Abuse Situation Awareness (Introduction)

[Amman Cyber Drill/000-AbuseSA][edit]

Slideshow ^ |< << Slide 2 of 23 >> >|

The Problem?

[Amman Cyber Drill/001-The Problem][edit]

Slideshow ^ |< << Slide 3 of 23 >> >|

Lari Huttunen

education
MA in Linguistics and Computer Science

past
University of Helsinki, Finnish Police

present
Codenomicon

contact@clarifiednetworks.com

[Usual Suspect][edit]
[Amman Cyber Drill/010-The Presenter][edit]

Sub Topics for Today

- Abuse Feed Ecosystem
- AbuseHelper
- VSRoom, Virtual Situation Room

[Amman Cyber Drill/020-The Presenter][edit]

Abuse Feed Ecosystem

Feeders
: Organizations, which gather intelligence on malicious activity and identities.

Proxies
: CSIRT teams, which collect this information from various sources and report it to the cleaners.

Cleaners
: Organisations, whose customers or networks are victims of cyber crime.

[Abuse Feed Ecosystem][edit]

[Amman Cyber Drill/030-Abuse Feed Ecosystem][edit]

Feeders

hobbyist
: Various projects with varying motivations, such as ZONE-H or Malc0de.

non-profit
: Organizations such as ShadowServer, abuse.ch, Dragon Research Group or SpamHaus.

commercial
: Feed providers, such as Arbor Networks, SpamHaus Technology or Team Cymru.

[Amman Cyber Drill/035-Feeders][edit]

Proxies

government
: National CERT teams, such as CERT-FI, CERT-EE, CERT-BE, CERT-IS, CERT-AT or CERT-EU.

academic
: Various university network CSIRT teams, such as FUNET CERT in Finland.

industry
: ISP or corporate CSIRT teams, which report to their constituency, such as their corporate customers.

[Amman Cyber Drill/042-Feeders][edit]

Cleaners

- Various CSIRT teams, whose networks or customers are victims of cybercrime.
- The biggest challenge for them usually is connecting the dots between an ip address and a timestamp in an abuse report and the customer.
- Another challenge is prioritization of abuse reports into different categories.
- AbuseHelper can help in this.

[Amman Cyber Drill/045-Cleaners][edit]

And Now teh Mad Tech ;)

[Amman Cyber Drill/047-Teh Technology][edit]

Everybody's Different, Nobody’s Perfect

abuse feeds
vary in format, formalism and transports.

data
varies in integrity, availability and duplication.

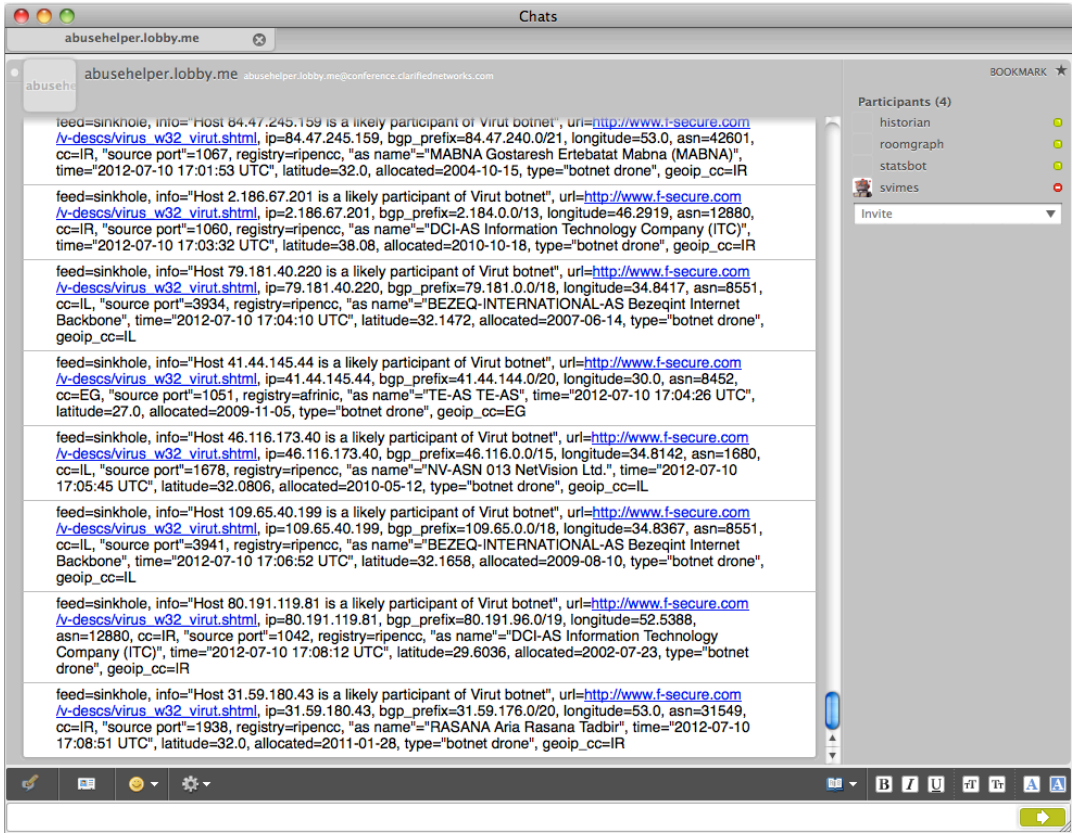
time
timespans, update frequencies, time and date formats.

ontology
provided details, schemas, terminology

[Everybody is Different - Nobody is Perfect][edit]

[Amman Cyber Drill/050-EDNP][edit]

AbuseHelper



[Amman Cyber Drill/099-AbuseHelper][edit]

AbuseHelper - Design Goals

> The initial implementation was a collaboration between CERT-EE and Clarified Networks, with the help of CERT-FI.

why

To enable you to systematically deal with abuse in your country.

botnet inspired

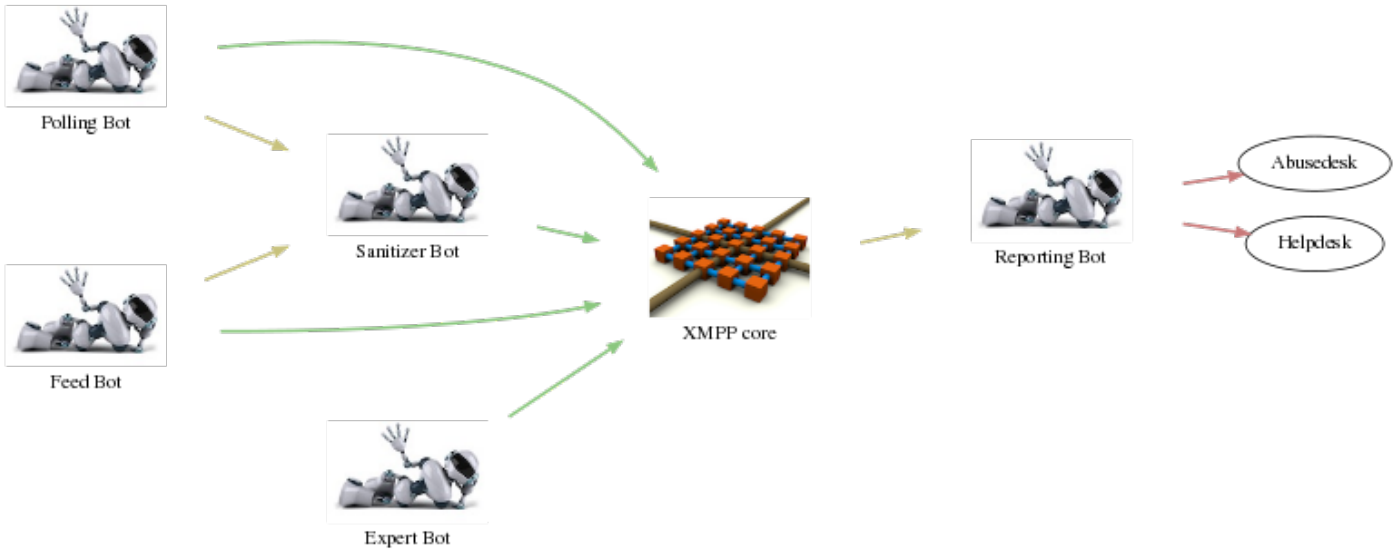
AbuseHelper is an XMPP-driven technology, a benign botnet to fight malicious botnets.

streaming architecture

Data is collected from various sources over various transports and fed through a processing pipeline to the final recipient of an actionable abuse report.

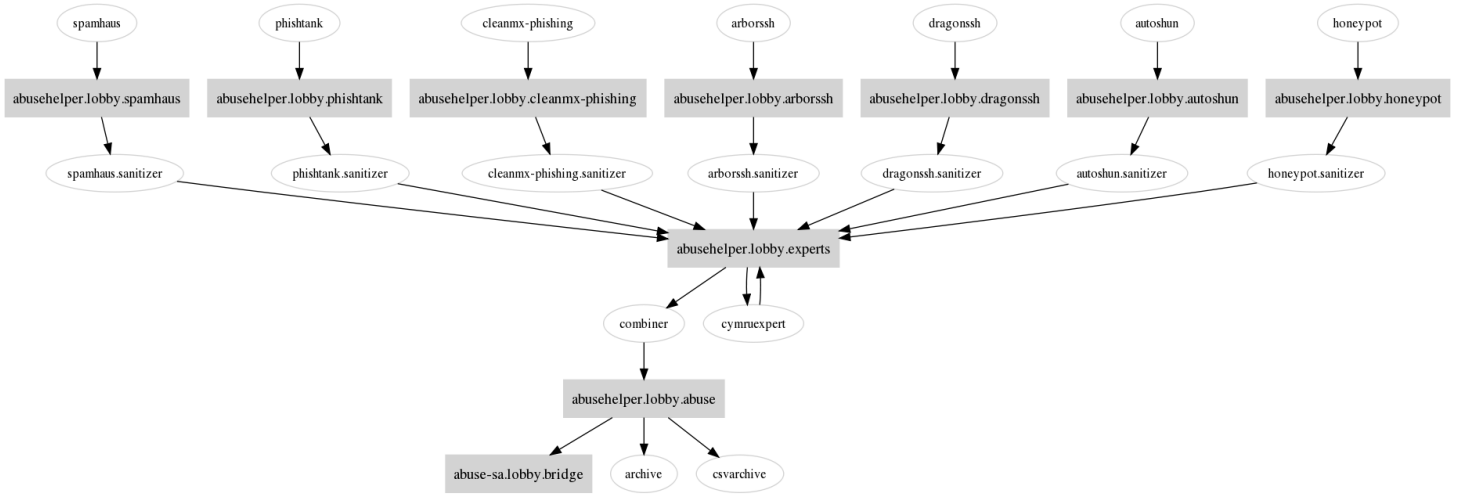
[Amman Cyber Drill/100-AbuseHelper][edit]

AbuseHelper - Bot Classes



[Amman Cyber Drill/110-Bot Classes][edit]

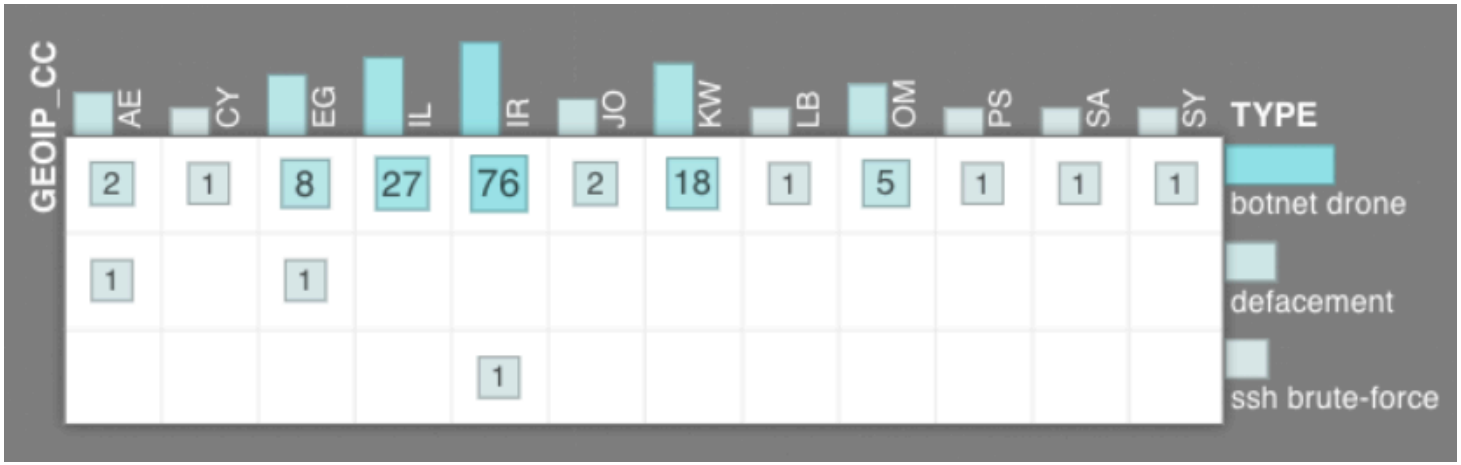
AbuseHelper - Example Botnet



[Amman Cyber Drill/120-Botnet][edit]

Slideshow ^ |< << Slide 15 of 23 >> >|

VSRoom, Virtual Situation Room



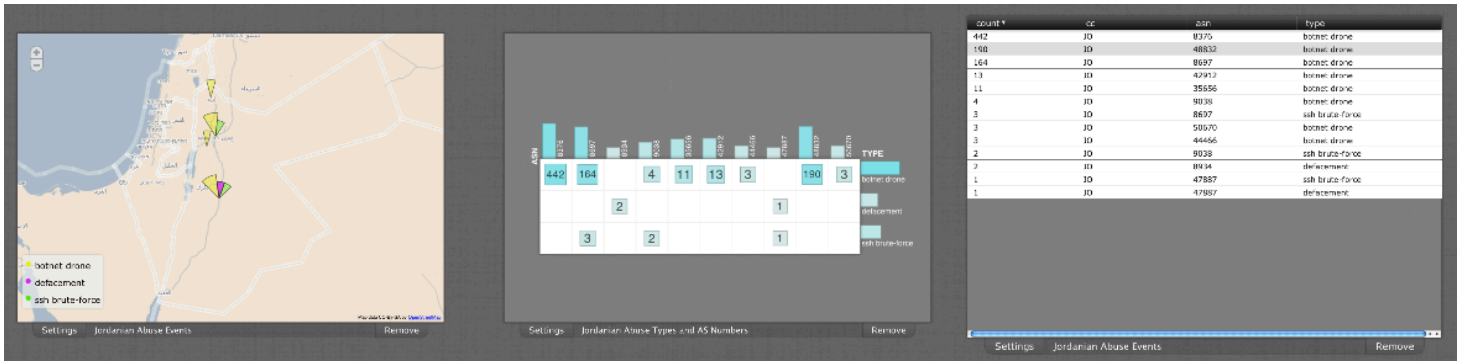
[Amman Cyber Drill/200-VSRoom][edit]

VSRoom - Design Goals

- Provide a generic browser-based user interface for visualizing XMPP event driven data.
  - Implemented in Javascript and HTML5.
  - Distinct views, view-specific and global parameters.
  - The user interface is a Javascript bot, which requests data from a historian bot.
- Enable the users to share their findings with their colleagues via VSRoom URLs.
  - Provide actionable visualizations and the ability to drill down to the level of a single abuse event.
- Visualize pre-processed and filtered data in the order of tens of thousands of events instead of millions.

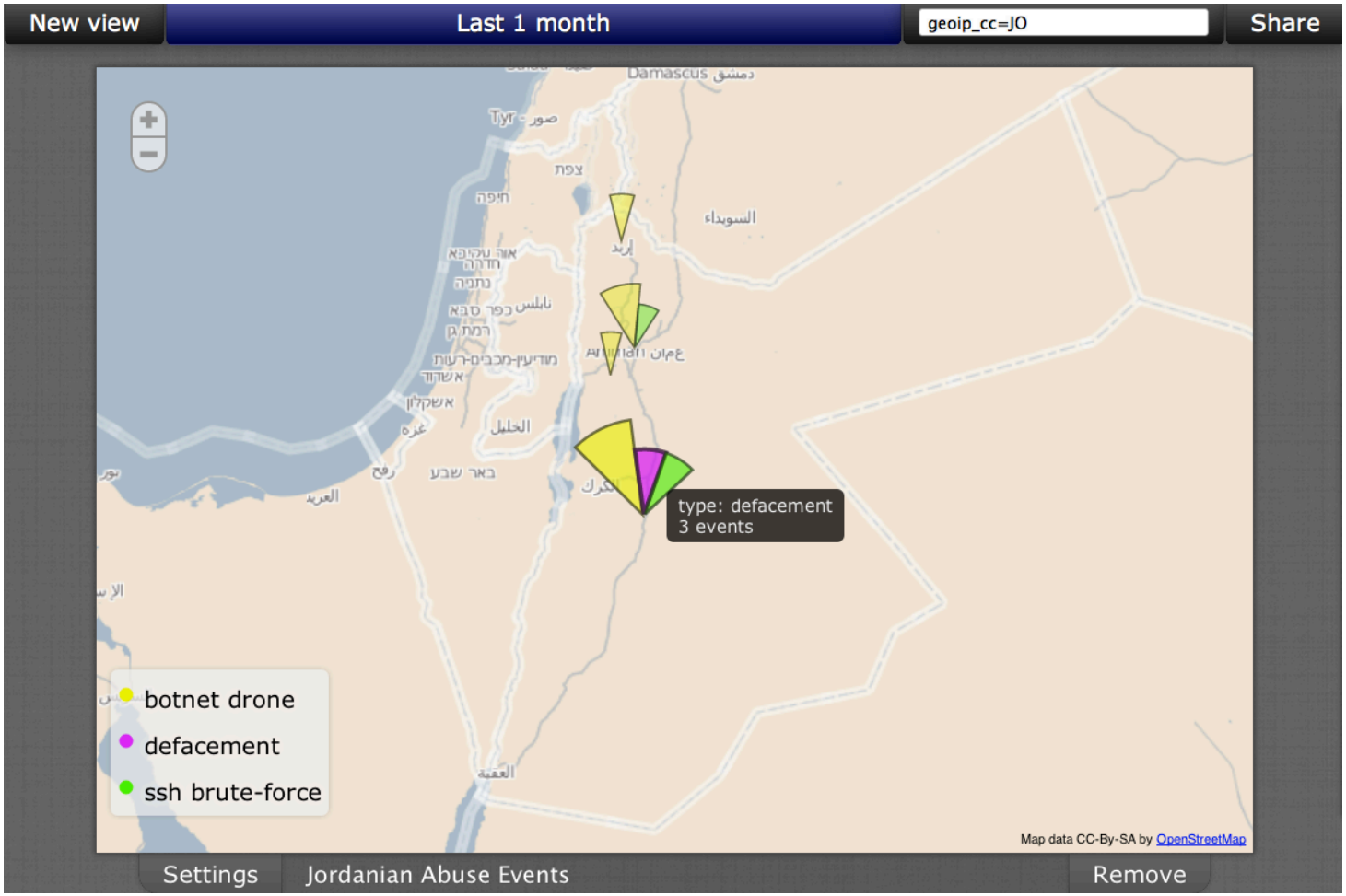
[Amman Cyber Drill/210-VSRoom-Design-Goals][edit]

VSRoom - Basic Views



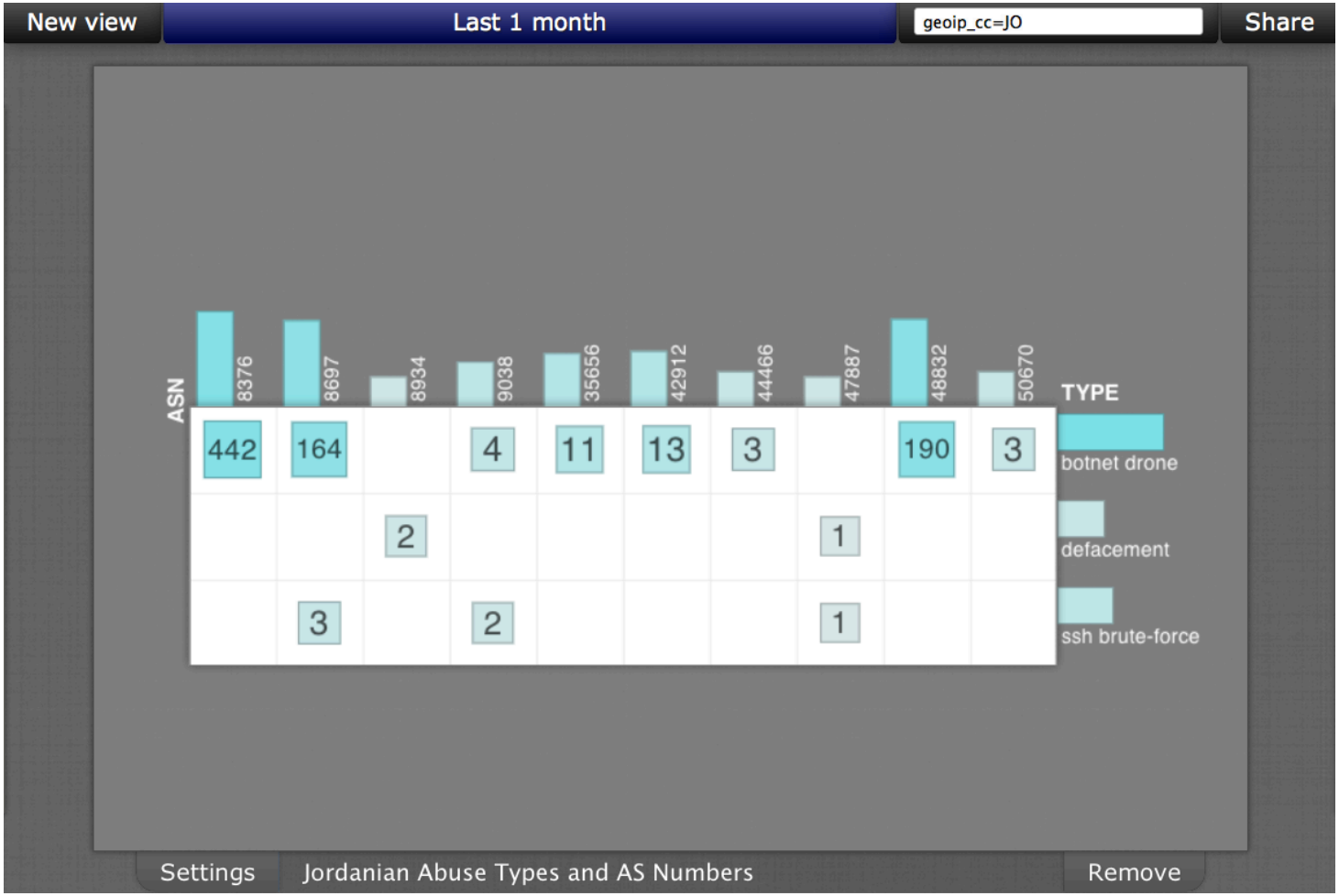
[Amman Cyber Drill/220-Teh-Views][edit]

VSRoom - Map



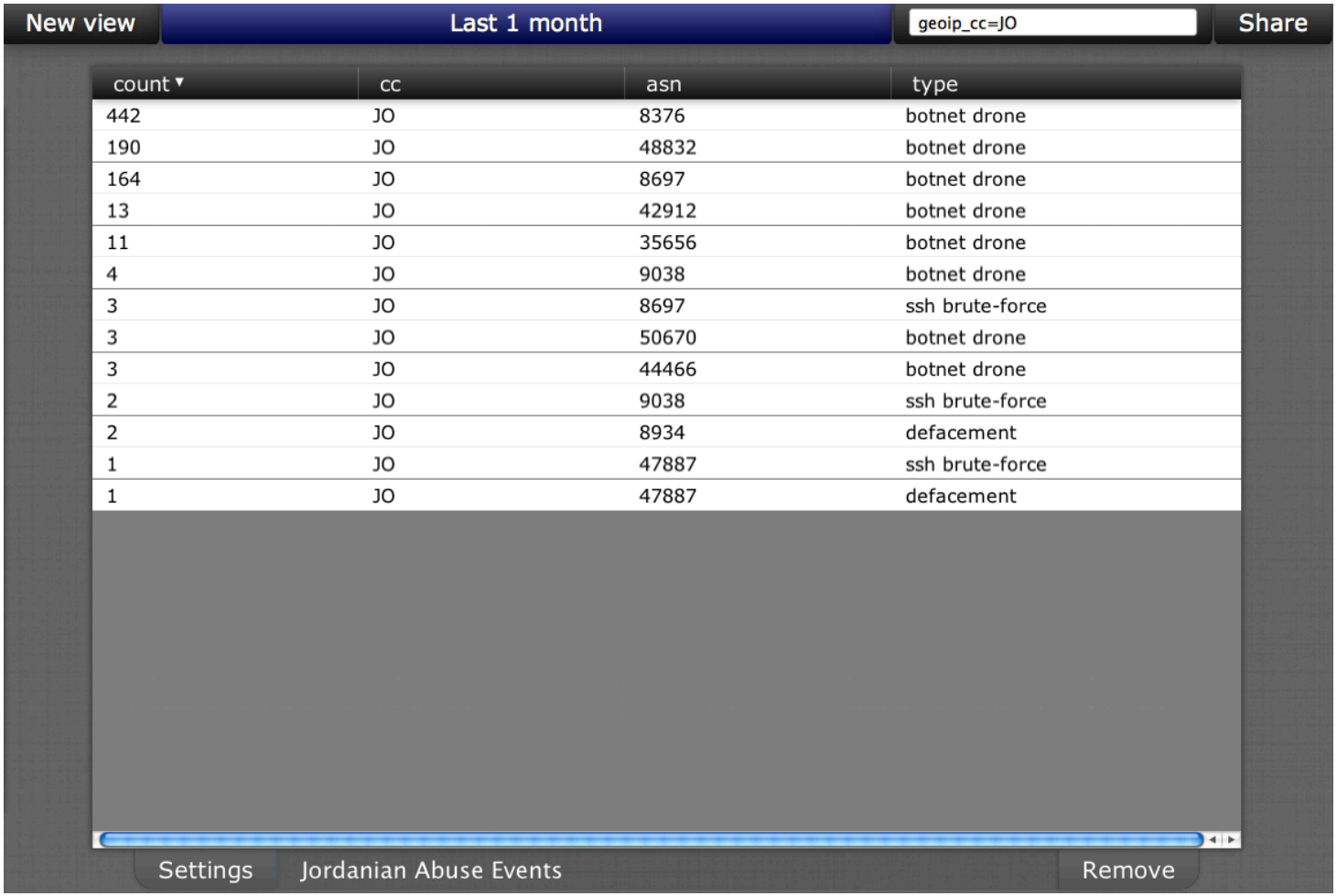
[Amman Cyber Drill/230-Map][edit]

VSRoom - Categorilla



[Amman Cyber Drill/240-Categorilla][edit]

VSRoom - List



[Amman Cyber Drill/250-List][edit]

On to the Demo, Let's Go

[Amman Cyber Drill/300-Teh Demo][edit]

Slideshow ^ |< << Slide 22 of 23 >> >|

Questions?

[Amman Cyber Drill/303-Questions][edit]

Thank You!

reminder

CERT-FI was able to amp up their abuse handling capabilities 100x through automation. 

[Amman Cyber Drill/999-Cest-Fini][edit]

Title

Abuse Situation Awareness (Introduction)

Author

Lari Huttunen

CategorySlideShow