Incident Response Action Card Denial of Service

Version:1

22 December 2022

1. Scope

1.1 This document applies whenever the security of an ICT system or data is impacted, or has the potential to be impacted, by a malicious denial of service (Dos) threat.

1.2 The action card is intended for use by operational officers, primarily within ICT and [response] teams. All ICT individuals who participate within incident response can adopt and use this action card where appropriate.

1.3 The guidance in this action card expands on and must be read in conjunction with the internal Council Cyber Security Incident Processes and Procedures. Adherence to guidance within both documents is required for effective Incident Response.

1.4 Any contractual, legal or government regulatory requirements mandating more stringent requirements than specified in this action card will supersede the requirements of this document.

2. Baseline Recommendations

2.1 Retain a full audit trail of your actions to avoid problems in a criminal case.

2.2 Implement the Triage phase immediately wherever possible.

2.3 Implement the Triage and Contain phases swiftly to avoid further criminal damage including system breaches and data loss.

2.4 Process assets individually through phases to avoid undue delays which increase the incident severity – i.e., do not wait for full information before acting.

2.5 Implement the Analysis and Search phases comprehensively to avoid persistent criminal presence within Council systems.

2.6 Defer the Recovery phase until the Isolate phase is complete to avoid persistent criminal presence within Council systems.

2.7 Regularly update [incident coordinator] on situation to avoid undue delays which cause the Council to breach legal requirements.

2.8 Use firewall botnet filter and monitoring for outgoing traffic, traffic from botnet primarily transmits via IRC, P2P, HTTPS.

3. Preparation

Pre-incident

Aim- implement proactive measures to improve threat preparedness

- Monitor these protocols and wherever possible block P2P and IRC

3.1 Utilise Network monitoring utility, which will allow for monitoring of traffic patterns

3.2 Enable IP accounting to get visibility into packets, volume, source, destination ports etc.

3.3 Disable DNS recursive queries, primarily used by attackers to launch DoS/ DDoS or cache poisoning attacks

3.4 Apply limits for:

- **ICMP packet rate**
  - SYN packet rate
  - DNS TTL for the exposed systems

3.5 Regularly review the load and log files of.

- **Servers**
  - Routers
  - Firewalls
  - Applications and other infrastructure

3.6 Identify what aspects of Dos traffic differentiate it from benign traffic, this may include.

- Source IP addresses, AS, etc
- Destination ports
- URLs
- Protocol flags

3.7 Utilise network analysis tools to review the traffic like tcpdump, ntop, NetFlow, MRTG etc.

3.8 Contact the ISP to provide details about the traffic sources as identified earlier including:

- Network blocks involved
- Source IP addresses
- Protocols

The details could be received in the following format: Parameter	Average Maximum Peak Utilisation	Maximum threshold value
Network bandwidth-MPLS links between offices	50%	80%