Chapter 42
Botnets and Cyber Security:
Battling Online Threats

Ahmed Mansour Manasrah
National Advanced IPv6 Center, Malaysia

Moein Mayeh
National Advanced IPv6 Center, Malaysia

Omar Amer Abouabdalla
National Advanced IPv6 Center, Malaysia

Nur Nadiyah Suppiah
National Advanced IPv6 Center, Malaysia

ABSTRACT

The Internet, originally designed in a spirit of trust, uses protocols and frameworks that are not inherently secure. This basic weakness is greatly compounded by the interconnected nature of the Internet, which, together with the revolution in the software industry, has provided a medium for large-scale exploitation, for example, in the form of botnets. Despite considerable recent efforts, Internet-based attacks, particularly via botnets, are still ubiquitous and have caused great damage on both national and international levels. This chapter provides a brief overview of the botnet phenomena and its pernicious aspects. Current governmental and corporate efforts to mitigate the threat are also described, together with the bottlenecks limiting their effectiveness in various countries. The chapter concludes with a description of lines of investigation that could counter the botnet phenomenon.

INTRODUCTION

A botnet is a collection of computers connected to the Internet that can interact to accomplish distributed activities, usually of an illegal nature. Such systems comprise a set of compromised machines, called *drones* or *zombies*, that run a malicious software application called a *bot*. The bot allows each individual system to be controlled discretely, without the owner's knowledge. And given the nature of the Internet and the prevalence of insecure systems, vast botnets can be created that have very large combined computing power. They can be used as a powerful cyber weapon to take down online services or as an effective tool for making illicit profits. Of course, the owner of a botnet could be located anywhere–another city, country, or continent–but importantly, the Internet is structured in such a way that the botnet can be controlled anonymously. Bots can be controlled either directly using built-in commands, or indirectly via a control centre or other compromised machines on the network.

DOI: 10.4018/978-1-4666-5942-1.ch042

The growth of botnets, and the increasingly inventive ways in which they are being used to steal personal data, harm government and business operations, or deny users access to information and services represents a serious threat to the Internet economy, to individuals' online privacy, and to national security. Unfortunately, whenever an attack occurs or an exploit is found, the underlying technology, being the easiest to blame, is held at fault. However, legal and political frameworks can be as powerful as technology in addressing cyber-security threats, and any technical solution must be aligned with community standards and values. Therefore, attempts to mitigate the botnet threat should not be limited to purely technical solutions. Although it is clear that technology is an important starting point, we still need to view the challenge with a clear and broad perspective as, perhaps, a mission integration challenge. In fact, it may be that the botnet threat can only be met through an integration of technology, strategy, policy, and legislation. This is supported by the fact that the substantial national and international efforts of various organizations to raise awareness, track malware, develop or amend legal frameworks, strengthen law enforcement, and improve the response to new threats in general have had little effect.

Thus, we argue that technology alone cannot make everything possible. Moreover, it is not enough for one country or one community to independently self-organize to try and address the problem, if others do not do so as well. Therefore, an international cross-border cyber security platform is needed. The platform should define a global research and development agenda by developing a global cyber security technology framework that can be used to establish an effective mechanism for knowledge dissemination at the national and global level. Moreover, the framework should also provide a better and dynamic global coordinated response to new attacks by possibly increasing monitoring activities at the global scale. Only a holistic approach involving an integrated mix of policy, operational procedure, and technical ingenuity can ensure effective and integrated information sharing, co-ordination, and cross-border co-operation. The success of such efforts would require the active engagement of all stakeholders. Such an effort, moreover, would demonstrate significant advances in the international community's ability to overcome obstacles to executing global co-ordinated actions. This chapter attempts to provide a comprehensive background on extant efforts and challenges faced by different organizations in the battle with botnets.

BACKGROUND

The term bot, short for *robot*, is derived from the Czech word *robota*, which means "work" (Saha & Gairola 2005). Usually, a network of tens to hundreds of thousands and, in some cases, several millions of bots constitute what is known as botnet. These bots are handled and commanded by a single, or sometimes a group, of commanders (attacker/botmaster) who have the ability to remotely instruct bots to perform certain tasks. Since the backbone of any botnet is the individual compromised host, botnets are seen in a variety of computer systems–on computers at homes, schools, business places, and governmental offices–all of which may contain valuable data that can provide financial benefits to the attacker (Cooke, Jahanian, Mcpherson, & Danny 2005; Dagon et al., 2005; Gu 2008).

MessageLabs, owned by Symantec, performed a survey in 2009 to identify the most active botnets (Symantec 2009). As shown in Table 1, Cutwail was the largest active botnet, which sent out 74,115,721,081 spam E-mail messages a day with a size of 1400–2100 KB each. Brazil, with 14% of infected hosts, was the country most affected by Cutwil. In addition, note that even Darkmailer, the lowest ranked botnet, sent out 93,954,453 spam E-mail messages a day with an estimated size 1 KB each (Symantec 2009).