From: Telstra Security Operations
To: NBN team (nbn@email)
Subject: URGENT: Active Malware Detected – Immediate Action Required
—
Hello nbn team,

We have detected a Malware attack that requires immediate response affecting NBN connection (Spring Framework 5.3.0) at 03:16:34 UTC 2022-03-20.

INCIDENT OVERVIEW:

ATTACK TYPE: Ongoing Remote Code Execution (RCE) via Data Binding

AFFECTED SYSTEMS: Spring Framework 5.3.0

CVE DETAILS: CVE-2022-22963 & CVE-2022-22965

SEVERITY: P1 CRITICAL

INDICATORS OF COMPROMISE :

Malicious URL: http:///tomcatwar[.]jsp

Next Steps:

1. immediately apply the necessary updates in the Spring Blog posts : Spring Cloud Function updates addressing CVE-2022-22963

   Spring Framework updates addressing CVE-2022-22965.

2. Ensure the network returns to its normal operation

3. block known malicious domains and IPs.

4. Begin forensic investigation and collect logs for analysis.

more resources on the vulnerability and mitigations:

https://spring.io/security/cve-2022-22965

https://www.kb.cert.org/vuls/id/970766

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

Kind regards,
Telstra Security Operations