THE STRAITS TIMES

Nearly 73,500 patients' data affected in ransomware attack on eye clinic in S'pore

Servers and several computer terminals at the clinic's Camden branch were affected, but its IT system at the Novena branch was not. PHOTO: EYE & RETINA SURGEONS

Kenny Chee
Senior Tech
Correspondent

UPDATED AUG 26, 2021, 7:18 AM

SINGAPORE - A ransomware attack earlier this month has affected the personal data and clinical information of nearly 73,500 patients of a private eye clinic, the third such reported incident in a month.

The information included names, addresses, identity card numbers, contact details and clinical information such as patients' clinical notes and eye scans, said Eye & Retina Surgeons (ERS) on Wednesday (Aug 25).

But the clinic said it has not paid any ransom, adding that no credit card or bank account information was accessed or compromised.

The Ministry of Health (MOH) said that the clinic's compromised IT systems are not connected to the ministry's IT systems, such as the National Electronic Health Record, and there have been no similar cyber attacks on MOH's IT systems.

The ministry added that it has asked ERS to investigate the incident, carry out a thorough review of its systems and work with the Cyber Security Agency (CSA) to "take immediate mitigating actions to strengthen its cyber defences".

The police, the Personal Data Protection Commission – which said it is seeking more information from ERS – and CSA have been informed of the incident.

ERS is also working with CSA and MOH to investigate the root causes of the attack and, together with security experts, is also trying to identify potential areas the company can better secure.

The clinic said in a statement that it uses "reputable and established external IT service providers to advise on and maintain its IT systems, and subscribes to appropriate anti-virus and other protective software, which is regularly updated".

ERS added that its IT system has been restored securely, and its IT providers have completed a thorough check of the clinic's system, reformatted servers and run anti-virus scans on all computer terminals.

Measures will be taken to prevent the breach from recurring, ERS said.

ERS had fallen prey to a sophisticated ransomware cyber attack by hackers on Aug 6. Such attacks usually involve locking up data until victims pay the hackers.

Servers and several computer terminals at the clinic's Camden branch were affected, but its IT system at the Novena branch was not.

While no data has been leaked publicly for now, the clinic said that it will monitor the situation closely.

ERS said that for data security reasons, it maintains active medical records separately on a cloud-based system, so they were not accessed or compromised in the cyber attack. Clinical operations were not affected too.

The clinic said it is now in the process of informing patients of the cyber attack.

"ERS regrets this breach and wishes to assure its patients that it takes patient confidentiality very seriously," the clinic said, adding that it will continue to do everything it can to protect and secure patient information.

MORE ON THIS TOPIC

Tough fight looms against ransomware 'epidemic'

Five facts about ransomware attacks

The attack is the latest in a series of ransomware attacks reported in the past month.

On Aug 16, insurer Tokio Marine Insurance Singapore said it was hit by a ransomware attack.

It said at the time that there was no indication of a breach of customer information nor confidential information of the Tokio Marine Group.

On Aug 19, The Business Times reported that Singapore-based tech company Pine Labs fell victim to ransomware too. The firm is a Temasek-backed payments platform.

Hackers were said to have stolen confidential documents between Pine Labs and several Indian banks, and held the information hostage.

Cyber-security experts said that ransomware is a growing threat. CSA figures showed that ransomware cases in Singapore surged 154 per cent from 2019's 35 cases to hit 89 last year.

The healthcare, government and banking industries have the biggest targets on their backs, said Mr Eric Nagel, cyber-security firm Cybereason's general manager for the Asia-Pacific.

Mr Jeffrey Kok, cyber-security firm CyberArk's vice-president of solution engineers for the Asia-Pacific and Japan, warned that hackers are increasingly targeting specific organisations.

Cyber crooks are pooling resources, conducting lengthy reconnaissance, and targeting people with direct access to critical assets and systems using social engineering tactics, he said.

MORE ON THIS TOPIC

Global increase in mobile malware but smartphone security lax in S'pore

More than 57,000 StarHub customers' personal data leaked

There are steps organisations can take to protect themselves.

On Tuesday, CSA, PDPC and the police offered advice on guarding against hacking group Altdos, which has been known to use a “double extortion” technique on victims.

The group is said to steal data from a victim’s servers and might later lock the data up.

Altdos will then demand payment from the victim, threatening to publish the data if the ransom is not paid.

It will also sometimes ask a victim to pay a separate ransom to decrypt its locked files.

The hacking group operates mainly in South-east Asia and Bangladesh. In Singapore, it is known to have targeted furniture retailer Vhive and consumer electronics retailer Audio House.

If a ransomware attack occurs, the Singapore authorities advise organisations not to pay the ransom and instead report the incident to public agencies.

“Paying the ransom does not guarantee that the data will be decrypted or that your data will not be published by threat actors,” CSA, PDPC and the police said.

“It also encourages the threat actors to continue their criminal activities and target more victims. Threat actors may also see your organisation as a soft target and may strike again in the future.”

MORE ON THIS TOPIC

It doesn't pay to pay ransom to hackers: Study

More Singapore businesses hit by ransomware attacks

To reduce the risks of being attacked by Altdos, the Singapore authorities recommend the following to organisations:

- Regularly patch software;

- Review logs regularly, like those for server access, to check for malicious activities;

- Segregate networks to limit communications between Internet-facing services and internal servers such as those containing sensitive data;

- Routinely back up important files to external and offline storage devices;

- Deploy Web application firewalls to filter malicious network traffic;

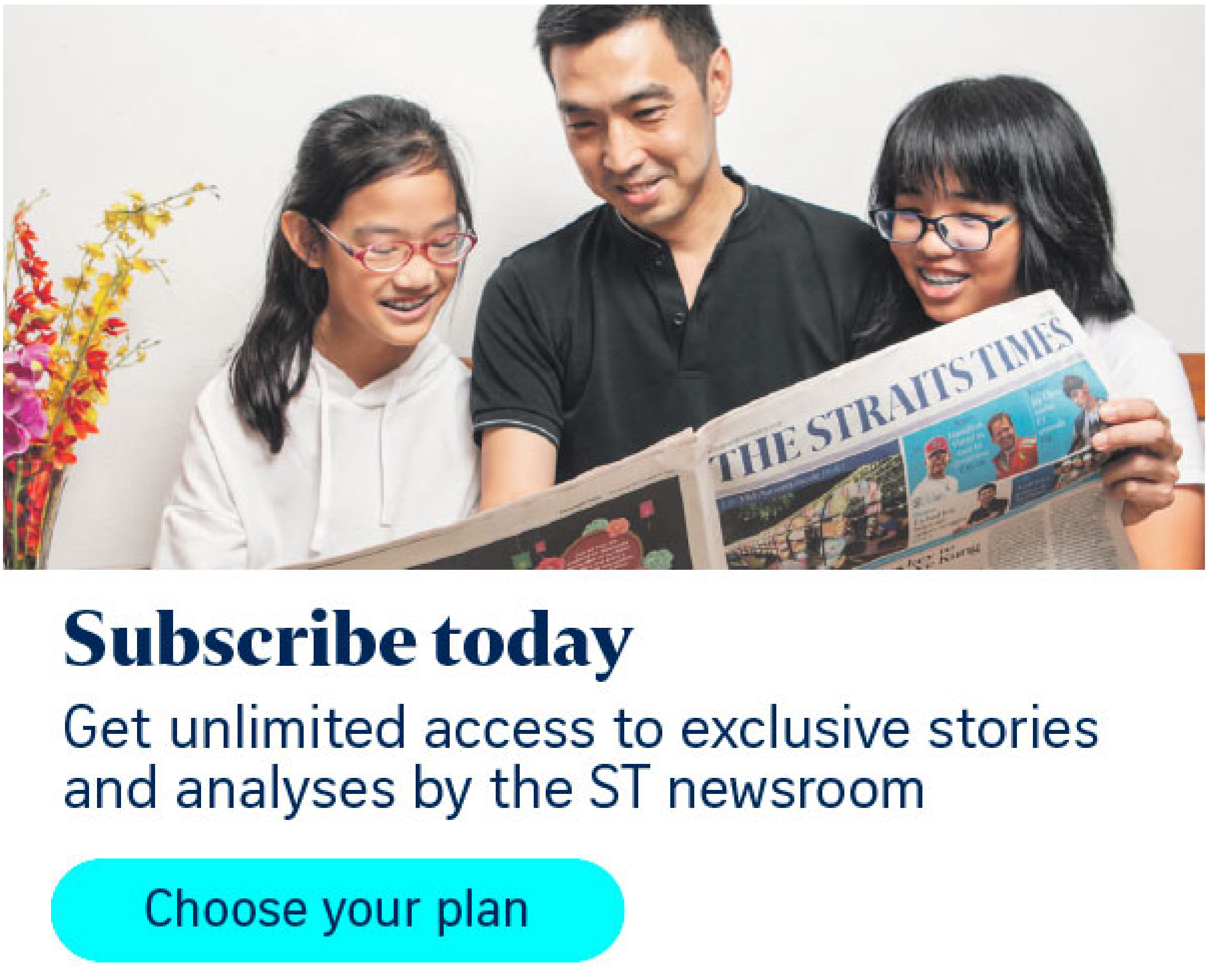
- Seek external help, such as hiring a professional firm, when an attack has been confirmed, or to regularly test systems for security holes.

MORE ON THIS TOPIC

askST: What can I do if my personal information has been hacked?

Victim of $813 million cyber attack offers its hacker a job

Join **ST's Telegram channel here** and get the latest breaking news delivered to you.


Subscribe today
Get unlimited access to exclusive stories and analyses by the ST newsroom
Choose your plan

E-paper
Podcasts
Facebook
RSS Feed