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

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.

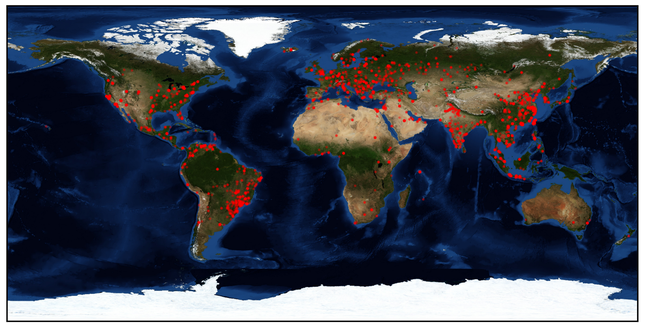

Figure 1: Approximate Locations of Detected IP Addresses

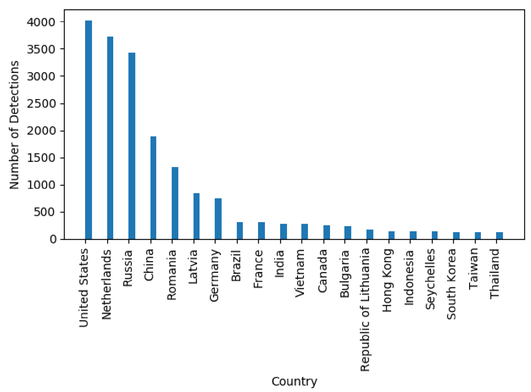

Figure 2: Breakdown of Detections by Country

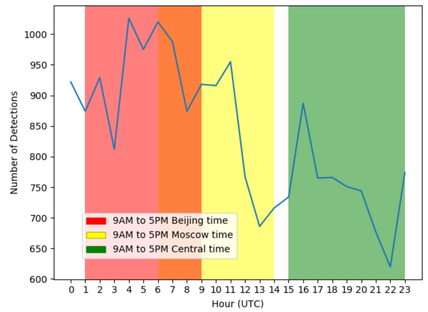

Figure 3: Breakdown of Detections by Time of Day (UTC)

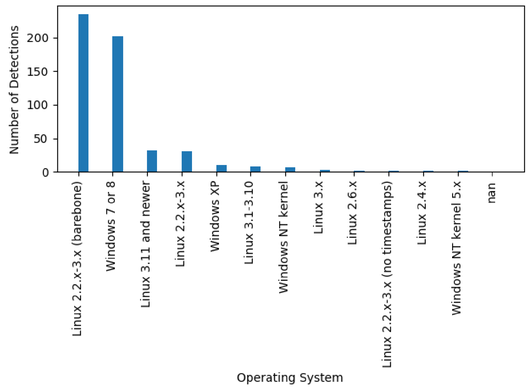

Figure 4: Breakdown of Detected Operating Systems

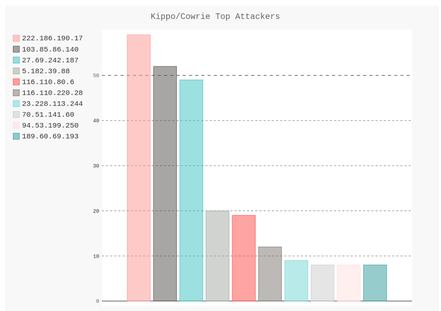

Figure 5: IP Addresses of Top Attackers

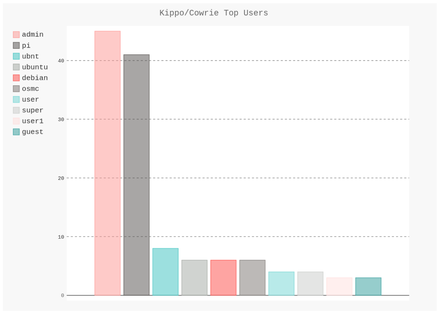

Figure 6: Top Usernames Attempted

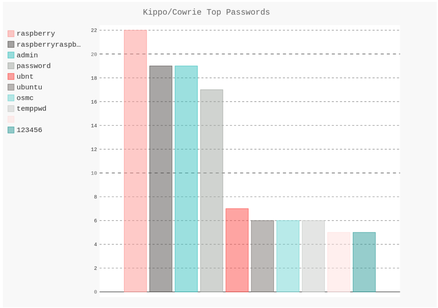

Figure 7: Top Passwords Attempted

Conclusion

In order to research the effectiveness of honeypots, we implemented and configured our own honeypot on an AWS server. Our honeypot network collected even more data than we expected over the course of a single week. We have analyzed the data collected by our honeypot network to find trends in the origin of attacks, the hardware used for attacks, which services are most heavily targeted, and more.

We have also seen that different honeypot solutions offer both various types of data and different quantities of data. From our findings, we could see that Snort was was able to capture a massive volume of information, but it was data that was generally more surface level. In contrast, Dionaea could provide examples of malware binaries that attackers attempted to run. However, this happened very infrequently, so it ultimately did not provide a great deal of data.

Our research has demonstrated that honeypots are an effective tool for monitoring malicious activity on a network. Our research also shows that honeypots can collect large amounts of data on many different types of trends. The data collected by a honeypot can be tailored to suit any organizations specific needs, making honeypots an effective tool not only for research, but also for securing enterprise environments.