NBA's Houston Rockets Face Cyber-Attack by Ransomware Group

https://www.bloomberg.com/news/articles/2021-04-14/nba-s-houston-rockets-face-cyber-attack-by-ransomware-group?utm_source=google&utm_medium=bd&cmpId=google

By Kartikay Mehrotra

April 14, 2021

The Houston Rockets of the National Basketball Association are investigating a cyber-attack against their networks from a relatively new ransomware group that claims to have stolen internal business data.

The Rockets confirmed the attempted intrusion. Tracey Hughes, a spokesperson for the team, said the attack hasn't impacted operations.

"It appears that the unknown actors attempted to install ransomware on certain internal systems at the Rockets," Hughes said in a statement. "However, our internal security tools prevented ransomware from being installed except for a few systems that have not impacted our operations."

Ransomware is a type of malicious code that typically encrypts a victim's data. The hackers then demand a ransom to decrypt the information. More recently, ransomware gangs have also stolen data and threatened to make it public unless the victim pays a fee.

In this case, it's unclear if the attackers encrypted any of the basketball team's networks.

But the hacking group, which goes by the name Babuk, claims on its dark web page to have stolen 500 gigabytes of Rockets' data -- including contracts, non-disclosure agreements and financial data -- and is threatening to publish it if the team declines to pay.

Hughes, the Rockets spokesperson, said the team is aware of the hackers' claims but didn't comment on their veracity or the scope of the compromise.

The extortion ad on Babuk's dark web page was removed on Wednesday.

Babuk is just the latest hacking group to use pages on the dark web to try to publicly extort victims into paying ransom demands.

Babuk was discovered early this year and has already compromised at least "five big enterprises," including one victim who paid as much as $85,000 after negotiations, according to security researchers at McAfee Inc. The

group advertises on both English-speaking and Russian-speaking dark web forums, focusing on the Russian sites to recruit affiliates and distribute its malware.