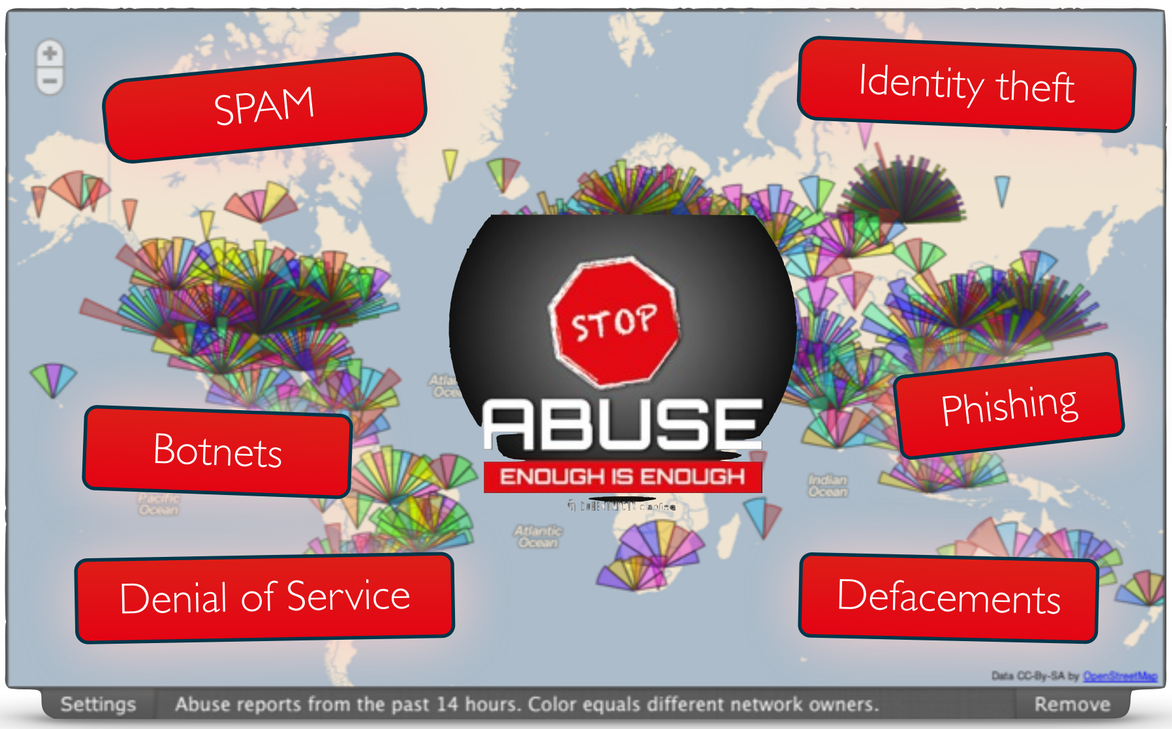
codenomicon

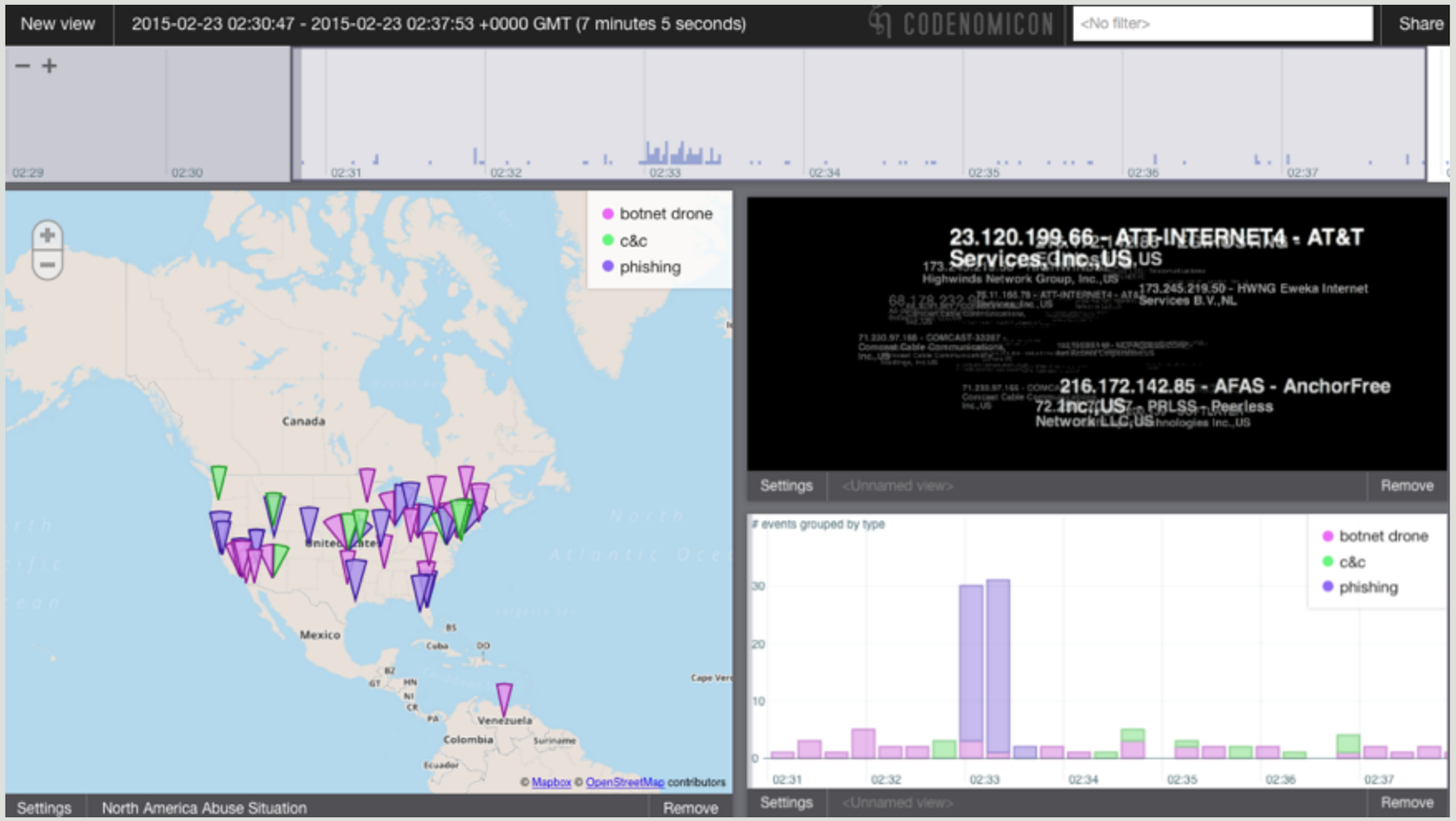
CARING IS SHARING

EFFICIENT THREAT INTELLIGENCE SHARING IN THE REAL WORLD



SOMETIMES
A PICTURE
IS WORTH A
THOUSAND
WORDS

SOMETIMES
IT IS NOT

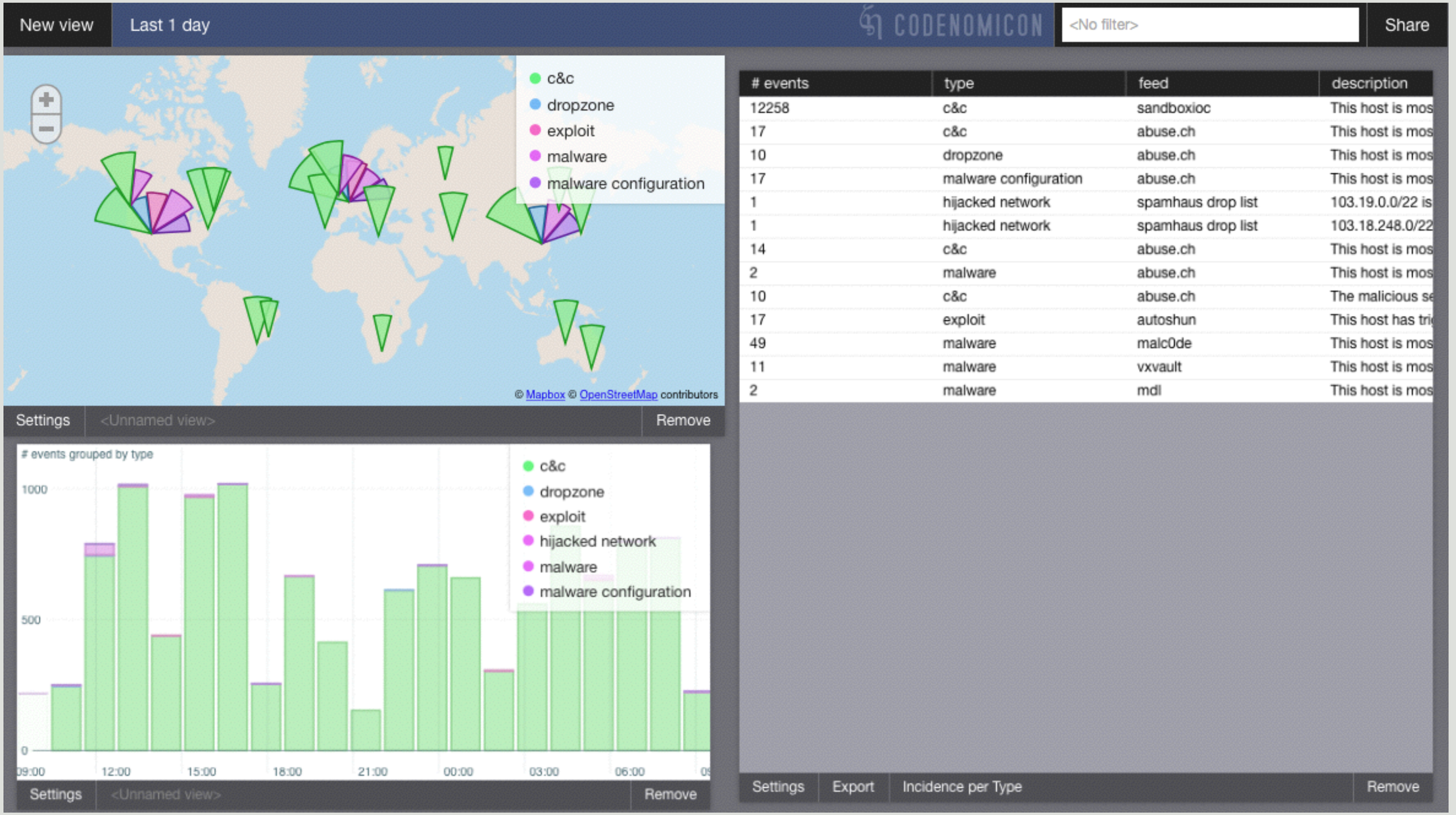


THE CURRENT LANDSCAPE

- Several active threat intelligence sharing projects already implemented
- Fairly trivial problem from a technical perspective
- Standardized frameworks for “sharing” available
- As with many CERT topics, it is subject to the risk of over analysis and unnecessary complications due to a priori assumptions
- We will observe some of the key properties of a successful sharing projects on a national level

THE CODENOMICON CONNECTION

- Codenomicon cooperates with several CSIRTs around the planet, many of which operate on a national level
- We had the pleasure of witnessing successful threat intelligence sharing projects materialize between CSIRTs
- Considering the potential benefits of these projects, it is hopefully useful to examine some of the important properties that (with high probability) determine their success



EFFICIENT THREAT INTELLIGENCE SHARING IN THE REAL WORLD

codenomicon

THE FUNDAMENTAL QUESTION

- How do we leverage the linear growth in the maturity level of a CSIRT against an apparent exponential growth in abuse
- Since the dawn of time, the human race has been facing this fundamental problem of CSIRT operations
- Codenomicon has been addressing that problem in cooperation with CSIRT for many years
- The governing factor in our approach is automation

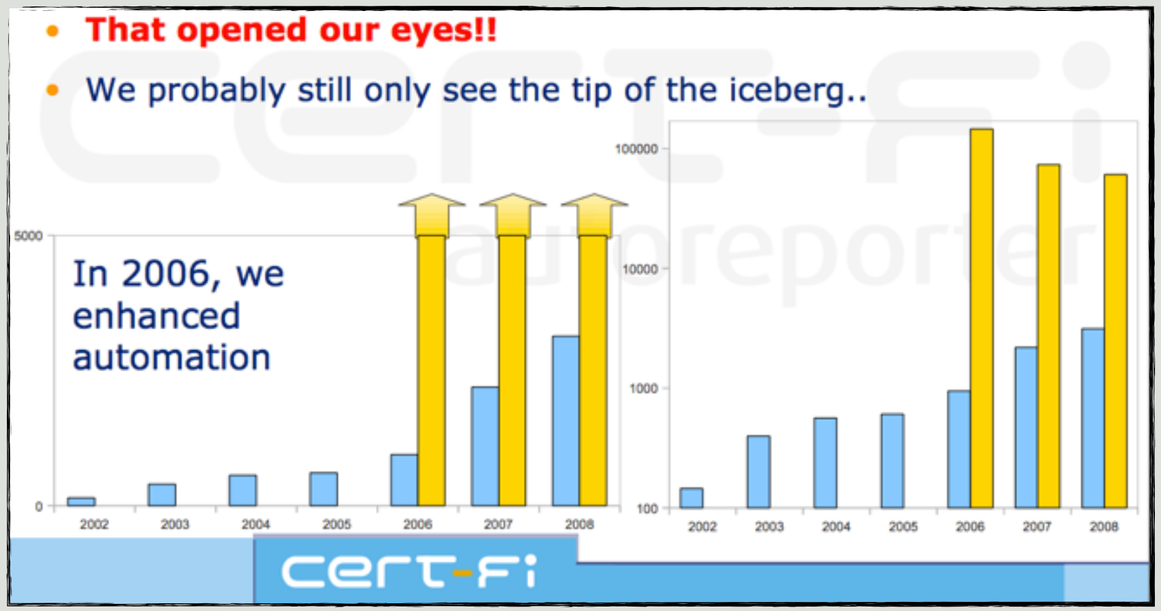
AUTOMATE EVERYTHING*

- Automate everything and let the analyst sort it out
- Focus on automating the critical components to any CSIRT operation; data-(acquisition, processing, reporting)
- The main objective is to provide CSIRTs with stable framework for implementing automation on the labor intensive parts of its daily operations
- Enable a rapid but sustainable gain of CSIRT maturity

IMPACT OF AUTOMATION

NCSC-FI, THE CSIRT FORMERLY KNOWN AS CERT-FI: DRASTIC INCREASE IN PROCESSED INTEL

- 2006, from 1000 processed incidents to 100000
- 2014 estimate is 600000 incidents



AUTOMATE EVERYTHING*

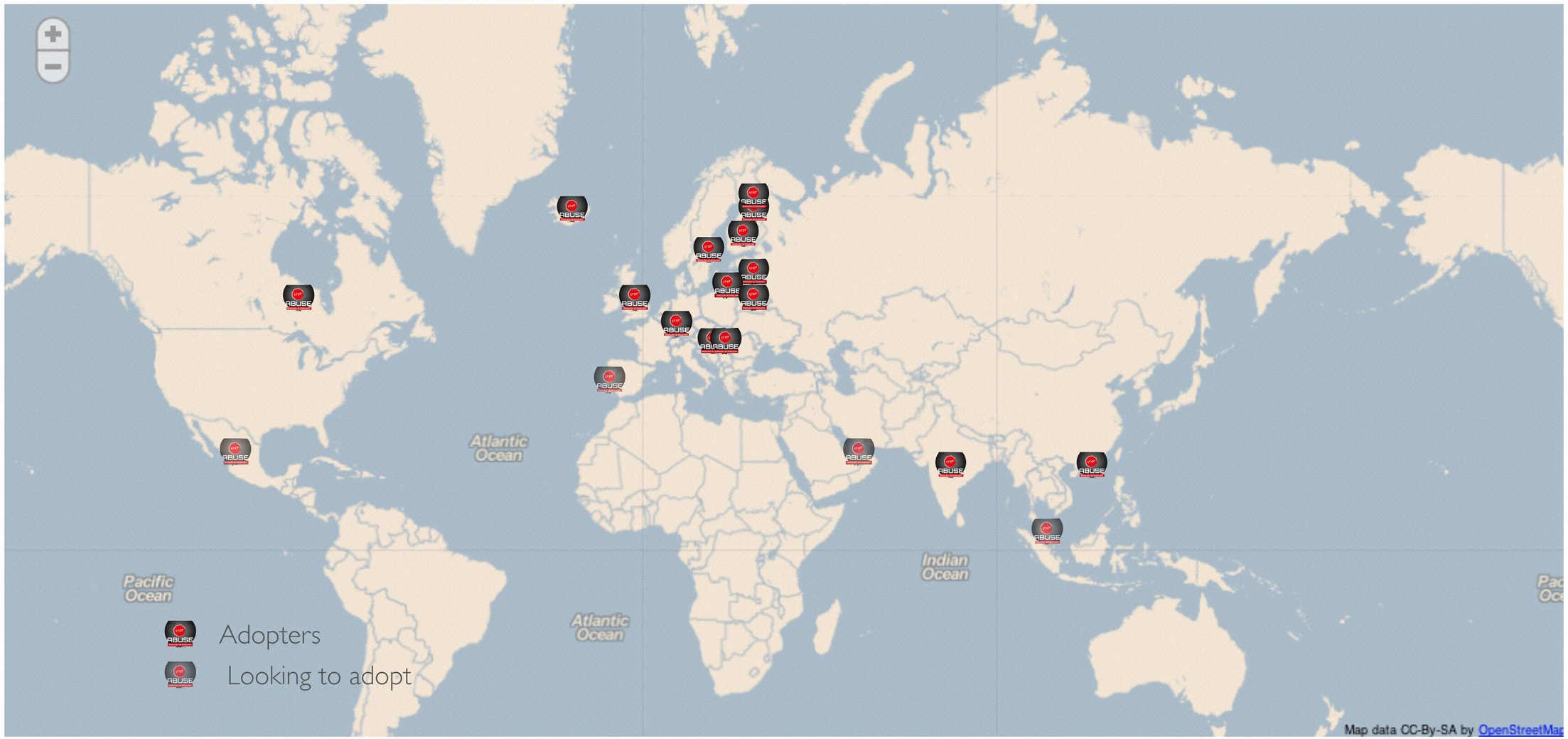
AbuseHelper

https://bitbucket.org/clarifiednetworks/abusehelper

AbuseSA

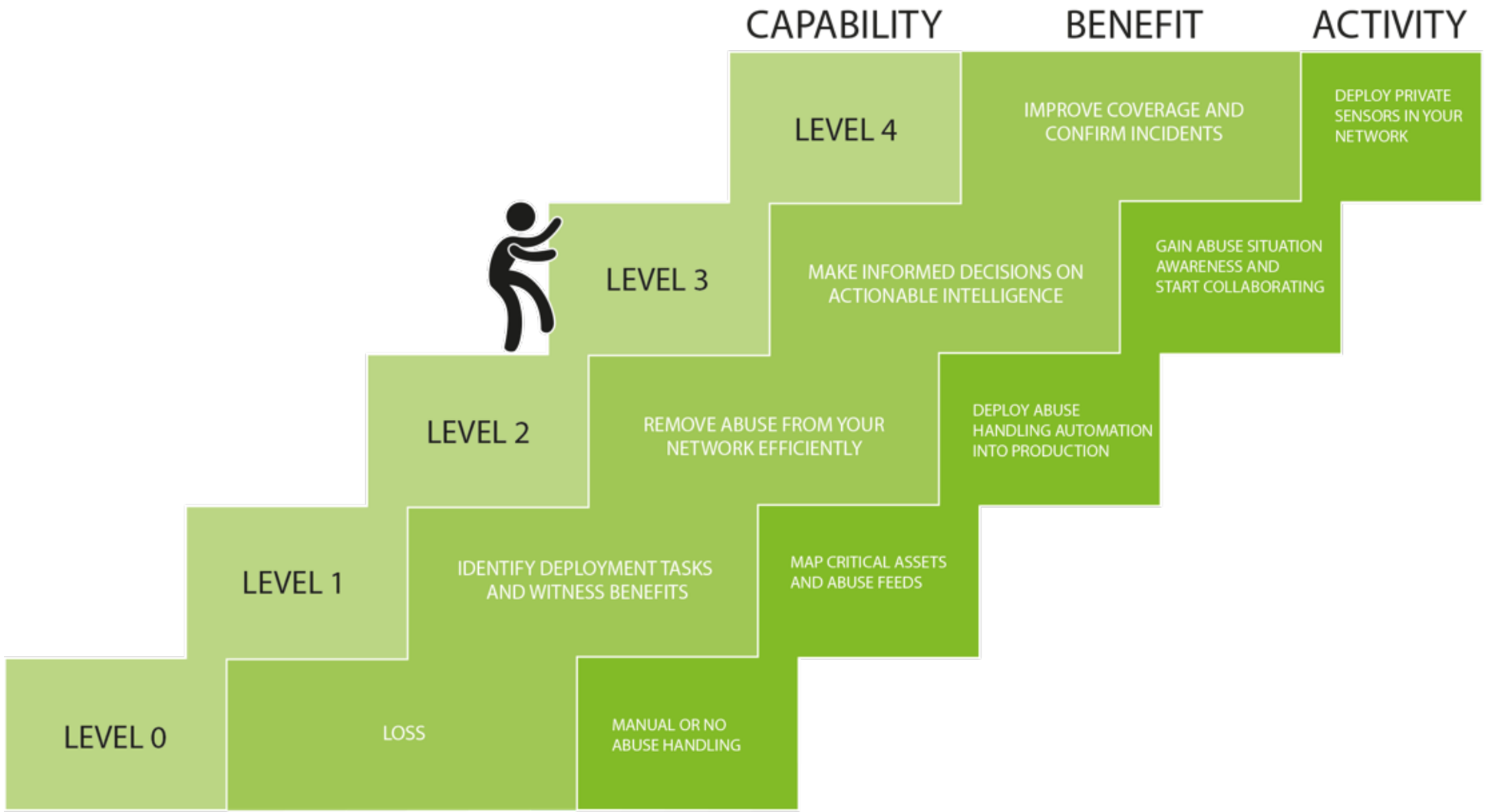
http://www.codenomicon.com/products/abusesa/

APPROACH GETTING POPULAR!



codenomicon

MATURITY LEVEL



codenomicon

IS THIS BUT A DIGRESSION?

- The inconvenient truth is that even with the availability of efficient methods for sharing threat intelligence, the success and sustainability of the sharing project will (with high probability) be determined by the maturity level of the CSIRTs involved
- Should emerge as a natural extension to the CSIRT operation after a certain maturity / confidence level is reached
- Premature / forced sharing efforts tend to end up as a recursive requirement analysis loop

AND THE POINT?

- Building TI sharing projects between CSIRTs on top of compatible frameworks makes everything better
  - Sharing threat intel is then a trivial effort on the technical level
  - Data integration to existing workflows becomes trivial (the response)
  - Extensions are readily available, shared knowledge through collaborative augmentation etc.
- Sharing becomes more about building lasting trust relationships instead of bonking heads over implementation details

INGREDIENTS MATRIX OF SILLY POINT MAKING

	SOURCE ACQUISITION	*DEPLOYMENT TIME*	*PRODUCTION TIME*
COMPATIBLE FRAMEWORKS	*EASY*	*MINIMAL*	*MINIMAL*
WORKFLOWS	*X*	*X*	*X*
INTEGRATION	*EASY*	*X*	*X*

THE REAL WORLD, NCSC-FI AND CERT-UK

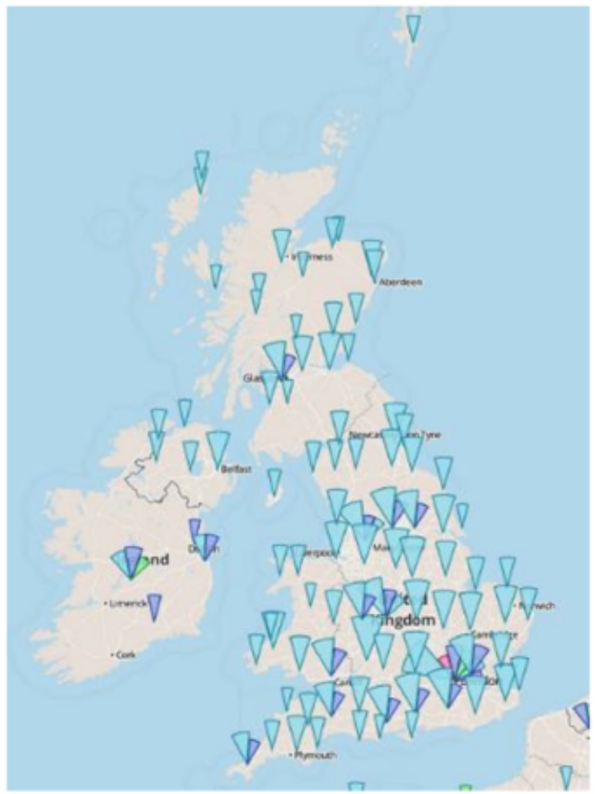
- Active IoC sharing between national CSIRTs
- Rapid implementation possible once the potential of collaboration is identified, compatible frameworks / workflows
- With minimal commitment of resources required, the value of the project is determined by the quality of data being shared
- The project can continue to evolve over time based on the flexibility of the underlying framework, e.g. start with minimal definition of IoC and allow it to expand based on real requirements

IT IS NOT OUR SUCCESS, IT IS OUR CUSTOMER SUCCESS

CERT-UK

QUARTERLY REPORT

CERT-UK processes over 250,000 reports of 'abuse' every day



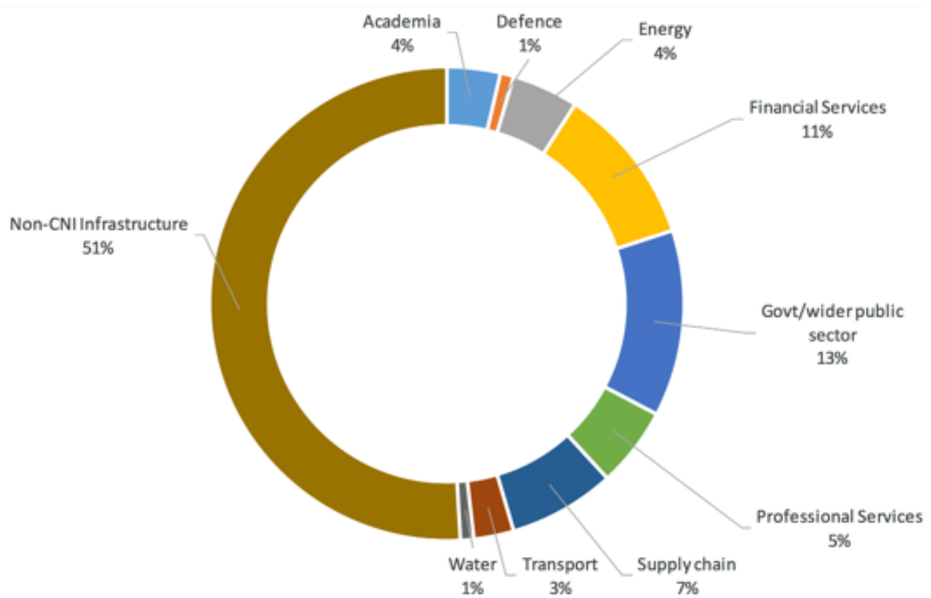
On CiSP, CERT-UK routinely publishes a list of the 'command and control' (C2) servers that we see being used by malware. This list is produced by the Fusion Cell and is aggregated from all of our feeds of commercial and non-commercial information. Using a specialist tool, we are able to take in over 250,000 reports of 'abuse' information that has been traced to the UK, every day. The 'abuse' could be anything from a botnet infected client to an IP address in the UK launching automated scans across the internet.

In addition to using this information to produce a list of C2 servers that businesses can use to identify malicious activity on their networks, CERT-UK provides an automated alerting system

Case Study: Heartbleed

On 7 April a vulnerability disclosure by the OpenSSL team quickly gained worldwide attention in the technical press as well as significant coverage in the mainstream media. What made Heartbleed garner such widespread attention, and was it justified?

Trends per Sector

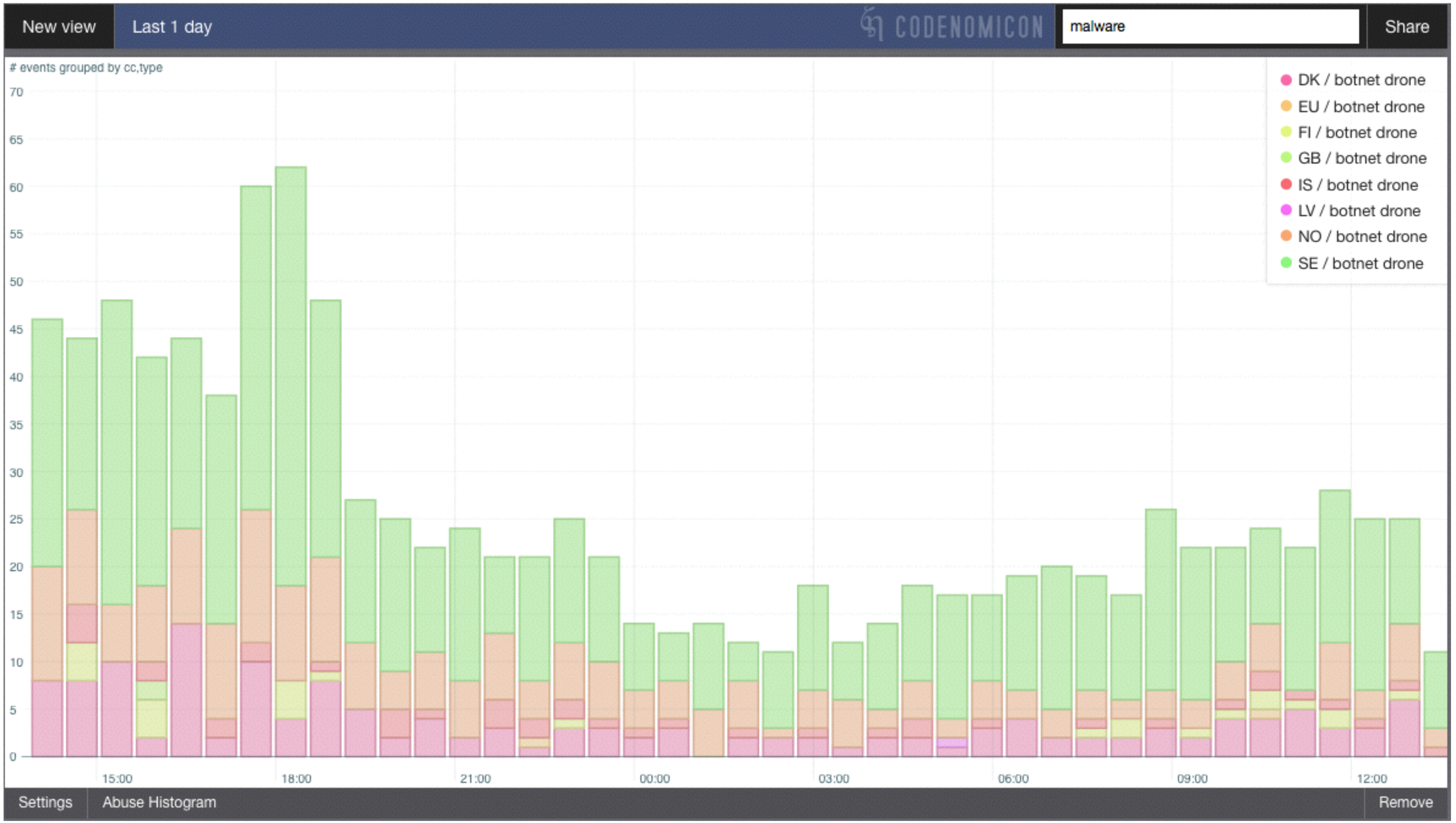


codenomicon

And then suddenly, we are in the position of exploring the potentials of sharing threat intelligence with other sources by evaluating the benefits of such scenarios … in contrast to letting the ever-changing data govern such efforts

SHARED SITUATIONAL AWARENESS ACROSS NATIONAL BORDERS

ENABLING LOCALIZED IOC'S TO COMPLEMENT A MULTI-NATIONAL SITUATIONAL AWARENESS

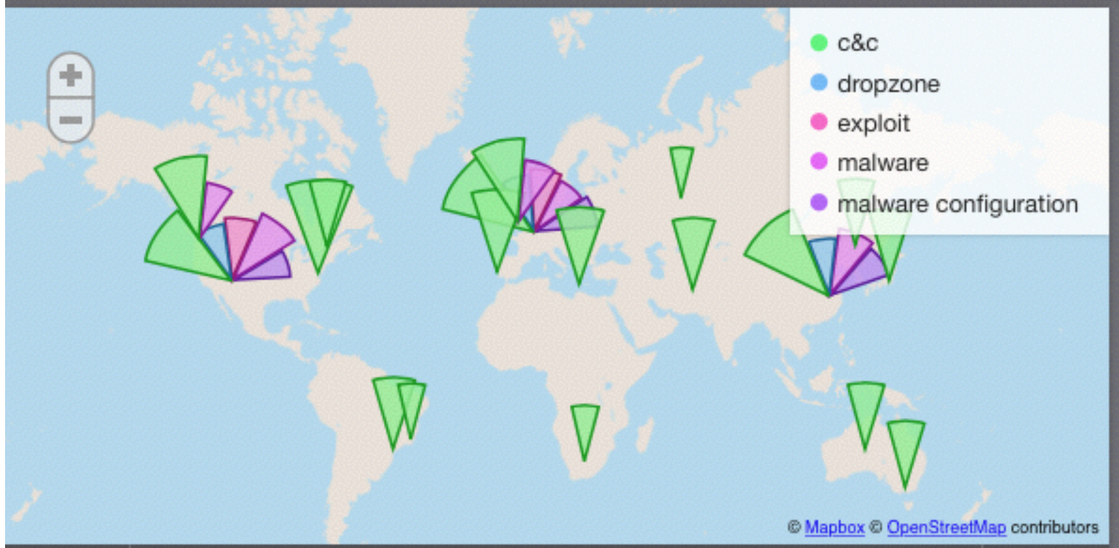

New view
Last 1 day
CODENOMICON
malware
Share
events grouped by cc,type
70
65
60
55
50
45
40
35
30
25
20
15
10
5
0
15:00
18:00
21:00
00:00
03:00
06:00
09:00
12:00
DK / botnet drone
EU / botnet drone
FI / botnet drone
GB / botnet drone
IS / botnet drone
LV / botnet drone
NO / botnet drone
SE / botnet drone
Settings
Abuse Histogram
Remove

COMMON UNDERSTANDING OF CRIMINAL INFRASTRUCTURE EVOLUTION

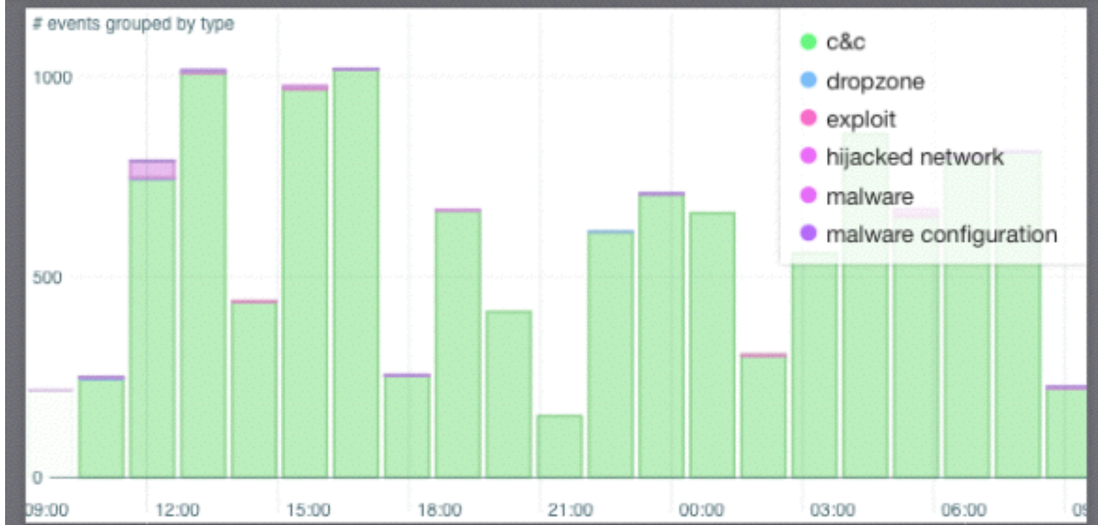
COMPLEMENTED BY A FIXED-POINT STATE

codenomicon

New view | Last 1 day | CODENOMICON | <No filter> | Share



Settings | <Unnamed view> | Remove



Settings | <Unnamed view> | Remove

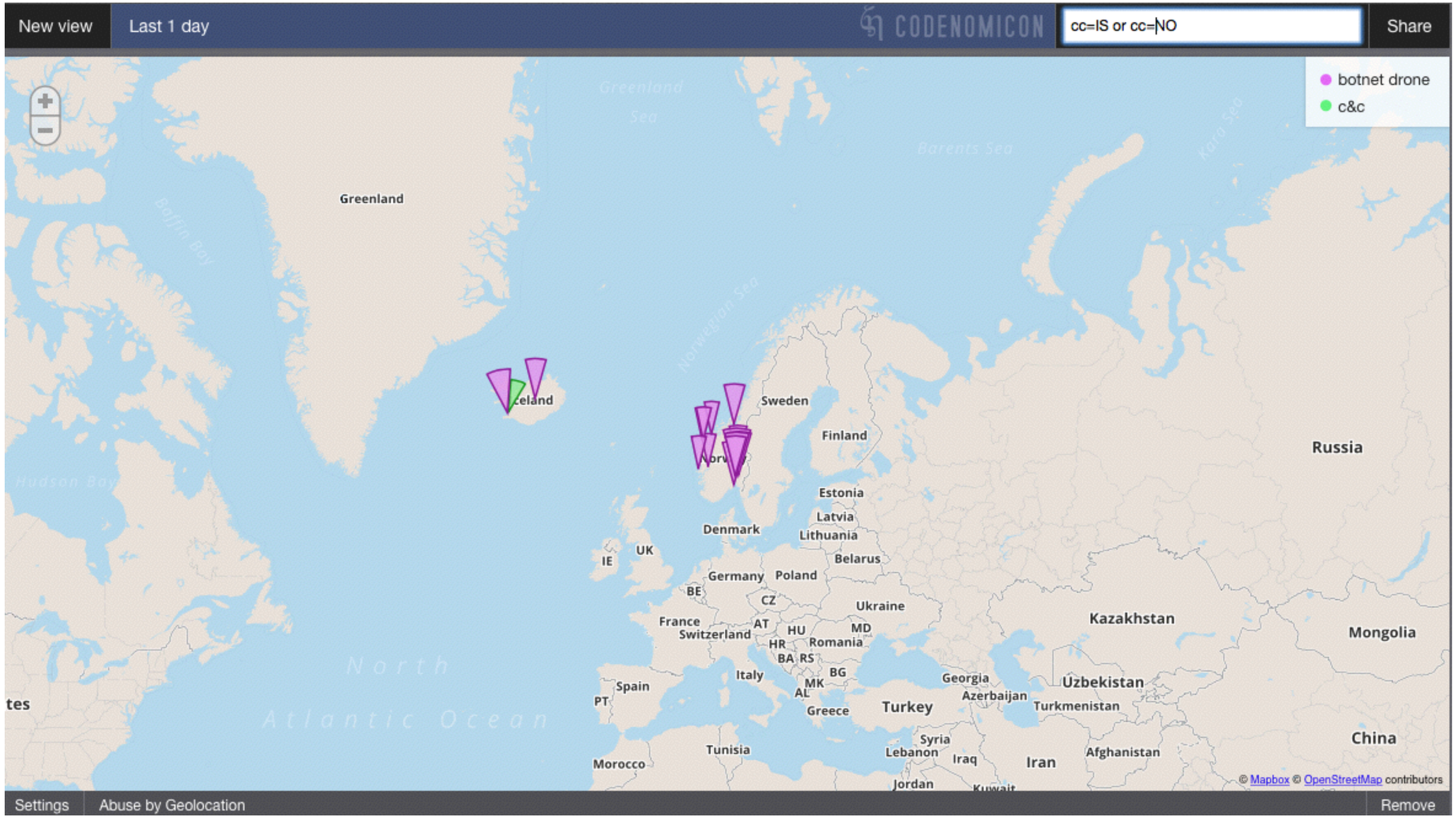
# events	type	feed	description
12258	c&c	sandboxioc	This host is mos
17	c&c	abuse.ch	This host is mos
10	dropzone	abuse.ch	This host is mos
17	malware configuration	abuse.ch	This host is mos
1	hijacked network	spamhaus drop list	103.19.0.0/22 is
1	hijacked network	spamhaus drop list	103.18.248.0/22
14	c&c	abuse.ch	This host is mos
2	malware	abuse.ch	This host is mos
10	c&c	abuse.ch	The malicious se
17	exploit	autoshun	This host has tri
49	malware	malc0de	This host is mos
11	malware	vxvault	This host is mos
2	malware	mdl	This host is mos

Settings | Export | Incidence per Type | Remove

ENABLING REALTIME MITIGATION BETWEEN NATION STATES

ENABLING SHARED MITIGATION THROUGH COMPATIBLE WORKFLOWS

codenomicon



EFFICIENT THREAT INTELLIGENCE SHARING IN THE REAL WORLD

codenomicon

SINDRI@CODENOMICON.COM