Password breach could have ripple effects well beyond Yahoo

September 27 2016, by Raphael Satter

This Jan. 14, 2015 file photo shows Yahoo's headquarters in Sunnyvale, Calif. As investors and investigators weigh the damage of Yahoo's massive breach to the internet icon, information security experts worry that the record-breaking haul of password data could be used to open locks up and down the web. While it's unknown to what extent the stolen data has been or will be circulating, giant breaches can send ripples of insecurity across the internet. (AP Photo/Marcio Jose Sanchez, File)

As investors and investigators weigh the damage of Yahoo's massive

breach to the internet icon, information security experts worry that the record-breaking haul of password data could be used to open locks up and down the web.

While it's unknown to what extent the stolen data has been or will be circulating, giant breaches can send ripples of insecurity across the internet.

"Data breaches on the scale of Yahoo are the security equivalent of ecological disasters," said Matt Blaze, a security researcher who directs the Distributed Systems Lab at the University of Pennsylvania, in a message posted to Twitter .

A big worry is a cybercriminal technique known as "credential stuffing," which works by throwing leaked username and password combinations at a series of websites in an effort to break in, a bit like a thief finding a ring of keys in an apartment lobby and trying them, one after the other, in every door in the building. Software makes the trial-and-error process practically instantaneous.

Credential stuffing typically succeeds between 0.1 percent and 2 percent of the time, according to Shuman Ghosemajumder, the chief technology officer of Mountain View, California-based Shape Security. That means cybercriminals wielding 500 million passwords could conceivably hijack tens of thousands of other accounts.

"It becomes a numbers game for them," Ghosemajumder said in a telephone interview.

So will the big Yahoo breach mean an explosion of smaller breaches elsewhere, like the aftershocks that follow a big quake?

Ghosemajumder doesn't think so. He said he didn't see a surge in new

breaches so much as a steady increase in attempts as cybercriminals replenish their stock of freshly hacked passwords. It's conceivable as well that Yahoo passwords have already been used to hack other services; the company said the theft occurred in late 2014, meaning that the data has been compromised for as long as two years.

"It is like an ecological disaster," Ghosemajumder said in a telephone interview. "But pick the right disaster. It's more like global warming than it is an earthquake. ... It builds up gradually."

The first hint that something was wrong at Yahoo came when Motherboard journalist Joseph Cox started receiving supposed samples of credentials hacked from the company in early July. Several weeks later, a cybercriminal using the handle "Peace" came forward with 5,000 samples—and the startling claim to be selling 200 million more.

On Aug. 1 Cox published a story on the sale , but the journalist said he never established with any certainty where Peace's credentials came from. He noted that Yahoo said most of its passwords were secured with one encryption protocol, while Peace's sample used a second. Either Peace drew his sample from a minority of Yahoo data or he was dealing with a different set of data altogether.

"With the information available at the moment, it's more likely to be the latter," Cox said in an email Tuesday.

The Associated Press has been unable to locate Peace. The darknet market where the seller has been active in the past has been inaccessible for days, purportedly due to cyberattacks.

At the moment it's not known who holds the passwords or whether a state-sponsored actor, which Yahoo has blamed for the breach, would ever have an interest in passing its data to people like Peace .

Even if the hack was a straightforward espionage operation, Gartner security analyst Avivah Litan said that wouldn't be a reason to relax. Spies can mine trivial-seeming data from apparently random citizens to tease out their real targets' secrets.

"That's how intelligence works," Litan said in a phone call.

Meanwhile Yahoo users who recycle the same password across the internet may still be at risk. While people can always change the passwords across all the sites they use, Yahoo's announcement that some security questions were compromised too means that the risks associated with the breach are likely to linger.

A password can be changed, after all, but how do you reset your mother's maiden name?