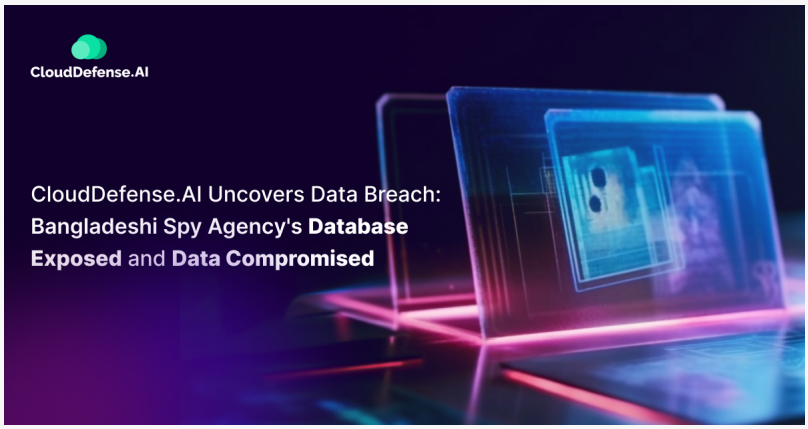
CloudDefense.AI Discovers Major Data Breach: NTMC Database Exposes Bangladeshi Citizens' Sensitive Information

CloudDefense.AI's cybersecurity researcher, Viktor Markopoulos, has uncovered a data breach of Bangladesh's National Telecommunications Monitoring Center (NTMC)



PALO ALTO, CALIFORNIA, UNITED STATES, November 17, 2023 /EINPresswire.com/ -- The research by Viktor uncovered an exposed database lying on the internet, which then went on to be hijacked by hackers due to a delay in action from the victim organization's side.

The compromised NTMC database contained 120 indexes with various logs, exposing citizens' calls and internet activities. Real citizen information, including call metadata, was compromised.

> This data breach is a serious reminder of the importance of cybersecurity"
>
> *Anshu Bansal, CEO of CloudDefense.AI*

Viktor reported the breach on November 8, but before the NTMC could secure the database, it was accessed by hackers who wiped the data and demanded a ransom payment of 0.01 bitcoins (Approximately $360).

The exposed database contained information about Bangladeshi citizens, including names, professions, parents' names, and more sensitive information such as their phone numbers, exam details, vehicle registration numbers, phone IMEI numbers, passport details, and biometric data, including fingerprints.

Although most of the data were identified to be test entries, it still helps to predict the structure of data the agency collects and the motive behind it. In between, there was data on real individuals, which was confirmed by contacting the victims. Jeremiah Fowler, Co-founder of Security Discovery, expressed his concerns over the various IMEI numbers available on the database. These numbers could easily be used to clone or track existing devices.

Investigation revealed the breach was caused by a myriad of flaws, including misconfiguration in NTMC's system, lack of access controls, and strong encryption methods. Viktor expressed concern over the intelligence agency being careless about the sensitive information of their country's citizens. He noted that they continued to use the database even after it was reported to them that it was exposed.

Countries like Bangladesh do not follow strict data protection regulations like those available in the EU or the US. This incident highlights the need for organizations to implement robust cybersecurity measures and strict adherence to industry security standards. CloudDefense.AI emphasizes the importance of fine-grained access controls and offers advanced security solutions. Read our blog to know more about this incident.

CloudDefense.AI offers an all-in-one suite of security solutions to prevent and detect data breaches. These solutions include Hacker's VIew™ for vulnerability detection and Cloud Security Posture Management (CSPM) to take care of misconfigurations. CloudDefense.AI urges all organizations to implement strong access controls, use data encryption, and regularly scan for misconfigurations. The company also recommends that organizations educate their employees about cybersecurity risks and best practices.

If you want hands-on experience with our industry-leading cybersecurity solutions, book a free demo with us here.

Emily Thompson
CloudDefense.AI
media@clouddefense.ai
Visit us on social media:
Facebook
Twitter
LinkedIn
YouTube