

Probe into cyberattacks stretches around the globe

Jeremy Kirk

July 14, 2009 ([IDG News Service](#)) British authorities have launched an investigation into the recent cyberattacks that crippled Web sites in the U.S. and South Korea, as the trail to find the perpetrators stretches around the world.

On Tuesday, the Vietnamese security vendor Bach Khoa Internet Security (Bkis) [said](#) it had identified a master command-and-control server used to coordinate the denial-of-service (DDoS) attacks, which took down major U.S. and South Korean government Web sites.

A command-and-control server is used to distribute instructions to zombie PCs, which form a botnet that can be used to bombard Web sites with traffic, rendering the sites useless. The server was on an IP (Internet Protocol) address used by Global Digital Broadcast, an IP TV technology company based in Brighton, England, according to Bkis. C, replay

That master server distributed instructions to eight other command-and-control servers used in the attacks. Bkis, which managed to gain control of two of the eight servers, said that 166,908 hacked computers in 74 countries were used in the attacks and were programmed to get new instructions every three minutes.

But the master server isn't in the U.K.; it's in Miami, according to Tim Wray, one of the owners of Digital Global Broadcast, who spoke to IDG News Service on Tuesday evening, London time.

The server belongs to Digital Latin America (DLA), which is one of Digital Global Broadcast's partners. DLA encodes Latin American programming for distribution over IP TV-compatible devices, such as set-top boxes.

New programs are taken from satellite and encoded into the proper format, then sent over VPN (Virtual Private Network) to the U.K., where Digital Global Broadcast distributes the content, Wray said. The VPN connection made it appear the master server belonged to Digital Global Broadcast when it actually is in DLA's Miami data center.

Engineers from Digital Global Broadcast quickly discounted that the attacks originated with the North Korean government, which South Korean authorities have suggested may be responsible.

Digital Global Broadcast was notified of a problem by its hosting provider, C4L, Wray said. His company has also been contacted by the U.K.'s Serious Organized Crime Agency (SOCA). A SOCA official said she could not confirm or deny an investigation.

Amaya Ariztoy, general counsel for DLA, said the company examined the server in question today and found "viruses" on it.

"We are doing an investigation internally," Ariztoy said.

Investigators will need to seize that master server for forensic analysis. It's often a race against the hackers, since if the server is still under their control, critical data could be erased that would help an investigation.

"It's a tedious process and you want to do it as quickly as possible," said Jose Nazario, manager of security research for Arbor Networks.

Data such as log files, audit trails and uploaded files will be sought by investigators, Nazario said. "The holy grail you are looking for are pieces of forensics that reveal where the attacker connected from and when," he said.

To conduct the attacks, the hackers modified a relatively old piece of malware called MyDoom, which first appeared in January 2004. MyDoom has e-mail worm characteristics and can also download other malware to a PC and be programmed to conduct denial-of-service attacks against Web sites.

Analysis of the MyDoom variant used in the attacks isn't that impressive. "I still think the code is pretty sloppy, which I hope means they [the hackers] leave a good evidence trail," Nazario said.

Find the right solutions and become
a smarter midsize business.



Get started