Findings from AWS Honeypot using T-Pot

1. Introduction

- This time with my honeypot I put it on a different region, I assigned it to an AWS server in Texas, and left it open for 72 hours to see where the attacks come from this time and to monitor the attacks and vulnerabilities. Some of the tools I used are Tpot, Kibana, Elastic Static, AWS S3.

2. Data Collection

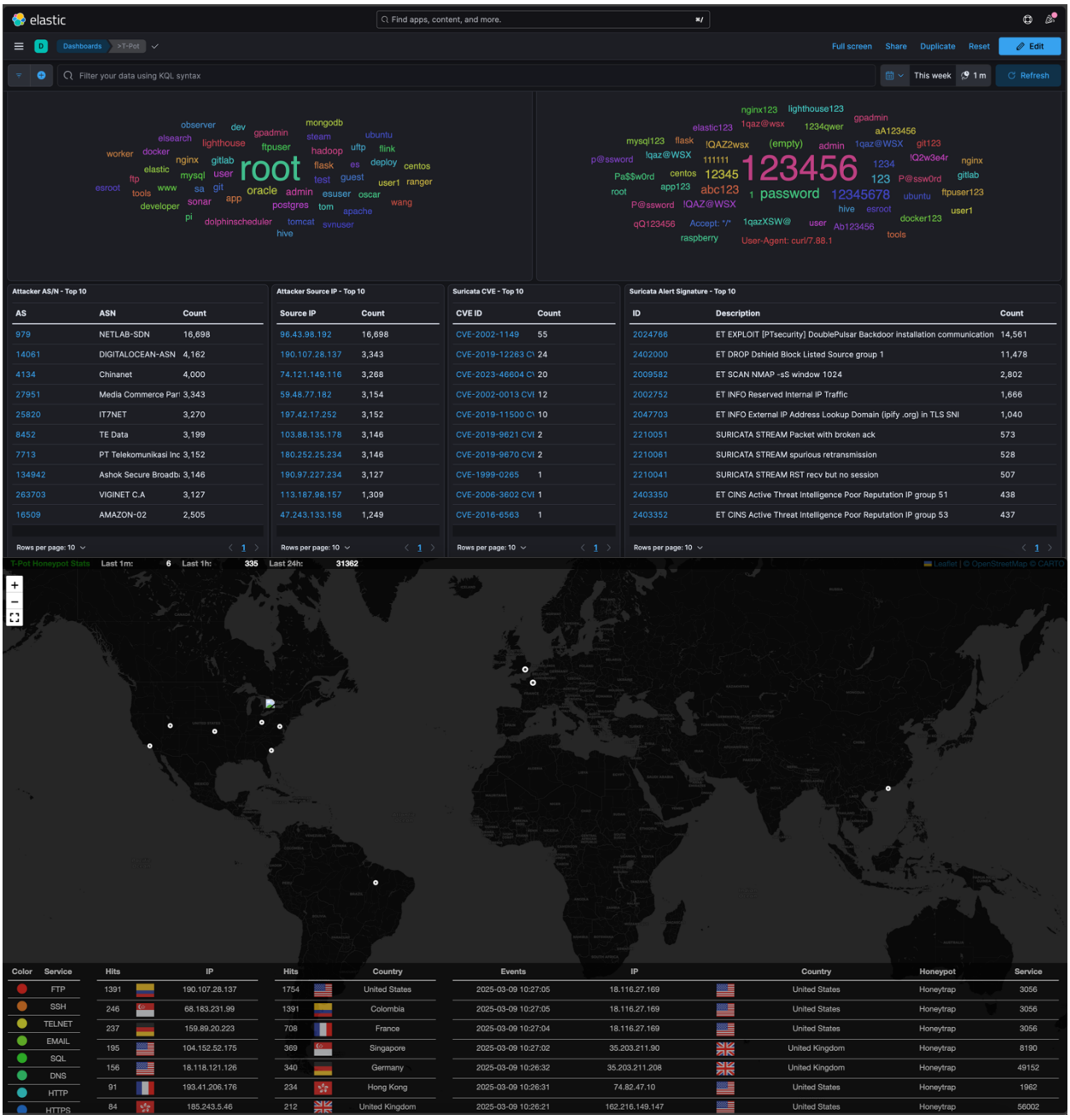
- **Observation Period**: I had the honeypot open from 2pm on March 6th and closed it at 2pm on March 9th.
- **Total Number of Attacks Logged**: There were 69K attacks total on the honeypot.
- **Top Targeted Services**: Some of the most attacked ports were SSH, RDP, HTTP, SMB.
- **Attack Sources**: Some of the top IP addresses to attack were 96.43.98.192 with 16,698 attacks and the second most were 190.107.28.137 with 3,343 attacks.
- **Common Exploits Detected**: The most common attacks were brute force, SQL injection and remote code execution.
- **Anomalies Noticed**: Some anomalies I notice were certain times during the day, I would get as many as 300 attacks, but then it would slow down, and I would get about 50-100 attacks for 4hrs.

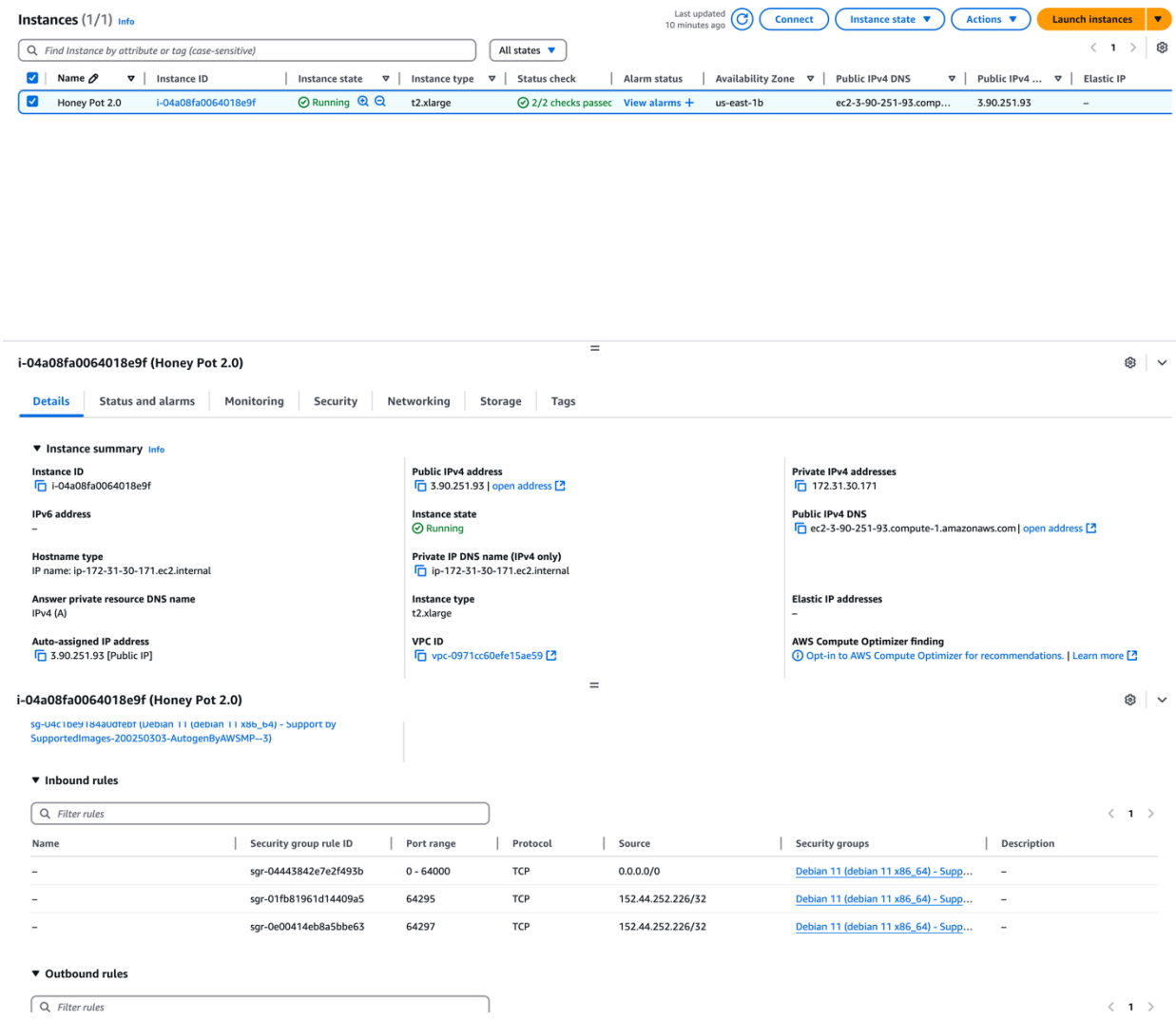
3. Data Analysis

- **Attack Trends Over Time**: In the pictures below
- **Common Attack Methods**: In the pictures below
- **Geolocation Breakdown**: the most active countries trying to hack my honeypot were the United States, Colombia, and France, which had the most attacks.
- **Detection of Repeated Attackers**: Yes, most of the attacks were happening multiple times from the same people trying different attempts.

4. Data Organization & Visualization


elastic
Find apps, content, and more.
Dashboards
T-Pot
Full screen
Share
Duplicate
Reset
Edit
Filter your data using KQL syntax
This week
Refresh
Honeypot Attacks
69k
Dionaea
22k
Honeytrap
17k
Redishoneypot
16k
Cowrie
12k
Tanner
869
Sentrypeer
625
ConPot
369
H0neytr4p
262
Ciscoasa
113
ElasticPot
113
Honeypot Attacks Bar
Honeypot Attacks Histogram
Attacks
Unique Source IPs
Attack Map - Dynamic
Elastic Maps Service, OpenMapTiles, OpenStreetMap contributors
Attacks by Destination Port Histogram
445
6379
22
80
8728
Attacks by Honeypot Histogram
Dionaea
Honeytrap
Redishoneypot
Cowrie
Tanner
Attacks by Country Histogram
United States
China
Colombia
France
India
Attacker Src IP Reputation
known attacker
mass scanner
bot, crawler
Attacks by Honeypot
P0f OS Distribution
Linux 2.2.x-3.x
Windows 7 or 8
Windows NT kernel
Attacks by Country
Attacks by Country and Port
Suricata Alert Category Histogram
Misc Attack
Misc activity
Username Tagcloud
root
Password Tagcloud
123456
password
Attacker AS/N - Top 10
AS
ASN
Count
979
NETLAB-SDN
16,698
14061
DIGITALOCEAN-ASN
4,162
Attacker Source IP - Top 10
Source IP
Count
96.43.98.192
16,698
190.107.28.137
3,343
Suricata CVE - Top 10
CVE ID
Count
CVE-2002-1149
55
24
Suricata Alert Signature - Top 10
ID
Description
Count
2024766
ET EXPLOIT [PTsecurity] DoublePulsar Backdoor installation communication
14,561
2402000
ET DROP Dshield Block Listed Source group 1
11,474


elastic
Find apps, content, and more.
Dashboards
>T-Pot
Full screen
Share
Duplicate
Reset
Edit
Filter your data using KQL syntax
This week
1 m
Refresh
root
123456
password
Attacker AS/N - Top 10
AS
ASN
Count
979 NETLAB-SDN 16,698
14061 DIGITALOCEAN-ASN 4,162
4134 Chinanet 4,000
27951 Media Commerce Part 3,343
25820 IT7NET 3,270
8452 TE Data 3,199
7713 PT Telekomunikasi Inc 3,152
134942 Ashok Secure Broadb 3,146
263703 VIGINET C.A 3,127
16509 AMAZON-02 2,505
Attacker Source IP - Top 10
Source IP
Count
96.43.98.192 16,698
190.107.28.137 3,343
74.121.149.116 3,268
59.48.77.182 3,154
197.42.17.252 3,152
103.88.135.178 3,146
180.252.25.234 3,146
190.97.227.234 3,127
113.187.98.157 1,309
47.243.133.158 1,249
Suricata CVE - Top 10
CVE ID
Count
CVE-2002-1149 55
CVE-2019-12263 CV 24
CVE-2023-46604 CV 20
CVE-2002-0013 CVI 12
CVE-2019-11500 CV 10
CVE-2019-9621 CVI 2
CVE-2019-9670 CVI 2
CVE-1999-0265 1
CVE-2006-3602 CVI 1
CVE-2016-6563 1
Suricata Alert Signature - Top 10
ID
Description
Count
2024766 ET EXPLOIT [PTsecurity] DoublePulsar Backdoor installation communication 14,561
2402000 ET DROP Dshield Block Listed Source group 1 11,478
2009582 ET SCAN NMAP -sS window 1024 2,802
2002752 ET INFO Reserved Internal IP Traffic 1,666
2047703 ET INFO External IP Address Lookup Domain (ipify .org) in TLS SNI 1,040
2210051 SURICATA STREAM Packet with broken ack 573
2210061 SURICATA STREAM spurious retransmission 528
2210041 SURICATA STREAM RST recv but no session 507
2403350 ET CINS Active Threat Intelligence Poor Reputation IP group 51 438
2403352 ET CINS Active Threat Intelligence Poor Reputation IP group 53 437
Rows per page: 10
T-Pot Honeypot Stats
Last 1m: 6
Last 1h: 335
Last 24h: 31362
Leaflet | © OpenStreetMap © CARTO
Color
Service
FTP
SSH
TELNET
EMAIL
SQL
DNS
HTTP
HTTPS
Hits
IP
1391 190.107.28.137
246 68.183.231.99
237 159.89.20.223
195 104.152.52.175
156 18.118.121.126
91 193.41.206.176
84 185.243.5.46
Hits
Country
1754 United States
1391 Colombia
708 France
369 Singapore
340 Germany
234 Hong Kong
212 United Kingdom
Events
IP
Country
Honeypot
Service
2025-03-09 10:27:05 18.116.27.169 United States Honeytrap 3056
2025-03-09 10:27:05 18.116.27.169 United States Honeytrap 3056
2025-03-09 10:27:04 18.116.27.169 United States Honeytrap 3056
2025-03-09 10:27:02 35.203.211.90 United Kingdom Honeytrap 8190
2025-03-09 10:26:32 35.203.211.208 United Kingdom Honeytrap 49152
2025-03-09 10:26:31 74.82.47.10 United States Honeytrap 1962
2025-03-09 10:26:21 162.216.149.147 United States Honeytrap 56002



5. Iteration & Next Steps

For the next time I run the honeypot I'd like to connect AI to its logs so it can better identify the attacks and have a better reading a logs to better forecast what attacks can happen and when they will happen and how frequently they're happening.