Review of the book

"Botnet Detection"

by Wenke Lee, Cliff Wand and David Dagon

Springer 2008

ISBN-13: 978-1-387-68766-7

Dr. Joerg Gerschuetz

1 Summary of the review

"Botnet Detection - Countering the largest Security Threat" is a collection of eight excellent research papers. It is not a textbook on botnet detection where the reader is led from the basics to advanced topics. So the book can be only recommended to a reader with some background on botnets and their behavior.

2 Summary of the book

Botnets are considered the scourge of the internet. They are "commercially" available to launch attacks including spam, phishing, key cracking, denial of service (DoS) to name only a few. The operators of these botnets earn millions of dollar each year.
Existing security mechanisms, e.g. anti-virus (AV) software and intrusion detection systems (IDS), are often inadequate to detect the so called bots, i.e. computers that are infected and therefore part of a botnet. So new approaches are needed for botnet detection and response.

"Botnet Detection - Countering the largest Security Threat" is a collection of eight research papers presented at a workshop held in June 2006 by the U.S. Army Research Office (ARO), Defense Advanced Research Project Agency (DARPA), and Department of Homeland Security (DHS).

① **Botnet Detection Based on Network Behavior** (*W. Timothy Strayer, David Lapsely, Robert Walsh, and Carl Livadas*)

Current techniques for detecting botnets examine traffic content for IRC commands, monitor DNS for strange usage, or set up honeynets to capture live bots. The authors suggest a detection approach where *flow characteristics* such as bandwidth, packet timing, and burst duration are used to examine evidence of botnet command and control activity: First traffic that is unlikely to be part of a botnet is eliminated. Then the remaining traffic is classified and correlated to find common communications patterns for botnet activity. The results show that botnet activity can be axtracted from a traffic trace containing more than 1.3 million flows.

② **Honeynet-based Botnet Scan Traffic Analysis** (*Zhichun Li, Anup Goyal, and Yan Chen*)

Botnet scanning behavior is ingrained to the botnet because this is the most effective way for them to recruit new bots. Monitoring scanning is relatively easy, e.g. with a honeynet installed the botnet scanning traffic can be easily captured. Understanding the scanning behavior is very important since it will help to understand how to detect and prevent botnet propagation. The authors develop a general paradigm for botnet scan event extraction.

③ **Characterizing Bots Remote Control Behavior** (*Elisabeth Stinson and John C. Mitchell*)

A bot responds to commands over a "command-and-control" overlay network. Each bot command takes some number of parameters in some fixed order. These commands are implemented by

invoking operating system services on the infected system. The remote control of bots through parameterized commands separates bot behavior from normal execution of innocuous programs as it uses data received from the network (an untrusted source) in a system call argument (a trusted sink). This hypothesis is tested experimentally by tracking data received over the network as it propagates via DLL calls to other memory regions. Presence of these network data in selected system call arguments is an effective indicator for malicious bots.

④ **Automatically Identifying Trigger-based Behavior in Malware** (*David Brumley, Cody Hartwig, Zhenkai Liang, James Newsome, Dawn Song, and Heng Yin*)

Malware often contains hidden behavior which is only activated when properly triggered. Trigger-based behavior analysis if often performed manually, so even a small amount of assistance would speed-up the analysis. The authors design an approach for automatic trigger-based behavior detection and analysis using dynamic binary instrumentation and mixed concrete and symbolic execution.

⑤ **Towards Sound Detection of Virtual Machines** (*Jason Franklin, Mark Luk, Jonathan M. McCune, Arvind Seshadri, Adrian Perrig, Leendert van Doorn*)

Virtual machine monitor (VMM) detection has two direct implications for botnet remediation: First, it provides defenders with the ability to detect bots which use VMMs for improved stealth. Second, exploring VMM detection allows defenders to assess the extent to which intelligent bots can identify and potentially bias virtualized analysis environments such as high-interaction honeypots. The authors design, implement, and evaluate a practical timing-based approach to detect VMMs without relying on VMM implementation details.

⑥ **Botnets and Proactive System Defense** (*John Bambenek and Agnes Klus*)

Fraud and identity theft are the primary drivers of botnet growth and development. The key to reduce those threats is to take the financial motivation out of compromising consumer computers. If no money or less money can be made, less people will be interested in botnets. So a defense-in-depth dynamic has to be established for the weakest link - the unprotected wild of consumer PCs.

⑦ **Detecting Botnet Membership with DNSBL Counterintelligence** (*Anirudh Ramachandran, Nick Feamster, and David Dagon*)

Many Internet Service Providers and enterprise networks use DNS-based blackhole lists (DBSBL) to track IP addresses that originate spam, so that future emails sent from these IPs can be rejected. Botmasters are known to sell "clean" bots not listed in any DNSBL at a premium. So a *passive* analysis of DNSBL lookup traffic can help discover identities of bots as the botmasters themselves must perform these lookups to determine their bots blacklist status.

⑧ **A Taxonomy of Botnet Structures** (*David Dagon, Guofei Gu, Christopher P. Lee*)

It seems to be inadequate to simply enumerate the botnets seen in the wild as they are a dynamic, evolving threat. The structural and organizational *potential* of botnets has to be considered. A small number of likely structural forms for botnets can be identified, based on a utilitarian analysis. Metrics for measuring a botnets effectiveness, efficiency, and robustness can be developed.

3 Would you recommend this book?

Due to the nature of this book as a *collection* of independent research papers there is no continuous, uniform style. It is not a textbook on botnet detection, so do not expect a logical thematic sequence from the first to the last page! Basics are often only covered in the references - if you lack them this book does not explain them! So the book can be only recommended to a reader with some background on the topic. Nevertheless the papers presented are of very high quality and give a detailed overview of different botnet detection techniques.

The reviewer is a student of Applied IT Security at International School of IT Security, Bochum, Germany.