

# Orchestrating A DDoS Attack

HACKERS HAVE BEEN GIVING WEB SITE OWNERS and administrators headaches for years now with several varieties of electronic chicanery falling under the heading of DoS (Denial of Service) attacks. DoS attacks such as Ping of Death, Teardrop, SYN Attack, Smurf Attack, and UDP Flood originate from a single computer and use sophisticated software and techniques to cripple sites on the Internet.

Eventually, however, Web site administrators and their computer gurus developed effective countermeasures for each of them, so in 2000 hackers began orchestrating new and more powerful attacks called DDoS (Distributed Denial of Service) attacks.

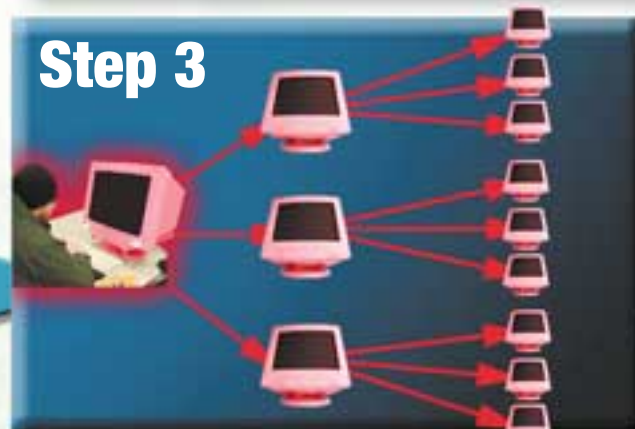
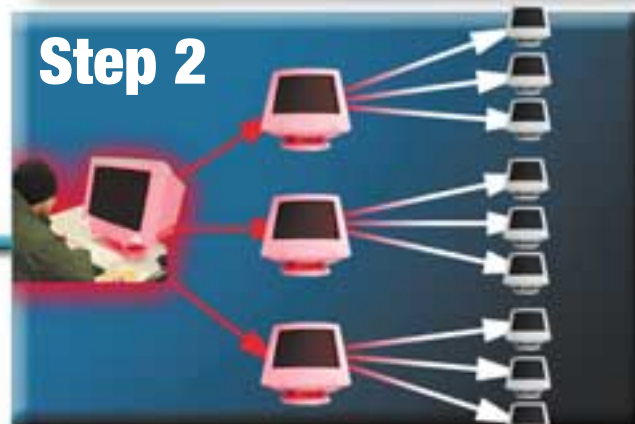
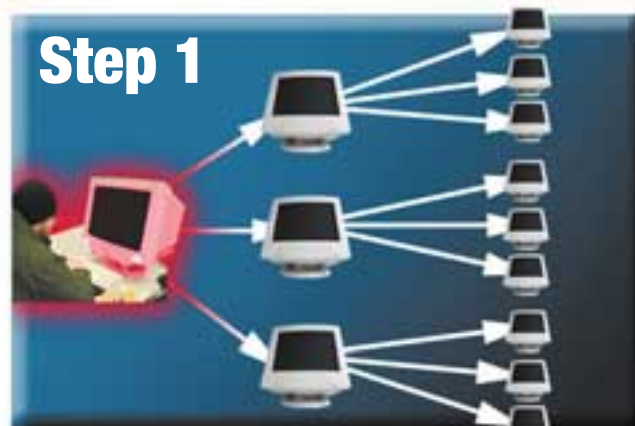
DDoS attacks involve the use of numerous anonymous and coordinated computers attacking Web site

servers en masse, and hackers have used them to shut down high-profile sites such as Yahoo!, Amazon.com, Buy.com, eBay, CNN, and others. To make matters worse, it is almost impossible to track down the people responsible, and there is currently no way to prevent these attacks. Here's how they work, broken into seven basic steps:

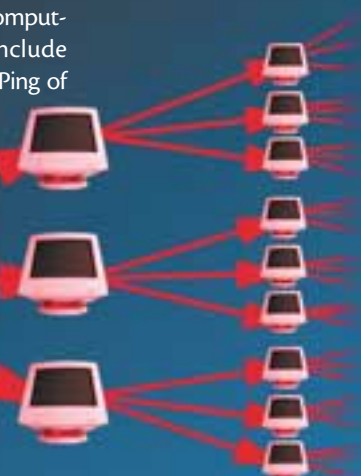
**1** The perpetrator uses specialized port scanning software to find several poorly secured computers across the Internet. Once he has access, he takes several steps. First, he installs software that conceals his break-in (and will conceal his future activities). Second, he installs remote-control software that lets him issue commands to the infiltrated computers over the Internet. He configures the software to launch automatically when each computer boots, thus concealing its presence from the computers' owners. Finally, he records the Internet address of these computers for future use. Hacker software is available to automate most of this process.

**2** The hacker uses these computers to gain control of even more computers by using the same approach (searching for vulnerable computers and then installing remote control software) as he used in Step 1. The perpetrator is only vulnerable during Step 1 where he is directly accessing computers to break into, so he will want to quickly switch to having his first victims' computers perform additional break-ins.

**3** The perpetrator assembles all of the computers he has infiltrated into a DDoS network. By now, there can be thousands of compromised computers, but thanks to the Internet the perpetrator doesn't have to physically connect them to create his network. All he has to do is store all of their addresses in a control file so he can easily send the attack command to all of them at once.



**4** The perpetrator uses the control file to send out the attack command to all of the computers at once. The attack command will include instructions on which type of DoS attack (Ping of Death, UDP Flood, etc.) to use.



**5** All of the computers in the DDoS network begin to flood the target with commands. According to the SANS (System Administration, Networking, and Security) Institute (<http://www.sans.org>) an attack on Yahoo! in February 2000 involved gigabytes per second of traffic.

**6** The Web site under attack is often unable to stave off the flood of intrusive transmissions and suffers as a result. Yahoo!, for example, was crippled for three hours by a DDoS attack that involved 3,500 computers, according to Yahoo! executive Jeff Mallett.

address 1  
address 2  
address 3  
address 4  
address 5

## Control File

**7** When (and if) the perpetrator decides to halt the attack, he sends a stop command to the DDoS network.

Since the perpetrator never communicates directly with the target, tracking him down can be very difficult, made even more so because the attacks generally use forged addresses. It is difficult for anyone other than the perpetrator to stop the attacks, since they come not from one central source but rather from hundreds or even thousands of computers.

