Researchers: Botnets Getting Beefier

April 17 2007

Botnets are moving to more resilient architectures and more sophisticated encryption that will make them even harder to track and fight, researchers say at HotBots, a Usenix event.

Think botnets are bad now? We ain't seen nothin' yet.

A select group of some 40 security researchers gathered on April 10 in the first Usenix event devoted to these networks of infected machines. The invitation-only event, called HotBots, was held in Cambridge, Mass.

At the event, researchers warned that botnets - which can contain tens or even hundreds of thousands of zombie PCs that have been taken over for use in spamming and thievery of financial and identity-related data - are on the brink of a technological leap to more resilient architectures and more sophisticated encryption that will make it that much harder to track, monitor and disable them.

Specifically, security researchers have spotted the early development stages of resilient botnets that have included peer-to-peer architectures. Botnets have traditionally been organized in a hierarchical structure, with one central command-and-control location. This centralization has been a blessing to researchers, as it gives them a single point of failure on which to focus.

With a P2P botnet, however, there is no centralized point for command and control. Each node in the network acts as both client and server, eliminating the central chokepoint. Individual nodes can be knocked

offline, but the gaps in the network will be closed without the loss affecting the botnet's operation or the attacker's control.

"P2P networks - are - the biggest challenge we're facing," Dr. Jose Nazario, senior security engineer for Arbor Networks, headquartered in Lexington, Mass., said in an interview with eWEEK. "Bad guys know this. - P2P botnets are hard to take down - for the same reasons that media companies have trouble shutting down P2P networks."

Not that P2P botnets are all that new. In a paper presented at HotBots titled "Peer-to-Peer Botnets: Overview and Case Study," Julian B. Grizzard, David Dagon, Vikram Sharma, Chris Nunnery and Brent ByungHoon Kang gave a timeline that shows the rise of malicious bots beginning at least as far back as 1998, with the release of GTBot Variants, an IRC (Internet Relay Chat) bot based on mIRC executables and scripts. A recent example of a P2P botnet was the Storm worm, also called the Peacomm Trojan. The Storm worm initially wreaked havoc via spam e-mail in January and then in February spawned a variant that used instant messaging platforms to spread.

Researchers the week of April 9 noted the return of the Storm worm, as more than 2 million spam e-mails arrived carrying the latest variant. Whereas the initial wave of spam used recent real or fake news headlines to convince users to execute malicious files, last week's Storm surge used e-mail subject lines claiming "Trojan Detected!" or "Worm Activity Detected!"

Although they are not new, P2P botnets have undergone recent breakthroughs in terms of design and modular code bases, the paper's authors argued, saying that one botnet in particular - Agobot - marked a "turning point in which botnets have become a more significant threat."

"Peer-to-peer bots are now under widespread development," the authors

wrote. "Some peer-to-peer bots have used existing peer-to-peer protocols while others have developed custom protocols. We predict that peer-to-peer botnets will mature to a level in which they might become more widespread than traditional decentralized C&C architectures."

Another problem in fighting botnets is that less savvy computers users can be oblivious to the need to update their anti-virus programs, Nazario said. "We see people with AV who don't update it or don't know it needs to be updated… We see protection that's way out of date," he said.

What to do about these sophisticated botnets? Nazario said Arbor Networks now looks for known nodes on P2P networks. The security firm works with a number of partners, including anti-virus software vendors, to make sure it has updated code for detecting bots on machines. Arbor also works with Internet operators to shut down access to command servers in traditional command-and-control botnets. "If we can shut down - a botnet - , machines are still infected, but the damage is lessened greatly," Nazario said.

One of the most efficient ways for enterprises to address the bot problem is to blacklist malicious sites and hosts and block access to them. Still, working with anti-virus signatures is "an arms race," Nazario said. "It's always a day or so behind. These guys are incentivized with the money we're seeing" in the bot economy - or what some are calling "botconomics," he said - and thus attackers are always one step ahead of their pursuers when it comes to technological advances and creating new bot networks.

Botnet watchers are also seeing a trend toward stronger encryption. Encryption is used by attackers to ensure that bots added to the network are in fact legitimate, as opposed to being nodes belonging to researchers working to infiltrate a botnet and block it or take it down.

The good news on that front is that, typically, attackers don't write very good encryption algorithms. "Breaking them is pretty trivial," Nazario said. "We're generally a smart bunch of people. We can break their home-brewed encryption pretty easily. The keys are exposed, so we can simply grab the keys and use existing encryptions and algorithms to take part in the network. It's easy as pie."