

10 January 2009



Screenshot of the "Help Israel Win" website  
Arbor Networks

By: Lucian Constantin, Web News Editor

## [Botnet Tool to Support Israel's Offensive](#)

### *End-users willingly turn their computers into zombies*

Israel supporters respond to the [cyber-attacks](#) launched by Islamic hackers through DDoS. A group of students have developed an application that allows Israel sympathizers to use their computer resources and Internet bandwidth in order to knock Palestinian websites offline.

The online group calling themselves "Help Israel Win," is distributing a Trojan-like application that enables them to launch DDoS attacks. Installing this program onto a computer will turn it into a drone, and will place it at the disposal of the hacktivists. What differentiates this tool from regular malware is that the installation is performed voluntarily by individuals who sympathize with Israel's efforts.

"Our goal is to use this power in order to disrupt our enemy's efforts to destroy the state of Israel. The more support we get, the more efficient we are," the website set up by the group reads. The hackers included an uninstaller for the application and vowed to dismantle the botnet, once the conflict in Gaza Strip is over.

Bojan Zdrnja, security researcher at the SANS Internet Storm Center, has [analyzed](#) the botnet client application and concluded that it can be a serious security risk, because of its update functionality. By using this option, the bot runners could theoretically install additional potentially malicious applications on the computers.

"While at the moment it does not appear to do anything bad (it just connects to the IRC server and sites there - there also appeared to be around 1000 machines running this when I tested this) the owner can probably do whatever he wants with machines running this," Bojan writes. He also confirms that the uninstaller seems to function correctly, as stated by its creators, but it would be useless if other malware is installed.

The botnet command and control server is located on IRC, and the application uses a legit IRC client library in order to contact it. The group claims that over 8,000 individuals have joined the cause so far by willingly installing the "Patriot" tool on their computers. The students have even gone to the length of translating their website in other languages such as French, Portuguese, Russian, Spanish, in addition to English and Hebrew.

This is not the first time when end-users have assisted hackers in launching politically-motivated attacks. A highly [similar project](#) was launched by a Russian group during the conflict in Georgia. The website encouraged Russian sympathizers to install a botnet client and allow their bandwidth to be used in order to launch denial of service attacks against Georgian websites.