Honeypot Threat Intelligence Report (AWS, Sep 11–13, 2025)

Executive Summary

Between **September 11, 2025 @ 18:28** and **September 13, 2025 @ 13:47** (Pakistan Standard Time), a Heralding honeypot was deployed on AWS to attract and record malicious activity. Over a span of just **2.5 days**, the honeypot registered **15,696 connection attempts**, exposing the scale, persistence, and automation behind global cyberattacks.

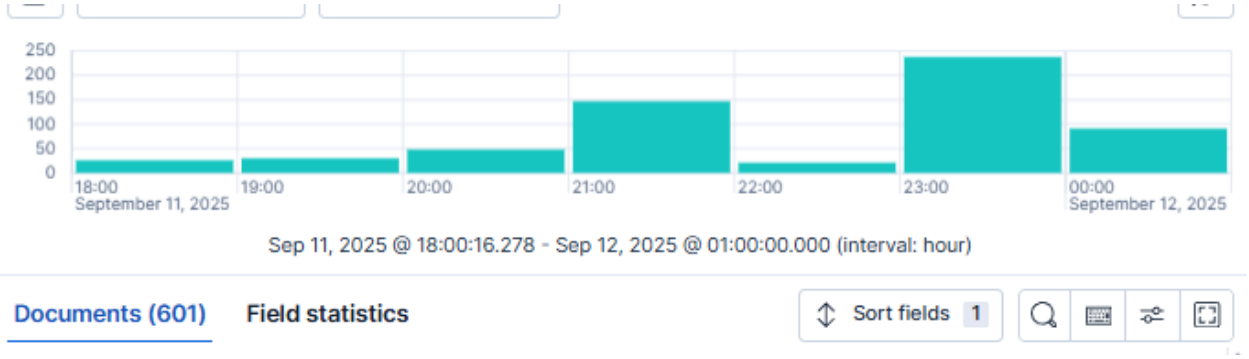
All logs, raw session data, and supporting files from this experiment have been uploaded to a dedicated [GitHub repository] for reference and further analysis.

This report details the timeline of activity, attack distribution, common credential attempts, and key insights gathered from the deployment. The findings reinforce the critical need for proactive defense strategies when managing exposed services.

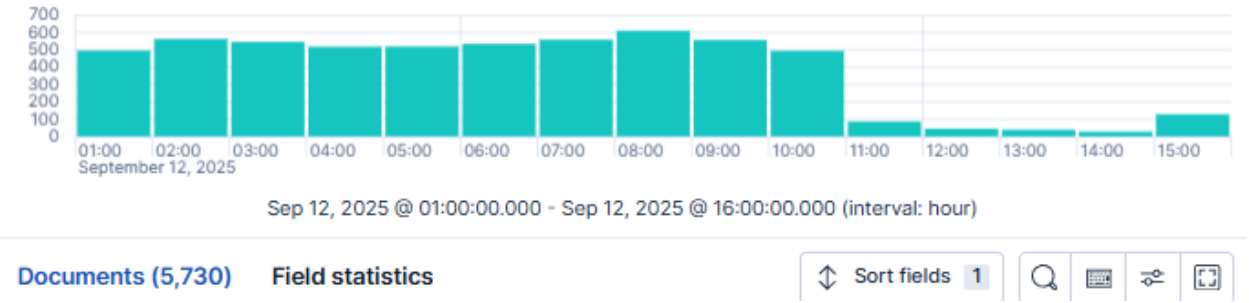
Timeline of Attack Activity

Breaking down the experiment into three distinct time windows shows how attacks evolved:

- **Sep 11, 2025 @ 18:00 → Sep 12, 2025 @ 01:00 (PKT)**
  Connections: 601
  → Initial reconnaissance phase with relatively low activity.



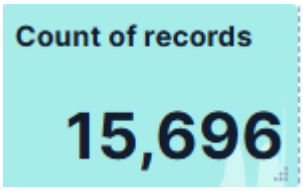
- **Sep 12, 2025 @ 01:00 → Sep 12, 2025 @ 16:00 (PKT)**
  Connections: 5,730



  → Major surge of brute-force attempts, especially targeting SSH.

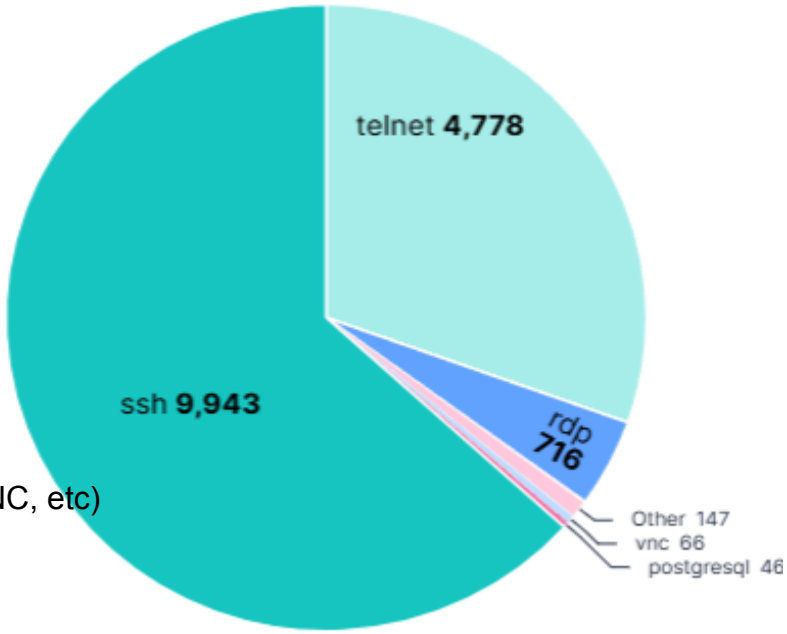
- **Sep 12, 2025 @ 16:00 → Sep 13, 2025 @ 14:00 (PKT)**
  Connections: 9,365
  → Peak attack activity, with botnets intensifying scans and login attempts.

Total Connections: 15,696 across the observation period.



Attack Distribution

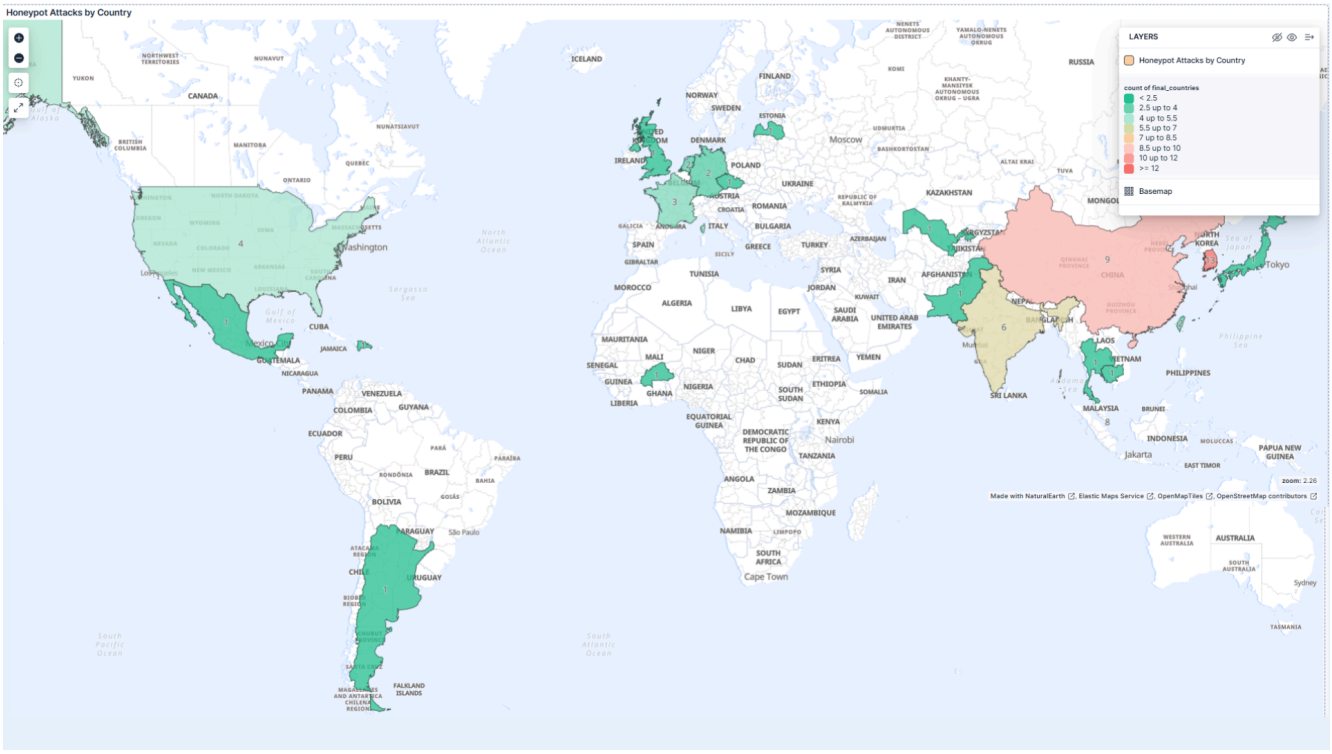
Targeted Ports



- **SSH (22):** 9,943 attempts
- **Telnet (23):** 4778, second only to SSH
- **RDP (3389):** 716 attempts
- Other services (SMTP, IMAP, FTP, POP3, VNC, etc) were probed but saw relatively lower volumes.

Geographic Origins

- **China:** 10,623 attacks (≈68%)
- **Japan:** 2,606 attacks
- **India:** 580 attacks
- **France:** 296 attacks
- **Singapore:** 240 attacks
- **Other countries combined:** remainder of attempts



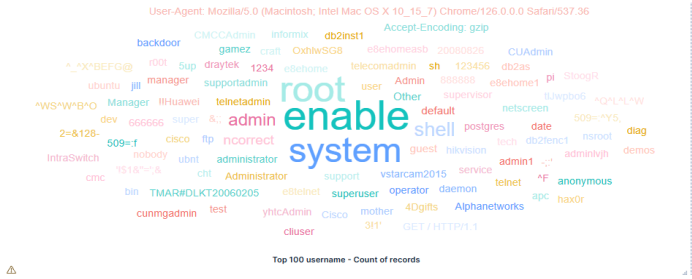
This distribution highlights how attacks are often concentrated in a few regions, but globally dispersed.

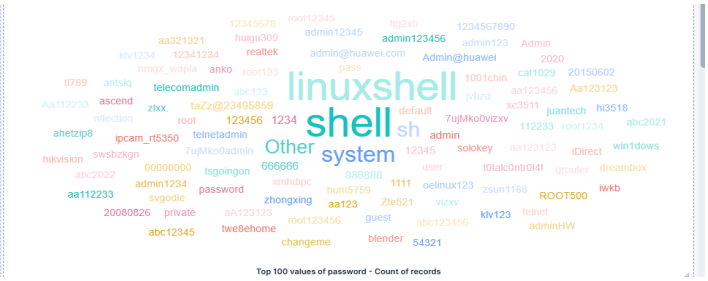
Credential Attacks

The honeypot captured thousands of login attempts using weak or default credentials. Many reflect automated botnets testing known vendor defaults.

- **Most Frequent Usernames:**
  `system`, `enable`, `root`, `admin`, `administrator`, `postgres`, `telnetadmin`, `daemon`, `supportadmin`, `superuser`, etc.
- **Most Frequent Passwords:**
  `linuxshell`, `shell`, `system`, `123456`, `1234`, `888888`, `666666`, `default`, `root123`, `telnetadmin`, etc.

Visual analysis of login attempts:





These word clouds reveal how attackers repeatedly cycle through common defaults and trivial variations.

Key Insights

1. **SSH as the Prime Target:** Nearly two-thirds of all attacks focused on SSH, confirming its status as the most abused entry point.
2. **Global but Uneven Distribution:** While attacks originated worldwide, the majority came from just a handful of countries.
3. **Automated Brute Force Dominance:** The reliance on default and weak credentials shows these were primarily bot-driven campaigns, not manual attempts.
4. **Escalating Threat Over Time:** The longer the honeypot stayed online, the more it was discovered and hammered, with the final window showing exponential growth.

Recommendations

- **Never expose critical services (SSH, RDP, Telnet) directly to the internet**. If exposure is unavoidable, enforce strict rate-limiting and IP restrictions.
- **Use key-based authentication and MFA** wherever possible. Disable password login for SSH entirely.
- **Remove or rename default accounts** (e.g., `admin`, `root`) to reduce the attack surface.
- **Apply geofencing and anomaly detection** to cut down on noise from high-volume attacker regions.
- **Deploy honeypots strategically** as part of a defense-in-depth approach, turning attacker activity into actionable threat intelligence.

Conclusion

This honeypot experiment demonstrates how quickly attackers swarm to exposed services. Within just 2.5 days, the honeypot attracted nearly **16,000 connections** — the vast majority consisting of automated brute-force attempts using recycled default credentials.

The findings stress the importance of **secure configurations, proactive monitoring, and layered defenses**. By studying real-world adversary behavior through honeypots, organizations gain not only early-warning data but also practical lessons in strengthening their security posture.

Github: https://github.com/muzi5622/Honeypot-Threat-Intelligence-Report

Linkedin: https://www.linkedin.com/in/m-muzammal-99m/