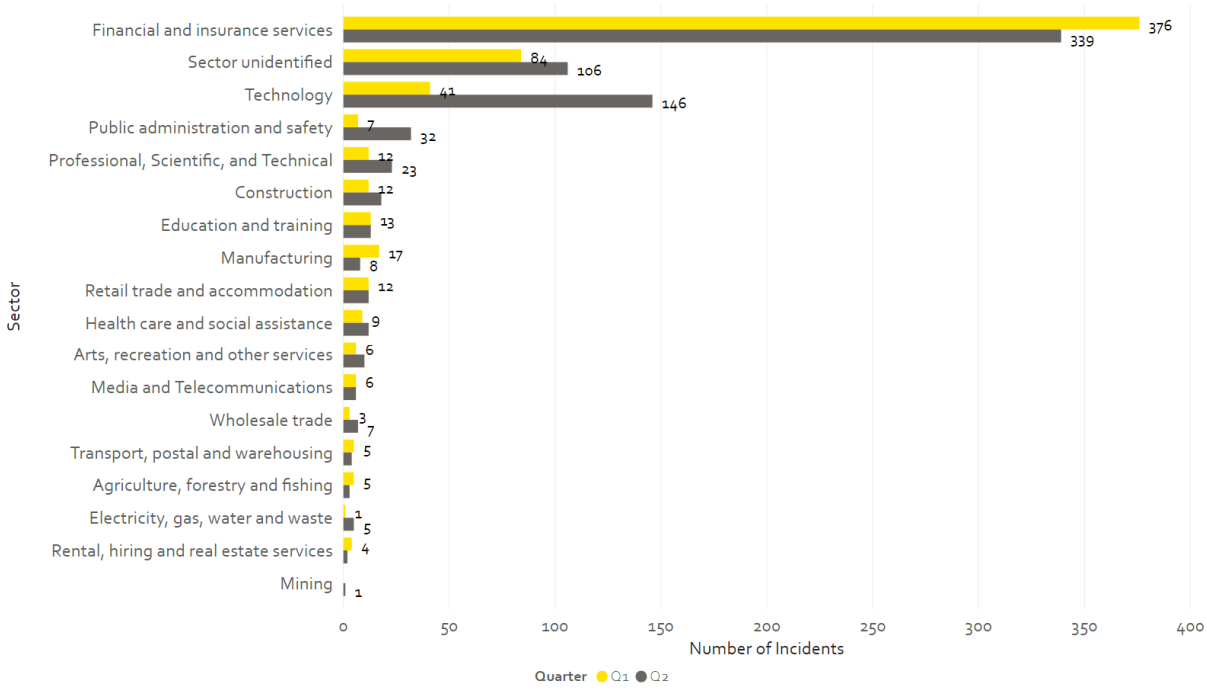
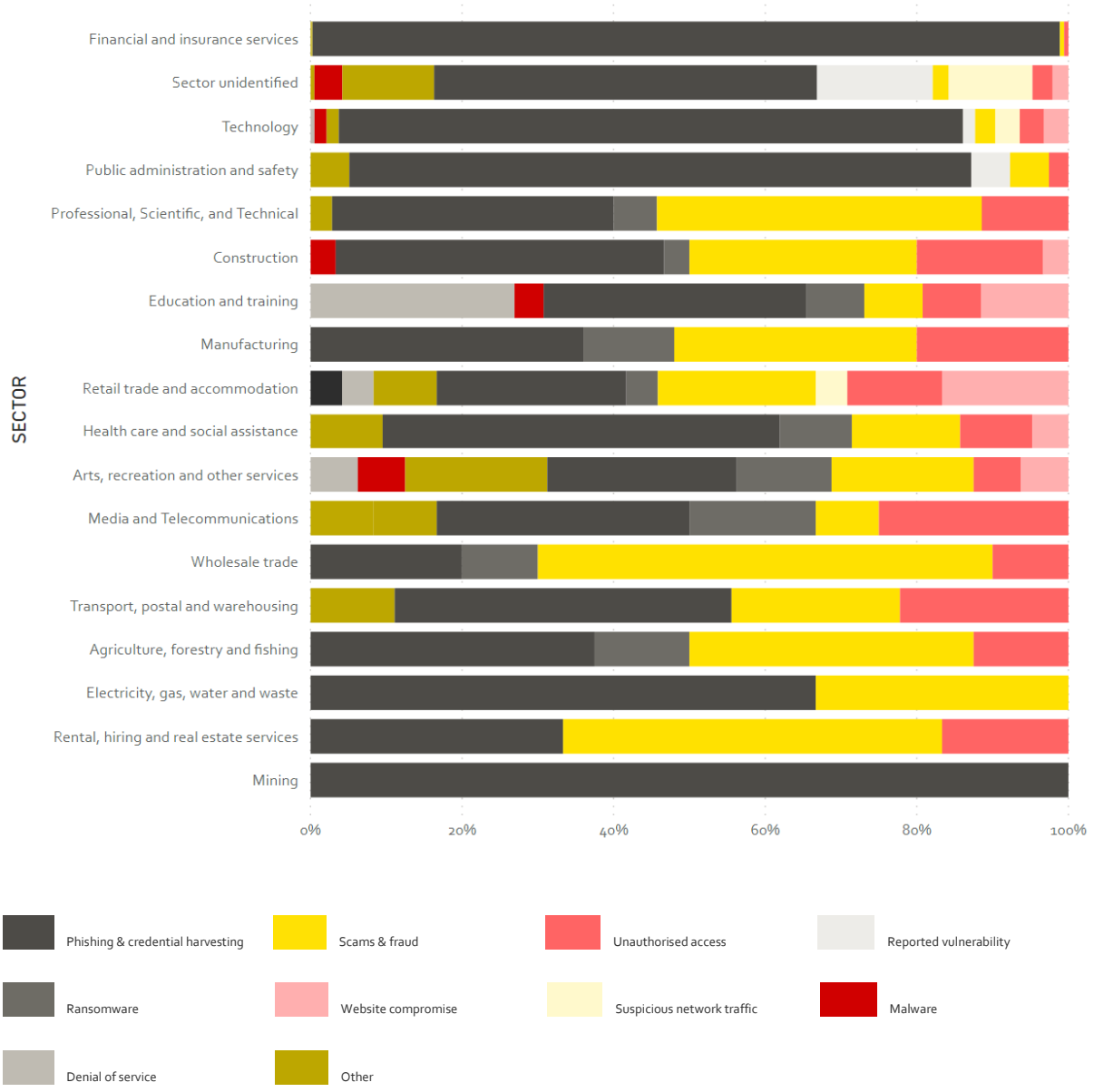


Figure 11: Breakdown by sector and incident category

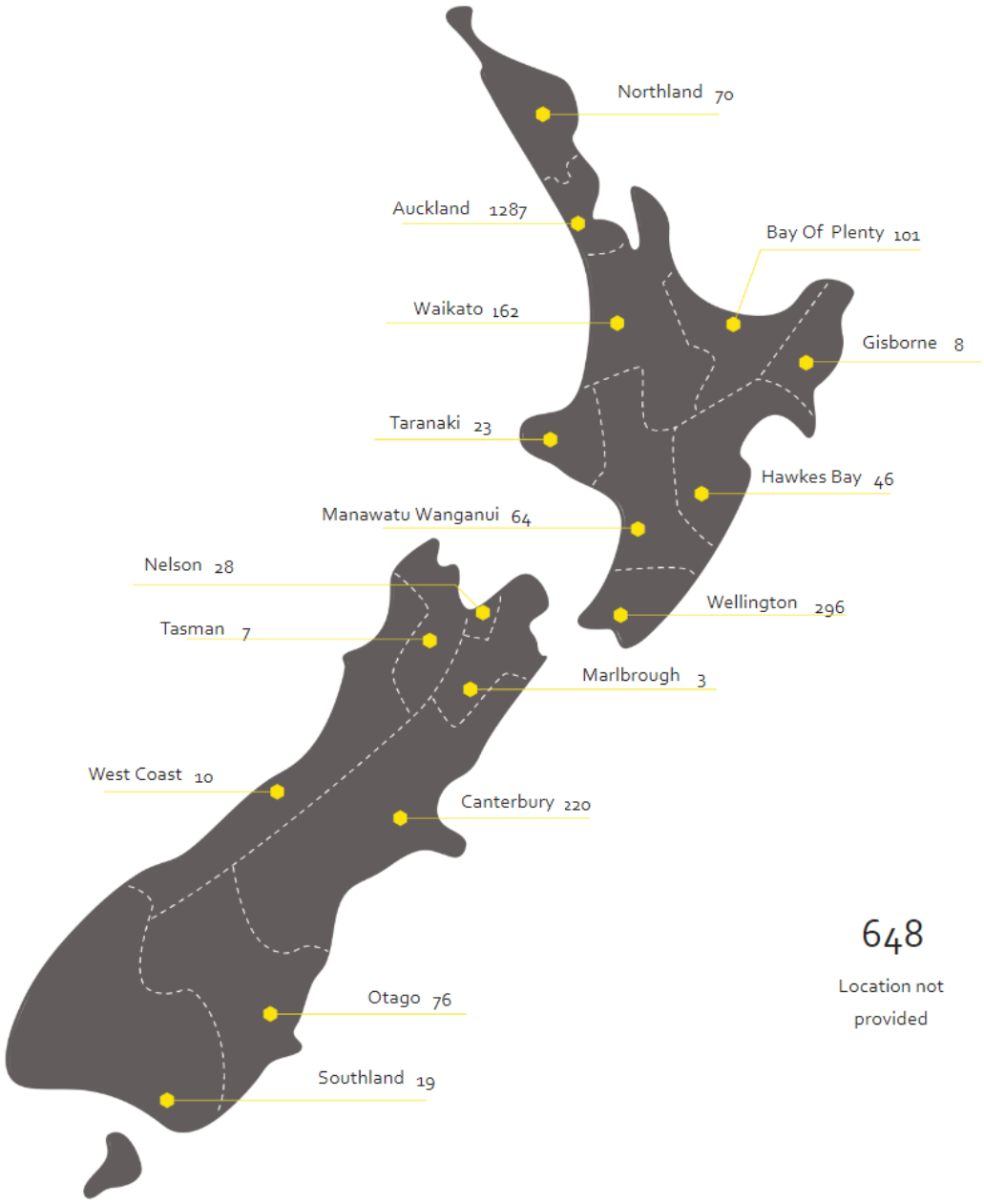
The largest number of reports came from the financial and insurance services sector, with 97% of their incidents relating to phishing and credential harvesting. The mining sector reported the fewest incidents – just one, concerning phishing and credential harvesting.



Reporting by region

Increases in incident volumes during Q2 were spread relatively evenly across all regions. The exception was Waikato, reporting a 226% increase in incidents between Q1 (38) and Q2 (124).

Figure 12: Breakdown of reports by region



Reporting by age

Of the 1,742 reports of incidents affecting individuals, 1,570 (90%) provided their date of birth.

Figure 13: Incidents affecting individuals – breakdown by age

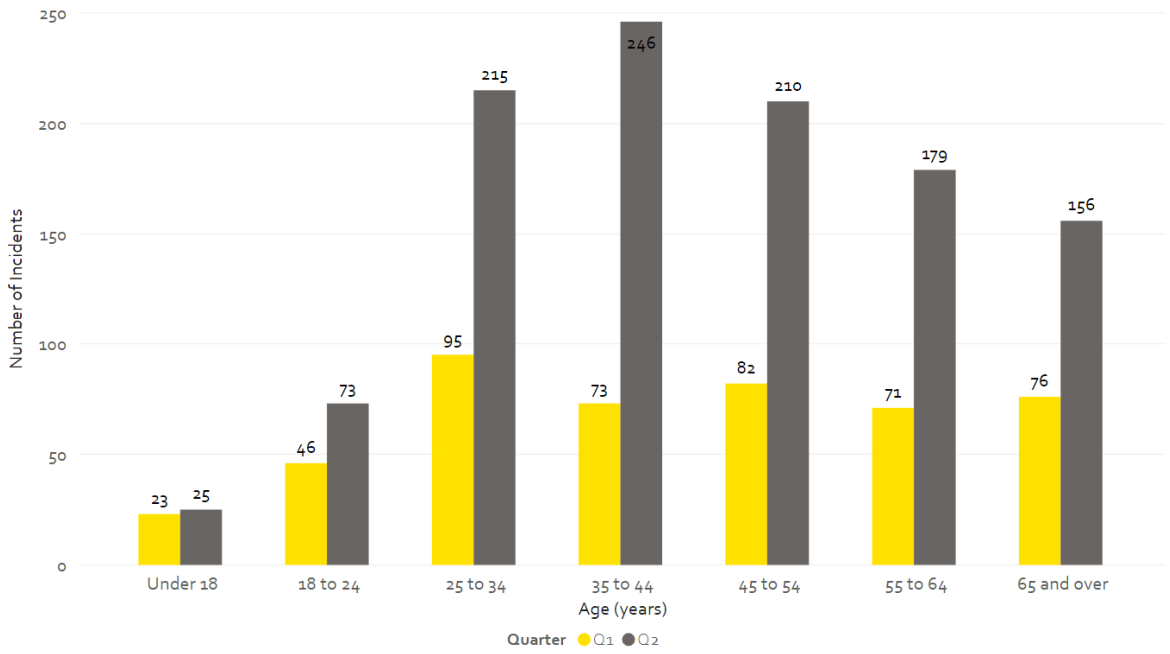
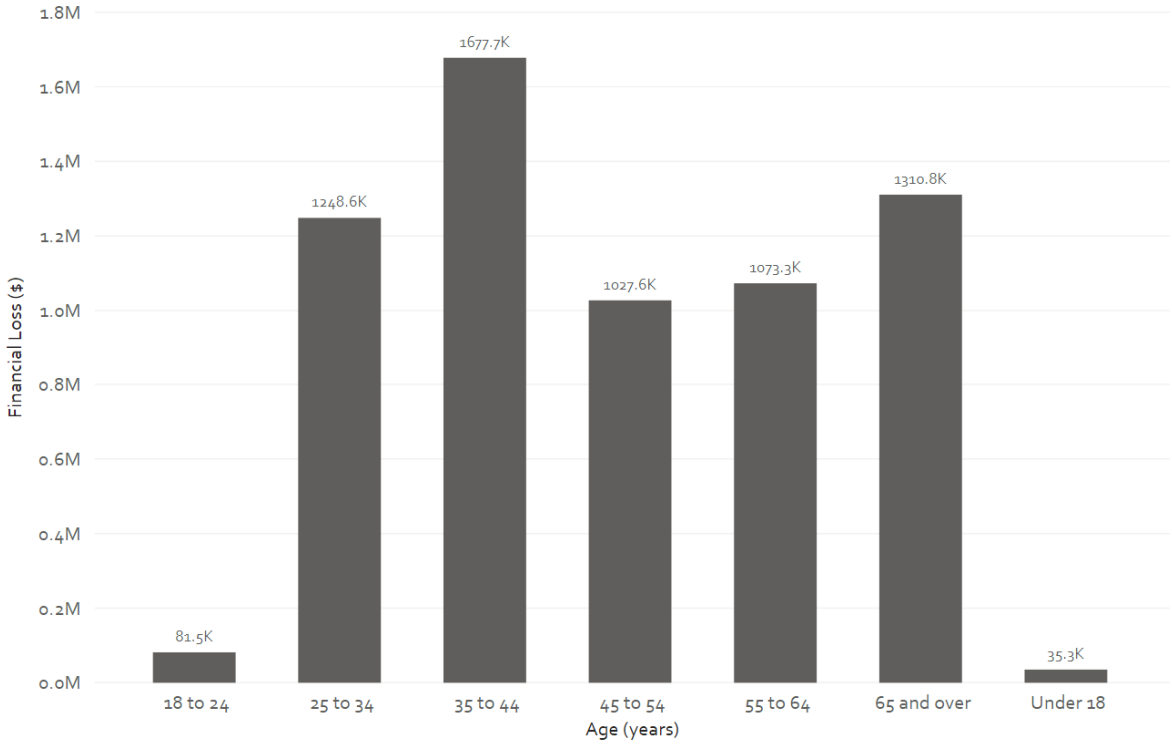


Figure 14: Distribution of direct financial losses reported by age



During Q1 and Q2 2020 there were 386 reports of incidents affecting individuals (rather than businesses), where the report included; a location in New Zealand, a date of birth and a loss amount.

Table 3: Distribution of direct financial losses reported by age

Under 18	18 - 24	25 -34	35 - 44	45 - 54	55 - 64	65 and over
$35,000	$82,000	$1,249,000	$1,678,000	$1,028,000	$1,073,000	$1,311,000

6. About CERT NZ

CERT NZ is New Zealand's Computer Emergency Response Team, and works to support businesses, organisations and individuals who are affected (or may be affected) by cyber security incidents. CERT NZ provides trusted and authoritative information and advice, while also collating a profile of the threat landscape in New Zealand. See www.cert.govt.nz for more information.

A word about our information

Reporting quarters are based on the calendar year, 1 January to 31 December.

This report covers Q1 and Q2 (1 January – 30 June) 2020.

Incidents are reported to CERT NZ by individuals and organisations. They choose how much or little information they are comfortable in providing, often about very sensitive incidents.

Sometimes CERT NZ may ask for additional information about an incident to gain a better understanding, or if we might need to do technical investigations. Before sharing specific details about an incident, CERT NZ will seek the reporting party's consent.

CERT NZ is not always able to verify the information we receive, though we endeavour to do so, particularly when dealing with significant cyber security incidents.

All information provided to CERT NZ is treated in accordance with our Privacy and Information Statement as published on our website, and this report is subject to the CERT NZ standard disclaimer.

The sectors we use are based on Stats NZ's New Zealand Industry Standard Industry Output Categories.

Our regional reporting uses the sixteen regions of the Local Government Act 1974.

Age is calculated from the date of birth provided and the date we received the incident report. The 'reporting by age' data does not include reported vulnerabilities, as those are from individuals proactively reporting issues, rather than having been affected by them.

Reporting an incident to CERT NZ

Anyone can report a cyber security incident to CERT NZ, from IT professionals and security personnel to members of the public, businesses, and government agencies. We also receive incident notifications from our international CERT counterparts when they identify affected New Zealand organisations in their investigations.

To report a cyber security incident, go to our website www.cert.govt.nz or call our freephone number 0800 CERT NZ (0800 2378 69). Your report will be received by an expert who can advise you on the best next steps to take.

With your permission, we may refer incidents to our partners such as the National Cyber Security Centre for national security threats, NZ Police for cybercrime, the Department of Internal Affairs for unsolicited electronic mail (spam), and Netsafe for cyberbullying.

Incident categories we use

We use broad categories to group incident reports. These will be refined as the data set grows.

The **incident** report categories are:

Botnet traffic. Botnets are networks of infected computers or devices that can be remotely controlled as a group without their owners' knowledge and are often used to perform malicious activities such as sending spam, or launching Distributed Denial of Service attacks.

C & C server hosting. A system used as a command-and-control point by a botnet.

Denial of Service (DoS).An attack on a service, network or system from a single source that floods it with so many requests that it becomes overwhelmed and either stops completely or operates at a significantly reduced rate. Assaults from multiple sources are referred to as Distributed Denial of Service attacks (DDoS).

Malware. Short for malicious software. Malware is designed to infiltrate, damage or obtain information from a computer system without the owner's consent. Commonly includes computer viruses, worms, Trojan horses, spyware and adware.

Phishing and credential harvesting. Types of email, text or website attacks designed to convince users they are genuine, when they are not. They often use social engineering techniques to convince users of their authenticity and trick people into giving up information, credentials or money.

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.

Reported vulnerabilities. Weaknesses or vulnerabilities in software, hardware or online service, which can be exploited to cause damage, or gain access, to information. Some are reported to CERT NZ under our Coordinated Vulnerability Disclosure (CVD) service.

Scams and fraud. Computer-enabled fraud that is designed to trick users into giving up money. This includes phone calls or internet pop-up advertisements designed to trick users into installing fake software on their computers.

Suspicious network traffic. Detected attempts to find insecure points or vulnerabilities in networks, infrastructure or computers. Attackers typically conduct a range of reconnaissance activities before conducting an attack, which are sometimes detected by security systems and can provide early warning for defenders.

Unauthorised access. Successful unauthorised access can enable an attacker to conduct a wide range of malicious activities on a network, infrastructure or computer. These activities generally fall under one of the three impact categories:

- compromise of the confidentiality of information
- improper modification affecting the integrity of a system
- degradation or denial of access or service affecting its availability.

Website compromise. The compromise, defacement or exploitation of websites by attackers for malicious purposes, such as spreading malware to unsuspecting website visitors.

Vulnerability categories we use

The **vulnerability** report categories we currently use are:

Applications or software. Vulnerabilities discovered in software products that could be exploited by a potential attacker. They are relatively common and, when discovered, are typically patched or mitigated through controls.

Authentication, authorisation and accounting. Common terminology for controlling access to computer resources, enforcing policies, auditing usage, and providing the information necessary to account for services. Vulnerabilities, if exploited to disrupt these functions, would have considerable impacts on the security of a network, system or device.

Human introduced. Vulnerabilities arising from human-introduced errors, misconfiguration or unintentional circumvention of security controls.

IoT devices. Internet of Things devices are internet-connected devices used to perform distributed functions over a network.

Mobile devices. Includes phones, handheld devices, hardware and mobile operating systems.

Networking. Covers vulnerabilities in network equipment, such as routers, gateways and firewalls, or the software and tools used to manage networks. This also includes vulnerabilities which may exist in routing, which could expose network traffic to compromise.

Operating systems or platforms. Low level software which provides, or supports, the basic operating environment of a computer.

PCs and laptops. Desktop and laptop computer hardware.

Printers, webcams and other peripherals. Hardware components used to support PC or laptop functions.

Servers (other than websites). Other kinds of enterprise servers organisations would typically use, such as mail, application and proxy servers. Vulnerabilities can be found in the hardware or firmware, and can also arise from misconfiguration or failures in security management.

Websites or webservers. Includes vulnerabilities in websites themselves, or the infrastructure they run on. An example would be unpatched websites or webservers which would potentially give an attacker the ability to compromise a website.

Malware categories we use

Hare some of the key terms we use 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 being tricked into being run by a user.

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.

Adware – malicious software that infects computers in order to designed to display advertisements, redirect search requests to advertising websites, harvest marketing-type data about the user or even stealthily browse to and click through web advertising without the users knowledge to artificially increase clicks and generate advertising revenue.

Spyware – as its name suggests, is designed to spy on what a user is doing. Hiding in the background on a computer, this type of malware will collect information without the user knowing, such as credit card details, passwords and other sensitive information.

Botnet – a group of malware infected computers able to be controlled remotely by an attacker as a group and at scale.

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.

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.

Web shell - a web shell is able to be uploaded to a web server to allow remote access to the web server, including the web server's file system. This can enable an attacker to gain remote access to a computer system via the internet, allowing the web shell to act as a remote access Trojan.

Keylogger - a programme that records users' keyboard inputs without their knowledge, often to steal credentials like passwords.