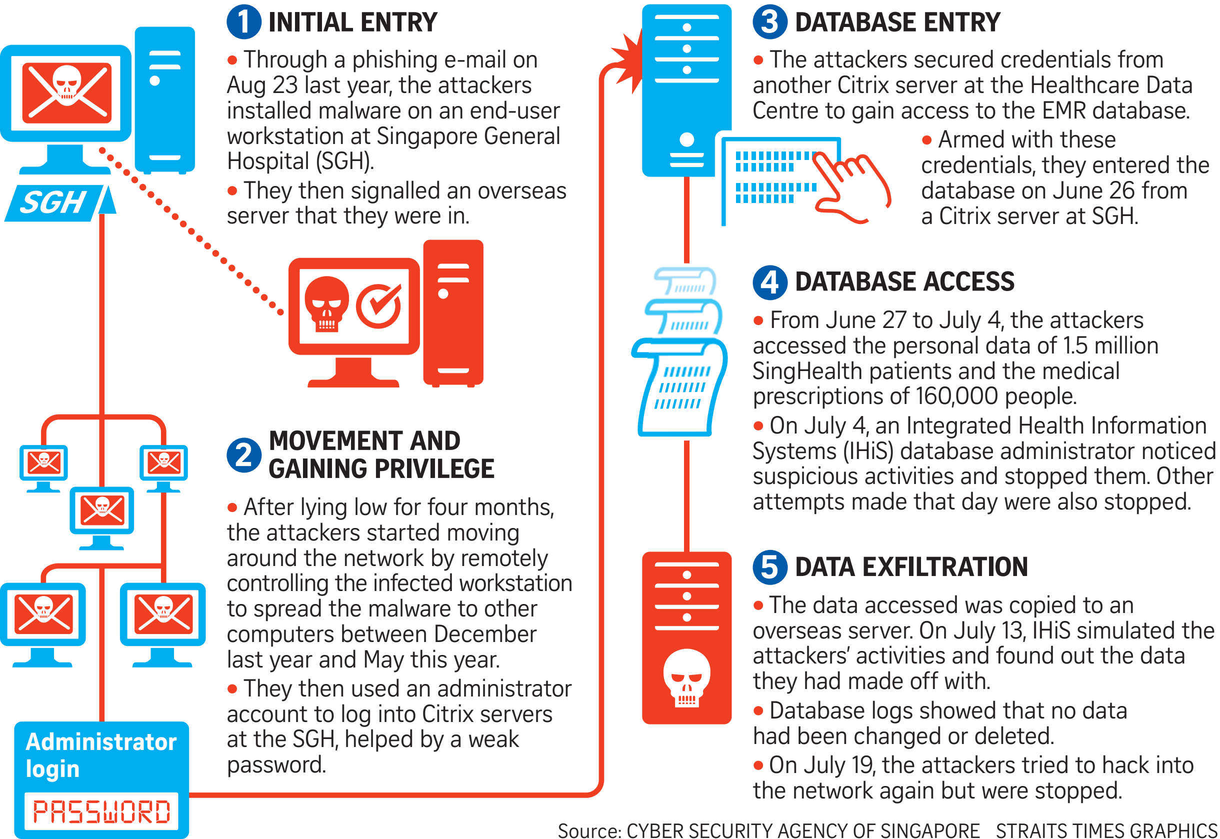
The cyber attack

Between June 27 and July 4, cyber attackers stole the personal data of 1.5 million SingHealth patients and the medical prescriptions of 160,000 people, including Prime Minister Lee Hsien Loong. Here is the route they took to access SingHealth's electronic medical records (EMR) database.



1 INITIAL ENTRY

- Through a phishing e-mail on Aug 23 last year, the attackers installed malware on an end-user workstation at Singapore General Hospital (SGH).
- They then signalled an overseas server that they were in.

2 MOVEMENT AND GAINING PRIVILEGE

- After lying low for four months, the attackers started moving around the network by remotely controlling the infected workstation to spread the malware to other computers between December last year and May this year.
- They then used an administrator account to log into Citrix servers at the SGH, helped by a weak password.

3 DATABASE ENTRY

- The attackers secured credentials from another Citrix server at the Healthcare Data Centre to gain access to the EMR database.
- Armed with these credentials, they entered the database on June 26 from a Citrix server at SGH.

4 DATABASE ACCESS

- From June 27 to July 4, the attackers accessed the personal data of 1.5 million SingHealth patients and the medical prescriptions of 160,000 people.
- On July 4, an Integrated Health Information Systems (IHiS) database administrator noticed suspicious activities and stopped them. Other attempts made that day were also stopped.

5 DATA EXFILTRATION

- The data accessed was copied to an overseas server. On July 13, IHiS simulated the attackers' activities and found out the data they had made off with.
- Database logs showed that no data had been changed or deleted.
- On July 19, the attackers tried to hack into the network again but were stopped.

Source: CYBER SECURITY AGENCY OF SINGAPORE STRAITS TIMES GRAPHICS