

**CNET News**

News - Security

September 23, 2008 12:37 PM PDT

## Infected U.S. PCs may have attacked Georgia

Posted by [Robert Vamosi](#)

When political tensions flared last month between [Georgia and its large neighbor to the north](#), the country was ready to block Internet traffic from Russia, hoping to avoid the denial-of-service attacks that shut down [Internet service in Estonia](#) for several days in 2007. Instead, most of the DoS attacks that were directed against Georgia came from an unlikely place: the United States.

"Russia is one of the most capable countries when it comes to launching system intrusion hacking attempts, distributed denial-of-service attacks, and operation of botnets," said Don Jackson, director of Threat Intelligence for SecureWorks. "Yet you'll notice the number of attacks coming from Russia are very low."

SecureWorks on Monday released a list ranking the countries with the most infected computers enlisted for use with botnets. On that list, Russia ranks 7th, far behind the United States, China, Brazil, South Korea, Poland, and Japan. The reason Russia is so low, Jackson said, is that hackers from Russia don't attack from within Russia.

Instead of attacking using Russian IP addresses, Jackson said, the hackers who wanted to attack Georgia used "computers and control servers located in Turkey while the bots (the infected computers) that they controlled were mostly in the United States."

Jackson said Georgia was not prepared to cut off traffic from the United States. "But they also couldn't cut off Turkey. The Turkish telecom network is their main upstream provider. So they couldn't really block Turkey either," he said.

On the SecureWorks list, the United States has more than 20 million botnet compromised PCs. The next highest is China at roughly one-third that number, or 7 million. At first glance that may seem due to the size of each country and the number of computer users. Jackson said that isn't necessarily the case.

"When we look at computers per capita," he said, "we obviously think of the United States. We have multiple computers per household now. But South Korea really has more computers than the United States. So it's not only a function of the numbers of computer per capita--it's also the number of insecure computers or computers that are unsecured or not patched. By far the United States is worse."

So why does the U.S. have so many infected PCs?

Jackson speculated that in the United States "we have a banking system that forgives us if spyware steals our credit number and it is used." He said the average home user in the U.S. has very little incentive to keep PCs patched.

He contrasted the situation with China where few home owners have computers; most of the country's computers are located inside companies and universities. This creates some interesting differences. For example, "these are homogeneous networks that are managed the same way, so if one exploit gets into the network, the worm will spread throughout the whole thing," he said.

And he said how botnets typically function within China is different than in the rest of the world. "With the Russian denial-of-service attack scenario we typically see a lot of incoming attacks from all over the world directed toward one place. In China it is less of a distributed attack and more of a traditional denial-of-service attack."

Beyond the U.S. and China, the eight other sources of compromised computers identified by SecureWorks include:

- Brazil
- South Korea
- Poland
- Japan
- Russia
- Taiwan
- Germany
- Canada