Final Project Covert Communication

Mario Enriquez

British Columbia Institute of Technology

COMP 8505, 7D

Aman Abdulla

December 12, 2016

Contents

Technical Report

About this report:

This is the technical report for the final project of COMP 8505, In which I'll explain how my protocol works as well as measures to take to detect one.

Protocol:

My protocol consisted on a host and a victim machine.

The host consisted of three components:

- The command execution
- The packet filter to get the responses for port knocking and command results
- The raw socket listening for any packet incoming trying to establish connection

The victim consisted of two components:

- The packet filter to get the responses for port knocking and command results
- The exfiltration command, waiting until a new file is created.

For my program, the covert channel part works as this:

The user sends an encrypted command to the victim, the victim decrypts info and executes the command. The result is encrypted and sent back to the host who prints the results. The exfiltration part discovers a new file, port knocks into the host ip, the host allows the connection to a specific port with the firewall and sends the packet.

Recommendations:

One of the most difficult aspects about detecting this kind of activities is that if the data is encrypted and hidden in the header of a protocol, it's hard to detect.

The most useful tool in this cases is a packet filter program like wireshark or tcpdump. There should be an analysis about detecting unusual patterns in the flow of data.

While the port knocking is a clever idea, if the Security Administrator has a suspicion, he/she could detect after some work the presence of one of these backdoors by checking the repeats of the port knocking.

Additionally, we can also use system monitoring tools to analyze any anomaly, some of these backdoors don't care about being detected so an unusual name would be noticeable. If not noticeable, then the amount of memory percentage or RAM used is a good indicator about a program that is using more resources than needed.

If there is an anomalous program in the computer, we can also analyze it with tools like OllyDbg and get a sense of what does this anomaly do.

If the firewall is compromised, we could always try to get the current firewall with iptables and check if there is no change,