

Bot armies: an introduction

Sheila Banks and Martin Stytz

Remotely controlled malicious software concealed in large numbers of computers offers unprecedented potential for damage to the Internet.

Botnets or 'bot armies' are large groups of malicious software, remotely controlled and operated, that can launch multiple penetration attacks and lead to massive denial of service (DOS) or similar network activity on a grand scale. Infested computers can be used to spread spam, conduct fraudulent activities, and interfere with authorized network traffic. Bot armies pose one of the most serious security threats to all networks.¹ They are controlled and operated by botmasters (also called bot-herders). While their activity has so far been limited to extralegal and criminal activity, their potential for causing large-scale damage to the entire Internet is incalculable.

Bot armies first arose with the development of Internet chat and their capabilities have grown ever since (see Figure 1).²⁻⁵ They are effective both because they can execute multiple overt actions against targets and, alternatively, they can provide multiple coordinated and covert listening points within targeted networks and computer systems.

Botnet creation requires a few basic steps. Software must be created and propagated to infest targets. A command and control system must be set up, together with a system enabling check-in for further instructions. To facilitate contact after infestation, the bot author typically encodes an initial contact domain name into the bot software. To prepare for contact from bots as they become active, a computer, or suite of computers, is set up to run an Internet relay chat (IRC) to provide command and control.

Bot software exhibits the triple characteristics of a virus, a worm, and a Trojan. From the point of view of a botmaster, virus technology is just a means for infecting a computer. Similarly, worm technology only enables bot software to move through the Internet. A bot employs Trojan technology to disguise itself by behaving like a program purporting to carry on some innocent behavior while in fact engaging in nefarious activities.

Once infestation is established, the bot checks in to receive instructions: these generally direct it to seek out and infest additional hosts, to locate and exfiltrate information of interest to the botmaster, or to participate in coordinated attacks on other

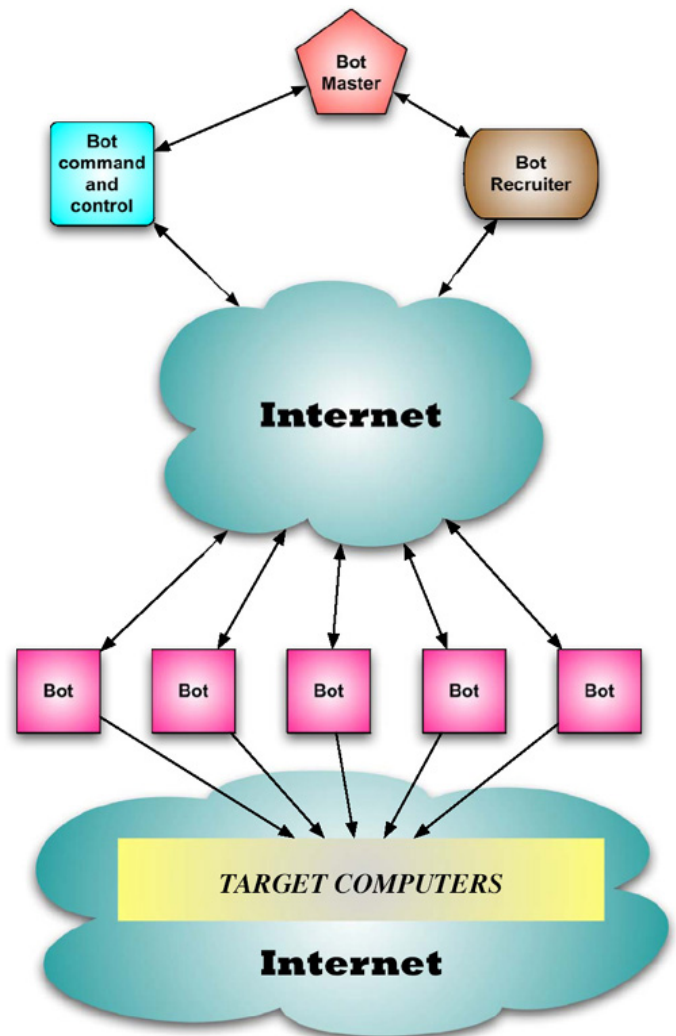


Figure 1. Notional Bot Army

targets. The botmaster has two main jobs: assigning tasks to the army and developing new software for it, to be distributed to the bots via the command and control nodes.

Currently, the key to botnet defense lies in detecting command and control activity and the subtle indicators of infestation. Because capturing a lone bot is difficult, scrutiny of command and

Continued on next page

control is the usual route for hunting bot armies. Avoiding discovery is a challenge for botherders, who avoid capture by directing bots to connect to specific machines. This approach is easy to implement but also simple to defeat. Botherders continually explore new ways to improve command and control of their bots.

Bot armies pose a threat to the Internet, with worse perhaps yet to come. Penetration of systems is not difficult and most bots go undetected unless the botmaster makes a mistake. At present we lack wide-ranging, capable defensive technologies. As botmasters continue to improve their capabilities, a philosophy of vigilance will be requisite in developing bot defenses.

Author Information

Sheila Banks

Calculated Insight
Orlando, FL

Sheila B. Banks, president of Calculated Insight, received her MS degree in electrical and computer engineering from North Carolina State University, Raleigh, NC, and her doctorate in computer engineering (artificial intelligence) from Clemson University, Clemson, SC. Her research interests include artificial intelligence, human behavior and cognitive modeling, and cyberwarfare modeling.

Martin Stytz

Institute for Defense Analyses
Washington, DC

Martin R. Stytz works for the Institute for Defense Analysis. A retired Air Force officer, he earned a BS degree from the U.S. Air Force Academy in 1975, two masters degrees and, in 1989, a PhD in computer science and engineering from the University of Michigan.

References

1. **Attack of the Zombie Computers is a Growing Threat**, New York Times, 7 January 2007.
2. E. Cooke and F. Jahanian, **The zombie roundup: understanding, detecting, and disrupting botnets, Steps to Reducing Unwanted Traffic on the Internet Workshop (SRUTI '05)**, Cambridge, MA., 2005.
3. Curve, *Just What is a Botnet?*, **Dalnetizen**, January 2003. <http://zine.dal.net/previousissues/issue22/botnet.php>.
4. R. Naraine, *Blue Pill' Prototype Creates 100% Undetectable Malware*, 2006. eWeek.com <http://www.eweek.com/article2/0,1895,1983037,00.asp>
5. A. Ramachandran, N. Feamster, and D. Dagon, **Revealing Botnet Membership Using DNSBL Counter-Intelligence, Usenix: Steps to Reducing Unwanted Traffic on the Internet (SRUTI) '06**, San Jose, CA, 2006. http://www.usenix.org/events/sruti06/tech/full_papers/ramachandran/ramachandran.html/