Matt Valentini

Honeypot Project 10/20 - 10/24 2021

**Table of Contents**

Introduction

Project setup

Attacker Location

Attacks observed

Overview

**Introduction**

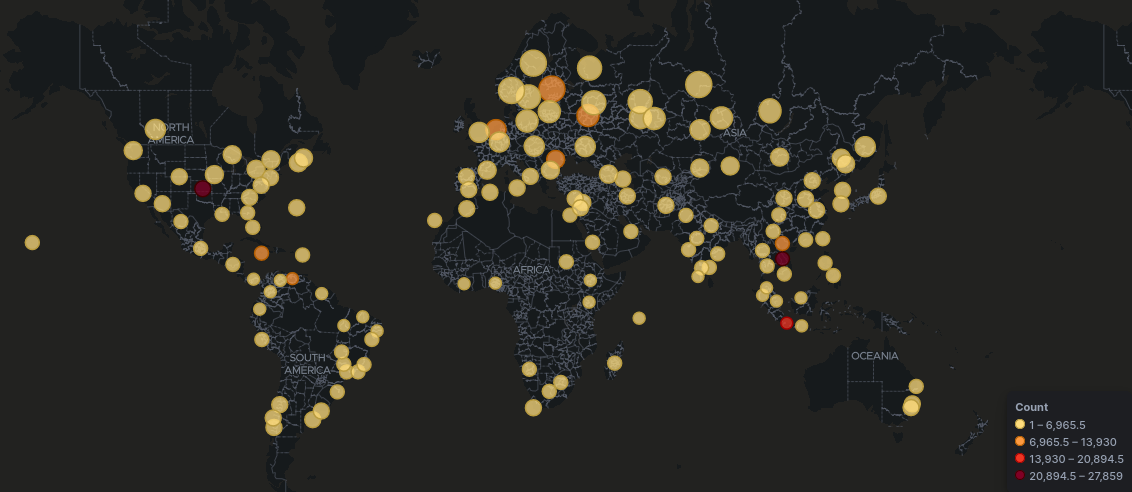
In this project, I will be setting up a “honeypot”, or a system left intentionally vulnerable to capture information about incoming attacks. This project was conducted to observe current attacks to learn the methods that an attack might use today. From the findings, we may want to research the way that the attack works, what programs or functions it is abusing, and how we may set up our network or machine to prevent these vulnerabilities.

**Project Setup**

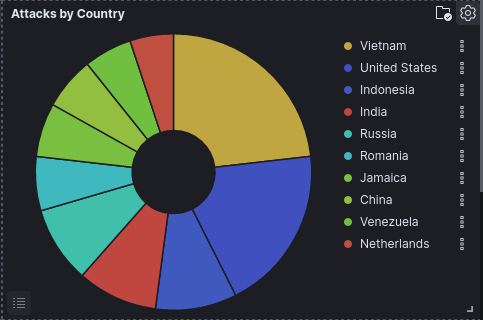
For this project, I used T-Pot, which is a tool that helps set up several honeypots for me to observe. I used AWS to spin up a virtual machine in California using Debian 10 Linux, installed the T-Pot framework, and began observing as many different attacks began to be deployed on my honeypots. This project took place from October 20th at 4:30 pm to October 24 at 6:00 pm.

**Attacker Location**

First, I wanted to learn where the attacks are coming from. I chose to launch my honeypots in California, and attack location may differ from location to location. Using Kibana, I was able to see a heat map of attack origin locations.



Above, you can see my global map, and not only where the attacks are coming from, but what locations are performing many attacks. As you can see, the two locations with the highest volume of attacks are Reno County, Kansas, USA and Thapangthong District, Laos.

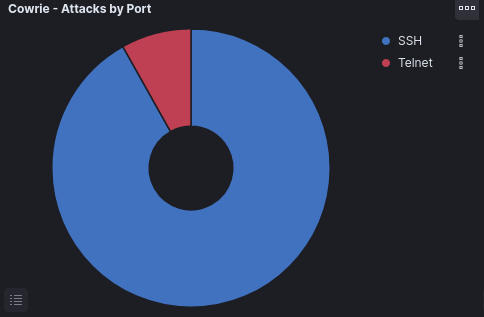


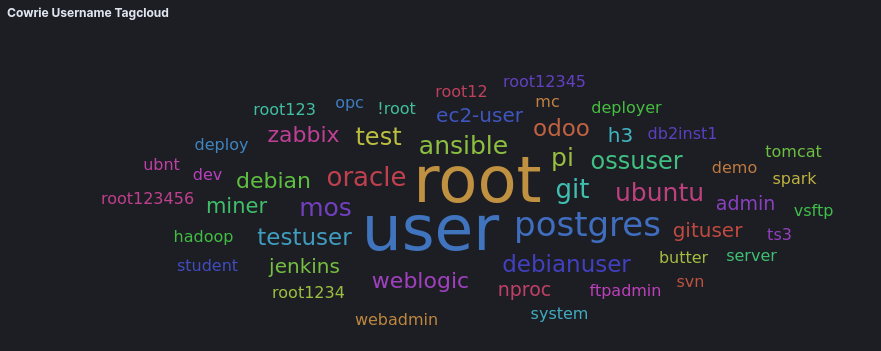
This pie chart shows the percentage of attacks from each country. While this chart says Vietnam, the coordinates given say these attacks are from Laos. It is unclear which country these attacks are actually originating, though the approximate location is somewhere near the border of the two countries.

**Attacks Observed**

Let’s observe the attacks that the machines are receiving. I have decided to look at each honeypot individually, as each honeypot has a specific vulnerability/vulnerabilities that it is targeted toward. For this report, I want to focus on the honeypot “Cowrie”.

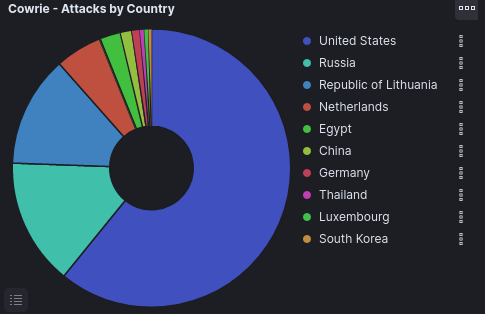
This Honeypot had lots of interaction, especially with the ssh and telnet ports. There were also many usernames and passwords that were attempted and stored in the database.







These tagclouds show the usernames and passwords attempted to login via ssh and telnet. Due to root and user being the most popular username attempted, and 123456, root, 1 and other common passwords being the most popular password attempted, we can assume that this honeypot is being “brute-forced”. This is when an attacker tries common usernames and passwords to attempt to login.



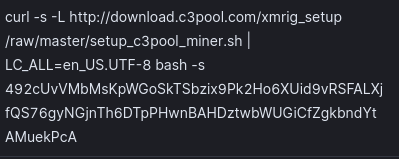
Most of these attacks came from the United States.

Another interesting command that was run on this machine was the following:



Breaking this command up, the hive-passwd command is attempting to change the password for the machine. This would allow the attacker to know the password, but also would lock the actual user out of their machine. Next, the attacker runs two pkill commands. These are both to attempt to turn off the machine. This way, if successful, the real user of the machine would not be able to login back into the machine. Lastly, as a fail safe, the uname -a command is attempting to find the command that does turn the machine off, if the previous two commands do not work.

Lastly, I want to look at the following command:



The command curl allows the user here to download something from a given url. After doing research on this command, I found that this command is trying to convert this honeypot into a crypto miner for a currency called Monero.

**Summary**

This project was an opportunity to witness firsthand the types of attacks that are deployed in the real world, how I might defend against them, and just how fast these attacks happen. Within the 4 day period, a total of 187,000+ attacks were deployed on my honeypots. This demonstrates how important it is to have a secure network, or almost instantly, an automated attack will exploit your network.