**From:** Telstra Cybersecurity Team  
**To:** Network Operations Team (networks@email.com)  
**Subject:** [URGENT] Request to Implement Firewall Rule – Ongoing Malware Incident

Hello Network Operations Team,

We are reaching out to request the implementation of a firewall rule in response to an active malware incident. Below are the details related to the attack:

**Incident Summary:**

An unauthorized party exploited a zero-day vulnerability (Spring4Shell) in the Spring Framework affecting our nbn services.

**Required Firewall Rule Configuration:**

* Deny all incoming traffic containing the client request path "/tomcatwar.jsp"
* Block any incoming HTTP traffic with the following headers:
  + suffix=%>//
  + c1=Runtime
  + c2=<%
  + DNT=1
  + Content-Type=application/x-www-form-urlencoded

**Additional Information:**

* The attack seems to be focused on our external-facing systems running Spring Framework version 5.3.0.
* Please monitor this endpoint closely for any new activity

If you need clarification or further support, feel free to get in touch.

Best Regards,  
**James | Telstra Cybersecurity Team**