Using Honeypot Data to Detect Adversarial Tactic, Technique, and Procedure Changes based on Victim Geolocation

Abstract

The financial and national security impacts of cybercrime globally are well documented. According to the 2021 FBI Internet Crime Report, financially motivated threat actors committed 86% of reported breaches, resulting in a total loss of approximately $4.1 billion in the United States alone. Firms can use cyber threat intelligence to help lessen the impact of threat actor activity. Our study seeks to determine if threat actors change their tactics, techniques, and procedures (TTPs) based on the geolocation of their target's IP address. To answer this research question, we deployed identically configured honeypots on multiple continents to collect attack data from geographically separate locations concurrently. This approach allowed us to aggregate log data about attacks against specific services commonly targeted by threat actors.