Summary for “Disrupting Stealthy Botnets through Strategic Placement of Detectors”

Krishna Sindhuja Kalusani

USC ID: T25568677

Abstract:

Botnet is a collection of the compromised (bots) systems remotely controlled by a botmaster. Botnets have become prevalent due to their ability to facilitate large-scale attack campaigns such as Distributed Denial of Service (DDoS), spamming, phishing, and click fraud. Botnets have become increasingly sophisticated that they can significantly reduce their footprint and increase dwell time. This paper focuses on an approach to strategically deploy detectors on selected network nodes so as to either completely disrupt the communication between bots and command and control nodes, or atleast force the attacker to increase the number of bots further increasing the footprint thereby the likelihood of detection. The detector placement problem is intractable and proposed heuristic placement startegies based on centrality measures. The proposed are ‘Degree Central Strategy’, ‘Global Betweenness Centrality Strategy’, ‘Mission Betweenness Centrality Strategy’, ‘Iterative Mission-Betweenness Centrality Strategy’, ‘Weighted Iterative Mission-Betweenness Centrality Strategy’, ‘Trivial Strategy’.

Contributions:

The approach was able to make the attacker increase the bots in the network making the detection easy for the owner.

They have indicated that the detector placement problem was intractable and proposed heuristic placement strategies.

Simulation results complemented that their approach can effectively increase complexity for the attacker.

Weakness:

The processing time increases quadratically with the increasing network size in weighted iterative mission betweenness centrality strategy. This strategy secures more centrality channels than the other strategies also has the lowest processing speed due to the additional computation incurred from computing the relative increase in shortest path length for each potential detector node.