News Corp discloses hack from "persistent" nation state cyber attacks

bleepingcomputer.com/news/security/news-corp-discloses-hack-from-persistent-nation-state-cyber-attacks/

Ax Sharma

By
[Ax Sharma](#)

- February 4, 2022
- 09:03 AM
- [0](#)

Image: News Corp/BleepingComputer

American media and publishing giant News Corp has disclosed today that it was the target of a "persistent" cyberattack.

The attack discovered sometime this January, reportedly allowed threat actors to access emails and documents of some News Corp employees, including journalists.

News Corp's major properties include Fox News, The Wall Street Journal, New York Post, and News UK.

Hack disclosed via securities filing

In a Securities & Exchange Commission (SEC) filing seen by BleepingComputer today, News Corp shared that one of its systems had been subject to "persistent cyberattack activity."

The attack was discovered this January but it isn't until today that the news conglomerate has publicly disclosed the attack, albeit quietly via a filing rather than a data breach notice.

Preliminary findings indicate the attackers are associated with a "foreign government" and that some data exfiltration did occur.

Although there is no indication so far of customer or financial data held by the company being affected, News Corp has engaged an external cybersecurity company, Mandiant, to assist with the investigation.

"In January 2022, the Company discovered that one of these systems was the target of persistent cyberattack activity. Together with an outside cybersecurity firm, the Company is conducting an investigation into the circumstances of the activity to determine its nature, scope, duration and impacts. The Company's preliminary analysis indicates that foreign government involvement may be associated with this activity, and that data was taken. To the Company's knowledge, its systems housing customer and financial data were not affected. The Company is remediating the issue, and to date has not experienced any related interruptions to its business operations or systems. Based on its investigation to date, the Company believes the activity is contained. At this time, the Company is unable to estimate the expenses it will incur in connection with its investigation and remediation efforts."

Possibly linked to China-backed threat actors

WSJ who first reported on the incident states the breach affected major news arms of the conglomerate including The Wall Street Journal, New York Post, and the company's U.K. news operation.

According to WSJ's report, the incident allowed threat actors to access emails and documents of some News Corp employees, including journalists.

A statement provided by Mandiant explains that the cyber attack is possibly linked to China-backed threat actors.

"Mandiant assesses that those behind this activity have a China nexus, and we believe they are likely involved in espionage activities to collect intelligence to benefit China's interests," says David Wong, vice president of incident response at Mandiant.

While disclosing further risks to its IT infrastructure, News Corp stressed, the cyber risk insurance policy it has in place may not be sufficient "to cover all losses from any breaches" that have occurred or may occur in the future.

"Cyber risk insurance has also become more difficult and expensive to obtain, and the company cannot be certain that its current level of insurance or the breadth of its terms and conditions will continue to be available on economically reasonable terms," states News Corp in its quarterly filing.

Related Articles:

Hackers target Russian govt with fake Windows updates pushing RATs

General Motors credential stuffing attack exposes car owners info

Ransomware attack exposes data of 500,000 Chicago students

Chinese 'Space Pirates' are hacking Russian aerospace firms

Engineering firm Parker discloses data breach after ransomware attack

Ax Sharma

Ax Sharma is a Security Researcher and Tech Reporter. His works and expert analyses have frequently been featured by leading media outlets including Fortune, Business Insider, The Register, TechRepublic, etc. Ax's expertise lies in vulnerability research, malware analysis, and open source software. He's an active community member of the OWASP Foundation, Open Source Security Foundation (OpenSSF), and the British Association of Journalists (BAJ). Send any tips via email or Twitter DM.