InformationWeek
BUSINESS INNOVATION POWERED BY TECHNOLOGY

Hackers Breaking Up Botnets To Elude Detection

While cybercriminals have spent months trying to build the largest botnets they could, now they're splitting them up into smaller, more manageable pieces.

By Sharon Gaudin, InformationWeek
Oct. 3, 2007
URL: http://www.informationweek.com/story/showArticle.jhtml?articleID=202200755

Cybercriminals are splitting their giant botnets up into smaller pieces to make them more agile and more easily hidden from detection, according to a security company.

Hackers and malware writers have been diligently building up massive botnets in recent months. Botners are a collection of compromised computers that can be remotely controlled by the hacker. When hackers build up an army of thousands or even millions of these zombie machines, they can use them to send out spam, malware, and to even launch denial-of-service attacks.

And until just recently, they appeared to be going by the philosophy that when it came to botnets, bigger was better. That's no longer the case, according to Iftach Amit, director of security research at security company Finjan.

"Smaller botnets get the job done, but smaller botnets generate a lot less traffic," he told *InformationWeek*. "That makes them harder to detect because they make much less noise. They fly under the radar when you're looking for anomalies in behavior."

The smaller botnets also are easier to manage and easier to keep online, Amit noted.

He explained that many botnets are operated from a single command center -- generally a server which the hacker uses to send out commands and updates. If security researchers or law enforcement find that command center, the botnet is effectively out of business. However, if the hacker splits the botnet up into several smaller botners, each with its own command center, if one goes down, the others remain operational.

"It comes down to financials," said Amit. "If you have a single botnet with a single point of failure and that goes down, you lose everything. If you cut it up into smaller botnets, you get added security."

He noted that researchers at Finjan have seen some botnets that used to number in the hundreds of thousands broken into ones that number in the tens of thousands.

What's not clear yet is what might be happening with the Storm worm botnet.

That zombie army has reportedly grown into a massive botnet, with estimates ranging from hundreds of thousands to several million. The botnet, which has pounded the Internet for the last several months with spam and denial-of-service attacks, has become one of the largest zombie grids researchers say they've ever seen.

Amit said it's not yet clear if the Storm worm botnet is being broken up into smaller pieces or if it's retaining its size. The Storm botnet, however, is not controlled by one command center, which has made it difficult for researchers to shut it down. That also may be a reason to not split it up into smaller pieces.