Singhealth Data Breach

(directly based on COI report)

Overview Diagram slide 5

Crisis in a Nutshell

- Between 23/8/17 -20/7/18, a cyberattack of unprecedented scale & sophistication was carried out on Singhealth patient database.
- DB was illegally accessed & personal particulars of 1.5 million patients, including names, NRIC numbers, addresses & dates of birth, were exfiltrated over the period of 27/6/18 to 4/7/18.
- Around 159,000 of these 1.5 million patients also had their outpatient dispensed medication records exfiltrated.
- The Prime Minister's personal and outpatient medication data was specifically targeted and repeatedly accessed.

Crisis in a Nutshell

- The crown jewels of the SingHealth network are the patient electronic medical records contained in the SingHealth "SCM" database.
- The SCM is an electronic medical records software solution, which allows healthcare staff to access real-time patient data.
- It can be seen as comprising front-end workstations, Citrix servers, and the SCM database.
- Users would access the SCM database via Citrix servers, which operate as an intermediary between front-end workstations & the SCM database.
- The Citrix servers played a critical role in the Cyber Attack.

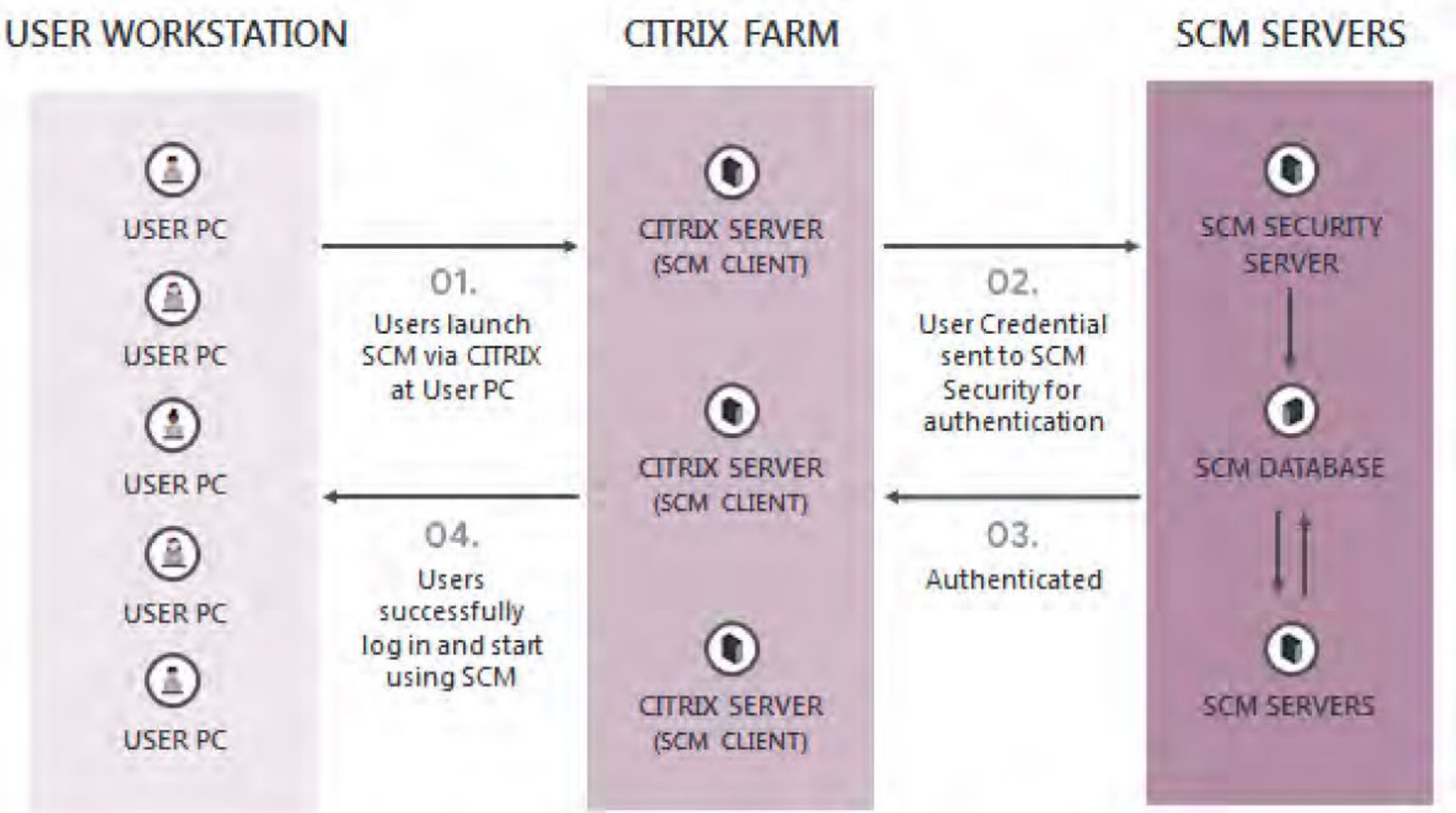
Crisis in a Nutshell

- At time of the Cyber Attack, SingHealth owns the SCM system.

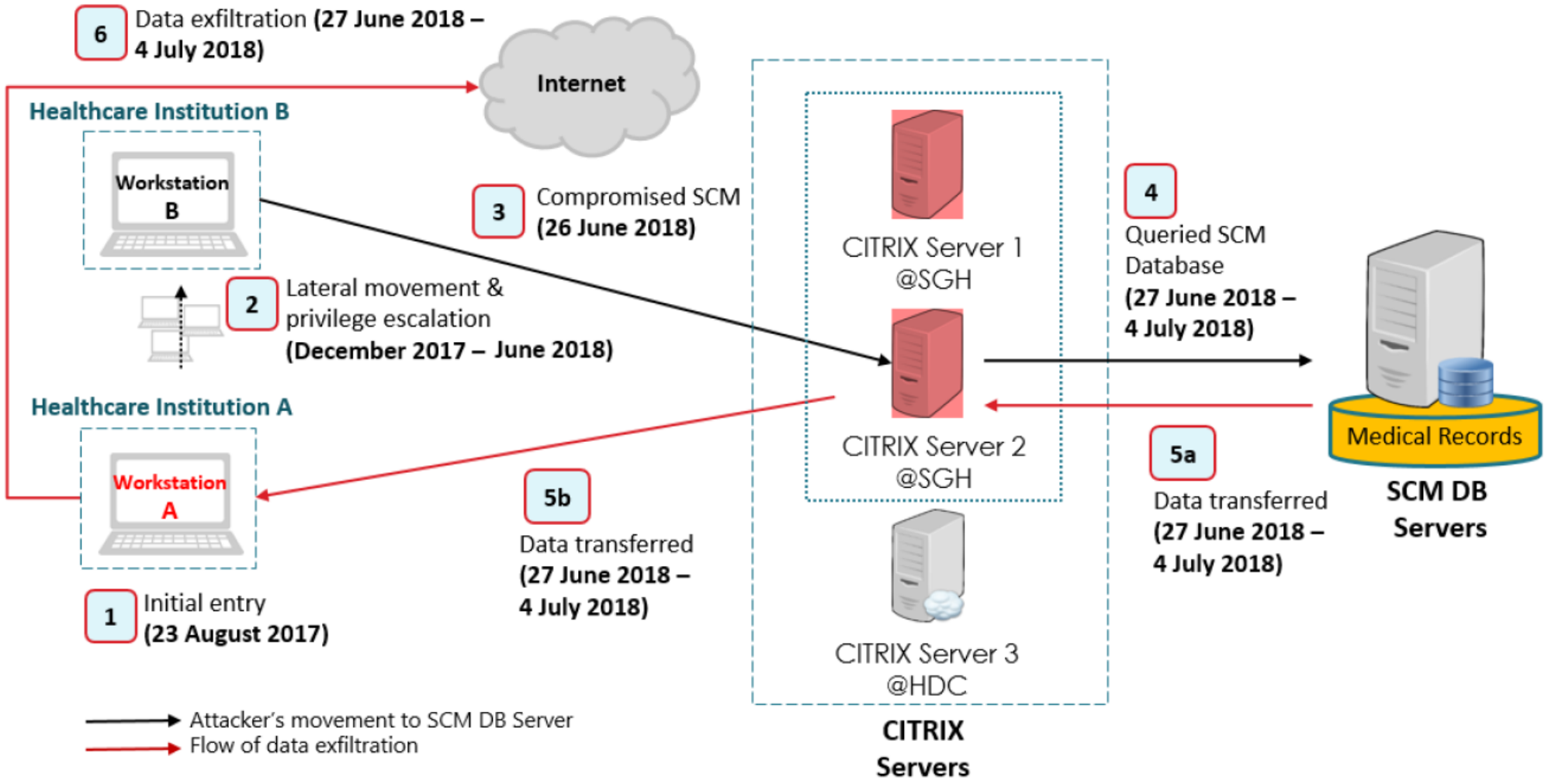
- Integrated Health Information Systems Private Limited ("IHiS") was responsible for administering and operating the system, including implementing cybersecurity measures.

- IHiS was also responsible for security incident response and reporting.

Figure 3:SingHealth user authentication process to access the SCM Database



Key Events of the Cyberattack -workflow



Summary of Key Events: 1

- The attacker gained initial access to SingHealth's IT network around 23/8/17, infecting front-end workstations, most likely through ***phishing attacks***.
- Attacker then lay dormant for 4 months, before commencing lateral movement (6 months) in the network between Dec2017 and Jun2018, compromising many endpoints and servers, including the Citrix servers located in SGH, which were connected to the SCM database.
- Along the way, the attacker also compromised a large number of user and administrator accounts.

Summary of Key Events: 2

- Starting from May 2018, the attacker made use of compromised user workstations in the SingHealth IT network and suspected virtual machines to remotely connect to the SGH Citrix servers.

Summary of Key Events: 3

- IHiS' IT administrators first noticed unauthorised logins to Citrix servers & failed attempts at accessing the SCM DB on 11 June 2018.

- On 27 June 2018, the attacker began querying the SCM database, stealing and exfiltrating patient records, and

- doing so undetected by IHiS.

Summary of Key Events: 4

- 1 Week later, on 4 July 2018, an IHiS administrator for the SCM system noticed suspicious queries being made on the SCM database.

- Working with other IT administrators, ongoing suspicious queries were terminated, and measures were put in place to prevent further queries to the SCM database.

- These measures proved to be successful, and the attacker could not make any further successful queries to the database after 4 July 2018.

Summary of Key Events: 5

- Between 11/6 & 9/7/18, the persons who knew of & responded to the incident were limited to IHiS' line-staff & middle management from various IT administration teams, & the security team.

- After 1 month, on 9/7/18, IHiS senior management were finally informed of the Cyberattack…

- 3 days later, 10/7/18, matter was escalated to Cyber Security Agency ("CSA"), SingHealth's senior management, the Ministry of Health ("MOH"), and the Ministry of Health Holdings ("MOHH")

Summary of Key Events: 6(*)

- Starting from 10 July 2018, IHiS and CSA carried out joint investigations and remediation.
- Several measures aimed at containing the
  - existing threat,
  - eliminating the attacker's footholds, and
  - preventing recurrence of the attack were implemented.

- In view of further malicious activities on 19 July 2018, internet surfing separation was implemented for SingHealth on 20 July 2018.
- No further suspicious activity was detected after 20 July 2018.

Summary of Key Events: 7

- The public announcement was made on 20 July 2018, and patient outreach and communications commenced immediately thereafter.
- SMS messages were used as the primary mode of communication, in view of the need for quick dissemination of information on a large scale.

- **COI Committee has identified 5 key Findings!**

KEY FINDING 1

- **IHiS staff did not have adequate levels of cybersecurity awareness, training, and resources**
  - **to appreciate the security implications of their findings and**
  - **to respond effectively to the attack.**

KEY FINDING 2

- **Certain IHiS staff holding key roles in IT security incident response and reporting**
  - **failed to take appropriate, effective, or timely action, resulting in missed opportunities to prevent the stealing and exfiltrating of data in the attack**

KEY FINDING 3

There were a number of vulnerabilities, weaknesses, and misconfigurations in the SingHealth network and SCM system that contributed to the attacker's success in obtaining and exfiltrating the data, many of which could have been remedied before the attack

KEY FINDING 4

The attacker was a skilled and sophisticated actor bearing the characteristics of an Advanced Persistent Threat group

Key Finding #4-1

1. The attacker had a clear goal in mind, namely the personal and outpatient medication data of PM in the main, and other patients.

2. The attacker employed advanced TTPs (tools/tactics, techniques, procedures), as seen from the suite of advanced, customised, and stealthy malware used, generally stealthy movements, and its ability to find and exploit various vulnerabilities in SingHealth's IT network and the SCM application.

Key Finding #4-2

3. The attacker was persistent, having established multiple footholds and backdoors, carried out its attack over a period of over 10 months, and made multiple attempts at accessing the SCM database using various methods.

4. The attacker was a well-resourced group, having an extensive command and control network, the capability to develop numerous customised tools, and a wide range of technical expertise.

KEY FINDING 5

While our cyber defences will never be impregnable, and it may be difficult to prevent an Advanced Persistent Threat from breaching the perimeter of the network, the success of the attacker in obtaining and exfiltrating the data was not inevitable

Key Notes

- Effective training methods to detect phishing must be conducted to all staff (Tutorial)
- Internet connections to our priced assets must be regulated, especially remote access when we are outside our company.
- Access to impt servers must have 2FA and shud not be by-passible
- Any coding vulnerability in the applications we used must be patched asap & we cannot rely on users to do so
- Strong passwords policy and enforcement (tutorial)
- Vulnerabilities highlighted in pen-tests etc must be fixed immediately.
- Inactive email accounts must be removed immediately to reduce attack surface area

Cyber Kill Chain Framework

- In considering the events of the Cyber Attack, it is useful to bear in mind the **7 Steps Cyber Kill Chain framework** developed by Lockheed Martin, which identifies what adversaries must complete in order to achieve their objectives, going through 7 stages starting from early reconnaissance to the final goal of data exfiltration.
- Having this framework in mind will facilitate understanding of the actions and the tactics, techniques and procedures ("**TTPs**") of the attacker in this case.


1
RECONNAISSANCE
Harvesting email addresses, conference information, etc.
2
WEAPONIZATION
Coupling exploit with backdoor into deliverable payload
3
DELIVERY
Delivering weaponized bundle to the victim via email, web, USB, etc.
4
EXPLOITATION
Exploiting a vulnerability to execute code on victim's system
5
INSTALL
INSTALLATION
Installing malware on the asset
6
COMMAND & CONTROL (C2)
Command channel for remote manipulation of victim
7
ACTIONS ON OBJECTIVES
With 'Hands on Keyboard' access, intruders accomplish their original goals

First evidence of breach and establishing control over Workstation A – August to December 2017

- Forensic investigations uncovered signs of callbacks to an overseas command & control server ("C2 server") from 23 August 2017.

- Callbacks refer to communications between malware and C2 servers, to either fetch updates and instructions, or send back stolen information.

First evidence of breach and establishing control over Workstation A – August to December 2017

- CSA discovered many malicious artefacts in Workstation A, including (i) a log file which was a remnant of a malware set;
- (ii) a publicly available hacking tool,
- (iii) a customised Remote Access Trojan referred to as "**RAT 1**".
  - (i) The log file was a remnant file from a known malware which has password dumping capability;
  - (iii) **RAT 1** provided the attacker with the capability to access and control the workstation, enabling the attacker to perform functions such as executing shell scripts remotely, and uploading and downloading files.

First evidence of breach and establishing control over Workstation A – August to December 2017

- (ii) The publicly available hacking tool enables an attacker to maintain a persistent presence once an email account has been breached, even if the password to the account is subsequently changed.

- Hacking tool also allows an attacker to
  - interact remotely with mail exchange servers,
  - perform simple brute force attacks on the user's email account password,
  - and serve as a hidden backdoor for the attacker to regain entry into the system in the event that the initial implants are removed;

First evidence of breach and establishing control over Workstation A – August to December 2017

- The log file was created on Workstation A on 29 August 2017. The file contained password credentials in plaintext, which appeared to belong to the user of Workstation A.

- The malware was likely to have been used by the attacker to obtain passwords for privilege escalation and lateral movement.

First evidence of breach and establishing control over Workstation A – August to December 2017

- Public hacking tool was installed on Workstation A on 1 Dec 2017 by exploiting a vulnerability in the version "**Outlook**" that was installed on the workstation.
- Although a patch was available at that time, but the patch was not installed on Workstation A then.
- The tool was thus successfully installed and was used to download malicious files onto Workstation A.
- Some of these files were masqueraded as .jpg image files, but in fact contained malicious PowerShell scripts, one of which is thought to be a modified PowerShell script taken from an open source post-exploitation tool.

First evidence of breach and establishing control over Workstation A – August to December 2017

- With the introduction of the hacking tool and RAT 1 in Dec 2017, the attacker gained the capability to execute shell scripts remotely, as well as to upload and download files to Workstation A.
- Referring to the Cyber Kill Chain framework referred to earlier, it can be seen that the attacker was able to go through the 'Delivery', 'Exploitation', 'Installation' and 'Command and Control' phases by 1 Dec 2017.

Privilege escalation and lateral movement – December 2017 to June 2018

- After the attacker established an initial foothold in Workstation A, it moved laterally in the network between December 2017 and June 2018,
  - compromising the Citrix servers located in SGH, which were connected to the SCM database.

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.

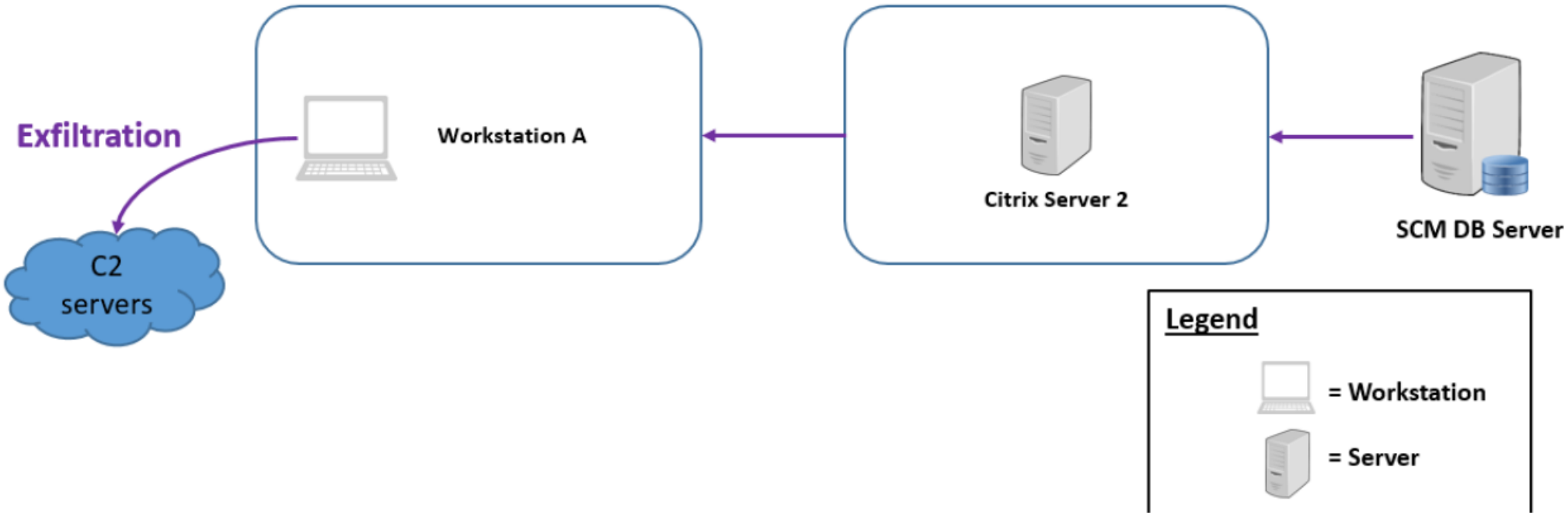
Queries to the SCM database from 26 June to 4 July 2018

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.

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

Figure 11: Data exfiltration route



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!

Lack of monitoring at the SCM database for unusual queries and access

From 26 June to 4 July 2018, attacker ran queries on the SCM database, including bulk queries. Attacker was able to do so unchallenged because of a lack of monitoring at the SCM database

- there were no existing controls to detect bulk queries being made to the SCM database.
- there were no controls in place at the time of the attack to detect or block any queries to the SCM database made using illegitimate applications.

Lack of monitoring at the SCM database for unusual queries and access

- database activity monitoring ("**DAM**") solutions available on the market which could address some or all of the three gaps highlighted above.
  - DAM was not implemented by IHiS at the time of the attack

SGH Citrix servers were not adequately secured against unauthorised access

The compromise of the SGH Citrix servers was critical in giving the attacker access to the SCM database.

- *Privileged Access Management was not the exclusive means for accessing the SGH Citrix servers, and logins to the servers by other means without 2-factor authentication were possible!*

- *IHiS Citrix administrators not only were aware of this alternative route, but made use of it for convenience!*

SGH Citrix servers were not adequately secured against unauthorised access

Lack of firewalls to prevent unauthorised remote access using RDP to the SGH Citrix servers

- RDP in cybersecurity stands for **Remote Desktop Protocol**. 
- It is a proprietary network communication protocol developed by **Microsoft** that enables a user to connect to and control another computer remotely over a network connection

Observations on the overall management of SGH Citrix servers

They were treated as not mission critical, unlike SCM database

- The SGH Citrix servers were not monitored for real-time analysis and alerts of vulnerabilities and issues arising from these servers.
- Vulnerability scanning, which was carried out for mission-critical systems, was not carried out for the SGH Citrix servers.
  - Vulnerability scanning is an inspection of the potential points of exploit on a computer to identify gaps in security.

Internet connectivity in the SingHealth IT network increased the attack surface

- The SingHealth network's connection to the Internet, while serving their operational needs, created an avenue of entry and exit for the attacker.
- This allowed the attacker to make use of an internet-connected workstation (Workstation A) to gain entry to the network, before making his way to the SCM database to steal the medical data.

Internet connectivity in the SingHealth IT network increased the attack surface

- The security risks arising from internet-connectivity in the SingHealth network were raised by CSA to MOH from as early as August 2015;
- By June 2017, the healthcare sector had determined, that
  - internet access would be removed for staff that did not require the internet for work,
  - for staff that required the internet for work, access would be through a secure internet access platform which, at that time, was to take the form of a 'remote browser'.

Versions of Outlook used by IHiS were not patched against a publicly available hacking tool

- The attacker was able to install the hacking tool (publicly available) on Workstation A on 1 December 2017 by exploiting a vulnerability in the version of the Outlook application installed on the workstation!

- A patch that was effective in preventing the vulnerability from being exploited (and thus to prevent the installation of the tool) was available since late-2017!

- Clear need to improve software upgrade policies!

Extensive C2 Infrastructure

CSA's forensic analysis revealed a number of network Indicators of Compromise ("**IOCs**") which appeared to be overseas C2 servers. CSA has explained that generally, the C2 servers were used for:

- Infection: where the server is used as a means of dropping malware into the system it is trying to infect;
- Data exfiltration: there were indications of technical data being sent to the servers; and
- Beacon: infected machines may have connected to C2 servers to establish a 'heartbeat', which refers to a slow, rhythmic communication meant just to sustain communications.

Actions of COI Committee

The Committee made 16 recommendations, 7 of which are priority ones, to be implemented immediately! They are

Recommendation #1: An enhanced security structure and readiness must be adopted by IHiS and Public Health Institutions

- Cybersecurity must be viewed as a risk management issue, and not merely a technical issue. Decisions should be deliberated at the appropriate management level, to balance the trade-offs between security, operational requirements, and cost.
- IHiS must adopt a "defence-in-depth" approach.
- Gaps between policy and practice must be addressed.

Recommendation #2: The cyber stack must be reviewed to assess if it is adequate to defend and respond to advanced threats

- Identify gaps in the cyber stack by mapping layers of the IT stack against existing security technologies.
- Gaps in response technologies must be filled by acquiring endpoint and network forensics capabilities.
- The effectiveness of current endpoint security measures must be reviewed to fill the gaps exploited by the attacker.
- Network security must be enhanced to disrupt the 'Command and Control' and 'Actions on Objective' phases of the Cyber Kill Chain.
- Application security for email must be heightened.

Recommendation #3: Staff awareness on cybersecurity must be improved, to enhance capacity to prevent, detect, and respond to security incidents

- The level of cyber hygiene among users must continue to be improved.
- A Security Awareness Programme should be implemented to reduce organisational risk.
- IT staff must be equipped with sufficient knowledge to recognise the signs of a security incident in a real-world context.

Recommendation #4: Enhanced security checks must be performed, especially on CII systems

- Vulnerability assessments must be conducted regularly.
- Safety reviews, evaluation, and certification of vendor products must be carried out where feasible.
- Penetration testing must be conducted regularly.
- Red teaming should be carried out periodically.
- Threat hunting must be considered.

Recommendation #5: Privileged administrator accounts must be subject to tighter control and greater monitoring

- An inventory of administrative accounts should be created to facilitate rationalisation of such accounts.
- All administrators must use two-factor authentication when performing administrative tasks.
- Use of passphrases instead of passwords should be considered to reduce the risk of accounts being compromised.
- Password policies must be implemented and enforced across both domain and local accounts.
- Server local administrator accounts must be centrally managed across the IT network.
- Service accounts with high privileges must be managed and controlled.

Recommendation #6: Incident response processes must be improved for more effective response to cyber attacks

- To ensure that response plans are effective, they must be tested with regular frequency.
- Pre-defined modes of communication must be used during incident response.
- The correct balance must be struck between containment, remediation, and eradication, and the need to monitor an attacker and preserve critical evidence.
- Information and data necessary to investigate an incident must be readily available.
- An Advanced Security Operation Centre or Cyber Defence Centre should be established to improve the ability to detect and respond to intrusions.

Recommendation #7: Partnerships between industry and government to achieve a higher level of collective security

- Threat intelligence sharing should be enhanced.
- Partnerships with Internet Service Providers should be strengthened.
- Defence beyond borders – cross-border and cross-sector partnerships should be strengthened.
- Using a network to defend a network – applying behavioural analytics for collective defence.

Additional 9 Recommendations

Recommendation #8: IT security risk assessments and audit processes must be treated seriously and carried out regularly

- IT security risk assessments and audits are important for ascertaining gaps in an organisation's policies, processes, and procedures.
- IT security risk assessments must be conducted on CII and mission-critical systems annually and upon specified events.
- Audit action items must be remediated.

Recommendation #9: Enhanced safeguards must be put in place to protect electronic medical records

- A clear policy on measures to secure the confidentiality, integrity, and accountability of electronic medical records must be formulated.
- Databases containing patient data must be monitored in real-time for suspicious activity.
- End-user access to the electronic health records should be made more secure.
- Measures should be considered to secure data-at-rest.
- Controls must be put in place to better protect against the risk of data exfiltration.
- Access to sensitive data must be restricted at both the front-end and at the database-level.

Recommendation #10: Domain controllers must be better secured against attack

- The operating system for domain controllers must be more regularly updated to harden these servers against the risk of cyber attack.
- The attack surface for domain controllers should be reduced by limiting login access.
- Administrative access to domain controllers must require two-factor authentication.

Recommendation #11: A robust patch management process must be implemented to address security vulnerabilities

- A clear policy on patch management must be formulated and implemented.
- The patch management process must provide for oversight with the reporting of appropriate metrics.

Recommendation #12: A software upgrade policy with focus on security must be implemented to increase cyber resilience

- A detailed policy on software upgrading must be formulated and implemented.
- An appropriate governance structure must be put in place to ensure that the software upgrade policy is adhered to.

Recommendation #13: An internet access strategy that minimises exposure to external threats should be implemented

- The internet access strategy should be considered afresh, in the light of the Cyber Attack.
- In formulating its strategy, the healthcare sector should take into account the benefits and drawbacks of internet surfing separation and internet isolation technology, and put in place mitigating controls to address the residual risks.

Recommendation #14: Incident response plans must more clearly state when and how a security incident is to be reported

- An incident response plan for IHiS staff must be formulated for security incidents relating to Cluster systems and assets.
- The incident response plan must clearly state that an attempt to compromise a system is a reportable security incident.
- The incident response plan must include wide-ranging examples of security incidents, and the corresponding indicators of attack.

Recommendation #15: Competence of computer security incident response personnel must be significantly improved

- The Computer Emergency Response Team must be well trained to more effectively respond to security incidents.
- The Computer Emergency Response Team must be better equipped with the necessary hardware and software.
- A competent and qualified Security Incident Response Manager who understands and can execute the required roles and responsibilities must be appointed.

Recommendation #16: A post-breach independent forensic review of the network, all endpoints, and the SCM system should be considered

- IHiS should consider working with experts to ensure that no traces of the attacker are left behind.