

As Seen On



Monday, April 7, 2008

## Kraken botnet balloons to dangerous levels

By Dennis Fisher, Executive Editor, SearchSecurity.com

A large botnet, estimated to be roughly twice the size of the one created by the Storm Trojan, has been gathering strength for the last several months, gaining more than 100,000 new machines in the last month alone.

Known as Kraken, the malware that infects the victims' PCs is somewhat similar to the Storm Trojan and others like it, in that it uses encrypted communications and has the ability to move command and control functionality around the botnet if need be, according to researchers at Damballa Inc., a security vendor that has been tracking the Kraken botnet. And, like most botnets, the purpose of the Kraken network seems to be the propagation of massive amounts of spam. Damballa officials say they have seen individual machines sending as many as 500,000 spam messages in a single day.

But, unlike both Storm and Nugache, the Kraken botnet does not use a peer-to-peer architecture. Instead, the malware code includes a list of domains in which the C&C server might be located, and once a new machine is infected it begins looking through that list to find the current location. If a C&C server is taken down, as often happens with large botnets, Kraken's creator can simply move the command and control function to another domain in the hard-coded list, said Paul Royal, principal researcher at Damballa, of Atlanta.

"What the guy who created this did is buy himself an insurance policy," Royal said. He has seen C&C servers in locations around the globe, including France, Russia and Dallas. Royal first saw signs of Kraken in late 2006, but wasn't able to pin it down until nearly a year later. Most recently, one of Damballa's customers had a large infection of the bot on its network. Damballa will be discussing the Kraken research at the RSA Conference on Monday.

The Kraken code arrives in a file disguised to look like a typical image file, such as a JPEG or a PNG, but with a hidden extension that prevents users from recognizing it as an executable. Once a user opens the file, it copies itself to the local machine, restarts and then deletes the original copy. One somewhat interesting feature of the code is that the binary is not packed, as many malware binaries tend to be. However, Royal said that the code does have some other forms of obfuscation that make it difficult to analyze completely.

Royal said Damballa saw more than 400,000 unique infected IP addresses on one day in March, with the number continuing to trend upward from about 300,000 in early March. Kraken is just the latest in a line of large-scale botnets to rear their heads in the last couple of years. Storm is perhaps the best-known of these, and is also the most resilient. The Storm Trojan's authors have shown themselves to be quite creative in developing new tactics for infecting machines. Nugache also has caused some trouble, and researchers say there likely are plenty of other botnets in operation right now that just haven't been noticed yet.

Damballa plans to publish a subset of the list of infected IP addresses it has seen within the next week or so.