Zombie Computers Decried As Imminent National Threat

By Ryan Singel April 09, 2008 | 12:03:30 PMCategories: RSA Conference

Homeland Security Secretary Michael Chertoff speaks about computer security at the RSA Conference on information security in San Francisco, Tuesday, April 8, 2008.
AP Photo/Paul Sakuma

SAN FRANCISCO -- Gangs of thousands of zombie home computers grinding out spam, committing fraud and overpowering websites are the most vexing net threat today, according to law enforcement and security professionals.

Today's botnet herders have hundreds of thousands of computers at their command and use technically sophisticated ways to hide their headquarters, making it easy for them to make millions from spam and credit card theft. They can also be used to direct floods of fake traffic at a targeted website in order to bring down a rival, extract protection money or less frequently, used to make a political point in the case of attacks on Estonia and the Church of Scientology.

Security pros and government officials are now describing the latter attacks, known as Distributed Denial of Service attacks, as serious threats to national security -- turning packet floods against public websites into the latest face of "cyberwar" hysteria.

Hence, the appearance Tuesday of a panel discussion at the RSA 2008 security conference entitled "Protecting the Homeland: Winning the Botnet Battle," which was marked by a mix of resignation, indignation and post-9/11 rhetoric.

Ronald Teixeira, the executive director of the non-profit National Cyber Security Alliance and the panel's moderator, began the discussion by describing botnets as "one of the largest threats we face on the internet today, and they can be used to attack critical infrastructure."

The Department of Homeland Security's representative Jordana Siegel, who works on public awareness at the National Cyber Security Division, echoed the line that botnets were a imminent threat to the nation's security.

Citing the attacks on Estonia last year by Russian nationalist hackers, Siegel said botnets can "disrupt an internet-reliant society," saying that the temporary takedown of Estonian newspaper and government websites "nearly crippled the country's cyber infrastructure." Earlier in the day, Homeland Security chief Michael Chertoff leaned on Estonia as evidence of the need for a federal government "Manhattan Project" for computer security.

Siegel said the DHS is working at fighting the problem, citing the annual October National Cyber Security Awareness month, which she said helped Americans learn that "all users need to practice safe online behavior."

McAfee's Joe Telafici, a vice president in their security lab, lamented the ease with which botnet herders can abuse domain registration services and the low cost of e-mail, which make the economics of online crime very attractive.

"We are seeing a model that is so economically viable that trying to tell the kids it is a bad thing to do is bound to fail," Telafici said, suggesting that botnet herders outnumber the 15,000 or so attendees at RSA. "Even if you don't have a computer, you are paying money to someone for the cost of dealing with the security ramifications."

FBI agent Matthew Fine cited two recent takedowns of U.S.-based botnets, operations dubbed Bot Roast, as an example of how the FBI is dealing with botnets. Fine declined to speculate, however, on whether the arrests actually put a dent in overall online criminality.

"I get paid to put bad guys in jail," the flat-topped Fine said, but he noted that as soon as one botnet herder was prosecuted another takes his place.

"It is a boulder coming down the hill and I am trying to keep it from getting to the bottom," Fine said.

Fine hopes Congress will step in with tougher criminal penalties for botnet runners, but noted that judges were now handing out substantial sentences of four to five years in cases brought to them by the feds.

Ira Winkler, a security consultant known for his outspoken ways, countered that this was all just caterwauling and that if the country thought that botnets were a real problem, ISPs and individual users would be held responsible for zombie machines.

"The problem is no one is doing anything," Winkler said, proposing that users be fined or blocked if their computer is infected.

"Guess what? If your system has a bot on it, you don't get on the internet," Winkler said, summarizing his proposal.

"We need to hold people responsible when they present an imminent threat to other people," Winkler said to wide applause from the audience. He contrasted the lack of computer regulation to laws preventing unsafe cars from taking the road.

Sparing no target, Winkler went on to ridicule DHS's awareness efforts as useless, and argued that the highest levels of government don't care about computer crime, citing the ability of a Russian cyber-criminal group known as the Russian Business Network to remain free.

"When they start putting the RBN in jail, then I will be impressed," Winkler said, noting that would require the feds to put pressure on the Russian government to stop protecting the gang -- not an easy task.

Still, Winkler argues, that's doable with political will.

"When the U.S. government wants to get things done, they know how to put people in jail."

So what really is the threat to the so-called Homeland from zombie computer armies?

When asked by Threat Level, the panel came to a split decision.

"Terrorism with botnets is overrated," McAfee's Telafici said. "But if you are looking at the economic burden of botnets, we could probably do without it."

Winkler suggests that botnets could be used in tactical small attacks, including, perhaps, inflicting minor power outages.

DHS's Siegel defended the use of overheated rhetoric, saying that temporarily unavailable government or financial websites would erode public confidence.

Missing from the panel discussion was any in depth talk about real solutions.

For instance, ISPs can easily learn or be told which of their customers has an infected computer, but due to the customer support costs of cutting off a zombified user -- angry phone calls, confusion -- they tend to do little.

Also not talked about are changes in internet governance that punish known domain sellers and ISPs that favored by online criminals for their lax policies.