Honeypot Analysis

Prepared by: Samyukthan Ananth
Period covered: Jun 11, 2025 - Jun 13, 2025

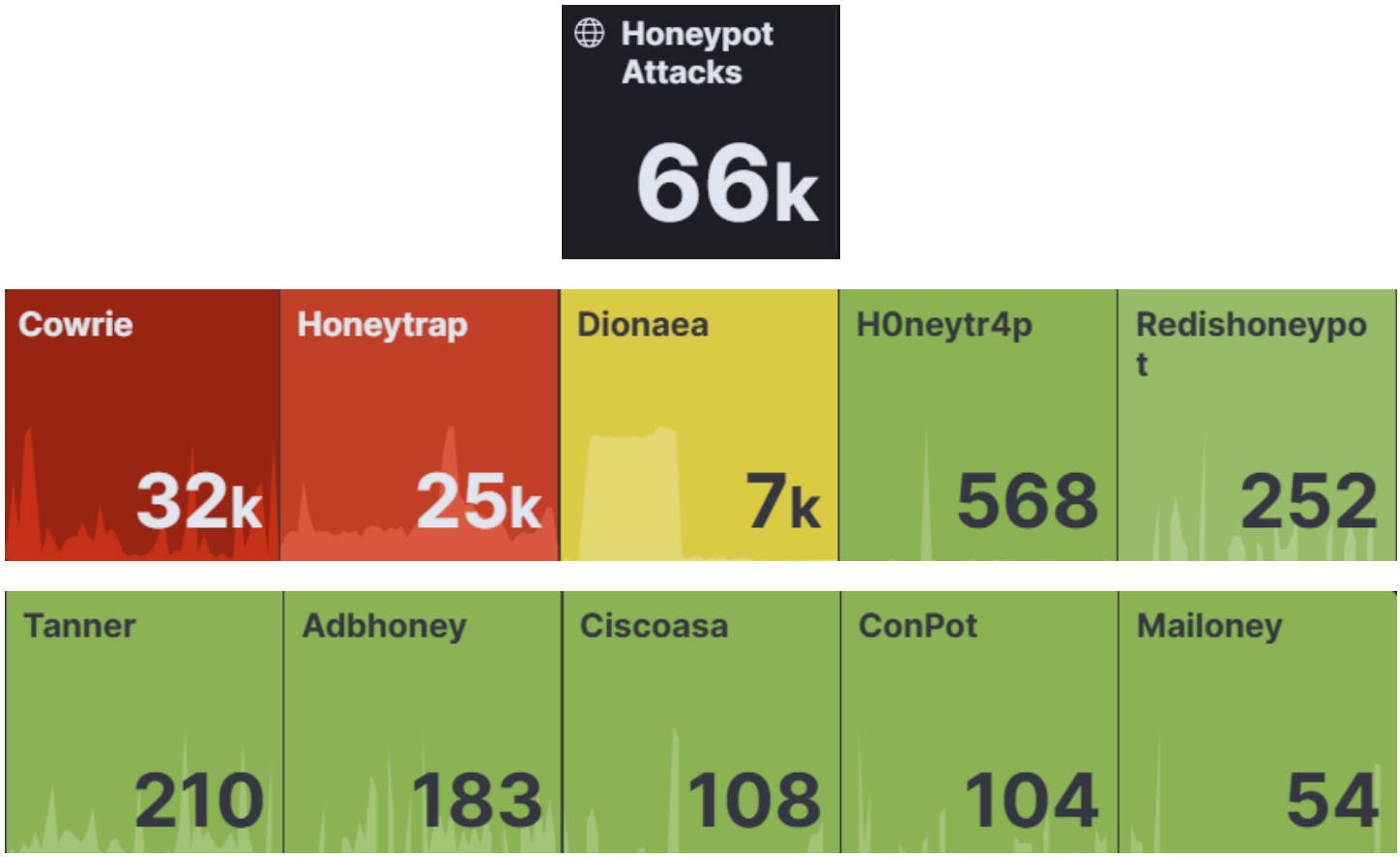
Introduction

This report details the deployment and initial findings of a honeypot system established to capture and analyze malicious network activity. Utilizing T-Pot, a comprehensive honeypot platform, the system was deployed on a Google Cloud instance running Ubuntu 24.04 LTS. Configured with 15 GB of RAM and 4 CPU cores, the honeypot was active for 24 hours, during which it recorded approximately 66,000 attack attempts. This report outlines the setup, configuration, and key observations from the collected data.

System Configuration

- **Platform**: Google Cloud
- **Operating System**: Ubuntu 24.04 LTS
- **Region Deployed**: us-west1-c
- **Honeypot Software**: T-Pot
- **Hardware Specifications**:
  - RAM: 15 GB
  - vCPUs: 4
  - n1-standard-4
  - Intel Broadwell x86/64
  - Ports Allowed: All
- **Deployment Duration**: 24 hours
- **Total Attacks Recorded**: ~66,000
- **Top Attack by Country:** USA
- **Most attacked Port:** 22 and 21

Attack Overview



Quick Numbers

92%

Known Attacker

79%

Linux Attacker

16k

Attacks from USA servers

65%

Attacks on Port 22

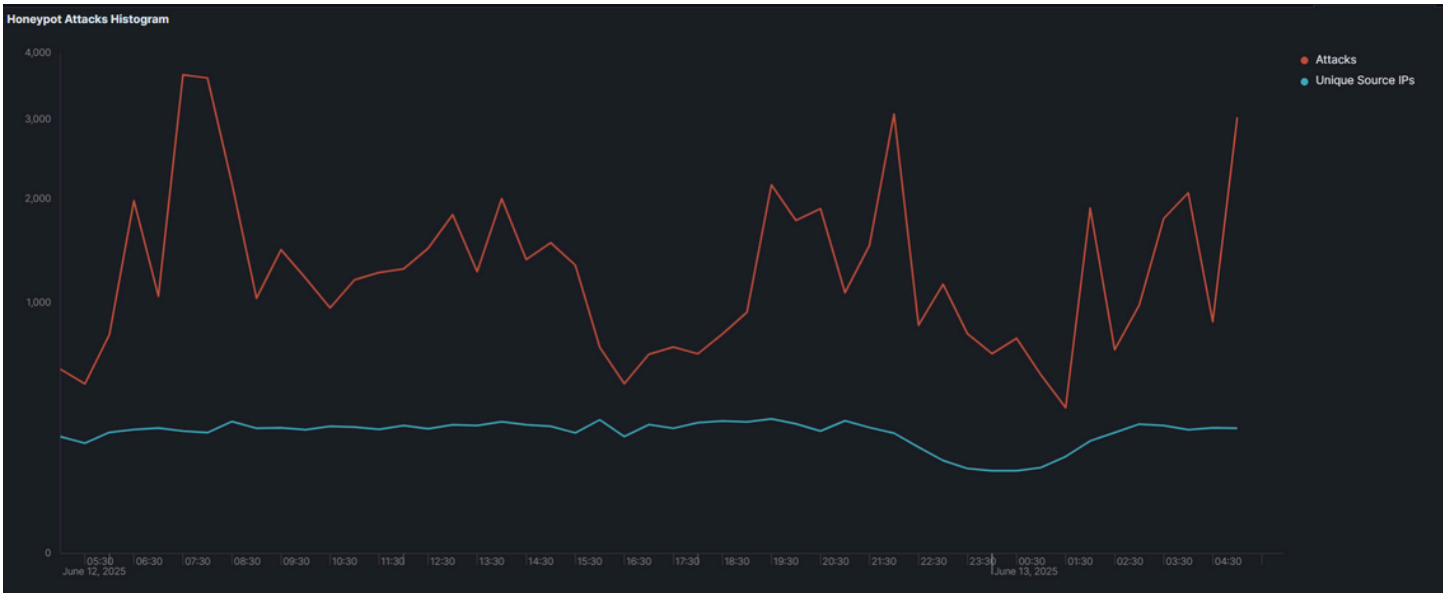
Root

Most Tagged Username

'123456'

Most Tagged Password

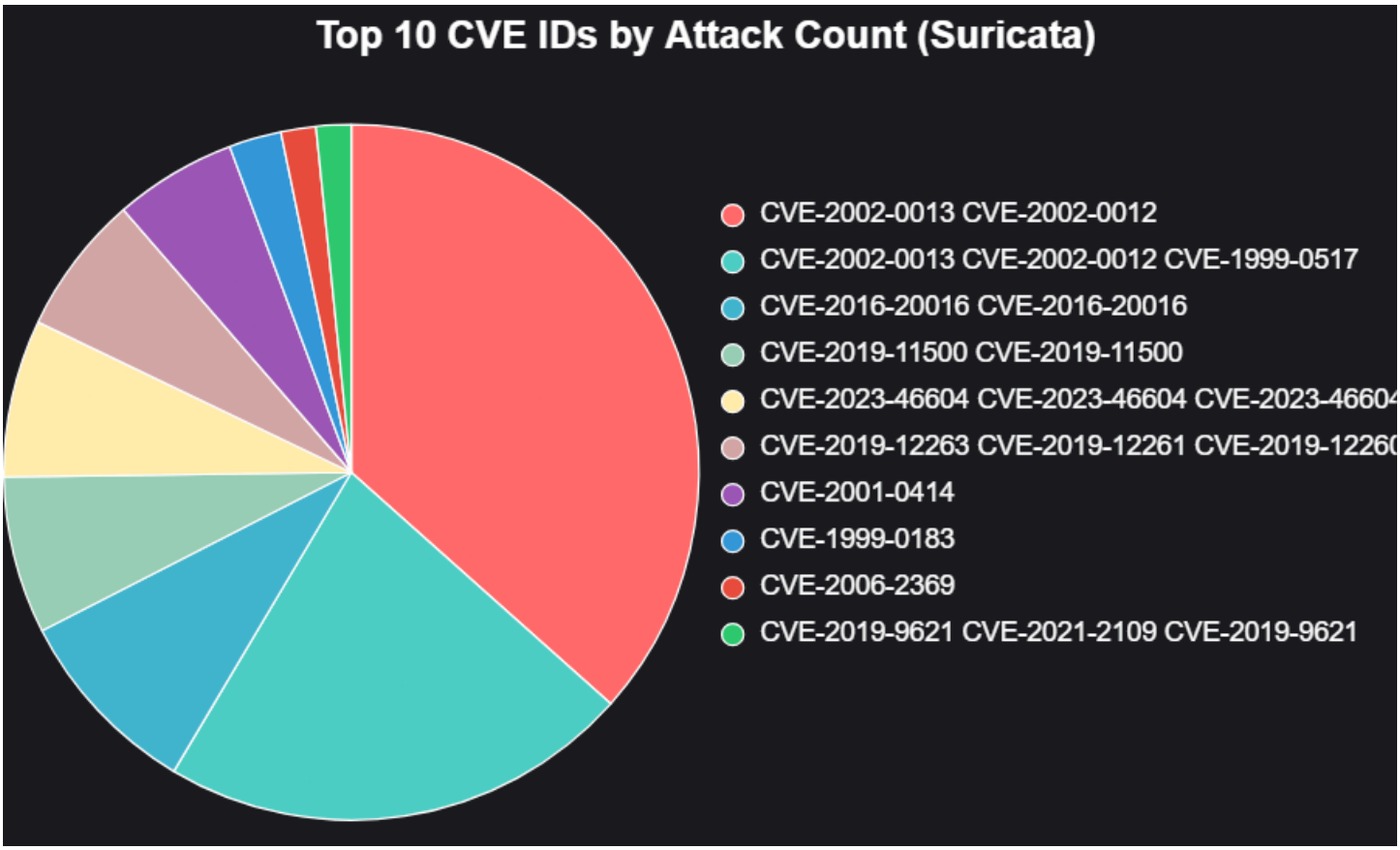
Attack Histogram



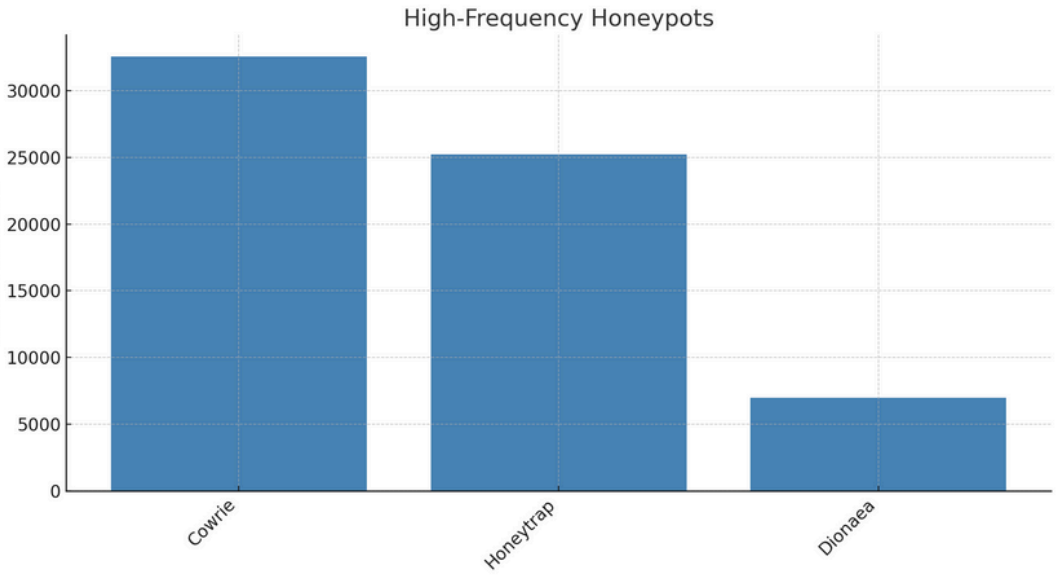
Unique Attackers IP: 11325

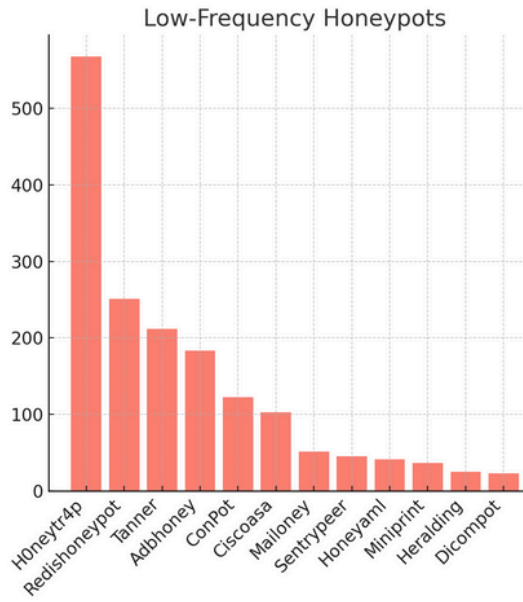
Over All Attack: 66186

CVE Pie Chart



Honeypot Attack Bar



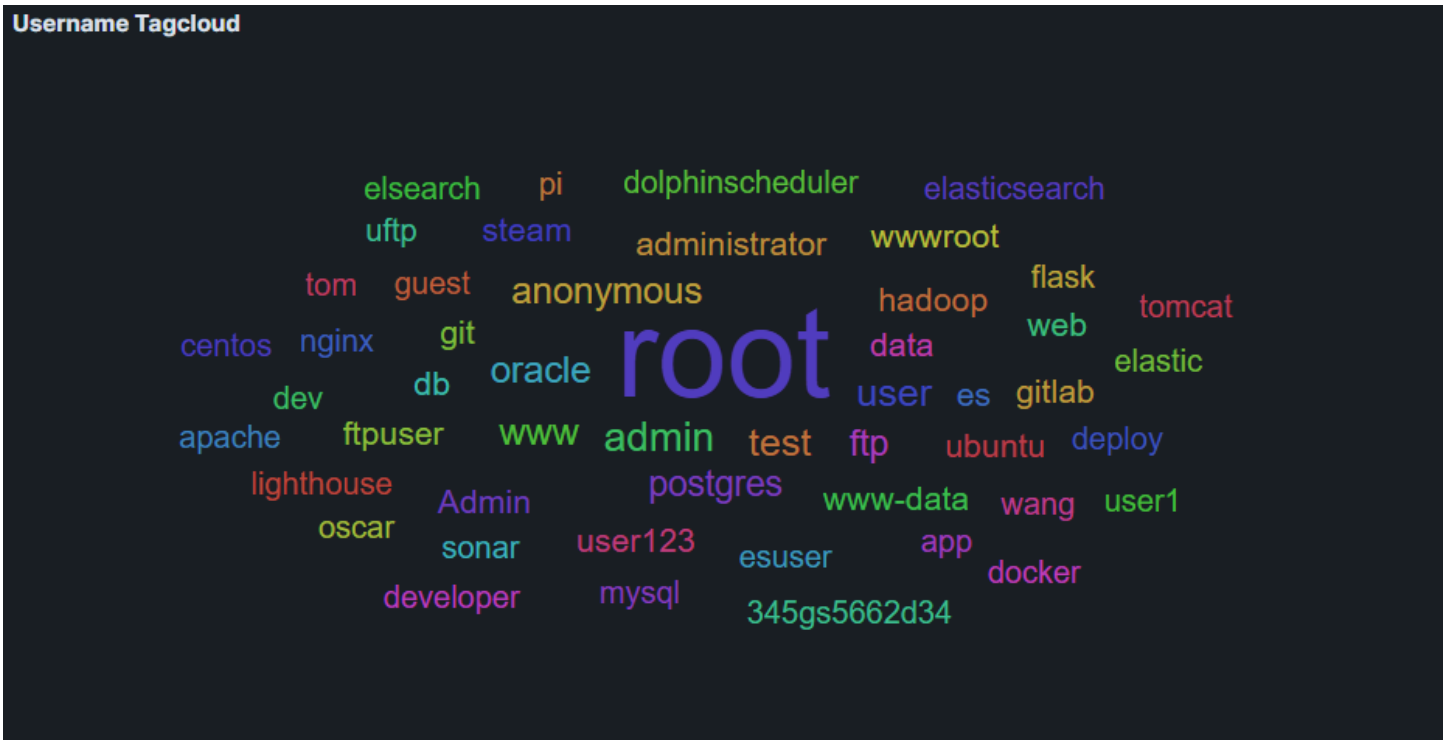


Suricate Alert Signature - Top 10

ID	Description	Count
2200003	SURICATA IPv4 truncated packet	33,632
2210048	SURICATA STREAM reassembly sequence GAP	3,989
2402000	ET DROP Dshield Block Listed Source group 1	3,137
2228001	SURICATA STREAM spurious retransmission	1,592
2228000	SURICATA SSH invalid banner	1,597
2024766	ET EXPLOIT [PTsecurity] DoublePulsar Backdoor installation communication	1,096
2260001	SURICATA Applayer Detect protocol only one direction	988
2010735	ET FTP FTP PWD command attempt without login	978
2009582	ET SCAN NMAP -sS window 1024	956

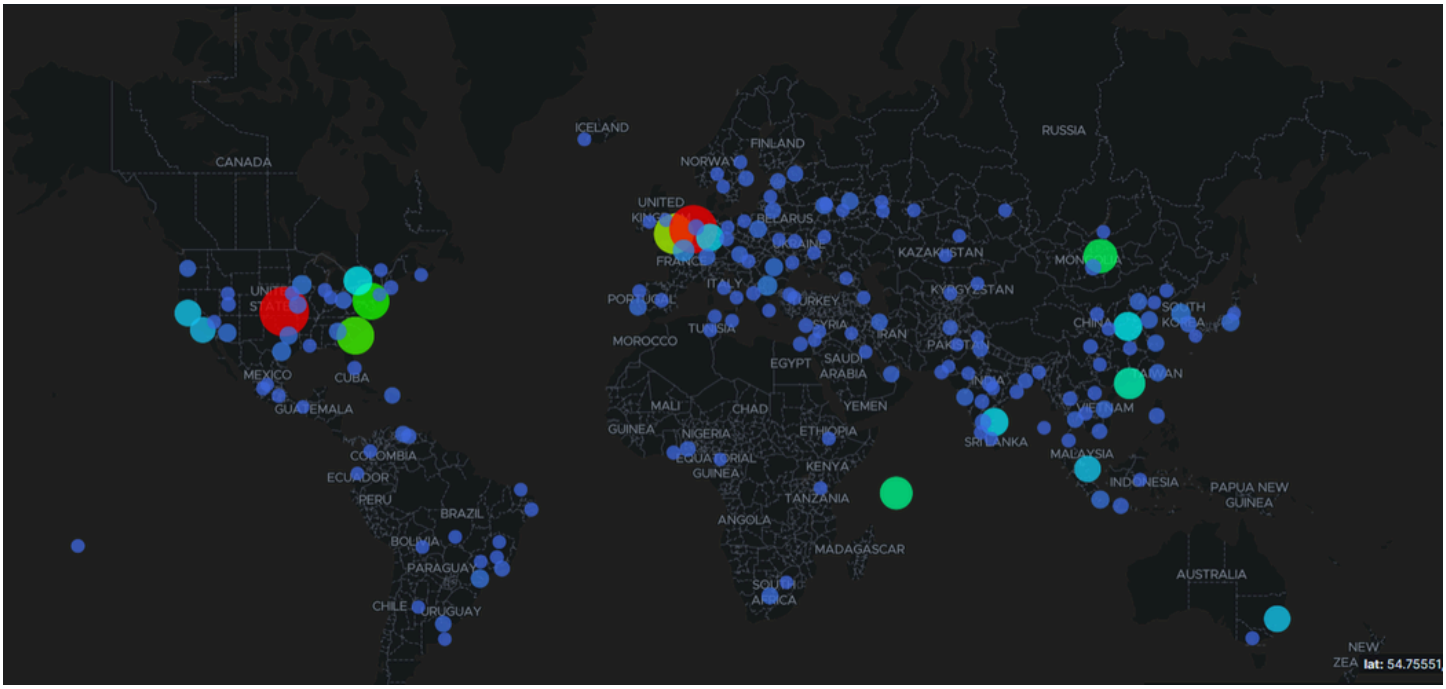
Most Tagged Credentials

Usernames:



Passwords:

Attack Map



Conclusion

The 24-hour deployment of the T-Pot honeypot on a Google Cloud instance running Ubuntu 24.04 LTS with 15 GB RAM and 4 CPU cores provided a comprehensive view of cyber threats, capturing approximately 67,000 attacks. The analysis of this data, including attack sources, honeypot activity, Suricata alerts, CVEs, and credential attempts, reveals several key insights into the threat landscape targeting your setup.

Key Findings:

1. **Attack Sources and Distribution:**
   - The world map and AS/N data show that attacks predominantly originated from cloud and hosting providers in the US, Western Europe, and East Asia. Top Autonomous Systems (AS) included GOOGLE-CLOUD-PLATFORM (8,987 attacks), CHEAPY-HOST (6,582), and Alibaba (6,510), indicating attackers leverage compromised or abused cloud infrastructure for scalability and anonymity. Geographically, the Eastern US, Western Europe (e.g., UK, France), and East Asia (e.g., China, India) were major hubs, aligning with the global distribution of data centers.
2. **Honeypot Activity:**
   - The honeypot attacks bar chart highlights that Cowrie (SSH honeypot) captured the most attacks at 33k, followed by Honeytrap (26k) and Dionaea (7k). This suggests a heavy focus on SSH brute-force attacks and generic network probes, with lesser interest in specialized services like Redis (Redishoneypot, 251 attacks) or industrial control systems (ConPot, 122 attacks). The total of 66k attacks across all honeypots underscores T-Pot's effectiveness in emulating high-value targets.
3. **Attack Techniques and Signatures:**
   - Suricata alerts revealed that the most common issue was "SURICATA IPv4 truncated packet" (33,632 alerts), indicating widespread malformed packets, possibly from scanners or evasion attempts. Other significant alerts included "STREAM reassembly sequence GAP" (3,989) and "ET DROP Dshield Block Listed Source group 1" (3,137), pointing to network anomalies and known

malicious sources. Targeted exploits like “DoublePulsar Backdoor” (1,587) and reconnaissance scans like “NMAP -sS window 1024” (956) were also detected.
    - The CVE data showed a focus on older vulnerabilities, such as CVE-2002-0013 and CVE-2002-0012 (45 attacks combined), often paired with CVE-1999-0517 (27 attacks). This suggests attackers are probing for legacy systems, though more recent CVEs like CVE-2023-46604 (9 attacks) indicate some interest in newer exploits.
4. **Credential Attacks:**
    - The password and username tag clouds confirmed that brute-force attacks targeted default and simple credentials. The most common username was root, paired with passwords like 123456 (most frequent), 111111, and password. Service-specific credentials like postgres, mysql, and hadoop, along with the recurring 345gs5662d34, suggest attackers are targeting databases, big data platforms, and specific devices with default credentials. This aligns with Cowrie’s high attack count and Suricata’s “SSH invalid banner” alert (1,592).

Implications:

- **Prevalence of Automated Attacks:** The dominance of SSH brute-force attempts (Cowrie, 33k) and simple credentials (e.g., root/123456) indicates that automated bots and scripts are a primary threat, likely part of global botnets scanning for vulnerable systems.
- **Cloud Infrastructure Abuse:** The AS/N data and world map highlight that attackers frequently use cloud providers (e.g., Google Cloud, DigitalOcean) to launch attacks, exploiting the scalability and anonymity these platforms offer.
- **Targeted Systems:** Attackers showed interest in databases (e.g., Postgres, MySQL), containerized environments (e.g., Docker), and big data platforms (e.g., Hadoop), as seen in the username/password data and low-volume honeypots like Redishoneypot.
- **Legacy and Modern Threats:** The CVE data reveals a mix of older vulnerabilities (e.g., CVE-2002-0013) and more recent exploits (e.g., CVE-2023-46604), suggesting a broad attack strategy targeting both outdated and current systems.

Recommended Solution:

1. **Strengthen SSH Security:** Given the high volume of SSH attacks, implement stronger authentication (e.g., disable password-based logins, use multi-factor authentication) and monitor for brute-force attempts.
2. **Audit Cloud Instances**: Investigate the sources of attacks from cloud providers, potentially reporting abuse to providers like Google Cloud or DigitalOcean. Secure your own cloud instances to prevent similar abuse.
3. **Patch Legacy Systems:** Address the targeting of older CVEs by patching or retiring legacy systems, and ensure modern systems are updated to mitigate newer exploits like CVE-2023-46604.
4. **Enhance Monitoring:** Focus T-Pot’s monitoring on high-traffic services (e.g., SSH, databases) and expand to include more specialized honeypots for emerging threats (e.g., containerized environments).
5. **Educate on Credential Security:** The use of default credentials like root/123456 underscores the need for better credential management. Enforce complex passwords and change defaults on all systems.

“Anything out there is vulnerable to attack given enough time and resources.

— Kevin Mitnick

Thank You.