MINISTRY OF HEALTH
SINGAPORE

MH 6:01/5 MOH Advisory No. 08/2021

25 August 2021

See Distribution List

CYBERSECURITY ADVISORY 08/2021 – REMAINING VIGILANT OF CYBERSECURITY ATTACKS

The Ministry of Health (MOH) was recently alerted to a ransomware attack which affected a clinic's medical records and database. The affected clinic had discovered that its IT systems had been breached as clinic staff were unable to access its servers to enter into its clinic management system (CMS) to provide medical care, and stacks of ransomware notes were found printed at their network printers.

RANSOMWARE

2. Ransomware is a form of malware designed to encrypt files on a device. Threat actors typically demand a ransom from the victim to decrypt the files. Some ransomware variants are also capable of spreading to other systems, devices and machines on the same network[1]. Ransomware may spread through several ways, including phishing emails that contain malicious links or attachments, and vulnerabilities in the web browser. Ransomware may also be distributed through other methods such as brute force attacks, exploitation of insecure Remote Desktop Protocols (RDPs), unpatched Virtual Private Networks (VPN) and spam campaigns.

3. Ransomware can disrupt or deny normal computer operations, steal information, or gain unauthorised access to data and systems. In severe cases, ransomware can result in malicious alteration of patient's health records, cripple healthcare and administrative services, and has a direct implication to the healthcare provider's reputation.

PROTECTION AGAINST RANSOMWARE

4. Prevention is paramount to prevent falling victim to a ransomware incident. Healthcare institutions are strongly encouraged to read the preventive measures on the Cyber Security Agency of Singapore (CSA)'s updated advisory "Protect your

[1] Source: Singapore Computer Emergency Response Team (SingCERT)

Ministry of Health, Singapore
College of Medicine Building
16 College Road
Singapore 169854
TEL (65) 6325 9220
FAX (65) 6224 1677
WEB www.moh.gov.sg

Systems and Data from Ransomware Attacks" dated 20 August 2021[2] (**Annex A**), and take appropriate measures to secure their computer infrastructure and systems, and protect the data. These include measures such as (i) updating applications, systems and software, (ii) enabling spam email filters, and (iii) reviewing settings on exposed ports, as ransomware commonly comes through vectors such as unpatched applications, systems and software, phishing emails, and exploiting open ports. It is also essential that healthcare institutions formulate a backup and recovery plan for their critical data and keep the backup data offline.

5. Healthcare institutions should remain vigilant of the constant and evolving cybersecurity threats and be aware of the signs to look out for to determine if you have been hacked. Institutions should also continue to exercise strong oversight of technology risks in your arrangements with third party service providers to ensure the security and integrity of your IT systems, medical devices, and patient medical records. **If you are a user of any CMS, please also actively check and review that your systems are continually secured.**

6. Institutions should also better protect their businesses by instituting baseline cybersecurity measures found in the **Healthcare Cybersecurity Essentials (HCSE)**, which has been issued to all PHMC-licensed institutions earlier on 6 Aug 2021. The guidelines set out twelve (12) key recommendations covering IT asset management, technical, process, and people aspects, to help providers improve their cybersecurity posture. Refer to **Annex B** for the previously issued circular and guidelines. Institutions are also encouraged to visit https://www.moh.gov.sg/licensing-and-regulation/cybersecurity-for-healthcare-providers for more information and resources.

STEPS TO TAKE DURING A CYBER-ATTACK INVOLVING RANSOMWARE

7. If your institution has been infected with ransomware, SingCERT recommends the following steps to aid response and recovery:

a) **Disconnect the infected computer immediately from your network**. Doing so isolates the infected system and prevents the ransomware from spreading to other computers. If several systems appear impacted, take the network offline at the switch level. If taking the network temporarily offline is not immediately possible, locate the network (e.g., Ethernet) cable and unplug affected devices from the network or remove them from Wi-Fi to contain the infection;
b) **Scan and disinfect the computer** with an updated anti-virus or anti-malware application;
c) **Go to https://www.nomoreransom.org/ to check if there is a decryptor available for it**; and

[2] https://www.csa.gov.sg/singcert/Advisories/ad-2020-006

Ministry of Health, Singapore
College of Medicine Building
16 College Road
Singapore 169854
TEL (65) 6325 9220
FAX (65) 6224 1677
WEB www.moh.gov.sg

d) **Perform data restoration from the backup sources**. Most types of ransomware create some form of persistence in the infected computer and may re-encrypt data if not properly removed. As such, be sure to perform data restoration on a clean installation that is completely free of the malware.

8. Institutions should also consider the need to immediately engage a third-party security vendor and/or their respective CMS vendor where relevant, to investigate the attack, highlight any security lapses or gaps, and subsequently remediate and fortify your systems where relevant. Institutions are also recommended to **proactively inform affected individuals** of any data leakage that may potentially compromise patient's confidentiality, and to also **consider proactively issuing a media statement** if the impact of the potential data breach is extensive and severe.

9. It is imperative that institutions also ensure that patient care and care continuity are not impacted by the disruption to business operations due to the ransomware attack. This includes reporting data breaches and cyber incidents promptly and **executing business continuity plans** so that normal service operations can continue while remediating your IT systems. Institutions should also raise cybersecurity awareness among staff who access systems and data through suitable training programmes that cover topics such as password security, logging out of applications and websites, using only trusted connections and sites, as well as staying informed and being aware of suspicious activities.

10. MOH **strongly discourages institutions from paying the ransom**. Paying the ransom does not guarantee that the encrypted data and systems will be decrypted, or that the threat actor will not publish any exfiltrated data. Doing so may instead encourage and embolden threat actors to continue their attacks on other institutions.

11. If you have been or suspect that you have been a victim of a ransomware attack, please report the incident to the following authorities immediately:

a) **SingCERT** at https://www.csa.gov.sg/singcert/reporting
b) **MOH Health Regulation Group** at eLIS@moh.gov.sg
c) **Singapore Police Force (SPF)** at https://eservices.police.gov.sg/
d) **Personal Data Protection Commission (PDPC)** at https://eservice.pdpc.gov.sg/case/db if the breach is likely to result in significant harm to affected individuals to whom the information relates OR if the breach is of a significant scale involving personal data of 500 or more individuals

12. Please ensure you disseminate the contents of this advisory to all staff in your institutions who should be aware and be kept up-to-date, so as to ensure that they know the steps to take in any suspected cyberattack.

Ministry of Health, Singapore
College of Medicine Building
16 College Road
Singapore 169854
TEL (65) 6325 9220
FAX (65) 6224 1677
WEB www.moh.gov.sg

13. For any further queries, please contact us at eLIS@moh.gov.sg.

Thank you.

ADJ ASSOC PROF (DR) RAYMOND CHUA
DEPUTY DIRECTOR OF MEDICAL SERVICES (HEALTHCARE REGULATION GROUP) & ASSISTANT COMMISSIONER (CYBERSECURITY)
MINISTRY OF HEALTH

MR LIONEL LEE
MINISTRY CHIEF INFORMATION SECURITY OFFICER
MINISTRY OF HEALTH

Distribution List

All PHMC-licensed institutions
Executive Director, Secretariat of Healthcare Professional Boards
CEO, Integrated Health Information Systems
CEO, Health Promotion Board
CEO, Health Sciences Authority
CEO, Agency for Integrated Care
Chief of Medical Corps, MINDEF
Chief Medical Officer, Home Team, MHA
Chief Medical Officer, Emergency Medical Services Department, SCDF
Director, Medical, ACE Group, MOM

Ministry of Health, Singapore
College of Medicine Building
16 College Road
Singapore 169854
TEL (65) 6325 9220
FAX (65) 6224 1677
WEB www.moh.gov.sg

Annex

Annex A	Protect Your Systems and Data From Ransomware Attacks Accessible from CSA at https://www.csa.gov.sg/singcert/Advisories/ad-2020-006
Annex B	MOH Circular No. 105/2021 Circular to all PHMC-licensed Institutions – Healthcare Cybersecurity Essentials (HCSE) 6 August 2021

Ministry of Health, Singapore
College of Medicine Building
16 College Road
Singapore 169854
TEL (65) 6325 9220
FAX (65) 6224 1677
WEB www.moh.gov.sg

Annex A

Ministry of Health, Singapore
College of Medicine Building
16 College Road
Singapore 169854
TEL (65) 6325 9220
FAX (65) 6224 1677
WEB www.moh.gov.sg

Annex B

Ministry of Health, Singapore
College of Medicine Building
16 College Road
Singapore 169854
TEL (65) 6325 9220
FAX (65) 6224 1677
WEB www.moh.gov.sg