Myspace Information Leak

View of the analyst

On the 26th of May, 2016, the sale of an information leak of 360 million Myspace user accounts was announced on a marketplace accessible through the Tor network for an initial price of 6 BTC, or some 3000 USD at the time of sale. The information includes emails, usernames and hashed passwords that would have been leaked during a period between the end of 2008 and the beginning of 2009. Myspace itself has recognised that the leak occurred prior to June 11th, 2013, and has reset all the passwords for accounts created prior to this date.

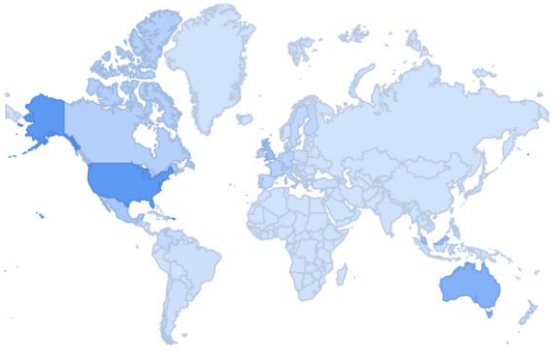
The user responsible for this announcement is `peace_of_mind` who is known on the platform used to announce the leak for having previously spread leaks of high-profile, important sites such as Tumblr, Fling or Linkedin[1] and, most recently, VK. Though the account was created in November, in only three weeks the leaks exposed by this user add up to more than 700 million records.

Technical file

Objective of the attack:	**Myspace**
Sector:	**Social media**
Date of the attack:	**Between 2008 and 2009 (estimation)**
Motivation:	**Cybercrime**
Author:	`peace_of_mind` **(original seller)**
Affected assets:	**Database of users**
Nature of the leaked information:	**Emails, usernames and hashed passwords**
Volume of the information:	**~360 million registrations (up to 35.3 GB unzipped)**
Online availability:	**Yes (to the sale: 6 BTC)**

Presence of the company:

Global



[1] «Research Report "LinkedIn data leakage"», ElevenPaths, radical and disruptive innovation in security, 30-may-2016. [Online]. Available at: https://www.elevenpaths.com/research-report-linkedin-data-leakage/. [Accessed: 02-jun-2016].

Details of the leak

Origin of the credentials

According to the perpetrator, the supplied information includes 360 million records that include emails, usernames and passwords hashed with the SHA1 algorithm without salt. In some cases, a second password has been identified which increases the number of passwords used to more than 427 million. Yes, the storage of passwords without salt is a bad practice, but some perpetrators that have had access to the samples, such as Troy Hunt (who also lowers the actual figure to 359,420,698 accounts) state that the *hashes* correspond to the SHA1 of the first 10 characters of lower case passwords[2].

Regarding the origin of the credentials, the provider has not clarified their origin. The company stated in an official press release on May 31st that the leaked information was from before June 11th, 2013[3]. This would correspond to the information from the platform's old technological infrastructure and confirm the conclusions from other independent studies that also pointed to it being an old database but that still preserved the leak dates. Troy Hunt himself established a time line between 2008 and 2009, basing this on the information facilitate by other others regarding the registration date and domains of the emails used by the leaked users that, in addition, coincides with a period of decline in platform use (see Figure 1). Eleven Paths has not been able to establish such a specific range, but does have evidence from users created at the end of 2007 that were affected and, therefore, back up said hypothesis.

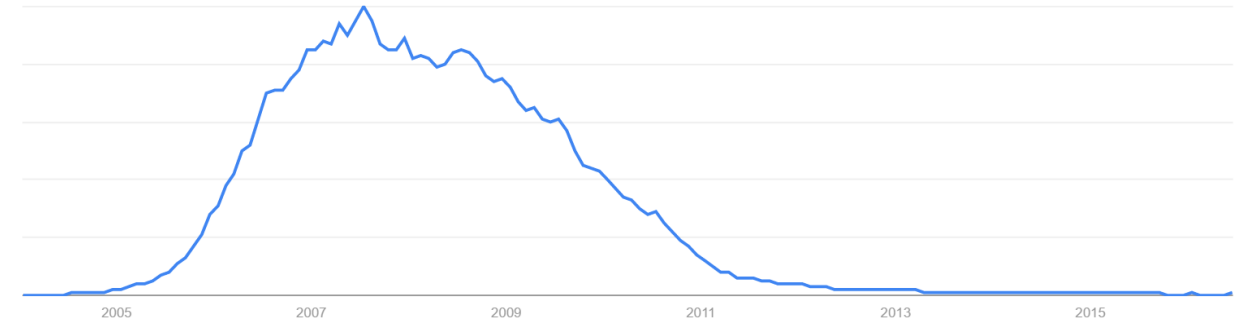


Figure 1. Evolution of the popularity of searches for 'Myspace' in Google. *Source: Google Trends.*

Presumed responsible parties

The leak was made known by user `peace_of_mind` on a marketplace accessible through Tor: The Real Deal. It has not been possible to determine if this is the original attacker or a re-seller of the leaks. In any event, in the past weeks, the alleged perpetrator has put up for sale information from other high-level websites to reach a volume of registers that exceeds 600 million accounts. Myspace specifies in its official notice that the alleged perpetrator of the leak is of Russian origin and responds to alias `Peace`. In this regard, and though no relationship with `peace_of_mind` can be confirmed, LeakedSource points out to Jabber account under the name

[2] «Dating the ginormous MySpace breach», Troy Hunt, 31-may-2016. [Online]. Available at: https://www.troyhunt.com/dating-the-ginormous-myspace-breach/. [Accessed: 03-jun-2016].
[3] Myspace, «May 31, 2016», Myspace Blog, 31-may-2016. [Online]. Available at: https://myspace.com/pages/blog. [Accessed: 06-jun-2016].

Tessa88@exploit.im as having facilitate the information[4]. The statement says «The database was provided to us by a user who goes by the alias "Tessa88@exploit.im"[5] and has given us permission to name them in this blog». It is not clear if there could be an organised group behind this identity. On the other hand, the explicit mention of a recognised sources amplifies the broadcast of the filterer, facilitates their sales and increases their visibility.

Both `Tessa88` and `peace_of_mind` correspond to very generic usernames with a confirmed network presence on over 46 different social network platforms. Email accounts associated with those usernames exist for at least 8 providers, three of which are of Russian origin and at least one other is associated with encrypted messaging. In any event, the use of generic names is not by chance. In fact, it is a recommended practice in underground settings in order to impede account tracking and obtaining identifying information about the attackers, even in the case that the implicated person, by mistake, accidentally leaks information.

Possible uses and general recommendations

The company has stated that it has begun to invalidate the passwords of accounts created prior to the month of June, 2013, as such access to the platform with the leaked passwords is not a current possibility. Likewise, it has also stated that security measures have been continuously improved since the summer of 2013, including password storage with salt and other unspecified additional measures following the incident. Though the leak is old, the passwords utilised by registered users may still be valid for other technological assets. It is not common to find corporate emails on this platform when it comes to taking more restrictive security measures for business assets. Nevertheless, the correlation between this information and other leaks could be an open door to more sophisticated attacks by adding the information available about the potential victims.

[4] LeakedSource, «LeakedSource Analysis of MySpace.com Hack», LeakedSource, 27-may-2016. [Online]. Available at: https://www.leakedsource.com/blog/myspace. [Accessed: 06-jun-2016].

[5] Exploit.im is a messaging platform of Russian origin that currently operates from a French server (specifically from Nord-Pas-de-Calais) and whose data logger uses a post code address whose validity has not been verified. Neither the address nor the post code corresponding to the information has been found within the metropolitan area of Moscow. On the other hand, messages sent between users of the provider are encrypted end to end by default.