Queries to the SCM database from 26 June to 4 July 2018

- The copying and exfiltration of data from the SCM database was stopped on 4 July 2018, after staff from IHiS discovered the unusual queries and took steps to prevent any similar queries from being run against the SCM database.

Attempts to re-enter the SingHealth Network on 18 and 19 July 2018

- After detection of malware on and communications from the S.P. server, CSA recommended that internet surfing separation should be implemented, to prevent the attacker from exercising command and control over any remaining footholds it may have in the network.
- Internet surfing separation was implemented on 20 July 2018.
- No further signs of malicious activity were detected thereafter.

CONTRIBUTING FACTORS LEADING TO THE CYBER ATTACK

Network connections between the SGH Citrix servers & SCM database were allowed

Network connections between the SGH Citrix servers & SCM database were allowed

- This open connection IS not necessary, more for convenience to administer database (we shud reduce attack surface area)
- A basic security review of the network architecture and connectivity between the SGH Citrix servers and the SCM database could have shown that the open network connection created a security vulnerability.
- However, no such review was carried out.
- MORAL: GET RID OF UNNECESSARY CONNECTIONS!