Understanding Botnets

by Blackwell N. Shelley Jr.

Recent news stories have reported that hacker groups, such as Anonymous and LulzSec, have threatened or carried out distributed denial of service (DDoS) attacks on websites in response to, for example, the arrests of Julian Assange and Kim Dotcom, and the threatened passage of the Stop Online Piracy Act (SOPA). The basic idea of a DDoS attack is simple: all websites are based on computer servers that can accept a finite number of simultaneous connections. To effectively shut down a website, hit it with more simultaneous connections than it can handle. Orchestrating the simultaneous attack requires a botnet.

A *botnet* is a network of computers that have been compromised by a malicious computer program (a "*bot*") and surreptitiously programmed to follow instructions issued by a different computer.[1] The compromised computers in a botnet, sometimes called *nodes* or *zombies*, are typically home or office desktop computers. The hacker who issues the command and control instructions to the botnet is called a *bot herder* or *bot master*.

The user of a zombie computer is rarely aware that the machine has been compromised because the process usually starts quietly, either by exploiting vulnerability in the computer's software or security system, or by tricking the user into installing the malicious code. Examples of this are varied, but include old school hacking ("password1" is not a strong password), or through bogus software (that animated screensaver that you downloaded for free, for example), or through deceptive email ("RE: Why did you put this photo online?"). The hacker, the bogus software, and the link sent through deceptive email all have the purpose of installing unwanted and malicious code — the bot — on the user's computer.

Technically sophisticated bot herders might choose to write the malicious code themselves, but as with so much on the Internet, bot creation has been simplified by the use of malware kits. These kits are collections of software tools that enable aspiring bot herders to assemble their own bots by creating and spreading customized malware variants. Some malware kits have been published as free open source code, and offer discussion forums for users to suggest new features and modules for the malware, report bugs and other errors, or enter into discussion with their fellow developers.[2] Other kits are developed by individuals or groups and sold like legitimate commercial software products.[3] For bot herders with money and little time, independent contractors will make bespoke code according to the bot herders' needs.[4]

By keeping a low profile, bots are sometimes able to remain active and operational for the life of the computer. Most office and residential Internet services are now high-speed, always-on connections that provide the bot-herder with a large contingent of accessible zombies. Botnets are attractive to criminals because investigators typically cannot follow the trail past the innocent owner of a zombie computer.

After the bot has infected the user's computer, it attempts to contact a centralized command and control server in order to get its instructions from the bot herder. A bot herder has several choices when setting up this command and control server. If the bot herder has already gained access to a compromised computer, he or she may install the server software on it. Other choices include establishing secret channels on public Internet Relay Chat[5] (IRC) servers, setting up servers on the bot herder's own computer, or signing on with a provider that resists or ignores efforts to disconnect lawbreakers.[6]

Once the botnet is up and running, it can be used to carry out a variety of criminal activities. Apart from the Denial-of-Service attacks, described above, a botnet may be used to steal the confidential information stored on each infected computer, as a spam generator, or for click fraud, depending on how the bot herder chooses to configure the individual nodes. A botnet can also be self-propagating, as a means of distributing more of the malicious code. With time and patience, a bot herder can use this latter technique to build networks of thousands of infected computers.

Once the botnet is up and running, it can be used to carry out a variety of criminal activities.

Notwithstanding the publicized attacks and threats of "hacktivist" groups like Anonymous and LulzSec, bot herding is almost entirely a for-profit endeavor. In May, 2012, an Armenian court sentenced 27-year-old Georgy Avanesov to four years in prison following his con-

viction on charges of computer sabotage. Avanesov, prosecutors said, was part of a group of bot herders making about $125,000 a month by renting out a botnet comprised of some 30 million zombie computers worldwide and 143 command and control servers in France and the Netherlands.[7] In an April, 2012, post on Reddit,[8] an admitted bot herder, who used the handle Throwaway236236, offered this prediction:

> The whole fraud system will soon escalate and only then people will start worrying about the fundamental flaws in the system. Antiviri don't work, firewalls never helped, fraud detection systems are blind when abusing the victim computer as a proxy. The only cure is strong cryptography and simple yet unbreakable solutions, even if it's unconvinient. Some European countries for example already use private/public key authentification for banking and only allow credit cards with chips. Magnetic stripes are the most hilarious thing ever, but still work almost everywhere on the globe. Today Cybercrime is already more profitable than drug dealing and it will grow even further.

When asked by other users how to stay secure on line, Throwaway236236 offered the following suggestions:[9]

- If the attachment is ending in .exe and pretending to be something else, it's malware for sure. …
- Facebook friends don't share funny cat pictures on randomly generated domain names.
- If your AV says it's clean … it can still be malware, been there, seen that. Srsly, don't trust your AV.
- Windows updates, yes, do them. If you have a pirated copy, just buy that s**t or use linux.
- Scan your [network] traffic while your PC is idle and see if you find something suspicious …
- Read a blog from [antivirus] vendors … That stuff is interesting and you are always informed what most common threats are.
- Most important: Try to step out of your consumer role, think about how malware works. The core functions of malware all work the same and are very fragile.

Endnotes:

1 *See FTC v. Pricewert LLC*, 2009 U.S. Dist. LEXIS 54043 (N.D. Cal. June 15, 2009).

2 *The Register*, "*Malware devs embrace open source*", February 10, 2012, *available at* http://www.theregister.co.uk/2012/02/10/open_source_malware/ (last visited June 10, 2012).

3 *See, e.g.,* Dell SecureWorks, *ZeuS Banking Trojan Report*, March 11, 2010, *available at* http://www.secureworks.com/research/threats/zeus/ (last visited June 10, 2012). ZeuS is a well-known banking malware program that steals data from infected computers via web browsers and protected storage. Once infected, the computer sends the stolen data to a bot command and control server, where the data is stored. As of March, 2010, prices for the Zeus kit started at $3,000 with additional modules available on an a la carte basis. In late 2010, the creator of ZeuS sold the source code to rival SpyEye, which continues to sell Trojan malware kits. Krebs on Security, *SpyEye v. ZeuS Rivalry Ends in Quiet Merger*, October 24, 2010, *available at* http://krebsonsecurity.com/2010/10/spyeye-v-zeus-rivalry-ends-in-quiet-merger/ (last visited June 10, 2012).

4 *See, e.g, The Bot Net*, "How to make a bot request", *available at* http://thebotnet.com/bot-requests/60829-how-to-make-a-bot-request/ (last visited June 10, 2012).

5 IRC is a real-time Internet chat protocol, designed for group text-based conferencing. An IRC "channel" is a named chat group which will all receive messages addressed to that channel. The Internet Engineering Task Force (IETF), "Internet Relay Chat Protocol, Section 1.3 Channels", *available at* https://tools.ietf.org/html/rfc1459 (last visited June 10, 2012).

6 Recently, botnets that use peer-to-peer (P2P) networks for remote control of the compromised machines have appeared in the wild. A P2P botnet does not use a central command point; instead, each zombie computer passes on instructions to each other zombie in the botnet. The lack of a centralized command and control server makes P2P botnets more difficult to shut down and the command source more difficult to track. *See The Hacker News,* "Thor, another P2P botnet in development," *available at* http://thehackernews.com/2012/03/thor-another-p2p-botnet-in-development.html (last visited June 10, 2012).

7 Wired.com, "Bredolab Bot Herder Gets 4 Years for 30 Million Infections," May 23, 2012, *available at* http://www.wired.com/threatlevel/2012/05/bredolab-botmaster-sentenced/ (last visited June 11, 2012).

8 Throwaway 236236, "IAmA malware coder and botnet operator", *AMA* (submitted April 24, 2012), *available at* http://www.reddit.com/r/IAmA/comments/sq7cy/iama_a_malware_coder_and_botnet_operator_ama/ (last visited June 11, 2012).

9 *Id.*

Blackwell N. Shelley Jr. is an attorney at Shelley & Schulte PC, in Richmond, Va. He is the former chair of the Virginia State Bar Special Committee on Technology and the Practice of Law.