Technology Profile Fact Sheet

Title: IRC Characterization and Behavior Observation Tool

Aliases: ICABOT

Technical Challenge: Signature-based Intrusion Detection Systems (IDS) are currently being used to identify automated Internet Relay Chat (IRC) clients but with varying levels of success. A signature-based IDS often performs string matching within network traffic to identify possible malicious communications. String matching is very basic and requires a known signature. New and/or, previously unseen, attacks are not detected using signature-based IDSs because there is no prior knowledge of specific packet information to search for, which is a disadvantage. Signature-based detection methods are also easy to evade since they rely heavily on specific packet payload information, which can be modified by an attacker. In relation to the IRC protocol, malicious IRC bot creators often change or modify their command strings to evade detection from the latest intrusion detection signatures.

Description: The invention is designed to detect automated IRC clients within computer network communications through behavior analysis. The invention distinguishes IRC clients controlled by human actors from those that are controlled by other software programs. Automated IRC clients are commonly used to control malware-infected computer systems with the purpose of creating command and control networks. The command and control networks can be utilized to perform malicious actions including Distributed Denial of Service (DDoS) attacks, vulnerability scanning, and computer exploitation. Malicious automated IRC clients are more commonly known as malicious IRC bots and are a great threat to computer networks. The invention consists of three behavior detection methods that can be applied either individually or in combination to identify automated IRC clients and thus IRC bots within network traffic in real-time. These methods can be integrated into existing technology or used independently.

Demonstration Capability: A demonstration is not currently available.

Potential Commercial Application(s): Many Internet Security, or Internet Service Provider companies would be interested in the protection provided by this patent. The patented methods would also be of benefit to IDS producers who wish to incorporate these techniques into their products to improve their capabilities.

Patent Status: A patent application has been filed with the USPTO.

Reference Number: 1443