Resilient Facebot

Orie Steele, Tom Parisi, Simon Sidhom, Ken Bodzak

RFB: Overview

- Build resilient and low-key botnet
- Utilize public resources and steganographic techniques for Command & Control of a botnet
- Develop methods of detecing the botnet

Social Networks and Resources

- Social Networks (where command nodes live)
  - Twitter
  - Tumblr
  - Facebook
  - Google+
  - LinkedIn
  - Myspace
- Media Sharing Services (where commands live)
  - imgur
  - dropbox
  - picasa
  - flikr
  - etc...

Important Definitions:

Resilient: able to overcome faults within the network

Puppetnet: Victims are told what to do but can leave easily unlike a botnet.

Low-Key: slowly completes malicious activity to hide itself from the user

Botnet: A distributed computer system of hosts that have been compromised. The hosts do what they are told by a bot master.

Related Work

- Built a Facebook application Trojan Horse
  - Legitimate application with a malicious component
- Every time a user clicks in the trojan application, the browser would download images in the background from another website
  - Denial of Service if enough users were downloading at once
- Used a least-effort approach
  - Did only the minimal to appeal to the most amount of people
  - Keep the costs down

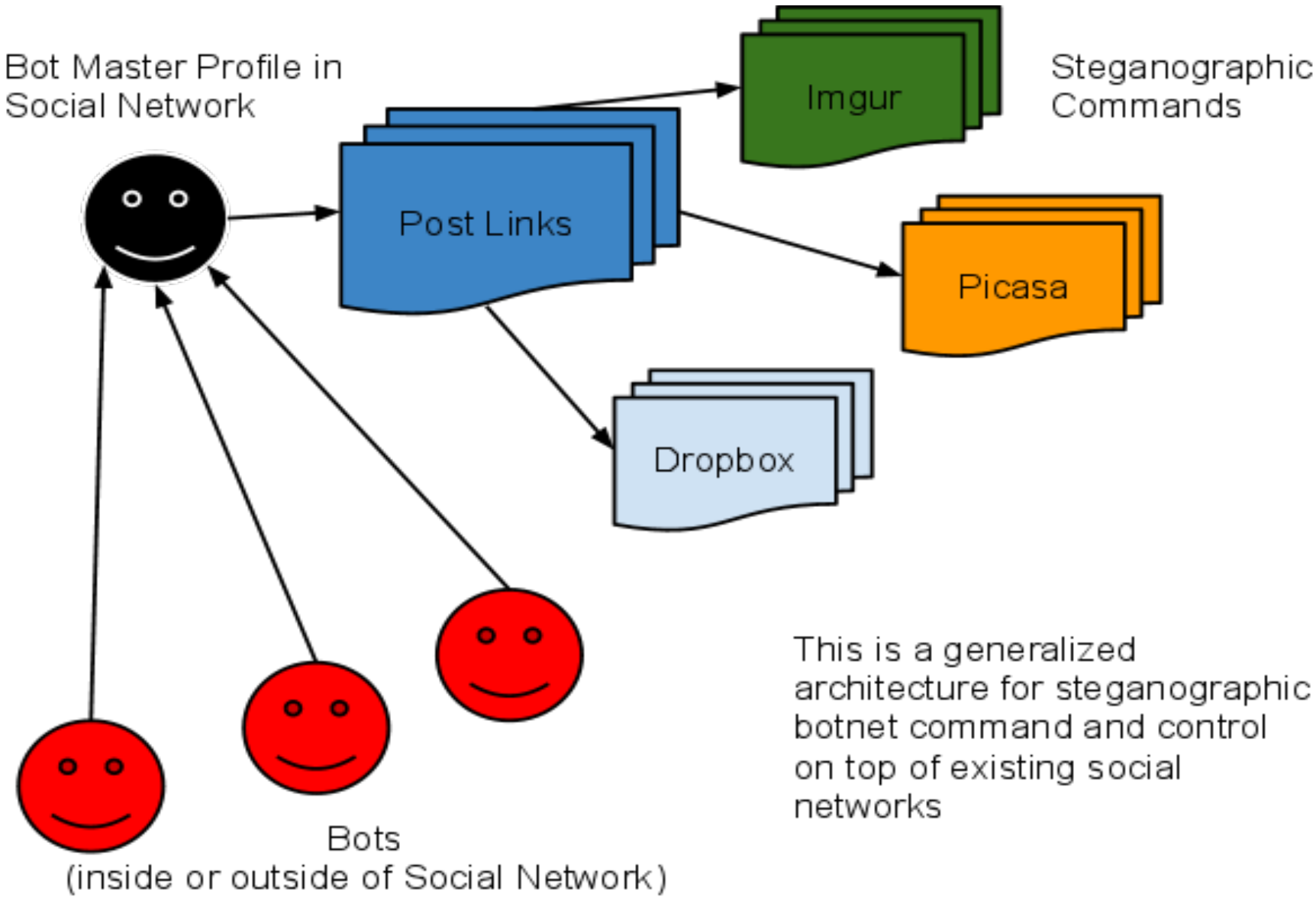
Why Use Social Networking?

- The network is already setup
- Millions of users already there
  - Most users don't think about the malware that don't think about the consequences
- Targets of the malware will be the younger people on social

FaceBot

- Out of Scope:
  - Writing of the actual malware
  - Insertion into actual Facebook (this is in scope) its essentially submitting a link or uploading a file...
- In scope:
  - Creating the network architecture
  - Communication through Steganography
  - Preventing a future FaceBot

FaceBot Architecture



FaceBot Architecture

- Work with the assumption that a piece of malware infects the victim in some way
- The victim's will then begin checking predefined profiles at regular intervals
  - Profiles to check are hidden in a file
  - Checks the most recent uploaded pictures or links to other media for instructions hidden in the media
- Each node will not know of the other nodes that are contained in the botnet
- Basic Command and Control structure with single point of command
  - Uses Facebook's load balancing and server architecture
    - Mitigates Single Point failure

Why Use Steganoraphy?

- Hides the communication from Facebook and computer user
  - Looks like regular traffic to a highly visited website
    - Packets look like normal packets from the website
- Allows the use of Facebook as the Command and Control server reducing costs of the botnet
- History of commands
  - Storing the commands in pictures gives a history of instructions in case a node has not been connected in a long time.

FaceBot Development

- Technology Details:
  - Python
  - Facebook Javascript API
- Steganography Program we might use:
  - Command & Control Tools
    - Ideally we would like to use a combination of the following:
      - Linking to 'command images' stored on sites like imgur
      - Stego in URL shorteners
        - http://www.byrnehobart.com/blog/steganographic-typo-based-url-shorteners-add-a-link-with-zero-new-characters/
      - Unicode and Text options
        - http://www.irongeek.com/i.php?page=security/steganographic-command-and-control
      - Stego in video:
        - http://lifehacker.com/5771142/embed-a-truecrypt-volume-in-a-playable-video-file
        - Could be used with dropbox
    - We could also investigate onion style routing within steganographic mediums

Preventing FaceBot

- Facebook tracks IP addresses for profiles
  - Those IP addresses could be used to find fake profiles
  - Each bot will look at the control profile at specific times
  - This would be clear from analyzing the IP logs of each profile
    - There are a lot of people who log into Facebook a lot during the day but it would not be a regular intervals
- Scrubbing the pictures on profiles
  - This would stop the steganography communication
- Facebook could track the profile usage of particular profiles.
  - Bot masters will generally not use facebook for social networking
- Tineye for detecting information stored in images

References

1. http://i.zdnet.com/blogs/facebotisc08.pdf
2. http://i.zdnet.com/blogs/facebotisc08.pdf
3. http://www.hatswitch.org/~sn275/papers/stegobot.pdf