(Pullar-Strecker, T., 2021)

Ransomware attack: Waikato DHB supporting patients after documents dumped online

Tom Pullar-Strecker • 17:08, Jun 29 2021

LIBBY WILSON/STUFF

Waikato DHB is not yet back to normal after May cyberattack, Health Minister says.

Waikato District Health Board is contacting patients whose personal information has now been dumped online following a ransomware attack in May, Health Minister Andrew Little says.

Little promised “a full, independent inquiry” into what appears to be the country’s most serious cyberattack, during an emergency debate in Parliament.

Stuff learnt on Tuesday morning that documents appearing to be from Waikato DHB had been published on the dark web.

The list of documents suggested it included folders containing patient information as well as information about employees and the DHB’s financial affairs. *Stuff* has not accessed the data to verify the contents.

More from Stuff:
* **'Presumed human remains' found in wreck of Titanic-bound sub Titan**
* **Madonna 'rushed to hospital after being found unresponsive'**

Brett Callow, a threat consultant with Nelson-based cybersecurity firm Emsisoft, said the information appeared to have been dumped by an organisation called Vice Society that may also have been known as HelloKitty.

Little confirmed the document dump.

MORE FROM
TOM PULLAR-STRECKER · SENIOR BUSINESS JOURNALIST
tom.pullar-strecker@stuff.co.nz

“I want to acknowledge the patients and staff whose information was held by the Waikato DHB who have now had that information compromised,” he told Parliament.

Waikato DHB had a system in place to contact patients to let them know the nature and extent of information about them that had been compromised, he said.

The DHB was working with victims to provide them with necessary support, he said.

“In addition, people, are entitled to go to the Office of the Privacy Commissioner and exercise their rights under the Privacy Act.”

Little said cyberattacks were “the reality of the world”, noting Ireland’s health service had also suffered a huge ransomware attack days before Waikato DHB discovered it had been attacked.

SUPPLIED

A partial list of the Waikato DHB document dump.

The DHB was still recovering from the May attack, he said.

Many systems are back online but there was “no question it is not back to normal yet”, he said.

The DHB has been approached for comment.

Little promised an inquiry once the DHB had recovered.

“There will be – because there has to be – an appropriate independent inquiry into the state of the system before the ransomware attack and the quality of the response to it,” he said.

“Only at that point will we have an understanding about the extent to which that system was vulnerable, or whether it was a DHB that had done everything expected of it,” he said.

Little previously made clear that the DHB would not pay a ransom to the criminals who hacked it.

ROBERT KITCHIN/STUFF

Health Minister Andrew Little has promised a full and thorough independent inquiry, down the track.

National Party communications spokeswoman Melissa Lee voiced strong support for that stance.

“I applaud the Government for not bowing down,” she said.

But Lee questioned whether it had sufficiently funded cybersecurity given how common attacks had become.

“Why did this Government not boost cybersecurity resilience through its Budget process?” she said.

Australia had done that with an A$1.6 billion (NZ$1.7b) budget boost this year, she said.

Callow said the threat of releasing the data was used as additional leverage to force payment.

“Organisations in this situation are without good options,” he said. “They’ve had a data breach and, whether they pay or not, that cannot be undone.”

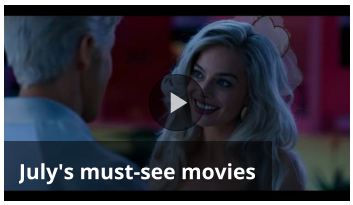
Emsisoft had no insight on who may have created HelloKitty ransomware or where they might be based, he said.

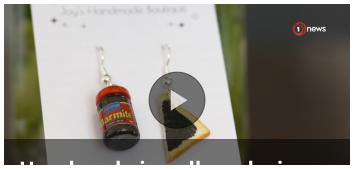
The software had no cryptographic vulnerabilities, he said.

“Consequently, the only way to recover encrypted files is to restore them from backups or pay the demand.”

Callow is among a growing number of cybersecurity professionals who have called for governments to ban the payment or facilitation of cybersecurity ransoms to try to make attacks less profitable, and has described the current state of affairs as a “feeding frenzy” for criminals.

latest video





Stuff Puna

more from stuff

sport

national

sport