Incident Postmortem: Malware Attack on nbn Services

## **Summary**

At 2022-03-20 03:16:34 UTC, Telstra Security Operations detected a malware attack on nbn services using a zero-day vulnerability affecting the Spring Framework.

Parties involved:

* Mobile Team
* nbn Team
* Networks Team

## **Impact**

The malware attack has led to downtime across our nbn network leading to impaired service functionality. It has also affected the mobile tower connection, home and business lines, as well as the ADSL Connect Infrastructures.

## **Detection**

The incident was detected via a triggered alert on our firewall dashboard.

## **Root Cause**

The root cause was due to a zero-day vulnerability affecting the Spring Framework. A Spring MVC or Spring WebFlux application running on JDK 9+ may be vulnerable to remote code execution (RCE) via data binding.

## **Resolution**

A firewall rule (Python script) was put into placed to prevent firewall bypasses in the future.

## **Action Items**

What was done to resolve the incident:

* Patterns in the attack were detected.
* New firewall rule was implemented according to the detected attack patterns.