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 19, 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 [3].

There are specific cases where bots perform beneficial and even vital activities [4], for example, the use of web crawlers by search engines to index web-pages can be considered as a type of bot, also, the participants of SETI@home initiative (Search for Extraterrestrial Intelligence), are, voluntary, part of a large botnet used to analyze radio telescope data in order to track evidence of intelligent extraterrestrial life [5].

Attackers usually install bots by exploiting vulnerabilities in software or by using social engineering tactics to trick users into installing malware. Users are often unaware that their computers are being used for malicious purposes [4].

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 the technological world since they are capable of strong attacks on services while remaining undetected for long periods of time. We think this is a field in computer security where there is still lack of learning tools and proper documentation for the better understanding of the behaviour and possibilities of using botnets.

So we propose a two-parts assignment, 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 tool on this matter.

2.1 Botnet Lab Framework

With the intuit of having a real hands-on tool for testing and developing proposes we will create a botnet lab framework, a botnet tool based on the IRC communication protocol, with built-in functionalities and an easy way of expanding functionalities, in a framework way.

As of now we are considering a simple bot framework with following built-in features:

- Keylogger (Capture and record computer users' keystroke);
- Screenlogger (Take print-screens of users' desktop);
- Webcam-stream capture functionalities;
- Spam;
- Distributed Denial of Service (DDoS);
- Private data scraping.

In addition to this bot framework there will also be added an IRC server part with the needed functionalities to control bots in a Command and Control way. For now we are considering using the open-source server *IRCD-Hybrid* [6].

The tool will be developed having in mind the following ideas:

- Encrypt all traffic between C&C and Bots
- Explore a pre-known exploit as a way of propagation (present in an old software or tool for example)
- Camouflage: make the bot run as part of something that usually runs on the target system
- Implementation of code obfuscation tools
- Bot self-propagation (Point-Of-Distribution - Worm)

The tool development will be done using Python Programming Language 2.7 [2] mainly due to its great on-line community in terms of size and amount of open-source resources available.

2.2 Botnet Wiki

In the botnet wiki, besides of the instructions/tutorials on the *Botnet Lab Framework*, there will be added general information about botnets including topics as the following:

- History of botnets;
- Botnet detailed structure and features (botnet anatomy);

- Kinds of attacks & uses;
- Current research;
- Countermeasures;
- Task-forces that detect and dismantle botnets;
- Good uses of botnets.

For this will be using the web standard technologies, namely HTML5, CSS3 and JavaScript.

3 Planning

In terms of planning, our team has already been divided by themes with the thematic *Botnets*. As for the first half of the project, where planning and research for the second half is done, we've made a simple division of sub-themes, which are:

- Anatomy
- Types of Attacks
- Countermeasures
- Historical occurrences of botnets the their impact

Most of this research's resulting content, as mentioned above, will be present in our Wiki, but more importantly, the research done on these items will the guide line for our future implementations. Each team member by the beginning of the week 19th of October, will hand-in his research done on his assigned topic and by the end of that same week all the work will be merged and ready for delivery on the 26th of October.

For the second part, the team will be divided in to two teams of 2, which for the duration of time until the delivery date, will work on two separate parts, gathering both teams' content of the very end composing the final project.

References

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

[2] Python Software Foundation. Python programming language, 2015.

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

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

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

[6] IRCD-Hybrid Development Team. Ircd-hybrid, 2015.