

Title:

Correlation-based Botnet Detection in Enterprise Networks

Abstract:

Most of the attacks and fraudulent activities on the Internet are carried by malware. In particular, botnets have become the primary "platforms" for attacks on the Internet. A botnet is a network of compromised computers (or, bots) that are under the control of an attacker (or, botmaster). A botnet typically has tens to hundreds of thousands of bots, but some had several millions of bots. Botnets are now used for distributed denial-of-service attacks, spam, phishing, information theft, etc. With the magnitude and the potency of attacks afforded by their combined bandwidth and processing power, botnets are now considered as the largest threat to Internet security.

In this talk, I focus on addressing the botnet detection problem in an enterprise-like network environment. I present a correlation-based framework for botnet detection that consists of detection technologies already demonstrated in several systems (BotHunter, BotSniffer, BotMiner, and BotProbe). The common thread of these systems is correlation analysis (vertical correlation, horizontal correlation, and cause-effect correlation). I will mainly discuss BotHunter, BotSniffer and their corresponding correlation techniques/algorithms in this talk. These systems have been evaluated in live networks and/or real-world network traces, and the results show that they can detect real-world botnets with a very low false positive rate. These systems are starting to make an impact in the real-world. For example, there have been more than 6,000 downloads of BotHunter in the first five months after its public release. In addition, BotHunter is now being transitioned into products by several security vendors.

Short bio:

Guofei Gu is a Ph.D. candidate in the College of Computing at Georgia Tech, where he is affiliated with the Georgia Tech Information Security Center and the Center for Experimental Research in Computer Systems. His research interests are in network and system security; specifically intrusion detection and malware detection, defense and analysis. Further information is available at <http://www.cc.gatech.edu/~guofei>.