Hajime

And the Mainline DHT

whoami

- Kevin O’Sullivan
- Apprentice -> Network design -> Security Web Dev -> SOC analyst -> BTCERT Investigator
- National Cyber Security Centre (NCSC) Industry Analyst

1,700 customers in **180** countries.

We've got a Ringside view of **cyber threats on the network.**

We protect BT from over **125,000** cyber attacks a month.

We monitor and manage over **100,000** devices for BT and our customers.

Technology agnostic working with **20** partners and over **200** security vendors.

2,500 security practitioners.

14 follow the sun **SOCs.**

108+ registered patents and **190+** security papers.

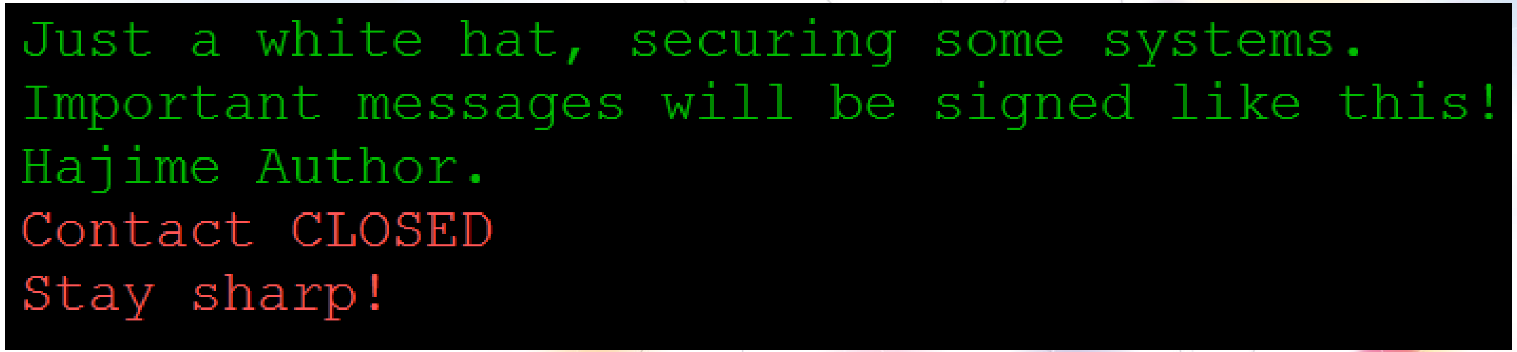
Our cyber defence operations unit provides insight ahead of and during security incidents.

Talking Points

- What is Hajime?
- Research goals
- Bit Torrent DHT – Some Background info
- Hajime's usage of Bit Torrent DHT
- Tracking Hajime Seeders/Leechers
- Hajime Remediation Trial
- Further Reading
- Q&A

Hajime?

- Discovered by Rapidity Networks in Oct 2016 [1]
- Mirai-like IoT Worm
- Scaled at ~200-300k nodes
- Decentralized via Bit-Torrent Mainline DHT



```
Just a white hat, securing some systems.
Important messages will be signed like this!
Hajime Author.
Contact CLOSED
Stay sharp!
```

[1] https://security.rapiditynetworks.com/publications/2016-10-16/hajime.pdf

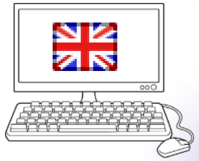
Research Goals

- Scale Hajime via Bit Torrent DHT
- Build a tracker that allow us to:
  - Identify affected BT customers
  - Monitor the botnet for growth

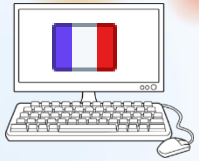
DHT
Distributed Hash Table

- Key/Value store across a number of connected devices

Key	Value
59066769B9AD42DA2E508611C33D7C4480B3857B	1.1.1.1:1001
59066769B9AD42DA2E508611C33D7C4480B3857B	2.2.2.2:2002
59066769B9AD42DA2E508611C33D7C4480B3857B	3.3.3.3:3003



Key	Value
59066769B9AD42DA2E508611C33D7C4480B3857B	4.4.4.4:4004
59066769B9AD42DA2E508611C33D7C4480B3857B	5.5.5.5:5005
59066769B9AD42DA2E508611C33D7C4480B3857B	6.6.6.6:6006



Key	Value
CFEBABC706B9BA9B1FB9D2F0A1ED7380D5D0D017	1.2.3.4:1122
CFEBABC706B9BA9B1FB9D2F0A1ED7380D5D0D017	3.4.5.6:3344
CFEBABC706B9BA9B1FB9D2F0A1ED7380D5D0D017	4.5.6.7:4455

Key	Value
59066769B9AD42DA2E508611C33D7C4480B3857B	1.1.1.1:1001
59066769B9AD42DA2E508611C33D7C4480B3857B	2.2.2.2:2002
59066769B9AD42DA2E508611C33D7C4480B3857B	3.3.3.3:3003
59066769B9AD42DA2E508611C33D7C4480B3857B	4.4.4.4:4004
59066769B9AD42DA2E508611C33D7C4480B3857B	5.5.5.5:5005
59066769B9AD42DA2E508611C33D7C4480B3857B	6.6.6.6:6006
CFEBABC706B9BA9B1FB9D2F0A1ED7380D5D0D017	1.2.3.4:1122
CFEBABC706B9BA9B1FB9D2F0A1ED7380D5D0D017	3.4.5.6:3344
CFEBABC706B9BA9B1FB9D2F0A1ED7380D5D0D017	4.5.6.7:4455

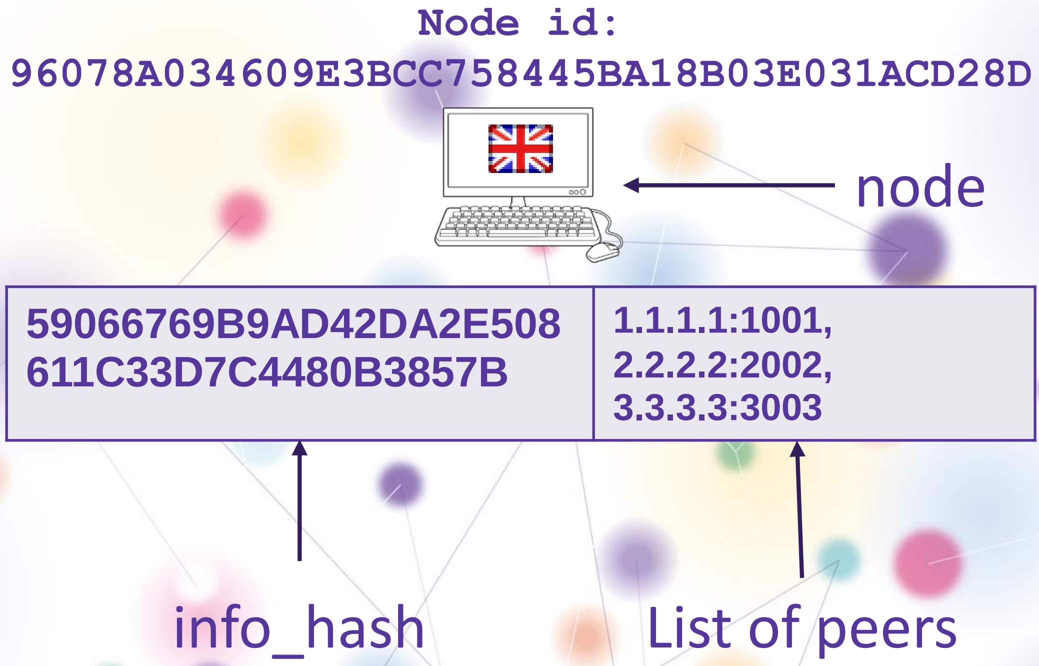
DHT

Distributed Hash Table

A "node" is a device listening on a UDP port implementing the DHT protocol

A “peer” is a device that is currently offering a file

- Each node in DHT has a 160-bit ‘node_id’
- Resources (e.g. files) tracked in DHT also given 160-bit ‘info_hash’
- Node_ids and info_hashes share a key-space



Node id:
96078A034609E3BCC758445BA18B03E031ACD28D

node

59066769B9AD42DA2E508611C33D7C4480B3857B	**1.1.1.1:1001, 2.2.2.2:2002, 3.3.3.3:3003**

info_hash

List of peers

Hajime’s Bit Torrent Usage

- Peer discovery
- Config/Module downloads via uTP (uTorrent Transport Protocol)

- New config generated daily with info_hash derived from following algorithm:
  - {Current UTC date (format D-M-Y-W-Z)}-{SHA1(filename)}

SHA1()

=

Info_hash

<u>Information</u>
D – Day of month
M – Month (0 for Jan, 1 for Feb…)
Y – Years since 1900
W – Day of the week (0 for Sun, 1 for Mon…)
Z – Number of days since Jan 01 of that year

Filename = ‘config’

How nodes find peers in DHT

‘Closeness’

96078a034609e3bcc758445ba18b03e031acd28d

⊕

5de384a9039e36923bc9758442b6a18b5372e93b1479d2a3c

=

cbe4c390d83fcf705eaf0f2874c10454c94ad540b1

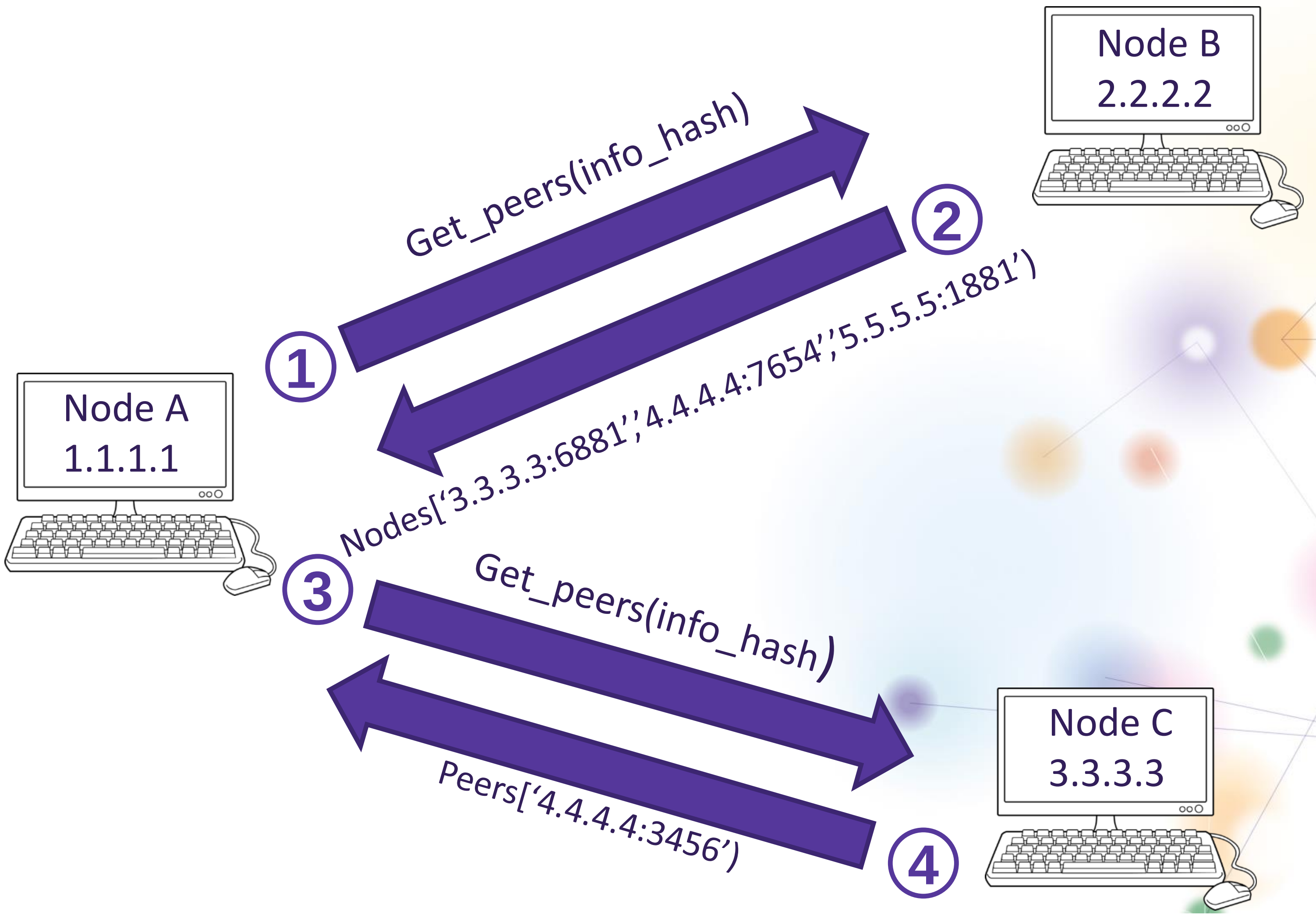
=

1164026732566366504511548603514468342761443447050420401

Not close at all

Pretty close!

How nodes find peers in DHT



1 **Node A sends a get_peers request for a resource to Node B.**
He sends the request to Node B because Node B’s Node_id is the closest Node_id to the info_hash that Node A has in his routing table.

2 **Node B doesn’t know of any peers for that info_hash.**
So he returns a list of closest nodes from his routing table that are closes to the info_hash.

3 **Node A now queries the newly acquired nodes in the same way as he did in step 1.**
In this case, Node C is queried.

4 **Node C is naturally ‘closer’ to the info_hash and therefore more likely to know of any peers for that resource.**
In this case, Node C has returned a peer – 4.4.4.4:3456.
If Node C didn’t know of any peers for the info_hash, he would return a list of closer nodes, just as Node B did earlier.

Scaling the botnet

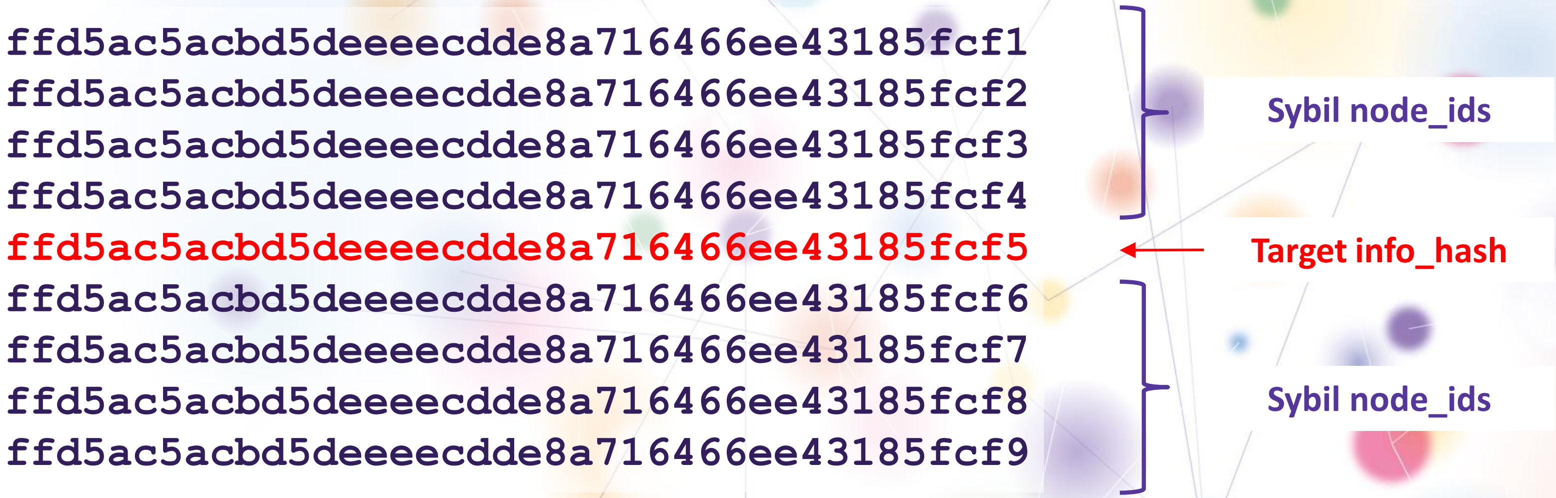
Finding Seeders

- Generate today’s config info_hash

- Generate a random 160-bit node_id for ourselves
- Perform a get_peers lookup for today’s config info_hash
- Store unique peers
- Push data into ELK (Elasticsearch, Logstash, Kibana)

Sybil Attacks

- Introduce multiple fake identities into the DHT
- Assign them node_ids close to that of a target info_hash



```
ffd5ac5acbd5deeeecdde8a716466ee43185fcf1
ffd5ac5acbd5deeeecdde8a716466ee43185fcf2
ffd5ac5acbd5deeeecdde8a716466ee43185fcf3
ffd5ac5acbd5deeeecdde8a716466ee43185fcf4
ffd5ac5acbd5deeeecdde8a716466ee43185fcf5
ffd5ac5acbd5deeeecdde8a716466ee43185fcf6
ffd5ac5acbd5deeeecdde8a716466ee43185fcf7
ffd5ac5acbd5deeeecdde8a716466ee43185fcf8
ffd5ac5acbd5deeeecdde8a716466ee43185fcf9
```

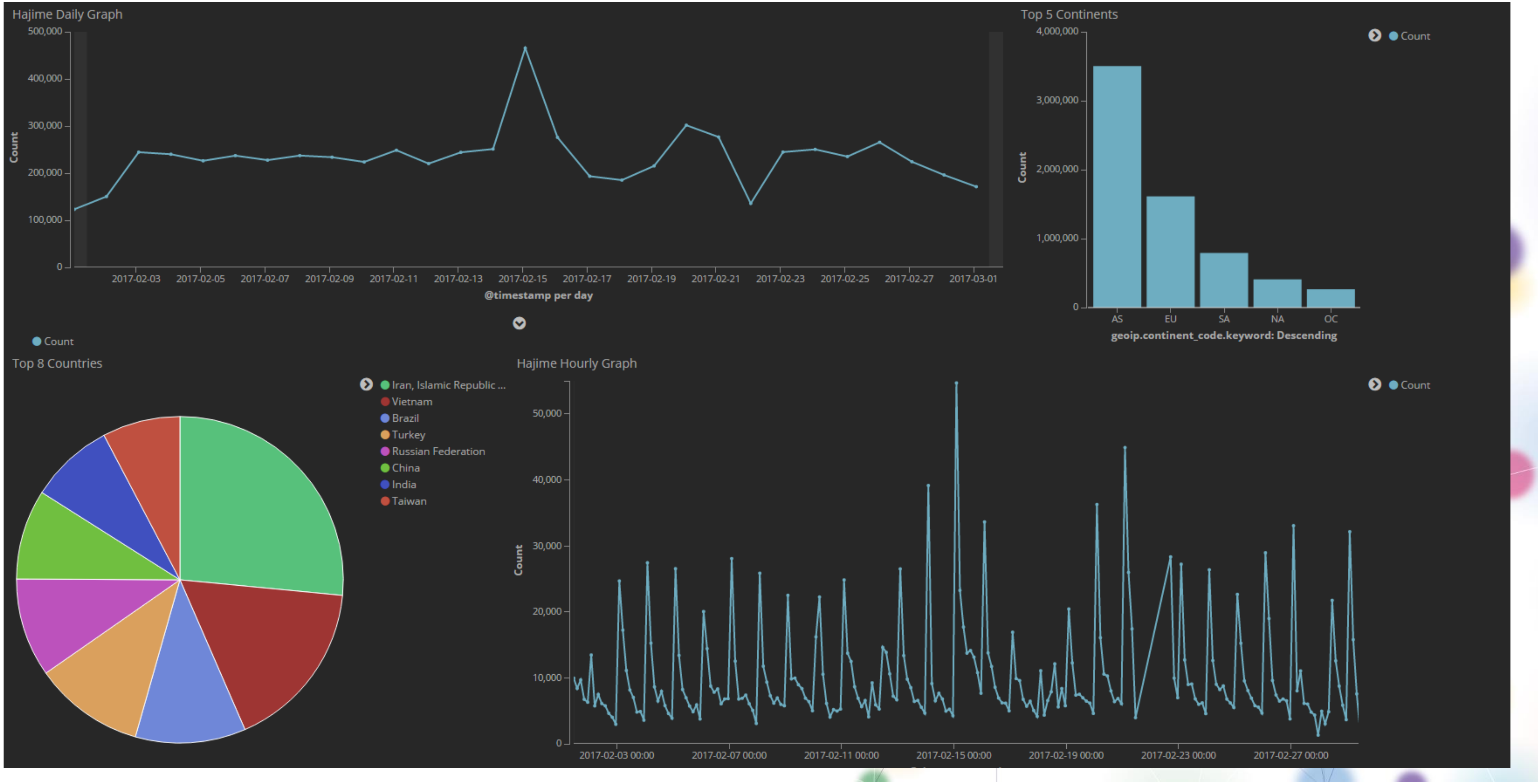
Scaling the botnet

Finding Leechers

- Generate today’s config info_hash

- Generate our node_id(s) ‘close’ to info_hash
- Sit and wait for get_peers requests to come in for today’s info_hash
- Store unique querying node IP addresses
- Push data into ELK (Elasticsearch, Logstash, Kibana)

Tracker Dashboard



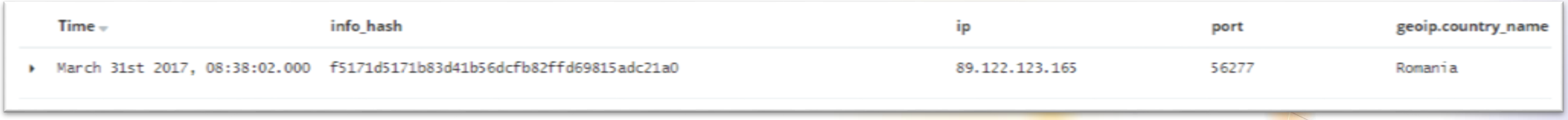
Hajime Daily Graph

Top 5 Continents

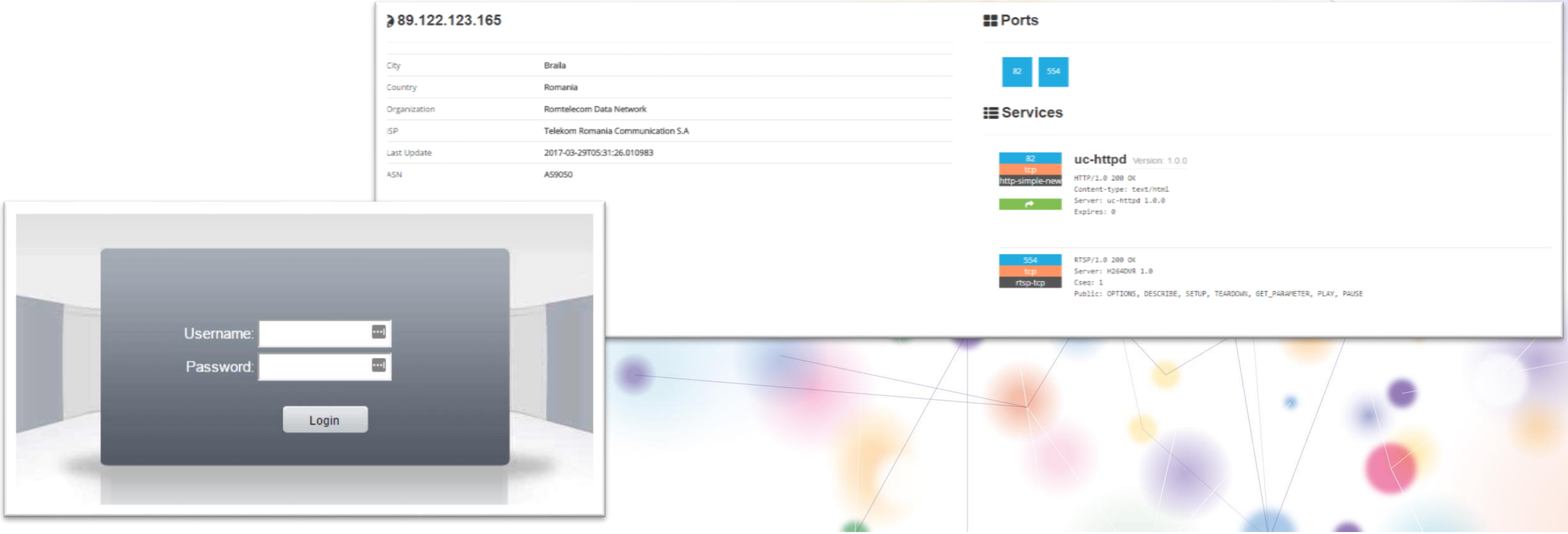
Top 8 Countries

Hajime Hourly Graph

Example peer



	Time	info_hash	ip	port	geoip.country_name
▸	March 31st 2017, 08:38:02.000	f5171d5171b83d41b56dcfb82ffd69815adc21a0	89.122.123.165	56277	Romania



89.122.123.165

City	Braila
Country	Romania
Organization	Romtelecom Data Network
ISP	Telekom Romania Communication S.A
Last Update	2017-03-29T05:31:26.010983
ASN	AS9050

Ports

Services

uc-httpd Version: 1.0.0

```
HTTP/1.0 200 OK
Content-type: text/html
Server: uc-httpd 1.0.0
Expires: 0
```

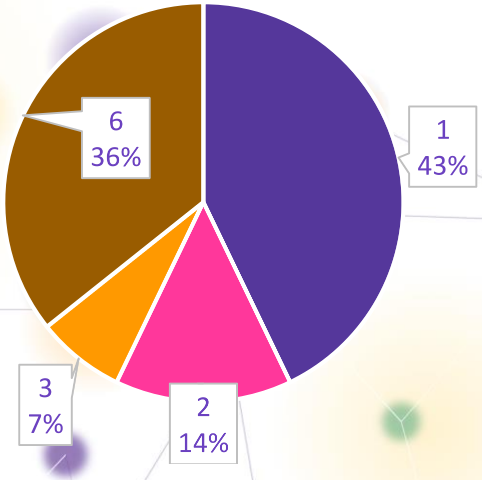
```
RTSP/1.0 200 OK
Server: H264DVR 1.0
Cseq: 1
Public: OPTIONS, DESCRIBE, SETUP, TEARDOWN, GET_PARAMETER, PLAY, PAUSE
```

Customer Remediation Trial

- 71% not found in scans since trial

- 86% of customers appreciated the feedback

How many devices (including Sound bars, DVR & IP Cameras) do you have connected to your BB connection?



Customer Feedback:

- Very happy with BT contacting them in this way
- Happy to be contacted in this manner, customer had been witnessing poor service for the last 2 weeks (ties in with virus) & has had numerous engineer visits where engineers could find no problem
- “Great”
- “Positive”
- “Very good”
- “Good”
- “Good thing”

Now what?

- Torrent poisoning attacks?
- Denial of service to Hajime configs?

Further Reading/IoCs

- Rapidity Networks Hajime write-up
  - https://security.rapiditynetworks.com/publications/2016-10-16/hajime.pdf
- Hajime follow-up binary analysis
  - https://x86.re/blog/hajime-a-follow-up/

Questions?