JumpCloud #1
–
Go-based egress monitoring

Client
Topher Marie, CTO

Company Background
JumpCloud is a venture-funded company located in Boulder. Founded in 2012 we now have seven engineers working in Go and Node.js backed with MongoDB in an Amazon-based environment. Our offerings are centered around server management, security, and authentication -- controlling who can get onto a machine and allowing administrators to manage the servers with complex orchestration, as well as managing the security posture of the system. More information is available at http://www.jumpcloud.com.

Project Goals
Customers have the desire to be able to monitor traffic that is leaving their servers. One of the most valuable indications of server compromise (i.e., I've been pwdn) is that some process is sending data or making connections to the outside world. Monitoring all connections constantly is a cpu-intensive operation, however, so care must be taken to do this intelligently. We'd like to add automatic light-weight egress monitoring to users' systems to allow them to be alerted to compromise.

Specifically we need to:
*Write GO code that can be configured to periodically check outbound traffic from a server. Alternately if we could be notified when a new connection is established (i.e., implement a listener) that would be better
*Intelligently detect anomalous traffic and notify appropriately. Not all outbound traffic is bad. We need to implement an algorithm to decide what indicates suspicious behavior.

Project Skills
*Basic programming knowledge.
*Go experience useful but not necessary.