Social Networks Part 2

Have you been Infiltrated?

by David Pace, Pierluigi Paganini, Ron Kelson, Fabian Martins, Benjamin Gittins

David Pace

Pierluigi Paganini

Ron Kelson

Fabian Martins

Published: 22nd August 2012

The explosion of social networks and new user accounts in recent years is staggering. There are now over 1,000 social networking sites on the Internet, with Facebook currently being the largest, with over 840 million user profiles. To put this into context, that is equivalent to the combined populations of the USA and UK combined, making it the third largest country by population.

This illustrates how social networks can be a virtual goldmine of information and knowledge for those who can potentially harvest it both openly and/or covertly as we explain below.

In our first article we explored how social networks can be described as powerful communication tools capable of reaching clique groups and/or vast audiences instantaneously and globally. We explored two theories behind social networking:

1) Social networks as a powerful tool enabling citizens to coordinate their observation and management of Government(s) and corporations, and where deemed necessary, coordinate (nonviolent) struggle against perceived injustices; and

2) Social networks as a powerful tool custom-built for exploitation by governments and powerful organisations to monitor individual, group, regional, and global sentiments and trends.

We then explored a variety of ways Governments are interacting with Social Media. Ranging from: Government interference in the activities of the major social networking companies; Adoption of tools for monitoring of communications over social networking; Implementation of methods for the direct analysis of social networks through active infiltration; Seeking legal authority to install software on your computer without your permission; and even Preventing access to social media.

In this article we discuss methods being employed to infiltrated user accounts, and the potential impact infiltration can have on persons and organizations on a potentially massive scale.

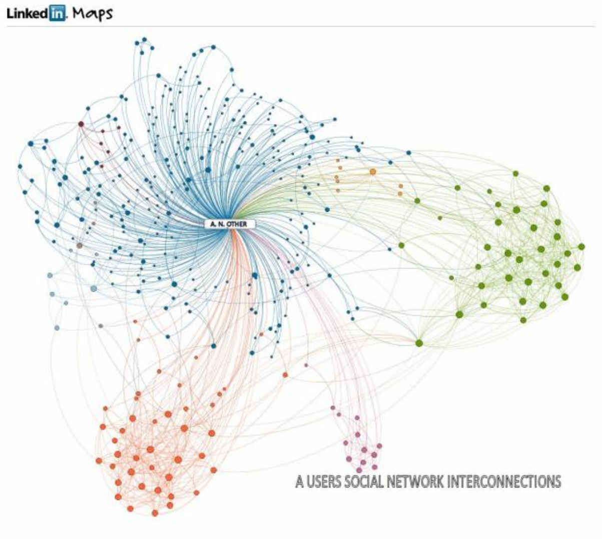
Countless criminal organisations have used social networks for all kinds of social engineering attacks with the intent of gathering sensitive information, or to spread malware or steal financial information from users.

"*Social engineering*" is an act of psychological manipulation. All social engineering techniques are based on specific attributes of human decision-making known as cognitive biases. These biases, sometimes called "bugs in the human hardware," are exploited in various combinations to create cyber attacks that exploit weaknesses in both computers and humans simultaneously.

Popularity can have it's down side: Are you excited about the new 'friend request' from that attractive looking stranger in your Facebook account? An experiment, over a short 8 week period, by researchers at British Columbia University in Canada, simply created 102 'fake' Facebook user accounts referred to as Socialbots, with the sole intent of making as many friends as possible and harvesting data. The Socialbots began contacting Facebook users by making random 'friend requests' and were accepted by 1 in 5 people they contacted. Once the Socialbot made some "friends" it increased its number of friends by using the social networks of those users who accepted it, befriending the friends of friends.

These friend requests by the now popular Socialbot were far more likely to be accepted. The research team found that a staggering 60-80% of these requests were successful. As a result, they were able to harvest 46,500 email addresses and 14,500 physical addresses from users' profiles, including a massive 250Gb of personal data. What is critical to understand is that this information can be gathered AS SOON as the friend request is accepted. Then a copy can be stored offline, for later recall at any time.

Therefore the actual owner can no longer recover, or change or delete that personal data that someone may have recorded. Facebook's "Facebook Immune System", the massive security system protecting users, and which checks some 25 billion actions every day, did not detect the infiltration of the Socialbots.



This demonstrates a very simple but effective capability to attack people at random. (We will talk about targeted attacks shortly below.)

Indiscriminate attacks in the wild: The well known Socialbot malware, called the "Koobface" virus, is specifically created to target social network platforms. Unlike most other malware, Koobface spreads "actively" by delivering messages to people who are "friends" of a user whose computer has already been infected.

Targeted social network platforms include Facebook, MySpace and Twitter as well as others. Once the host has been infected, Koobface connects back to so-called command and control servers (C&C), or receives directives on actions to perform or to upload compromised information. In this way the agent is able in a short time to build its own botnet, a huge number of Internet computers that, although their owners are unaware of it, have been set up to forward spam or viruses to other hosts on the Internet.

The most common infection method is via fake content on a compromised web site. It is sufficient to click on one of the links which Koobface has posted on the fake web site. Typically this link would attract users by offering a download of a cool video or application. If they then download and execute the file, Koobface infects their system.

This malware is a typical example of an agent that could be used:

1. by cyber crime to monetize an assault to social networks platforms; and
2. by Governments to infiltrate social networks to perform intelligence operations, or to spread viruses developed for with cyber espionage intent.

Let's recall a case in recent months when a NATO chiefs' personal details were exposed thanks to a series of attacks moved through social network platforms.

Targeted attacks: As the NATO chief example proves, social engineering techniques can also be used to target specific individuals. In the first phase of the attack a little bit of research is required to determine the target's "position" in society, and their likely "network" of superiors, respected peers and colleagues. Once the attacker has identified those people who are "important" to the target, a series of fake accounts are created on the social network. Recall that more than one person can be called by the same name. Furthermore, much of the data you need to create the fake account (name, face, activities) is already public on other social networks. In the case of NATO'S most senior commander, several fake Facebook accounts for several of his colleagues were created, apparently by Chinese spies.

In a second phase of the attack the fake accounts try to contact the real one, by establishing a relationship. This is exactly what happened when Senior British military officers and Ministry of Defence officials accepted "friend requests" from the bogus account for American Admiral James Stavridis.

At this point, the infiltration attack has now been successfully executed. As a result, it is now possible to steal sensitive information such as personal email account addresses, photos, messages, knowledge of the targets network of friends, which are all potential future targets for subsequent phases of the attack.

Similar "social engineering" incidents are worrying and show how vulnerable even the higher echelons of strategic command, can be.

Some risks you face when your "trusted" social network platform has a data breach:

An interesting case study occurred when the professional social network LinkedIn was recently hacked, and users' passwords stolen and leaked on the Internet. The company, through its blog, confirmed the event, declaring that more than six million passwords were compromised.

The LinkedIn hack is considered particularly serious, because the popular social network focusses on networking people in a business/professional context. LinkedIn members share information about their professions and employments both in private business and in governments. Each public association between user accounts acts as a type of credential establishing a person's standing and credibility in the community as previously described.

Accessing a LinkedIn account can expose significant information on the (potential) victims, their relations, and participation in events and discussions related to specific 'closed' professional areas, with their inherent privacy levels. It is clear that the information could represent the basis for other types of attacks, and *cyber espionage*.

Another real risk is the possibility of a massive *phishing* campaign being launched during these 'compromised' hours, inviting LinkedIn users to change their passwords, potentially providing additional information to the criminal. Typically, such campaigns may include strategic dissemination of additional malware types, typically via an email with a link (although this hypothesis has been excluded by LI) which redirects him to the infected web site.

Ultimately, all this information that has been garnered can be *stored forever* and utilized for a multitude of reasons, to the benefit of the criminals and the perpetrators of your infiltrated account and private information and network of friends and colleagues.

What can you do to avoid being compromised or exploited?

- *Actively manage your privacy settings*
- *Don't accept friend requests from random people.* Share your data with fewer people, and only those that you really DO know. CONFIRM with your friend via SMS / phone, BEFORE accepting online. Actually KNOW the people you are friending! Follow up any flagged concerns you may have about a friend's online behaviour – they may not be who you think they are, or their account may have been compromised.
- *Think before you click.* Never click on suspicious links. Just because they "purportedly" came from a friend or organisation you know, does NOT make them safe. Report any abuse to the network service provider. You will be helping others be safer as well.
- *Never enter your username/password* on a site that is not using the URL of your social network provider.
- *Always update your browsers and anti-virus* to latest versions as they can protect against phishing and other attacks.
- *Clear and delete old social network accounts*. Over time you stop using accounts for one reason or another. Make sure they are deleted by the social network provider.
- *Don't assume your online correspondence is private.* Many accounts have a default setting to 'share' (indiscriminently publish) when first created. Anything shared can be saved (and stored for ever), copied, and can of course even be indexed by search engines.
- *Don't share your location*. Turn off broadcast features. Don't leave notes saying you are on holiday. This is an invitation for criminals to visit your home.

Be sure to read our next article in this series where we explore the *physical* risks associated with online social networking.

This article was first published in the Malta Independent on Sunday – Original article below.

About the Authors :

David Pace is Project Manager of the ICT Gozo Malta Project, and a freelance IT Consultant.

Pierluigi Paganini, Security Specialist, CISO Bit4ID Srl, is a CEH Certified Ethical Hacker, EC Council and founder of Security affairs - *http://securityaffairs.co/wordpress* .

Prof. Fabian Martins, Banking security expert and Product Development Manager at Scopus Tecnologia, http://www.scopus.com.br/) owned by Bradesco Group. http://br.linkedin.com/in/fabianmartinssilva

Ron Kelson is Vice Chair of the ICT Gozo Malta Project and CEO of Synaptic Laboratories Limited.

Ben Gittins is CTO of Synaptic Laboratories Limited.

ICT Gozo Malta is a joint collaboration between the Gozo Business Chamber and Synaptic Labs, part funded in 2011 by the Malta Government, Ministry for Gozo, Eco Gozo Project, and a prize winner in the 2012 Malta Government National Enterprise Support Awards. The web portal at www.ictgozomalta.eu *provides extensive links to free cyber awareness resources for all age groups.*

To promote Maltese ICT, we encourage all ICT Professionals to register on the ICT GM Skills Register and keep aware of developments, both in Cybersecurity and other ICT R&D initiatives in Malta and Gozo.
For further details contact David Pace at dave.pace@ictgozomalta.eu

Other Articles in the Series

Insider perspectives on the Global Cyber Safety and Security Status – Part 1
Insider perspectives on the Global Cyber Safety and Security Status – Part 2
Insider perspectives on the Global Cyber Safety and Security Status – Part 3
Insider perspectives on the Global Cyber Safety and Security Status – Part 4
A Picture of the Hacktivism Phenomenon
Serious Safety and Security Problems in Automotive, Aviation, Aerospace and other Cyber-Physical Systems – Part1
Serious Safety and Security Problems in Automotive, Aviation, Aerospace and other Cyber-Physical Systems – Part2
The Cyber War Era Began Long Ago
Are your Business Operations Secure?
Cyber Security at Large Sporting Events
Malware – It's all about you!
Phishing the Financial and Banking seas

Understanding the risks of Mobile Banking Transactions

Social Networking series Part 1:   Who exactly are you disclosing your story to?

Social Networking series Part2:   Have you been infiltrated?

Social Networking series Part3: Are you unnecessarily exposing yourself to physical threats?

...

All the above articles, and more, are available at www.ictgozomalta.eu/events/documents-list. They may also be available from the respective author's websites.