FEATURED

Ookla unveils top performers for Q1 in global internet connectivity and consistency

TECHNOLOGY

PhilHealth under siege: Medusa group demands US$300,000, threatens to leak data

DICT officials and cybersecurity teams rally to counteract the menace

BY ART SAMANIEGO

Sep 23, 2023 06:41 PM

AT A GLANCE

- The Medusa ransomware group has executed a sophisticated attack on PhilHealth, compromising sensitive data and exposing select samples online,

underscoring the emergent and serious nature of this cyber threat.

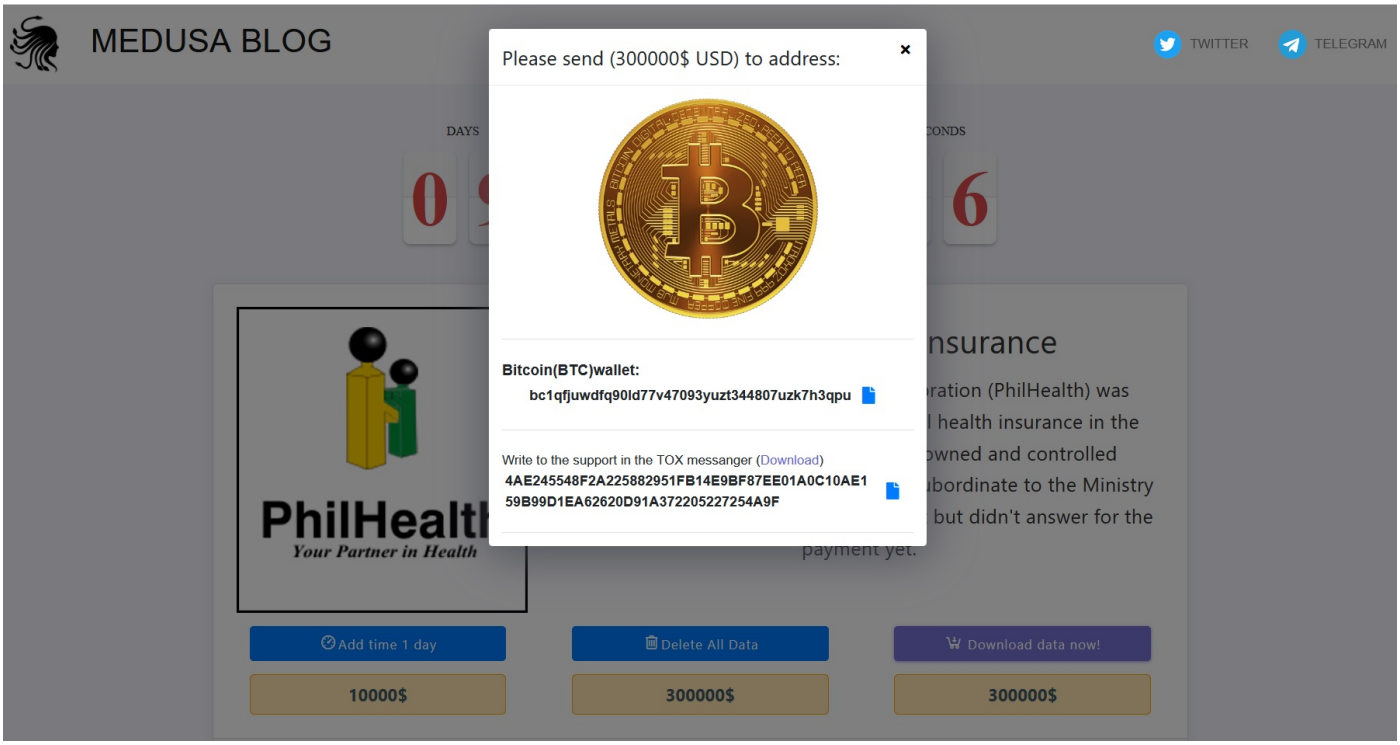
- Medusa has demanded a ransom of $300,000, threatening to release the entirety of the stolen PhilHealth data online if the ransom is not paid, highlighting the significant financial implications of such cyber threats.

- The compromised data includes confidential information of Filipinos such as names, addresses, contact information, and medical records, as well as internal memos and memoranda from PhilHealth officers, signifying the extensive range of data vulnerable to such attacks.

- The Philippine government, steadfast in its resolve, has denied any intentions to pay the ransom, and PhilHealth is collaboratively working with the DICT and other relevant agencies to recover the stolen data and ensure the culprits are brought to justice, indicating a united front against cybercrime.

- The exposure of such sensitive data poses significant risks, including identity theft and fraud, emphasizing the need for PhilHealth members to enhance their vigilance against phishing emails, monitor credit reports, and secure online accounts through strong passwords and two-factor authentication, reflecting the broader call to action for individuals in the face of rising cyber threats.

The Medusa ransomware group has made the PhilHealth data available online for US$300,000. The group's blog entry shows PhilHealth data with more than 31 pages of sample files.



The data, which includes the personal information of Filipinos, was stolen in a ransomware attack on PhilHealth recently. The Medusa ransomware group has threatened to release the data online if PhilHealth does not pay the ransom.

A security professional involved in recovering the Philhealth data has denied that the government agency plans to pay the ransom. Philhealth is working with the DICT and other relevant agencies to recover the data and bring the perpetrators to justice.

When Technews asked Jeffrey Ian Dy, Undersecretary for Connectivity, Cybersecurity, and Upskilling at the Department of Information and Communications Technology (DICT), about the incident, he said, "The National Computer Emergency Response Team (NCERT) of DICT, our outsourced providers, and Philhealth are working round the clock to restore the Philhealth systems. The ransomware has been contained. We don't see the malware moving laterally to other computers in Philhealth. Pending other due diligence checks, we can confidently advise Philhealth to resume online services in the next few days."

Releasing the PhilHealth data online would be a significant blow to the Philippines as the data includes sensitive information such as names, addresses, contact information, and medical records. It also contains internal memos and memoranda from officers of Philhealth. If the data is released, it could be used for identity theft, fraud, and other criminal activity.

The Medusa ransomware group is relatively new, but it has quickly become one of the most feared ransomware groups in the world. The group is known for its sophisticated attacks and willingness to target large organizations.

The group's name is derived from the Greek mythological figure Medusa, who was known for her ability to turn people to stone with her gaze. The Medusa ransomware group uses a similar tactic to extort money from its victims: it encrypts their data and threatens to release it online if they do not pay the ransom.

If you are a Philhealth member, you can take the following steps to protect yourself from the potential consequences of the release of the PhilHealth data:

Be vigilant about phishing emails and other scams. Phishing emails are designed to trick people into revealing their personal information or clicking on malicious links. If you receive an email that claims to be from PhilHealth or another government agency, be sure to verify the sender's identity before clicking on any links or opening any attachments.

Monitor your credit report for any suspicious activity. If you see any unauthorized charges or other signs of fraud, contact your bank or credit card company immediately.

Be careful about what information you share online. Avoid sharing personal information on social media or other websites. If you need to share personal information, do so on a secure website.

Use strong passwords and enable two-factor authentication on all of your online accounts.

RELATED STORIES