certnz

Quarterly Report: Highlights.

Q3 1 July – 30 September 2018

New Zealand Government

/// Director's message

Building New Zealand's resilience to cyber security threats is a key role for CERT NZ. As we continue to grow our presence as a central front door to recover from cyber security incidents, more New Zealanders are seeking our help and guidance.

Once again this quarter we have received our highest number of reports, 870, about threats and vulnerabilities impacting New Zealanders and the organisations they work for. While taking reports is a key part of the work we do, our goal is not to collect an ever-increasing volume of reports. Instead, we aim to provide timely, actionable information that enables people and businesses to shore up their defences before they are impacted, while maintaining a support service for incidents and vulnerabilities when they occur.

We analyse the reports we receive to understand the broader impacts these incidents could have on New Zealanders. When we combine these insights with information from international partners and global threat data, we can create and share actionable advice. Our open-by-default model means that the guidance we create can in turn be used by international partners.

Analysis of the reports we've received in our 18 months of operation shows that a broad cross section of New Zealanders and their organisations are impacted by cyber security issues. The mitigations to help them recover or prevent the incident in the first place can be boiled down to the same simple measures. It's these simple measures that we distil and share widely, through the likes of our Critical Controls, Get Cyber Smart campaigns and this Highlights Report, to help New Zealanders build their resilience and defences.

> "We provide timely, actionable information that enables people and businesses to shore up their defences before they are impacted."

Rob Pope
Director, CERT NZ

/// Q3 highlights

870 incident reports

were received in Q3 2018, up 18% from Q2.

$2.9 million

in direct financial losses, up 35% from Q2.

198 reports related to scams and fraud

an increase of 90% from Q2.

Phishing remains the largest incident category

although they have plateaued this quarter.

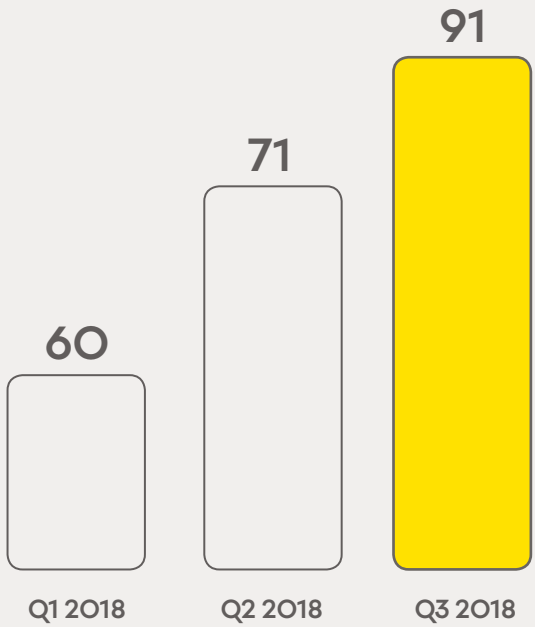
Unauthorised access reports

Reports of unauthorised access continues to increase. 91 reports were received in Q3 – a 28% increase on Q2.

More than a third of these reports (37) related to unauthorised access of business and personal email accounts, with an average loss of just over $78,000. The reports we've seen show that this access can be gained in a range of ways, with half reporting that their email accounts were compromised because attackers got access to their email password.

One of the strongest mitigations CERT NZ recommends to protect email accounts is to apply two-factor authentication (2FA). See our website for more information on 2FA[1].

Number of unauthorised access reports in 2018



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

1. https://www.cert.govt.nz/businesses-and-individuals/guides/getting-started-with-cyber-security/two-factor-authentication/

Scam and Fraud reports increase by 90%

There were 198 scam and fraud reports in Q3, a 90% increase from Q2. These resulted in $2.3 million of loss.

This jump was led by a large number of webcam and password extortion scam reports (46), and a number of smaller campaigns including invoice scams and Facebook-based scams (25), many of which CERT NZ and NZ Police have responded to.

On 23 July, CERT NZ first issued an advisory[2] about the increase in webcam and password blackmail scams, in response to the reports.

The webcam campaign is being experienced internationally and is affecting large numbers of everyday New Zealanders.

Case Study: Weak password opens door for attacker

A large New Zealand business was affected when an attacker gained access to its email marketing tool.

The attacker loaded thousands of new, legitimate email addresses to the account database, and sent out emails with fake invoices, replicating the business's style and branding.

The email marketing tool account was compromised as it had a weak password which the attacker was able to easily guess. Fortunately, in this case, an employee quickly discovered the breach before any financial transactions were made. The business blocked the account, improved password security and informed affected customers.

In response to the report, CERT NZ worked with the business to help it implement best practices for password management. These recommendations, which apply to all businesses, include making sure that important accounts and platforms are properly protected with strong, unique passwords and, wherever possible, with multi-factor authentication, especially when those accounts are internet accessible.

See our Guide for creating good passwords[3].

> "Protect with strong, unique passwords and multi-factor authentication."

2. https://www.cert.govt.nz/businesses-and-individuals/recent-threats/webcam-and-password-blackmail-scam/
3. https://www.cert.govt.nz/businesses-and-individuals/guides/getting-started-with-cyber-security/how-to-create-a-good-password/

Case Study: Business compromise leads to advisory

An IT provider noticed that one of its clients was receiving emails pretending to be a recognised supplier.

The emails contained fake invoices and were attempting to trick the client into paying the invoiced amount into the attacker's account.

The affected business investigated and discovered that the emails and fake invoices had been sent to people within the business and to some of its external customers.

The emails seemed legitimate. For example, they included knowledge of recent goods requests and costs. However, there were small differences in the email addresses which staff picked up on before any payments were made.

The business discovered that an employee's email account had a simple password, making it easy for the attackers to gain access and forward emails containing words like 'account', 'invoice' and 'pay' to an external address belonging to the attacker. These emails allowed the attackers to gather information about the business's billing cycles and behaviours, helping the attackers to create invoices that looked legitimate.

The compromise went unnoticed for at least six months as the attacker was deleting the forwarded emails from the employee's account.

CERT NZ analysed the detail from this report and others, and published an advisory about the extent and nature of invoice scams, how to protect against them, and the types of checks to perform if fake invoices are received.[4]

CERT NZ recommends these simple steps to protect your business:

- **Protect against email spoofing –** which is when attackers send you emails pretending to be from legitimate businesses. Protect against this with solutions such as DomainKeys Identified Mail (DKIM) and Domain-based Message Authentication, Reporting and Conformance (DMARC).
- **Strengthen your email account security –** by patching your systems and using strong, unique passwords on each account.
- **Secure your network –** especially when using systems that can be accessed remotely (including remote desktop protocol (RDP). Use strong, unique passwords and enable two-factor authentication (2FA) where you can.
- **Review your business processes –** to ensure that your processes don't rely solely on email. Verify payments to new or different accounts by phone before making the transaction. This can help prevent losses.

For more information, see CERT NZ's top 11 cyber security tips for business[5].

4. https://www.cert.govt.nz/businesses-and-individuals/recent-threats/invoice-scams-affecting-new-zealand-businesses/
5. https://www.cert.govt.nz/businesses-and-individuals/guides/cyber-security-your-business/top-11-cyber-security-tips-for-your-business/

/// Focus area - malware insights

Malware is one of the most intrusive and disruptive types of cyber security threats facing New Zealand organisations. Malware compromises can have major technical, financial and operational impacts, and can take significant efforts to recover from.

Malware compromise reports have climbed steadily during 2018. There were a total of 37 malware reports, including 14 of ransomware.

15 reports involved compromises of websites in order to distribute malware, and eight actual infections of computers or endpoints. This diagram illustrates how the use of websites for malware distribution works.

Typical malware distribution model

The reports received come from a wide range of sectors, suggesting that many attackers do not select targets based on organisation type but on level of account security.

Once a compromise occurs, the malware can perform a range of actions, including collecting information, stealing usernames and passwords or other financial data, causing damage to the system, or installing disruptive ransomware.

Many malware types are designed to spread laterally to other computers on the same network. It is also not unusual for more than one type of malware to be present in a payload or in an infection – and once a computer is infected, this can be followed by downloading additional malware with additional capabilities. Malware is often more insidious and difficult to detect than ransomware because it usually attempts to conceal its presence and actions from the host.

Common malware variants reported in Q3 were: Emotet, Gozi, Zeus, ramnit, spinx, kronos and gootkit. Common ransomware variants reported in Q3 were: Dharma, Everbe, Nemesis and Hermes.

Reports to CERT NZ show the impacts on a business are limited by early detection, having backup processes that are resilient to ransomware (or data loss) attacks, and robust logging processes.

These insights demonstrate the importance of strengthening businesses cyber security.

For more information on how to protect your organisation from malware, see the CERT NZ Critical Controls[6].

6. https://www.cert.govt.nz/it-specialists/critical-controls/