Cyber Incident Response

Denial of Service Playbook v2.3

Document Control

Title	Denial of Service Playbook
Version	2.3
Date Issued	20/01/2020
Status	Draft
Document owner	Scottish Government
Creator name	
Creator organisation name	NCC Group
Subject category	Cyber Incident Response Management
Access constraints	

Document Revision History

Version	Date	Author	Summary of changes
2.3	22/01/2020	SG CRU	Generic Version Created from Public Sector Playbook

Contents

1. Introduction

1.1. Overview

In the event of a cyber incident, it is important that the organisation is able to respond, mobilise and execute an appropriate level of response to limit the impact on the brand, value, service delivery and the public, client and customer confidence. Although all cyber incidents are different in their nature and technologies used, it is possible to group common cyber incident types and methodologies together. This is in order to provide an appropriate and timely response depending on the cyber incident type. Incident specific playbooks provide incident managers and stakeholders with a consistent approach to follow when remediating a cyber incident.

References are made to both a Core IT CIRT and a CIRT within this document. This is in recognition the playbook will be used by organisations of different sizes. Some may initially manage an incident with a small response team within IT services but where there is a confirmed compromise, this may be escalated to an extended level CIRT comprised of members of the organisation outside IT services who will deal with agreed categories of compromise. The Playbook as with the Cyber Incident Response Plan (CIRP) will require to be adjusted to reflect the organisational make up.

Playbooks describe the activities of those directly involved in managing specific cyber incidents. However, it is important to acknowledge the speed at which cyber incidents can escalate and become a significant business disruptor requiring both business continuity and consequence management considerations. Early consideration should be given to engaging Business Continuity, Resilience and Policy Area Leads in order that the wider issues can be effectively managed. Business Continuity and Resilience leads within the organisation must therefore be familiar with the Cyber Incident Response Plan (CIRP) and Playbooks and how they link to wider incident response arrangements.

1.2. Purpose

The purpose of the Cyber incident Response: Denial of Service (DoS) Playbook is to define activities that should be considered when detecting, analysing and remediating a DoS attack. The playbook also identifies the key stakeholders that may be required to undertake these specific activities.

1.3. Denial of Service Definition

A denial-of-service (DoS) attack is the intentional paralysing of a computer network by flooding it with data to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services.

See Appendix A.

1.4. Scope

This document has been designed for the sole use of the first responders such as the Service Desk team when responding to a cyber incident. It is not standalone and must be used alongside your Cyber Incident Response Plan (CIRP).

1.5. Review Cycle

This document is to be reviewed for continued relevancy by the Cyber Incident Response Team (CIRT) lead at least once every 12 months; following any major cyber incidents, a change of vendor, or the acquisition of new security services.

2. Preparation Phase

Preparation Phase		
Phase objectives	The preparation phase has the following objectives: • Prepare to respond to cyber incident in a timely and effective manner; • Inform employees of their role in remediating a DoS incident including reporting mechanisms.	
Activity	**Description**	**Stakeholders**
Prepare to respond	Activities may include, but are not limited to:	
	Review and rehearse cyber incident response procedures including technical and business roles and responsibilities, escalation to major incident management where necessary.	• Head of Information Governance • CISO • Head of IT • Information Security Manager / ISO • Team Leader • Service Delivery Manager • Service Desk Analysts/Technicians • Legal Team • Communications Team • Police Area Lead • Resilience Lead Business Continuity Lead
	Review recent cyber incidents and the outputs.	• Information Security Manager

	Review threat intelligence for threats to the organisation, brands and the sector, as well as common patterns and newly developing risks and vulnerabilities.	• Information Security Manager
	Ensure appropriate access to any necessary documentation and information, including out-of-hours access, for the following: • CIRP; • <<Network Architecture Diagrams>>; (insert Links) • <<Data Flow Diagrams>>.(insert Links)	• Information Security Manager
	Identify and obtain the services of a 3rd party Cyber Forensic provider.	• Information Security Manager
	Define Threat and Risk Indicators and Alerting pattern within the organisation's security information and event management (SIEM) solution.	• Information Security Manager
Activity	**Description**	**Stakeholders**
Inform employees	Activities may include, but are not limited to:	
	Conduct regular awareness campaigns to highlight cyber security risks faced by employees, including: • Phishing attacks and malicious emails; • Ransomware; • DoS attacks; • Reporting a suspected cyber incident.	• Head of IT • Information Security Manager • Resilience Lead • Business Continuity Lead
	Ensure regular security training is mandated for those employees managing personal, confidential or high risk data and systems.	• Head of IT • Information Security Manager • HR • L&D Department

		• Resilience Lead • Business Continuity Lead

3. Detect

Detection Phase		
Phase objectives	The detection phase has the following objectives: • Detect and report a DoS attack. • Complete initial investigation of the attack. • Report the incident to the correct team as a cyber incident.	
Activity	**Description**	**Stakeholders**
Detect and report the incident	Activities may include, but are not limited to:	
	Confirm system is under attack: • Confirming a system is under attack rather than heavy load is often only possible if the system has previously been baselined to establish normal operational loads. This must account for changes in load over time as some systems will only be used at financial day/month/year end. • Consult with the Product Manager to establish whether the current condition is within acceptable parameters to be considered in service.	• Information Security Manager • Product Manager • Core IT CIRT

	If a normal system load exists then it can be compared against the current traffic seen. The review should identify if there are any common traffic patterns, and will need the input from network specialists. DoS attack packets often have a common element, it may help to familiarise yourself with the current most prevalent examples in **Appendix A: DoS Attack Types**. It will be necessary to work with network engineers who have diagnostic tools/facilities (such as Netflow) to capture and analyse incoming packets to the affected system(s) to identify: • Common sending IP address; • Common port; • Common protocol; • Common user agent; • Common payload; and • Common packet flags.	• Information Security Manager • Core IT CIRT
	Report the cyber incident via the Service Desk. If a ticket does not exist already, raise a ticket containing minimum information. To report an incident, follow the process defined in the CIRP (insert link to CIRP).	• Information Security Manage • Core IT CIRT
	Assign Classification to the cyber incident, based upon available information related to the DoS attack and the incident types (see CIRP).	• Information Security Manager • Core IT CIRT
	Report the Cyber Incident in accordance with the organisation's CIRP. Consider the Intelligence value to other organisations and share on the CiSP	• Information Security Manager • Core IT CIRT • CIRT
	Where appropriate consider reporting requirements to Information Commissioner's Office (ICO), relevant regulator and or Competent Authority (NISD), National Cyber Security Centre (NCSC), and / or Police Scotland	• Information Security Manager • Core IT CIRT • CIRT

Activity	Description	Stakeholders
	Activities may include, but are not limited to:	
	Mobilise the Core IT CIRT to begin initial investigation of the cyber incident (see CIRP for staff contact details for further information).	• Information Security Manager • Ciore IT CIRT • CIRT The following may also be included in the CIRT where appropriate for the incident: • Service Desk Analysts • Server Desk Technicians • Server Team • Mobile Device Team
Initial investigation of the incident	Collate initial incident data including as a minimum for the following; • What systems and/or applications are being targeted? • What impact is it having on them and, since you have identified the attack, is it getting worse, and is there a pattern to the attack? • Is the attack spreading or is it still confined to the same systems/applications? • What impact is this having on the company's bandwidth? • Has the attack spread to any shared components, or from what has been seen so far, could it extend to any shared components? (e.g. infrastructure components, directory services etc.) • Is the attack affecting internal corporate systems and/or has the attack spread into the corporate network? • Have any support calls been received from any customers? • Does it appear to distract from a more targeted exploit that could result in a breach of data from other company systems or the company systems targeted by the DoS? • Has any communication been received from a purported attacker? (via social media, email, phone call etc.)	• Head of IT • Information Security Manager • Core IT CIRT • CIRT

	• A timeline of when the attack was first detected • A list of the services that are known to be affected • Confirm whether systems are accessible internally and externally • Ensure you are clear whether systems are offline or operating with reduced performance • Details of the type attack (if known at this stage)	
	Research Threat Intelligence sources and consider Cyber Security Information Sharing Partnership (CiSP) submission to gain further intelligence and support mitigation by others.	• Information Security Manager • Core IT CIRT • CIRT
	Review cyber incident categorisation to validate the cyber incident type as a DoS attack and assess the incident priority, based upon the initial investigation. (See CIRP for Incident Severity Matrix)	• Information Security Manager • Core IT CIRT • CIRT • Resilience Lead • Business Continuity Lead
Activity	**Description**	**Stakeholders**
Incident reporting	Activities may include, but are not limited to:	
	Report the cyber incident in accordance with the organisation's CIRP.	• Information Security Manager • Core IT CIRT • CIRT
	Report the Cyber Incident in accordance with the organisation's CIRP. Consider the Intelligence value to other organisations and share on the CiSP	• Information Security Manager • Core IT CIRT • CIRT

	Where appropriate consider reporting requirements to Information Commissioner's Office (ICO), relevant Regulator and or Competent Authority (NISD), National Cyber Security Centre (NCSC) and / or Police Scotland	• Information Security Manager • Core IT CIRT • CIRT
	Escalate using the appropriate steps in the CIRP.	• Information Security Manager • Core IT CIRT • CIRT • Resilience Lead • Business Continuity Lead • Policy Lead
Activity	**Description**	**Stakeholders**
Establish the requirement for a full forensic investigation	Activities may include, but are not limited to:	
	Consider conducting a full forensic investigation, on the advice of legal counsel. All evidence handling should be done in line with the Association of Chief Police Officers (ACPO) Good Practice Guide for Digital Evidence.	• Information Security Manager • Core IT CIRT • CIRT

4. Remediation – Contain, Eradicate and Recover

Remediation Phase		
Phase objectives	The remediation phase has the following objectives: • Contain the effects of the DoS attack on the targeted systems; • Recover affected systems and services back to a Business As Usual (BAU) state.	
Activity	**Description**	**Stakeholders**
Containment	Initial containment considerations include:	
	If the attack is disabling services, are there any immediate steps that could be taken to regain some level of service – e.g. requesting the Internet Service Provider (ISP) to drop all traffic targeting the affected service/application. In an absolute extreme case, if it is imperative to maintain internal services, then all traffic from the ISP could be blocked (Note, this will have implications including: potentially loss of email, Internet access, customer access).	• Information Security Manager • Core IT CIRT • CIRT
	Consideration should be given to whether the Business Continuity Plan should be enacted. If a decision is made to use a different data centre, it should also be borne in mind that the attack may follow to the new location.	• Information Security Manager • Core IT CIRT • CIRT • Business Continuity Lead
	Once an analysis of the traffic has been completed, the company may be able to filter traffic at the border. If the attack is focussed on maximising computer resource usage of the target (such as a Slowloris attack) then this may be effective. However, if, the attacker is looking to simply overwhelm the internet connection with excessive network packets this may not offer a viable defence.	• Information Security Manager • Core IT CIRT • CIRT

	Placing IP restrictions on sensitive services is an effective method to reduce the impact of traffic.	• Information Security Manager • Core IT CIRT • CIRT
	Segregation of internet services; separate internal email and web traffic from product services to reduce the impact.	• Information Security Manager • Core IT CIRT • CIRT
	The network team should contact the ISP and discuss what filtering they can provide. The contractual relationship with the ISP should identify any actions they are obliged to take. As a DoS attack tends to impact everyone using the same equipment, the ISP may include contractual options to cut the company connections in order to protect other customers from the attack. This would then impact all of the company's services using that network link.	• Information Security Manager • Core IT CIRT • CIRT
	Inform stakeholders of the progress of containment activities in accordance with the CIRP.	• Information Security Manager • CIRT • Resilience Lead • Business Continuity Lead • Policy Areas Lead • Corporate Comms
Activity	**Description**	**Stakeholders**
Eradication	Activities may include, but are not limited to:	
	• Systems patched to protect against vulnerabilities exploited in the attack. • Network segmentation implemented. • Removal of vulnerable systems/services. • Blacklist attack source IPs. • Whitelist of source IPs and services allowed into the network.	• Information Security Manager • Core IT CIRT • CIRT

5. Post Incident

Post-Incident Activities Phase		
Phase objectives	The post-incident activities phase has the following objectives: • Complete an incident report including all incident details and activities; • Complete the lessons identified and problem management process; • Publish appropriate internal and external communications.	
Activity	**Description**	**Stakeholders**
Incident reporting	Draft a post-incident report that includes the following details as a minimum: • Details of the cyber incident identified and remediated across the network to include timings, type and location of incident as well as the effect on users; • Activities that were undertaken by relevant resolver groups, service providers and business stakeholders that enabled normal business operations to be resumed; • Recommendations where any aspects of people, process or technology could be improved across the organisation to help prevent a similar cyber incident from reoccurring, as part of a formalised lessons identified process.	• Senior Stakeholders • Head of Information Governance • Head of IT • Audit Committee • Information Security Manager • Resilience Lead • Business Continuity Lead • Policy Area Lead
Lessons Identified & Problem Management	Complete the formal lessons identified process to feedback into future preparation activities.	• Information Security Manager • CIRT

	Consider sharing lessons identified with appropriate external stakeholders	• Information Security Manager • CIRT • Resilience Lead • Business Continuity Lead • Police Area Lead
	Conduct root cause analysis to identify and remediate underlying vulnerabilities.	• Information Security Manager • Core IT CIRT • CIRT
Human Resources	Review staff welfare; working hours, overtime, time off in lieu (TOIL) and expenses.	• Information Security Manager • HR
Communications	Activities may include, but are not limited to:	
	Publish internal communications in line with the communications strategy to inform and educate employees on DoS attacks and security awareness.	• Information Security Manager • CIRT • Communications
	Published external communications, if appropriate, in line with the communications strategy to provide advice to customers, engage with the market, and inform press of the cyber incident. These communications should provide key information of the cyber incident without leaving the organisation vulnerable or inciting further DoS attacks.	• Head of IT • Information Security Manager • Communications Team • Resilience Lead • Business Continuity Lead • Policy Area Lead

6. Appendix A: DoS Attack Types

Name	Description
HTTP Flood	A type of resource exhaustion attack. The attacker sends a large volume of apparently legitimate requests for a web page. The server is simply unable to respond to the number of requests. This type of attack is very common as it requires very little knowledge to invoke.
ICMP (Ping) Flood	A type of volumetric attack, and sub-type of UDP flood. The attacker sends a large amount of ICMP Ping packets (typically used to confirm networks are operating correctly) with the intent of using up the target's bandwidth.
Network Time Protocol (NTP) Amplification	A type of volumetric attack. An attacker manipulates a third party NTP service that has been left exposed on the internet, pretending to make requests from the target. The NTP server responds to the requests with its normal packets. What makes this attack work is that the attacker sends 1 maliciously crafted packet to the NTP server and by design the NTP server responds by sending 200 packets to the target, believing that it had asked for them.
Ping of Death 'POD'	A type of volumetric attack. Similar to the ICMP flood above, but this time the packet sent is deliberately crafted to be larger than the system was designed to cope with. Older systems such as the original version of Windows 98 would immediately crash when they received the packet. Modern systems were thought to discard this attack vector automatically, but had only introduced controls for the older IPv4. With IPv6 it has returned with unpatched Microsoft Windows 2012 confirmed as vulnerable to PODv6.
Slowloris	A type of resource exhaustion attack. This is unusual in DoS in that it is targeted and can overwhelm a single machine without affecting others. It can be used as a distraction whilst an attacker's true activity carries on unnoticed by the IT team busy trying to fix a rebooting web server. The attack sends packets that open a large number of requests with the server, but once the server starts responding the system asks the server to slow down transmission, stalling the connection and preventing the server from closing the connections. Whilst it is slowing down the existing connections, the attack typically sends additional requests to open yet more connections until the server has run out of memory. If

	a legitimate client is able to get a response from the server it may report HTTP error 503: The service is unavailable.
SNMP Flood	A type of volumetric attack. Similar to the NTP flood. This attack has a lower rate of packets returned so is less effective, and consequently less common but is expected to be seen more as fewer NTP servers are left open to the internet.
SYN Flood	A type of resource exhaustion attack. This leverages weaknesses in TCP, one of the underlying protocols on the internet to use up all resources in the operating system of the target. These resources are often strictly limited by the hardware available and, as the attack is against the operating system, the attacker can easily identify what is the most effective method by performing test runs themselves against their own systems.
UDP Flood	A type of volumetric attack. The attacker sends a large amount of session-less packets to the target IP addresses with the intent of using up the target's bandwidth. These may be directed to a single port or multiple ports. Typically results in the clients receiving an ICMP Destination Unreachable response when they try to access the service.
Zero Day Attacks	These attacks are characterised by their lack of characterisation. They are brand new and may target previously believed secure systems.

7. Appendix B: Flow Diagram