Creation and Management of Social Network Honeypots for Detecting Targeted Cyber Attacks

Researchers

Abigail Paradise
abigailparadise@gmail.com

Dr. Asaf Shabtai
shabtaia@bgu.ac.il

Dr. Rami Puzis
puzis@bgu.ac.il

Aviad Elyashar
aviade@post.bgu.ac.il

Prof. Yuval Elovici
elovici@inter.net.il

Dr. Mehran Roshandel
Mehran.Roshandel@telekom.de

Dr. Christoph Peylo
Christoph.Peylo@telekom.de

Publications

A. Paradise, R. Puzis, A. Elyashar, Y. Elovici, and A. Shabtai, "Creation and Management of Social Network Honeypots for Detecting Targeted Cyber Attacks." IEEE Transactions on Computational Social Systems (IEEE T-CSS), 2017.

Goals

Reconnaissance is the initial and essential phase of a successful advanced persistent threat (APT). In many cases attackers collect reconnaissance information from social media, such as professional social networks. This information is used to select members that can be exploited to penetrate the organization. Detecting such malicious reconnaissance activity is extremely hard because it is performed outside the organization premises.

Description

The researchers propose a framework for management of social network honeypots to aid in detection of APTs at the reconnaissance phase. Using a field trial conducted with the cooperation of a large European organization, they analyzed the deployment process of the social network honeypots and their maintenance in real social networks. The honeypot profiles were successfully assimilated into the organizational social network and received suspicious friend requests and mail messages that revealed basic indications of a potential forthcoming attack.

The project also includes exploring the behavior of employees in professional social networks, their resilience and vulnerability toward social network infiltration.