Title:
Zombie Computers Roam The Internet

Word Count:
456

Summary:
Spyware and viruses are so common that you would be hard pressed to find anyone that isn't aware of them. Under the umbrella term Malware, these little programs have been causing trouble for computer users for many years, and they seem to get more powerful everyday. A new incarnation of malware is becoming very common as of late, and it involves using a virus or trojan horse to place a computer under the remote control of a hacker. The controlled computer is referred to as a ...

Keywords:
Computers, Internet, Refurbished Laptops, Satellite Internet, Virus, Malware, Trojan

Article Body:
Spyware and viruses are so common that you would be hard pressed to find anyone that isn't aware of them. Under the umbrella term Malware, these little programs have been causing trouble for computer users for many years, and they seem to get more powerful everyday. A new incarnation of malware is becoming very common as of late, and it involves using a virus or trojan horse to place a computer under the remote control of a hacker. The controlled computer is referred to as a zombie and it is used to commit various dastardly deeds without the knowledge of the computer owner.

Zombie computers are almost always attached to the Internet via a broadband connection such as DSL or Satellite Internet. This is important as spammers have found that by using zombie computers to send out their junk mail they can easily avoid detection. As of 2005 it was estimated that up to 80% of all spam was sent via zombie computers, and that number is on the rise.

The increase can be attributed to smarter hackers and better technology, but the real driving causes behind the increased zombie trend are better spam filters and anti-spam laws. According to Tom Spring at PC World Magazine, "spammers are hiring virus writers and hackers to help them create armies of zombie PCs to send spam." This union of hackers and spammers has been beneficial to both parties in opening new revenue steams that are extremely difficult to shut down.

Gregg Mastoras, a senior security analyst at the security firm Sophos says, “A new underground economy is evolving." This new economy is for the most part illegal and to date impossible to stop completely.

As of late the Chinese hackers have thrown their hat into the game and have taken the zombie computer business to the next level. Senior Pentagon Advisor Paul Strassmann recently said, “As of September 14th 2007 there were exactly 735,598 computers in the United States infested with Chinese zombies”.

Large groups of zombie computers can be used to form a “botnet” or network of slave computers. This network can be used to send out millions of spam mails in a short period of time. Slave networks are also used to commit a DoS attack. DoS attacks, or Denial of Service, target a particular website and overwhelm the server with information requests until the server can no longer handle the load. These attacks or in no way secretive, and once discovered are easily shut down. There will be a period of time however when site traffic will be disrupted by the DoS attack. Larger more sophisticated networks such as those used by governments or large firms have defensive measures in place to prevent damage from a DoS attack.