Security experts warn of new 'almost indestructible' TDL-4 botnet threat

1 July 2011, by Bob Yirka

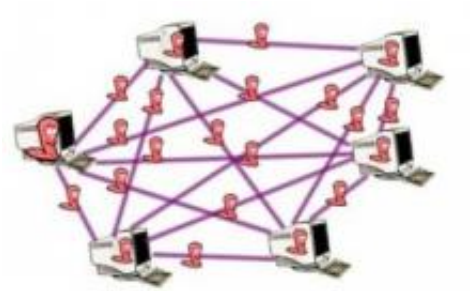

Image credit: Security Networks

(PhysOrg.com) -- Security experts Sergey Golovanov and Igor Soumenkov of Kaspersky Lab have detailed the threats of a new strain of the TDSS botnet, dubbed TDL-4, on SECURELIST, calling it likely the most sophisticated botnet to date, and describing it as *almost indestructible*.

Botnets, or groups of computers that have been infected by code that allows them to be controlled by someone other than the owner, have become the latest tool in an international cyberwar that involves malevolent coders and law enforcement, with computer users stuck in-between, quite often completely unaware of what it going on.

Botnets are a bad thing because computer owners can become victims of identity theft, be directed to onerous sites while cruising the web, or worse become unwitting partners in crime as their computer is hijacked and used for nefarious purposes, such as being directed to take part in a denial of service attack against a corporate web site.

TDL-4, comes on the heels of news that its previous incarnation, TDL-3 was sold by its creators to another group of hackers bent on reaping profits from its use; a sign the experts note, indicates the creators of the botnet are so sure of the superiority of the new version, that the old has become obsolete.

What makes the new botnet so hard to find and eradicate is the fact that it lodges itself in the master boot record on a computer's hard drive, the part the computer uses to get itself going when you turn it on. By inserting code where the hardware looks first, the malware is able to load before the operating system (Windows), allowing it to mask itself. Another problem is that in the new version, the creators of the malware have switched from using a proprietary network to control the computers in the botnet, to using a public Peer to Peer public network, which means commands can be sent even if the command and control computers used by the people who unleashed the botnet, lose access.

It should be noted that the security team behind this latest announcement Golovanov and Soumenkov, both work for Kaspersky Lab, a company that sells anti-virus and computer security software; not that this means their loud warnings should be ignored, but it is possible that their claims are a little exaggerated. For example, one of the new "features" of the botnet code is the ability to remove other malware from the computers they infect, partly to make sure their own code works as expected, but also to avoid drawing attention to problems the computer might be experiencing, which would likely lead to the detection of their own code. Thus, when they report that the botnet might be impossible to kill, they mean the botnet as a whole, not the code on an individual computer. Also, in their paper, there is no mention of what computer users can do to see if their computer is infected, and if it is, what they might do about it, which might make some wonder if a future announcement isn't coming soon, detailing how Kaspersky Lab, has just the product to help users with both.

© 2010 PhysOrg.com

APA citation: Security experts warn of new 'almost indestructible' TDL-4 botnet threat (2011, July 1) retrieved 26 November 2020 from https://phys.org/news/2011-07-experts-tdl-botnet-threat.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.