Understanding the Threat of Botnets

Basheer Al-Duwairi
Department of Network Engineering and Security
Faculty of Computer and Information Technology
Jordan University of Science and Technology, Irbid 221100, Jordan
Email: basheer@just.edu.jo

A Half-Day Tutorial

Botnets represent an immanent threat for today's Internet. The people directing these botnets, called botmasters or botherders, are increasingly using these large networks of compromised machines to generate different types of attacks that include spam, distributed denial of service (DDoS), click fraud, identity theft, etc. In this context, botnets can be viewed as a dangerous attack infrastructure and a source for many of the security incidents that we see every day. These malicious networks generally operate in two main planes: the command and control (C&C) plane where bots receive commands from the botmaster and take several forms with different levels of sophistication and robustness, and the activity plane where bots execute these commands to launch different types of attacks.

In this tutorial, an in depth understanding of botnets is provided. We first discuss fundamental concepts of botnet, including formation and exploitation, lifecycle, and different kinds of topologies. Then, several related attacks, detection, tracing, and countermeasures, will be introduced. Academic researchers will appreciate the exposure to the latest research in this field, a consolidated overview of the relevant papers on this topic, as well as online resources.

Outline

1. **Fundamentals and terminology:** Basic networking and routing protocols; Cryptography/cryptanalysis.
2. **Introduction to malware:** Droppers, agents, IRC bots, Trojans; Evolution of attack tools.
3. **Botnet formation:** Propagation**,** Life cycle**,** Command and control (C&C) techniques in use,Topologies, Fast flux, Domain flux,.
4. **Botnet characteristics:** Botnet size, Geographical distribution, spatial and temporal characteristics of botnets.
5. **Botnet-Based Attacks:** Distributed Denial of Service, Email Spam, Click Fraud, phishing attacks.
6. **Countering Botnet-Based Attacks:** DDoS mitigation, Spam detection, detecting and mitigating other attacks.
7. **Botnet Detection:** Honeypot/Honeynets, Sink-hole based detection, traffic traces based detection, DNS black list based detection.

Prerequisites

A basic understanding of IP networking, network protocols, and routing as well as an understanding of computer security fundamentals is required.

Audience

The tutorial is intended to be useful to system administrators, network administrators and computer security practitioners and researchers.

Speakers Biography

Basheer Al-Duwairi received the PhD and MS degrees in computer engineering from Iowa State University in Spring 2005 and Spring 2002, respectively. Prior to this, he received the BS degree in electrical and computer engineering from Jordan University of Science and Technology (JUST) Irbid, Jordan in 1999. He joined the JUST as a faculty member in Fall 2005. The focus of his PhD work was on designing and analyzing practical schemes for mitigating and tracing-back DDoS attacks in the Internet. He has coauthored several research papers in these fields. His research interests are in the areas of Internet security and real-time systems. http://www.just.edu.jo/~basheer

Professional services (tutorials)

- Tutorial Speaker: “Understanding the threat of Botnets”, Half-day tutorial, The International Conference on Information and Communications Systems (ICICS2009), Amman, Jordan.

- Tutorial Co-Speaker: “Internet Infrastructure Security”, Half-day tutorial, IEEE Hot Interconnects 2005, Stanford University, USA. (Co-speacker: Dr. G. Manimaran, Iowa State University).

Relevant publications

- B. Al-Duwairi and AbdulRaheem Mustafa, “Request Diversion: A Novel Mechanism to Counter P2P-Based DDoS Attacks”, Accepted for publication in International Journal of Internet Protocol Technology (IJIPT), Special Issue on: "Recent Advances in Network Security Attacks and Defences".
- B. Al-Duwairi and G. Manimaran, “JUST-Google: A search engine based defense against botnet-based DDoS attacks,”. In Proc. IEEE ICC 2009, Dersen, Germany 2009.
- B. Al-Duwairi and G. Manimaran, “Novel Hybrid Schemes Employing Packet Marking and Packet Logging for IP Traceback,”. In Proc. of IEEE Transactions on Parallel and Distributed Systems (IEEE TPDS), Volume 17 , Issue 5, May 2006, Pages: 403 - 418.

- B. Al-Duwairi and G. Manimaran, “Distributed Packet Pairing for Reflector Based DDoS Attack Mitigation,”. In Proc. Of Computer Communications Journal. Volume 29, Issue 12, 4 August 2006, Pages 2269-2280.
- B. Al-Duwairi and G. Manimaran, “Victim-Assisted Mitigation Technique for TCP-Based Reflector DDoS Attacks,”. In Proc. of IFIP Networking May 2005, Waterloo, Ontario, Canada.
- B. Al-Duwairi and G. Manimaran, “Intentional Dropping: A Novel Scheme for SYN flooding Mitigation,”. In Proc. of 8th IEEE Global Internet Symposium/Infocom March 2005, Miami, FL, USA.
- B. Al-Duwairi and Tom E. Daniels, “Topology Based Packet Marking ,”. In Proc. of IEEE International Conference on Computer Communications and Networks (ICCCN 2004), Chicago, IL, USA.
- B. Al-Duwairi and G. Manimaran, “A Novel Packet Marking Scheme for IP Traceback,”. In Proc. of IEEE International Conference on Parallel and Distributed Systems (ICPADS 2004), Newport Beach, California, USA.
- B. Al-Duwairi, A. Chakrabarti, and G. Manimaran, “An Efficient Packet Marking Scheme for IP Traceback,”. In Proc. of Networking 2004, Athens, Greece.