30 June 2011 Last updated at 06:34 ET

Cracking the TDL-4 botnet is going to be hard, say security experts.

More than four million PCs have been enrolled in a botnet security experts say is almost "indestructible".

The botnet, known as TDL, targets Windows PCs and is difficult to detect and shut down.

Code that hijacks a PC hides in places security software rarely looks and the botnet is controlled using custom-made encryption.

Security researchers said recent botnet shutdowns had made TDL's controllers harden it against investigation.

The 4.5 million PCs have become victims over the last three months following the appearance of the fourth version of the TDL virus.

The changes introduced in TDL-4 made it the "most sophisticated threat today," wrote Kaspersky Labs security researchers Sergey Golovanov and Igor Soumenkov in a detailed analysis of the virus.

"The owners of TDL are essentially trying to create an 'indestructible' botnet that is protected against attacks, competitors, and anti-virus companies," wrote the researchers.

Recent successes by security companies and law enforcement against botnets have led to spam levels dropping to about 75% of all e-mail sent
, shows analysis by Symantec.

A botnet is a network of home computers that have been infected by a virus that allows a hi-tech criminal to use them remotely. Often botnet controllers steal data from victims' PCs or use the machines to send out spam or carry out other attacks.

The TDL virus spreads via booby-trapped websites and infects a machine by exploiting unpatched vulnerabilities. The virus has been found lurking on sites offering porn and pirated movies as well as those that let people store video and image files.

The virus installs itself in a Windows system file known as the master boot record. This file holds the list of instructions to get a computer started and is a good place to hide because it is rarely scanned by standard anti-virus programs.

The majority of victims, 28%, are in the US but significant numbers are in India (7%) and the UK (5%). Smaller numbers, 3%, are found in France, Germany and Canada.

However, wrote the researchers, it is the way the botnet operates that makes it so hard to tackle and shut down.

The makers of TDL-4 have cooked up their own encryption system to protect communication between those controlling the botnet. This makes it hard to do any significant analysis of traffic between hijacked PCs and the botnet's controllers.

In addition, TDL-4 sends out instructions to infected machines using a public peer-to-peer network rather than centralised command systems. This foils analysis because it removes the need for command servers that regularly communicate with infected machines.

"For all intents and purposes, [TDL-4] is very tough to remove," said Joe Stewart, director of malware research at Dell SecureWorks to Computerworld.
"It's definitely one of the most sophisticated botnets out there."

However, the sophistication of TDL-4 might aid in its downfall, said the Kaspersky researchers who found bugs in the complex code. This let them pry on databases logging how many infections TDL-4 had racked up and was aiding their investigation into its creators.

Read more http://goo.gl/MMlLG