Peer-To-Peer in Botnets

Moritz Marc Beller,
Ben Nachname

Fakultät für Informatik,
Technische Universität München
`{beller,bennachname}@in.tum.de`

Zusammenfassung Diese Arbeit behandelt ein interessantes Thema.

1 Einleitung

2 Definitions

A computer able of executing remotely-triggered commands is called a *bot* or *zombie.* A *botnet* is a group of bots forming a common network structure.[SK07] In most recent papers on the subject ([WWAZ09], [ARZMT06]), the term botnet is defined as purely negative, i.e. a network performing destructive aims such as DDoS attacks, sending spam or hosting a phishing website[SI07]. A common aim is to provide the aggregated CPU resources of the botnet, or stealing user's credentials. [Bor] We'd like to propose a bias-free definition of botnet as per our understanding technology is generally ethics-free. Additionally, there are many examples where botnets are used in a non-destructive way (e.g. [oC11]), or even to destroy existing "evil-minded" botnets.

A *botmaster* is referred to as the controller of the botnet. This doesn't necessarily have to be the founder of the botnet (cf. 4.1).

The expression *bot candidates* specifies the set of computers which are target to becoming a bot themselves.

Peer-to-Peer, being a technology buzz word of the internet in the late 1990s with file sharing services like Napster[Inc11], has attracted less attention in recent years. *P2P* defines an unstructured information network amongst equals — so-called peers. Two or more peers can spontaneously exchange information without a central instance. According to [SFS05] "P2P networks promise improved scalability, lower cost of ownership, self-organized and decentralized coordination of previously underused or limited resources, greater fault toler- ance, and better support for building ad hoc networks." These properties coupled with the fact that files circumfloating in P2P networks are prone to malware, trojans and viruses make P2P networks a most-attractive base for building botnets. Well-known P2P networks include the Napster[Inc11], Gnutella, Overnet and Torrent network.

The so-called *C&C*, command and controll structure, specifies the way and protocols in which the botmaster and the bots communicate with each other. It is the central property of any botnet. Common protocols for C&C include IRC, HTTP, FTP and P2P.[Bor]

IRC — internet relay chat — is a "teleconferencing system"[irc], typically used for text chatting in channels joined by a large number of participants. While its protocol is relatively easy to implement, it provides a lot of features. It has thus become the de-facto standard for C&C in conventional botnets.

The process of *bootstrapping* generally describes starting a more complex system ontop of a simple system. In regard to botnets, the term usually means loading of the bot code (often injected into the original filesharing program) and establishing a connection to other bots.[WWAZ09]

3 A brief history of botnets

It is not surprising that the first bot — Eggdrop — was a non-malicious IRC bot. Its origins go back to the year 1993. However, in April 1998 a deriviant called GT-Bot formed the first malicious botnet, using IRC's C&C structures. Four years later, in 2002, Slapper was the first worm to make use of P2P for C&C.[LJZ]

4 The genesis of a P2P botnet

4.1 Classification P2P networks

There are three types of P2P networks: "parasite", "leeching" and "bot-only".[WWAZ09]

Parasite and leeching bots infiltrate existing P2P networks, while "bot-only" networks are designed as new networks.

Parasite botnets recruit new bots only from the set of existing P2P participants; they try to infect system inside the P2P network and make them become bots. Due to the often illegal content distributed in file sharing networks, they are a perfect culture medium of viruses, malware and worms. It is thus convenient for an attacker to spread a highly-demanded file (e.g. porn) containing the injection code sequences of his bot. This code is then injected into the file sharing client. Vulnerable hosts in the network are infected this way. On the downside, this means that the spread of the bot is limited to the size of the P2P network.

In contrast, leeching bots not only try to infiltrate systems which are already part of the P2P network, but also systems outside of the P2P network. Natuarally, they are bigger in size as they have to deliver the P2P client, too. This might be more difficult to achieve as it means that systems must unwillingly take part in the network. Often, firewalls and port-forwarding are not properly configured on these systems, reducing the performance of the botnet. Leeching bots can spread through any possible measure: File sharing, downloads on websites, email attachments and instant messanging.

There are good reasons for either strategy: Using an existing P2P network as a base like parasite and leeching bots do unburdens the botmaster from setting up and building a botnet infrastructure. It profits from the established P2P network, making use of filtering, error-correction and encryption as far as the chosen network has support for it. On the other hand, features are limited to the existing P2P protocol. A specifically-built P2P bot-only network is natuarally more tailored towards its purpose. Due to the bot-exclusive memberships, it might be easier to shutdown as all participants can be considered bots and there is no risk of accidentally shutting down an innocent member.

4.2 Lifetime of P2P botnets

Wang et. all[WWAZ09] differentiate three stages of P2P botnets:

- recruiting bot members
- forming the botnet
- standing by for instruction This is the actual "operational" phase of the botnet. Bots are awaiting instructions from their master. Instructions can either be actual commands or performing updates. In this phase, the chosen C&C structure is essential.

It should be noted that these phases are not strictly exclusive, e.g. during the third phase building of the botnet may well continue. In fact, this is a typical property of any P2P network. It is only until a critical mass of bots has proceeded past phase one and two, that the botnet can be called operational.

5 C&C in P2P botnets

Central server, hybrid, completely decentralized

6 Comparison: Conventional bots vs. P2P bots

7 Counter measure against evil P2P botnets

Literatur

ARZMT06. M. Abu Rajab, J. Zarfoss, F. Monrose, and A. Terzis. A multifaceted approach to understanding the botnet phenomenon. In *Proceedings of the 6th ACM SIGCOMM conference on Internet measurement*, pages 41–52. ACM, 2006.

Bor. R. Borgaonkar. An analysis of the asprox botnet. In *Emerging Security Information Systems and Technologies (SECURWARE), 2010 Fourth International Conference on*, pages 148–153. IEEE.

Inc11. Napster Inc. Napster. http://www.napster.com, June 2011.

irc. Irc - protocol defintion. http://tools.ietf.org/html/rfc1459section-1.

LJZ. C. Li, W. Jiang, and X. Zou. Botnet: Survey and case study. In *Innovative Computing, Information and Control (ICICIC), 2009 Fourth International Conference on*, pages 1184–1187. IEEE.

oC11. University of California. Seti@home. http://setiathome.berkeley.edu/, June 2011.

SFS05. D. Schoder, K. Fischbach, and C. Schmitt. Core concepts in peer-to-peer. *Peer-to-peer computing: the evolution of a disruptive technology*, page 1, 2005.

SI07. M. Steggink and I. Idziejczak. Detection of peer-to-peer botnets. *University of Amsterdam, Netherlands*, 2007.

SK07. R. Schoof and R. Koning. Detecting peer-to-peer botnets. *University of Amsterdam*, 2007.

WWAZ09. P. Wang, L. Wu, B. Aslam, and C.C. Zou. A systematic study on peer-to-peer botnets. In *Computer Communications and Networks, 2009. ICCCN 2009. Proceedings of 18th Internatonal Conference on*, pages 1–8. IEEE, 2009.