## Denial of Service

On the evening of May 4th, 2001, the website GRC.COM got attacked by a series of malicious packets over flooding its bandwidth and therefore dropping off the website, after capturing real time traffic and analyzing it, Steve Gibson (the website owner) noticed huge UDP packets aimed at the bogus port “666” of grc.com. As a temporary solution he contacted Verio (his ISP) and applied “brute force” filters to the Verio router, shutting down all UDP and ICMP traffic, resulting in the website getting back online.

The website was attacked by 474 windows pc, but the question was who where does PCs and where did the PCs reside? Later he found out that the attacker was using “cable bots , a zombie program installed on a windows machine allowing the user to control the infected computer.

The attack was carried by a 13 year old that was angry at GRC.com because he felt offended by comments made on the forum. After inspecting the bots and sacrificing a laptop using it as guinea pig he discovered how the zombie works: The zombie program had especial names to help it hide itself in the registry files, and when I got into a PC it immediately connected with a remote, pre-programmed IRC chat server, then it joined a secret and password key-protected channel on that server and waited for instructions. Also the hackers used a Sub7Server Trojan that was designed to give its master virtually complete control over the compromised PC (complete file system inventorying, file access and real-time keyboard logging). And when the attacker was finally ready to attack, he would login to the IRC server and join into the Bots channel and type the following commands: “!p4 207.71.92.193” and “!udp 207.71.92.193 9999999 0” being 207.71.92.193 the IP address of the victim; the first command makes the host pc execute the command “ping.exe 207.71.92.193 –l 65500 –n 10000” making the pc send 10000 64kbyte ping packets to the victim pc, while the second command (which is the worst) makes the host pc send the number specified (9999999) maximum size UPD packets as fast as the machine would allowed (0 inter-packet delay).

Thanks to all his investigation, he discovered how it worked and after infiltrating to one IRC chat room and talking to one of the main hackers, he was able to make the 13 year old kid stop. As far as how you could have prevented the attack, the best way is the one mention in the article, using a personal firewall like “ZoneAlarm”.