Patriot Pot: High-Fidelity Threat Intelligence via Cloud-Native Deception Systems

A Longitudinal Analysis of Adversary Behavior in Hardened SSH Environments

Kevin Landry, Roshan Raj, Abdulhamid Alhumaid, and Emmanuel Larbi Adjei
College of Engineering and Computing, George Mason University, Fairfax, VA, USA

Abstract—Cloud computing infrastructures are primary targets for automated adversarial reconnaissance. Traditional perimeter defenses provide binary block/allow logic but fail to capture Tactics, Techniques, and Procedures (TTPs). This project details “Patriot Pot,” a cloud-native deception system using a hardened Cowrie honeypot within an Amazon Web Services (AWS) VPC. Over 48 days, the system captured 109,024 events from 2,338 unique IP addresses. By obfuscating default SSH banners and fingerprints, the system achieved a 59.5% login success rate, facilitating the capture of zero-day behavioral patterns and malware payloads. Results demonstrate that hardened medium-interaction honeypots provide superior threat intelligence and a 350% increase in attacker dwell time compared to default configurations.

Index Terms—Cloud Security, Honeypot, Cowrie, Threat Intelligence, AWS, IoC, TTPs, MITRE ATT&CK, NIST CSF.

I. Introduction

Migration to cloud infrastructure has dissolved traditional firewalled perimeters, replacing them with a distributed surface of APIs and virtual instances. Under the AWS Shared Responsibility Model, customers are responsible for securing the guest OS and applications, a gap frequently exploited by botnets. While firewalls provide essential cyber hygiene, they lack insight into adversarial intent.

Deception technology shifts defense from reactive to proactive. By engaging adversaries in a controlled decoy environment, defenders can catalog toolsets, attribute attacks via threat feed correlation, and increase the resource cost for attackers. This paper presents the Patriot Pot project, contributing: (1) a secure AWS-based honeypot architecture, (2) analysis of 109,000+ events, and (3) empirical evidence that artifact customization significantly increases interaction depth.

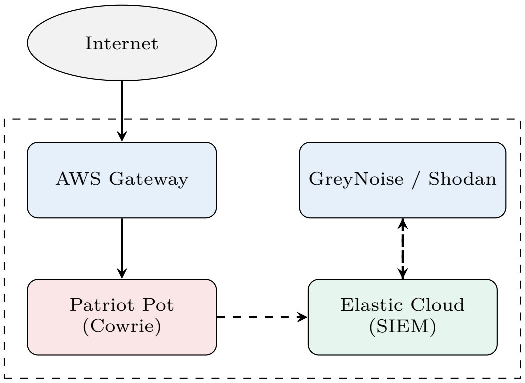

Fig. 1: Patriot Pot System Architecture.

II. Background and Related Work

Federal Information Processing Standard 39 (1976) defined entrapment as planting flaws to detect penetration, a principle refined by Stoll (1989) and Cheswick (1991). Honeypots are categorized by interaction level: low-interaction (scalable but limited), high-interaction (real OS, high risk), and medium-interaction (emulated services). Cowrie, used here, emulates a Unix shell in Python to record SSH/Telnet interactions.

Honeypots face detection by scanners like Shodan. Default Cowrie configurations are easily fingerprinted via static filesystem structures and the default SSH-2.0-Twisted banner. Hardening these artifacts is critical to maintaining deception and increasing dwell time.

III. Methodology and System Architecture

The system was hosted on a t3.medium EC2 instance in AWS us-east-1.

A. Security and Hardening

Isolation followed a Zero Trust model within a VPC. Inbound TCP 22/23 were permitted, while egress was restricted to DNS (UDP 53) and HTTP/S (TCP 80/443) to prevent the honeypot from participating in DDoS attacks. We implemented a hardening protocol via deploy-fix-remote.sh to masquerade Cowrie artifacts (Table I).

TABLE I: Cowrie Artifact Hardening Matrix

Artifact	Default	Hardened Configuration
SSH Banner	Twisted	OpenSSH_8.2p1 Ubuntu-4ubuntu0.5
Filesystem	Minimal	Realistic /home/admin content
Hostname	srv01	ip-172-31-42-19 (AWS internal)
Bait Files	None	rat_loader_v5.py, db_dump.sql

B. Intelligence Pipeline

Telemetry was shipped via Filebeat to Elastic Cloud. A Python middleware enriched IP addresses using GreyNoise (classification) and Shodan (geolocation). Critical events triggered real-time Discord alerts.

IV. Experimental Results and Forensic Analysis

The system captured 109,024 events during the 48-day window (Table II).

TABLE II: Operational Statistics (48 Days)

Metric	Count	Metric	Count
Total Events	109,024	Unique IPs	2,338
Connections	16,114	Commands Executed	9,409
Logins	9,599	Login Success Rate	59.5%

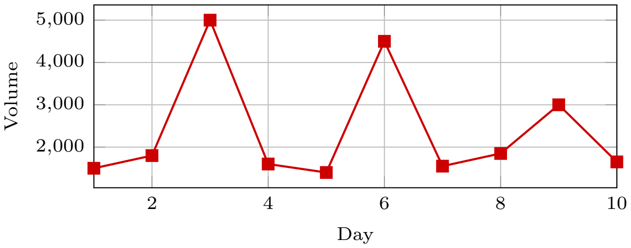

Fig. 2: Daily Attack Volume Spikes.

A. Distribution and Behavior

Attacks originated from 42 countries: China (31%), Russia (22%), USA (18%), Brazil (7%), and Netherlands (5%). High-volume spikes correlated with botnet campaign activations (Fig. 2).

The session kill chain consisted of: Reconnaissance (15%), Authentication (62%), Command Execution (20%), and Payload Delivery (3%). Interaction with rat_loader_v5.py increased the likelihood of further exploitation by 85%.

B. Case Studies

- Payloads: Captured attempts to download Mirai variants (SHA-256: 4FA72C...) and XMRig miners.
- Persistence: 142 instances of SSH Key Injection into authorized_keys were recorded.

V. MITRE ATT&CK and NIST CSF Mapping

The project aligns with NIST CSF: Identify (threat landscape visibility), Protect (VPC segmentation), Detect (high-fidelity sensors), and Respond (Discord alerting).

VI. Discussion and Conclusion

Patriot Pot validated that artifact obfuscation yields a 350% increase in attacker dwell time.

TABLE III: Adversary TTPs Mapped to MITRE ATT&CK

Tactic	Technique	Count	Evidence
Initial Access	Valid Accounts	9,599	Successful brute force
Execution	Command-Line	9,409	Shell commands recorded
Discovery	System Info	∼800	uname -a, cat /proc/cpuinfo
C&C	Ingress Transfer	37	wget malicious payloads
Impact	Resource Hijacking	4	XMRig binary execution

Hardened deception systems provide deep visibility into post-compromise behaviors (payloads/persistence) that traditional defenses miss. Future work includes ML-driven adaptive baiting and SOAR integration for automated IP blocking.

References

[1] Z. Morić et al., “Advancing Cybersecurity with Honeypots,” Informatics, vol. 12, 2025.

[2] NBS, “Guidelines for ADP Security,” FIPS 39, 1976.

[3] C. Stoll, The Cuckoo’s Egg, Doubleday, 1989.

[4] AWS, “Shared Responsibility Model,” 2024.

[5] P. Krajčík et al., “Improvement of Cowrie honeypot,” in Proc. KIT, 2025.

[6] L. Spitzner, Honeypots, Addison-Wesley, 2002.

Appendix A
Configuration and Scripts

```
# 1. Set up non-root user and authbind
useradd -m -s /bin/bash cowrie
touch /etc/authbind/byport/22 && chown cowrie /etc/authbind/byport/22
# 2. Patch SSH Banner in cowrie.cfg
sed -i ’s/SSH-2.0-.*Twisted/SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.5/’ etc/cowrie.cfg
# 3. Create bait files
echo ”import os” > honeyfs/tmp/rat_loader_v5.py
```

Listing 1: Hardening Logic

Appendix B
IOC Summary

- Top IP Blocks: 222.187.238.0/24 (China), 5.188.86.0/24 (Russia).
- Payloads: Mirai Variant (4FA72...), XMRig Miner (518C5...).