

Yahoo pressed to explain huge 'state sponsored' hack

23 September 2016



Yahoo believes that information associated with at least 500 million user accounts was stolen

Yahoo faced pressure Friday to explain how it sustained a massive cyber-attack—one of the biggest ever, and allegedly state-sponsored—allowing hackers to steal data from half a billion users two years ago.

The US online giant said its probe concluded that "certain user account information was stolen" and that the attack came from "what it believes is a state-sponsored actor."

The comments come after a report earlier this year quoted a security researcher saying some 200 million accounts may have been accessed and that hacked data was being offered for sale online.

"Yahoo is working closely with law enforcement on this matter," said Yahoo, adding it believes data linked to at least 500 million user accounts was stolen—in what could be the largest-ever breach for a single organization.

Yahoo said the stolen information may have included names, email addresses, birth dates, and scrambled passwords, along with encrypted or

unencrypted security questions and answers that could help hackers break into victims' other online accounts.

While there is no official record of the largest breaches, many analysts have called the Myspace hack revealed earlier this year as the largest to date, with 360 million users affected.

In 2014 a US firm specialised in discovering breaches said that a Russian group has hacked 1.2 billion usernames and passwords belonging to more than 500 million email addresses.

The firm, Hold Security, gave no details of the companies affected by the hack.

Ammunition for hackers

Computer security analyst Graham Cluley said the stolen Yahoo data "could be useful ammunition for any hacker attempting to break into Yahoo accounts, or interested in exploring whether users might have used the same security questions/answers to protect themselves elsewhere on the web."

He noted that while Yahoo said that it believes the hack was state-sponsored, the company provided no details regarding what makes them think that is the case.

"If I had to break the bad news that my company had been hacked... I would feel much happier saying that the attackers were 'state-sponsored,'" rather than teen hackers, Cluley said in a blog post.

University of Notre Dame associate teaching professor and data security specialist Timothy Carone told AFP that the Yahoo hack fit the "big picture" when it comes to cyberattacks launched by spy agencies in Russia, China, North Korea or other countries.

"It just smacks of traditional trade craft," Carone said.

Chinese hackers have been accused of everything from stealing corporate secrets to an enormous breach of US government personnel files that affected a staggering 21.5 million people and reportedly led Washington to pull its intelligence operatives out of China.

North Korea is known to operate an army of thousands of elite hackers accused of launching crippling cyber-attacks on South Korean organisations and officials over the years.

But it was the high-profile hacking attack on Sony Pictures in December 2014 that shed light on the growing threat of the North's hacking capability, although Pyongyang denied responsibility for the attacks.

It appeared that looted Yahoo data did not include unprotected passwords or information associated with payments or bank accounts, the Silicon Valley company said.

Yahoo is asking affected users to change passwords, and recommending anyone who has not done so since 2014 to take the same action as a precaution.

Users of Yahoo online services were urged to review accounts for suspicious activity and change passwords and security question information used to log in anywhere else if it matched that at Yahoo.

"Online intrusions and thefts by state-sponsored actors have become increasingly common across the technology industry," Yahoo said in a statement.

"Yahoo and other companies have launched programs to detect and notify users when a company strongly suspects that a state-sponsored actor has targeted an account."

Yahoo being bought

Confirmation of the major cyber breach comes two months after Yahoo sealed a deal to sell its core

internet business to telecom giant Verizon for \$4.8 billion, ending a two-decade run as an independent company.

It was not immediately clear if the data breach could impact the closing of the deal or the price agreed by Verizon.

"Frankly, the timing couldn't be worse for Yahoo," Cluley said.

The telecom firm said it was reviewing the new information.

"Within the last two days, we were notified of Yahoo's security incident," Verizon said in a statement.

"We will evaluate as the investigation continues through the lens of overall Verizon interests, including consumers, customers, shareholders and related communities."

© 2016 AFP

APA citation: Yahoo pressed to explain huge 'state sponsored' hack (2016, September 23) retrieved 9 December 2021 from <https://phys.org/news/2016-09-yahoo-huge-state-sponsored-hack.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.