Twitter, Washington Post targeted by hackers

February 3 2013, by Anne D'innocenzio

In this Sept. 14, 2010 file photo, Twitter CEO Evan Williams makes a presentation about changes to the social network at Twitter headquarters in San Francisco, In the latest online attack, Twitter says hackers may have gained access to information on 250,000 of its more than 200 million active users, Friday, Feb. 1, 2013. (AP Photo/Marcio Jose Sanchez, File)

Social media giant Twitter is among the latest U.S. companies to report that it is among a growing list of victims of Internet security attacks, saying that hackers may have gained access to information on 250,000 of its more than 200 million active users. And now, The Washington Post is joining the chorus, revealing the discovery of a sophisticated cyberattack in 2011.

Twitter said in a blog post on Friday it detected attempts to gain access to its user data earlier in the week. It shut down one attack moments after it was detected.

But Twitter discovered that the attackers may have stolen user names, email addresses and encrypted passwords belonging to 250,000 users they describe as "a very small percentage of our users." The company reset the pilfered passwords and sent emails advising the affected users.

The Twitter attack comes on the heels of recent hacks into the computer systems of U.S. companies, including The New York Times and The Wall Street Journal. Both newspapers reported this week that their computer systems had been infiltrated by China-based hackers, likely to monitor media coverage the Chinese government deems important.

On Friday, The Washington Post disclosed in an article published on its website that it was also the target of a sophisticated cyberattack, which was discovered in 2011 and was first reported by an independent cybersecurity blog. Washington Post spokeswoman, Kris Coratti, didn't offer any details including the duration of the attack or the origins. But according to sources that the newspaper quoted, who it said spoke on condition of anonymity, the intruders gained access as early as 2008 or 2009. According to the sources, Chinese hackers are also suspected.

Coratti couldn't be reached immediately for comment by The Associated Press. According to her comments made to the newspaper, the company

worked with security company Mandiant to "detect, investigate and remediate the situation promptly at the end of 2011."

China has been accused of mounting a widespread, aggressive cyber-spying campaign for several years, trying to steal classified information and corporate secrets and to intimidate critics. The Chinese foreign ministry could not be reached for comment Saturday, but the Chinese government has said those accusations are baseless and that China itself is a victim of cyberattacks.

Twitter didn't provide any clues as to whether it believes that China was behind its hack. However, the blog post by the company's director of information security, Bob Lord, made clear that the hackers knew what they were doing. Lord said in the blog that the attack "was not the work of amateurs, and we do not believe it was an isolated incident."

"The attackers were extremely sophisticated, and we believe other companies and organizations have also been recently similarly attacked," Lord said. "For that reason we felt that it was important to publicize this attack while we still gather information, and we are helping government and federal law enforcement in their effort to find and prosecute these attackers to make the Internet safer for all users."

Reached on Saturday, Twitter spokesman Jim Prosser had no further comment.

Based on the few details released about the Twitter and Washington Post attacks it's hard to say whether Chinese hackers were involved, said Rich Mogull, CEO of Securosis, an independent security research and advisory firm. There are certain pieces of malicious software that are characteristic to Chinese hackers, he said, but "the problem is not enough has been made public."

One theory is that the Twitter hack happened after an employee's home or work computer was compromised through vulnerabilities in Java, a commonly used computing language whose weaknesses have been well publicized. Independent privacy and security researcher Ashkan Soltani said such a move would give attackers "a toehold" in Twitter's internal network, potentially allowing them either to sniff out user information as it traveled across the company's system or break into specific areas, such as the authentication servers that process users' passwords.

The relatively small number of users affected suggests that attackers weren't on the network long or that they were only able to compromise a subset of the company's servers, Soltani said.

Twitter is generally used to broadcast messages to the public, so the hack might not immediately have yielded any important secrets. But the stolen credentials could be used to eavesdrop on private messages or track which Internet address a user is posting from.

That might be useful, for example, for an authoritarian regime trying to keep tabs on a journalist's movements.

"More realistically, someone could use that as an entry point into another service," Soltani said, noting that since few people bother using different passwords for different services, a password stolen from Twitter might be just as handy for reading a journalist's emails.