Covert Command and Control Channel

Luke Bradford ’16
Faculty Advisor: Peter A. Yoon

A Covert Command and Control Channel is a cyber attack asset that provides cyber attackers with abilities critical for winning a cyber engagement. Control of cyberspace is becoming the deciding factor of modern conflicts. In order to gain the upperhand, it is important to have a plethora of cyber attack assets. A Covert Command and Control Channel is the perfect cyber attack asset. Covert Command and Control Channels allow attackers to remotely and covertly issue commands to enemy computers. This project implemented a channel that uses Twitter to enable undetected communication between the attacker’s computer and enemy computers. When the attacker issues a command, it is sent as a tweet to a Twitter page. Enemy computers check the Twitter page for new tweets containing the attacker’s commands. If an enemy computer finds a new command, it executes the command and sends notification to the attacker.

This Covert Command and Control Channel gives attackers familiar command line interaction with an enemy computer. Command line interaction is simple to use, yet it provides attackers with a wide array of critical abilities. Using the channel, attackers can access much of the functionality provided by the command prompt such as issuing commands, navigating directories, and viewing the contents of files. Undetected command line interaction with an enemy computer provides the means for stealing sensitive information, surveillance, and disrupting of services. These are important capabilities for winning a cyber engagement. This channel underwent several rounds of testing in a simulated environment comprised of two virtual machines. One machine simulated the attacker’s machine, and the other simulated the enemy computer which received and executed commands sent by the attacker's machine. Testing showed the channel to be reliable, user friendly, and effective.