

10 April 2008

By: Bogdan Popa, Security and Search Engines Editor



Sorry, no botnets
allowed here!
hyperlearn.com

[Meet Srizbi, the Largest Botnet Ever](#)

SecureWorks presents the most dangerous botnets

Security company SecureWorks has published a report revealing the most dangerous botnets spotted on the web and, even some of you may expect to the Storm on the first position, it's only the fifth. Thus, the first place was "won" by Srizbi, also known as Cbeplay and Exchanger, which is a rootkit enabled botnet that sends no less than 60 billion spams per day using approximately 315,000 bots. Bobax comes on the second place with an estimated number of bots of 185,000 and no less than 9 billion spams sent every day. In case you didn't know, Bobax is also known as Bobic, Oderoor, Cotmonger, Hacktool.Spammer and Kraken. The well-known Storm is only the fifth botnet in this hierarchy with approximately 85,000 bots from which only 35,000 send emails. However, they manage to produce an average of 3 billion spams per day. Getting back to king Srizbi, SecureWorks explains that it is a "highly capable botnet spamming machine" especially to its advanced SMTP engine which permits it to send spams while remaining unidentified. "However, Srizbi is not a monolithic botnet - it is split between several customers of Reactor Mailer, with over a dozen control servers. Because of this, a wide variety of spam can be seen coming from Srizbi at any given time. In addition, Srizbi is one of the most active botnets attempting to seed new infections by advertising links to porn-related video files of different celebrities, which are actually new copies of Srizbi," SecureWorks stated. The hierarchy released by the security company is ended by Spamthru (a.k.a. Spam-DComServ, Covesmer, Xmiler), a less known botnet that has "only" 12,000 bots and sends approximately 350 million spams per day. Having a look at this number clearly shows us that botnets tend to become an important part of our lives and, as long as we don't protect our computers with powerful security software, they will reach more and more vulnerable systems.