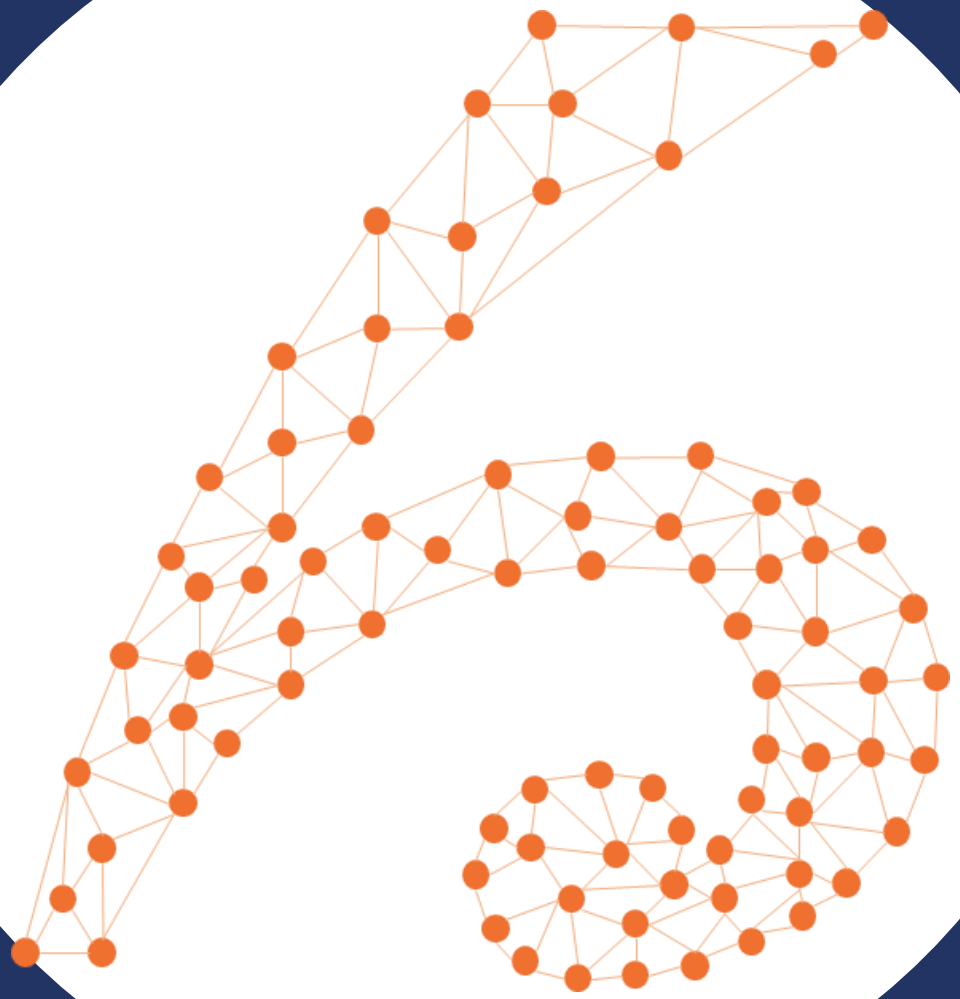


DDOS attack

Briefing Pack

31 August 2020

DDOS Attack Summary

New Zealand Stock Exchange (NZX) experienced multiple Distributed Denial of Service (DDOS) attacks. Heightened risk that other sectors could also be the target

What is it?

A DDOS attack is where hackers flood web services with network traffic so the website or service can not be accessed or crashes. Typically includes a ransom demand.

What do we need?

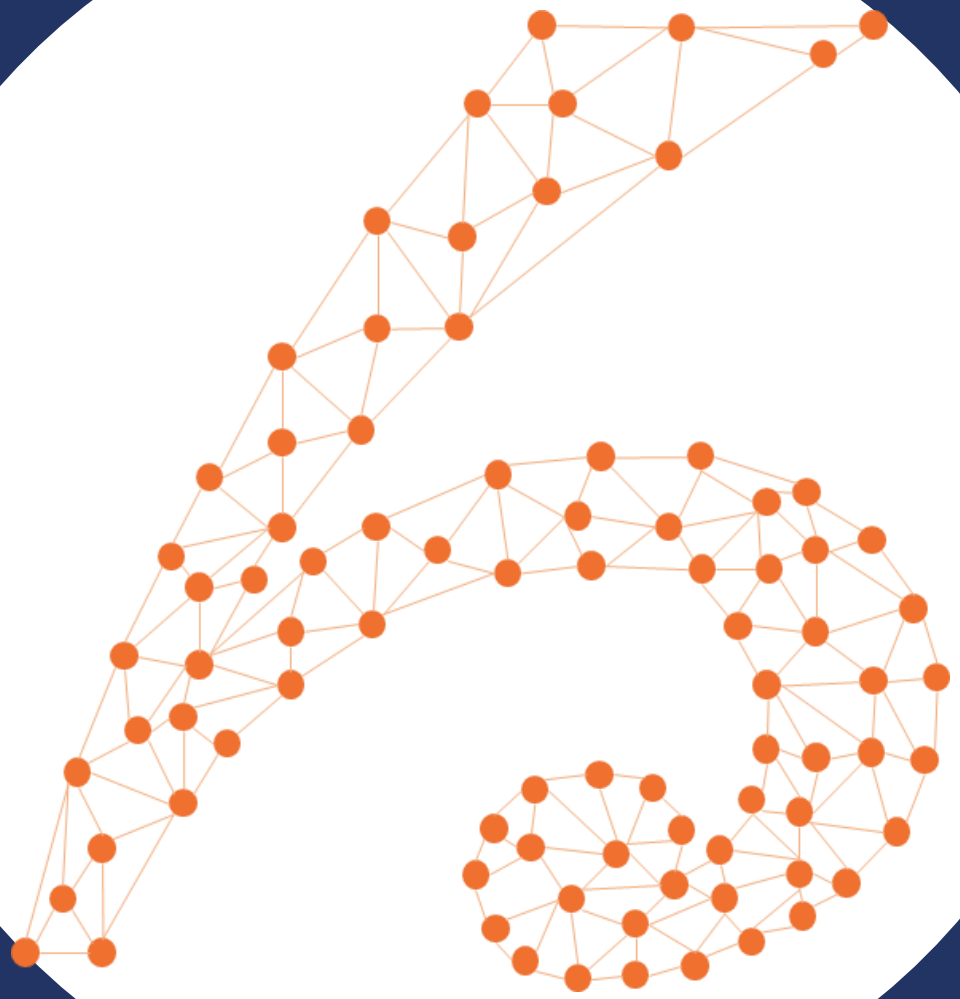
1. Prioritised list of websites and / or systems that if taken offline would have a **significant** impact on health service delivery.
2. Confirm the key contact(s) for DDOS attack incident for your organisation.
3. Ensure you have adequate protection and are prepared
4. Ensure you have a clear incident response plan.

Guidance

- Internet facing services (or those reliant on internet connectivity) are at greatest risk
- Prepare for the worst case
- Prioritise based on business impact, consider pandemic response
- Understand where BCP is needed (and where it isn’t)
- Brief your executive, keep them informed
- Direct communications and media enquiries to Ministry of Health
- Reach out for help to your colleagues, Ministry or GCDO where needed
- Review the NCSC Advisory to inform your actions, in particular:
    - Have an incident response plan and BCP in place
    - Practice what you would do in an incident
    - Check with your internet provider that your external services / websites have DDOS protection, and that your external services and networks flow through your DDOS protection services
    - Consider critical services ability to function with no internet or restricted internet
    - Implement real time availability monitoring

Potential risks to consider

- Public websites (eg .health.govt.nz)
- Public cloud services (eg. AWS, SF)
- Email/desktop tools (O365)
- Collaboration tools (Zoom, MS Teams)
- Remote access (business access, vendor support, external partners)
- Critical applications/services (eg. NHI/HPI, NCTS/MIQ services)
- Telephony services (eg. Healthline, Ministry call centre)
- Messaging and integration (eg. Connected Health, NZePS, test results, claims and payments)
- External service dependencies/vulnerabilities (eg. ISP, shared services)



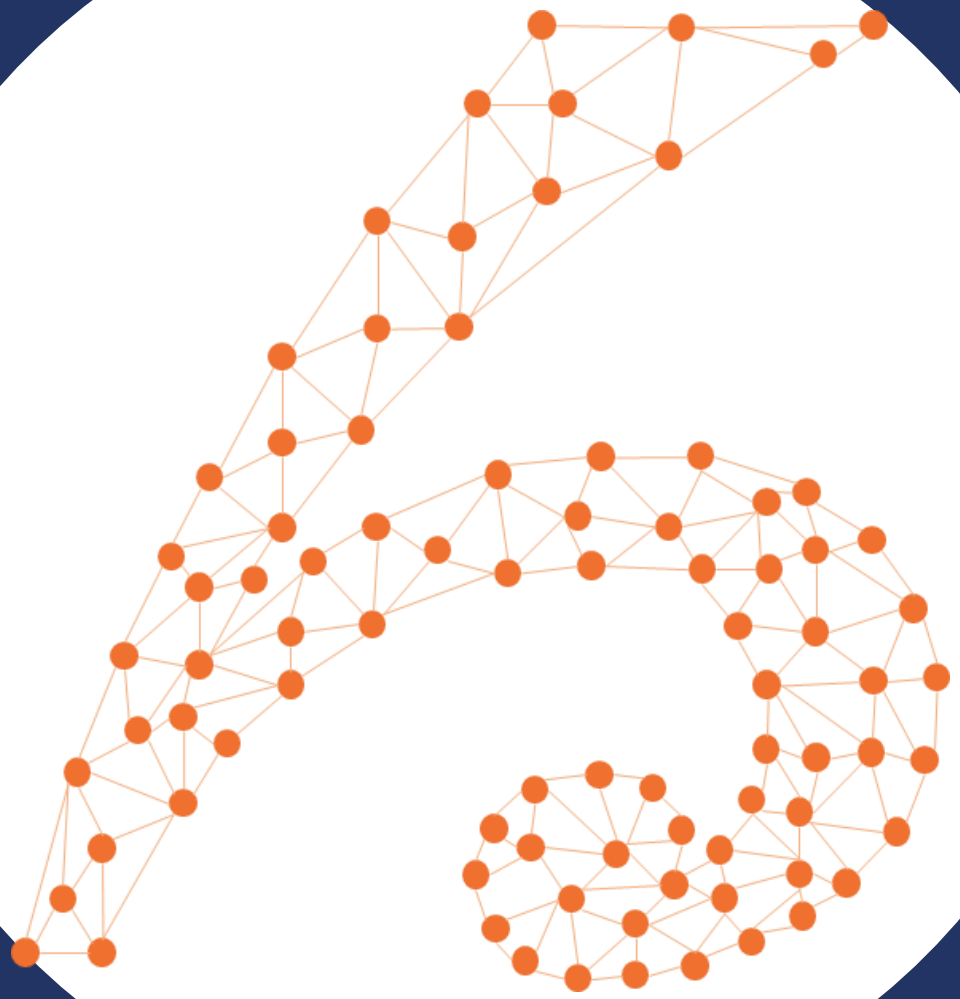
healthAlliance approach

Ministry contacts

Matthew Lord (sector and NDS engagement) 027 801 9821

Escalation contacts are:

Darren Douglass (sector) 027 455 6091 (Shayne Hunter from 2 Sept, 021 688 440)



Questions?

NCSC Advisory Recommendations

- Before implementing any measures to prepare for denial-of-service attacks, organisations should determine whether a business requirement exists for their online services to withstand denial-of-service attacks, or whether temporary denial of access to online services is acceptable to the organisation.
- Determine what functionality and quality of service is acceptable to legitimate users of online services, how to maintain such functionality, and what functionality can be lived without during denial-of-service attacks.
- Discuss with service providers the details of their denial-of-service attack prevention and mitigation strategies. Specifically, the service provider's:
    - capacity to withstand denial-of-service attack
    - any costs likely to be incurred by customers resulting from denial-of-service attacks
    - thresholds for notifying customers or turning off their online services during denial-of-service attacks
    - pre-approved actions that can be undertaken during denial-of-service attacks
    - denial-of-service attack prevention arrangements with upstream providers (e.g. Tier 2 service providers) to block malicious traffic as far upstream as possible.
- Protect organisation domain names by using registrar locking and confirming domain registration details (e.g. contact details) are correct.
- Ensure 24x7 contact details are maintained for service providers and that service providers maintain 24x7 contact details for their customers. Establish additional out-of-band contact details (e.g. mobile phone number and non-organisational email) for service providers to use when normal communication channels fail.
- Implement availability monitoring with real-time alerting to detect denial-of-service attacks and measure their impact.

NCSC Advisory Recommendations

- Pre-prepare a static version of a website that requires minimal processing and bandwidth in order to facilitate continuity of service when under denial-of-service attacks.
- Use cloud-based hosting from a major cloud service provider (preferably from multiple major cloud service providers to obtain redundancy) with high bandwidth and content delivery networks that cache non-dynamic websites.
- If using a content delivery network, avoid disclosing the IP address of the web server under the organisation's control (referred to as the origin web server), and use a firewall to ensure that only the content delivery network can access this web server.
- Use a denial-of-service attack mitigation service.
- Responding to denial of service attacks:
    - Work with service providers to implement responsive actions
    - Temporarily transfer online services to cloud-based hosting hosted with high bandwidth and content delivery networks that cache non-dynamic websites.
    - Use a denial-of-service attack mitigation service for the duration of the denial-of-service attacks.
    - Deliberately disable functionality or remove content from online services that enable the current denial-of-service attack to be effective