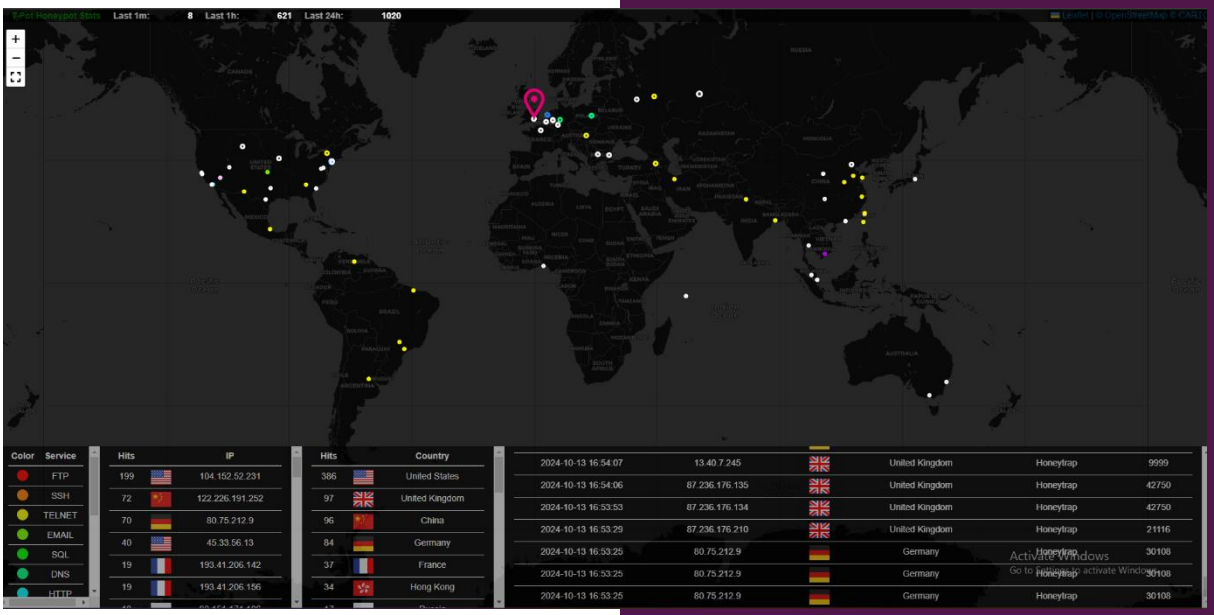
Cyber Threats: Analyze Attack Patterns



K Moreki

10/14/2024

Table of Contents

Introduction

Honeypots are designed to attract and monitor malicious activities by simulating vulnerable systems. They act as decoys to lure attackers, allowing cybersecurity professionals to study intrusion techniques and understand attacker behaviour and gather intelligence on evolving threats without exposing actual production systems to risk.

For this paper, I will be setting up a T-Pot honeypot, an advanced multi-honeypot platform, on a virtual machine (VM). The purpose of this setup is to intentionally create an environment that appears vulnerable to attackers, thereby inviting real-world attacks. Once the honeypot is operational, my VM will likely become a target for various types of cyberattacks. I will assess these attacks to gather insights into several key areas:

-**Origins of the attacks**: By analysing the incoming traffic, I will determine where the attacks are originating from, providing a geographical or network context for threat actors.

-**Attack vectors and methodologies**: I will study how the attackers managed to infiltrate the system, including the vulnerabilities they exploited, their access methods, and any patterns of intrusion.

Threat actor motives: Part of the research will involve assessing what the attackers are seeking. Whether they are attempting to steal data, compromise the system for control, or use it for launching further attacks, understanding their goals will provide valuable insights.

Attacker behaviour after infiltration: By closely examining the commands executed by the attackers after gaining access, I will be able to understand their tactics, techniques, and procedures. This includes the commands they run, the files they access or any backdoors they attempt to install.

Through this research, I aim to gain a comprehensive understanding of how threat actors operate in real-world scenarios. This will not only shed light on current cyberthreat trends but also provide practical knowledge on defensive strategies. Additionally, the results of this project will contribute to broader cybersecurity efforts by offering data that can help improve detection, prevention, and response mechanisms.

Methodology

Setup

- Signed up for AWS services and used EC2 to run instances. Using Ubuntu as my virtual machine running on the highest specifications to handle the platform capabilities.
- Saved a private key on my personal computer in order to ssh to connect to the instance on my computer
- Connected to the instance and ran commands to install GitHub to be able to further install T-Pot on the machine
- After installation I configured the security group traffic on AWS to make the machine vulnerable by allowing all IPs to access the below ports and configured some ports for me to access the admin side of the platform

Security group rule...	IP version	Type	Protocol	Port range	Source	Description
sgr-093b508fa604e6259	IPv4	Custom TCP	TCP	64297	[redacted]	T-Pot Management: SSH
sgr-0f53c6262ed144216	IPv4	Custom TCP	TCP	64295	[redacted]	T-Pot Management: SSH
sgr-00655e5fa38215e08	IPv4	Custom TCP	TCP	0 - 64000	0.0.0.0/0	TCP for Attacker
sgr-0911141c5bebfd419	IPv4	Custom UDP	UDP	0 - 64000	0.0.0.0/0	UDP for Attacker

After configuration I used the instance Ip address to access it on google chrome followed by the port number required to access the management area of the honeypot

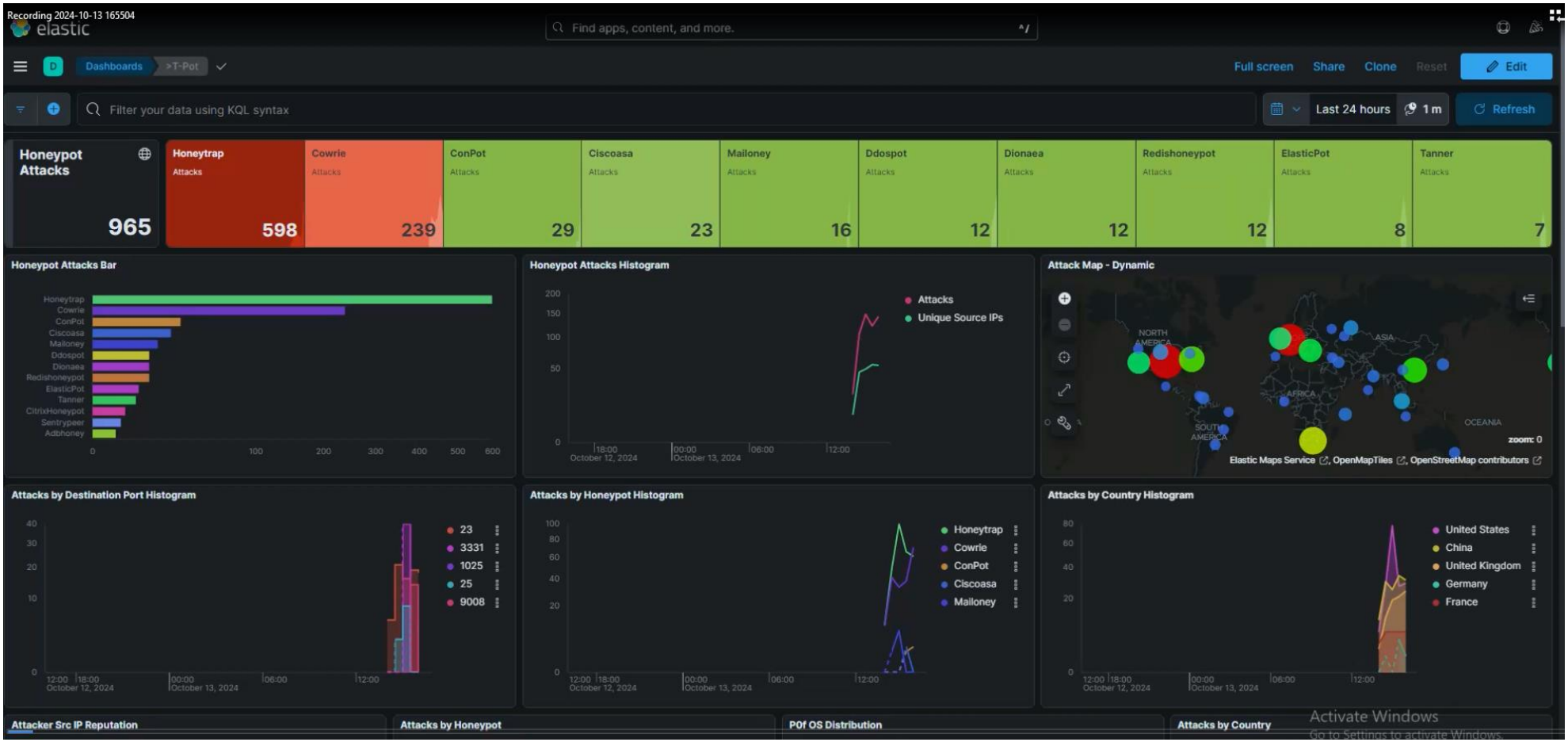
Tools of analyses

After setting up the T-Pot honeypot tool on a virtual machine (VM), I accessed Kibana to analyse and visualize the attacks. Kibana is an open-source data visualization and exploration tool designed to work with Elasticsearch. It allows users to create dynamic dashboards and reports based on real-time or historical data.

By using Kibana, I was able to view detailed logs from the honeypots, showing insights into each attempted attack. These visualizations helped track where the attacks were originating, which ports were being targeted, and the specific commands or actions taken by the threat actors after accessing the VM. This information is crucial in understanding the tactics and techniques used by attackers, allowing for better defensive strategies in cybersecurity.

Results

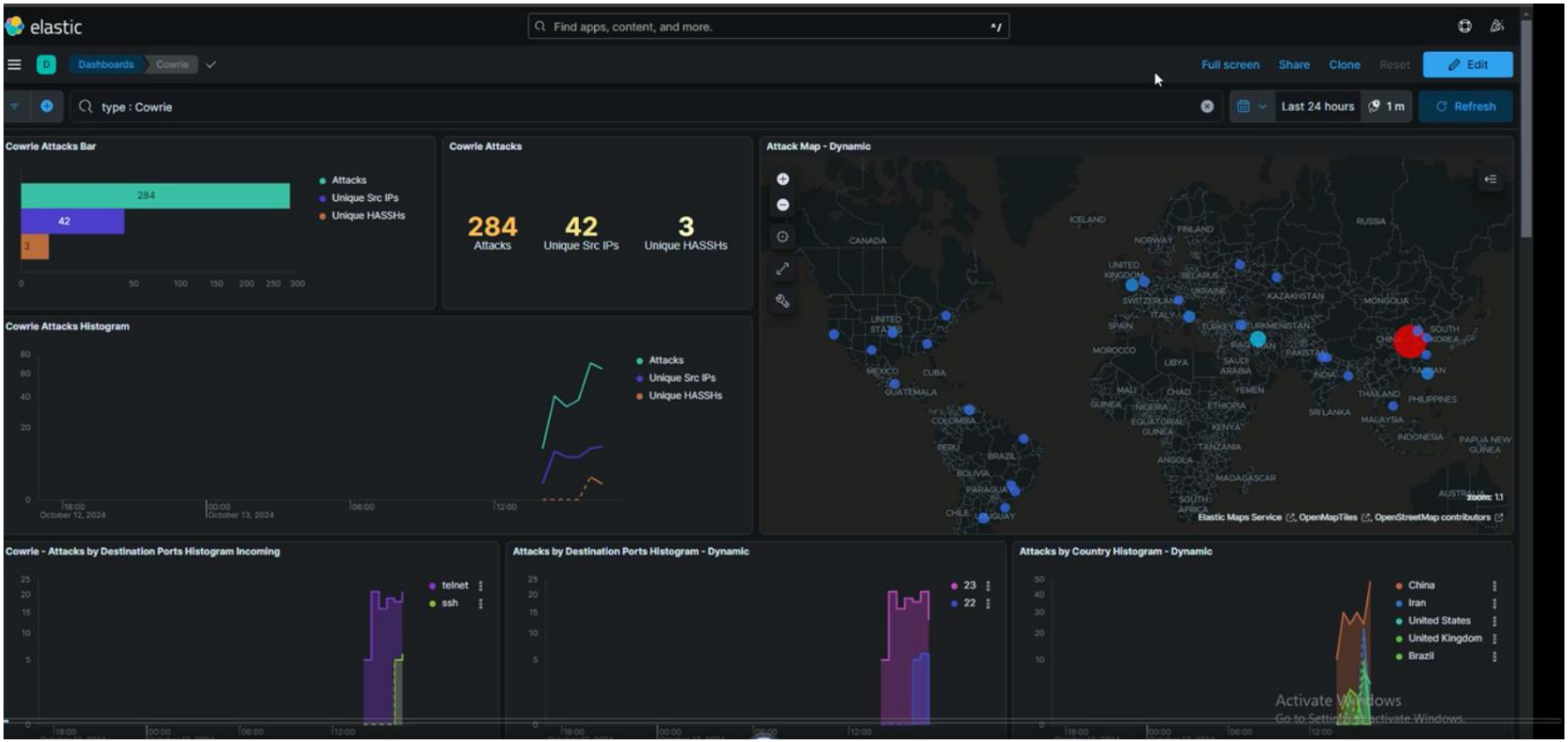
Upon opening Kibana you can instantly see a visual representation of of the amount of attacks for the honeypot and all kinds of pots the platform is running, the image below illustrates the number of attacks within one hour of the machine being public for infultration



Cowrie

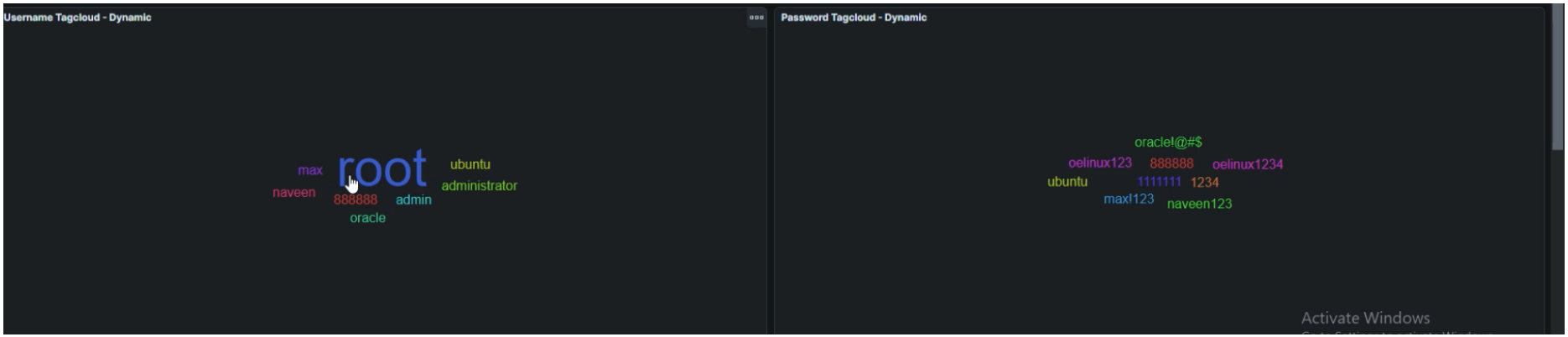
Cowrie is a popular open-source honeypot used to simulate a vulnerable SSH or Telnet service. It is designed to deceive attackers by emulating a realistic environment that mimics a legitimate system, allowing researchers and security professionals to capture and analyse the actions of threat actors.

By the illustration below it is shown that there were 284 attacks on our SSH service coming from 42 unique Ips, with the amount of time the platform ran and number of attacks it is assumed these attacks are automated



Most the attacks appear to have come from China and more of them came from the country. The first few minutes of the platform ran they all started in China and continued to increase as time went on

The image below shows a graph highlighting the most commonly used usernames and passwords attackers used to brute force their way to the system, root being the most used username attempt from attackers



Analyses

- The usernames attackers were using were targeting administrative accounts with the most frequent being “Root” which is primarily the most common username for the superuser in a linux machine
- Followed by the usernames such as “administrator” which is the most common administrator username
- The passwords all seem to to be using rainbow table passwords that are related to the machine they were trying to access

Prevention

- Ensure all superuser accounts to not have default passwords
- Make use of RBAC to ensure only specific users that are required to have access to this admin user
- Firewall rules that ensure to ensure it is taken into consideration of geolocation access control because most of the hackers came from China while the machine was hosted in London and harden IP access to not allow everyone access to the machine which is what I have done for research purposes

On the Left table you can see the top 10 autonomous systems and their count

In the middle you can see the source IP of these attacks and the number of attacks within the hour. One of the IPs having 154 within an hour concludes that these attacks where autonomous.

One the far right you can see the commands used after infultrating the SSH service which will be analysed

Attacker AS/N - Top 10 - Dynamic

AS	ASN	Count
4134	Chinanet	177
58224	Iran Telecommunication Com	22
135377	UCLOUD INFORMATION TECI	10
3462	Data Communication Busines	7
48090	Pptechnology Limited	7
8048	CANTV Servicios, Venezuela	6
9829	National Internet Backbone	6
7303	Telecom Argentina S.A.	4
14987	RETHEMHOSTING	4
24444	Shandong Mobile Communica	4

Rows per page: 10 1

Src IP - Top 10 - Dynamic

Source IP	Count
122.226.191.252	154
93.118.104.33	22
182.242.224.196	17
165.154.174.27	10
195.178.110.65	7
104.152.52.231	4
181.164.122.179	4
104.45.233.173	3
104.248.204.195	2
106.41.83.11	2

Rows per page: 10 1

Cowrie Input - Top 10

Command Line Input	Count
shell	2
system	2
/bin/busybox MEBFD	1
cat /proc/mounts; /bin/busybox MEBFD	1
cd /dev/shm; cat .s || cp /bin/echo .s; /bin/bu	1
dd bs=52 count=1 if=.s || cat .s || while read	1
enable	1
rm .s; exit	1
sh	1
tftp; wget; /bin/busybox MEBFD	1

Rows per page: 10 1

Activate Windows
Go to Settings to activate Windows.

Analyses

Using the Feodo Tracker I scanned the AS with the highest count (4134) and discovered they were using malware called Qakbot, which has backdoor capabilities and is primarily used to steal credentials. It is also revealed this attack comes from China

It also revealed the same results for AS:7303 , it appears only public networks could be scanned hence these two it was easier to retrieve the information and for both instances it was qakbot malware

Qakbot features

- Monitoring keystrokes and sending the logs to attacker-controlled systems
- Enumerating system files to identify stored password hashes
- Searching browser password caches to steal passwords stored using the browser's autofill feature

Prevention

- Awareness training to educate users on phasing techniques
- Configure email clients to notify users when emails originate from outside the organization
- Configure Microsoft Office applications to block the execution of VBA macros
- Install and update OS patches as soon as they are available

Commands	Purpose	Attack Type	Mitigation
/bin/busybox MEBFD	BusyBox is a software suite that provides several Unix utilities in a single executable file.	DDOS	Patch Vulnerabilities
cat/proc/mounts; /bin/busybox MEBFD	Reading an executable file and plugging, seems the executable file is busybox as used before	DDOS	Detect Anomalies
cd/dev/shm cat .s || cp/bin/echo .s	Change directory to a temporary one with device files it then copies it. suppress repeated empty lines in output	DDOS (Distributed denial of service)	Restrict permissions

Key Network Events and Potential Threat Indicators

- ***SURICATA STREAM Packet with broken ack (ID: 2210051):*** This entry has the highest count at **7,512**, indicating a significant number of packets possibly pointing to a network issue or a potential attack.
- **ET DNS Query for .co TLD (ID: 2027759)**: There are **260** recorded DNS queries targeting the .co top-level domain, which might suggest unusual activity or interest in domains under this TLD.
- **ET DROP Dshield Block Listed Source group 1 (ID: 2402000)**: This indicates **224** attempts from IP addresses that are part of a blocked source group, which is a measure to enhance network security by blocking known malicious sources.
- **ET INFO Inbound HTTP CONNECT Attempt on Off-Port (ID: 2008284)**: With **200** records, this suggests attempts to connect to a web server on non-standard ports, which could indicate probing for vulnerabilities.
- **GPL ICMP Destination Unreachable Port Unreachable (ID: 2100402)**: There are **188** instances where ICMP packets indicate that destination ports are unreachable, possibly a result of misconfigured networks or attacks.

ID	Description	Count of records
2210051	SURICATA STREAM Packet with broken ack	7,512
2027759	ET DNS Query for .co TLD	260
2402000	ET DROP Dshield Block Listed Source group 1	224
2008284	ET INFO Inbound HTTP CONNECT Attempt on Off-Port	200
2100402	GPL ICMP Destination Unreachable Port Unreachable	188
2009582	ET SCAN NMAP -sS window 1024	156
2002752	ET INFO Reserved Internal IP Traffic	123
2010908	ET HUNTING Mozilla User-Agent (Mozilla/5.0) Inbound Likely Fake	88
2210041	SURICATA STREAM RST recv but no session	73
2024766	ET EXPLOIT [PTsecurity] DoublePulsar Backdoor installation communication	49

Obfuscated Attack Patterns

The table presented shows requests made to a service, with the data indicating obfuscation in the commands, suggesting potential attempts to evade detection or analysis.

The obfuscation in the commands is evident from the random strings of characters, many of which include repetitive sequences such as "AAAAAAAAAAAA" and base64-like encoding in others (e.g., "TSI1RUFSOggbXlBIVFIQuZEuMQOK9G"). This indicates that attackers might be trying to bypass detection systems by masking the true nature of their requests.

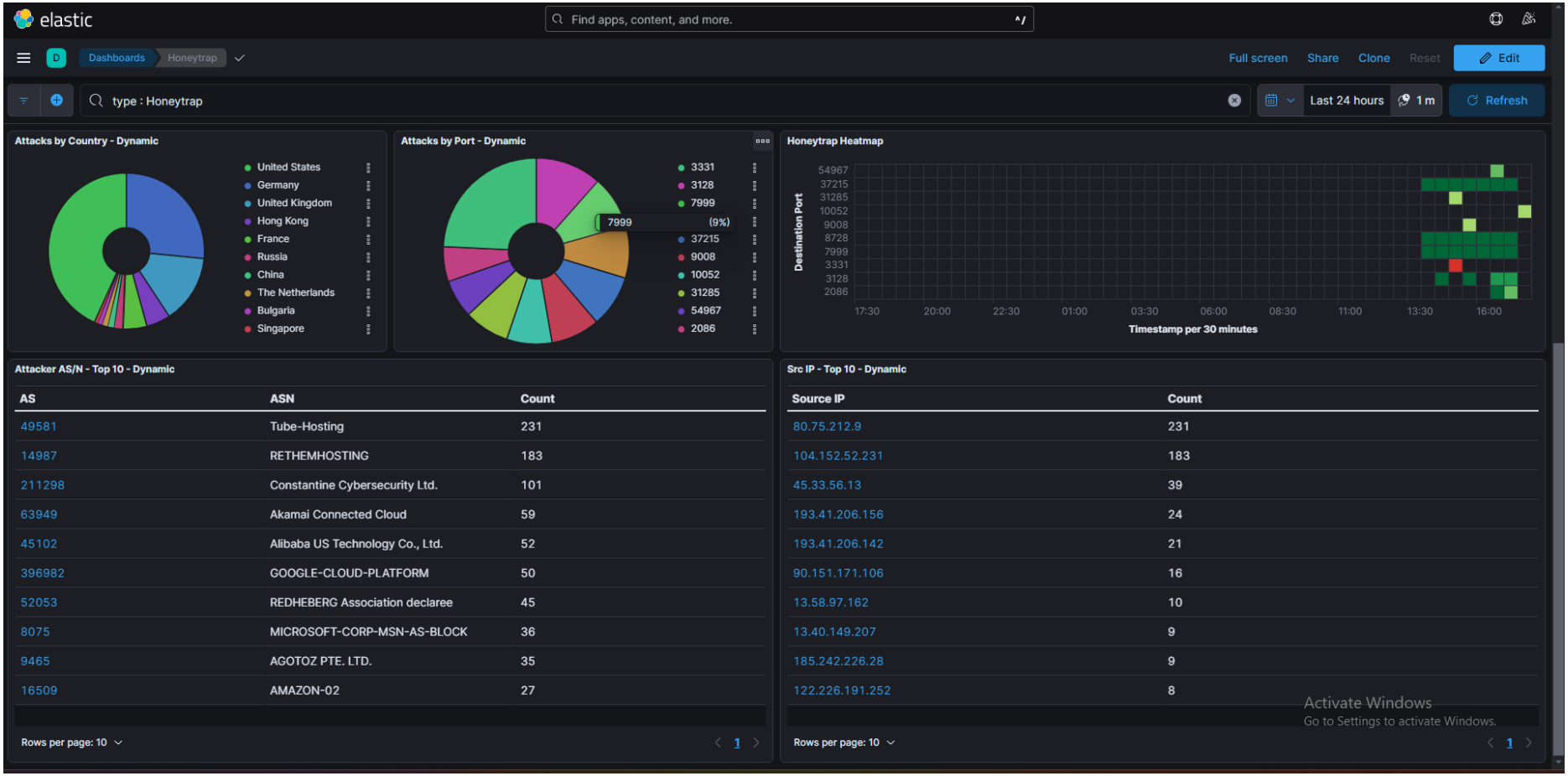
Possible Techniques Used:

- **Base64 Encoding**: The presence of strings resembling base64 encoding, such as "TSI1RUFSOggb..." suggests that the attackers could be hiding malicious scripts or commands, which might be decoded and executed once they bypass initial security layers.
- **Command Overflow**: The long sequences of "A"s (for example, "FwDAKjAAAAAAAAAAAAAAAA...") could be an attempt at buffer overflow attacks, where the attacker sends excessive data to overwhelm the system's memory allocation and potentially execute arbitrary code.
- **Target Ports**: The requests are targeting various destination ports, such as **123**, commonly associated with the **NTP (Network Time Protocol)**, and **1900**, related to **SSDP (Simple Service Discovery Protocol)**. These ports are frequently targeted by attackers for amplifying DDoS attacks or for exploiting vulnerabilities in services that may be running on those ports.

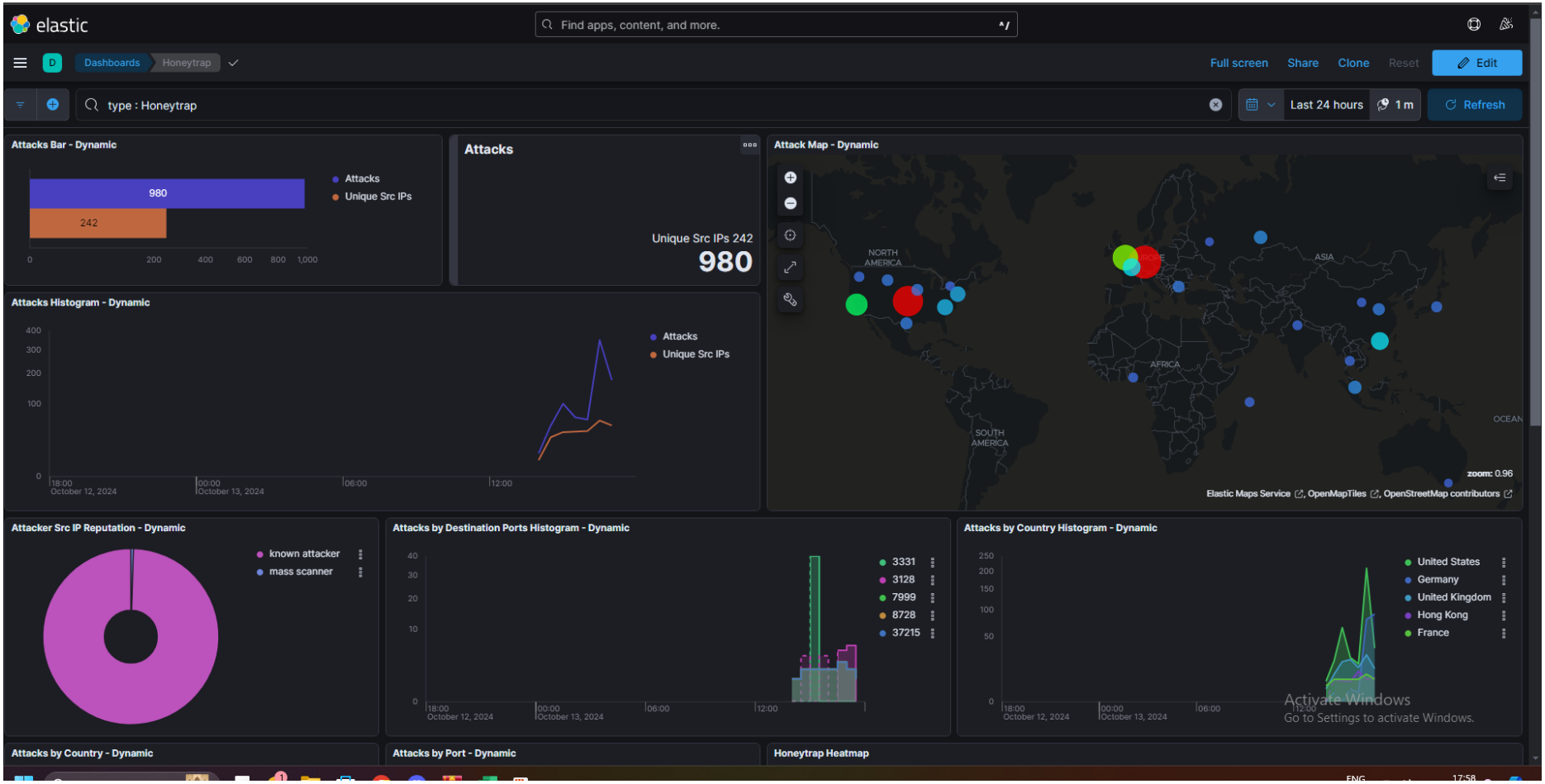

```
Request Packet,"Destination Port",Count
FwADKgAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AQ==,19,2
4wAE+gABAAAAAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAMVPI0txsVLz,123,1
FgIAAQAAAAAAAAAA,123,1
FwADKgAAAAA=,123,1
FwADKgAAAAAAAAAA,123,1
FwADKgAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA,123,1
TS1TRUFSQ0ggKiBIVFRQLzEuMQ0KSG9zdDogMjM5LjI1NS4yNTUuMjUwOjE5MDANCk1hbjogInNzZHA6ZGlzY292ZXIiDQpNWDogMw0KU1Q6IHNzZHA6YWxsDQoNCg==,1900,1
TS1TRUFSQ0ggKiBIVFRQLzEuMQ0KSG9zdDoyMzkuMjU1LjI1NS4yNTA6MTkwMA0KU1Q6dXBucDpyb290ZGV2aWNlDQpNYW46InNzZHA6ZGlzY292ZXIiDQpNWDozDQoNCg0K,1900,1
bWFzc2Nhbi10ZXN0,19,1
```

Honeytrap

High volume of attacks targeting specific countries, ports, and autonomous system numbers (ASNs). The United States and Germany are the most affected countries, while port 17215 is the most targeted port. The ASNs ABBAT, RETHEMHOSTING, and Constantine Cybersecurity Ltd. have also been involved in a significant number of attacks. The source IP 104.152.52.231 has been particularlyactive.



Below is an illustration of attacks in the honey trap. From what we can see a lot coming from USA and Germany from 980 unique source IPs



Interpretation of Results

The T-Pot honeypot setup provided valuable insights into real-world cyberattacks. Through the analysis conducted using Kibana, the following key results were observed:

1. **Origins of Attacks**: The honeypot recorded multiple attacks from various geographical locations, indicating a global spread of threat actors. This highlights the widespread nature of cyber threats, demonstrating how attacks can originate from diverse networks, possibly involving botnets or proxy networks.
2. **Attack Vectors and Methodologies**: Attackers exploited several vulnerabilities to infiltrate the system. The analysis uncovered specific patterns and tactics, such as scanning for open ports and exploiting them to gain access. This showcases common vulnerabilities that hackers target, providing crucial information on how organizations should prioritize patching and system hardening.
3. **Threat Actor Motives**: By studying the behaviour of the attackers after gaining access, it was evident that some sought to compromise the system to install backdoors or launch further attacks, while others aimed at data theft or system control. Understanding these motives offers insight into the different categories of attackers such as those seeking financial gain versus those pursuing control over systems for further exploitation.
4. **Attacker Behaviour After Infiltration**: The commands executed post-infiltration were analysed, revealing the technical approaches attackers use once inside a system. These include attempts through backdoors, exfiltration of sensitive data, and modifications to system files. The use of specific tools and commands provided a clearer understanding of how attackers operate in compromised environments.

Conclusion

The T-Pot honeypot research effectively simulated a vulnerable environment, attracting and monitoring a wide range of cyberattacks. Through this exercise, the study successfully:

- Highlighted the diverse origins of cyber threats.
- Identified common attack vectors and methodologies used by threat actors.
- Provided insight into the attackers' motives and behaviours.

These results emphasize the importance of continuous monitoring and defence in cybersecurity, as the tactics used by cybercriminals are constantly evolving. The data gathered through this research can be used to strengthen cybersecurity measures by improving detection, prevention, and response strategies. This kind of analysis is essential for anticipating future threats and developing proactive security mechanisms.

Bibliography

Wikipedia (2024) *BusyBox*. Available at: https://en.wikipedia.org/wiki/BusyBox (Accessed: 14 October 2024).

Telekom Security (2024) *T-Pot Community Honeypot Edition (T-PotCE)*. Available at: https://github.com/telekom-security/tpotce (Accessed: 14 October 2024).

Cisco Talos Intelligence Group Available at: https://talosintelligence.com(accessed 01 December 2024)

Feodo tracker from abuse Available at: https://feodotracker.abuse.ch