Honeypot Configuration and Data Analysis

Jared Campbell & David Zehden
The University of Texas at Austin

Main Objectives

1. Setup Amazon Web Services EC2 instance
2. Explore Honeypot options
3. Deploy Honeypot of choice on AWS
4. Configure Honeypot as needed
5. Collect data over time
6. Explore collected data to determine trends

Honeypot Use Cases

- Defending an Enterprise Network
  - Analyze trends in attacks against an organization's network
  - Slow down attackers by allowing them to target a honeypot instead of critical infrastructure
- Information Security Research
  - Gather data on attack trends across the internet
  - Discover potential zero-day attacks

Results

Our honeypot made over 20,000 detections. We received traffic from all over the world, as you can see in Figure 2. In order to generate this map, we took all the IPs we detected and used the PyGeoIpMap library.

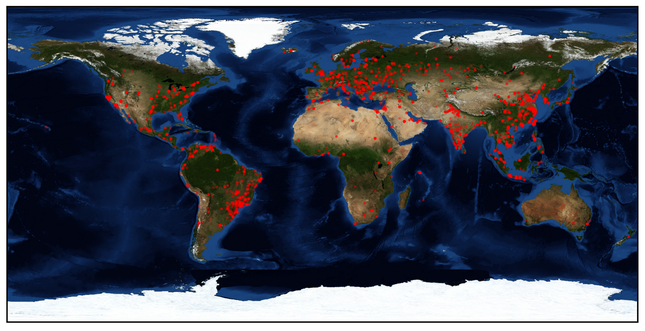

Figure 1: Approximate Locations of Detected IP Addresses

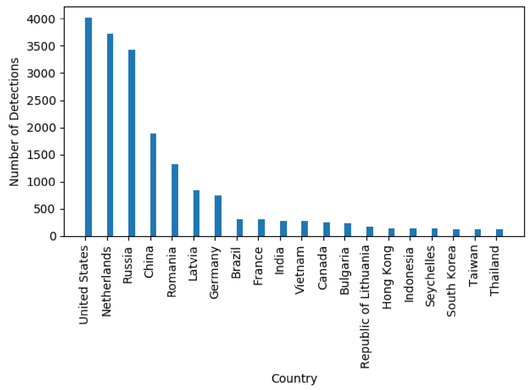

Figure 2: Breakdown of Detections by Country

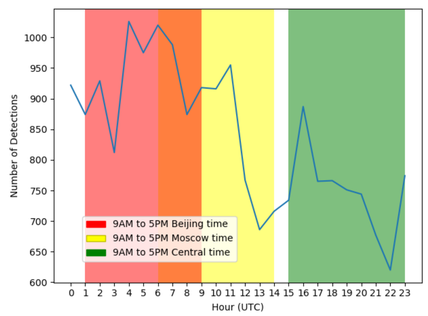

Figure 3: Breakdown of Detections by Time of Day (UTC)

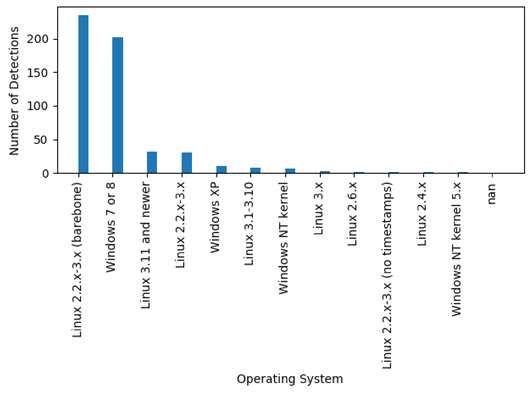

Figure 4: Breakdown of Detected Operating Systems

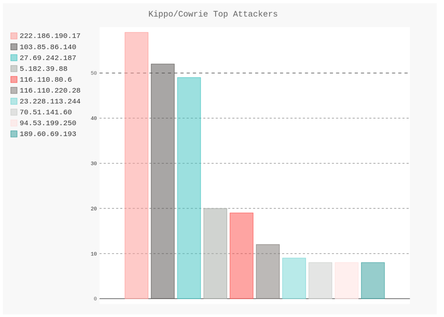

Figure 5: IP Addresses of Top Attackers

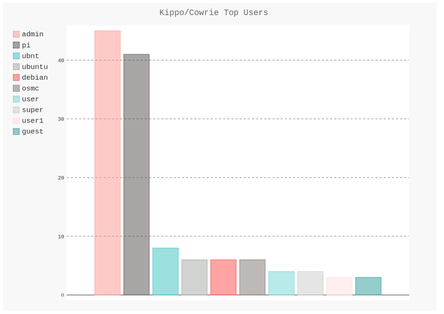

Figure 6: Top Usernames Attempted

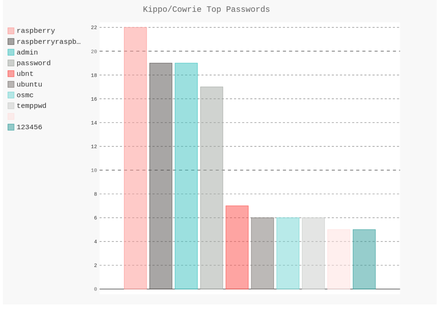

Figure 7: Top Passwords Attempted