

# **AWS HONEYPOT PROJECT**

**Hector Agwara**

**4/23/2025**

## Observations

Time: 04/22/25: 4:00AM: -> 04/23/25: 04:00AM

**Background Info:** What are honeypots and why are they important in cybersecurity?

Honeypots are beneficial for cybersecurity because they provide a way to study the tactics and techniques used by attackers without risking actual systems or data. By analyzing the data collected by honeypots, security professionals can identify new threats, vulnerabilities, and attack patterns, which can be used to enhance security measures and develop more effective countermeasures. Additionally, honeypots can be used to detect attacks that traditional security measures might miss, such as zero-day attacks and advanced persistent threats.

T-Pot is an open-source honeypot platform that deploys multiple honeypots with various network services and protocols to attract attackers and record their activities. T-Pot's versatility in deployment extends beyond any restrictions of cloud platforms or virtual machines, as it can be conveniently installed on a wide range of Debian instances, including those in AWS, Azure, and other cloud platforms, thereby providing a flexible and scalable solution to honeypot deployment.

### Lab Summary:

This report presents an initial assessment of a T-Pot honeypot's performance installed on a Debian 11 AWS Instance, focusing on the first 24 hours of activity between April 22nd, 04:00AM, and April 23rd, 4:00AM. By analyzing trends and significant activity, the report aims to provide insights into predicting future cyber-attacks and determining the underlying factors contributing to the elevated volume of attacks observed on certain days of the week.

By also running a parallel T-Pot instance in Tokyo, Japan, my study aims to determine the potential impact of geographic location on the frequency and nature of cyber-attacks, providing insights into how network security can be tailored based on location-specific risk factors. The report's insights can aid in formulating comprehensive measures to enhance network security, including pinpointing systemic weak spots, identifying compromised usernames and passwords, and evaluating the effectiveness of existing security controls in thwarting brute force attacks.

This report will specifically outline what each honeypot does, analyze the overall T-Pot statistics and those of the top three attacked honeypots (Dionaea, Honeytrap, Cowrie) as well as determine outliers and their causes, highlight encountered issues and their resolutions, and provide predictions on the anticipated trends over the next week based on the data analyzed.

**Table of Contents:**

[Defining the Top 10 HoneyPots](#)/Page 3

[Overall Statistics](#)/Page 4

[-The Top CVEs Exploited](#)/Page 9

[Cowrie Analysis](#)/Page 11

[Dionaea Analysis](#)/Page 15

[Honeytrap Analysis](#)/Page 19

[Problems](#)/Page 21

**Overview****Defining the Top 10 HoneyPot Types:**

**Honeytrap** is designed to emulate various types of network services and protocols to attract and trap attackers. These emulated services include SSH, Telnet, FTP, HTTP, SMTP, and other common protocols. The Honeytrap module can be configured to listen on multiple ports and can be customized to mimic the behavior of real services as closely as possible.

**Dionaea** is a low-interaction honeypot that emulates vulnerable Windows environments and services, capturing information on malware and attack payloads. It uses Python as a scripting language, libemu to detect shellcodes, and supports IPv6 and TLS, and logs include hash values of detected files that can be used for further intelligence gathering.

**Cowrie** is a high-interaction SSH and Telnet honeypot designed to capture and record attacker activity on a simulated system. It provides a simulated shell environment that records all the attacker's actions, including login credentials, tools used, and techniques employed to gain unauthorized access.

**Tanner** is a low-interaction honeypot designed to emulate Windows-based systems and services, which captures attacker activity and sends alerts to security personnel. It can capture attacker's IP addresses, commands, and payloads to identify attack patterns.

**SentryPeer** is an open-source, peer-to-peer (P2P) network designed to detect and prevent fraudulent activities in real-time communication systems, particularly in Voice over IP (VoIP) and Session Initiation Protocol (SIP) networks. It functions as a distributed **blacklist** and **reputation system** where users share data about suspicious or malicious IP addresses, phone numbers, and SIP endpoints involved in scams, spam, or hacking attempts.

**ADB HoneyPot** is a security tool that emulates an ADB-enabled Android device to detect and log unauthorized access attempts.

**h0neytr4p** (or honey-trap) is a cybersecurity tool or framework designed to detect and analyze malicious activity by deploying deceptive systems (honeypots) that attract attackers. These traps log interactions with attackers, providing valuable threat intelligence.

**DICOMpot** is a DICOM honeypot that mimics medical imaging systems (PACS) to detect attacks targeting healthcare networks. When integrated with Elastic, it logs malicious activity (e.g., unauthorized DICOM queries, exploit attempts) into Elasticsearch, enabling analysis via Kibana dashboards (attack trends, geolocation) and Elastic SIEM (automated alerts, correlation with other threats). Mailoney is a honeypot that emulates a vulnerable email server environment.

Redishoneypot is a Redis-server honeypot that logs brute-force attacks, unauthorized access attempts, and malicious commands (like FLUSHDB or exploit attempts) targeting Redis databases. When integrated with Elastic, it sends logs to Elasticsearch for storage, enables attack visualization via Kibana dashboards (showing attack sources, frequency, and patterns), and triggers SIEM alerts for suspicious activity (e.g., ransomware or data-wiping attempts like CVE-2022-0543).

**Conpot** is a low-interaction honeypot designed to emulate industrial control systems and SCADA protocols.

## Overall T-Pot Statistics

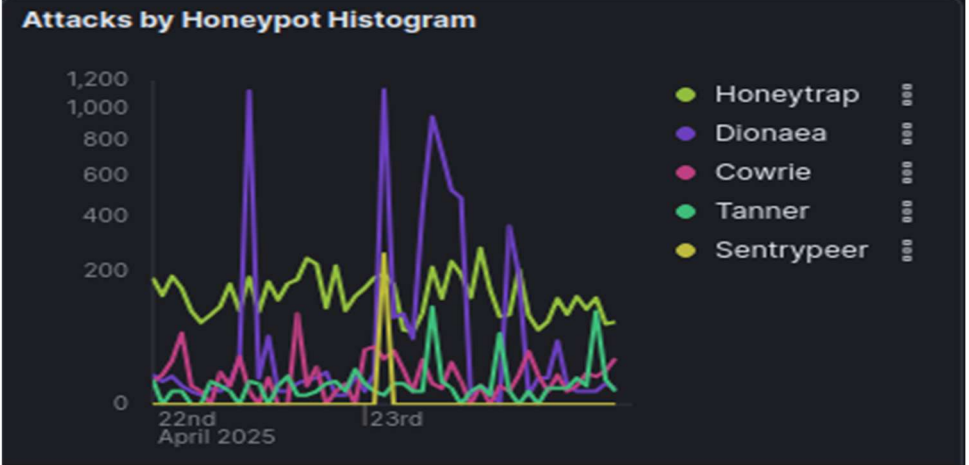
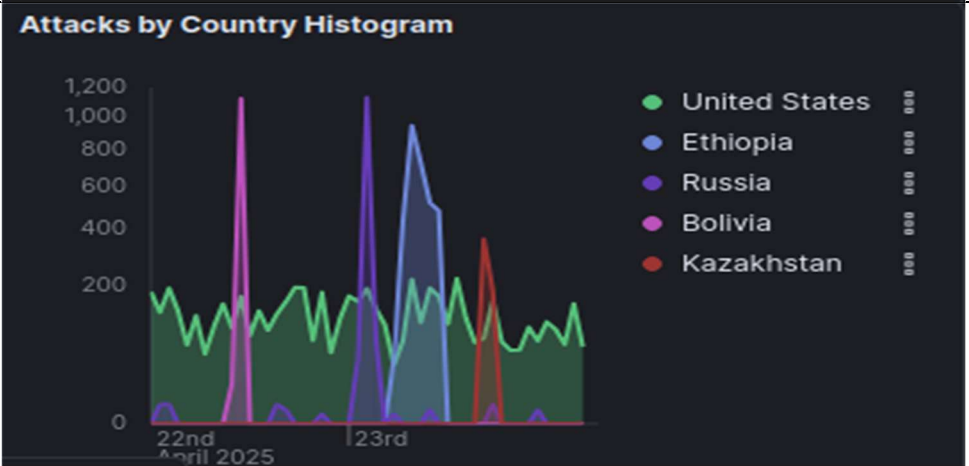
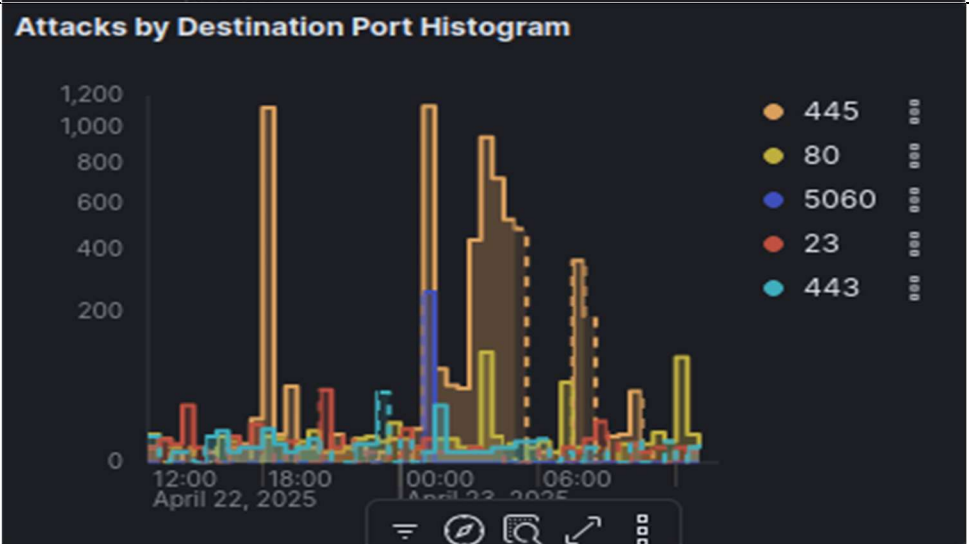
In this report we'll be covering the top three most attacked honeypots, honeytrap, Dionaea, and cowrie, but first, overall T-Pot statistics:

Honeypot	Honeytrap	Dionaea	Cowrie	Tanner	SentryPeer	Adbhoney	H0neytr4p	Dicompot	Redishoneypot	ConPot
15k	7k	6k	614	414	259	171	171	158	61	52

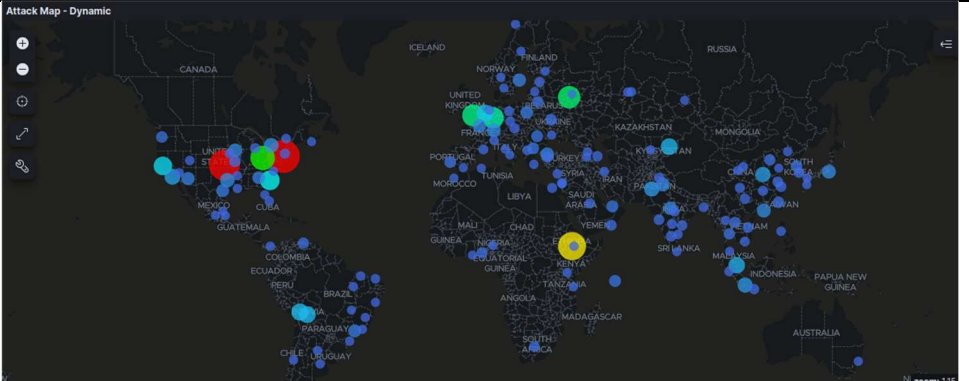
We can see that a majority of the attacks (15000) were against the honeytrap honeypot with 6964 attacks (45%), followed by Dionaea with 6,445 attacks (42%), and 614 on the cowrie honeypot (4%).

Honeytrap's versatility and broader protocol support lead to more hits from automated scans, while Dionaea's specialized malware capture yields fewer but higher-value interactions

Overall STAT T-POT Board

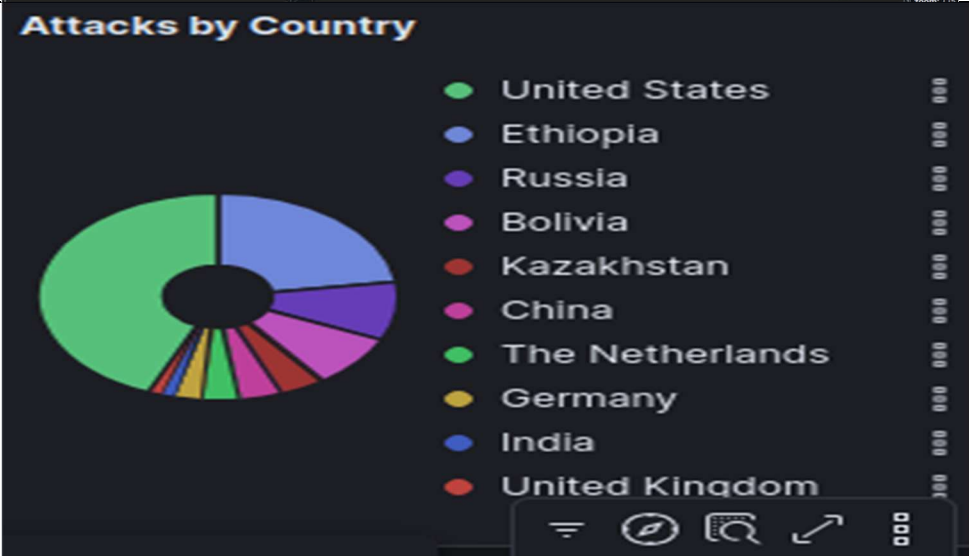
<p><b>Analysis:</b></p> <p>During this time period, most attacks spiked at 18:00, 1:00, 3:30-4:00, and 7:30. Most attacks appear to occur during the early hours of the day. Dionaea attacks are by far the most numerous, but also appear in bursts, while honeytrap is more constant.</p>	<p><b>Diagram:</b></p> <div><p><b>Attacks by Honeytrap Histogram</b></p><p>Legend: Honeytrap (green), Dionaea (purple), Cowrie (pink), Tanner (light green), Sentrypeer (yellow)</p></div> <div><p><b>Attacks by Country Histogram</b></p><p>Legend: United States (green), Ethiopia (blue), Russia (purple), Bolivia (pink), Kazakhstan (red)</p></div> <div><p><b>Attacks by Destination Port Histogram</b></p><p>Legend: 445 (orange), 80 (yellow), 5060 (blue), 23 (red), 443 (teal)</p></div>
<p>The large spikes in attacks also appear to correlate with certain countries. Although the USA seems to be the most consistent with the volume of honeytrap attacks, Boliva, Russia, Ethiopia, and Kazakhstan seem to “spike” in attacks, surging at certain times and dying back down just as quickly.</p>	
<p>Port 445, which is commonly used for HTTPS traffic, appears to be the most targeted port based on the available data. This is followed by port 80, which is commonly used for unencrypted HTTP, and ports 5060, 23, and 443.</p>	

We can see that attacks are primarily clustered around the Eastern half of the US, Coastal south America, Northern Europe, southeast Asia and India.

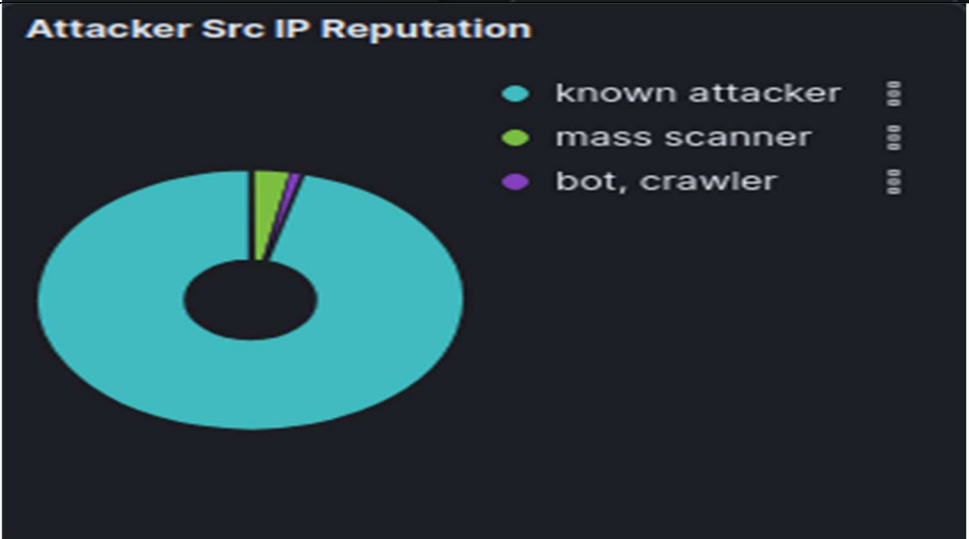


We can see here the top 10 countries by percentage of attacks.

- United States: 44%
- Ethiopia: 23%
- Russia: 9%
- Bolivia: 8%
- Kazakhstan: 4%
- China: 4%
- Netherlands: 3%
- Germany: 2%
- Canada: 1%
- United Kingdom: 1%

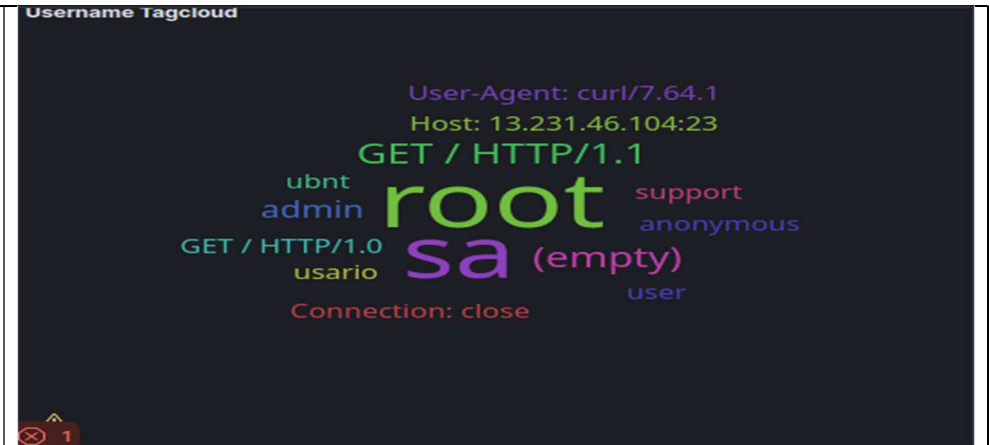
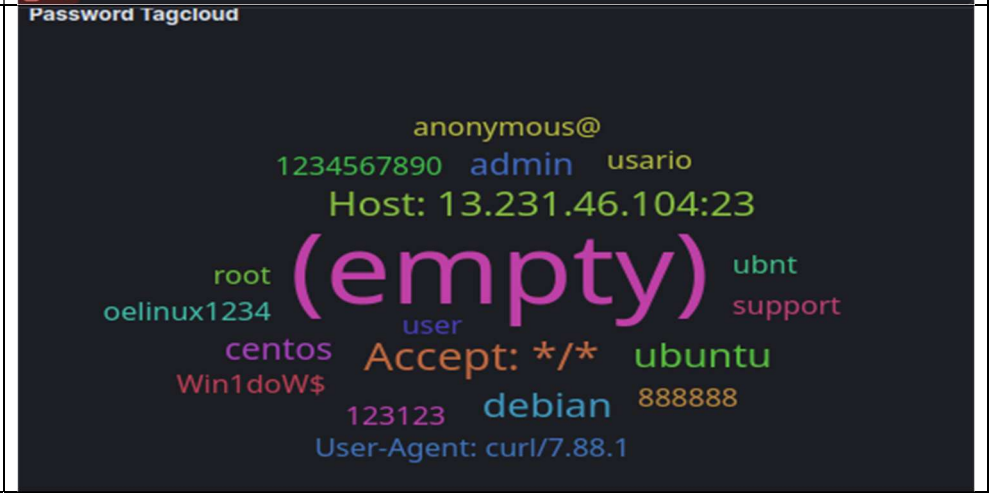


It appears that most attackers are known attackers,, or at least the ones that have an identifiable reputation.



<p>Some of the most commonly used OS distributions by attackers are , Linux 2.2.x-3.x (41%), Linux 2.2.x-3.x (barebone) (18%) ,Windows 7 or 8 (16%) and Windows NT (10%).</p> <p>Attackers may choose these OSes to exploit vulnerabilities that have not yet been patched or updated on those systems. These older systems may also be more prevalent in certain environments, particularly those with limited resources or technical expertise. Additionally, some attackers may use these systems as a means of evading detection by security measures that are designed to identify and block attacks originating from more current and widely used operating systems.</p>	<div><h3>POf OS Distribution</h3><table><tr><td>Linux 2.2.x-3.x</td><td>41%</td></tr><tr><td>Linux 2.2.x-3.x (barebone)</td><td>18%</td></tr><tr><td>Windows 7 or 8</td><td>16%</td></tr><tr><td>Windows NT</td><td>10%</td></tr></table></div>	Linux 2.2.x-3.x	41%	Linux 2.2.x-3.x (barebone)	18%	Windows 7 or 8	16%	Windows NT	10%				
Linux 2.2.x-3.x	41%												
Linux 2.2.x-3.x (barebone)	18%												
Windows 7 or 8	16%												
Windows NT	10%												
<p>Attacks from US, Ethiopia, Russia, and Bolivia mostly target ports 445 and https, while the China is an outlier with a mix of ports 80, 22, 443, 23, and 6379 being attacked the most. These unique ports are high-value targets for automated bots and hackers due to weak defaults or misconfigurations.</p>	<div><h3>Attacks by Country and Port</h3><table><tr><th>Country</th><th>Ports</th></tr><tr><td>United States</td><td>445, 2404, 80</td></tr><tr><td>Ethiopia</td><td>2181, 7001</td></tr><tr><td>Russia</td><td>445, 23</td></tr><tr><td>Bolivia</td><td>445, 23</td></tr><tr><td>China</td><td>445, 23, 8888, 80, 2181, 7001</td></tr></table></div>	Country	Ports	United States	445, 2404, 80	Ethiopia	2181, 7001	Russia	445, 23	Bolivia	445, 23	China	445, 23, 8888, 80, 2181, 7001
Country	Ports												
United States	445, 2404, 80												
Ethiopia	2181, 7001												
Russia	445, 23												
Bolivia	445, 23												
China	445, 23, 8888, 80, 2181, 7001												
<p>This data reveals timed attack patterns: brute-force surges at midnight (2,732 attacks) and mornings (1,500+) targeting RDP/SSH for EC2 access; evening vulnerability scans (200+/hr) probing for misconfigured S3 buckets and APIs; and pre-dawn Redis attacks (100+) attempting cryptojacking.</p> <p>Attackers automate these waves—using midnight strikes to evade detection, business-hour traffic to blend in, and protocol exploits for data theft—highlighting cloud-specific risks like exposed services and weak credentials.</p>	<div><h3>Suricata Alert Category Histogram</h3><table><tr><th>Category</th><th>Count</th></tr><tr><td>Attempted Administrator Access</td><td>2732</td></tr><tr><td>Misc Attack</td><td>1500+</td></tr><tr><td>Generic Protocol Communication</td><td>200+/hr</td></tr><tr><td>Misc activity</td><td>100+</td></tr><tr><td>Attempted Information Leak</td><td>-</td></tr></table></div>	Category	Count	Attempted Administrator Access	2732	Misc Attack	1500+	Generic Protocol Communication	200+/hr	Misc activity	100+	Attempted Information Leak	-
Category	Count												
Attempted Administrator Access	2732												
Misc Attack	1500+												
Generic Protocol Communication	200+/hr												
Misc activity	100+												
Attempted Information Leak	-												



<p>These are the most used usernames to try to gain access to my instance. The usernames used by attackers tend to be predictable and commonly used or are vulnerable to dictionary attacks. Consequently, it is imperative to adopt strong and unique usernames to enhance the resilience of the system against unauthorized access attempts.</p>	<p>Username Tagcloud</p>  <p>This tagcloud visualizes the most common usernames used in attack attempts. The most prominent words are 'root' and 'sa', both in large green and purple fonts respectively. Other visible words include 'admin', 'ubnt', 'usuario', 'support', 'anonymous', 'user', 'GET / HTTP/1.1', 'GET / HTTP/1.0', and 'Connection: close'. The background is dark grey.</p>
<p>Interestingly, the most used password is simply no password at all, maybe hopefully guessing that the server has no password. This is followed by the usual top 10 passwords like password or 123456 or admin, root, or user, highly predictable and easily cracked.</p>	<p>Password Tagcloud</p>  <p>This tagcloud visualizes the most common passwords used in attack attempts. The most prominent word is '(empty)' in a large pink font, indicating that many attempts were made with no password. Other visible words include 'anonymous@', '1234567890', 'admin', 'usuario', 'Host: 13.231.46.104:23', 'root', 'oelinux1234', 'centos', 'Win1doW\$', '123123', 'debian', '888888', 'User-Agent: curl/7.88.1', 'Accept: */*', 'ubuntu', 'support', 'ubnt', and 'user'. The background is dark grey.</p>



## The Top CVE's Exploited Were:

**CVE-1999-0265:** What it is: A very old Windows weakness that lets hackers take control of unpatched systems. Why targeted: Many outdated servers or devices (like old printers) still haven't fixed this, making them easy targets.

**CVE-2002-0013:** What they are: Flaws in email (SMTP) or file transfer (FTP) services that let hackers run malicious code.

Why targeted: Attackers scan for these to hijack servers or spread malware.

**CVE-2021-3449:** What it is: A bug in OpenSSL (used for secure web connections) that can crash systems or leak data.

Why targeted: Cloud services and websites use OpenSSL hackers exploit this to disrupt sites or steal info.

**CVE-2019-011500:** What it is: A *critical* flaw in Pulse Secure VPNs that lets hackers break in without a password. Why targeted: VPNs are gateways to company networks—this CVE is a "golden ticket" for thieves.

**CVE-2002-1149 & CVE-2009-2765** What they are: Lesser-known bugs in network services (like DNS or Linux tools). Why targeted: Opportunistic attacks if a system is vulnerable, hackers will try.

## Suricata CVE - Top 10

CVE ID	Count
CVE-1999-02	8
CVE-2002-00	5
CVE-2021-34	3
CVE-2019-11	2
CVE-2002-11	1
CVE-2009-27	1

Source: <https://www.cvedetails.com/>

Note: **Suricata** is a free and open-source intrusion detection system (IDS) and intrusion prevention system (IPS) developed by the Open Information Security Foundation (OISF). It is designed to monitor network traffic and detect and prevent a wide range of cyber threats including malware, viruses, and other malicious activities, and in the case of the honeypot, detect when CVEs are exploited.

Top 10 IP Adresses	ASN	Count	City/State	Country	ISP
172.254.94.10	20115	3,151	New York	United States	Charter communications
196.190.222.242	24757	3,146	Addis Ababa	Ethiopia	Ethio telecom
85.192.171.116	12389	1,207	Orenburg	Russia	pjsc rostelecom
200.105.196.189	28081	587	La Paz	Bolivia	axs bolivia s. a.
91.203.21.143	21245	550	Otegen Batyr	Kazakhstan	astek jsc
181.115.190.30	6147	379	La Paz	Bolivia	entel s. a. - entelnet
89.163.231.174	206349	259	Weeze	Germany	wiit ag
190.181.26.29	28081	174	La Paz	Bolivia	axs bolivia s. a.
18.219.47.173	16509	131	Columbus	United States	Amazon technology inc
45.33.33.185	63949	117	Fremont	United States	linode llc

### Analysis of Top 10 Attacker IPs

By parsing the Top 10 IP Address data, I identified the ASNs, geolocations, and ISPs associated with these addresses. The majority of malicious traffic originated from the United States (Charter Communications, AWS, Linode), Ethiopia (Ethio Telecom), Russia (Rostelecom), and Bolivia (AXS Bolivia, Entel). While some IPs could be spoofed, the prevalence of

ISPs like Ethio Telecom and Rostelecom suggests these are likely real attack sources often linked to botnets or compromised devices.

Notably, AWS (AS16509) and Linode (AS63949) IPs indicate possible cloud-hosted attacks, while the high volume from Charter Communications (AS20115, 3,151 attacks) points to hijacked residential networks. Countries like Bolivia and Ethiopia may attract attackers due to lax cybersecurity regulations, but the U.S. and German (WIIT AG) IPs remind us that threats are global and not limited to low-income regions.

#### Suricata Alert Signature - Top 10

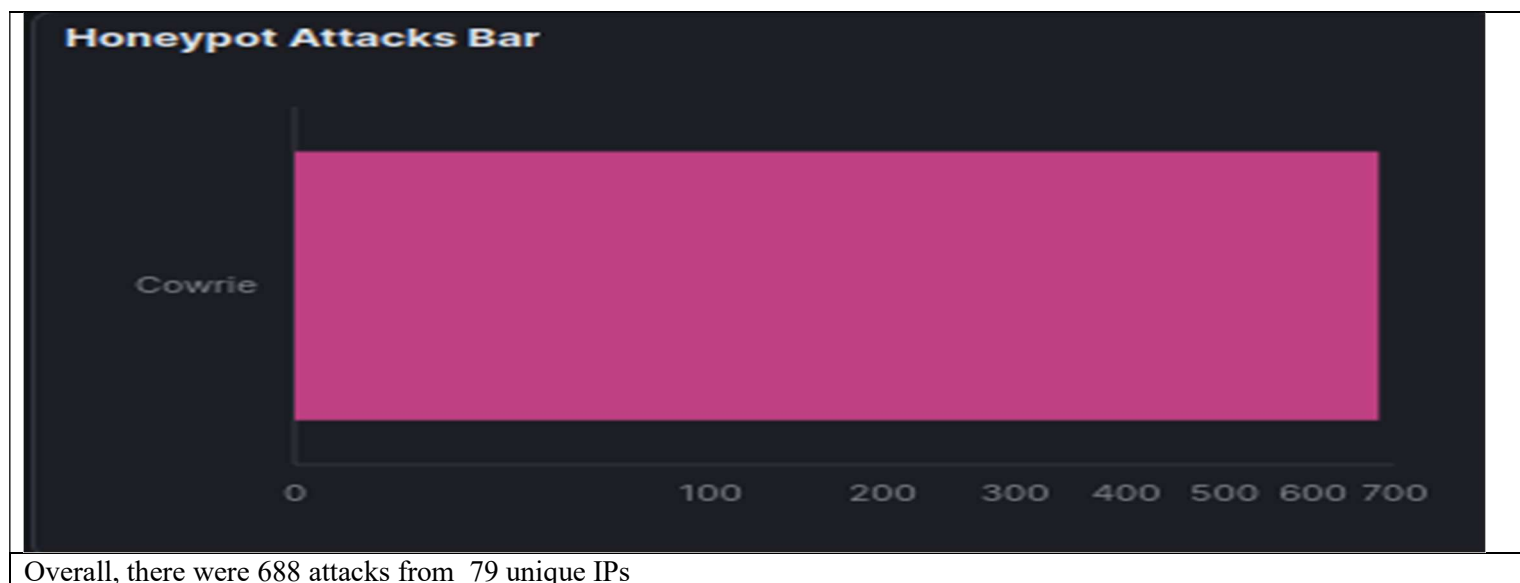
ID	Description	Count
2024766	ET EXPLOIT [PTsecurity] DoublePulsar Backdoor installation communication	12,796
2402000	ET DROP Dshield Block Listed Source group 1	3,377
2009582	ET SCAN NMAP -sS window 1024	749
2002752	ET INFO Reserved Internal IP Traffic	624
2210037	SURICATA STREAM FIN recv but no session	390
2228000	SURICATA SSH invalid banner	368
2038967	ET INFO SSH-2.0-Go version string Observed in Network Traffic	309
2400038	ET DROP Spamhaus DROP Listed Traffic Inbound group 39	301
2001984	ET INFO SSH session in progress on Unusual Port	289
2023753	ET SCAN MS Terminal Server Traffic on Non-standard Port	243

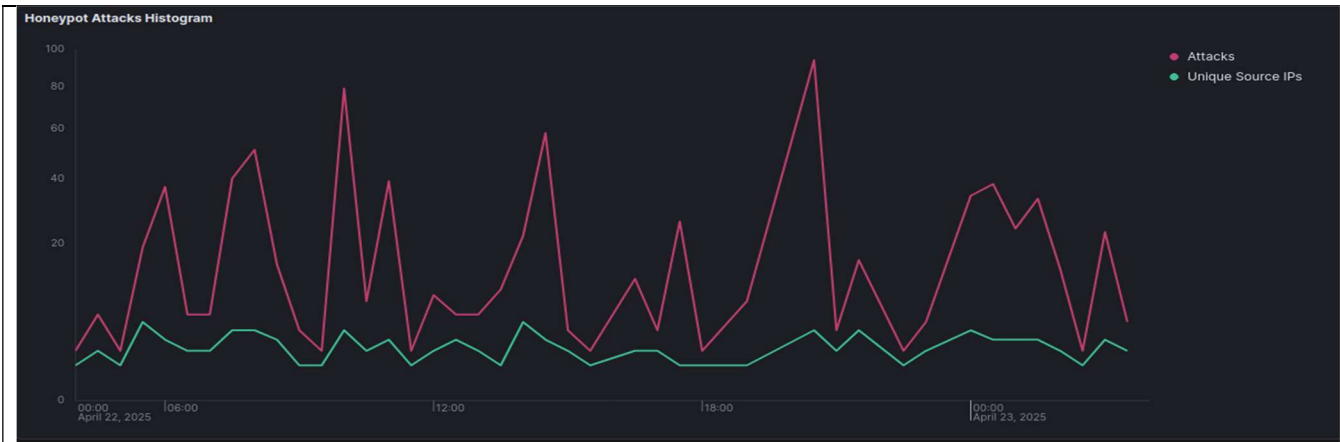
1. **ET EXPLOIT DoublePulsar (12,796 hits):** The prevalent EternalBlue/DoublePulsar backdoor exploit targeting unpatched Windows systems demonstrates the critical need for SMBv1 patching and network segmentation to prevent ransomware attacks.
2. **ET DROP Dshield Block (3,377 hits):** Blocking known malicious IPs from DShield's threat feed effectively prevents connections from compromised hosts and botnet nodes.
3. **ET SCAN NMAP -sS (749 hits):** Detection of Nmap SYN scans with a 1024 window size reveals attackers conducting stealthy network reconnaissance for vulnerability mapping.
4. **ET INFO Reserved IPs (624 hits):** Spoofed internal IP traffic indicates potential phishing attempts or lateral movement probes that should be blocked at network perimeters.
5. **SURICATA FIN no session (390 hits):** Malformed TCP FIN packets suggest possible DoS probes or connection hijacking attempts requiring TCP state inspection.

6. **SURICATA SSH invalid banner (368 hits):** Malicious SSH banners often conceal brute-force attacks or exploit attempts, necessitating SSH hardening and fail2ban deployment.
7. **ET INFO SSH-2.0-Go (309 hits):** Suspicious "Go" client strings in SSH traffic may mask automated bot attacks that should trigger access restrictions.
8. **ET DROP Spamhaus (301 hits):** Filtering Spamhaus DROP-listed traffic automatically blocks known spam/malware sources when list updates are maintained.
9. **ET INFO SSH unusual port (289 hits):** Detection of SSH services on non-standard ports reveals attacker scanning for backdoored or misconfigured access points.
10. **ET SCAN MS Terminal Server (243 hits):** RDP scans on alternate ports expose vulnerable remote desktops that should be protected with VPNs and MFA.

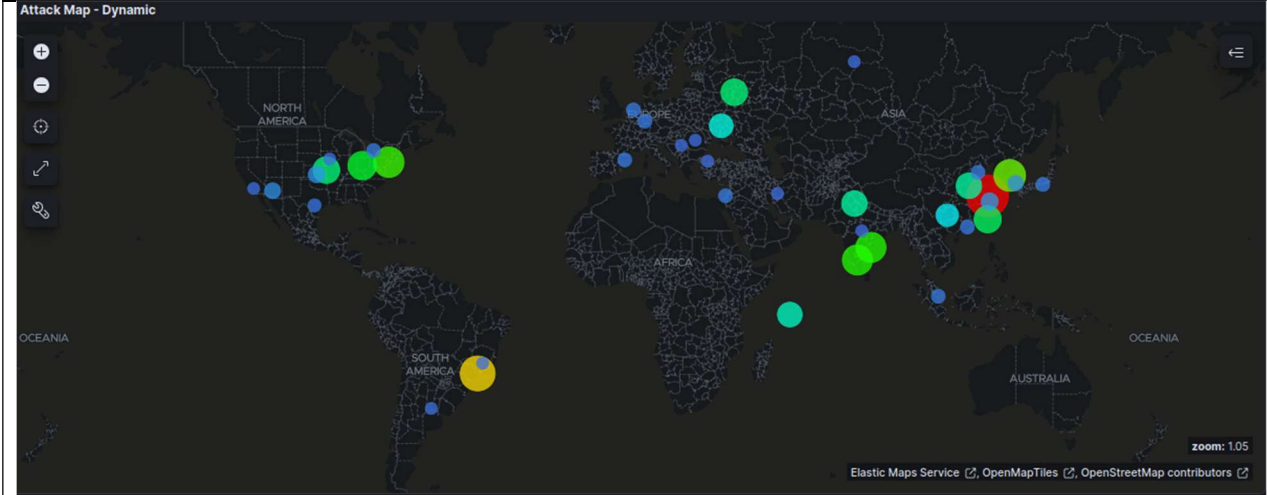
Although not the most attacked honeypot, I think Cowrie offers the most insight into the attackers motives and behavior.

Cowrie:

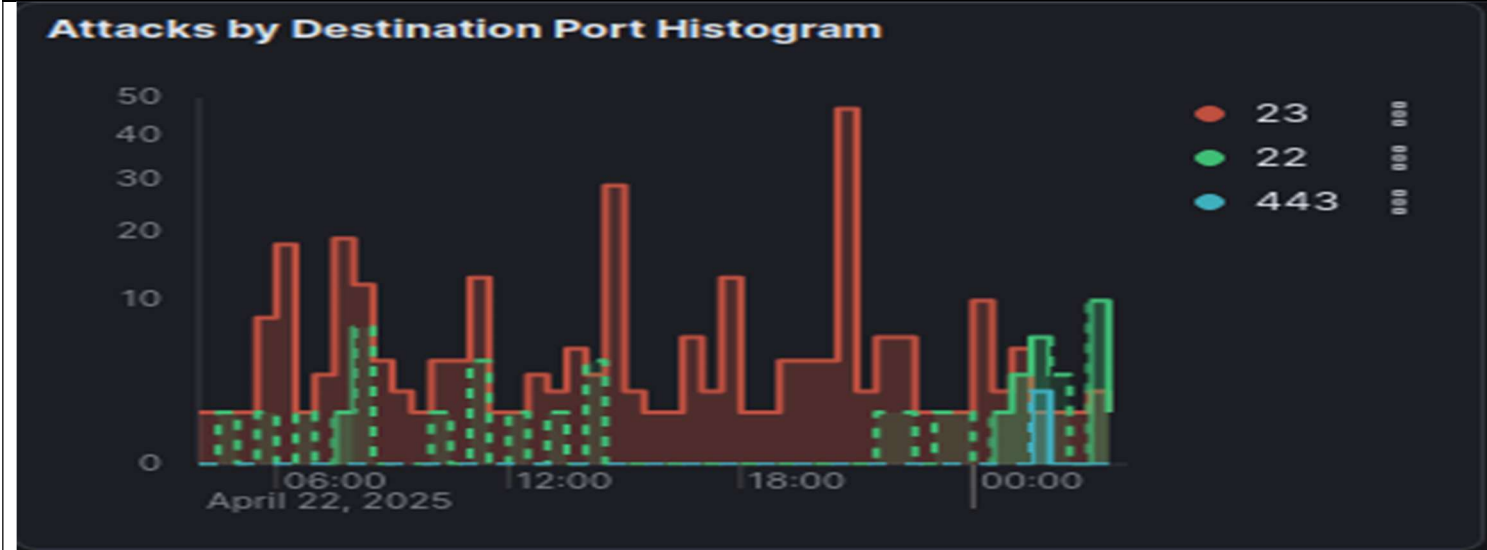




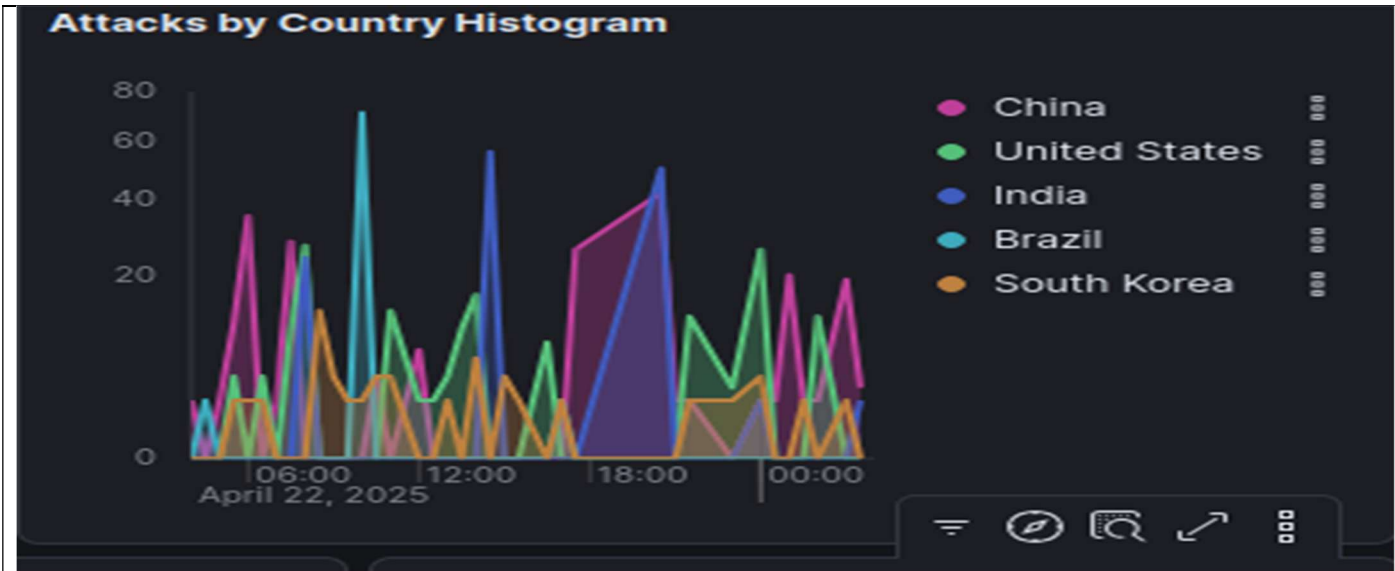
These attacks were remained mostly constant throughout the day, with attacks peaking at 10 am and 8pm.



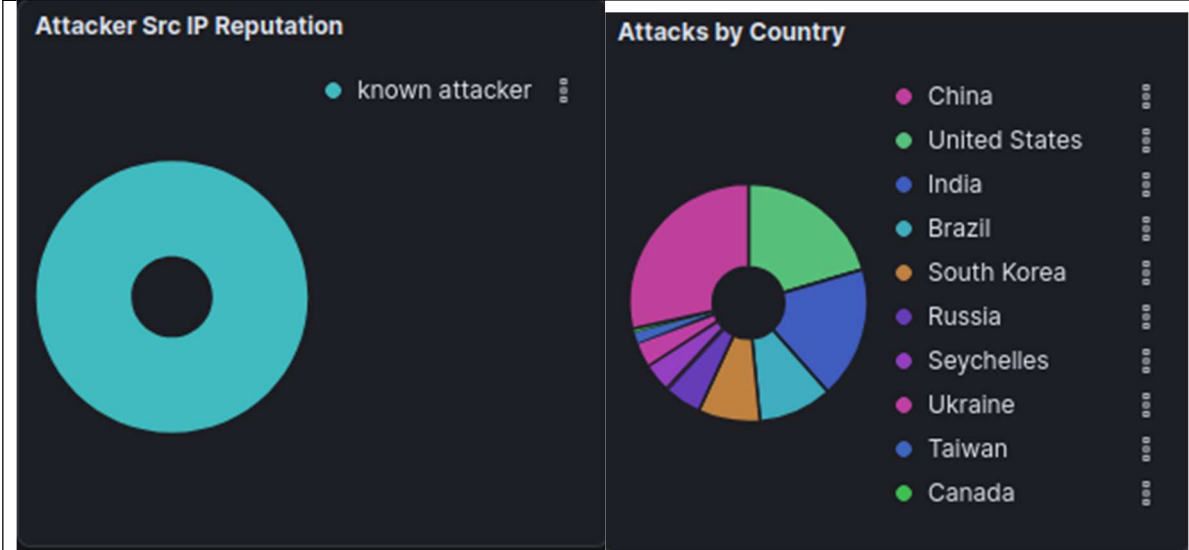
It appears that most of the attacks came from the China, Bolivia, India, Central europe, and the Eastern United States.



Interesting Telnet was used to connect way more often then SSH was, though that could be because of the inherit insecurity and plaintext nature of Telnet connections meaning they're less traceable.



As noted in the global map earlier, China, United states and India are some of the top countries.

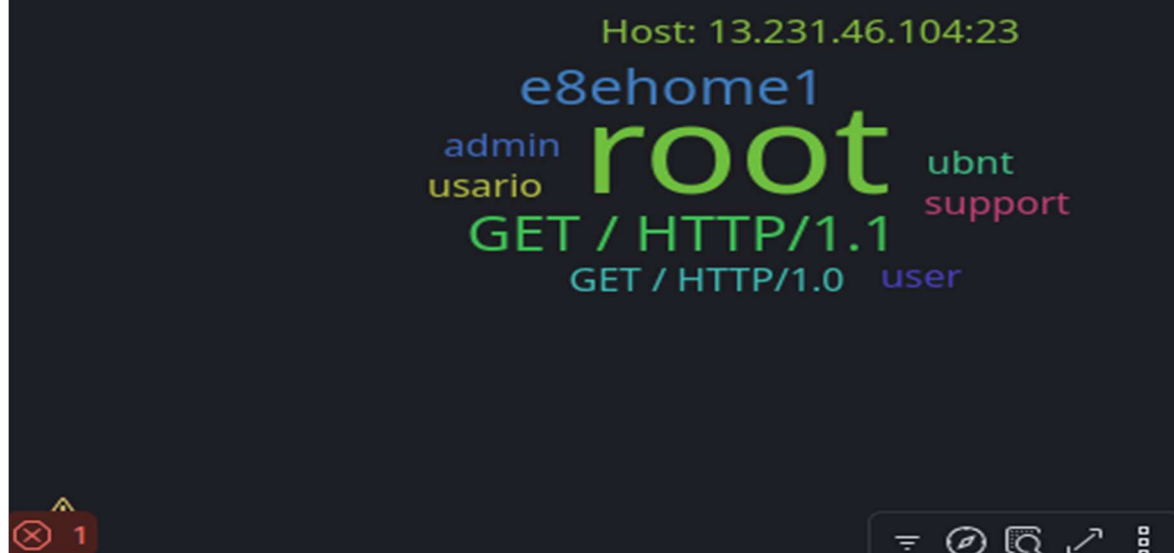


Here we can see a majority of the IPs are known attackers, which I assume is because they're from questionable countries like China or US, which made up the majority of Cowrie attacks.

- China: 29%
- United States: 20%
- India: 18%
- Brazil: 10%
- South Korea: 8%
- Russia: 5%

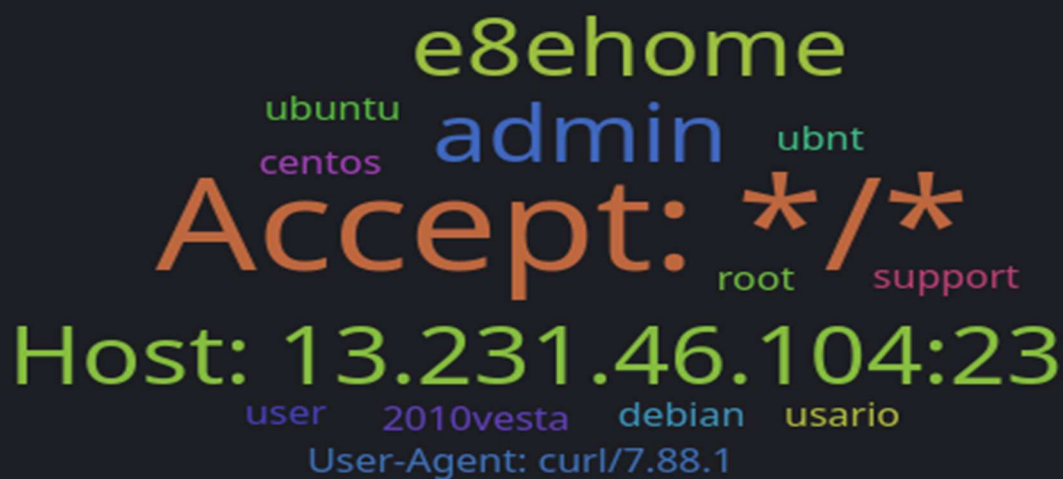


## Username Tagcloud



Here we can see the usernames used in these attacks. There's a lot more variety in the types of usernames used, including some Get requests and html, possibly to try to perform SQL injections. Most of these usernames are still predictable like root, support, admin, user.

## Password Tagcloud

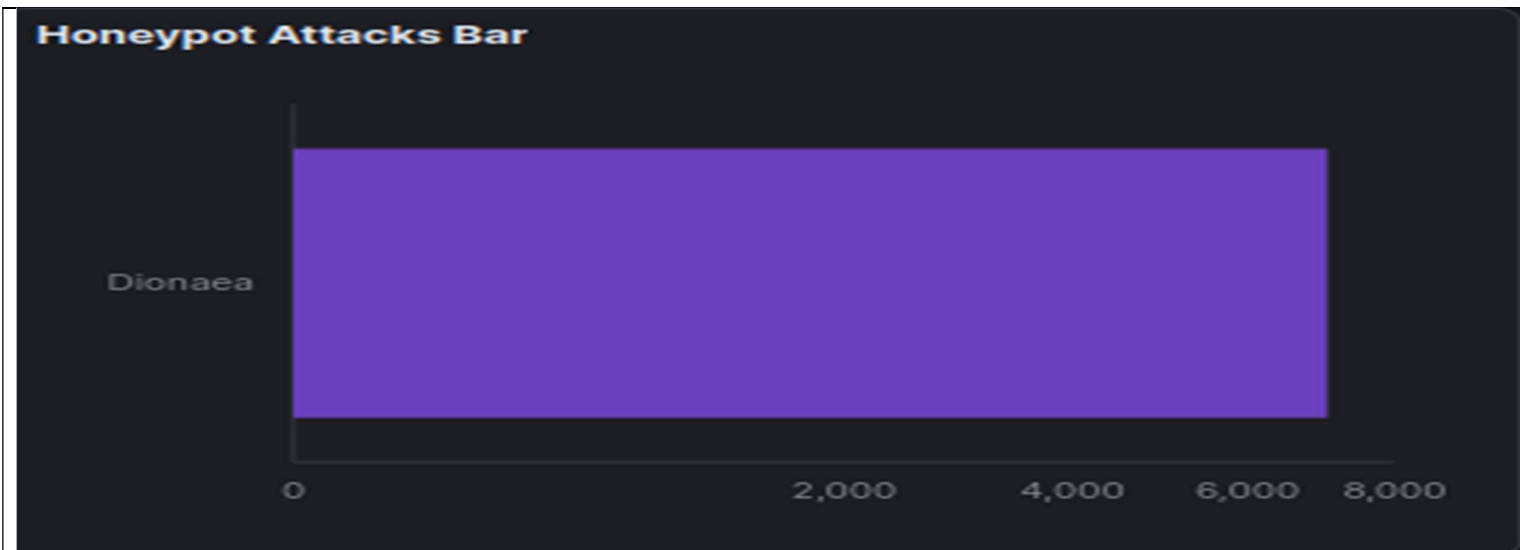


The same story occurs for the passwords too. Most of them are predictable like admin or user, but making sure your passwords are strong and you use two factor authentication is key in securing your systems from brute force or dictionary attacks.

Top 10 IP Adresses	ASN	Count	City/State	Country	ISP
191.140.13.239	28573	71	Taubate	Brazil	rede brasileira de comunicacao sa
117.215.61.152	9829	50	Bangalore	India	bharat sanchar nigam limited
59.96.197.201	No info	50	No info	No info	No info
182.252.38.24	3786	40	Dangha-dong	South Korea	ig dacom corporation
98.156.3.21	20115	36	Overland Park	United States	charter communications
91.207.115.249	48347	34	Protvino	Russia	Aleksandr bezzubov
196.251.83.136	328704	29	Victoria	Seychelles	secure internet limited
112.51.49.88	56042	26	Xiucun	China	china mobile communiucations corporation
3.16.139.93	16509	26	Columbus	United States	amazon technologies inc
122.97.214.161	17621	26	Daguang	China	china unicom jigangsu province network

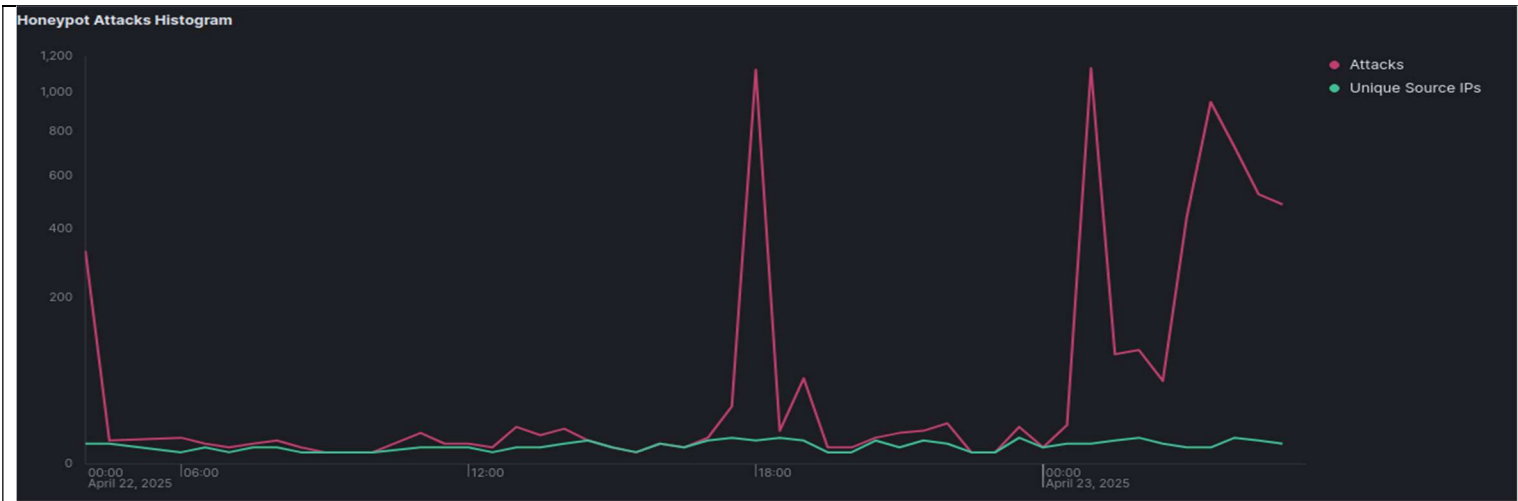
The IP addresses associated with the attack traffic show a notable concentration in specific countries, including Brazil, India, Russia, China, and the United States. Interestingly, we observe cases where IPs from distinct geographic regions share the same Autonomous System Number (ASN), such as 191.140.13.239 (Brazil) and 98.156.3.21 (United States) both being associated with major telecommunications providers (AS28573 and AS20115 respectively). A particularly curious case is 91.207.115.249 in Russia, which shows an individual (Aleksandr Bezzubov) as the ISP (AS48347) - an unusual pattern for attack traffic. Additionally, a significant portion of malicious traffic originates from AS16509 (Amazon Technologies), suggesting potential abuse of cloud infrastructure. The geographic distribution combined with these ISP patterns could indicate either legitimate regional operations of large providers or potentially malicious actors leveraging distributed infrastructure to obscure their origins. The presence of an IP with no ASN or geographic information (59.96.197.201) further complicates attribution, potentially representing deliberate obfuscation attempts. These patterns warrant deeper investigation to determine whether they represent coordinated malicious activity abusing global infrastructure or simply reflect the natural distribution of these large service providers.

### Dionaea:

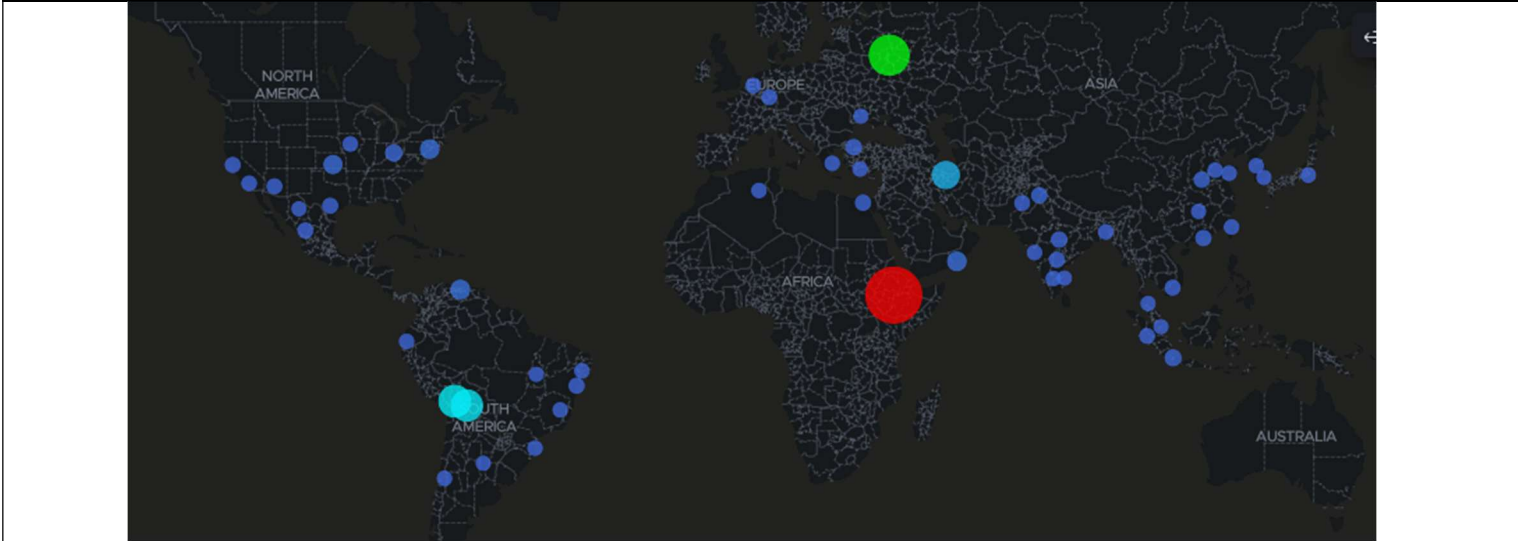


There were 6445 attacks from 123 unique IPs.



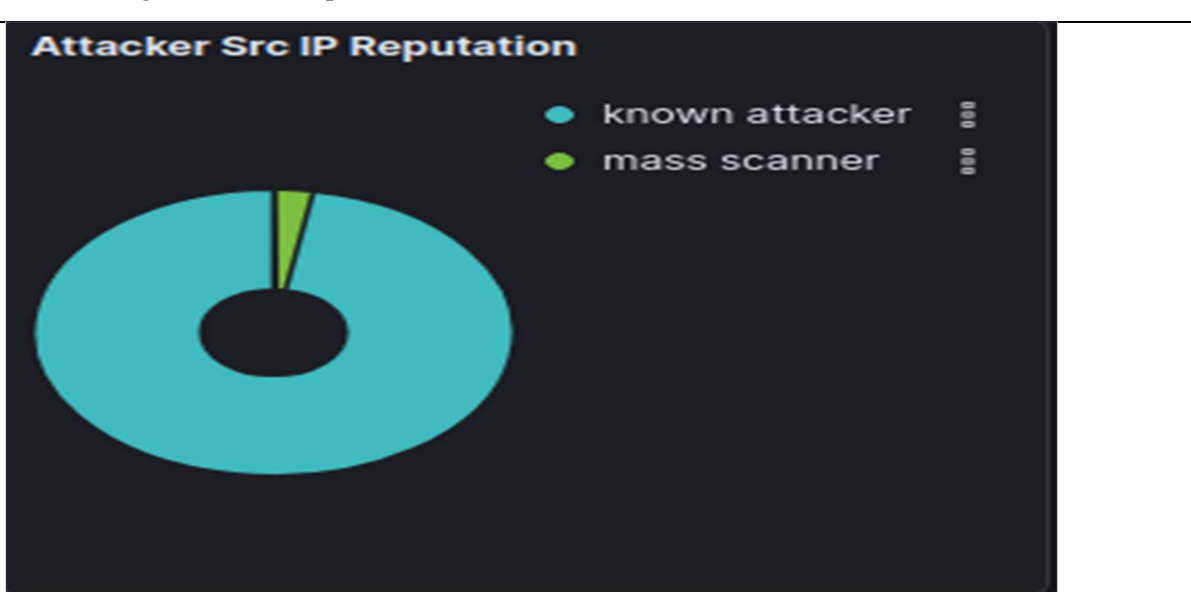


These attacks spiked at 4 am, 17:30-18:00-, 00:30-1:00, and, 03:00-04:30..

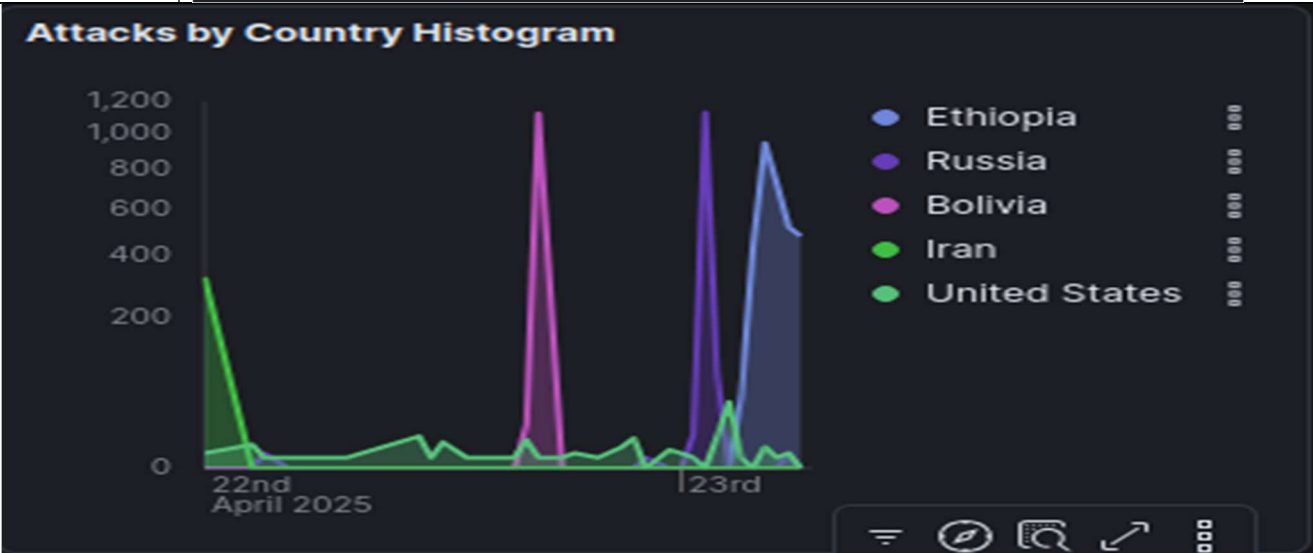
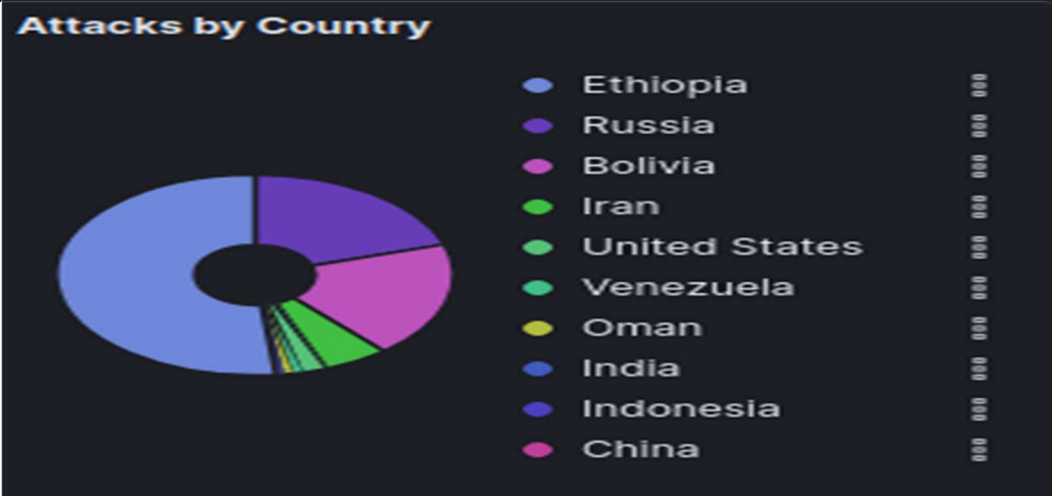


The bulk of these honeypot attacks originated in Ethiopia , Russia , Bolivia and India.

97% of these attacks were from known attackers, and 3% were from mass scanners.

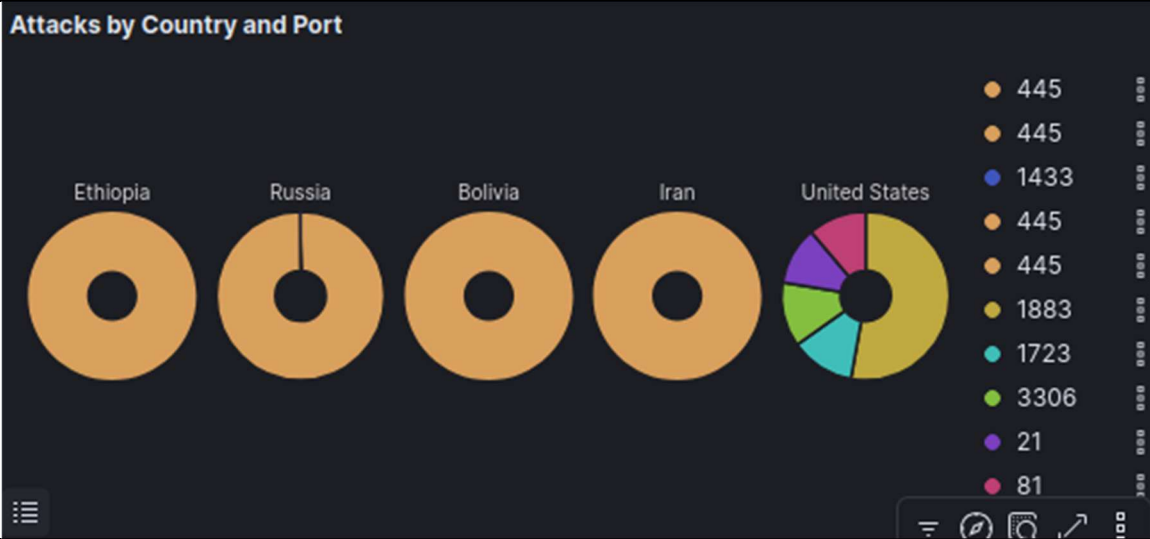


Most attacks originated from Ethiopia: 52%  
Ruusia: 20%  
Bolivia: 19%  
Iran: 5%  
United states: 2%  
Venezuela:1%



We can see that each of the spikes in attacks corresponds to a specific country, which is interesting and may show that these scans occur in waves or at specific times.

We can also see like for most of the honeypots, the port attacked is mainly 445, or https, which makes sense since the instance is hosted in the cloud.



There were a lot less usernames recorded since this honeypot is not specifically geared towards that but it still includes some predictable **ones**.



For both usernames and passwords, the most prevalent was just a lack of input.



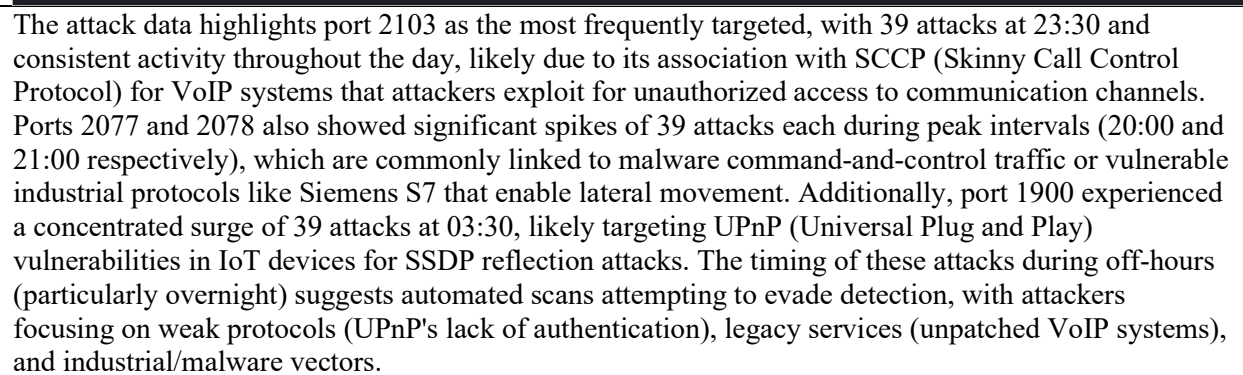
Top 10 IP Adresses	ASN	Count	City/State	Country	ISP
196.190.222.242	24757	3146	Addis Ababa	Ethiopia	ethio telecom
85.192.171.116	12389	1207	Orenburg	Russia	pjsc rostelecom
200.105.196.189	28081	587	La Paz	Bolivia	axs bolivia s. a.
181.115.190.30	6147	379	La Paz	Bolivia	entel s.a. - entelnet
78.38.0.90	44244	325	Tarbz	Iran	iran information technology company pjsc
201.242.102.92	8048	47	El Tigre	Venezuela	cantv servicious venezuela
85.154.180.132	24835	46	Salalah	Oman	omantel
157.245.93.207	14061	39	North Bergen	United States	digital Ocean inc
3.140.246.154	16509	11	Colombus	United States	Amazon technologies inc.

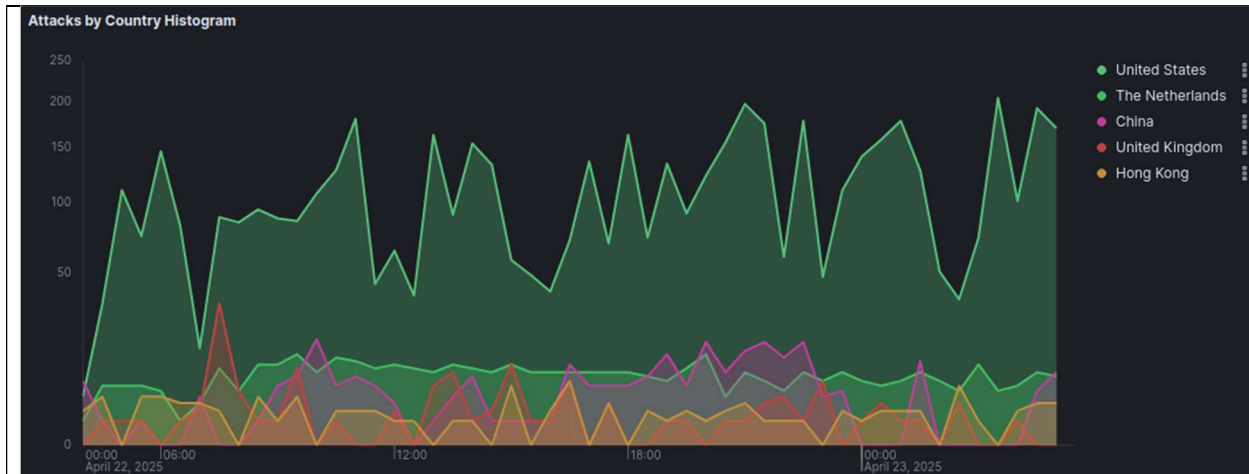
Here we can see that basically the same amount of attacks came from Mexico, Taiwan, India, and Columbia, the same culprits that we saw in the overall T-Pot dashboard. These are definitely IPs to flag, and check if there are actually legitimate connections coming from these geographical regions.

Overall this honeypot didn't give me a whole lot of information that I didn't already know, which makes sense since this is a low interaction honeypot. I gleaned a lot more from the other honeypots, especially Cowrie.

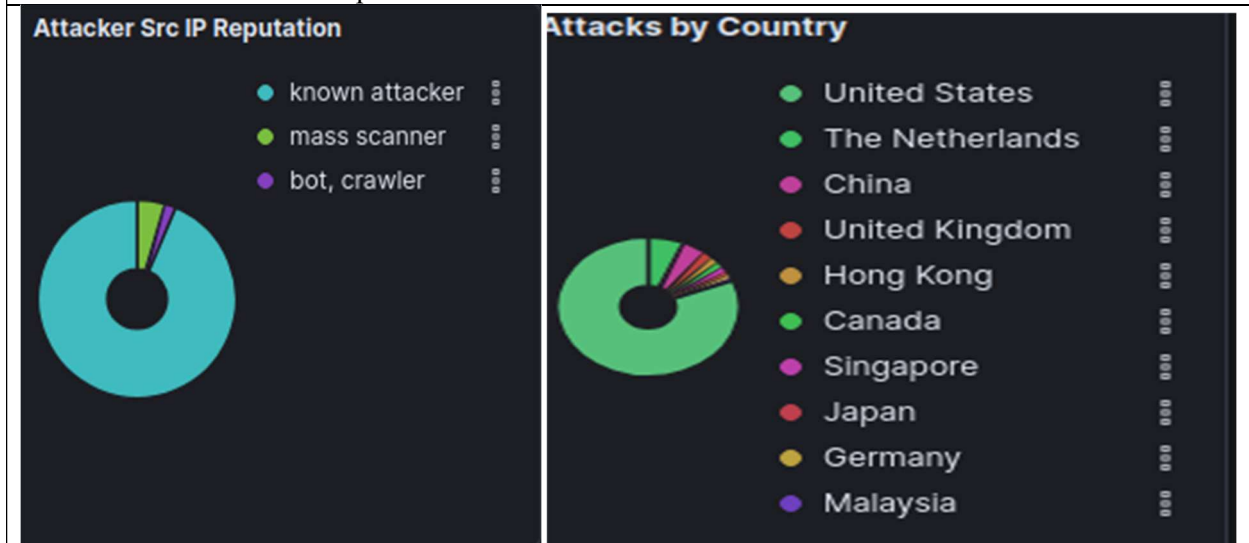
### Honeypot Attacks Bar

Attack Type	Count
Honeytrap	7,800





In contrast to other honeypots, the vast majority of attacks are domestic, with the United States remaining a constant source of attacks during the entire 24 hour time period. Other countries like The Netherlands or China have spikes but never to the level of the US.



Adding on to that, most of the attackers are known or mass scanners, and the US takes up a whopping 81% of the attacks, followed by The Netherlands, and China.

Top 10 IP Adresses	ASN	Count	City/State	Country	ISP
45.33.33.185	63949	117	Fremont	United States	linode llc
18.217.128.63	16509	111	Colombus	United States	Amazon technologies inc
52.15.176.212	16509	66	Colombus	United States	Amazon technologies inc
18.117.99.85	16509	57	Colombus	United States	Amazon technologies inc
3.141.37.46	16509	51	Colombus	United States	Amazon technologies inc
3.7.193.14	16509	50	Colombus	United States	Amazon technologies inc
13.58.84.7	16509	47	Colombus	United States	Amazon technologies inc
18.224.63.82	16509	45	Colombus	United States	Amazon technologies inc
3.129.148.131	Unknown	44	Unknown	Unknown	Unknown
13.59.107.126	16509	41	Colombus	United States	Amazon technologies inc

Analysis of the honeypot data reveals that the majority of attacking IP addresses originate from cloud infrastructure in the United States, with eight of the top ten IPs belonging to Amazon Web Services (AS16509) and located in Columbus, Ohio - Amazon's US-East-2 cloud region. The remaining two IPs include one from Linode LLC (AS63949) in Fremont, California and one with unknown ASN/geolocation information. This concentration in U.S.-based cloud infrastructure suggests either

compromised cloud instances being used for attacks or scanning activity originating from these providers. The presence of multiple IPs sharing the same ASN (AS16509) and geographic location (Columbus) indicates this is likely legitimate AWS infrastructure rather than spoofing, though the unknown IP (3.129.148.131) with no ASN or location data warrants investigation as potentially malicious traffic attempting to obscure its origin. The data highlights how attackers increasingly leverage major cloud providers' infrastructure, making attribution more challenging while enabling global attack distribution from centralized locations.

## Problems Encountered:

I did encounter a few problems, mainly with extracting the data from the Elasticview servers. They are very finicky with the wording of requests. Another problem is cost, this server costs quite a bit, as 24 cents per hour adds up to \$5.76 a day, and it quickly adds up.

## Conclusions:

Over the 24-hour monitoring period, the T-Pot honeypot captured a wide range of cyberattacks, revealing important patterns about where, when, and how hackers operate. The data shows that attackers frequently target weak or outdated systems, with many attacks coming from cloud services and specific high-risk regions. The U.S., Ethiopia, Russia, and Bolivia were the top sources of malicious activity, each showing different attack behaviors. For example, the U.S. had a steady stream of attacks, while Ethiopia and Russia had sudden spikes in activity, likely from automated scans or botnets.

The most common attacks focused on exploiting old vulnerabilities in systems like Windows (CVE-1999-0265) and OpenSSL (CVE-2021-3449), as well as brute-forcing weak passwords on services like SSH and Telnet. Many attackers also scanned for exposed cloud services, IoT devices, and industrial systems, looking for unsecured ports or misconfigurations. Notably, a large number of attacks originated from Amazon Web Services (AWS) and Linode IPs, suggesting that hackers are increasingly using cloud platforms to hide their activities.

## Recommendations

To defend against these threats, organizations should prioritize patching known vulnerabilities, especially in older systems. Strong passwords and multi-factor authentication (MFA) should be enforced for remote access services like RDP and SSH. Blocking traffic from high-risk regions and suspicious IP ranges (such as those linked to Ethio Telecom or Rostelecom) can also reduce exposure. Additionally, monitoring unusual port activity—particularly on ports 445 (SMB), 2103 (VoIP), and 1900 (UPnP)—can help detect attacks early.

## Future Trends

Looking ahead, attackers will likely continue abusing cloud infrastructure to launch attacks while avoiding detection. IoT devices and industrial systems remain prime targets due to weak security controls. Regions with less strict cybersecurity laws, such as Ethiopia and Bolivia, may see even more malicious activity. To stay protected, businesses should adopt proactive security measures, including regular

vulnerability scans, threat intelligence sharing, and honeypot deployments to study emerging attack methods.

**Final Thoughts**

This honeypot experiment provided valuable insights into real-world cyber threats, but managing costs and refining data analysis remain challenges. The findings highlight that attackers exploit both old weaknesses and modern misconfigurations, meaning security teams must stay vigilant across all systems. By learning from these attack patterns, organizations can better defend against evolving threats.