YGN ETHICAL HACKER GROUP

Whitepaper

# Defeating Powerful X-Rummer Spam Bot

**By**

**d0ubl3_h3lix**

**Mon Feb 19, 2007**

# Abstract

X-Rummer is a very powerful spam bot that I have ever seen. It is supposed to be developed in Russia. Due to its built-in capcha recognition engine, it can recognize cache images. It can spam any types of popular boards/forums like phpBB, YaBB, Bulletin Board with any messages you like. You don't need to do anything complicated. It is totally user-friendly and extremely easy to use. Relatively bad guys can flood all forums. It is multi-threaded; meaning that you can spam dozens of spam requests simultaneously. It has self-registration accepted and processed with some mail servers and thus can response confirmed challenges such as 'Confirmation Email', 'Confirm your account info' …etc.

Please watch its videos here:
http://www.botmaster.net/movies/XFull.htm
http://www.botmaster.net/movies/XDemo.htm

# Defeating

Every developer is amazed by X-Rummer's powerful features. They feel as if they cannot protect it at all because the spam bot defeats spam-protected security measures that are currently employed in today popular message boards. In fact, it is not that difficult to defeat it back. X-Rummer was designed fixedly to attack exact patterns of processing. Its spamming can be totally protected by adding one or more field of protections either of another capcha or simple text box that randomly asks visitors something like 'what is the result of 100+1'.

# Defeating Scenario

## phpBB Example

My dear friend Ko Min Thu's forum (http://forum.flashband.net) was spammed by X-Rummer. I implemented a very simple security measure that fooled X-Rummer. You can check it out when you first register for membership: simply a text box that asks you to type FB. Personally, using capcha seems burdensome to users, especially if capcha image is complicated to view.

## Proof-Of-Protection