**From:** Telstra Security Operations

Provides a clear and professional summary of the issue. Ensures the email subject is taken seriously without seeming like a potential phishing attempt.

**To:** nbn Team <nbn@email>

**Subject:** Critical Incident: Malware Detected on NBN Connection Infrastructure

—

Briefly states the nature of the problem. Quickly informs the team of a significant issue needing attention.

**Body:**

Hello NBN Team,

We detected a critical issue with the NBN Connection infrastructure.

Provides specific information about the attack, including what was affected, when it happened, and the nature of the attack.

Ensures the team understands the scope and specifics of the incident for proper diagnosis and response.

**Incident Details:**

Affected Infrastructure: NBN Connection  
Hostname: nbn.external.network  
Timestamp: March 20, 2022, at 03:21:00 UTC  
Attack Details: Multiple suspicious bypass actions using POST requests to ‘/tomcatwar.jsp’. These requests seem to carry harmful payloads.

**Impact:** The NBN Connection Service is currently down and not working properly.  
  
Telstra Security Operations is monitoring the incident and will provide an update ASAP. Please be on standby for mitigation.

Describes the current effect of the attack on the service.  
  
Conveys the severity and urgency of the situation to prompt immediate action.

For any questions or issues, don’t hesitate to reach out to us.

Kind regards,

Telstra Security Operations

Informs the team that the situation is being monitored and they should be ready for further instructions.  
  
Assures the team that the issue is being actively managed while preparing them for potential mitigation actions.