

Internet Attacks Grow More Potent

SAN FRANCISCO — Attackers bent on shutting down large Web sites — even the operators that run the backbone of the Internet — are arming themselves with what are effectively vast digital fire hoses capable of overwhelming the world's largest networks, according to a new report on online security.

In these attacks, computer networks are hijacked to form so-called botnets that spray random packets of data in huge streams over the Internet. The deluge of data is meant to bring down Web sites and entire corporate networks. Known as distributed denial of service, or D.D.O.S., attacks, such cyberweapons are now routinely used during political and military conflicts, as in Estonia in 2007 during a political fight with Russia, and in the Georgian-Russian war last summer. Such attacks are also being used in blackmail schemes and political conflicts, as well as for general malicious mischief.

A survey of 70 of the largest Internet operators in North America, South America, Europe and Asia found that malicious attacks were rising sharply and that the individual attacks were growing more powerful and sophisticated, according to the Worldwide Infrastructure Security Report. This report is produced annually by Arbor Networks, a company in Lexington, Mass., that provides tools for monitoring the performance of networks.

The report, which will be released Tuesday, shows that the largest attacks have grown steadily in size to over 40 gigabits, from less than half a megabit, over the last seven years. The largest network connections generally available today carry 10 gigabits of data, meaning that they can be overwhelmed by the most powerful attackers.

The Arbor Networks researchers said a 40-gigabit attack took place this year when two rival criminal cybergangs began quarreling over control of an online Ponzi scheme. "This was, initially, criminal-on-criminal crime though obviously the greatest damage was inflicted on the infrastructure used by the criminals," the network operator wrote in a note on the attack.

The attack employed a method called reflective amplification, which allowed a relatively small number of attack computers to generate a huge stream of data toward a victim. The technique has been in use since 2006.

“We’re definitely seeing more targeted attacks toward e-commerce sites,” said Danny McPherson, chief security officer for Arbor Networks. “Most enterprises are connected to the Internet with a one-gigabit connection or less. Even a two-gigabit D.D.O.S. attack will take them offline.”

Large network operators that run the backbone of the Internet have tried to avoid the problem by building excess capacity into their networks, said Edward G. Amoroso, the chief security officer of AT&T. He likened the approach to a large shock absorber, but said he still worried about the growing scale of the attacks.

“We have a big shock absorber,” he said. “It works, but it’s not going to work if there’s some Pearl Harbor event.”

Over all, the operators reported they were growing more able to respond to D.D.O.S. attacks because of improved collaboration among service providers.

According to the Arbor Networks report, the network operators said the largest botnets — which in some cases encompass millions of “zombie” computers — continue to “outpace containment efforts and infrastructure investment.”

Despite a drastic increase in the number of attacks, the percentage referred to law enforcement authorities declined. The report said 58 percent of the Internet service providers had referred no instances to law enforcement in the last 12 months. When asked why there were so few referrals, 29 percent said law enforcement had limited capabilities, 26 percent said they expected their customers to report illegal activities and 17 percent said there was “little or no utility” in reporting attacks.