Privilege escalation and lateral movement – December 2017 to June 2018

- Evidence of the attacker's lateral movements was found in the proliferation of malware across a number of endpoints and servers.
  - Malware samples found and analysed by CSA were either tools that were stealthy by design, or unique variants that were not seen in-the-wild and not detected by standard anti-malware solutions.
- Such malware included RAT 1, another Remote Access Trojan referred to in this report as "**RAT 2**", and the malware associated with the earlier-mentioned log file.

Privilege escalation and lateral movement – December 2017 to June 2018

- Evidence of PowerShell commands used by the attacker to distribute malware to infect other machines, and of malicious files being copied between machines over mapped network drives..
- CSA has also assessed that the attacker is likely to have compromised the Windows authentication system and obtained administrator and user credentials.
- This meant that the attacker would have gained full control over
  - all Windows based servers and hosted applications,
  - all employee workstations, and underlying data, within the domain.

Privilege escalation and lateral movement – December 2017 to June 2018

- *Establishing control over Workstation B on 17 April 2018*
  - Attacker gained access to Workstation B (SGH) & planted RAT 2, thus gaining control of the workstation -which **had access** to the SCM application.
  - Workstation B was used to log in remotely to the SGH Citrix Servers 1 and 2.

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

From 26 June 2018, the attacker began querying the database from Citrix Server 2 using the A.A. account.

3 types of "**SQL**" queries which the attacker ran:

- (i) reconnaissance on the schema of the SCM database,
- (ii) direct queries relating to particular individuals, and
- (iii) bulk queries on patients in general.

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

The attacker was able to retrieve the following information from the SQL queries:

1. The Prime Minister's personal and outpatient medication data;
2. The demographic records of 1,495,364 patients, including their names, NRIC numbers, addresses, gender, race, and dates of birth;
3. The outpatient dispensed medication records of about 159,000 of the 1,495,364 patients mentioned in sub-paragraph (b) above.