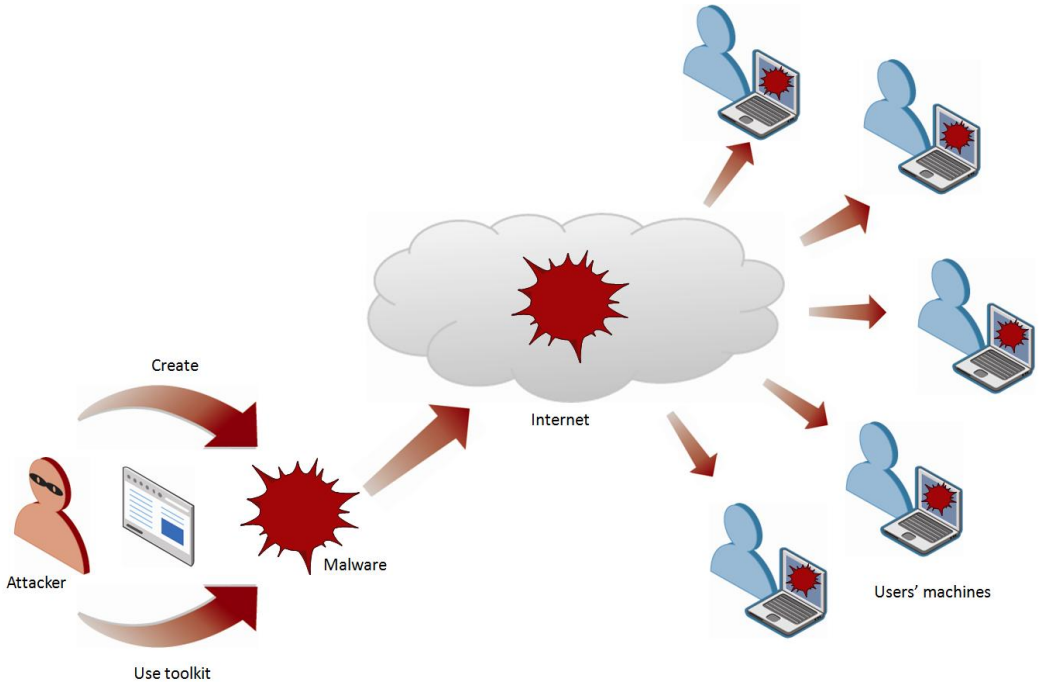
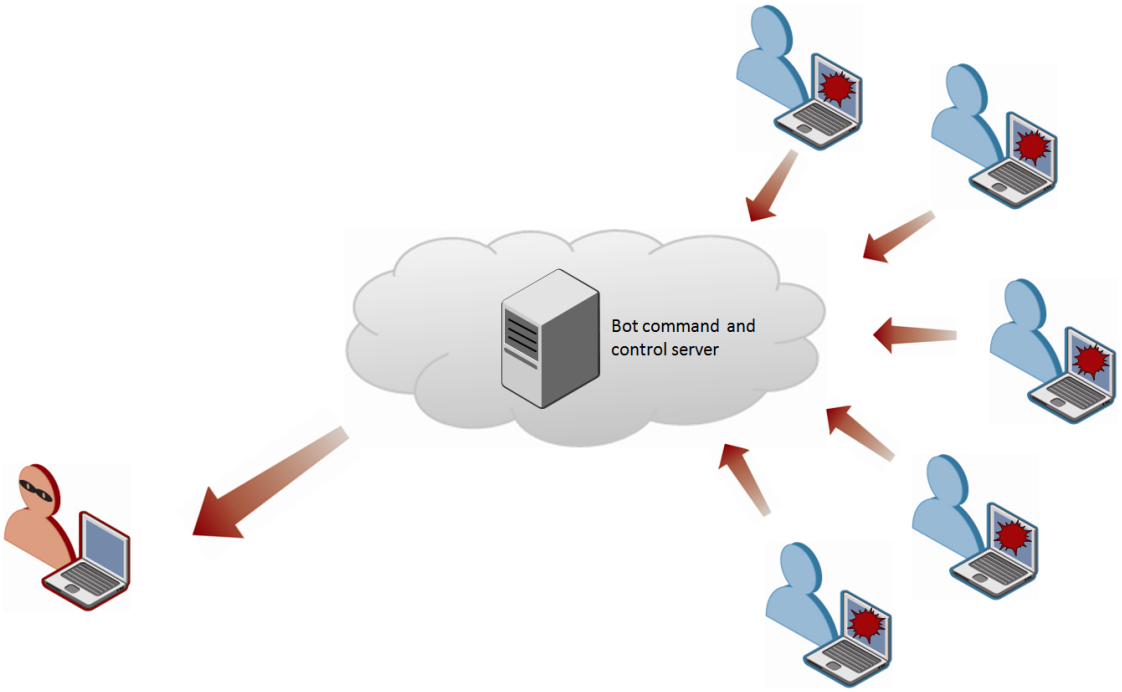
Botnets: The Virtual Armies Driving Modern-Day Cybercrime

A bot network, more commonly known as a botnet, is a collection of malware-infected computers, called bots or zombies, distributed wide and far across the Internet and under the control of an attacker called a botmaster. Usually, botnets consist of thousands of individual bots, giving botmasters virtual armies of zombie computers ready to carry out whatever nefarious deeds they command.

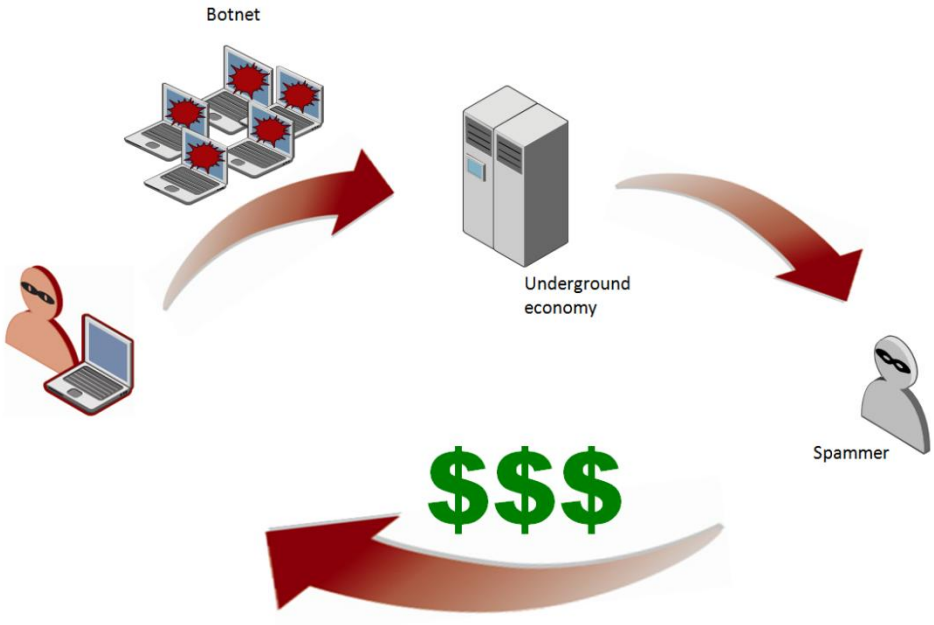
Because botnets are so versatile—able to perform denial-of-service attacks; distribute spam and phishing attacks; spread spyware, adware and rogue antivirus scams; propagate malicious code; and harvest personal and confidential information on compromised computers—they have developed into the engine driving much of today's malicious online activity. In fact, according to Symantec's Internet Security Threat Report (ISTR) XV, released April 20, 2010, botnets alone were responsible for the distribution of approximately 85 percent of all spam e-mail in 2009. Symantec also witnessed an average of 46,541 active bot-infected computers per day in 2009. With botnets such a big part of today's threat landscape, it's wise to understand how they work, and how to keep your computer from becoming part of one!



The birth of a botnet begins when an attacker creates malware specifically designed to infect the computers that will become part of his zombie army. This first step used to be a significant barrier to entry into the bot business for many would-be cybercriminals, but now, with the increasing popularity and availability of malicious toolkits, such as the Zeus toolkit, the creation and use of such malware is almost easy enough that mere novice Internet miscreants can do it. Indeed the Zeus toolkit was so popular in 2009 that Symantec observed close to 90,000 unique Zeus binaries. However the necessary malware is obtained, once an attacker has gotten hold of it, his next move is to release the virus, worm or Trojan into the wilds of the Internet, where it seeks out and infects unprotected and poorly updated computers ripe for the plucking.

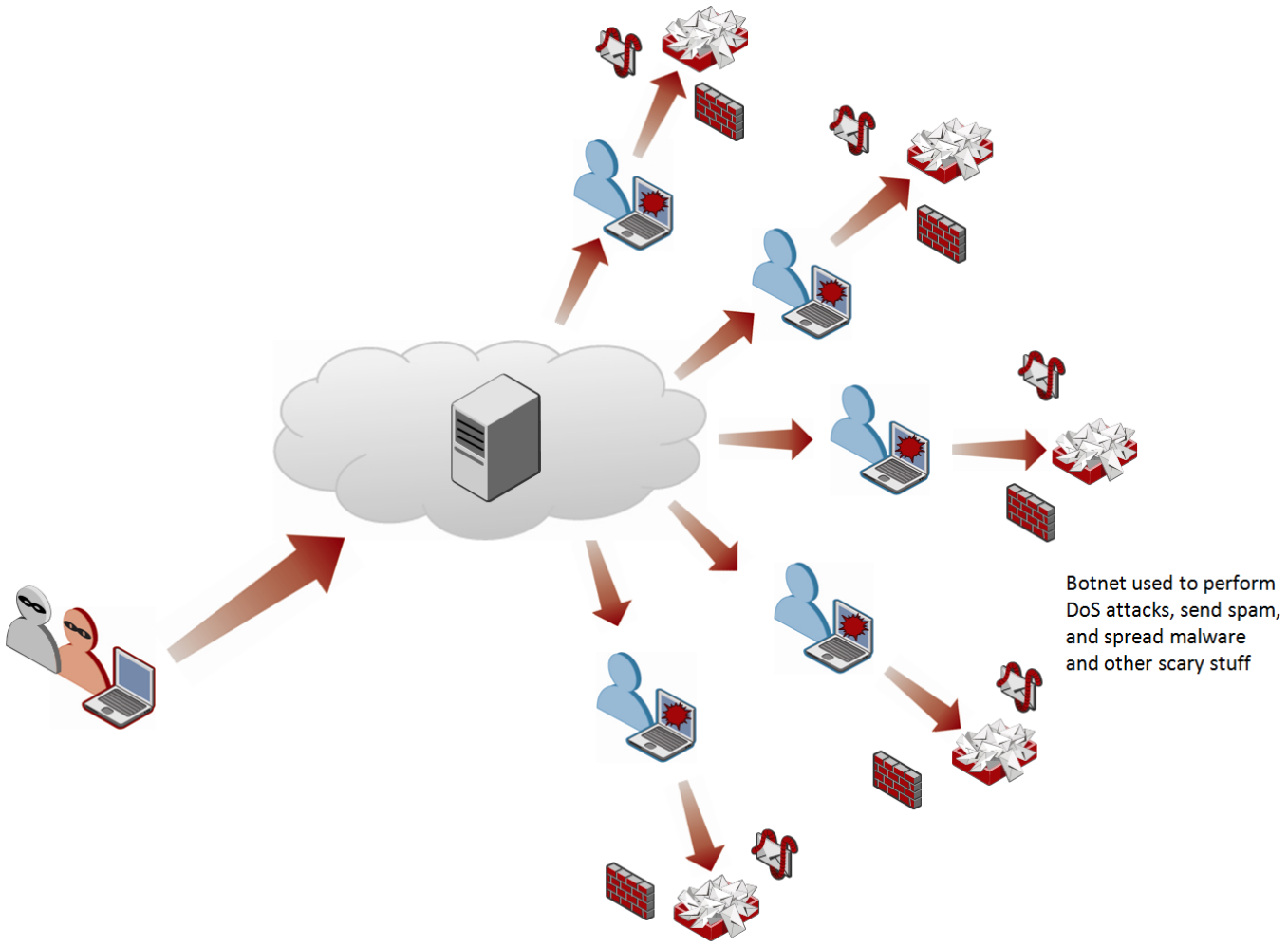


Once the malware finds its way onto an unsuspecting computer user's machine, that computer has effectively become a part of the botnet. The newly created zombie computer, which typically appears to be working just fine to the actual owner, reports back to the botmaster that it's ready for orders by silently logging onto a command and control server. This command and control server is the conduit through which the botmaster communicates with the botnet and sends orders to carry out malicous activities. To demonstrate the growing botnet problem, in 2009 Symantec identified 17,432 distinct new botnet command-and-control servers, an increase from 15,197 in 2008. Of note, the United States was home to the most bot command and control servers in 2009, accounting for 34 percent of the global total.



After a botmaster has collected enough zombie machines, it's time for them to go to work. Botmasters have a couple of options for how to get the biggest bang for the buck out of their creations. First they can use their botnets for their own dingy deeds, or they can sell or rent their botnets out to other cybercriminals by advertising them on the underground economy. The inexpensive nature of botnets advertised on the underground economy is another reason for their

popularity with cybercriminals. Symantec observed individual bots for sale for as little as $0.03 a piece. However, not much can be done with an individual bot from a cybercrime perspective, so most bots are actually sold in bulk as an entire botnet.



Whether a botmaster uses the botnet himself or rents it out to someone else, the next step is to send orders to the bots via the command and control server. As mentioned, these orders can be to carry out any number of malicious activities, including performing denial-of-service (DoS) attacks, which involve each zombie computer simultaneously flooding some Internet resource with requests, all in an attempt to block normal access to it; sending spam messages, some of which could be phishing attacks; spreading malware; and even stealing personal or confidential information, such as credit card information and banking account credentials, from the owners of the infected computers.

You can protect your computer from being recruited into a botnet army by following a few simple steps. First, keep your entire computer system up-to-date with the latest security patches—this means not only the operating system, but all

applications and plug-ins, too. Second, use security software from a well-known vendor. Finally, keep that security software running at all times and up-to-date. Doing all this will go a long way in ensuring that you and your computer are safe, secure and happy.