0-CNN Money-More than 6 million LinkedIn

More than 6 million LinkedIn passwords stolen

By David Goldman @CNNMoneyTech June 7, 2012: 9:34 AM ET

Researchers say a stash of what appear to be LinkedIn passwords were protected by a weak security scheme.

NEW YORK (CNNMoney) — Russian hackers released a giant list of passwords this week, and on Wednesday security researchers identified their likely source: business social networking site LinkedIn.

LinkedIn (LNKD) confirmed in a blog post late Wednesday afternoon that some of the stolen passwords correspond to LinkedIn accounts.

The company did not offer any information about how the passwords were stolen or the extent of the damage, but it said it is "continuing to investigate" the matter *[Rebuild]*.

Dating site eHarmony also announced Wednesday that some of its users' passwords were stolen in the attack.

The 6.5 million leaked passwords were posted Monday on a Russian online forum, camouflaged with a common cryptographic code called SHA-1 hash. It's a format that's considered weak if added precautions aren't taken. Roughly half of the "hashed" passwords have already been decoded and posted online in human-readable text.

Several security researchers tweeted Wednesday that they have found their passwords among those that were revealed. Web security firm Sophos said it matched many of its researchers' own passwords that are used exclusively on LinkedIn.

Countless passwords on the list contain the word “linkedin.” On a popular hacker forum, many reported finding passwords such as “linkedout,” “recruiter,” “googlerecruiter,” “toprecruiter,” “superrecruiter,” “humanresources” and “hiring.”

There’s good news and bad news about this break-in.

The good news is that so far, no user names have been discovered in the list. It’s highly recommended that you change your password, but after that you should be okay.

The bad news is that LinkedIn was using an outdated form of cryptography to secure its users’ private information. The company should have known better than to guard its lists with just SHA-1, experts say. *[Disappointment, Worry]*

The problem with SHA-1 is that it translates the same text the same way each time. So if your password is “password” and your friend’s password is also “password,” they will be hashed exactly the same way. That makes reversing the process to uncover the original password significantly easier.

That’s why security experts recommend that companies with giant lists of private data like LinkedIn add another security layer called “salt.”

Salt randomly adds another piece of information to the password. It could be a user name, first name, or even a random number — the point is that it changes the underlying text enough to make it almost impossible to decode.

“Any organization using SHA-1 without salting user passwords is running a great risk — much higher than they should,” said Per Thorsheim, chief information security advisor at Norwegian IT services company EVRY. “We’ve seen this time and time again. This is not good practice. Salt should be a minimum.”

In its blog post, LinkedIn said that it “recently” put in place enhanced security, “which includes hashing and salting of our current password databases.” *[Rebuild]*

A spokeswoman declined to comment on how “recently” that security was added. *[Deny]*

EHarmony said in a blog post that it “uses robust security measures,” but it did not include salting in the list of its protections.

The potentially worse news is that far more than 6.5 million users’ passwords were likely stolen.

Each hashed password on the hacked list is unique, according to those who have looked at the data. Since SHA-1 encodes all identical passwords the same way, it’s very likely that multiple people among LinkedIn’s 150 million users had the same password.

What’s really bad is that we don’t know the identity of the hackers or what they’re capable of. *[Worry]*

If they simply stole a bunch of passwords without any way to match them with user names, it’s a wake-up call for LinkedIn but not much more. But the attack came from Russia, a country known for its expert and mischievous hackers. There could be more fallout. *[Worry]*

“If it’s random idiots that have done this, the chances are slim that they could actually exploit this to the amount where it would actually hurt LinkedIn or you and me,” *[]*Thorsheim said. *[Neutral] [Worry]* “But if this is organized crime and these guys are serious, then the damage potential is very high.” *[Worry]*

The password hack is the second piece of bad security news to hit LinkedIn this week.

The company’s mobile application was caught collecting data from users’ calendars and sending it back to the company for analysis. The tool matches up information about the people users have scheduled with information from their LinkedIn profiles.

LinkedIn responded in a blog post that it seeks permission first, but it pledged to be more transparent about the way it collects and analyzes its

users’ personal information.