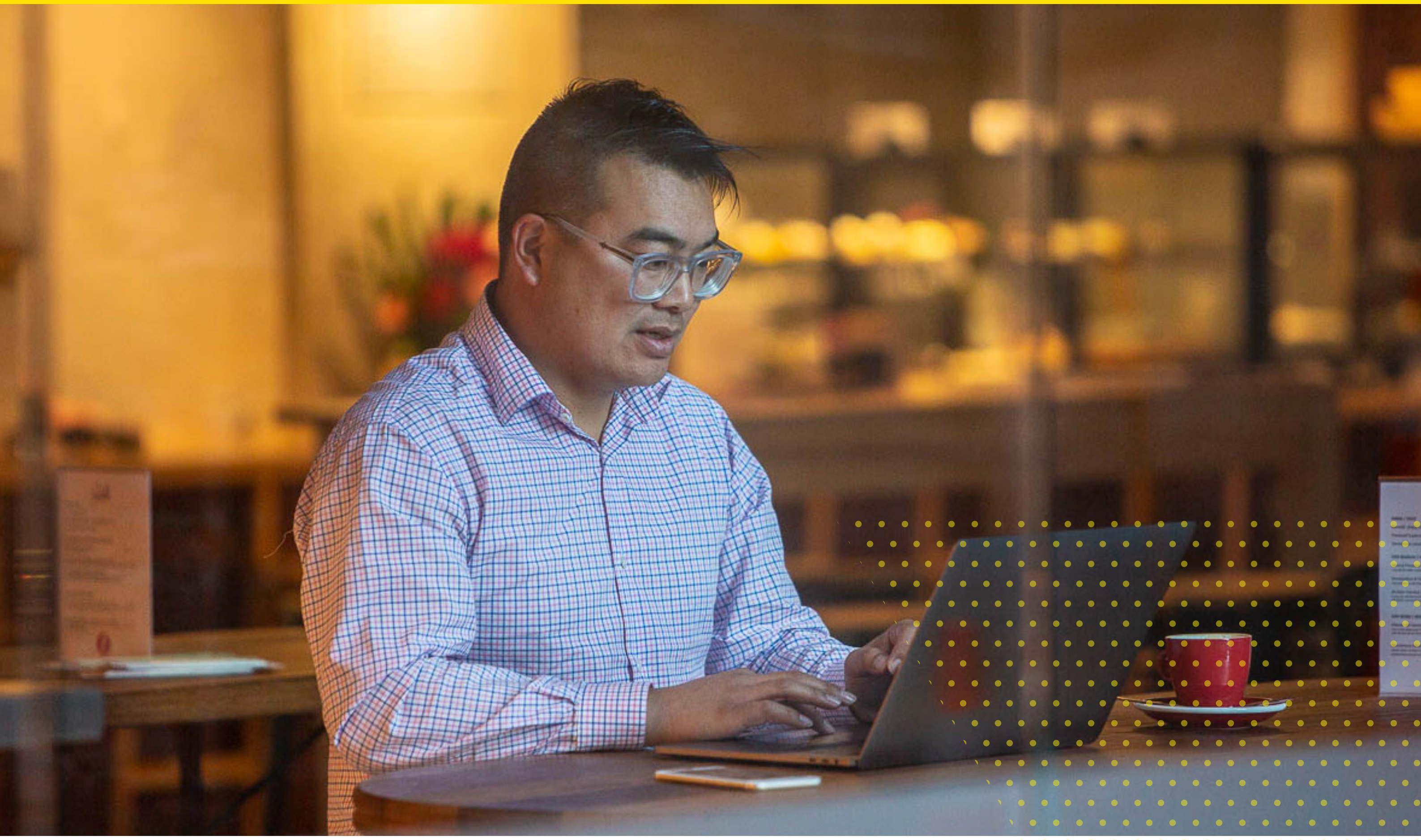


certnz

Quarterly Report: Highlights.

Q2

1 April – 30 June 2018

New Zealand Government

/// Director's message

CERT NZ values working with people and organisations at all levels and layers of the cyber security ecosystem in New Zealand; from other cyber security agencies, to the security community, to everyday internet users.

Being able to act as a central front door was a key consideration when CERT NZ was first created. With over 700 incidents reported to CERT NZ this quarter – our largest ever volume for a single quarter - our role as a central coordinator has become more important and apparent than ever.

Of course, the volume of reports is only one aspect of the work we do. Continuing to build a large and broad evidence base also helps us better understand the impact of cyber security issues on New Zealanders. In response to feedback from the information security community, CERT NZ is pleased to be able to share deeper analysis and categorisation of reported vulnerabilities this quarter.

> "We want New Zealanders to be able to build their resilience to cyber threats"

A vulnerability is a weaknesses in software, hardware or an online service that can be exploited to damage a system or access information. When a vulnerability is found, CERT NZ can help the finder communicate with the organisation whose systems are affected. We also have an important role to play in supporting organisations when they find themselves the subject of a report. CERT NZ encourages all organisations to have a plan for handling vulnerabilities; a little careful planning and talking to us ahead of time helps the process run smoothly.

We want New Zealanders to be able to build their resilience to cyber threats so we recognise the need for a safety net that allows vulnerabilities to be disclosed and actioned. Our vulnerability disclosure service continues to be used regularly for vulnerabilities of all types – these are covered in more depth in this report. Just as our approach to incident reporting focuses on helping affected people and organisations to recover quickly and stay resilient in the future, our approach to vulnerability reporting is about helping organisations and finders to feel supported and solution focused and prevent incidents before they happen.

Rob Pope
Director, CERT NZ

/// Q2 highlights

736 incident reports

were made in Q2, up from 506 in Q1.

$2.2 million in losses

down 24% from the last quarter.

68% of incidents

reporting loss are for amounts below $500.

55 and over report largest losses

representing 75% of the value of direct losses reported by individuals[1].

Phishing reports double

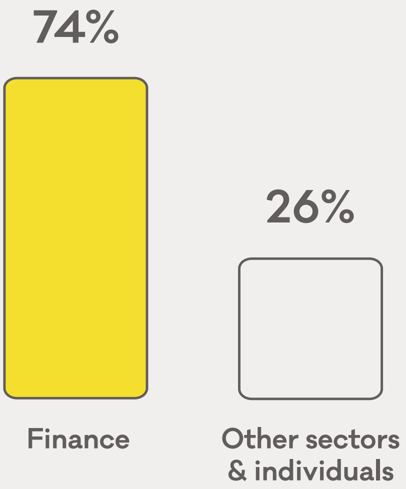
Phishing and credential harvesting reports have significantly increased, up from 196 in Q1, to 455 in Q2.

337 of these phishing and credential harvesting reports were from the financial sector, with 321 of these masquerading as known New Zealand brands.

This increase in reports comes from closer collaboration with the finance sector, enabling us to get a better picture of the phishing campaigns that constantly target New Zealanders.

We continue to see phishing emails pretending to be Office 365 documents and emails offering fake tax refunds.

Phishing and credential harvesting by sector



[1] Where a date of birth was provided.

Vulnerability reports: small business websites at risk

69 vulnerability reports were received in quarters 1 and 2, with 15 handled under our coordinated vulnerability disclosure policy (CVD).

A vulnerability is a weakness in software, hardware, or an online service that can be exploited to access information or damage a system.

Vulnerability reports were received across a range of vulnerability categories, including websites (54%), authentication, authorisation and accounting (14%), and networking (13%).

As a result of the vulnerability reports we have received, along with incident data, we have launched our first Cyber Smart mini campaign which is focused on helping small to medium sized businesses do the basics to protect their websites.

Vulnerability reports received in quarters 1 and 2 2018

For the first time, CERT NZ can share insights about the types of vulnerability reports we have received.

37 reports
related to websites or webservers

10 reports
related to authentication, authorisation and accounting

9 reports
related to networking

3 reports
related to applications or software

2 reports
related to mobile devices

8 reports
related to servers, printers, webcams, internet of things devices and other

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

Case study: Helping an e-commerce business recover

CERT NZ received a report in Q2 from an online e-commerce store that had repeatedly suffered breaches from a criminal actor over the course of a year.

These breaches led to their customers being tricked into paying money into the attacker's bank account, even though customers were using the store's real website. In some cases, the attacker even sent customers goods to try and hide their activities.

A specialist IT services company had been hired to rebuild the website and try to improve the website's security. However, the attacker kept returning and compromising the website, despite the store's attempts to also seek help from overseas hosting providers and payment portal providers.

The business then contacted CERT NZ. We were able to help them identify the key areas where their website's security was falling short and to understand why these weaknesses hadn't been resolved by their temporary and partial fixes, which allowed the hackers to regain access and conceal their operations.

Once the business was able to diagnose the root security weaknesses with guidance from CERT NZ, they were able to take steps to resolve the weaknesses and keep the attacker out for good.

The CERT NZ guide to securing business websites is available on our website[2].

> "With guidance from CERT NZ, they were able to take steps to resolve the weaknesses and keep the attacker out for good."

[2] https://www.cert.govt.nz/businesses-and-individuals/guides/cyber-security-your-business/protect-it/

/// Focus area – coordinated vulnerability disclosure

CERT NZ would like to thank WatchGuard Technologies and ZX Security for effectively and constructively participating in our CVD process and for giving us permission to share this case study.

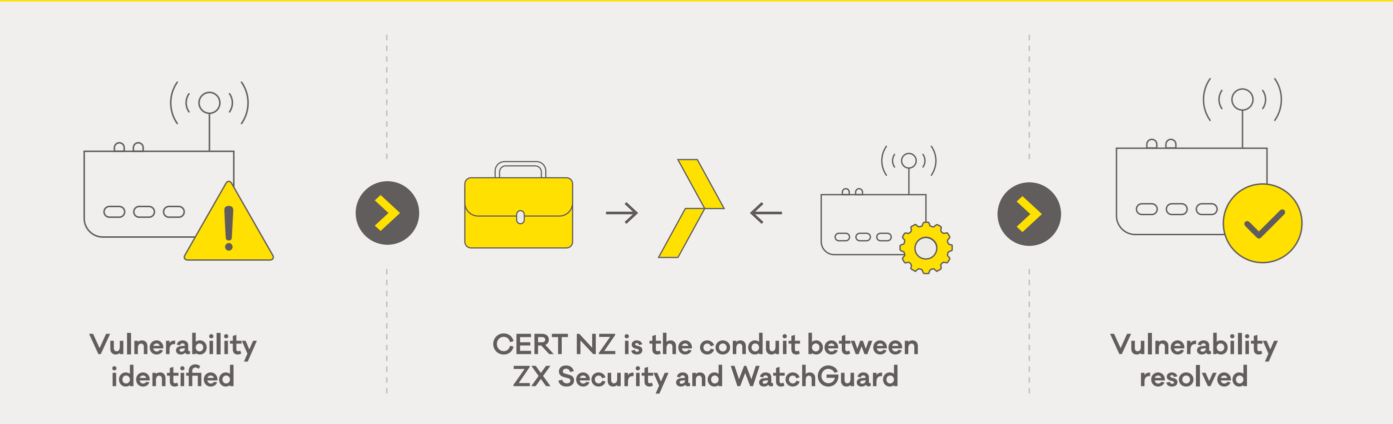
This quarter CERT NZ received a report from a security researcher at ZX Security about newly discovered vulnerabilities in products produced by a global network device company, WatchGuard Technologies.

The vulnerabilities were found in three of WatchGuard's wireless access point products that are commonly used in businesses, offices, stores and classrooms. The nature of the vulnerabilities meant that an attacker could potentially gain access to the devices, exposing users to a range of risks.

The report was treated as a coordinated vulnerability disclosure (CVD)[3], meaning CERT NZ acted as a safe, trusted conduit of information between the researcher and WatchGuard.

Information about the report was provided to WatchGuard and several questions about the nature of the vulnerabilities were relayed back to ZX Security's researcher.

Working collaboratively with CERT NZ, WatchGuard secured all of the information they needed to verify the vulnerabilities and understand their impacts. Both parties reached an agreement to publish Common Vulnerabilities and Exposure (CVE) identifiers for the findings.



CVEs are a key part of the process used by international organisations to provide public notification and resolution for vulnerabilities discovered in hardware and software products around the world.

Timing is critical in successfully addressing CVDs. CERT NZ's policy sets out reasonable timeframes so that vulnerabilities are resolved in a timely fashion before being made public. In this case, WatchGuard responded to the vulnerability by releasing patches and information for the affected products, within agreed timeframes.

By working together, potentially serious flaws in these products were able to be resolved in a timely and positive way, helping keep New Zealand businesses and organisations safe.

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