Socialbots Studies

Goals

In recent years, adversaries have taken advantage of online social networks in order to collect private information regarding users, such as e-mail addresses, phone numbers, and other personal data that have monetary value. Such information can then be used for online profiling and large-scale e-mail spamming and phishing campaigns. We have two major goals: first, we seek to demonstrate how easy it is to extract private information about a specific organization's employees using socialbots. Second, we use socialbots to infiltrate employees' private social networks. By means of these infiltrations, we are able to study targeted organizations and their employees.

Description

In the first study, we introduced a method for mining an organization's information through social networks and socialbots. We created socialbots and used them to send friend requests to Facebook users who worked at a targeted organization. By accepting friend requests through socialbots, users exposed information about themselves and about their workplace. We tested the proposed method on two real organizations and successfully infiltrated both of them. Compared to our previous studies, our method was able to discover up to 13.55% more employees and up to 18.29% more informal organizational links.

In the second study, we introduced a method for attacking specific users in targeted organizations by using organizational social network topologies and socialbots. To target users, we randomly chose ten Facebook users from every targeted organization. Our socialbots sent friend requests to all the specific users' mutual friends who worked or work in the same targeted organization. The rationale was to gain as many mutual friends as possible and thus increase the probability that our friend requests would be accepted by the targeted users. We tested the proposed method on targeted users from two different organizations. Our method achieved success rates of 50% and 70%, respectively, among the ten targeted users.

In the last study, we enhanced our previous study and evaluated our suggested method for infiltrating key employees of targeted organizations on two well-known OSNs – Facebook and Xing. The results obtained demonstrate how adversaries can infiltrate social networks to gain access to valuable private information regarding employees and their organizations. Moreover, the results indicate that users who wish to protect themselves should not disclose information on online social networks and should be cautious of accepting friend requests from unknown persons.

Researchers

Aviad Elyashar
aviade@post.bgu.ac.il

Michael Fire
mickyfi@post.bgu.ac.il

Dima Kagan
kagandi@post.bgu.ac.il

Prof. Yuval Elovici
elovici@inter.net.il

Publications

Aviad Elyashar, Michael Fire, Dima Kagan, and Yuval Elovici, "Organizational Intrusion: Organization Mining Using Socialbots," 2012 International Conference on Social Informatics (SocialInformatics).

Aviad Elyashar, Michael Fire, Dima Kagan, and Yuval Elovici, "Homing Socialbots: Intrusion on a Specific Organization's Employee Using Socialbots," International Workshop on Social Network Analysis in Applications (SNAA), co-located with ASONAM 2013, Niagara Falls, Canada, August 2013.

Aviad Elyashar, Michael Fire, Dima Kagan, and Yuval Elovici, "Guided Socialbots: Infiltrating User's Friends List," AI Communications, 2014.