Botnets move P2P as centrally controlled zombie networks come under fire

April 22 2011, by Bob Yirka

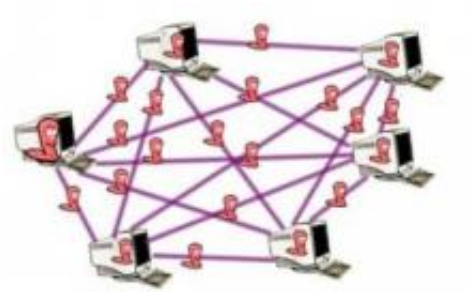

Image credit: Security Networks

(PhysOrg.com) -- Botnets, those networks of computers infected with bots (little pieces of code that allow a computer to be manipulated from an outside source) have increasingly of late come under attack by law enforcement agencies as it's become apparent that criminals are using them to steal personal information such as credit card numbers and pins. But, as the centrally based botnets go down, new peer to peer (P2P) botnets are cropping up to replace them.

Traditionally, botnets have relied on a small group of control computers to send out instructions to thousands of infected PC's to do their dirty work, despite the fact that is has a very large major weakness; take away the few central computers and the botnet dies. Because of this, another type of botnet, where each bot contains additional code that allows it to pass along instructional information, is starting to emerge. With these so-

called P2P networks, no central command is needed, instructions are fed to just one or two members of the network, and those few pass them along to others, who in turn pass them on until the whole network has been updated and is working as one.

Clearly this new type of botnet would be a lot harder to kill. Enter researchers from Los Alamos National Laboratories, in New Mexico, where Stephan Eidenbenz and his colleagues have been creating and killing botnets in a secure lab. Recently, they published a paper in Computer Networks describing a modified version of a P2P botnet that they believe would create a significant problem for those looking to stamp out botnets in general. In this new configuration, the bot network would set itself up into a hierarchy with instructions coming only from a computer higher up the in the hierarchy, who would in turn only receive commands from one higher up yet, until the one at the top is reached.

Creating such a network would overcome some of the technical difficulties that botnet builders have been running into when trying to create strong stable conventional P2P botnets, and that is, the complications that arise when trying to create a network that relies purely on individual PC's being able to communicate with one another; that would be sort of like relying on information from word of mouth, or rumor, rather than getting it straight from the top. In the new configuration (wherein the authors clearly don't disclose the how-to part, as that would give the bad guys the goods) there is once again just a few computers running the show, but the trick is, the hierarchy is scrambled anew each day allowing different computers to sit at the top issuing commands down the line, thus making it virtually impossible for law enforcement to track down which machines are actually issuing the commands at any given point in time.

By doing research of this kind, those on the right side of the law are hoping to create the next generation botnets before those on the wrong

side figure out how to create them for themselves; and hopefully by that time, ways to kill them.

More information: AntBot: Anti-pollution peer-to-peer botnets, *Computer Networks*, doi:10.1016/j.comnet.2011.02.006

Abstract

Botnets have emerged as one of the most severe cyber-threats in recent years. To evade detection and improve resistance against countermeasures, botnets have evolved from the first generation that relies on IRC chat channels to deliver commands to the current generation that uses highly resilient P2P (peer-to-peer) protocols to spread their C&C (Command and Control) information. On an encouraging note, the seminal work done by Holz et al. [14] showed that P2P botnets, although relieved from the single point of failure that IRC botnets suffer, can be easily disrupted using pollution-based mitigation schemes.

For white-hat cyber-security practitioners to be better prepared for potentially destructive P2P botnets, it is necessary for them to understand the strategy space from the attacker's perspective. Against this backdrop, we analyze a new type of P2P botnets, which we call AntBot, that aims to spread their C&C information to individual bots even though an adversary persistently pollutes keys used by seized bots to search the C&C information. The tree-like structure of AntBot, together with the randomness and redundancy in its design, renders it possible that individual bots, when captured, reveal only limited information. We mathematically analyze the performance of AntBot from the perspectives of reachability, resilience to pollution, and scalability. To evaluate the effectiveness of AntBot against pollution-based mitigation in a practical setting, we develop a distributed high-fidelity P2P botnet simulator that uses the actual implementation code of aMule, a popular Kademlia-based P2P client. The simulator offers us a tool to evaluate the attacker's strategy in the cyber space without causing

ethical or legal issues, which may result from real-world deployment. Using extensive simulation, we demonstrate that AntBot operates resiliently against pollution-based mitigation. We further suggest a few potential defense schemes that could effectively disrupt AntBot operations and also present challenges that researchers need to address when developing these techniques in practice.

via Technology Review