
# CYBR 171 /// 2023

Sam Leggett – Senior Analyst, Threat and Incident Response CERT NZ

certnz

# CERT NZ

Computer Emergency Response Team New Zealand

- Established in 2017, part of the Ministry of Business Innovation and Employment
- Our goal is to improve the cyber resilience and online safety of all New Zealanders.
- We work to support businesses, organisations and individuals affected by cyber security incidents.
- Part of a global network of CERT teams and government security organisations

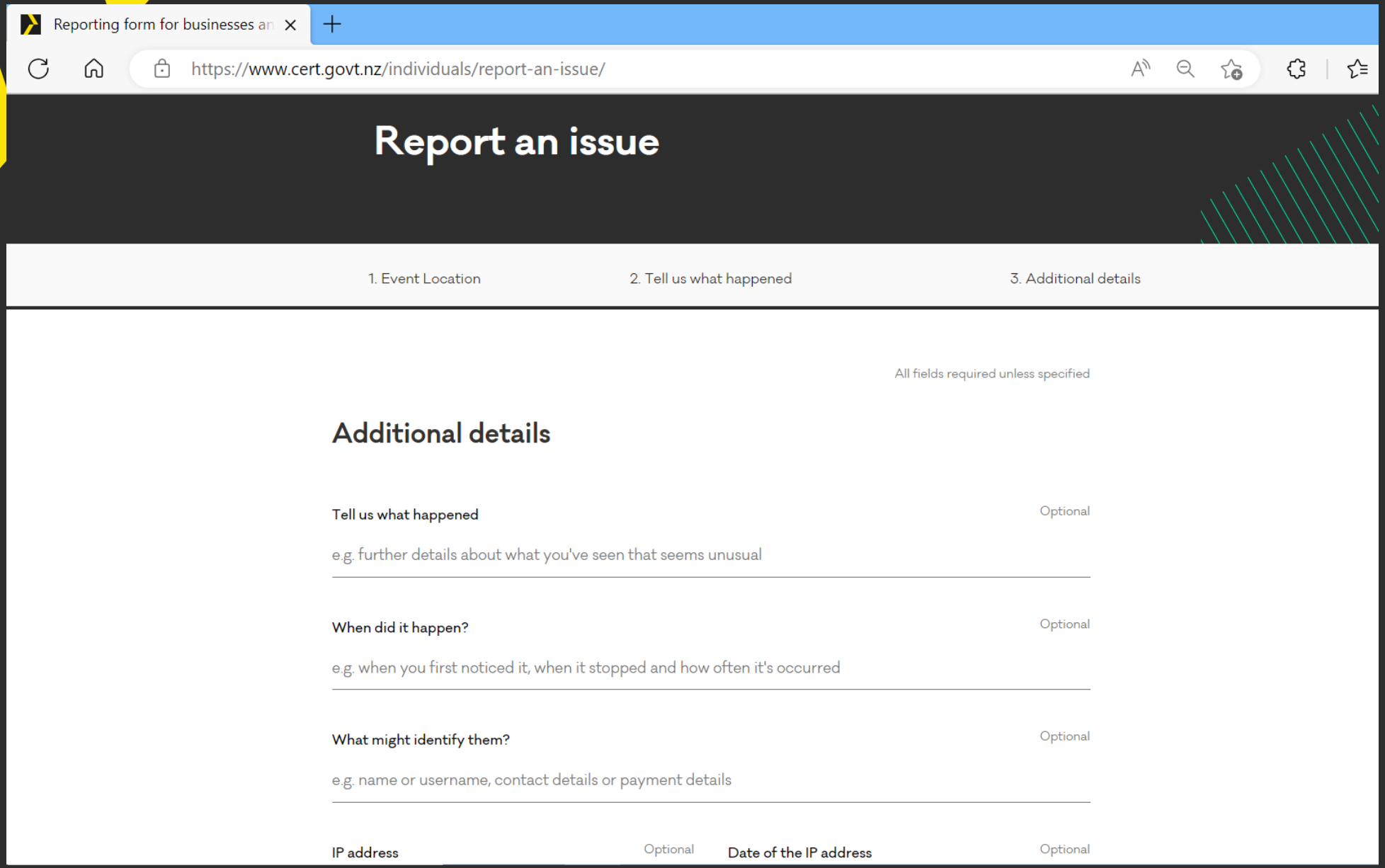
https://www.cert.govt.nz/

certnz

# Threat and Incident Response

- Online incident reporting and response
- Major incident coordination
- Major event support
- Phishing (PDS, credential dumps)
- Data breaches
- Coordinated Vulnerability Disclosure
- Advisories and alerts
- Critical Controls and other online resources

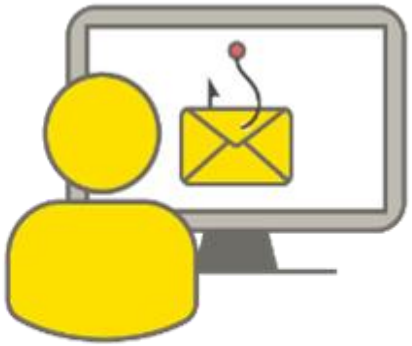
certnz


Reporting form for businesses an
https://www.cert.govt.nz/individuals/report-an-issue/
Report an issue
1. Event Location
2. Tell us what happened
3. Additional details
All fields required unless specified
Additional details
Tell us what happened
Optional
e.g. further details about what you've seen that seems unusual
When did it happen?
Optional
e.g. when you first noticed it, when it stopped and how often it's occurred
What might identify them?
Optional
e.g. name or username, contact details or payment details
IP address
Optional
Date of the IP address
Optional

# Threat and Incident Response

- Online incident reporting and response
- Major incident coordination
- Major event support
- Phishing (PDS, credential dumps)
- Coordinated Vulnerability Disclosure
- Advisories and alerts
- Critical Controls, guidance and other online resources

certnz



Phishing email received


Recipient reports phishing to CERT NZ


CERT NZ analyses report and identifies phishing activity


CERT NZ publishes phishing information to partners


Partners consume information and use it to disrupt phishing campaigns (blocking or stopping)

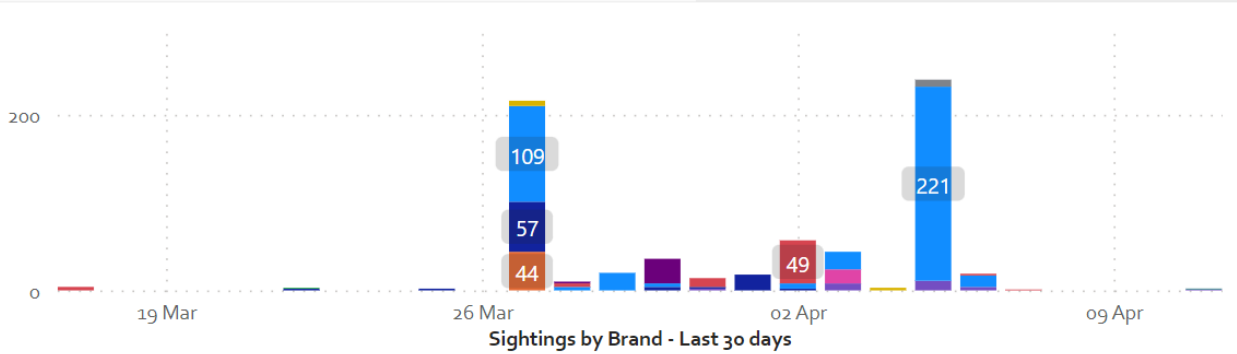
New Zealanders are protected from further impacts of the phishing campaign

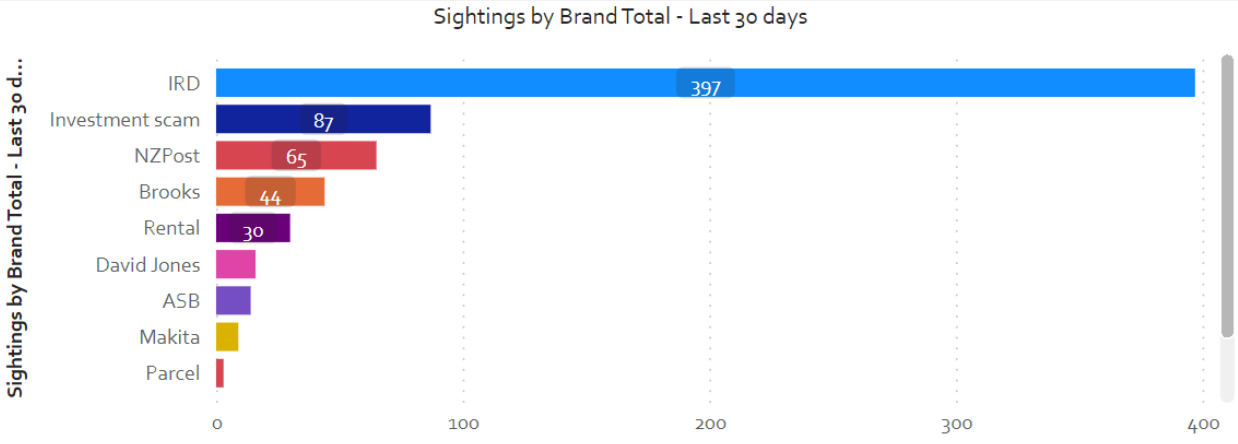
# Phishing Disruption Service

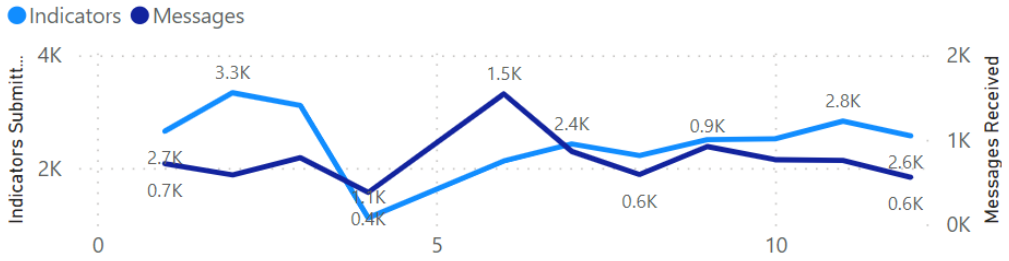
Earliest Date Last Refreshed

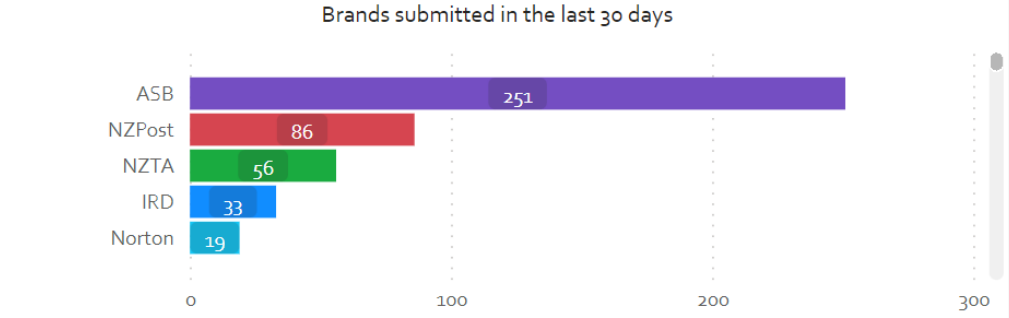
**In the last 30 days:**

| Msgs recieved | IOC Published | Sightings |
|---|---|---|
| 1346 | 551 | 721 |
| **Msgs Processed** | **Unique Brands submitted** | **Sightings YTD** |
| 850 | 56 | 1203 |




CERT NZ runs a phishing disruption service. This disruption service aims to minimise the impact of phishing emails via stopping malicious links to be either loaded or blocks the emails themselves.

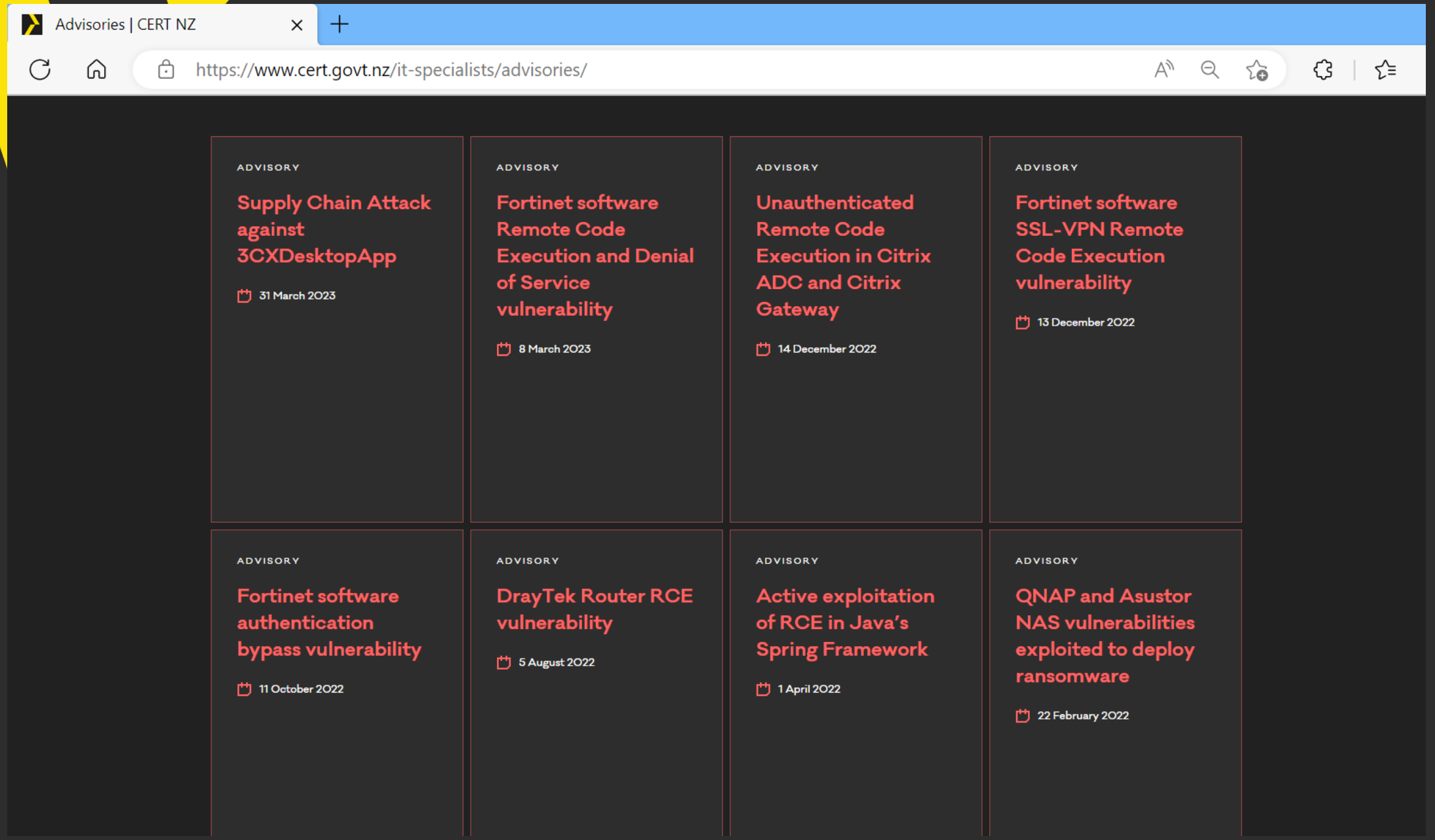
What is a msg? What is an IOC?
What sightings mean

Whats the purpose of Phish disrupt?

# Threat and Incident Response

- Online incident reporting and response
- Major incident coordination
- Major event support
- Phishing (PDS, credential dumps)
- Coordinated Vulnerability Disclosure
- Advisories and alerts
- Critical Controls and other online resources

certnz


Advisories | CERT NZ
https://www.cert.govt.nz/it-specialists/advisories/
ADVISORY
Supply Chain Attack against 3CXDesktopApp
31 March 2023
ADVISORY
Fortinet software Remote Code Execution and Denial of Service vulnerability
8 March 2023
ADVISORY
Unauthenticated Remote Code Execution in Citrix ADC and Citrix Gateway
14 December 2022
ADVISORY
Fortinet software SSL-VPN Remote Code Execution vulnerability
13 December 2022
ADVISORY
Fortinet software authentication bypass vulnerability
11 October 2022
ADVISORY
DrayTek Router RCE vulnerability
5 August 2022
ADVISORY
Active exploitation of RCE in Java's Spring Framework
1 April 2022
ADVISORY
QNAP and Asustor NAS vulnerabilities exploited to deploy ransomware
22 February 2022

# Threat and Incident Response

- Online incident reporting and response
- Major incident coordination
- Major event support
- Phishing (PDS, credential dumps)
- Coordinated Vulnerability Disclosure
- Advisories and alerts
- Critical Controls and other online resources

certnz

Critical controls | CERT NZ

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

CRITICAL CONTROLS

## CERT NZ's Critical Controls

Each year, we review our critical controls against the incidents we have seen over the past 12 months. When correctly im

CRITICAL CONTROLS

## Security awareness building

Cyber attackers often rely on human behaviour, such as clicking on links or downloading and...

CRITICAL CONTROLS

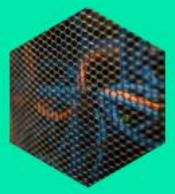
## Password manager

Providing a password manager for your staff to store their passwords, or other secrets like...

CRITICAL CONTROLS

## Asset Lifecycle Management

Limiting and securing your internet-exposed services will help you prevent unauthorised...



CRITICAL CONTROLS

## Network segmentation and separation

When paired together, segmentation and separation can add an additional level of access...

CRITICAL CONTROLS

## Centralised logging

Storing and securing your logs in a central place makes log analysis and alerting easier.

CRITICAL CONTROLS

## Implement and test backups

After an incident, restoring your data from backups is often the best way to return to business as...

CRITICAL CONTROLS

## Principle of least privilege

The principle of least privilege

CRITICAL CONTROLS

## Multi-factor authentication and verification

CRITICAL CONTROLS

## Implement application control

CRITICAL CONTROLS

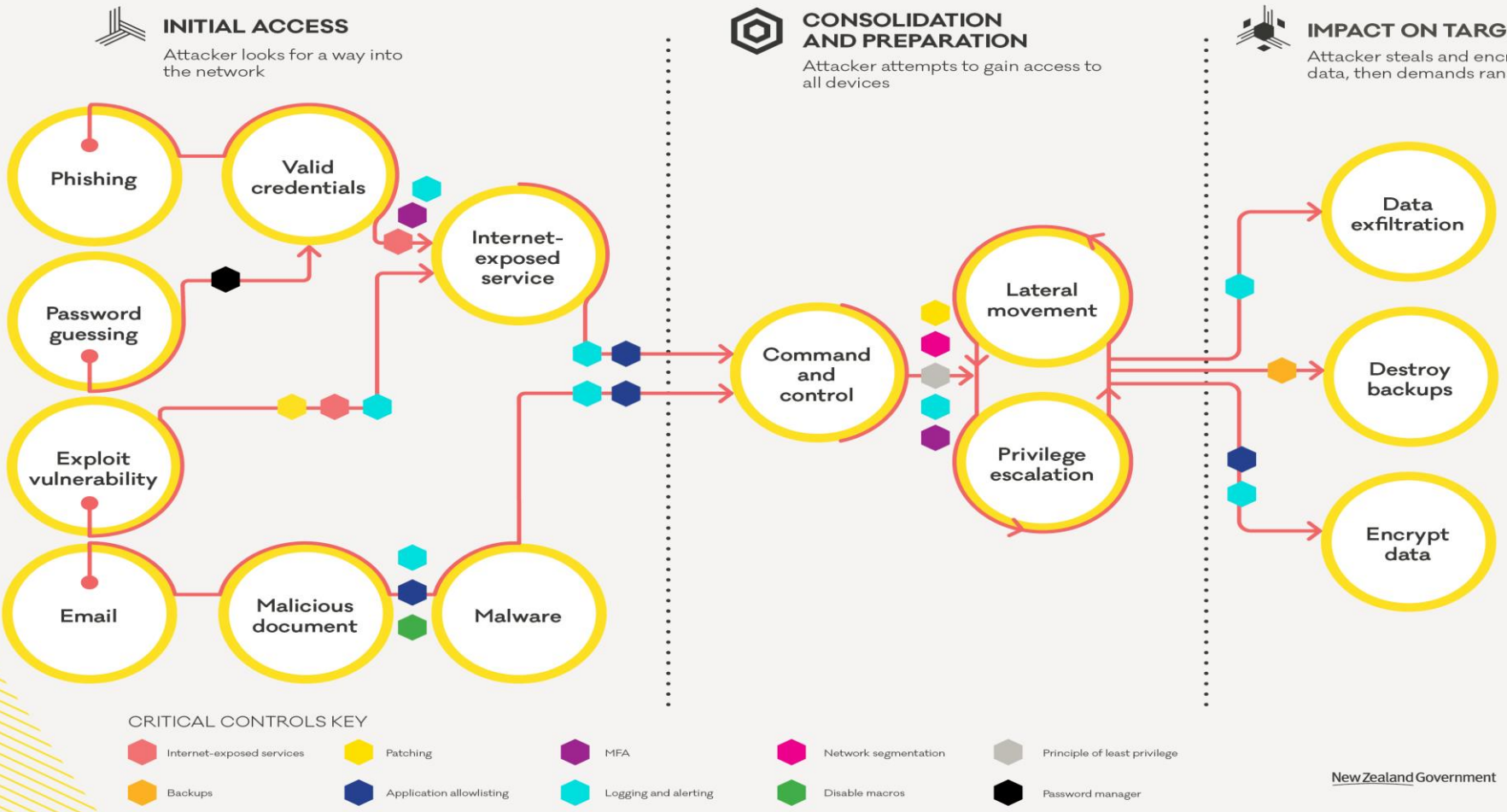
## Patching

Keeping your software up-to-date

# LIFECYCLE OF A RANSOMWARE INCIDENT

certnz

How the CERT NZ Critical Controls can help you stop a ransomware attack in its tracks.



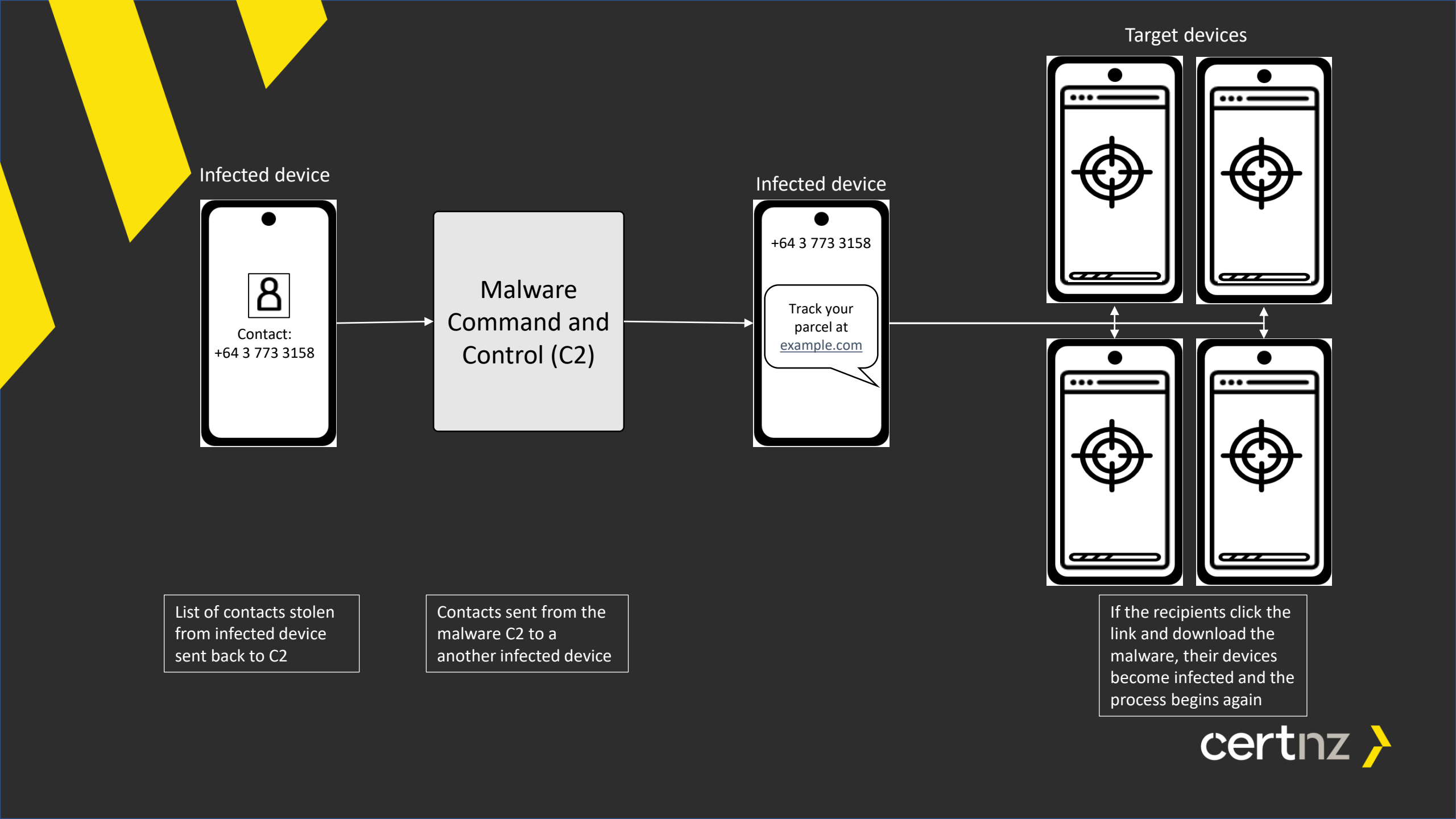

New Zealand Government

certnz

# Major incident coordination

- Widespread supply chain attack
- Banking targeted DDoS attacks
- Flubot malware

certnz

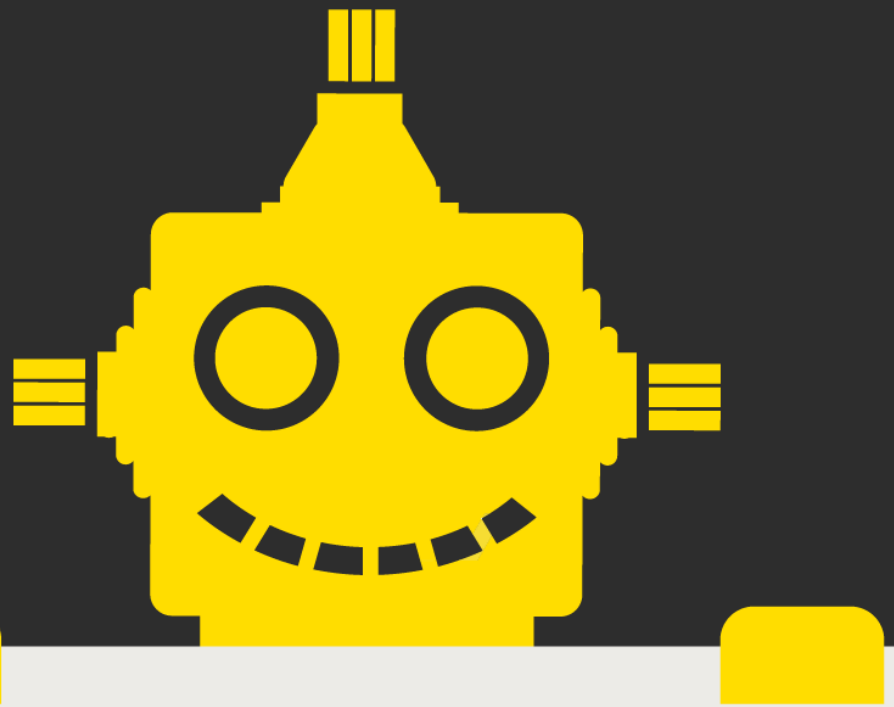

Target devices
Infected device
Contact:
+64 3 773 3158
Malware Command and Control (C2)
Infected device
+64 3 773 3158
Track your parcel at example.com
List of contacts stolen from infected device sent back to C2
Contacts sent from the malware C2 to a another infected device
If the recipients click the link and download the malware, their devices become infected and the process begins again

# Social Engineering

- Phishing
- Tech-scam calls
- Sim-swapping
- Dating and Romance scams
- Gift-card scams
- Extortion scams
- Investment scams
- Job opportunity scams
- Government services scams

certnz

# Any Questions?



# Thank you