Botnets

Introduction

A botnet is a network of computers infected by a remote attacker, who controls them in a distributed manner for malicious and profit-making purposes. These infected computers form a network of software agents (e.g., bots) at the attacker's service. The attacker becomes the operator of a complex and powerful network whose services will ultimately be sold to organizations of all kinds. For example, the network's services can be sold to criminal organizations for the execution of large-scale coordinated attacks, such as distributed denial-of-service attacks, spamming campaigns, the sale of illegal products, and so on.

In this chapter, we present the origin and current techniques that make the existence of these networks possible. We outline the necessary phases for their construction, study the architectures, protocols, and communication models that enable them. We survey some of the techniques used by operators to ensure that infected computers go undetected and their networks are not dismantled. Finally, we look at some specific examples of botnets that have been discovered and present some data on the economic model that guaranteed their existence.

Objectives

The aims to be achieved with this chapter are the following:

1. To know what a botnet is and to understand how they emerged.

2. To know and understand the propagation model of a traditional botnet.

3. To know and understand the communication and collaboration model between infected nodes and operators.

4. To explore some of the techniques used by the operators, e.g., to protect their equipment and prevent the botnet from being dismantled.

5. To understand the economic model that promotes the creation and maintenance of a botnet, as well as the associated activities.

1. Background and preliminaries

A botnet is understood today as a collection of computers connected to the internet, whose resources (such as memory, process execution, file systems, and network connections) are controlled remotely without the knowledge of their users and/or owners. Botnet operators (often known as botmasters) create the network by spreading malicious code that infects the resources of future botnet computers, ensuring their permanent control.

Origin of the term

The term botnet comes from the combination of the following two words: ro**bot** and **net**work.

Once infected, botnet computers are viewed by their operators as a collection of software robots at the service of the botnet's clients. These clients can rent the computers to carry out activities such as spam campaigns, distributed denial-of-service attacks, storage of illicit multimedia content, and so on. Most of the infected computers, and future botnet robots, are typically home computers, often actively connected to the internet for extended periods (hours, days, weeks) and with relatively low levels of security protection .

The botnet operator (usually the one responsible for finding and infecting the computers) periodically sends control messages via traditional protocols such as IRC (Internet Relay Chat) or HTTP (Hypertext Transfer Protocol). The botnet's robots can even be reprogrammed by third parties (sometimes factions from different malicious communities) to expand their domains or reclaim resources from existing botnets .

A botnet consists of equipment infected by malware, to offer their resources to illegitimate services. Such equipment, referred to as zombies, agents or just bots, are controlled remotely, in a distributed manner, by one or more operators (referred to as botmasters).

Botnets have not always been associated to illegitimate services. Next, we explore the origins of these networks. We discuss, though not exhaustively, the evolution of their services over the past few years. As we will see, botnets have not always had the negative connotation they currently carry. Some were initially conceived to automate the maintenance and updating of some pioneering internet services.

1.1. A brief timeline of known botnets

Botnets emerged in the late 1980s. Figure 1.1 summarizes, in a non-exhaustive way, the name and (approximate) date of appearance of some of the botnet deployments that have had the greatest impact since then.

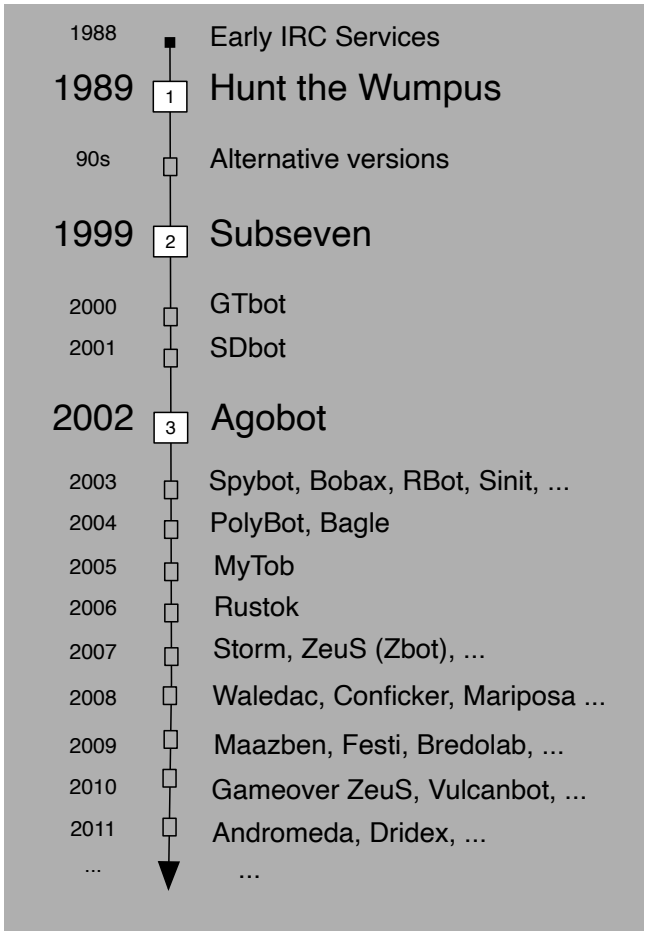

Figure 1.1. Brief timeline of known botnets since the late 80s.

Hunt the Wumpus

Considered by most as one of the earliest botnets in history, Hunt the Wumpus is also a famous video game that pioneered some artificial intelligence techniques. It is a conversational adventure networked through a command console to parse remote user actions in the game. The original version of the game, programmed in Basic, dates back to the 1970s. The player has to travel through a geometric structure (similar to a dodecahedron) composed of rooms and tunnels. Similar to the myth of the Minotaur, a mysterious monster, the Wumpus, is hidden within rooms and tunnels, waiting for the players and devour them. Additionally, some rooms may contain other deadly traps (bottomless pits, giants bats, etc.

The emergence of the first botnet is closely linked to the spreading of IRC (Internet Relay Chat) tools, as well as the online version of the Hunt the Wumpus game via IRC channels. Such first botnets, initially offering legitimate and harmless services, were conceived for the automation of virtual management tasks for the IRC channels. Operators of those first botnets developed tools and services to monitor and maintain games for IRC users. Those automated tasks, referred to as platform's bots, had to be available 24 hours a day to offer users the opportunity to play with them. Quickly, and spontaneously, similar networks were deployed to support operators of other services.

An important aspect in the development of these precursors to today's botnets is the ability to create a communication channel between operators and bots, as well as the inclusion of access control mechanisms to prevent third parties from taking control of the network's management equipment. Most architectures from this first period were based on control channels, through which operators could communicate command and control instructions, such as service initialization, task resumption, version updates and maintenance. These bots evolved from simple autonomous programs capable of playing games and entertaining internet users, into automated task managers, capable of launching new applications for third parties. It is common to find in the source code of those early bots from '90s the ability to create user accounts with layered privileges, as well as the inclusion of console commands with the ability for users with sufficient privileges to execute macros and scripts.

The term **botnet** was first used in 1993, referring to the creation of IRC repeater networks by controlling ordinary computers connected to the internet. Controlling these computers to form the IRC server network, relied on using the protocol's own commands. Since this initial use in 1993, botnets have evolved into complex networks of infected computers controlled by the operators who spread the infection.

It was not until the late 1990s that the first botnets with malicious intent emerged. One of the first significant cases to highlight was the deployment of bots based on the large-scale infection of the IRC/Jobbo worm and the subsequent installation of the SubSeven tool on the infected machines. The IRC/Jobbo worm's transmission vector was the remote exploitation of programming errors in IRC clients of the time (primarily the mIRC client for MS Windows systems). By exploiting vulnerabilities and subsequently escalating privileges, the result was the creation of a network of computers controlled by injecting Trojan-type malware into the victims. The tool installed on these computers, SubSeven, gave the botnet operator complete administrative control over each infected machine.

Complementary reading

A complementary reading to understand the evolution of botnets is the article “The Evolution of Malicious IRC Bots”, published by Symantec and written by John Canavan. It reports a complementary case to the Subseven spreading, known as Pretty Park's. Just like Subseven's large-scale spreading, Pretty Park is characterized with the installation of trojan malware, which allows malware operators full control over the infected devices.