An Army of Soulless 1's and 0's

By *srlinuxx*
Created *25/06/2005 - 2:46pm*
Submitted by srlinuxx on Saturday 25th of June 2005 02:46:43 PM Filed under Security [1]

For thousands of Internet users, the offer seemed all too alluring: revealing pictures of Jennifer Lopez, available at a mere click of the mouse. But the pictures never appeared. The offer was a ruse, and the click downloaded software code that turned the user's computer into a launching pad for Internet warfare.

On the instructions of a remote master, the software could deploy an army of commandeered computers - known as zombies - that simultaneously bombarded a target Web site with so many requests for pages that it would be impossible for others to gain access to the site.

And all for the sake of selling a few more sports jerseys.

The facts of the case, as given by law enforcement officials, may seem trivial: a small-time Internet merchant enlisting a fellow teenager, in exchange for some sneakers and a watch, to disable the sites of two rivals in the athletic jersey trade. But the method was far from rare.

Experts say hundreds of thousands of computers each week are being added to the ranks of zombies, infected with software that makes them susceptible to remote deployment for a variety of illicit purposes, from overwhelming a Web site with traffic - a so-called denial-of-service attack - to cracking complicated security codes. In most instances, the user of a zombie computer is never aware that it has been commandeered.

The networks of zombie computers are used for a variety of purposes, from attacking Web sites of companies and government agencies to generating huge batches of spam e-mail. In some cases, experts say, the spam messages are used by fraud artists, known as phishers, to try to trick computer users into giving confidential information, like bank-account passwords and Social Security numbers.

Officials at the F.B.I. and the Justice Department say their inquiries on the zombie networks are exposing serious vulnerabilities in the Internet that could be exploited more widely by saboteurs to bring down Web sites or online messaging systems. One case under investigation, officials say, may involve as many as 300,000 zombie computers.

More than 170,000 computers every day are being added to the ranks of zombies, according to Dmitri Alperovitch, a research engineer at CipherTrust, a company based in Georgia that sells products to make e-mail and messaging safer.

"What this points out is that even though critical infrastructure is fairly well secured, the real vulnerability of the Internet are those home users that are individually vulnerable and don't have the knowledge to protect themselves," Mr. Alperovitch said. "They pose a threat to all the rest of us."

Full Article [2].

Security

Source URL: http://www.tuxmachines.org/node/1488

Links:
[1] http://www.tuxmachines.org/taxonomy/term/59
[2] http://www.nytimes.com/2005/06/24/technology/24zombie.html?