# Chapter 14
# Successful Computer Forensics Analysis on the Cyber Attack Botnet

**Kavisankar Leelasankar**
*Hindustan Institute of Technology and Science, India*

**Chellappan C.**
*GKM College of Engineering and Technology, India*

**Sivasankar P.**
*National Institute of Technical Teachers Training and Research, India*

## ABSTRACT

*The success of computer forensics lies in the complete analysis of the evidence that is available. This is done by not only analyzing the evidence which is available but also searching for new concrete evidence. The evidence is obtained through the logs of the data during the cyberattack. When performing analysis of the cyberattack especially the botnet attacks, there are many challenges. First and the foremost is that it hides the identity of the mastermind, the botmaster. It issues the command to be executed using its subordinate, the command and control (C&C). The traceback of C&C itself is a complex task. Secondly, it victimizes the innocent compromised device zombies. This chapter discusses the analysis done in both proactive and reactive ways to resolve these challenges. The chapter ends by discussing the analysis to find the real mastermind to protect the innocent compromised system and to protect the victim system/ organization affected by the botnet cyberattack.*

## INTRODUCTION

Successful prosecution of computer-based crime is dependent upon the investigation. The investigator should be asking all these questions like who, what, how and when a criminal event occurred. It depends upon how the evidence is examined. The general public will not understand or even know that they are under some kind of cyber attack. Victim of these attacks is not only the large corporations but also the

DOI: 10.4018/978-1-5225-4100-4.ch014

unaware public. The hackers come with the number of ways to bypass or intrude the network using the number of methods. First and foremost thing they do is that they hide their identity or they use the trusted source identity to intrude the network. They try to compromise the number of cyber devices, where these cyber devices become the compromised zombies. These compromised zombies cyber devices belong to the unaware public. The hackers use the internet which provides them the borderless environment. The internet, compromised zombies are used and they are brought into a network. This network is very powerful and it can be used to launch the intended attack on the intended victim.

Botnets are networks of robots or robot net. A software program bot obeys the instructions of command-and-control (C&C). They act as remotely located, a single coordinated central collection point of the bots. They would be taking over a remote machine (victim 1) and using that, attack another machine (victim 2). Botnets are compromised hosts under a common C&C (command and control) server. Their purpose is to produce Denial of Service attacks (DOSs), id theft, flood the user with spams, and many more.

A large number of the system is compromised using Active worms. These compromised systems are the bots or zombies. The botnet is formed by these large number bot or zombies when networked together with help of the C&C. The number of destruction done using botnet: (i) large-scale distributed voluntary advertisement through emails spam or malware. (ii) large scale sniffing of traffic which gives access to critical information that can be misused. (iii)The network components are destroyed by launching the massive DDoS attack.

Botnet when comparing with customary malware is more dangerous because of the C&C channel. It is one of the high-risk security threats. Where the malware used for fun is now turning to be malware used for financial benefit.

The detailed analysis and discussion are made on onetime request flooding using a Botnet are generally detected and defended against, using a number of schemes. The detection schemes provide the detection of three major components of Botnet architecture, namely, Bot, C&C, and Botmaster. These detection schemes are in two modes, active and passive. First, the passive detection of Bot is done by two major ways i.e. Correlation and Behavioral analysis.

There are various Botnet Detection Schemes; a few botnet detection schemes developed are Mining-based Detection, Signature-based Detection, and Anomaly-based detection techniques. Most importantly the detection scheme like Host-based detection is a detected scheme built on the host system. Some of the Host-based detection is a detected schemes are HoneyPots / Virtual HoneyPots, DNS- based detection techniques, Infiltration, Filtering, Packet Filtering, Remedial measure and Index Poisoning Attack.

For performing the forensic analysis the trace back to botmaster is required. Packet marking Techniques is used to Traceback of Botmaster, similarly Probabilistic Packet Marking Schemes is also used in Traceback of Botmaster, Other Schemes like Deterministic Packet Marking Schemes, and Probabilistic Packet Marking Schemes.

Even using all these techniques one of the most challenging tasks of the botnet network is that the identity of the botnet master is hidden, Traceback to command and control is also very difficult, since the attack is from the compromised zombies, these compromised zombies are the unaware public who get victimized by the crime they haven't done. A proper computer forensics investigation is required here. In the first instance, you will criminalize the compromised zombies. But when you criminalize you have to criminalize a huge number of compromised system that is legally impossible adding to that point they are totally unaware what is happening. It is the part of the security experts to build all the cyber devices with additional security features.