In Yahoo breach, hackers may seek intelligence, not riches

23 September 2016, by Brandon Bailey

In this June 5, 2014, file photo, people walk in front of a Yahoo sign at the company's headquarters in Sunnyvale, Calif. Yahoo says the personal information of 500 million accounts have been stolen in a massive security breakdown that represents the latest setback for the beleaguered internet company. The breach disclosed on Thursday, Sept. 22, 2016, dates back to late 2014. Yahoo is blaming the hack on a "state-sponsored actor." (AP Photo/Marcio Jose Sanchez, File)

If a foreign government is behind the massive computer attack that compromised a half billion user accounts at Yahoo, as the company says, the breach could be part of a long-term strategy that's aimed at gathering intelligence rather than getting rich.

Yahoo says the breach involved users' email addresses, passwords and other information—including birthdates—but not payment card or bank account numbers. Although the stolen data could still be used in financial crimes, such as identity theft, experts say a foreign intelligence agency might combine the Yahoo files with information from other sources to build extensive dossiers on U.S. government or corporate officials in sensitive positions.

"With state-sponsored attacks, it's not just financial information that's of value," said Lance Hoffman, co-director of the Cyberspace Security and Privacy Institute at George Washington University. "In the long run, if the state accumulates a lot of information on you, and especially if it corroborates that with other sources, it can assemble a pretty good profile."

Governments have also been known to hack email accounts to keep tabs on their own citizens or dissidents. Experts believe that was one motive behind a 2010 hacking of Google Gmail accounts used by Chinese human rights activists.

Yahoo hasn't revealed the evidence that led it to blame a "state-sponsored actor" for the latest attack, which the Sunnyvale, California, company said occurred two years ago and was discovered only in recent weeks.

Some analysts warn that "state sponsored" can be a vague term. It might also be an easy excuse to deflect blame for a company's own security lapses, by suggesting it had no hope of defeating hackers who had all the resources of a government intelligence agency behind them, warned Gunter Ollmann, chief security officer at Vectra Networks, a San Jose, California, security firm.

Yahoo declined comment, but its top security official, Bob Lord, has said the company would make that claim only "when we have a high degree of confidence." In a policy statement last year, Lord also said the company wouldn't release details about why it believes attacks are state-sponsored because it doesn't want to risk disclosing its methods of investigating breaches.

This wouldn't be the first time that governments were implicated in high-profile hacking attacks.

U.S. officials have hinted that China might be to blame for a 2015 breach at the U.S. Office of

Personnel Management, in which background files and even fingerprints of millions of federal employees were stolen. China denied any official involvement. More recently, news reports say U.S. intelligence officials have blamed Russian spies for the hack of Democratic National Committee files, although Russia's government has also denied this.

Some security experts believe the OPM attack was carried out by the same hackers who also stole data files from large U.S. insurance and health-care companies in 2014 and 2015. It may have been part of an effort to gather sensitive or compromising information to blackmail or coerce individuals working at a variety of federal agencies.

Hackers could also use such personal information to concoct bogus emails and send them to a person's Yahoo account, in what might be a sophisticated "phishing" scheme aimed at getting the target to click on a link containing "spyware" or other malicious computer code.

"They'd have the ability to conduct targeted phishing attacks against individuals with potentially valuable information, without going through their government email accounts," said Tim Erlin, senior director of security and risk strategy at Tripwire, a cyber-security firm.

Similarly, governments might want to target executives at multi-national corporations, especially if they're competing with companies based in the country that sponsored the attacks. In such cases, intelligence officials might share useful commercial secrets with their home-grown industries, said Jeremiah Grossman, an official at SentinelOne, a Silicon Valley computer security firm. He noted that the 2010 attack on Google was blamed on Chinese hackers who also targeted U.S. companies outside the tech industry.

In any event, security experts warn that the Yahoo breach could still put ordinary users at risk, particularly if the hacked information finds its way to online marketplaces where stolen data are bought and sold. Many people use the same email address and password for a variety of online services, where they might also have provided financial information such as credit card numbers. And hackers with access to a Yahoo email account could try to reset passwords for other services, if a user registered for those accounts with a Yahoo address.