Botnet Analysis Framework

Ali Shiravi and Ali A. Ghorbani {ali.shiravi, ghorbani}@unb.ca

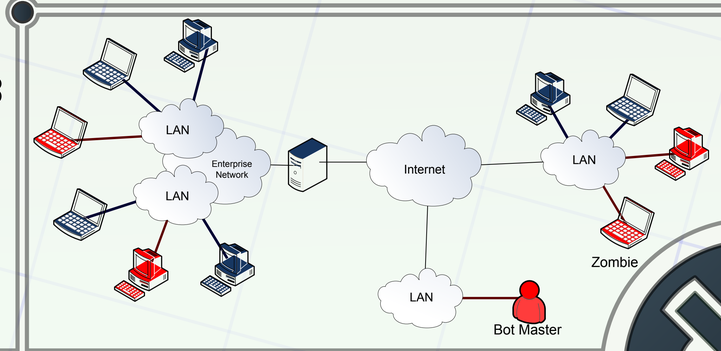
Introduction

Botnet is a coordinated group of malware instances (bots) that are controlled by a botmaster via some command and control (C&C) channel.

Botnets are the largest threat to Internet security. Most of the attacks and fraudulent activities on the Internet are carried out by malicious software, i.e., malware, which includes viruses, trojan, worms, spyware, and recently botnets. Such malware has risen to become a primary source of most of the scanning, distributed denial-of-service (DDoS) activities, direct attacks, and fraudulent activities taking place across the Internet.

All bots distinguish themselves from the previous malware forms by their ability to establish a command and control (C&C) channel through which they can be updated and directed by a botmaster. Traditionally 3 structures are defined for botnets:

1) Centralized
2) Peer-toPeer
3) Random



Background

Research community has been pursuing techniques to detect and respond to these malicious activities. A variety of techniques have been developed and applied to various data sources. Counteracting this emerging threat requires better techniques that assist in identify botnets (bots and/or their C&C servers) and providing the mechanisms necessary to mitigate their damage and defend against them. Botnets exhibit properties that require new approaches for detection and elimination.

However, these projects have largely been pursued in isolation and final result as single-purpose collection of methods, analysis results, and response directives.

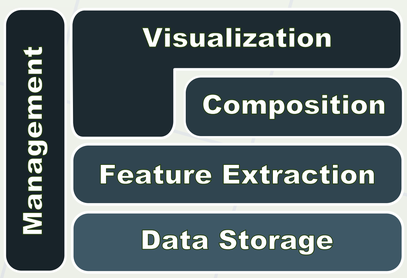
Much of the efforts within current projects are directed at tuning the system for a very specific C&C structure and bot behavior. As a result, systems tend not to provide comprehensive detection coverage for botnet activity across a spectrum of structures and communication protocols. Thus, to effectively cover the potential threats, it is desirable to provide a platform which integrates many detection systems that provide complementary coverage and provide the necessary mechanisms to customize the methods or manipulate their workings. This would necessarily mean the requirement to add, remove, rearrange, and rework the components in question.

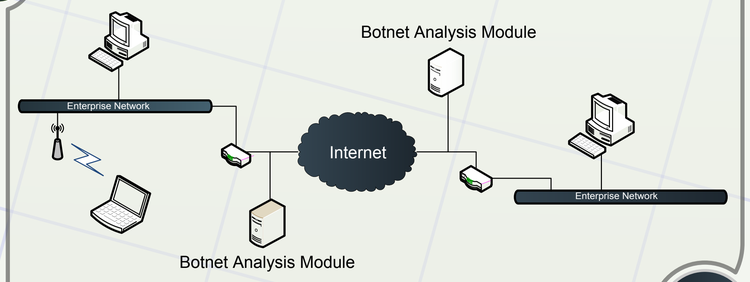
Objectives

We intend to addresses the research questions involved in implementing such a framework.

A Botnet Analysis Framework is a framework in which it defines, how to organize the modules, methods, components and structures associated with the concept of analysing Botnets, to gain better iinsight to how we should defend againt it.

The concept of defence here encompasses detection, mitigation, and visualization. The various top-level components are shown in the following diagrams.





Benefits

The design of this framework aims to facilitate botnet analysis by allowing enterprises, designers, researchers and programmers to spend more time on meeting requirements rather than dealing with the more standard low-level details of providing a working system and methods.

For example, an enterprise using such a framework to analyse the existance of bots on their network can focus on the operations of high level detectors and mitigation methods, rather than the mechanics of components facilitating defence.

An incomplete list of the overall features would be of the following attributes:

- Low learning curve to use the framework.
- Extensibility
- Scalability
- Open interfaces (API)

network security laboratory

UNIVERSITY OF NEW BRUNSWICK

UNB