U. PORTO

FEUP FACULDADE DE ENGENHARIA
UNIVERSIDADE DO PORTO

A hands-on approach on botnets for a learning proposal

Specification

Computer Systems Security (EIC0072)

Eduardo José Valadar Martins (ei11104@fe.up.pt)
João Pedro Matos Teixeira Dias (ei11137@fe.up.pt)
José Pedro Vieira de Carvalho Pinto (ei12164@fe.up.pt)
João Carlos Teixeira de Sá (ei11142@fe.up.pt)

Group 6 - Theme 12

October 12, 2015

Contents

1 Introduction

A botnet is, by definition, the name given to any collection of compromised hosts (PCs) controlled by an attacker remotely. Botnets generally are created by a specific attacker or small group of attackers using one piece of malware to infect a large number of machines. The individual machines that are part of the botnet are, generally, called *bots*, *nodes* or *zombies*. There are botnets of various sizes (there is no minimum number of infected machines to the group be called a botnet), and they can vary from small ones with hundreds or low thousands of infected machines and larger ones with millions of compromised hosts [2].

There are specific cases where bots perform beneficial and even vital activities [3], for example, the use of web crawlers by search engines to index webpages can be considered as a kind of bot, and, in other hand, the participants of SETI@home initiative (Search for Extraterrestrial Intelligence), are, voluntary, part of a large botnet used for analyze radio telescope data for evidence of intelligent extraterrestrial life [4].

Attackers usually install bots by exploiting vulnerabilities in software or by using social engineering tactics to trick users into installing the malware. Users are often unaware that their computers are being used for malicious purposes [3].

Botnets can be used for various activities but the most traditional and common use is for DDoS (Distributed Denial of Service) attacks. These attacks rely on the computing power and bandwidth of hundreds or thousands of PCs to send huge amounts of traffic at a specific Web site in an effort to knock the site offline. Other uses for botnets are, for example, spamming, sniffing traffic, keylogging and even manipulating online polls and games [1].

2 Proposal

As today, botnets have a great impact in technological world since they are capable of strong attacks on services and remaining undetected sometimes along years. We think this is a field in computer security where there is still lack of learning tools and proper documentation for understand the behavior and possibilities of using the botnets.

So we propose a two-parts work, namely:

- Botnet Lab Framework - A simple-approach and extensible open-sourced framework for making and deploying a botnet system completed with instructions and samples.
- Botnet Wiki - A website/wiki with detailed information about botnets, its impact and state of art.

With this we try to build a complete solution for the ones who are interested in learning about this computer security topic and, even, using this as a teaching solution on this matter.

2.1 Botnet Lab Framework

2.2 Botnet Wiki

topics as history of botnets, botnet detailed structure and features, kinds of attacks and uses and, finally, research made on the topic complemented with countermeasures and existing task-forces that detect and dismantle botnets.

3 Planning

References

[1] P. Bächer, T. Holz, M. Kötter, and G. Wicherski. Know your enemy: Tracking botnets. 2005.

[2] Kaspersky Lab. What is a botnet?, April 2013.

[3] Microsoft. What is a botnet?, 2015.

[4] University of California. What is seti@home?, 2015.