**From:** Telstra Security Operations

**To:** nbn@email

**Subject:** Critical Ongoing Malware Attack - Immediate Action Required

—

**Body:**

Hello nbn Team,

This is to inform you of an ongoing malware threat (CVE-2022-22965: Spring Framework RCE via Data Binding on JDK 9+) that has been detected within our network infrastructure and alerted our firewall logs. The incident occurred at [ 2022-03-20T03:16:34Z ],

affecting the critical network **nbn.external.network**

The **Spring Framework 5.3.0** service is down and functionality is impaired due to the malware attack. We urge all team members to remain vigilant and to follow best practices for cybersecurity, such as refraining from clicking on suspicious links or downloading unknown files.

As part of our incident response plan and mitigation preparedness, we are taking the following actions:

1. **5.3.x users should upgrade to 5.3.18+**
2. Isolating the affected infrastructure to prevent further spread of the malware.
3. Conducting a thorough analysis of the malware to identify its origin and capabilities.
4. Implementing enhanced security measures to protect our network from future threats.

We will provide further updates as more information becomes available

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

Kind regards,

Telstra Security Operations