certnz

Quarterly Report

Q3

1 July - 30 September

2017

newzealand.govt.nz

Executive summary ///

Welcome to CERT NZ's Quarter Three (Q3) Report for 1 July – 30 September 2017. This report provides a snapshot of the types of cyber security threats and incidents that have been reported, and an update on our work to protect New Zealanders online.

Analysis of our data shows:

- Over half of all incidents reported were from individuals from technical and non-technical backgrounds.
- The highest volumes of incidents reported were from organisations in the technology, public administration and safety, retail, trade and accommodation, and financial and insurance services sectors.
- Targeted invoice scams are on the rise.
- A number of new threats have come onto the scene, such as the BlueBorne vulnerability, which can affect devices that use Bluetooth.
- 29% of incidents reported experienced some form of loss.
- The value of the financial losses attributed to incidents in this period is $1,179,259 – up from $731,813 in the previous quarter.

This quarter there has been a similar spread of incidents to the Q2 report, with three noticeable trends:

- A large number of reports were from businesses affected by invoice scams. We have continued to work with Netsafe and NZ Police to understand the types of scams and fraud being reported.
- There was a noticeable drop in the number of ransomware cases being reported in Q3, following the global ransomware events in Q2.
- There was also a number of vulnerabilities reported to CERT NZ. Our new coordinated vulnerability disclosure service (CVD) strengthens New Zealand's defence by enabling researchers and analysts to report them to a neutral third party, CERT NZ, who then works with the affected organisations to get them fixed.

> " The value of the financial losses attributed to incidents in this period is **$1,179,259** – up from $731,813 in the previous quarter. "

Director's message ///

Since CERT NZ's launch in April 2017 (Q2), we have been building our unique data set. We've used that to identify important stories and information that we can share widely so that all New Zealanders can be protected from online threats and confidently participate in the digital economy.

In Q3, we used our data to identify effective controls – things people can use, change or avoid for better cyber security. If implemented, these could significantly reduce the prevalence and impact of incidents on our people and businesses. To this end, CERT NZ has launched two new initiatives in November.

The first is Cyber Smart Week[1] , delivered in partnership with Connect Smart. This mobilised partners across the public and private sectors to encourage Kiwis to do just one thing to protect themselves.

Cyber Smart Week ran from 27 November – 1 December 2017 and focused on four simple steps to help people keep their data safe.

The second is CERT NZ's Critical Controls 2018[2], which summarises the ten controls that would mitigate or contain most of the information security incidents reported to us. The controls are designed to give organisations greater certainty about what to focus their time, effort and money on.

The controls are based on the research and incidents we've seen to date as well as other sources we have access to through the global CERT network and international data feeds.

We launched these initiatives because the data tells us that the best way to protect individuals and organisations is to show people how to do the basics well. The most effective steps are simple and easy to do, but require a little effort. International evidence[3] shows that 85% of cyber security incidents can be prevented by simple measures, like updating your operating system.

Rob Pope
Director, CERT NZ

About CERT NZ ///

CERT NZ is a specialist cyber security unit and part of the Ministry of Business, Innovation and Employment (MBIE). We gather information on cyber threats and incidents in New Zealand and overseas, and advise organisations of all sizes and the public on how to avoid and manage cyber security risks.

If any individual or organisation needs to report a cyber security problem, we are a first port of call via www.cert.govt.nz or through 0800 CERT NZ. Our team of cyber security experts will look into the incident, provide advice, and, if necessary, refer it to another agency such as NZ Police or Netsafe with the customer's consent.

CERT NZ also works with other government agencies to refer and respond to cyber security threats where appropriate, including the Department of Internal Affairs and the National Cyber Security Centre.

We report on threats by analysing international incidents and trends, track and analyse local data, co-ordinate multi-agency responses to cyber threats and incidents, and generally raise awareness of cyber security best practices in New Zealand.

[1] www.cert.govt.nz/cybersmart
[2] www.cert.govt.nz/it-specialists/guides/10-critical-controls/
[3] Canadian Cyber Incident Response Centre (CCIRC)

Results ///

Between 1 July and 30 September, **390** incidents were reported to CERT NZ, up from the previous quarter which saw 364 incidents reported.

Breakdown by responding organisation

390 **incident reports received**

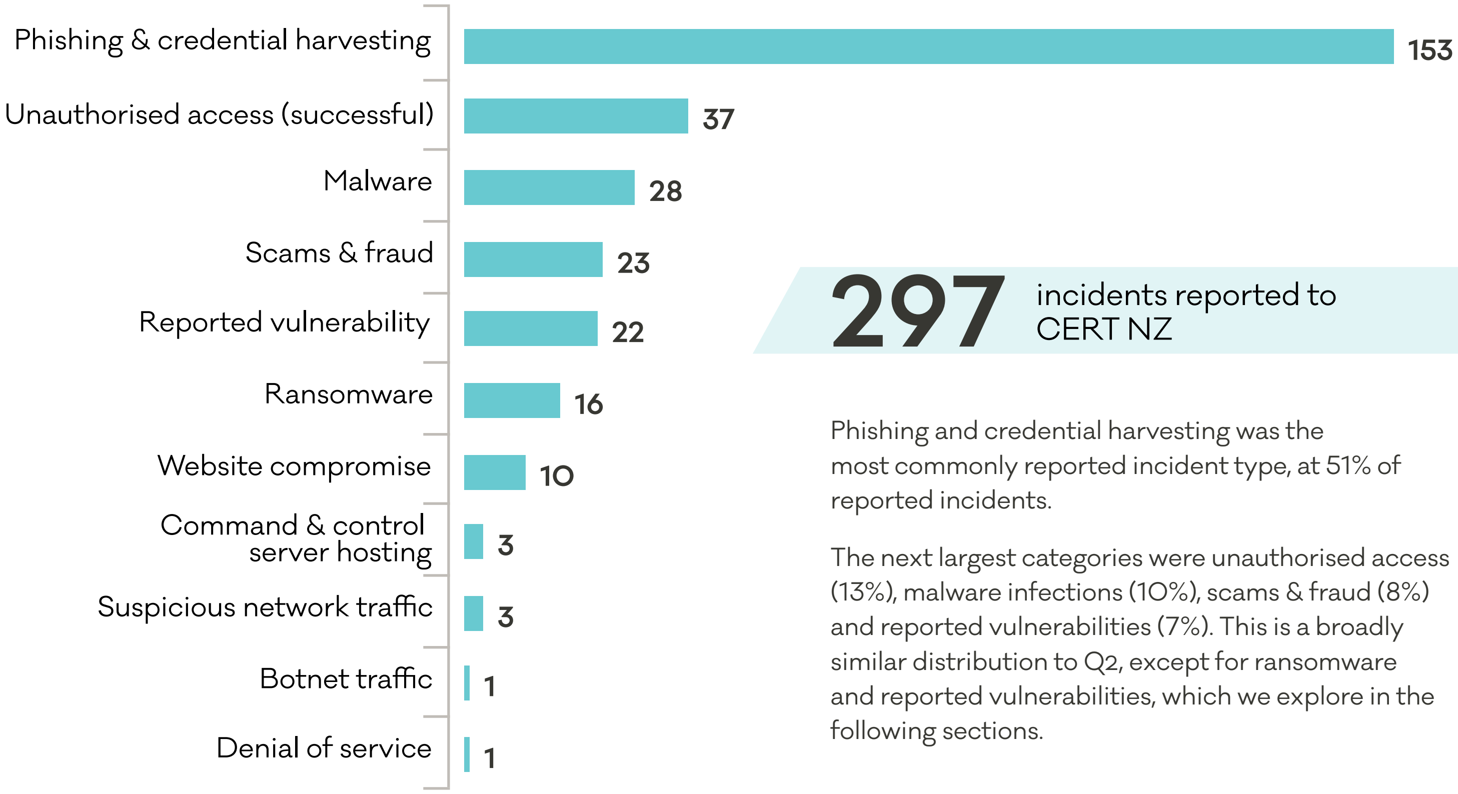
297
reports responded to directly by **CERT NZ**

78
reports referred to **NZ Police**

15
reports referred to **Netsafe.**

We have categorised incidents by type, region and sector to help us understand patterns and prevalence. Incidents reported for this quarter were slightly higher than the previous quarter, with a similar proportion of referrals to NZ Police and Netsafe.

Breakdown by category: incidents CERT NZ responded to directly

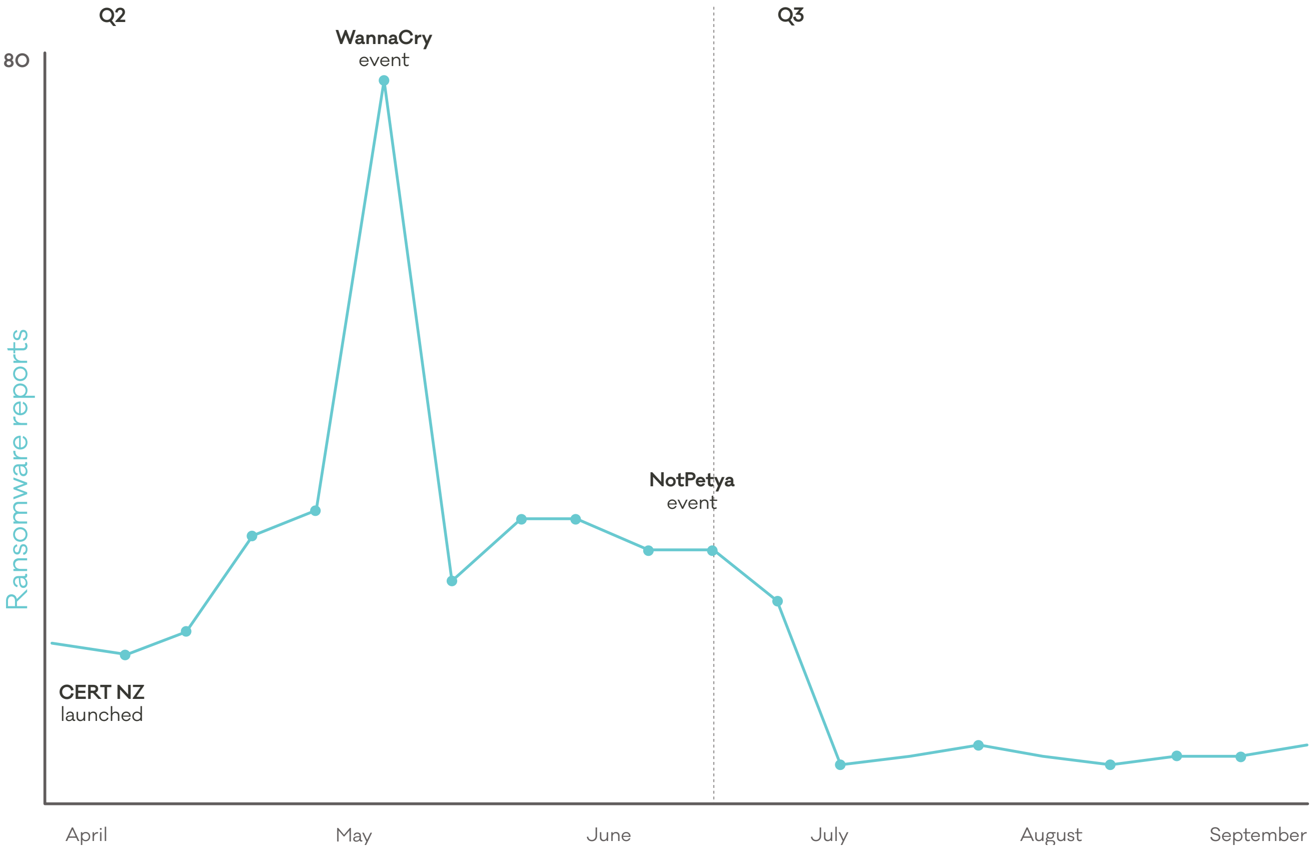


297 incidents reported to CERT NZ

Phishing and credential harvesting was the most commonly reported incident type, at 51% of reported incidents.

The next largest categories were unauthorised access (13%), malware infections (10%), scams & fraud (8%) and reported vulnerabilities (7%). This is a broadly similar distribution to Q2, except for ransomware and reported vulnerabilities, which we explore in the following sections.

Ransomware threats less prevalent



Ransomware reports have decreased considerably in Q3 to 5% (from 12% in Q2). This chart shows the spike in ransomware reports in Q2 surrounding the WannaCry and NotPetya events, and the subsequent decline of reports in Q3.

This trend may be the result of heightened awareness and improved controls in response to ransomware threats, but could also be the result of recent international law enforcement efforts to disrupt some of the dark web market places[4] where ransomware variant 'kits' are often traded.

The main ransomware variants reported were Cryptolocker and Locky.

Case study - Who's paying?

CERT NZ received a report from a New Zealand organisation that sends out regular invoices.

They had discovered that Mandarin-speaking scammers were contacting NZ-based Mandarin speakers via the WeChat messaging app. The scammers were offering to pay 100% of their NZ bills, in return for 60 – 80% of the cost of the bill being sent to the scammers.

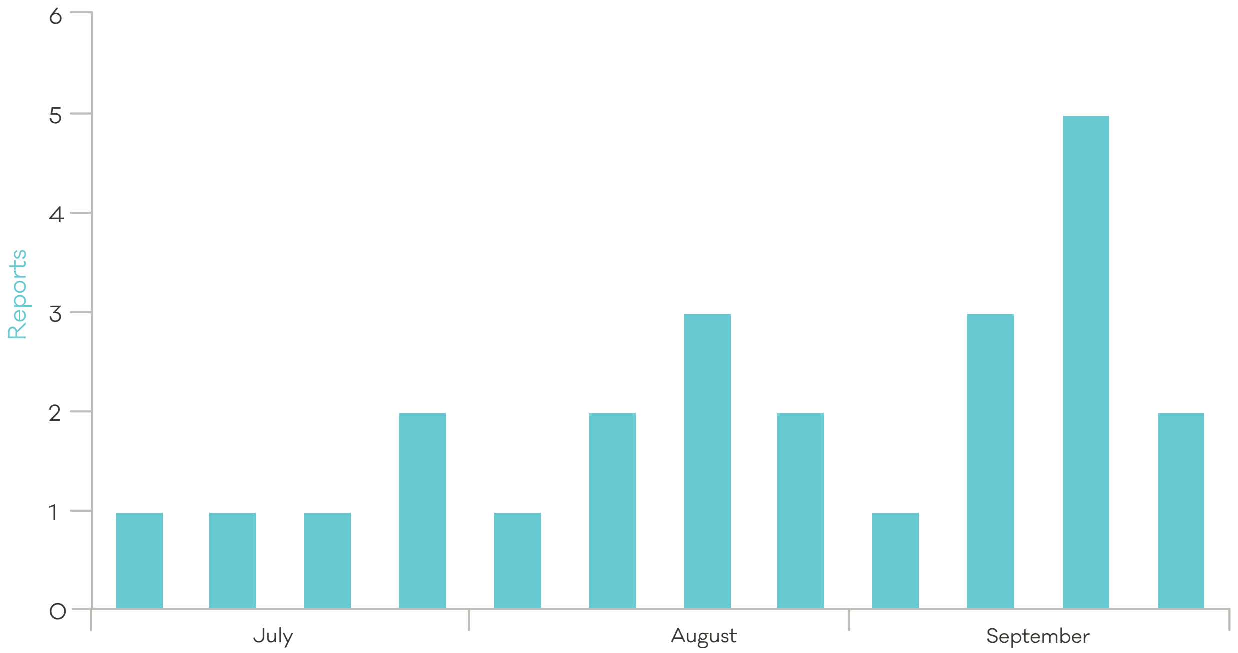
In turn, the scammers were apparently paying the bills in their entirety, but from suspected stolen credit cards. CERT NZ received reports that these scammers had offered to pay bills from at least four New Zealand companies, and there may be more. The case was referred to the NZ Police for further investigation.

[4] https://www.justice.gov/opa/pr/alphabay-largest-online-dark-market-shut-down
https://www.europol.europa.eu/newsroom/news/massive-blow-to-criminal-dark-web-activities-after-globally-coordinated-operation

Preventing incidents before they happen – reporting vulnerabilities

Reported vulnerabilities is a new category in Q3. This follows the launch of CERT NZ's coordinated vulnerability disclosure service (CVD)[5] in July 2017. A vulnerability is a weakness in software, hardware, or an online service that can be exploited to access information or damage a system.

These reports represent 7% of the total number of incidents reported, with the number increasing steadily since the service launched.



The vulnerabilities reported to CERT NZ have ranged in severity and complexity, and each case is a chance to prevent a cyber security incident before it occurs.

For example, a security researcher discovers vulnerabilities in software that could be exploited by an attacker. The researcher wishes to remain anonymous and does not want to contact the vendor directly, but wants to ensure the issue is resolved. By offering a CVD service, CERT NZ acts as an intermediary, coordinating with the researcher and the vendor to get the vulnerability fixed.

Coordinated vulnerability disclosure balances the needs of the public with the needs of the vendor. More information about CERT NZs CVD service can be found on www.cert.govt.nz.

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.

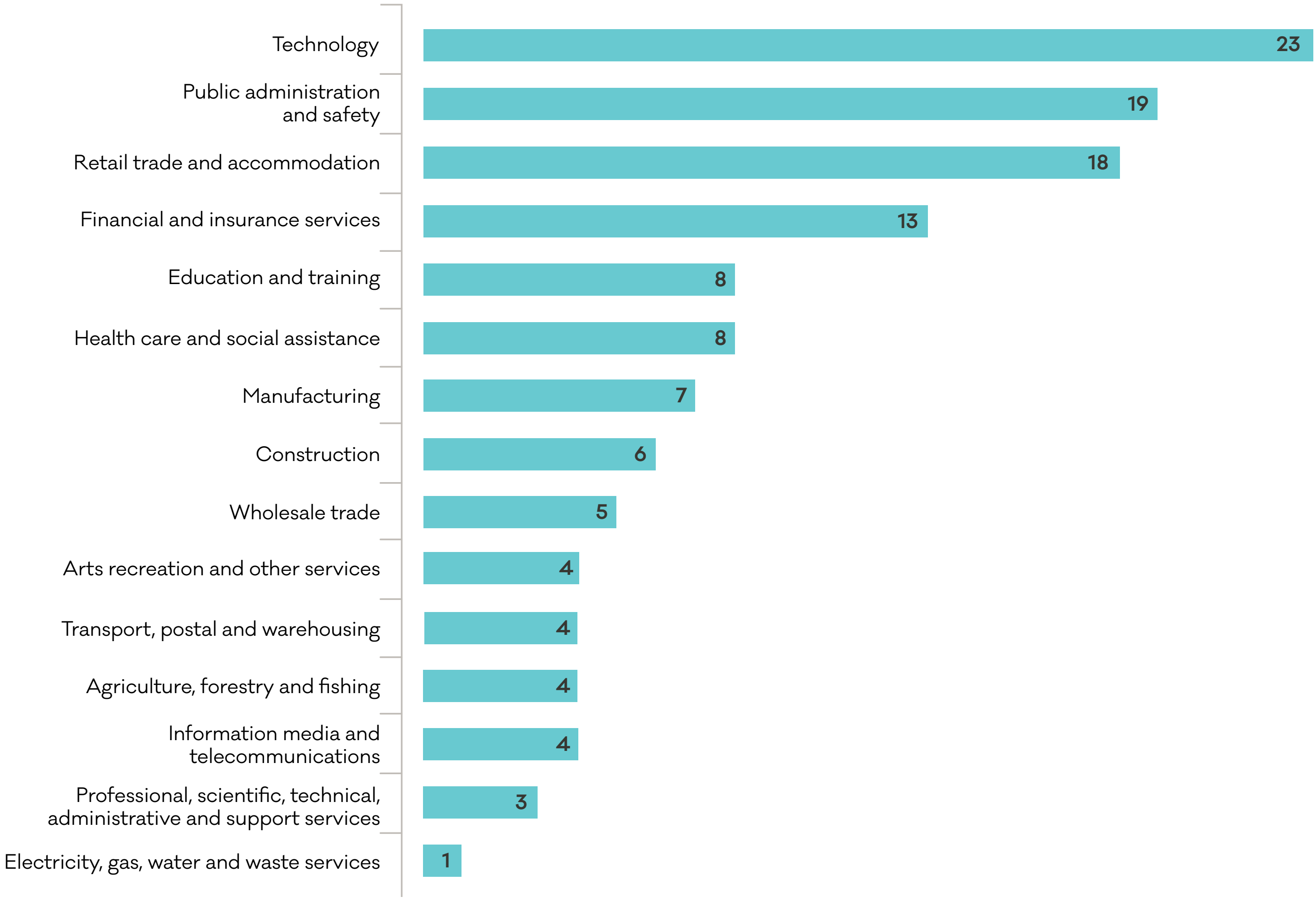
[5] https://www.cert.govt.nz/it-specialists/guides/reporting-a-vulnerability/

Reporting by sector

This quarter we have introduced baseline data on sectors using the New Zealand Standard Industry Output Categories (NZSIOC).

Reports about individuals accounted for 57% of all incidents.

The remaining 43% were about organisations. The four largest sectors were technology (8%), public administration and safety (6%), retail trade and accommodation (6%), and financial and insurance services (4%).

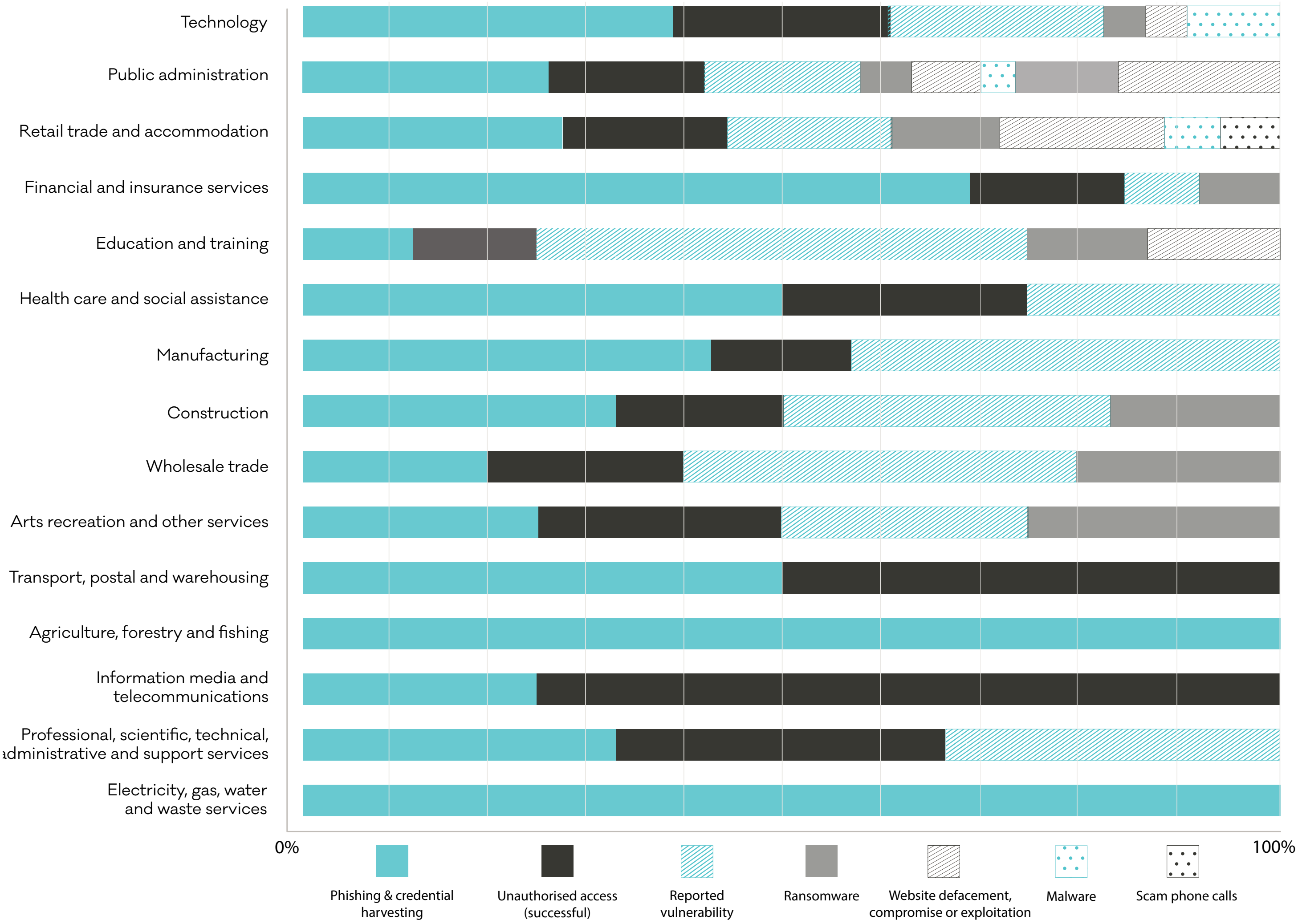


Case study - Invoice scam costs company over $300,000

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 their invoices, 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.

Reporting by sector: Incident breakdown

The graph shows incident breakdown by sector.



The highest proportion of incidents reported by organisations are:

38%
phishing and credential harvesting

17%
unauthorised access

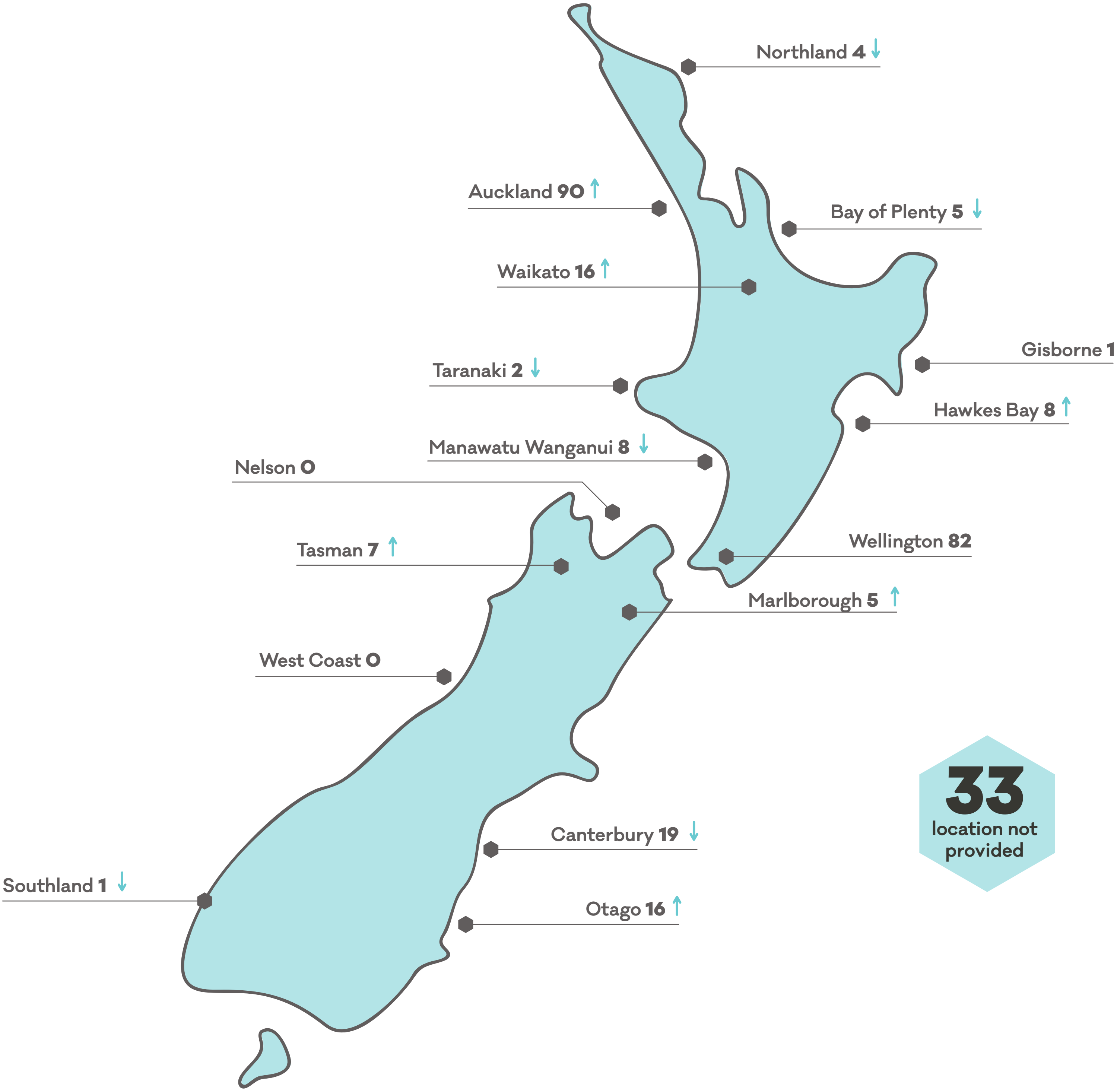
8%
ransomware

7%
website compromise

There have been a number of phishing campaigns targeting businesses and their customers, most visibly the rise of invoice scam campaigns, which we cover later in this report.

Reporting by region

Our data captures the regions that people are reporting incidents from. Auckland had the highest percentage of incident reports at **30%**, followed by Wellington with **27%**. Respondents who didn't provide a location remained the third largest category at **11%** (down from 15% in Q2). As the number of reports grows over time, more identifiable trends may be observed.



Impacts ///

Over $1.1 million

in direct financial loss has been reported to CERT NZ in Q3.

We are continuing to build a picture of how cyber security incidents affect New Zealand, including the negative impacts that individuals and businesses can experience.

These impacts can range from damage to business operations, damage to personal reputation, and loss of data, records and intellectual property. These impacts are self-reported and are not verified. Impacts analysed in this section include all reports to CERT NZ, including those referred to NZ Police and Netsafe.

Losses from incidents reported via CERT NZ

29% of incidents reported some form of loss. This is consistent with Q2 (28%).

Financial loss is up considerably to 13% (from 5% in Q2). This is reflected in the reported losses totalling $1,179,259 in Q3. This is greater than the reported losses in Q2 ($731,813). **The combined loss in Q2 and Q3 is $1,911,072.**

Losses experienced are broken down by type as follows:

13%	**Financial loss:** The direct financial costs of an incident. This could be money lost as a result of an incident, but can also include the costs of recovering, such as needing to contract IT security services or investing in new security systems after an incident.
5%	**Data loss:** Loss or unauthorised copying of data, business records, personal records and intellectual property.
3%	**Operational impacts:** The time, staff and resources that need to be spent on recovering from an incident, taking people away from normal business operations.
2%	**Reputational loss:** Damage to the reputation of an individual, business or organisation as a result of being the victim of an incident.
2%	**Technical damage:** Impacts on services like email, phone systems or websites, resulting in disruption to a business or organisation.
7%	**Other:** Includes specific types of loss not covered in the other categories.

Note: Some reports may include multiple types of loss.

Case study - Scammers target professional services provider

A small accountancy firm contacted CERT NZ after an attacker gained unauthorised access to their email server through a phishing email. Once the attacker got in, they e-mailed the business' customers, pretending they were the firm and seeking payment to the scammers account.

It was discovered after a number of customers unfortunately paid the invoices, losing money. The business experienced considerable reputational damage as a result of the incident.

Focus on scams & fraud ///

Scams & fraud can be categorised as a single incident in itself or part of a wider attack.

This section focuses on all of the incidents that have a scams & fraud component, including the 23 direct scams & fraud incidents reported earlier in the results section.

We have combined reporting data with Netsafe to provide a more complete picture of scams & fraud in New Zealand.

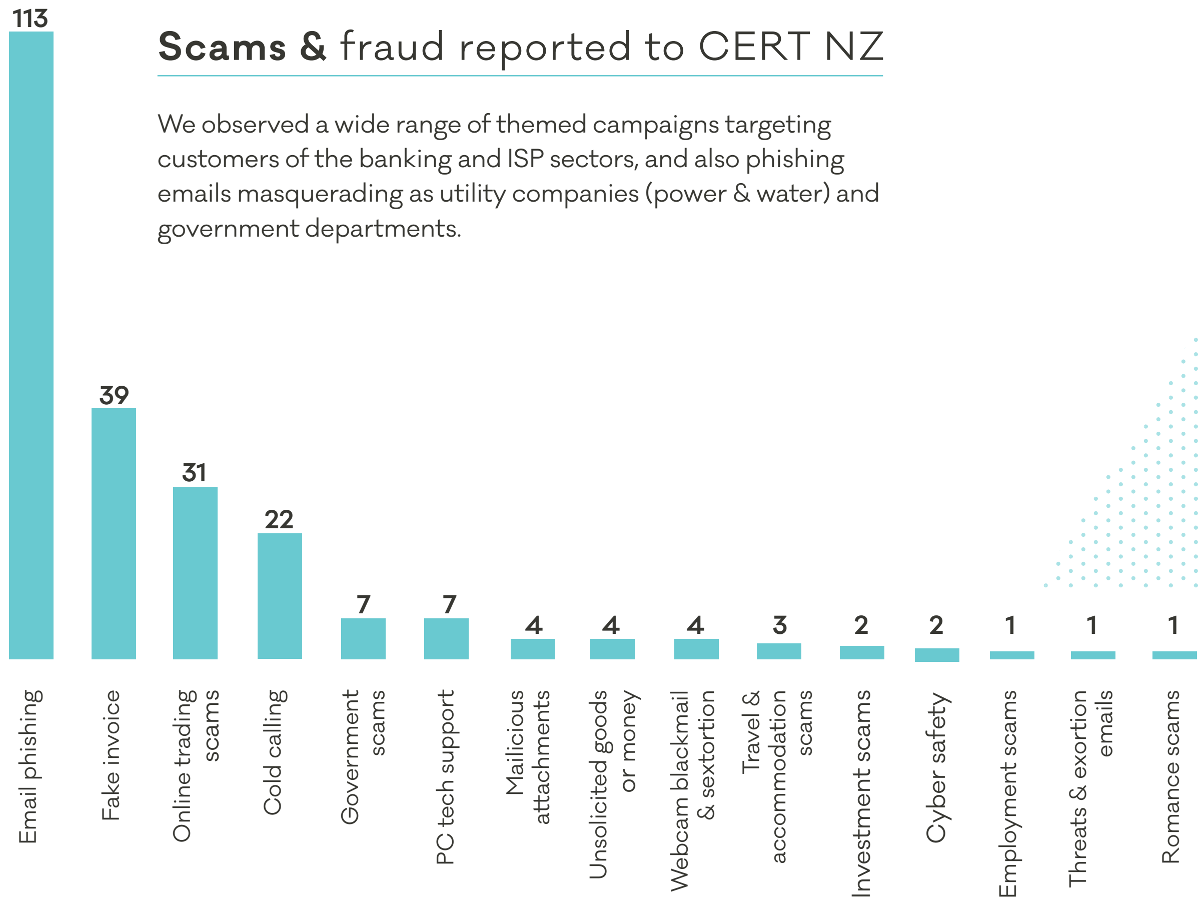
2619 scams & fraud reports were received by CERT NZ and Netsafe resulting in over **$2.1 million** financial loss.

	Scam & fraud reports	% involving loss	Reported losses
CERT NZ	242	14%	$585,987
Netsafe	2377	9%	$1,557,493
Total	**2619**	**9%**	**$2,143,480**

This may include some duplicate reports made to both organisations. CERT NZ and Netsafe are working together to align our reporting categories for scams & fraud to create a better picture of the landscape.

Scams & fraud reported to CERT NZ

We observed a wide range of themed campaigns targeting customers of the banking and ISP sectors, and also phishing emails masquerading as utility companies (power & water) and government departments.



Fake invoice scams

Targeted invoice scams are on the rise. Invoice scams were identified in 39 (16%) 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 contact 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 use phishing techniques to gain access to businesses email addresses, making the fake invoices much harder to detect.

We have had several reports from businesses with overseas suppliers, who have received fake copies of the suppliers invoices. They have also reported that in some cases their suppliers were compromised by attackers, who altered invoices by changing the bank account number from them in order to steal money from legitimate transactions.

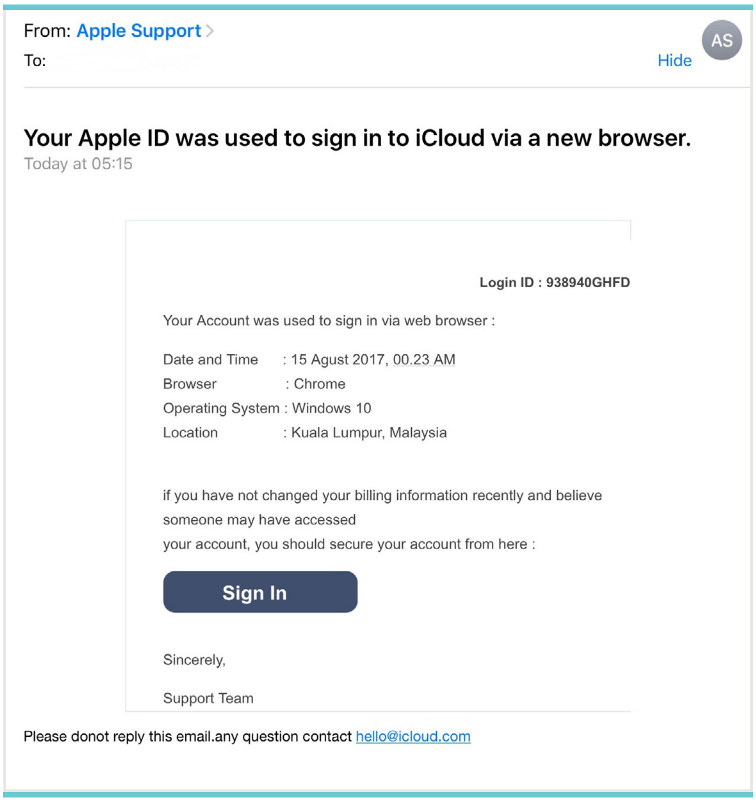
There are a number of excellent resources available to help protect yourself or your business from invoice scams:

Is this a scam?[6]

Identifying and preventing business email compromise[7]

Protecting your business from spear phishing and whaling[8]

Examples of recent phishing emails



From: Apple Support
To: [redacted]

Your Apple ID was used to sign in to iCloud via a new browser.
Today at 05:15

Login ID : 938940GHFD

Your Account was used to sign in via web browser :

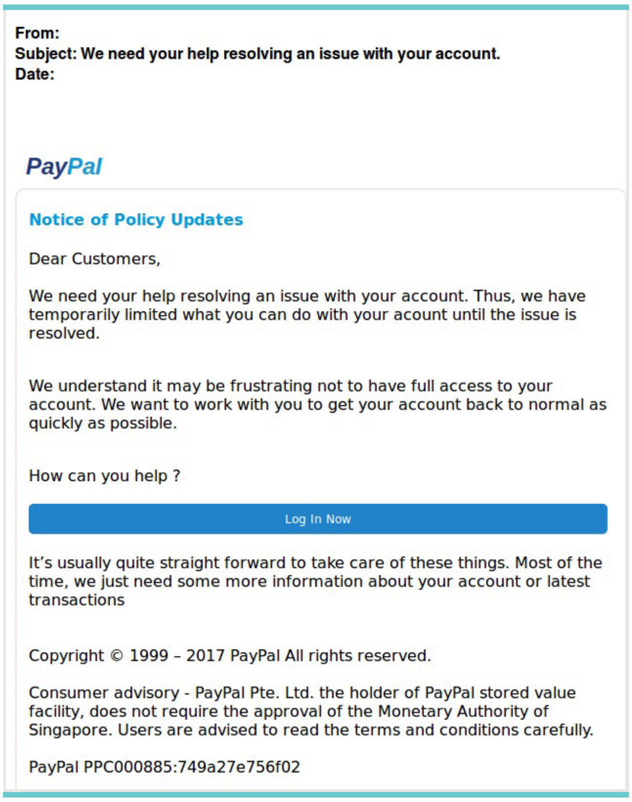
Date and Time : 15 Agust 2017, 00.23 AM
Browser : Chrome
Operating System : Windows 10
Location : Kuala Lumpur, Malaysia

if you have not changed your billing information recently and believe someone may have accessed
your account, you should secure your account from here :

Sincerely,

Support Team

Please donot reply this email.any question contact hello@icloud.com



From:
Subject: We need your help resolving an issue with your account.
Date:

Notice of Policy Updates

Dear Customers,

We need your help resolving an issue with your account. Thus, we have temporarily limited what you can do with your acount until the issue is resolved.

We understand it may be frustrating not to have full access to your account. We want to work with you to get your account back to normal as quickly as possible.

How can you help ?

It's usually quite straight forward to take care of these things. Most of the time, we just need some more information about your account or latest transactions

Copyright © 1999 – 2017 PayPal All rights reserved.

Consumer advisory - PayPal Pte. Ltd. the holder of PayPal stored value facility, does not require the approval of the Monetary Authority of Singapore. Users are advised to read the terms and conditions carefully.

PayPal PPC000885:749a27e756f02

[6] https://www.consumerprotection.govt.nz/get-guidance/scamwatch/identify-a-scam/is-this-a-scam/
[7] https://www.netsafe.org.nz/identifying-and-preventing-business-email-compromise/
[8] https://www.cert.govt.nz/businesses-and-individuals/guides/cyber-security-your-business/protecting-your-business-from-spear-phishing-and-whaling/

Office 365 phishing campaign

We had a number of reports in Q3 from people who had received emails claiming that someone wanted to share a large file or photos, and provided a link to log in and download the file.

Clicking on the link would take the recipient to a convincing looking website that looked like an Office365 login. If the person entered their user name and password when prompted, those details would be sent to the attacker, and the user would be redirected to a blank page.

Once credentials were obtained, the attacker would access the affected persons email account, and send the same phishing email to all of the contacts in their email address book.

This process has been repeated at scale; the new phishing emails sent out will appear to come from a known contact, when they have actually been hacked.

The campaign has hit a wide range of New Zealand organisations, across multiple sectors and regions. At this stage it appears to be focused on harvesting users' credentials. However, the information gained could be exploited for a range of different attacks, particularly if the credentials attackers gain have been used over multiple websites, systems or accounts.

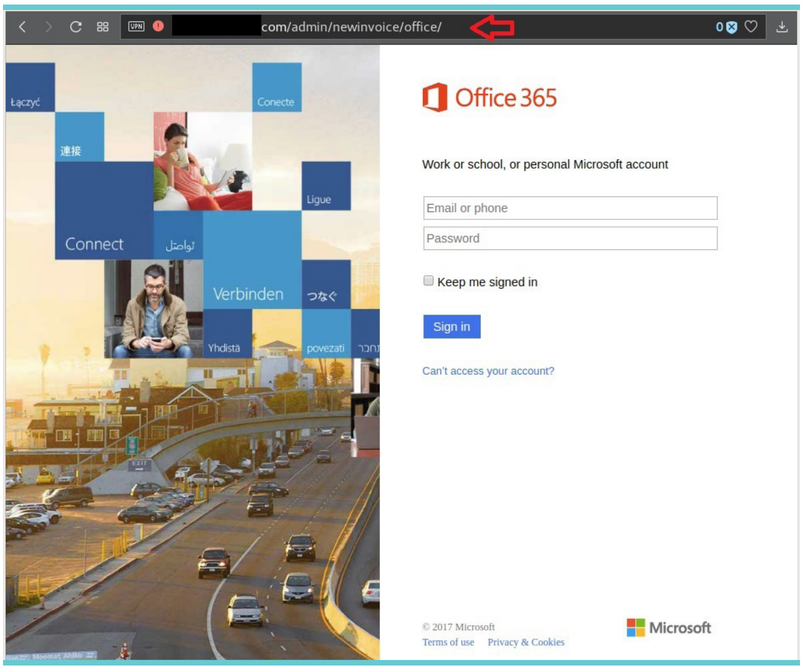
Prevention:

- Enable multi-factor authentication across company and personal email accounts.
- Contact the person by phone to ask if they have sent you a file.
- Be careful of links in emails. Use your own bookmarks or type the URL to make sure you are getting to the site you intend to.
- Hover over links to see if the URL refers to the site you're expecting before you decide whether to visit the site.
- Confirm that the URL in the search bar is the site you intended to visit.
- Report phishing attempts to CERT NZ and delete the email after it has been forwarded to us.

Mitigation:

- Change your email password immediately, make sure your new password is very different to the previous one, and that you haven't used that password anywhere else. If you use the same or similar passwords for any other accounts, change those too.
- Advise your IT department or your email provider that you have been affected by the Office 365 phishing campaign.
- Work with your IT team or IT provider to check your email logs and ensure that all access attempts to your email were legitimate and authorised.

Examples of Office 365 phishing



[redacted]com/admin/newinvoice/office/

Office 365

Work or school, or personal Microsoft account

Email or phone

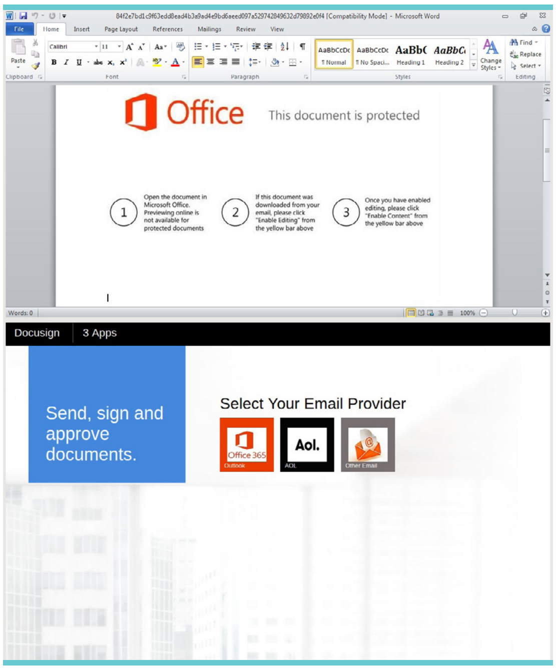
Password

□ Keep me signed in

Sign in

Can't access your account?

© 2017 Microsoft
Terms of use Privacy & Cookies



84f2e7bd1c9f63edd8ead4b3a9ad4e9bd6aeed097a529742849632d79892e0f4 [Compatibility Mode] - Microsoft Word

Office This document is protected

1 Open the document in Microsoft Office. Previewing online is not available for protected documents

2 If this document was downloaded from your email, please click "Enable Editing" from the yellow bar above

3 Once you have enabled editing, please click "Enable Content" from the yellow bar above

Words: 0

Docusign 3 Apps

Send, sign and approve documents.

Select Your Email Provider

A word about our information ///

About this report

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

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

Sometimes CERT NZ may ask for additional information about an incident to gain a better understanding, or 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 published on our website[8] and this report is subject to the CERT NZ standard disclaimer.[9]

Reporting an incident to CERT NZ

Anyone can report a cyber security incident to CERT NZ, from IT professionals & 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 next steps.

With your permission, we may refer incident reports 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.

[8] https://www.cert.govt.nz/about/privacy-and-information-statement/
[9] https://www.cert.govt.nz/about/disclaimer/

Categories we use

We use broad categories to group incident reports - over time we will refine these categories to a more granular level as the data set grows. The categories are:

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.

Ransomware - A common malware variant, with a specific purpose. If installed (usually by tricking a user into doing so, or 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.

Phishing & credential harvesting - Types of email, text or website attacks designed to convince users they are genuine, but 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.

Unauthorised access (successful) – Successful unauthorised access can enable an attacker to conduct a wide range of malicious activities on a network, infrastructure or computer. These activities are generally categorised by the three types of impact:

- Compromise of **confidentiality** of information
- Improper modification affecting the **integrity** of a system
- Degradation or denial of access or service affecting its **availability**

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

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

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

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.

Suspicious network traffic - Detected attempts to find insecure points or vulnerabilities in networks, infrastructure or computers. Threat actors 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.

Command & control server hosting – a system used as a command-and-control point by a botnet.

Reported vulnerabilities – Weaknesses or vulnerabilities in software, hardware or online service, which can be exploited to cause damage or gain access to information. They are reported to CERT NZ under our Coordinated Vulnerability Disclosure (CVD)[10] service.

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

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