Stegobots in Social Network

Nithin V Nath, Shamil C M, Sreeraj S, Vivek Anand T Kallampally
Vineeth Thomas Alex, Aravind A N, Arun Kuruvila
Department of Computer Science and Engineering
National Institute Of Technology, Calicut

Objective

To study the working of stegobots in a social network. Stegobots[1] are covert social network botnets, which steal the affected user's information and transmit them through a social network like Facebook, Google Plus etc. The second phase was to implement a trojan horse to steal saved passwords in Google Chrome and encode it in user's images. These images when shared by the user will transmit these passwords through Google Plus from one affected computer to another finally reaching a malicious user (botmaster). This demonstrates the functioning of a social network botnet.

Work Done

1. **Network Simulation**: The first stage was to simulate sending and receiving packets by the botmaster in a social network. The tool we used for the simulation was `NS3` [2]. We performed the simulation using a graph with approximately 500 nodes. Nearly 600 packets was recevied by the botmaster when the node with the maximum edges was selected as the botmaster. `NS3` was memory intensive and so we restricted the dataset to a 500 node graph. The number of packets received will depend on the structure of the social network graph. (Source Code: `http://github.com/sreeraj-altair/ns3botnet`)

2. **JPEG Steganography**: JPEG, unlike other image formats undergo compression when the image is saved. We tried to implement YASS [3] or Yet Another Steganographic Scheme for JPEG which used a RA (Repeat Accumulate) error correcting scheme [4]. However, we used a different error correcting scheme. In our scheme, a bit to be encoded was repeated q times and while decoding errors are corrected by selecting the bit with the highest occurance. Encoding was performed on the Green Channel of a Lena (RGB) image and decoding was successful when the quality factor was between 95 and 100.
(Source Code: `http://github.com/nithinvnath/yass`)

3. **Trojan Horse (Bot)**: We implemented a trojan horse which acts as the bot in the botnet. The trojan infects a user's PC by attaching itself to some genuine software. The trojan steals saved passwords in Google Chrome, and encodes it in users images using steganography. It also scans the images downloaded by the user for saved passwords of other infected users and re-encodes it in the current users images. These images when shared on Google Plus, transmits the passwords to bots(trojans) in other infected computers. A single encoded image will contain an independent login information of a particular user (username/email , password and hostname). (Source Code: `http://github.com/vivekzhere/botplus`)

4. **Botmaster's Photo Scanner**: A Google+ application was developed which made use of Google Plus API, Google Contacts API and Picasaweb Albums API to scan for photos shared with the botmaster. The application extracts the passwords saved in these images and adds it to the botmsater's password database. Photos shared by the people in botmaster's contacts are scanned iteratively for encoded passwords.
(Source Code: `http://github.com/shamilcm/gplus-photo-scanner`)

References

[1] Shishir Nagaraja, Amir Houmansadr, Pratch Piyawongwisal, Vijit Singh, Pragya Agarwal, Nikita Borisov, "Stegobot: A Covert Social Network Botnet", *International Workshop on Information Hiding* 2011: 299-313.

[2] `http://www.nsnam.org/docs/release/3.15/tutorial/ns-3-tutorial.pdf`

[3] Kaushal Solanki , Anindya Sarkar , B. S. Manjunath, "YASS: yet another steganographic scheme that resists blind steganalysis", *International Workshop on Information Hiding* 2007

[4] Kaushal Solanki , N. Jacobsen; U. Madhow , B. S. Manjunath, S. Chandrasekaran,"Robust image-adaptive data hiding using erasure and error correction", *IEEE Transactions on Image Processing* 2004