Finding source of hacking attack on registrar's site will be tough, expert says

SAN DIEGO (CNS) - Finding the ultimate source of an off-shore cyber attack on San Diego County's main website on election night will be a huge challenge, an expert at the Supercomputer Center at UC San Diego said Friday.

A firewall in the county's information technology system detected an attempt to overload the site with more than 1 million hits per minute just before 8:15 p.m. Tuesday, just as residents were trying to access the first election results on the Registrar of Voters website.

The firewall took sdcounty.ca.gov offline and sdvote.com, part of the same system but with a different web address, also went down for roughly two hours. The county's other departments, such as the library system and animal services, also lost their websites, county spokesman Michael Workman said.

"The IP address that was sending it to us was off-shore," Workman said. He said its exact location was unknown.

Josh Polterock, manager of scientific projects for the Cooperative Association for Internet Data Analysis at the Supercomputer Center, told City News Service the trouble for investigators will be that people who launch attacks generally use other people's computers.

People who send out "malware" over the Internet are able to harness thousands of compromised computers thanks to the widespread use of broadband and a propensity of North Americans, Europeans and some others to leave their systems on all the time, Polterock said.

He said another way they attack websites is through the use of "spoof" identifications, in which they randomly generate IP addresses that may or may not actually be in use. The Supercomputer Center owns a large number of IP addresses not tied to a device, yet they see activity with those identifications daily.

Experts at the center try to find interesting data among the 100 gigabytes of daily "garbage" to find useful correlations, Polterock said.

Other problems for cyber sleuths include the lack of a controlling authority over more than 40,000 networks that transmit data around the world, an inability to see many website attacks as they're happening, difficulty in differentiating between normal packets of data and others that contain malware, and data packets that can suddenly multiply, he said.

Workman said the good news was that the firewall worked and prevented damage to county IT systems or data. In fact, it only shut off the websites to outsiders -- county staff were able to obtain election data from sdvote.com and use other county websites, he said.

"We want to blunt this in the future, find a work-around and maybe prosecute," Workman said.

He said, as far as he knew, the website attack had nothing to do with the sdvote.com site specifically.

Hewlett Packard ruled out any hardware or software issues, and there was plenty of capacity for the number of users who tried to use sdvote.com, according to the county.