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]. 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.

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 to each other. It is the central property of any botnet.

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 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]

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.

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

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

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.