



Guest Editors

Ronaldo Salles

Military Institute of Engineering
Praça General Tibúrcio 80,
22290-270, R.J. – Brazil
salles@ieee.org

Guofei Gu

Texas A&M University
3112 TAMU, HRBB College
Station, TX 77843-3112 – USA
guofei@cse.tamu.edu

Thorsten Holz

Ruhr-University Bochum
Universitätsstrasse 150, 44780
Bochum – Germany
thorsten.holz@rub.de

Morton Swimmer

Trend Micro Deutschland, GmbH
Zeppelinstr. 1
85399 Hallbergmoos
Germany
swimmer@acm.org

Important dates

Paper submission:

1st Dec 2011

Acceptance notification:

1st Mar 2012

Final papers:

1st May 2012

Call for Papers

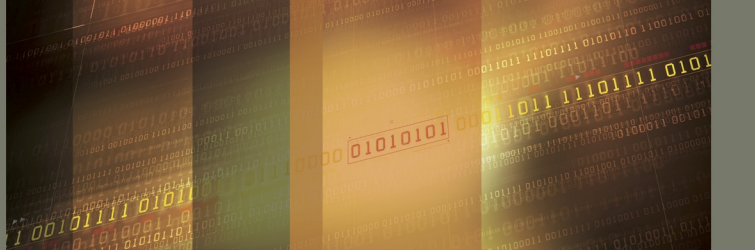
A Special Issue of Computer Networks On “Botnet Activity: Analysis, Detection and Shutdown”

Large scale attacks and criminal activities experienced in recent years have exposed the Internet to serious security breaches, and alarmed the world regarding cyber crime. In the center of this problem are the so called botnets -- collections of infected zombie machines (bots) controlled by the botmaster to perpetrate malicious activities and massive attacks. Some recent botnets are composed of millions of infected machines, making use of this attack vector inevitably harmfully. Hence, it is paramount to detect, analyze and shutdown such overlay networks before they become active. Research on botnet activity is mostly related to detection and disruption. Detection of botnets has focused on monitoring bot activities, especially during the spread of malicious software to infect new hosts (initial infection phase) and the communication messages exchanged between bots and botmasters (rallying and updating phases). Some behavioral aspects are common: bots have to signal the botmaster informing they are alive, each time their hosts are started; bots send messages whenever connecting and joining with the botnet; the botmaster has to send commands to each zombie machine before initiating malicious activities.

This special issue of Computer Networks is intended to foster the dissemination of high quality research in all aspects regarding botnet activity, detection and countermeasures. The objective of this special issue is to publish papers presenting detection algorithms, traffic monitoring and identification, protocols and architectures, as well as botnet modeling, behavior, simulation, statistics, dissemination, analysis, preventive procedures and possible countermeasures.

Only technical papers describing previously unpublished, original, state-of-the-art research, and not currently under review by a conference or journal will be considered. We solicit papers in a variety of topics related to botnet research including, but not limited to:

- Traffic Monitoring and Detection Algorithms
- Data Collection, Statistics and Analysis
- Modeling Behavior and Simulation
- Protocols and Architectures (IRC, HTTP, P2P, etc)
- Firewalls and IDS
- Cyber Crime Case Studies
- Reverse Engineering and Automated Analysis of Bots
- Honeypots and Honeynets
- New Platforms: Cellular and Wireless networks, Mobile devices, TV, etc.
- Legal Issues and Countermeasures
- Underground Markets, Vulnerability Markets and Zero-day Economics
- Mini-Botnets



Submission format

The submitted papers must be clearly written in excellent English and describe original research which is not published nor currently under review by other journals or conferences. Author guidelines for preparation of manuscript can be found at www.elsevier.com/locate/comnet

Submission Guideline

All manuscripts and any supplementary material should be submitted through the Elsevier Editorial System (EES). The authors must select "Special Issue: Botnets" when they reach the "Article Type" step in the submission process. The EES website is located at:

<http://ees.elsevier.com/comnet/>

Guide for Authors

This site will guide you stepwise through the creation and uploading of you article. The guide for Authors can be found on the journal homepage (www.elsevier.com/comnet/).