360 Million Newly Stolen Credentials on Black Market: Cybersecurity Firm

By Jim Finkle
BOSTON Tue Feb 25, 2014 6:36pm EST

***Note from Pastor Kevin Lea**: I believe it is possible that the harvesting of all this data (using NSA capabilities) has been allowed in order to set the stage for a new crisis. For example, what if some day, tens-of-thousands (or millions) of hacks occur at once, causing massive disruption? People would demand a solution! Would the solution be a biometric (or chip implant) identification system required for every person on the planet? If so, this would likely result in a loss of our freedoms and privacy and lead to a global police state – just as the prophets foretold would be the case in the last days.*

A magnifying glass is held in front of a computer screen in this picture illustration taken in Berlin May 21, 2013.
Credit: Reuters/Pawel Kopczynski

(Reuters) - A cybersecurity firm said on Tuesday that it uncovered stolen credentials from some 360 million accounts that are available for sale on cyber black markets, though it is unsure where they came from or what they can be used to access.

The discovery could represent more of a risk to consumers and companies than stolen credit card data because of the chance the sets of user names and passwords could open the door to online bank accounts, corporate networks, health records and virtually any other type of computer system.

Alex Holden, chief information security officer of Hold Security LLC, said in an interview that his firm obtained the data over the past three weeks, meaning an unprecedented amount of stolen credentials is available for sale underground.

"The sheer volume is overwhelming," said Holden, whose firm last year helped uncover a major data breach at Adobe Systems Inc in which tens of millions of records were stolen.

Holden said he believes the 360 million records were obtained in separate attacks, including one that yielded some 105 million records, which would make it the largest single credential breaches known to date.

He said he believes the credentials were stolen in breaches that have yet to be publicly reported. The companies attacked may remain unaware until they are notified by third parties who find evidence of the hacking, he said.

"We have staff working around the clock to identify the victims," he said.

He has not provided any information about the attacks to other cybersecurity firms or authorities but intends to alert the companies involved if his staff can identify them.

The massive trove of credentials includes user names, which are typically email addresses, and passwords that in most cases are in unencrypted text. Holden said that in contrast, the Adobe breach, which he uncovered in October 2013, yielded tens of millions of records that had…

To read this article in its entirety, go to:
http://www.reuters.com/article/2014/02/25/us-cybercrime-databreach-idUSBREA1O20S20140225?feedType=RSS&feedName=technologyNews