LinkedIn Information Leak

View of the analyst

On the 17th of May, the existence of a database was published with more than 167 million suspected leaked LinkedIn credentials, which the company recognised in a personal email directed to its users and sent on May 25th[1]. In that email, and according to specialised sources who had access to the leak, it was recognised that the information seems to come from an information leak that occurred in 2012. As an action of mitigation, the company proceeded to invalidate the accounts of those users that were created prior to the presumed leak date and who had not restored their account since then. The company itself has recognised that the hashing algorithm used at the time was SHA1 (without salt) which allowed a significant portion of the leaked passwords to be violated (up to 86% according to the source).

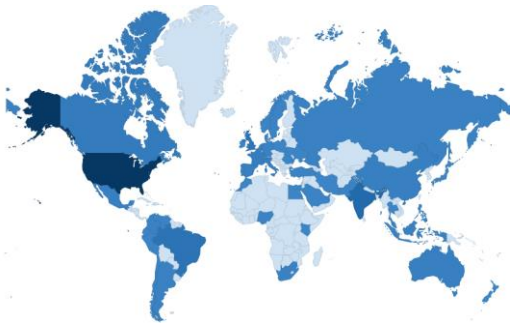
The information leak was put up for sale by a user with the generic alias `peace_of_mind` at the price of 5 BTC (about 2650 USD at the time of writing[2]) on TheRealDeal, a known marketplace in the deep web. In the following days, some platforms such as LeakedSource or Have I Been Pwned put forth the following tools to allow users to check if an email had been affected.

Technical file

Objective of the attack:	**LinkedIn**
Sector:	**Social media**
Date of the attack:	**17/05/2016**
Motivation:	**Cybercrime**
Author:	**Undetermined**
Affected assets:	**Databases**
Nature of the leaked information:	**ID** **Email** **Passwords (*hash* SHA1)**
Volume of the information:	**167 370 940**
Online availability:	**NO**

Presence of the organism:

Global



[1] LinkedIn Legal <legalnotice@linkedin.com>, «Información importante sobre tu cuenta de LinkedIn», 25-may-2016.
[2] Blockchain.info, 2016. Market Price in USD. [Online] Available at: https://blockchain.info/es/charts/market-price [date of query: 30th of May 2016].

Details of the leak

Origin of the credentials

On the 17th of May, 2016, the sale of 167,370,940 LinkedIn user credentials were made public for sale. The leak, which is still available for sale through one of the existing marketplaces in the deep web, was conducted by a single seller under the alias `peace_of_mind`, and was presented at an initial price of 5 BTC. The disclosure of the affected accounts by experts who have had access to the information and the policy put into place by LinkedIn[3] to restore all the affected accounts, has favoured the devaluation of the information, whose price not sits are around 2 BTC at the time of writing (see Figure 1).

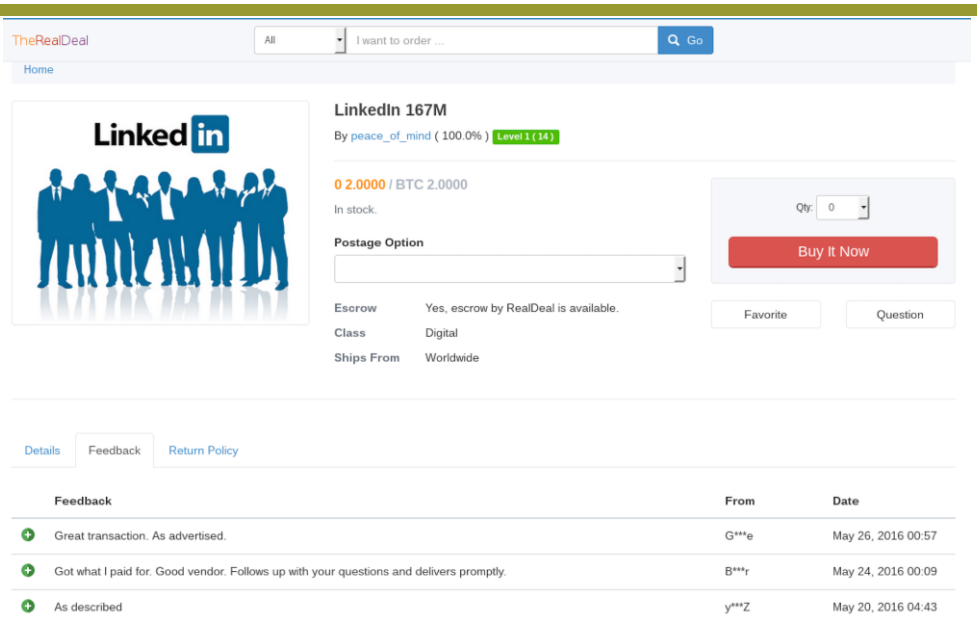


Figure 1. Screenshot of TheRealDeal where the LinkedIn leak is for sale as of May 30th, 2016.

The seller proves the veracity of the information by showing up to 220 trial credentials, without facilitating the hash-related field of the password of the affected accounts. The sample analysed by the CyberThreats service includes the following fields:

- ID: Unique identifier used by LinkedIn for user management.
- EMAIL: Main email account, stored in plain text.
- PASSWORD: Service access password, stored using an SHA-1 hashing algorithm.

In the leak, it was stated that only 117,000,000 of the accounts have an associated hash stored, which would correspond to the users that registered with LinkedIn using their Facebook profiles which avoids having to create a new password. Due to the sizeable volume of exposed credentials, actors interested in braking the password hashes are emerging, with the goal of trying to violate third party services. In only 10 days, passwords have been

[3] «Protecting Our Members». [Online]. Available at: https://blog.linkedin.com/2016/05/18/protecting-our-members. [Accessed: 27-May-2016].

extracted from more than 90% of the exposed hashes[4]. Concurrently, packages of passwords that have already been violated are being sold, as can be seen in Figure 2, while other actors known as `0x2Taylor`, and implicated in the RemoteStaff information leak, are revealing smaller information fragments free of charge.

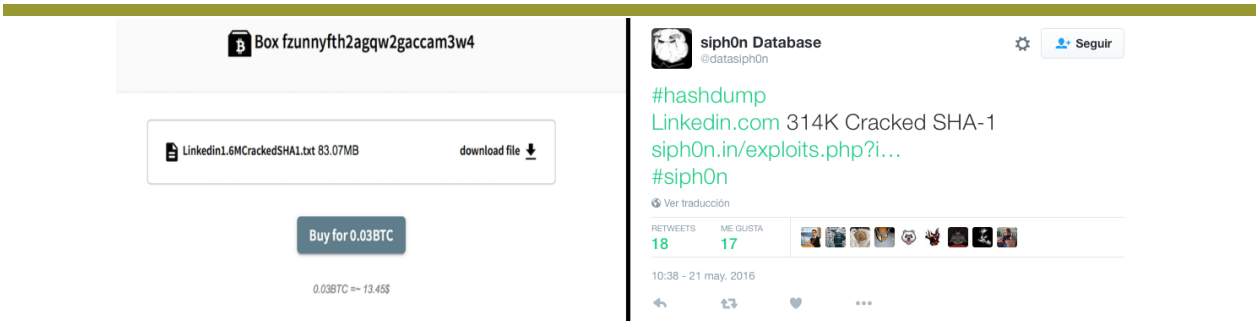


Figure 2. Example of the sale of 1.6 million supposed passwords (left) and screenshot of the reveal on Twitter of 314,000 violated hashes (right).

Many different companies are also allocating resources for information leak analysis. The results obtained by companies such as KoreLogic Security[5] reveal that the number of hashes found in the entire leak is some 177,500,189, of which only 61,829,207 are unique. Table I displays the ten most commonly used passwords.

Num. of uses	*Hash*	Password
1 135 936	7c4a8d09ca3762af61e59520943dc26494f8941b	123456
207 488	7728240c80b6bfd450849405e8500d6d207783b6	linkedin
188 380	5baa61e4c9b93f3f0682250b6cf8331b7ee68fd8	password
149 916	f7c3bc1d808e04732adf679965ccc34ca7ae3441	123456789
95 854	7c222fb2927d828af22f592134e8932480637c0d	12345678
85 515	3d4f2bf07dc1be38b20cd6e46949a1071f9d0e3d	111111
75 780	20eabe5d64b0e216796e834f52d61fd0b70332fc	1234567
51 969	dd5fef9c1c1da1394d6d34b248c51be2ad740840	654321
51 870	b1b3773a05c0ed0176787a4f1574ff0075f7521e	qwerty
51 535	8d6e34f987851aa599257d3831a1af040886842f	sunshine

Table I. Top 10 passwords most commonly used by users appearing in the LinkedIn leak.

With this volume of leaked information, tools such as PACK[6] (Password Analysis and Cracking Toolkit) help evaluate the length of the passwords used, as can be seen in Figure 3. With regard to typology, is it worth pointing out that almost 50% of the passwords are alphanumerical and do not include capital letters or special characters. Secondly, we can emphasise that 20% only contain alphabetical characters and only 1% could be considered secure, by including alphanumerical characters, capital letters and symbols.

[4] «KoreBlog linkedin_passwords_2016». [Online]. Available at: https://blog.korelogic.com/blog/2016/05/19/linkedin_passwords_2016. [Accessed: 27-May-2016].

[5] «KoreLogic, Inc., Security Services, Solutions». [Online]. Available at: https://www.korelogic.com/prs.html. [Accessed: 26-May-2016].

[6] «password analysis and cracking kit | projects | sprawl». [Online]. Available at: Http://thesprawl.org/projects/pack/. [Accessed: 27-May-2016].

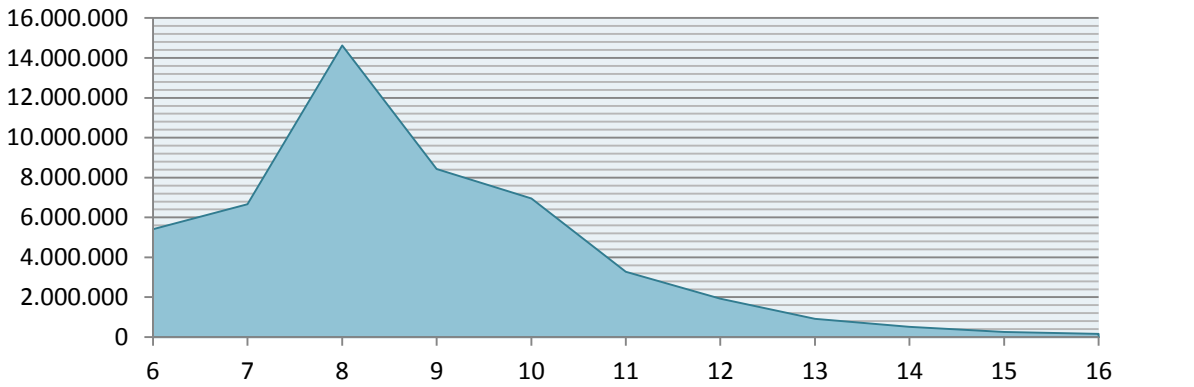


Figure 3. Distribution of the length of the exposed passwords.

Presumed responsible parties

The perpetrator of the sale uses the generic alias `peace_of_mind`, but the elevated number of votes received on TheRealDeal shows that this is a regular seller of this type of material and has a certain reputation. On the other hand, the leak of 6.5 million credentials that occurred in 2012 was attributed to a Russian group[7], presupposing the fact that the information was available for their use and exploitation over a four year period, though a relationship between `peace_of_mind` and said group has not been confirmed.

Possible uses and general recommendations

When faced with this kind of leak, reliably verifying the existence of potentially affected corporate email accounts that make use of said services becomes necessary. Once identified, and due to the plausible legitimate character of the disclosure, it will be necessary to review the services that the exposed credentials share, as they could be directly compromised. Likewise, the very nature of the affected platform increases the risk factor for the affected corporate profiles, given the possibility that the contact information exposed on this social network could be used to carry out more sophisticated spear phishing attacks.

[7] «Russian hacker leaks 6.5million LinkedIn account passwords on cybercrime forum», *Mail Online*, 06-jun-2012. [Online]. Available at: http://www.dailymail.co.uk/sciencetech/article-2155368/LinkedIn-passwords-leaked-Russian-hacker-puts-6-5m-account-details-cybercrime-forum.html. [Accessed: 27-May-2016].