News Corp. hacked, reporters targeted; believed China-linked

February 4 2022, by Eric Tucker and Frank Bajak

The News Corporation headquarters building is seen Aug. 1, 2017, in New York. News Corp, publisher of The Wall Street Journal, said Friday, Feb. 4, 2022, that it had been hacked and had data stolen from journalists and other employees, and a cybersecurity firm investigating the intrusion said Chinese intelligence-gathering was believed behind the operation. Credit: AP Photo/Richard Drew, File

News Corp., publisher of The Wall Street Journal, said Friday that it had been hacked and had data stolen from journalists and other employees, and a cybersecurity firm investigating the intrusion said Chinese intelligence-gathering was believed behind the operation.

The Journal, citing people briefed on the intrusion, reported that it appeared to date back to February 2020 and that scores of employees were impacted. It quoted them as saying the hackers were able to access reporters' emails and Google Docs, including drafts of articles.

News Corp., whose publications and businesses include the New York Post and Journal parent Dow Jones, said it discovered the breach on Jan. 20. It said customer and financial data were so far not affected and company operations were not interrupted.

But the potential impact on news reporting and sources was a serious concern. News organizations are prime targets for the world's intelligence agencies because their reporters are in constant contact with sources of sensitive information. Journalists and newsrooms from Mexico and El Salvador to Qatar, where Al-Jazeera is based, have been hacked with powerful spyware.

Mandiant, the cybersecurity firm examining the hack, said in a statement that it "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."

The timing of News Corp.'s announcement, including in a regulatory filing Friday, coincided with the opening of the Winter Olympics in Beijing, to which foreign athletes and journalists were advised to bring "burner" phones and sanitized laptops to protect against cyberespionage.

In the regulatory filing, News Corp. said it had discovered in January

that one of its technology providers was "the target of persistent cyberattack activity." It did not elaborate.

In an email to staff, News Corp. said the hack "affected a limited number" of email accounts and documents from News Corp. headquarters, News Technology Services, Dow Jones, News UK, and New York Post.

"Our preliminary analysis indicates that foreign government involvement may be associated with this activity, and that some data was taken," the email said. "Our highest concern is the protection of our employees, including our journalists, and their sources," it added, saying it believed the "threat activity is contained."

FBI Director Christopher Wray said in a speech this week that the bureau opens investigations tied to suspected Chinese espionage operations about every 12 hours, and has more than 2,000 such probes. He said Chinese government hackers have been pilfering more personal and corporate data than all other countries combined.

While state-backed Russian hacking tends to get more headlines, U.S. officials say China has been stealthily stealing far more valuable commercial and personal data over the past few decades as digital technology took hold.

Major newsrooms, including The New York Times, against which a Chinese cyberespionage operation was uncovered in 2013, have previously been compromised.

Runa Sandvik, former senior director of information security at the newspaper, said that while major newsrooms have shown a lot of progress in the last few years in helping their journalists navigate an increasingly hostile digital world, those efforts are not adequate to

defend against a skilled and determined adversary like China.

A spokesperson for the Chinese embassy in Washington did not explicitly deny Beijing's involvement in the hack, but said in a statement Friday evening that "China firmly opposes and combats cyber attacks and cyber theft in all forms."

The reported onset of the News Corp. hack—February 2020—coincides with Beijing's revocation of press credentials of three Journal reporters based in the Chinese capital in what China's Foreign Ministry said was punishment for an opinion piece the newspaper published.

News Corp.'s assets also includes the publishing house HarperCollins, News Corp. Australia and Storyful, which the email to employees said were apparently not targeted by the hackers.

—

The story has been corrected to say that the hacking of Al-Jazeera took place in Qatar.