November 10th, 2009, 10:48 GMT · By Lucian Constantin

Botnet Command and Control Server Hosted on Google App Engine

Security researchers have discovered a botnet that queried a rogue application hosted on Google's App Engine platform for commands. Its command and control server instructed infected computers to download and install a backdoor component.

The unusual piece of malware was discovered by researchers from network security company Arbor Networks, who tracked its connections to a Google App Engine application. "The app in question is being used to feed URLs to the zombies for them to download," Jose Nazario, manager of security research at Arbor, explains.

The Google App Engine allows developers to run the Web applications on Google's infrastructure. Hosting an application that does not require more than 500 MB of storage space and five million page views per month is free. So far, the platform features a Java Runtime Environment and a Python interpreter.

Google has been notified of the abuse and has taken the rogue application offline. Researchers were not able to uncover much of the specific commands that this botnet C&C server was able to give as they did not obtain access to the code hosted on Google App Engine.

The only relevant malicious behavior they noticed was the command to download a file called aa.exe from a third-party URL. This file is actually an installer for a backdoor component known as PCClient.

Another URL of the application appears to have been used to count visits to it, which might indicate the number of infected computers comprising the botnet. The monthly count at the time when the app was analyzed was 587.

This is not the first C&C server to be hosted on a public service. Several such sightings have been reported in recent months, beginning with a **Twitter feed** that was being used to relay commands to bots. Security researchers from Symantec later discovered a botnet that was **using a Google group** for a similar purpose.