

What I Learned While Playing with Honeypots: A Day with T-Pot

Author: Susana Noto

Date: February 25, 2026



Figure 1: Full dashboard by T-Pot from my Honeypot that was up for about 52 minutes.

1. EXECUTIVE SUMMARY

The Objective: During an informational interview recently, we discussed Honeypots and their application in the cybersecurity workforce. Having never encountered one in my academic studies, I decided to make a simple Honeypot using T-Pot and Microsoft Azure.

Key Discovery: Over a period of about 52 minutes, my honeypot received 659 hits- averaging more than 12 attacks per minute from at least 10 different countries. Additionally, credential analysis showed the use of “orangepi” during attacks.

2. THE METHODOLOGY

2.1 Infrastructure & Environment

To observe real-world attacker behavior, I deployed a high-interaction honeypot environment using the T-Pot (Telekom Security) ecosystem. I followed a guide on CyberNow¹ that walks through how to set up a simple Honeypot using a Microsoft Azure Virtual Machine with all its ports open using a Network Security Group to allow all inbound traffic on ports 0-65535.

2.2 The Monitoring Stack

The system (T-Pot) utilized the **ELK Stack (Elasticsearch, Logstash, Kibana)** to aggregate data from multiple decoys:

- **Cowrie:** For capturing SSH and Telnet interactions.
 - **Honeytrap:** Used as the primary "catch-all" for the wide port range.
 - **Suricata:** Acting as the Intrusion Detection System (IDS) to identify specific exploit signatures.
-

3. DATA VISUALIZATION & GLOBAL ANALYSIS

3.1 Geographic Origin of Attacks

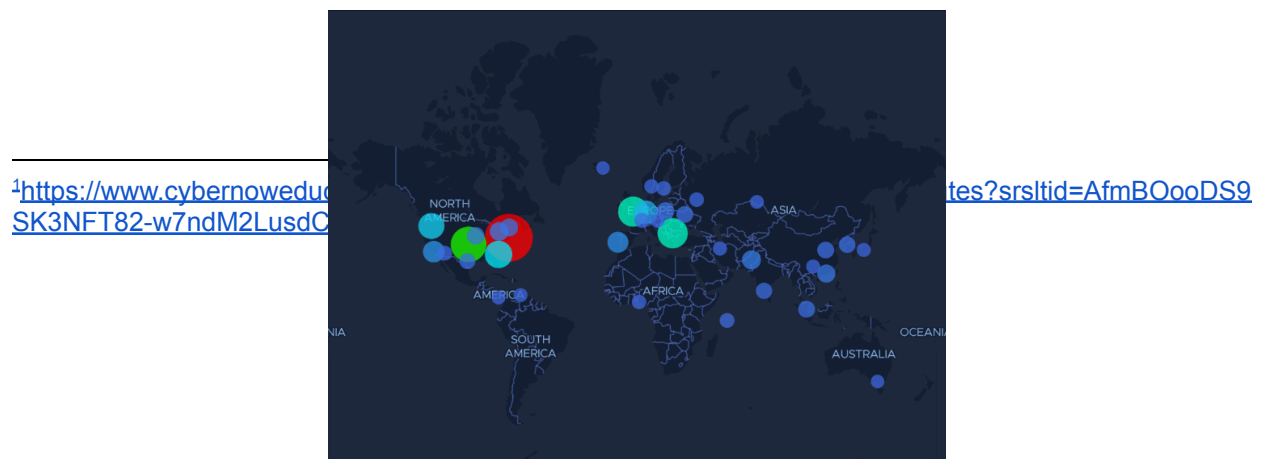


Figure 2: Real-time geographic distribution of attack origins.

Attacks came from all over the world, covering almost all 7 continents. Primarily, attacks came from the United States and Western Europe, with less attacks in Asia, and only a few in Africa and Oceania.

3.2 Attack Volume & Frequency

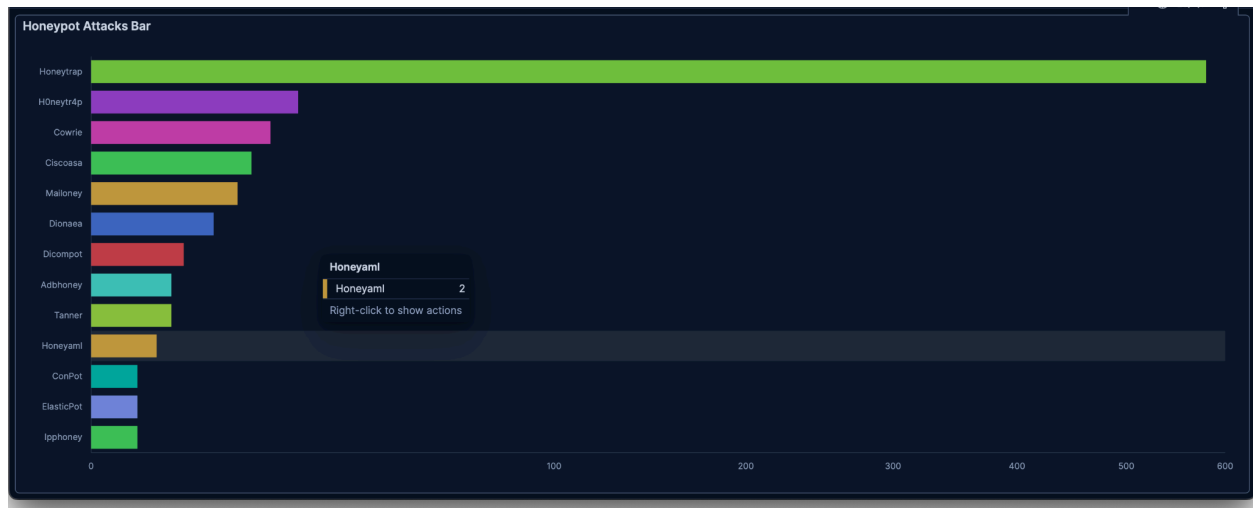


Figure 3: Distribution of activity across various honeypot services.

With all the ports open, the Honeytrap averaged 11 attacks per minute, over the course of about 52 minutes. There were a total of 659 distinct attacks, showing the speed that automated threat actors discover and probe internet infrastructure. Luckily, this VM had absolutely nothing on it, but imagine the damage possible for a non-security minded individual deploying an insecure device on the internet.

4. THE INVESTIGATION

4.1 The "Orangepi" IoT Botnet Pattern

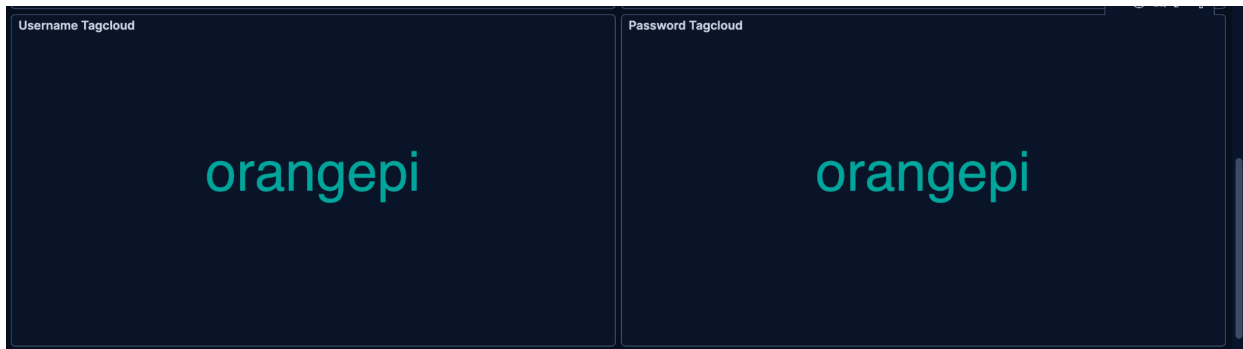


Figure 4: Common credentials attempted during brute-force sessions.

During the Honeypot deployment, the credentials “orangepi” were used to try a brute-force attack. Orangepi² is a company that makes single board computers that are commonly used in various IoT devices. The default configuration for these devices have all the credentials (username, password, and root password) as “orangepi”. Therefore, attackers try to brute force into these devices using the default credentials, in hopes to compromise an IoT device.

4.2 Exploits and Signature Identification

CVE ID	Count
CVE-2002-0013 CVE-2002-0012	1
CVE-2002-0013 CVE-2002-0012 CVE-1999-0517	1
CVE-2019-11500 CVE-2019-11500	1
CVE-2021-3449 CVE-2021-3449	1
CVE-2024-14007 CVE-2024-14007	1

Figure 5: IDS alerts identifying specific CVE exploitation attempts.

T-Pot detects different common exploit methods that are already logged with the National Institute of Standards and Technology. The exploit attempts tried during this specific Honeypot are:

- **CVE-2002-0013³ and CVE-2002-0012⁴:** Attackers can gain privileges or do a denial of service through vulnerabilities in the SNMPv1.
- **CVE-1999-00517⁵:** SNMP community name is the default, null, or missing.
- **CVE-2019-11500⁶:** mishandled ‘\0’ characters led to processing failures in Dovecot and Pigeonhole.
- **CVE-2021-3449⁷:** A vulnerability in OpenSSL TLS server when sent a malicious ClientHello leads to a denial of service attack.

² <http://www.orange-pi.org/>

³ <https://nvd.nist.gov/vuln/detail/cve-2002-0013>

⁴ <https://nvd.nist.gov/vuln/detail/cve-2002-0012>

⁵ <https://nvd.nist.gov/vuln/detail/CVE-1999-0517>

⁶ <https://nvd.nist.gov/vuln/detail/CVE-2019-11500>

⁷ <https://nvd.nist.gov/vuln/detail/cve-2021-3449>

- **CVE-2024-14007⁸**: a remote attacker can gain privileged access to DVR/NVR/IPC products using NVMS-9000 firmware.

4.3 Ports Accessed



Figure 6: Ports accessed by attackers over the course of Honeypot being deployed.

T-Pot detects attacks over each port and logs them. The ports⁹ most commonly attacked were:

- **443**: HTTPS
- **2323**: Backup port for Telnet
- **8087**: Internal communications and diagnostics
- **8090**: Alternate port for HTTP
- **8728**: Default TCP port for MikroTik Routers OS API

5. LESSONS LEARNED & DEFENSIVE STRATEGY

Based on the data captured, the following security recommendations are vital:

1. **Eliminate Default Credentials:** When getting a new device, especially a new IoT device, change the default credentials as soon as possible. Default credentials can be compromised as soon as a device is deployed.
2. **Strict Port Management:** Ensure your ports are closed or closely monitored.
3. **Proactive Monitoring:** Monitor the activity on your ports, device, and network. Investigate any suspicious activity and keep all credentials private.

⁸ <https://nvd.nist.gov/vuln/detail/CVE-2024-14007>

⁹ <https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.txt>