The Moscow Times
30 YEARS
INDEPENDENT NEWS FROM RUSSIA

Russian Hacker Gang Stole 1.2 Billion Internet Credentials, U.S. Firm Says

By Anna Dolgov

August 06, 2014

A man types on a computer keyboard.

A Russian hacker gang has amassed the largest-known cache of stolen Internet credentials ever — about 1.2 billion username and password combinations lifted from databases and websites around the world, a U.S.-based online security firm said.

The unique Internet logins belonged to holders of more than 500 million email addresses, Holds Security said in a statement Tuesday, adding that some people had been robbed of more than one login set.

Holds Security, a Milwaukee, Wisconsin-based firm that has a history of identifying major online security breaches, described the collection as the "largest cache of stolen personal information" and possibly "largest data breach known to date."

The gang, which Holds Security dubbed "CyberVor" with "vor" meaning "thief" in Russian, targeted more than 420,000 websites, including top companies in "virtually all industries across the world," as well as small or even personal websites, the statement said.

The total volume of the collection compiled by the gang reaches a staggering 4.5 billion records, Holds Security said, adding that while the volume "seems like an impossible number ... just think of how many sites require you to register your email address."

As most people reuse their passwords from one website to the next, many of those records overlapped, but sorting through the data produced 1.2 billion unique sets of logins, the firm added.

The gang began by buying stolen credentials from fellow hackers on the black market, and then using them to attack email providers, social media and other websites to plant viruses that redirected traffic to the hackers' systems and to distribute spam, Holds Security said.

But the gang changed its tactics earlier this year when it started buying data from criminals that exposed website vulnerabilities, allowing CyberVor to also steal login details from those websites' databases, the statement said.

Holds Security did not release the names of the websites that have been affected. But The New York Times reported that "a security expert not affiliated with Hold Security analyzed the database of stolen credentials and confirmed it was authentic."

The security firm identified the massive breach at U.S. discount retailer Target last December, when hackers stole 40 million customers' credit and debit-card records, and a further 70 million sets of personal information that included names, addresses and phone numbers.

The firm also identified a data breach with software company Adobe Systems in October last year.

See also:

[How Communism Gave Birth to the Russian Hacker Scene]

Contact the author at newsreporter@imedia.ru