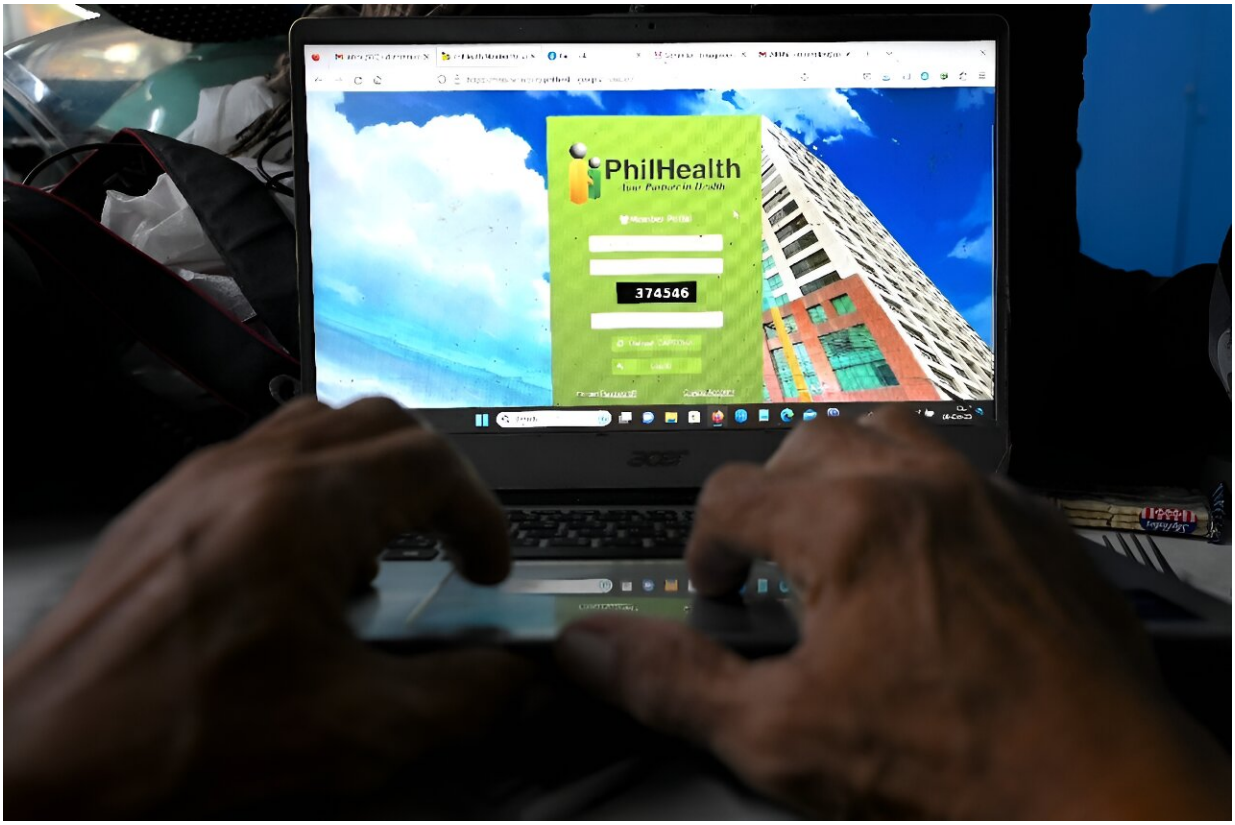
Philippines health insurer hacked: What we know

October 9 2023, by Pam Castro, with Qasim Nauman in Seoul



Hackers have stolen hundreds of gigabytes of data from PhilHealth, the national insurer of the Philippines.

Hackers have stolen the personal data of potentially millions of people from the Philippines's national health insurer, which has urged members

to change their passwords after the "staggering" cyberattack.

The hackers have started releasing files including confidential memos from the stolen data to pressure the government into paying a $300,000 ransom.

Here is what we know so far about the attack, which was discovered by the Philippine Health Insurance Corporation (PhilHealth) on September 22:

What did the hackers steal?

PhilHealth and the government have yet to say exactly how many people have been impacted, but the insurer warned members in a notice that data such as addresses, phone numbers and insurance IDs was compromised.

As of June 30, according to its website, PhilHealth had more than 59 million direct and indirect contributors—more than half the population of the Philippines.

PhilHealth asked members to monitor credit card transactions and change passwords, especially for financial services.

Separately, employee information was also stolen from the targeted computers.

The hackers released some of the data on the dark web, showing health memos and other information that a top government official described as confidential.

An investigation into the scale of the attack is ongoing, but the National Privacy Commission has described the amount of data stolen as

"staggering".

Who are the hackers, and what do they want?

The Philippine government has referred to the attackers as the Medusa group, who have demanded $300,000 to restore access to PhilHealth computers and delete the stolen data.

MedusaLocker, first detected in late 2019, has been used to mainly target health care organizations and its creators took particular advantage of the emergency situation during the COVID-19 pandemic, according to a US government report.

The ransomware has been sold to criminal actors, and a US government cybersecurity advisory said its creator receives a cut of any ransom.

It was not clear if the Medusa group identified by the Philippines government is the creator of or an entity that purchased MedusaLocker.

How did they get the data?

On September 22, PhilHealth staff were unable to access a number of computers, which displayed a message saying hackers had locked the machines and encrypted the data.

The insurer shut down the affected systems to try and stop the attack from spreading, slowing or entirely shutting down some online services for days.

The government has so far not said exactly how hackers got access to the computers.

But in interviews with local media last week, senior PhilHealth official

Israel Pargas said the insurer did not have an antivirus software at the time of the attack.

How has the government responded?

With a blunt 'No'. The Philippines does not pay ransom in any criminal cases, including cyberattacks, officials have said.

However, with hackers releasing more data from the stolen files, calls have grown for the government to conduct an audit of its cyber defenses.

The National Privacy Commission said Saturday it has started an investigation into any potential lapses and data law violations by PhilHealth.

The NPC said its analysis of 734 GB of stolen data revealed "sensitive personal data", and warned the public that anyone who downloads this information could face criminal charges.

Citation: Philippines health insurer hacked: What we know (2023, October 9) retrieved 9 May 2024 from https://techxplore.com/news/2023-10-philippines-health-hacked.html