

SDBBot targeting health sector

cyber.gov.au/acsc/view-all-content/alerts/sdbbot-targeting-health-sector

[Report](#)

[Contact us](#)

[Portal login](#)

You are here

The ACSC has observed increased targeting activity against the Australian health sector by actors using the SDBBot Remote Access Tool (RAT).

Alert status

HIGH

The ACSC has observed increased targeting activity against the Australian health sector by actors using the SDBBot Remote Access Tool (RAT).

SDBBot is comprised of 3 components; an installer which establishes persistence, a loader which downloads additional components, and the RAT itself. Once installed, malicious actors will use SDBBot to move laterally within a network and exfiltrate data. SDBBot is a known precursor of the Clop ransomware.

While the recently observed activity is targeting the health sector, the ACSC recommends that all network owners review their controls against ransomware as per ACSC's publication [Ransomware in Australia](#).