International Journal of Innovative
Computing, Information and Control
Volume **6**, Number **10**, October **2010**

ICIC International ©2010 ISSN 1349-4198
pp. 4305–4317

A USERID-CENTRALIZED RECOVERABLE BOTNET: STRUCTURE RESEARCH AND DEFENSE

Wei Wang[1,2], Binxing Fang[1,2], Xiang Cui[2] and Jinqiao Shi[2]

[1]Research Center of Computer Network and Information Security Technology
Harbin Institute of Technology
Harbin 150001, P. R. China

[2]Research Center of Information Security
Institute of Computing Technology, Chinese Academy of Sciences
Beijing 100190, P. R. China
wang.wei@hit.edu.cn; wangwei@software.ict.ac.cn

Received May 2009; revised October 2009

Abstract. *Nowadays, botnets have become common platforms for many Internet attacks. However, most of current Command and Control (C&C) architectures of botnets suffer from the risk of being shut down or poisoned. Once the C&C channel is disrupted, the whole botnet will become a set of isolated compromised machines. Consequently, considering how to construct a recoverable C&C channel in case it is closed is attractive for botmasters. Most of current research focus on botnet detection and monitor, but these are not enough. Defenders should research new attacks that could be developed by botmasters in the near future. In this paper, a recoverable botnet, extending current C&C channel designs with User Identity (UserID) Addressing, is proposed. It could recover the destroyed C&C channel with acceptable effort and latency which security defenders must pay more attention to. Based on the analysis of the UserID-centralized C&C architecture, possible defenses against this botnet are suggested. Security researchers should concern that traditional shutting down of a botnet may not eliminate the botnet really.*
Keywords: Botnet, Recoverability, User identity addressing, Defense

1. **Introduction.** Botnet is a common distributed computing platform for launching the Internet attacks such as distributed denial-of-service (DDoS), sending spam, seeding malwares, identity theft, phishing, etc. A botnet can be defined [19] as *A coordinated group of malware instances running on incoordinate resources that are remotely controlled via Command and Control (C&C) channels.* Here *malware* means bots are used to perform malicious activities and *incoordinate resources* means bots are installed without legal users' permission. The term *remotely controlled* means the botmaster could control these bots via C&C channel remotely. And the term *coordinated group* means that multiple (at least two) bots within the same botnet will cooperate to finish a command issued by the botmaster such as sending spams. The four terms discussed above reflect not only four features but also four components of a botnet that are bot, zombie, botmaster and command and control channel. Bot is the malware instance, zombie is the incoordinate resource, botmaster is the controller of a botnet and C&C channel is the control policy.

As botnet-based attacks are becoming more and more popular and dangerous, great efforts have been made on botnets detection, monitor, measurement and defence [2-4,7,9,11,34]. However, this is not enough. Besides current botnet threats, more attention should be paid in advance to novel botnet designs, which are possibly adopted by attackers in the near future. Otherwise, people will still be perplexed when facing new botnet-based threats developed by wicked attackers.