PandaLabs Bulletins:

Social Networks in the spotlight

wwwpandasecurity.com/homeusers/security_info | www.pandalabs.com

Index

1.- Introduction

Social networking sites can be defined as “web-based services that allow individuals to construct a public or semi-public profile within a bounded system, articulate a list of other users with whom they share a connection, and view and traverse their list of connections and those made by others within the system. The nature and nomenclature of these connections may vary from site to site” [1].

We live in an increasingly globalized world in which there are many mechanisms for breaking down geographical boundaries. Our concept of communication has changed and social networks have become a useful tool in this new context of global communication.

Social networks stretch around the globe, connecting millions of people, enabling them to share knowledge, hobbies, advice, concerns…

Although these networks vary widely in terms of subject matter, the basic concept is the same: to provide a channel through which users can communicate.

However, the growing popularity of these sites and the trust they engender among users has attracted the attention of cyber-criminals, who have found in them a new conduit for their fraudulent activities.

This article will look at the history and functionality of these networks and will analyze the reasons for their popularity, supported by data and statistics, before going on to examine how they have been attacked by the criminal fraternity on the Web.

2.- History

The first online social network appeared in 1995, when Randy Conrads created *classmates.com*, a site designed to enable old school or college friends to keep in touch.

Two years later, *SixDegrees.com* became the first social network allowing users to create profiles and lists of friends. It originated as tool for allowing users to interconnect and send messages. This service shut down in the year 2000 however.

In 2002, a series of sites, such as *Friendster* and *Fotolog*, came online offering people the chance to form groups of friends across the Web, and in 2003, sites including *MySpace*, *Hi5* and *LinkedIn* joined the fray.

Even some of the foremost search engines created their own social networking sites, with Google launching *Orkut* in 2004 and the appearance of *Yahoo! 360º* in 2003. *Facebook* was originally created solely for students of Harvard University in 2004, and became available to all Internet users in 2006.

In 2005, AOL set up the *Bebo* social network, which also became one the most popular.

In 2006 *Twitter* was launched and also *Tuenti*, a social network dubbed the Spanish *Facebook*.

1995	1997	2002	2003	2004	2005	2006
Classmates	**SixDegrees**	**Friendster**	**MySpace**	**Orkut**	**Yahoo! 360º**	**Facebook**
		Fotolog	**LinkedIn**		**Bebo**	**Twitter**
			Hi5			**Tuenti**

Chronology of the leading social networking sites

3.- Source

The origin of social networking sites is based on the theory of Six Degrees of Separation, according to which if a person is one step away from each person they know and two steps away from each person who is known by one of the people they know, then everyone is an average of six "steps" away from each person on Earth.

This theory was initially put forward in 1929 by Frigyes Karinthy[1].

Each person knows on average around a hundred people, including friends, family and colleagues. If each of these friends or acquaintances knows another 100 people, each individual can send a message to some 10,000 people, simply by asking their friends to forward the message.

If each of these 10,000 people knows another 100 people, the network extends to one million people at the third level, 100,000,000 at the next level, then 10,000,000,000 and finally 1,000,000,000,000 at the sixth level. In six steps, with the available technology, it would be possible to send a message to anyone on the planet.

4.- Operation

Despite the diversity of the social network sites that exist, they basically operate in the same way. To join the network, users must first register, almost always free, and then enter a series of personal details in the form of a profile (interests, photo, etc). The profile can be added to at any time, thereby increasing the chances of the user encountering someone with similar likes or interests

Once registered, users can extend their social network, inviting new ‘friends’ to join. The websites offer a series of tools to improve operability, including filters, messages, forums, communities, chats, etc. While some are clearly focused on specific objectives (finding a partner, sharing photos, etc.), others leave it up to the individuals themselves how they use the service: making friends, starting businesses, finding work, buying and selling, etc. The possibilities are endless.

[1] Frigyes Karinthy (1887 – 1938) was a Hungarian writer who put forward the theory of ‘Six Degrees of Separation’ in a short story called *Chains* or *Chain-Links*, included in his work *Everything is Different*.

Social networking sites also offer features such as automatic updating of address books, visible profiles and other online social connection services.

The respective online communities have developed different tools for maximizing the efficacy of the network ('social software'), operating jointly in three areas, "the 3 Cs":

- Communication: sharing knowledge
- Community: finding and building communities
- Cooperation: doing things together

5.- Popularity of Social Networking Sites

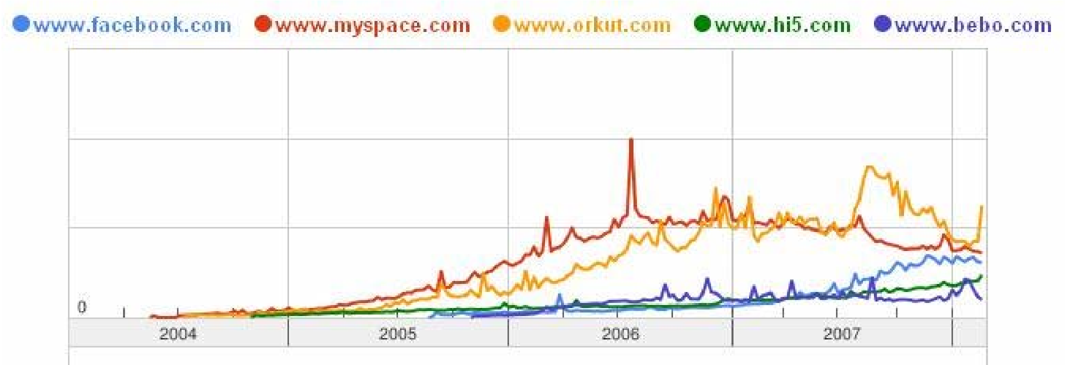
Since social networking sites first appeared, the number of users has grown exponentially. Recent data released by Alexa of the 500 most visited sites on the Internet[2], reveals that there are seven social networks in the Top 50.

The first of these is *Myspace*, in sixth place, followed by *Facebook* in eighth position, then *Orkut* and *Hi5* in 11th and 19th place respectively. Positions 39, 40 and 41 were occupied by *Flickr*, *Friendster* and *Skyrock* respectively.

Social network	Position	URL
Myspace	**6**	www.myspace.com
Facebook	**8**	www.facebook.com
Orkut	**11**	www.orkut.com
Hi5	**19**	www.hi5.com
Flickr	**39**	www.flickr.com
Friendster	**40**	www.friendster.com
Skyrock	**41**	www.skyrock.com

Ranking of social networks [2]

The Google Trend graph below illustrates the number of searches made by users for a word or phrase corresponding to some of the most widely used networking sites:



Searches made for the leading social networking sites

[2] Data from July 29, 2008 taken from the Web page: http://www.alexa.com/site/ds/top_sites?ts_mode=global&lang=none

The reasons for the success of online social networking are summarized in the following points:

- Human beings are essentially social animals. They need to communicate with others and strive to extend their connections.

- There are no barriers. Social networks break down geographical and even economic barriers that hinder traditional communication.

- Source of knowledge and information. Users of the network share knowledge and data among themselves.

- Online presence. Not everyone is able to have their own Web page. Yet social networks allow individuals to have their own personal page, customized to their own preferences.

- Viral nature. The desire to expand the network of contacts leads users to invite friends, who invite more friends and so on.

6.- Attacks on Social Networks

The popularity of these sites has aroused the interest of cyber-crooks, who have been exploiting them for some years now as a conduit for their fraudulent activities.

The attractions of social networks for the criminally-minded are clear:

- They offer access to countless users, ideal for rapid propagation of malware. If one user is infected, any other user who accesses their infected profile will automatically be infected.

- They store a lot of personal data about people, as in order to use the service users have to create personal profiles. This information can range from names and email addresses to interests, age etc.
  All these details are easily accessed by criminals and can be used for identity theft and targeted attacks or simply sold on to third parties.

- Users of social networks normally trust their contacts. It is not particularly difficult for attackers to steal the identity of a network user and exploit their trusted relationships.

Attacks on social networks are not new phenomenon; the first recorded incident occurred in 2005. However, attacks have increased and diversified just as the number of users has grown. These attacks aren't focused exclusively on distributing malware, but also involve phishing, identity theft or propagation of spam.

Notable cases

Most attacks have targeted the most popular social networks such as *MySpace*, *Orkut* or *Facebook*. This doesn't mean that they are any less secure than others, just that they have more users and therefore the chances of the attack being successful are greater.

Below we take a look at some of the most significant attacks on social networks.

MySpace, the most frequently attacked

MySpace, one of the most popular networks, was the first victim and has been attacked on numerous occasions. It was first attacked by a worm created by a *MySpace* user called MySpace.A, which enabled users to add a million contacts to their list.

At the end of 2006, another worm exploited user profiles to propagate, infecting all users that visited an infected profile.

Around that time, an advertising banner in *MySpace* exploited a Windows Metafile vulnerability to infect over a million users with spyware. Some days later a worm was uncovered at *MySpace* that inserted Java script in user profiles. When somebody tried to visit some of those profiles, they were redirected to a Web page that blamed the U.S. government for the 9-11 attacks.

However, the most serious case took place at the end of 2007. The attackers exploited a feature of Apple's QuickTime player to spread a worm in files that tried to pass themselves off as movies. The film had an HREF track with JavaScript code, allowing hackers to alter the profile of any user that visited the infected profile.

This worm was also designed to send spam massively to all the contacts of infected users. These messages supposedly contained a film. Yet users that tried to see the film would be taken to a pornographic website which downloaded Zango, a type of adware designed to display customized adverts.

Security problems in Facebook

Facebook has become one of the most successful social networking sites on the Internet, and consequently, a prime target for criminals.

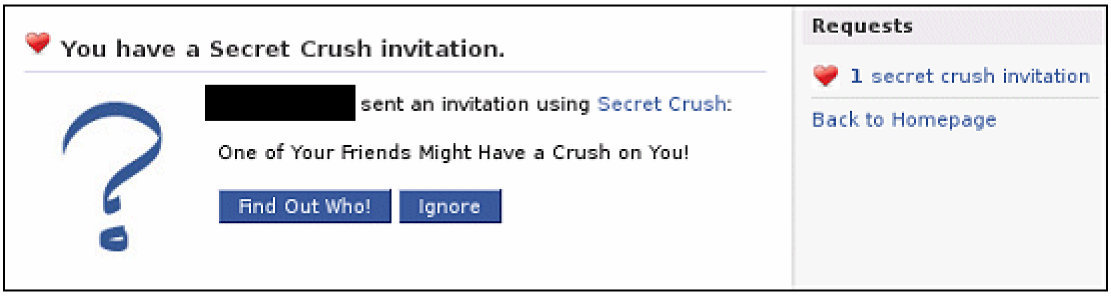
In 2007, an Illinois man posed as an adolescent to befriend young people and exchange photos with them. The man was arrested, and *Facebook* was widely criticized for its failure to protect youngsters.

In July 2007, *Facebook* had yet more security problems. In this case it was a security issue which meant that when a user entered their login details, instead of going to their own account they were taken to the mailbox of another user revealing confidential information of some users.

However the most serious error occurred during December, when *Facebook* claimed that a Canadian pornography company had hacked the accounts of 200,000 users, accessing details such as the username, password and email address.

At the beginning of this year, more than 50,000 *Facebook* were affected by the installation of adware, camouflaged as an additional social networking tool.

Victims received a message claiming to be a “Secret Crush” invitation. However, in order to find out who had sent the message, they were asked to invite another five people to install the application.



You have a Secret Crush invitation.

[redacted] sent an invitation using Secret Crush:

One of Your Friends Might Have a Crush on You!

Image of the “Secret Crush” invitation

Once they had made the five invitations, instead of finding out the identity of their secret admirer, they were told to install another additional application called Crush Calculator, which contained the adware.

In February, a rather unusual case of identity theft in *Facebook* came to light. A 26 year-old IT engineer was sentenced to three years in prison for stealing the identity of Moulay Rachid, younger brother of the King of Morocco.

In March this year, a group of hackers launched an attack against *MySpace* and *Facebook*. This attack took advantage of an exploit in the ActiveX control for posting images on profiles. The vulnerability allowed attackers to overflow the buffer of the control, and include their own commands.

Trojan in Orkut

Also in February, a Trojan detected as Orkut.AT used the *Orkut* social network to propagate. The process was as follows:

First, a profile appeared in the targeted user’s scrapbook, containing an image from a YouTube video of ‘Giselle’, a participant in the Brazilian version of Big Brother.

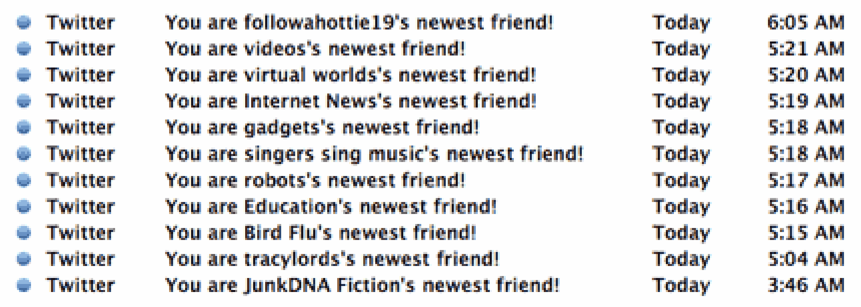
This in itself is a clear indication of how cyber-crooks still find social engineering one of the most useful techniques for spreading malware.

In this case, if the user clicked the link, a message appeared informing them that the video couldn’t be played as the corresponding codec was missing. Users were then asked to download it. However, they would really be downloading a copy of the Trojan. To avoid arousing suspicion, while the Trojan was downloading users would then be redirected to the page showing the promised video.

Once in the targeted computer, the Trojan posted a malicious message in the scrapbook of all the victim's Orkut contacts.

Spam in Twitter

As mentioned previously, spam has also reached social networks and at the end of May, a series of spam messages were detected in *Twitter*.



Twitter	You are followahottie19's newest friend!	Today	6:05 AM
Twitter	You are videos's newest friend!	Today	5:21 AM
Twitter	You are virtual worlds's newest friend!	Today	5:20 AM
Twitter	You are Internet News's newest friend!	Today	5:19 AM
Twitter	You are gadgets's newest friend!	Today	5:18 AM
Twitter	You are singers sing music's newest friend!	Today	5:18 AM
Twitter	You are robots's newest friend!	Today	5:17 AM
Twitter	You are Education's newest friend!	Today	5:16 AM
Twitter	You are Bird Flu's newest friend!	Today	5:15 AM
Twitter	You are tracylords's newest friend!	Today	5:04 AM
Twitter	You are JunkDNA Fiction's newest friend!	Today	3:46 AM

Spam messages in Twitter

Twitter users received waves of emails through the *Twitter* internal system, advising of the existence of new followers. The problem was that these profiles really contained spam-type adverts. So when a user tried to see who the new follower was, all they saw was spam.

7.- Practical tips for using Social Networking Sites

- Install a security solution with proactive technologies on the computer: This way, you will be protected against malicious codes designed to spread across these networks, even if no previous attack has been launched.

- Keep the computer up-to-date: Users must be aware of and solve all the vulnerabilities that affect the programs installed on their computer.

- Don't share confidential information: If you access forums and chats to exchange information, talk, etc. remember not to provide confidential information (email addresses, login details, etc.).

- Teach children: Children must know which information they can share and which information should remain confidential. To do so, parents must know the social networks they access and teach them the correct and safe way of using them.

- Only provide the information necessary in the profiles: When creating user profiles, only provide the information necessary. If the site requests private data like an email address, select the option to prevent other users from seeing the information, to ensure no users other than yourself and the administrator can access your data.

- Report crimes: If you observe inappropriate or criminal behavior (attempts to contact children, inappropriate photos, modified profiles, etc.) you must inform the social network administrators.

8.- References

[1] Definition taken from a study on social networking sites.
Boyd, d. m., & Ellison, N. B. (2007). Social network sites: Definition, history, and scholarship. *Journal of Computer-Mediated Communication*, 13(1), article 11.
http://jcmc.indiana.edu/vol13/issue1/boyd.ellison.html

[2] Global index of most visited web pages according to Alexa indicators:
http://www.alexa.com/site/ds/top_sites?ts_mode=global&lang=none

Appendix

General information about social networking and the theory of the Six Degrees of Separation
http://es.wikipedia.org/wiki/Red_social

http://en.wikipedia.org/wiki/Six_degrees_of_separation

Links to News

Illinois case
http://www.theregister.co.uk/2007/02/08/facebook_security/

Facebook pornography
http://www.pcpro.co.uk/news/148908/facebook-hacked-by-porn-site.html

Secret Crush
http://www.theregister.co.uk/2008/01/04/facebook_adware/

Orkut worm
http://www.theregister.co.uk/2008/02/29/orkut_worm_reloaded/

Myspace attacks
http://www.pandasecurity.com/spain/enterprise/media/press-releases/viewnews?noticia=8686&ver=18&pagina=7&numprod=&entorno