
Preface

Bots are computers infected with malicious program(s) that cause them to operate against the owners' intentions and without their knowledge. Bots communicate with and take orders from their "botmasters". They can form distributed networks of bots, or botnets, to perform coordinated attacks. Botnets have become the platform of choice for launching attacks on the Internet, including spam, phishing, click fraud, key logging, key cracking and copyright violations, and denial of service (DoS). More ominously, botnets can be an effective malware launching platform in such a way that a new worm or virus is sent out instantaneously by numerous bots. Such lightning strike significantly shortens the response time and patch window that network administrators need to perform basic maintenance. There are many millions of bots on the Internet on any given day, organized into thousands of botnets. It is clear that botnets have become the most serious security threat on the Internet.

New approaches are need for botnet detection and response because existing security mechanisms, e.g., anti-virus (AV) software and intrusion detection systems, are inadequate. Since bots are "computing resources", the botmasters have the incentive to keep the bots under their control for as long as possible. Therefore, the bots employ active evasion techniques to hide their activities. For example, malware (or botcode) can be "packed" to evade AV signature matching, bots use standard (or, common) protocols (e.g., IRC, `http`, etc.) for communication, and their activity level can be set to below the normal user/computer activity level, etc.

In June 2006, the U.S. Army Research Office (ARO), Defense Advanced Research Project Agency (DARPA), and Department of Homeland Security (DHS) jointly sponsored a workshop on botnets. At the workshop, leading researchers as well as government and industry representatives presented talks and held discussions on topics including botnet detection techniques, response strategies, models and taxonomy, and social and economical aspects of botnets.

This book is a collection of research papers presented at the workshop, as well as some more recent work from the workshop participants.

Network monitoring is essential to botnet detection because bots have to communicate with a command center and/or with each other relatively frequently to get updates and coordinate their activities. Chapter One, "Botnet Detection Based on

Network Behavior”, presents an approach to identify botnet command and control activities using network flow statistics such as bandwidth, packet timing, and burst duration. Chapter Two, “Honeynet-based Botnet Scan Traffic Analysis”, shows how to use a honeynet to capture bots, study their scanning behavior, and then infer some general properties of botnets.

A bot is a (compromised) computer running a malware or botcode. The botcode dictates when and where a bot should contact a command center and what (malicious) activities that bot needs to perform. Thus, if we can analyze the behavior of the botcode, we can provide the critical information for botnet detection and response. Chapter Three, “Characterizing Bot’s Remote Control Behavior”, describes an approach to differentiate a botcode and benign programs and identify the bot command and control behavior.

Malware or botcode often tries to evade and resist analysis. One evasion technique that botcode can use is to contain hidden behavior that is only activated when the (input) conditions are right. Chapter Four, “Automatically Identifying Trigger-based Behavior in Malware”, describes how to automatically identify and satisfy the conditions that will activate the hidden behavior so that the triggered malicious behavior of botcode can be observed and analyzed. Since many malware analysis techniques rely on virtual machines, an evasion or defensive technique used by the botcode or a remote botnet command server is to detect whether a bot is running on a virtual machine. Chapter Five, “Towards Sound Detection of Virtual Machines”, demonstrates that indeed it is quite feasible to detect virtual machine monitors remotely across the Internet.

A major difference between botnets and previous generations of attacks is that botnets are often used “for profit” (or, various forms of financial frauds). Chapter Six, “Botnets and Proactive System Defense”, analyzes how botnets can compromise the security of online economy and suggests several directions in proactive defense. Chapter Seven, “Detecting Botnet Membership with DNSBL Counterintelligence”, illustrates that “market-related activities” by the botmasters can be used to detect botnets. In the case study, the botmaster wants to check that his spamming bots are “fresh”, i.e., they are not listed in block-lists, so that they can be sold/rented for a good price to the spammer. However, look-ups by the botmaster can be detected as different from normal/legitimate look-ups, and thus his bots can be identified.

Botnet detection and response is currently an arms race. The botmasters rapidly evolve their botnet propagation and command and control technologies to evade the latest detection and response techniques from security researchers. If there are fundamental trade-offs and limitations associated with each type of botnets, then we can design countermeasures with the objective to minimize the utility (or increase the “cost”) of botnets. Chapter Eight is a study on taxonomy of botnets. It analyzes possible (i.e., existing and future) botnets based on the utility of the communication structures and their corresponding metrics, and identifies the response most effective against the botnets.

We believe that this book will be an invaluable reference for security researchers, practitioners, and students interested in developing botnets detection and response technologies. Together, we will win the war against botnets.

We wish to thank the generous financial support from the U.S. Army Research Office that made it possible to run the Botnet workshop and publish this book.

Atlanta, GA
Research Triangle Park, NC
August 2007

Wenke Lee
Cliff Wang
David Dagon

Botnet Detection

Countering the Largest Security Threat

Lee, W.; Wang, C.; Dagon, D. (Eds.)

2008, XII, 168 p., Hardcover

ISBN: 978-0-387-68766-7