Yahoo hack shows data's use for information warfare (Update)

December 15 2016

The latest Yahoo hacking is the largest on record and comes just months after the internet giant disclosed a separate breach of data from 500 million users

The 2013 hack affecting a billion Yahoo users shows how seemingly innocuous bits of data gleaned from cyber attacks can be exploited for espionage and information warfare, as well as for profit.

The breach, disclosed Wednesday, is the largest on record and comes

just months after Yahoo disclosed a separate attack in 2014 affecting data from 500 million users.

On the surface, the trove of data is "a bunch of junk," said John Dickson of the security consultancy Denim Group.

But the ability to create a searchable database with data tidbits such as birth dates and phone numbers makes it enormously valuable to hackers seeking to make a profit or engage in industrial or state espionage, he said.

"If you're trying to research and get information about a target, you're going to use everything you can find," said Dickson, a former officer in the Air Force Information Warfare Center.

The Yahoo hack did not collect credit card or Social Security numbers, according to the company, leading some analysts to speculate that the goals were not financial.

"For someone using data as a weapon, this is of tremendous value," said Steve Grobman, chief technical officer at Intel Security.

Information warfare?

James Scott, a senior fellow at the Institute for Critical Infrastructure Technology, a cybersecurity think tank, said that while details are still unknown, the attack could fuel disinformation campaigns by governments.

Scott noted that the data had not appeared for sale on Deep Web markets—that is, in murky corners of the web that cannot be reached by standard search engines.

"And since a significant number of victims (if any) have not reported identity theft resulting from the incident, there is a strong likelihood that the breach was not conducted for monetary gain," Scott said.

"This could indicate that the breach was an espionage stage of an information warfare effort."

The disclosure of the breach comes amid intense scrutiny of cybersecurity in the US election campaign and of the potential impact of hacked email accounts from people close to Democratic presidential candidate Hillary Clinton.

US officials have claimed Russia was behind the attack aimed at disrupting the election.

One of the hacks was a Gmail account of Clinton campaign chairman John Podesta. Media reports say he or an assistant was fooled by a fake email that prompted him to reveal his password.

Security analysts say such attacks are often preceded by lengthy data-gathering campaigns that might look for personal information such as a birth date or former school or university.

Signs of a state actor

Yahoo said it was not clear who was behind the billion-user hack but that some evidence pointed to "the same state-sponsored actor" believed responsible for the previously disclosed cyber attack.

The security firm InfoArmor said in September that its analysis of the first breach indicated "professional" hackers stole the Yahoo data, and only later sold it to a state entity.

InfoArmor said at the time that the breach "opens the door to significant opportunities for cyber espionage and targeted attacks to occur."

Grobman said some attackers may mix real data with manipulated information to distort facts, creating further confusion and mistrust.

"One of the things we are concerned about is that the public is conditioned to see leaked data as legitimate, and this data can be manipulated," Grobman said.

Some analysts argue that the hackers' goals may be more financial than political.

Security researcher Graham Cluley said certain bits of information such as phone numbers could be of value to criminals.

"If a hacker or scammer has your telephone number, they can ring you up and trick you into believing they are an organization you already have a relationship with, which means that you might be tempted to hand over more personal information," Cluley said in a YouTube posting.

'A lot of money'

James Lewis, a senior fellow specializing in cybersecurity at the Center for Strategic and International Studies, said new analytics tools can sift through databases for political espionage purposes, but that it is not clear if Russia has those capabilities.

"If you're a criminal, you would think you could monetize a billion accounts," Lewis said. "Even if you got a penny or a dime for each, you would still be making a lot of money."

The attacks also pose a threat to the future of Yahoo, the former internet

star which has seen its fortunes decline and is in the process of selling its main assets to telecom group Verizon.

Dickson said that it's likely that "Verizon is doing a double take" on the $4.8 billion deal.

"If this kills that deal, I think it will increase the focus on cybersecurity hygiene across the board," he said.