

# **BOTNET : AN EMERGING CYBER SECURITY THREAT WITH ITS EVALUATION**

**S. Aanjan Kumar**

*(Assistant Professor)*

**Sri Raaja Raajan College of  
Engineering & Technology,  
Karaikudi, Tamil Nadu, INDIA.**

**Dr. S. Poonkuntran**

*(Professor)*

**Velammal College of  
Engineering & Technology,  
Madurai, Tamil Nadu, INDIA.**

# **BOTNET : AN EMERGING CYBER SECURITY THREAT WITH ITS EVALUATION**

Copyright © : S. Aanjan Kumar  
Publishing Right © : VSRD Academic Publishing  
*A Division of Visual Soft (India) Pvt. Ltd.*

**ISBN-13: 978-81-931580-4-3**  
**FIRST EDITION, FEBRUARY 2016, INDIA**

*Typeset, Printed & Published by:*  
**VSRD Academic Publishing (A Division of Visual Soft (India) Pvt. Ltd.)**

**Disclaimer:** The author(s) are solely responsible for the contents of the papers compiled in this book. The publishers or its staff do not take any responsibility for the same in any manner. Errors, if any, are purely unintentional and readers are requested to communicate such errors to the Editors or Publishers to avoid discrepancies in future.

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without the prior permission of the Publishers & Author.

*Printed & Bound in India*

**VSRD ACADEMIC PUBLISHING**  
*A Division of Visual Soft (India) Pvt. Ltd.*

## **REGISTERED OFFICE**

154, Tezabmill Campus, Anwarganj, KANPUR – 208 003 (UP) (IN)  
Mob.: +91 99561 27040, Ph.: +91 512 6553705  
Web.: [www.vsrdpublishing.com](http://www.vsrdpublishing.com), Email: [vsrdpublishing@gmail.com](mailto:vsrdpublishing@gmail.com)

## **MARKETING OFFICE (NORTH INDIA)**

Basement-2, Villa-10, Block-V, Charmwood Village, FARIDABAD–121009 (HY)(IN)  
Mob.: +91 98999 36803, Ph.: +91 129 4036803  
Web.: [www.vsrdpublishing.com](http://www.vsrdpublishing.com), Email: [vsrdpublishing@gmail.com](mailto:vsrdpublishing@gmail.com)

## **MARKETING OFFICE (SOUTH INDIA)**

340, FF, Adarsh Nagar, Oshiwara, Andheri(W), MUMBAI–400053 (MH)(IN)  
Mob.: +91 9956127040  
Web.: [www.vsrdpublishing.com](http://www.vsrdpublishing.com), Email: [vsrdpublishing@gmail.com](mailto:vsrdpublishing@gmail.com)


# P R E F A C E

This book “**BOTNET: AN EMERGING CYBER SECURITY THREAT WITH ITS EVALUTION**” is about the introductory ideas on botnets used in real world in cyber space. It emphasizes the history, effect, threat, spreading and evaluation of botnet in the cyber world utilizing by the cyber criminals. It gives an ideology towards the botnet system, attacks and identifies the problem with botnet attacks in the computer system damage system leads to shut down by applying the special attack. It provides an idea for readers toward understanding of creating intelligent prevention methods over botnet to increase the data security and prevent system damage using special methods.

This book provides logical method of explaining various complicated concepts and stepwise methods to explain important topics and it's not only covers the entire scope of subject but explains the philosophy of the subject .This makes the clear understanding of subject more clear and makes more interesting. The book will very useful not only for students but also the subject teachers.

I wish to express my profound thanks to my guide **Dr. S. POONKUNTRAN**, *Professor, Department of Computer Science & Engineering, Velammal Engineering College and Technology, Madurai*, my well wisher **Dr. MANI SHANKAR**, *Head of Department & Professor, Department of Chemistry, Alagappa University*, then higher official permit me to carry my survey in field of botnet in my working college Sri Raaja Raajan College of Engineering and Technology,

**Chairman, Dean P.L. SUBRAMANIAN** and My colleagues, friends last but not least my all in all inspire living gods in front of me my *father* **Mr. P. SURESH KUMAR** and my *mother* **Mrs. S. SUSILA DEVI** to encourage me in this work helping me to making this book a reality.

 *S. Aanjan Kumar*

# CONTENTS

## **Chapter 1 : Cyber Security . . 1-52**

- CYBER SECURITY: A SHORT HISTORY ..... 3
- CYBER SECURITY TODAY ..... 6
- INTERNATIONAL CONFLICT IN CYBER SECURITY ..... 11
- CYBER SECURITY STANDARDS ..... 20
- CYBER ATTACK CATEGORIES..... 22
- THE RISE OF MALICIOUS CODE..... 25
- RISKS IN CYBER SECURITY ..... 29
- DETERRENCE OF CYBER ATTACKS..... 31
- CYBER SECURITY THREATS..... 41
- CYBER RISK ..... 46
- CYBER ATTACK MITIGATION STRATEGIES ..... 48

## **Chapter 2 : Most Advance Threat in Cyberspace: BOTNETS . . . . . 53-106**

- BOTNET..... 55
- CONTROLLING THE BOTNET ..... 59
- WHY BOTNETS ARE SO DANGEROUS ..... 60
- THE BOTNET SAGA BEGINS..... 61
- HISTORIC EVENTS LEADING TO BOTNETS..... 65
- CHARACTERISATION OF BOTNETS..... 73
- BOTNETS CHARACTERISATION USE OF MALWARE ..... 79
- EVOLUTION OF BOTNETS ..... 82
- SPREADING MODELS OF THE BOTNETS..... 85
- MOTIVATION AND USAGE OF BOTNETS..... 92
- ATTACK POTENTIAL AND THREAT CHARACTERISATION ..... 101

- BOTNET SIZE AND BOT ORIGIN ..... 105

**Chapter 3: Introduction to BOTNET Intrusion Detection Systems ..... 107-146**

- A REVIEW ON INTRUSION DETECTION SYSTEMS ..... 110
- INTRUSION DETECTION MODELS ..... 110
- COMPUTER ATTACK TAXONOMY ..... 113
- SIGNIFICANT FEATURE SELECTION FOR INTRUSION DETECTION ..... 122
- ATTACKS ON INTRUSION DETECTION SYSTEMS ..... 123
- ATTACKS ON BOTNET TOOLS ..... 128
- DESIGNING EFFICIENT INTRUSION DETECTION SYSTEMS ..... 131
- ANALYSIS OF FLOW RECORDS ..... 135

**Chapter 4: Enumeration of Powerful Peer-to-Peer BOTNET ..... 147-170**

- OVERVIEW OF POWERFUL P2P BOTNET ..... 151
- PEER-TO-PEER PROTOCOL..... 152
- INFECTION VECTORS AND AFFILIATE SCHEME ..... 154
- CODE CHANGES ..... 161
- BOTNET CRAWLER..... 164
- THE ROLE OF GOVERNMENTS IN BOTNETS..... 168

**Chapter 5: ZEUS: Evolving BOTNET ..... 171-180**

- ZEUS NETWORK TOPOLOGY ..... 173
- ZEUS ENCRYPTION..... 175
- ZEUS COMMUNICATION PATTERNS..... 175
- ZEUS FORMING ALGORITHM..... 178

**Chapter 6: A Master: Gameover  
ZEUS BOTNET ..... 181-194**

- RECENT REPORTS ON GAMEOVER ZEUS BOTNET ..... 183
- GAMEOVER ZEUS BOTNET ..... 185
- IS ZEUS P2P BOTNET POWERFUL?..... 187
- GAME OVER ZEUS BOTNET: EVOLUTION ..... 189
- ACTION PERFORMED BY GAMEOVER ZEUS  
BOTNET..... 193

**Chapter 7: Future Enhancement  
with Study ..... 195-198**

- FUTURE ENHANCEMENT ..... 197

**References ..... 199-218**

- REFERENCES ..... 201

