Tech 101: How a denial-of-service attack works

July 8 2009, By JORDAN ROBERTSON , AP Technology Writer

An official gives a briefing about cyber attacks at the National Police Agency in Seoul, South Korea, Wednesday, July 8, 2009. South Korean intelligence officials believe North Korea or pro-Pyongyang forces in South Korea committed cyber attacks that paralyzed major South Korean and U.S. Web sites, a lawmaker's aide said Wednesday. (AP Photo/Yonhap, Hwang Kwang-mo)

(AP) -- Investigators are piecing together details about one of the most aggressive computer attacks in recent memory - a powerful "denial-of-service" assault that overwhelmed computers at U.S. and South Korean government agencies, companies and institutions, in some cases for days.

How does this type of cyber attack work? And how can people make sure their computers are safe?

Here are some questions and answers about the attack.

Q: What is a "denial-of-service" attack?

A: Think about what would happen if you and all your friends called the same restaurant over and over and ordered things you didn't even really want. You'd jam the phone lines and overwhelm the kitchen to the point that it couldn't take any more new orders.

That's what happens to Web sites when criminals hit them with denial-of-service attacks. They're knocked offline by too many junk requests from computers controlled by the attackers.

The bad guys' main weapon in such an attack is "botnets," or networks of "zombie" personal computers they've infected with a virus. The virus lets the criminals remotely control innocent people's machines, which are programmed to contact certain Web sites over and over until that overwhelms the servers that host the sites. The servers become too busy to respond to anything, and the Web site slows or stops working altogether.

It's different from what usually happens when you try to access a Web site. Normally, you just make one request to see the site, and unless there's a crush of traffic from something like a big news event, the servers respond well. Hijacked PCs, on the other hand, are programmed to send way more traffic than a normal user could generate on his or her own.

Q: How often do these attacks happen?

A: People try denial-of-service attacks all the time - many government and private sites report being hit every day. Often the assaults are unsuccessful, because Web sites have ways of identifying and intercepting malicious traffic. However, sites really want to avoid blocking legitimate Web users, so more often than not, Internet traffic is

let through until a problem is spotted.

Denial-of-service attacks are noisy by design, and they intend to make a statement. They're not subtle attempts to infiltrate a Web site's defenses, which can be much more insidious because that gives hackers access to whatever confidential information is stored there.

Often the attacks take a site out for a few hours, before Web site administrators can respond. What made the most recent attack notable is that it was widespread and went on for a while, beginning over the July Fourth holiday weekend and running into this week. It's not yet clear how the attack was able to last that long.

Q: Some organizations appear to have fended off these recent attacks, while other Web sites went down. How can this be?

A: The sites that went down probably were less prepared, because they are less accustomed to being hit or aren't sensitive enough to warrant extra precautions.

Popular Web sites, like e-commerce and banking sites, have a lot of experience dealing with denial-of-service attacks, and they have sophisticated software designed to identify malicious traffic. Often that's done by flagging suspicious traffic flowing into the site, and if there's enough of it, preventing it from ever reaching the site's servers.

Another approach is to flag suspicious individual machines that seem to be behind an attack, and ban any traffic from them from reaching the site.

That can often be difficult, though, because criminals use "proxy" computers to route their traffic, masking the source of the original requests. Proxy computers are often other infected computers that are

part of a botnet.

Q: Is there usually evidence of who the culprits were? Or is the nature of the attack such that it leaves few fingerprints?

A: It's usually easier to stop a denial-of-service attack than it is to figure out who's behind it. Simply identifying where the malicious traffic is coming from won't get investigators very far, since the infected PCs that get roped into a botnet are owned by innocent people who don't know their computers are being used for nefarious purposes.

Pat Peterson, a security researcher and fellow at Cisco Systems Inc., says sophisticated attackers have also been adding a more subtle approach to evade detection.

Instead of directing huge amounts of traffic at a target site, they'll make more complicated requests one at a time that eat up more of the site's computing power, like trying to log in using bogus usernames and passwords. If enough of those requests are made, on a site that requires a lot of computing power, the effect can be the same, and the site gets knocked out.

This type of attack is trickier because it doesn't involve the sort of massive traffic surge that would normally tip off network administrators.

This advanced tactic wasn't necessarily used in the most recent attacks. In fact there are signs the attacks were relatively amateurish. The programming code appears to have been patched together largely from material that has been circulating in the criminal underground for several years, according to Jose Nazario, manager of security research for Arbor Networks.

Q: If these attacks make use of compromised computers corralled into a

"botnet," should I be worried about whether my PC is one of them? What could I do to prevent that or fix it?

A: If your computer is being used in a denial-of-service attack, you're likely to see a significant slowdown, because your processing power is being siphoned for the assault. But there aren't always obvious signs that your computer has been infected.

So the best thing is to focus on prevention, namely by having up-to-date antivirus software. In particular, make sure your antivirus software gets updated over the next few days.

If you're concerned your machine might be infected, it's wise to run an antivirus scan. Many antivirus companies offer a free scan from their Web sites.