Using Janet for cyber security research

Using Janet for cyber security research

Title:	Using Janet for cyber security research
Issue:	1
Document owner:	John Chapman, Director information security policy and governance
Authorised by:	John Chapman, Director information security policy and governance
Date:	17 August 2022
Last Reviewed:	3 November 2023

Document control

1. First release in this format

1 Introduction

This document is intended to provide guidance for organisations connected to the Janet network on the subject of lawful cyber security research. It outlines the policies that must be followed and the technical controls that should be considered to mitigate against risks associated with this type of research and to protect the institution’s reputation.

2 Background

Many institutions connected to the Janet network undertake lawful cyber security research

and we occasionally get asked if doing so is a legitimate use of Janet.

3 Acceptable use

Section 6 of the Janet Acceptable Use Policy [1] states that (Subject to clauses 8 to 16), Janet may be used by a Connected Organisation for any lawful activity in furtherance of the missions of the Connected Organisation. In most cases undertaking lawful cyber security research will therefore be an acceptable use of Janet, provided that the activity complies with the Janet Acceptable Use Policy [1] and the Janet Security Policy [2], however it is the institution's responsibility to ensure the proposed activity is both lawful and compliant with the Janet policies.

4 Technical controls

The following guidance should be considered by the institution before undertaking cyber security research. These points are not exhaustive and are listed here to aid internal discussions as to how to safely undertake this type of research. It is the institution’s responsibility to ensure they are in full compliance with the Janet Acceptable Use and Security policies and that the activities to be undertaken are lawful.

- Cyber security research activity must be segregated entirely from the rest of the institution’s network.
- The institution must inform Jisc CSIRT (via irt@jisc.ac.uk [3]) of the subnet that is associated with this activity.
- The institution should monitor the traffic transiting that subnet and regularly check that only expected activity is being seen, i.e. no attempts to connect to the organisation’s main network or IP space belonging to other members.
- It is recommended that there is filtering/rate-limiting of outbound traffic from such subnets, in case research systems are compromised.
- Any systems in the cyber security research enclave must be kept hardened.
- The institution should ensure there is a documented and well tested process in place for how the institution would respond to abnormal activity in or from their cyber security research network and to complaints received from Jisc or other network users (see AUP Note 5 [1]).

5 Information sharing

The Jisc Cyber Threat Intelligence (CTI) function would be interested in receiving any relevant findings from institutions using Janet for cyber security research that can be used to help protect the education and research sector. Jisc CTI can be contacted via irt@jisc.ac.uk [3].

Links
[1] https://community.jisc.ac.uk/library/acceptable-use-policy
[2] https://community.jisc.ac.uk/library/janet-policies/security-policy
[3] mailto:irt@jisc.ac.uk