

Malware targets social networks

If you thought malware only lurked in suspicious emails or on dubious Web pages, you're wrong! You only have to access social networks such as MySpace or Facebook

The use of these pages to distribute malware has increased notably in recent months

Cyber-crooks are continually perfecting their ability to stalk users and infect them with their creations. Massive user communities, such as social networks, allow them to infect a large number of Internet users rapidly.

The first attack on social networks took place in 2005, when a [MySpace](#) user created a worm (detected by Panda as MySpace.A) that allowed him to add a million entries to his contact list.

MySpace.A launched cross-site scripting attacks; the worm launches a script to users, searching for exploitable vulnerabilities to carry out malicious actions such as infecting cookies with malware, opening SSL connections, etc.

The first attempt at causing a serious infection through [MySpace](#) took place at the end of 2006, when a worm was created that used the network's user profiles to spread. The worm infected everybody that visited a certain user 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 US government for the 9/11 attacks.

However, the most serious case took place at the end of 2007, when attackers exploited a feature of Apple's QuickTime player to spread a worm. Cyber-crooks associated several films loaded in this player to different profiles. The film had an HREF track which was associated to a JavaScript code. . This allowed hackers to modify the profiles of users who visited the infected profile created to view the film.

Two modifications were made; firstly, the malicious film was included in the visitors' profiles, so the worm continued to spread. Secondly, the worm modified the profiles' headers (which display the groups, forums, etc. tabs) so that all of them pointed to a fraudulent website. This was a spoofed version of MySpace's official site, used for stealing the user names and passwords.

Cleaning the profile does not save users from infection, since if one of the contacts is infected, it can continue spreading.

Although it exploited new structures such as [MySpace](#), it was still standard worm propagation. However, in the XXI century malware creators want to do more than cause damage and achieve notoriety, they want money. . Consequently, they implemented a new function in the worm: it was designed to send spam massively to all infected users' contacts.

Although the spam claimed to contain a film, when clicked by users, it redirected them to a porn site. . . Hackers wanted users to purchase items (videos, photos, etc.), as well as infecting them with a Zango-family adware designed to display customized publicity. In short: this is a malware-based business structure.

To deal with the problem, which according to MySpace affected 10,000 users, Apple had to eliminate the feature which allowed the infection via QuickTime, by releasing an urgent patch.

The Facebook case

In just four years, [Facebook](#) has accumulated some 50 million affiliates with over 200,000 new users each day. It has become one of the most famous social networks and one of the biggest cybernetic phenomena in the last few years.

It owes part of its success to the ease with which friends are added to profiles. However, its misuse could have negative consequences. As with other social networks, [Facebook](#) users provide excessive information.

Data loss, malware infections or unwanted encounters are some of the dangers of social networks such as [Facebook](#).

The first security problems in [Facebook](#) appeared at the beginning of 2007. As it started to gain followers, suspicion started to arise among users. One of the first cases occurred in Illinois (USA), when a man passed himself off as an adolescent to attract children and exchange photos. The man was arrested and several media and associations began to criticize Facebook's record of protecting children¹.

In mid-July, [Facebook](#) faced a new security problem; due to a programming problem, when users entered their password, they were redirected to another user's mailbox and their confidential information was exposed to others. Fortunately for the company, other more sensitive data such as the phone number or the contact address were not displayed.

In September, [Facebook](#) once again attracted the attention of the technology media. On this occasion, the New York Attorney General had claimed that in its desire to expand rapidly, the company wasn't giving priority to security measures in which he claimed there were significant defects. Child security was once again the most harshly criticized issue².

However, the most serious case occurred in mid-December, when according to [Facebook](#), a Canadian porn company hacked 200,000 users' accounts, gaining access to data including their user name, password or email address³.

One of the latest scandals took place in January this year, when a company created a tool which when installed on users' computers for use with [Facebook](#), copied the Zango adware. Several security companies criticized [Facebook](#) for the time they took to withdraw the tool.

Finally, in August 2008, PandaLabs has detected a worm called Boface.A which spreads through the [MySpace](#) and [Facebook](#) social networks. The worm inserts a link in comments posted on both networks to take users to a fake web page that resembles the actual YouTube site. When the user tries to watch the video they are encouraged to install the latest Flash Player version. However, if they do so, they will be actually letting a copy of the worm into their computers.

The worm uses subjects like "Hello; You must see it!!!" or "LOL. My friend caughted you on hidden cam" to entice users into watching these videos.

In short, [Facebook](#) has been criticized on several occasions due to security problems, mainly those regarding its ease to provide sexual predators with hiding places and the incorrect management of sensitive profile data.

A Trojan in Orkut

In March, PandaLabs detected a Trojan called Orkut.AT, which used the popular [Orkut](#) social network to spread. The process was as follows:

First, a profile appeared in the targeted user's scrapbook, which contained an image from a YouTube video. The image is that of Giselle, a contestant in the Brazilian edition of the Big Brother reality TV show.

“That’s the bait they use”, explains Luis Corrons, Technical Director of PandaLabs. “Cyber-crooks take advantage of people’s interest in celebrities to entice users to open files or click malicious links”.

In this case, if the users clicked the link, a message was displayed informing them that the video couldn’t be played as the corresponding codec was missing. Users could then download it. However, if they did, they actually downloaded a copy of the Orkut.AT Trojan on their computers. To avoid raising suspicions, the Trojan redirected users to a Web page where they could find the video in question.

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

Also in March, a group of hackers attacked [MySpace](#) and [Facebook](#) using an exploit in the ActiveX control which allowed users to load images to their profiles. The vulnerability allowed them to saturate the control buffer so it interpreted the instructions sent by cyber-crooks instead of those it was originally designed for.

Other risks: Inappropriate content and confidential information loss

A common component of social networks is the need to create a personal profile to access them. These profiles often contain data such as name, age, etc.

Bear in mind that it is unnecessary to provide this information and that simply an email address and name (which could be false) will do. Users are advised to avoid giving out data like age, address, etc. Similarly, children’s photos should be protected so that only trusted people can access them (peers, family, etc.).

Many social networks allow users to have a blog, the online version of traditional personal journals. As such, these online journals frequently contain far more information than is advisable. It is particularly important to avoid publishing any data that could identify the user as a young person, or that could reveal their address or place of study, etc.

Similarly, on certain social networks, such as [MySpace](#), it is possible to share files with other users. Users must be especially careful with what they share and who they share it with. There is no problem in, say, posting photographs, provided they are protected with a password which is only distributed among friends and family.

In the case of children, you must be careful with inappropriate content published on those networks, since a lot of it is unsuitable for children and users are not informed before accessing it. Children also risk having a bad online experience, since the person contacted on forums or chats, could be lying as to who they are, and could seek to contact children, ask them to send them photos, etc.

Tips for using social networks

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

- **Keep the computer up-to-date:** users must be aware of and resolve all the vulnerabilities that affect the programs installed on the 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, credentials, etc.).

- **Teach children:** Children must know which information they can share and which not. To do so, parents must know the social networks they access and teach them the correct and safe way of playing.

- **Only provide the information necessary in the profiles:** When creating user profiles, only provide the information necessary. If it requests private data like the 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, inadequate photos, modified profiles, etc.) you must inform the social network administrators.

You can check whether you are infected on the Infected or Not website (<http://www.infectedornot.com>)

-
1. http://www.theregister.co.uk/2007/02/08/facebook_security/
 2. http://www.theregister.co.uk/2007/09/25/facebook_subpoena/
 3. <http://www.pcpro.co.uk/news/148908/facebook-hacked-by-porn-site.html>