Visual Investigations of Botnet Command and Control Behavior

Tom Cross and Andrea Fletcher
Lancope Inc.
Alpharetta, Georgia, US

Keywords: botnets, malware, command and control, visual analysis of datasets

Malicious botnets are a problem that continues to plague the Internet. Every year, attackers infect millions of computer systems with botnet software that is designed to steal information or launch other attacks. Attackers control these networks of infected computer systems using command and control protocols that operate over TCP/IP. Once botnet software has infected a computer system, it reaches out to a predesignated command and control system for further instructions.

Our research explores the command and control behaviors a collection of nearly two million unique botnet malware samples that were active between 2010 and 2012. These samples reached out to nearly 150,000 different command and control servers on over 100,000 different TCP and UDP ports. This data set is complex and heterogeneous, and thus it is difficult to analyze. However, when the data is represented visually, patterns emerge that lead to interesting insights.

The figures below present the combined TCP and UDP port popularity in both color and grayscale on 255x257 pixel charts. (In the grayscale image, the lighter colored ports are more popular.) We will compare these results to control data of network activity from an office LAN and investigate notable features including horizontal and diagonal bands of popular port numbers. The goal of our investigation is to better understand and characterize botnet command and control behavior in search of ways to differentiate botnet activity from legitimate network traffic.