
Steve Gibson (<http://www.grc.com>) has published a long and detailed report on the DDoS attack his site suffered in May 2001 (<http://grc.com/dos/grcdos.htm>). In a nutshell, starting at 20:00 on 2001-05-04, Gibson's site was flooded with bogus UDP and ICMP packets, completely flooding his T1 lines and preventing legitimate access to his Web pages. Working with his ISP, Gibson was able to arrange to discard the spurious traffic before it hit his own firewall. Analysis showed that the attacks were coming from 474 compromised computers running Windows operating systems. Luckily, most of the compromised machines were running Windows 9x and Windows NT systems that were unable to forge packet headers, so it was possible to identify the source IP addresses and institute firewall policies to block traffic from those sources.

Over the next two weeks, the attackers changed their tactics several times to break through the firewall rules in place, putting Gibson's site down for many hours at a time. Over the course of the attacks, Gibson and his ISP logged about 2.4 billion bogus requests directed to various ports on his systems.

The originator of the attacks, apparently a 13 year old child in Kenosha, WI, communicated with Gibson and explained that he had heard rumors that Gibson had been disrespectful towards "script kiddies." Based on this hearsay, the child and his friends had put a Web site into limbo for several days. The transcripts of some of Gibson's conversation with the perpetrator of the DDoS attack are highly revealing and well worth reading.

Eventually, someone sent Gibson a copy of the zombie program they found on an infected PC, and Gibson was able to locate the IRC channel where the zombies were communicating with the 13-year-old's master program. He also documented the infection of home PCs by the Sub7Server Trojan, which automatically reports on compromised machines. After discussing his problems with a leader in the criminal hacker underground, Gibson was able to convince the child to stop harassing him.

The experience convinced Gibson that we are heading for serious difficulties on the Internet if a little kid can exert that much power over the adult world.

[other comments on importance of DDoS]
In the next article in this series, I will review some of the more important techniques of simple (not distributed) denial-of-service attacks as a foundation for understanding and fighting DDoS attacks.

* * *

Mich Kabay can be reached by e-mail at <mkabay@atomictangerine.com>. He invites inquiries about a wide range of information security courses and INFOSEC consulting services that he and his colleagues at AtomicTangerine would be delighted to deliver to your employees at your site and at your convenience. For Web-based or CD-ROM online training in security from our Information Security University project, see <http://infosecu.com>.

For information about AtomicTangerine, visit <http://www.atomictangerine.com>.

Copyright © 2001 M. E. Kabay. All rights reserved.

Permission is hereby granted to Network World to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.