Automated incident handling

The Finnish way

Mostly harmless?

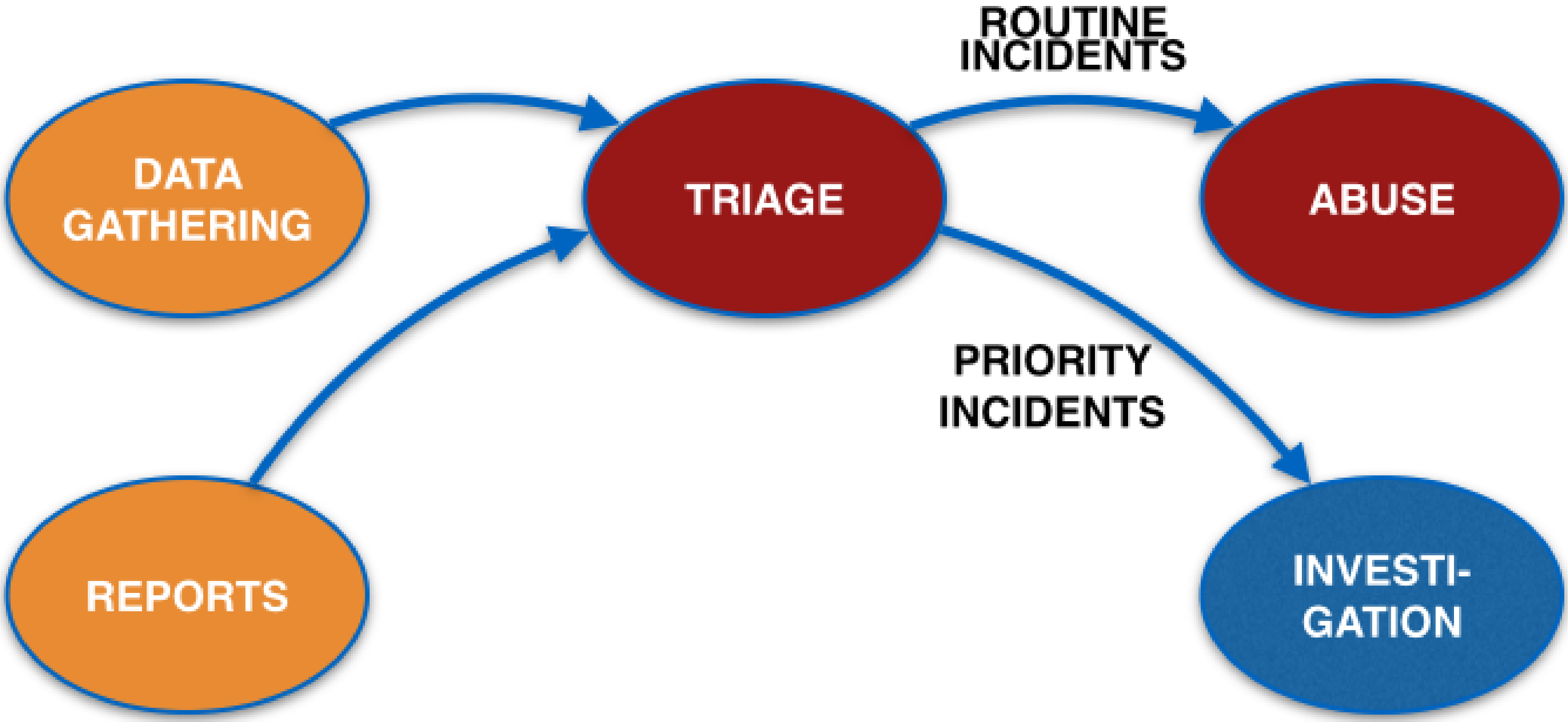
In the beginning - CERT-FI 2002

- Regulation for internet service providers (ISP:s)
  - Basic security of facilities and processes
  - Mandating best current practices
  - Block outgoing spam
- Mandatory reporting for ISP:s
- Establishing a national Computer Emergency Response Team (CERT)

Early problems

- Regulation: now we're being the good neighbor, but still get attacked
- Mandatory reporting: Most incidents out of scope
- CERT functions: No ownership/visibility of networks, small number of incident reports

CERT work

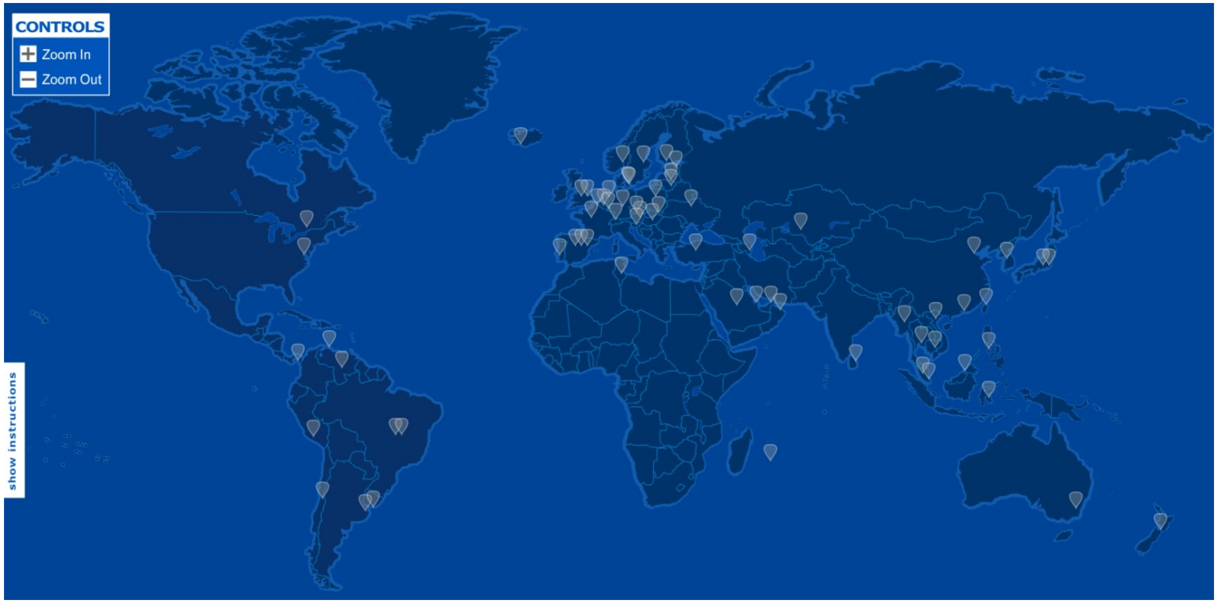

DATA GATHERING
REPORTS
TRIAGE
ROUTINE INCIDENTS
ABUSE
PRIORITY INCIDENTS
INVESTI-GATION

Key facts for enhancing CERT work

- Most attacks are opportunistic or collateral damage
- Most incidents are first detected by third parties

➢ Gathering and handling third-party reports is the low-hanging fruit

Global network of data sources

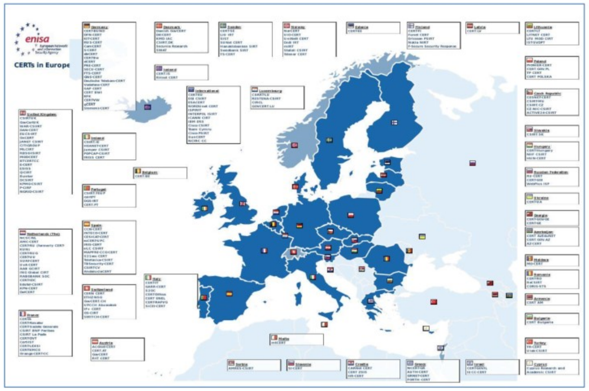


FIRST
Improving Security Together

enisa

TRUSTED
Introducer

EGC group
European Government CERTs group



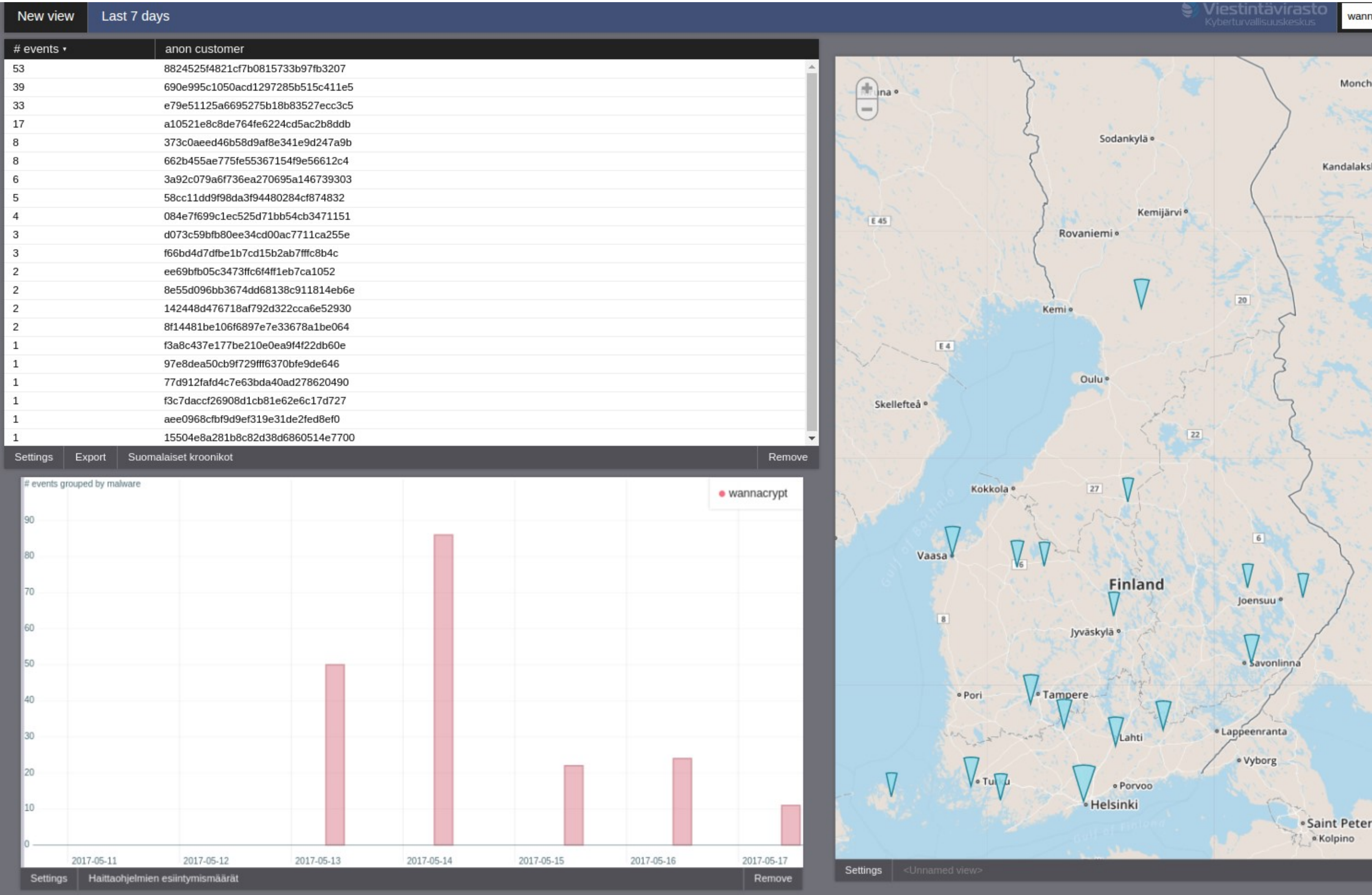
Autoreporter 2005-

- Autoreporter gathers data on incidents related to Finnish networks and sends reports to the ISP:s
- The system is based on AbuseHelper and Codenomicon AbuseSA
- Highly automated system
  - No human operator, very light administration

How is the data gathered?

A sinkhole

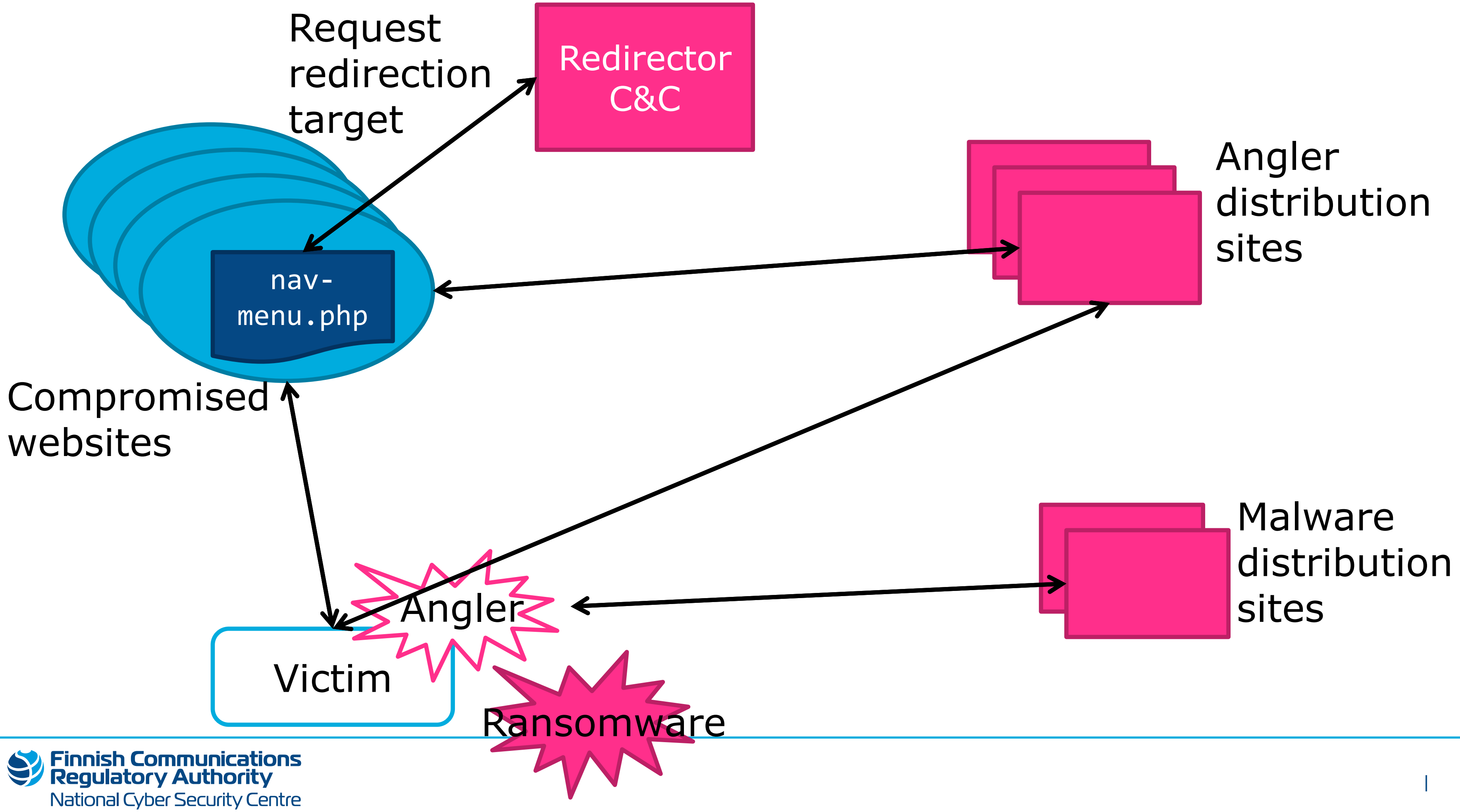
WanaCrypt0r



New view | Last 7 days

# events ▾	anon customer
53	8824525f4821cf7b0815733b97fb3207
39	690e995c1050acd1297285b515c411e5
33	e79e51125a6695275b18b83527ecc3c5
17	a10521e8c8de764fe6224cd5ac2b8ddb
8	373c0aeed46b58d9af8e341e9d247a9b
8	662b455ae775fe55367154f9e56612c4
6	3a92c079a6f736ea270695a146739303
5	58cc11dd9f98da3f94480284cf874832
4	084e7f699c1ec525d71bb54cb3471151
3	d073c59bfb80ee34cd00ac7711ca255e
3	f66bd4d7dfbe1b7cd15b2ab7fffc8b4c
2	ee69bfb05c3473ffc6f4ff1eb7ca1052
2	8e55d096bb3674dd68138c911814eb6e
2	142448d476718af792d322cca6e52930
2	8f14481be106f6897e7e33678a1be064
1	f3a8c437e177be210e0ea9f4f22db60e
1	97e8dea50cb9f729fff6370bfe9de646
1	77d912fafd4c7e63bda40ad278620490
1	f3c7daccf26908d1cb81e62e6c17d727
1	aee0968cfbf9d9ef319e31de2fed8ef0
1	15504e8a281b8c82d38d6860514e7700

Pseudo-Darkleech, Angler EK and CryptoWall


Request redirection target
Redirector C&C
Angler distribution sites
nav-menu.php
Compromised websites
Malware distribution sites
Angler
Victim
Ransomware

Angler epidemic, June 2015

- Lots of Angler EK hits seen in detection and early warning system HAVARO in late June 2015.
- Lots of compromised sites redirecting to Angler EK distribution sites.
- Hard to get compromised sites cleaned up
- Redirector server identified
- Domain name for redirector server seized
- Requests from compromised sites coming in
  - » List of compromised sites -> notifications

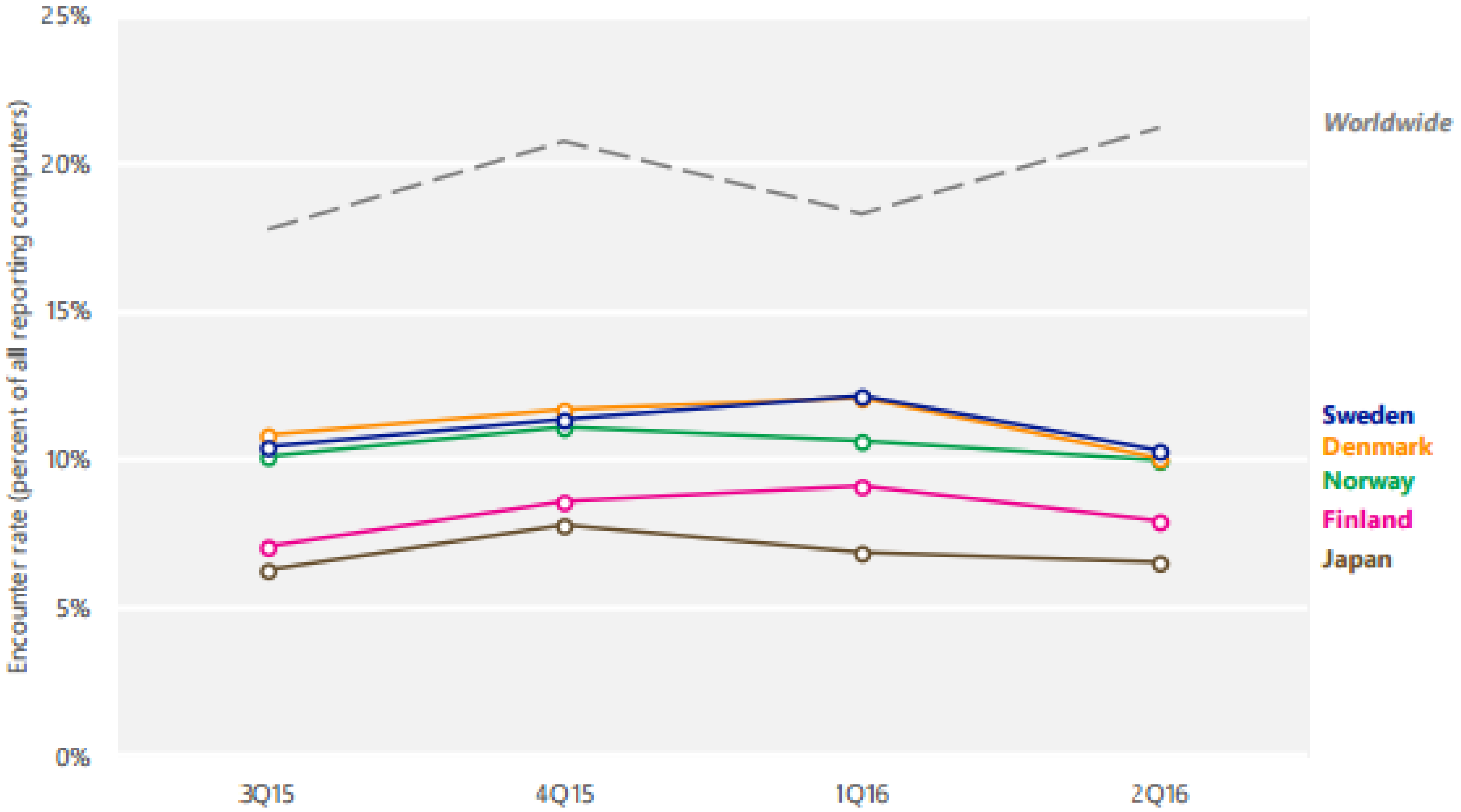
Results

Statistics 2016

- Roughly 82 000 automatically handled incidents in Finnish networks
  - 91% Malware
  - 7% Scanners (likely also malware)
  - Compromised websites, Spam, Distributed Denial of Service (DDoS) etc.
- 7454 voluntary reports
- Only 17 based on mandatory reporting

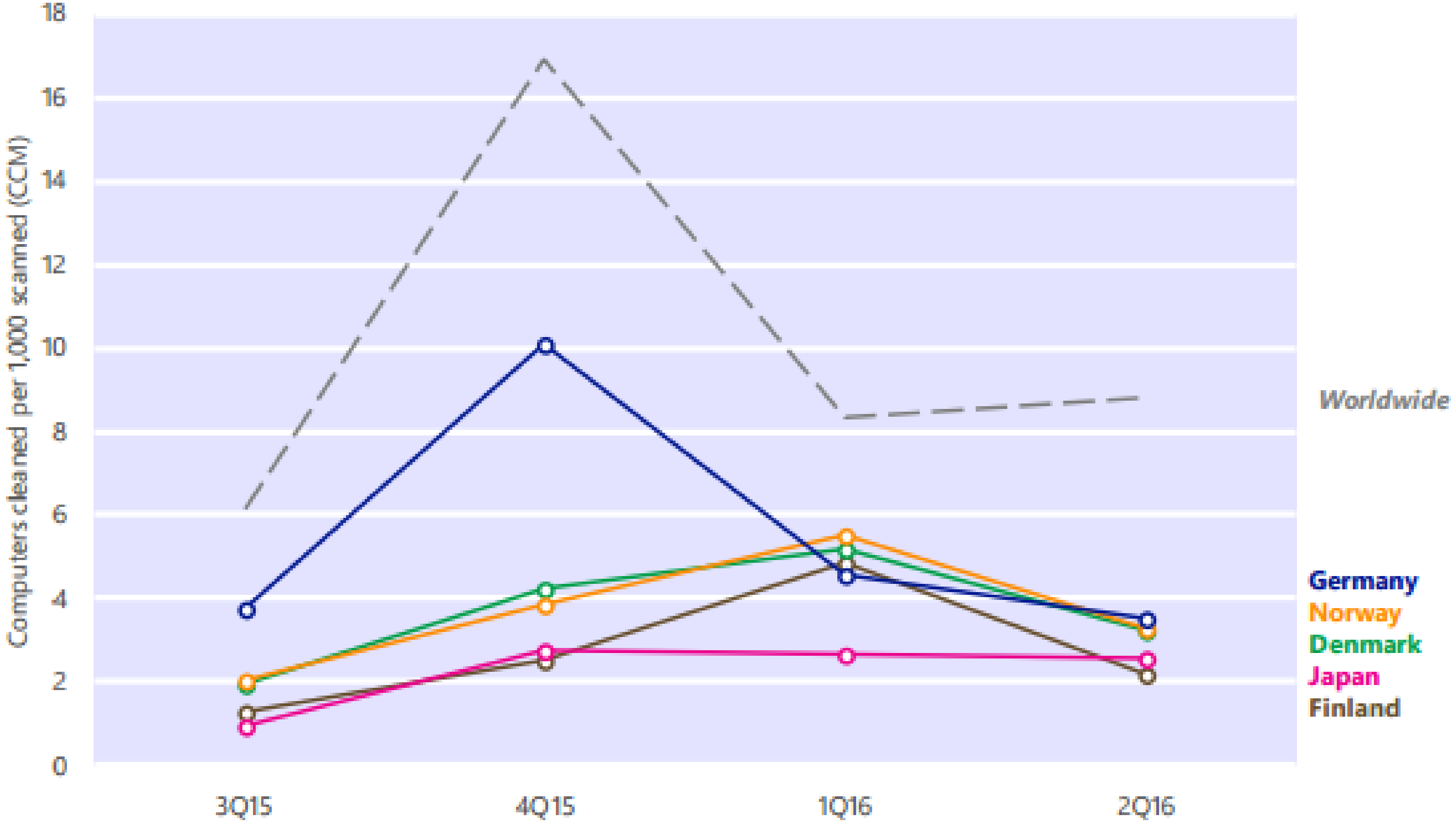
Microsoft Security Intelligence Report 21

Figure 49. Trends for locations with low encounter rates in 1H16 (100,000 reporting computers minimum)



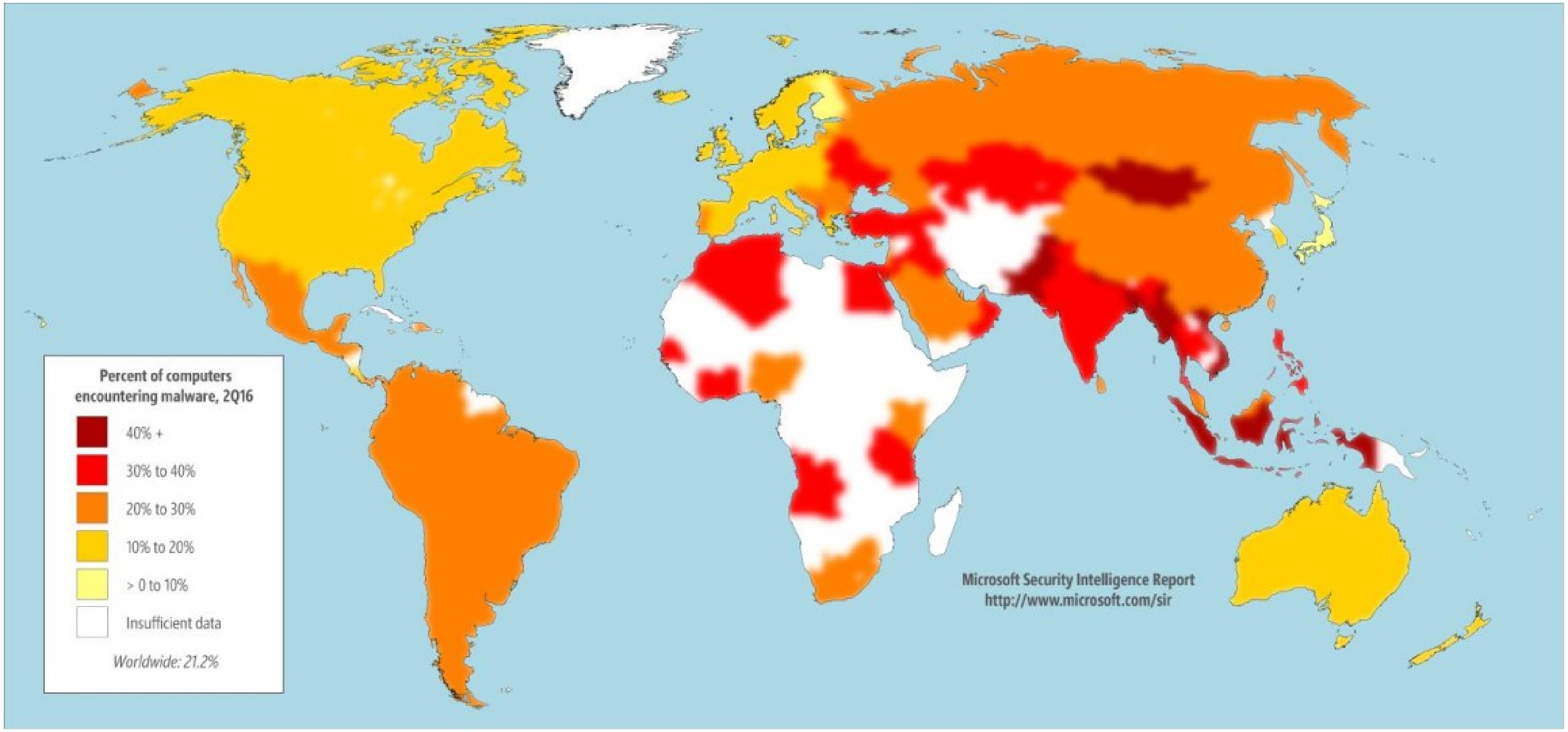
Microsoft Security Intelligence Report 21

Figure 50. Trends for locations with low infection rates in 1H16, by CCM (100,000 reporting computers minimum)



Microsoft Security Intelligence Report 21

Figure 46. Encounter rates (top) and infection rates (bottom) by country/region in 2Q16

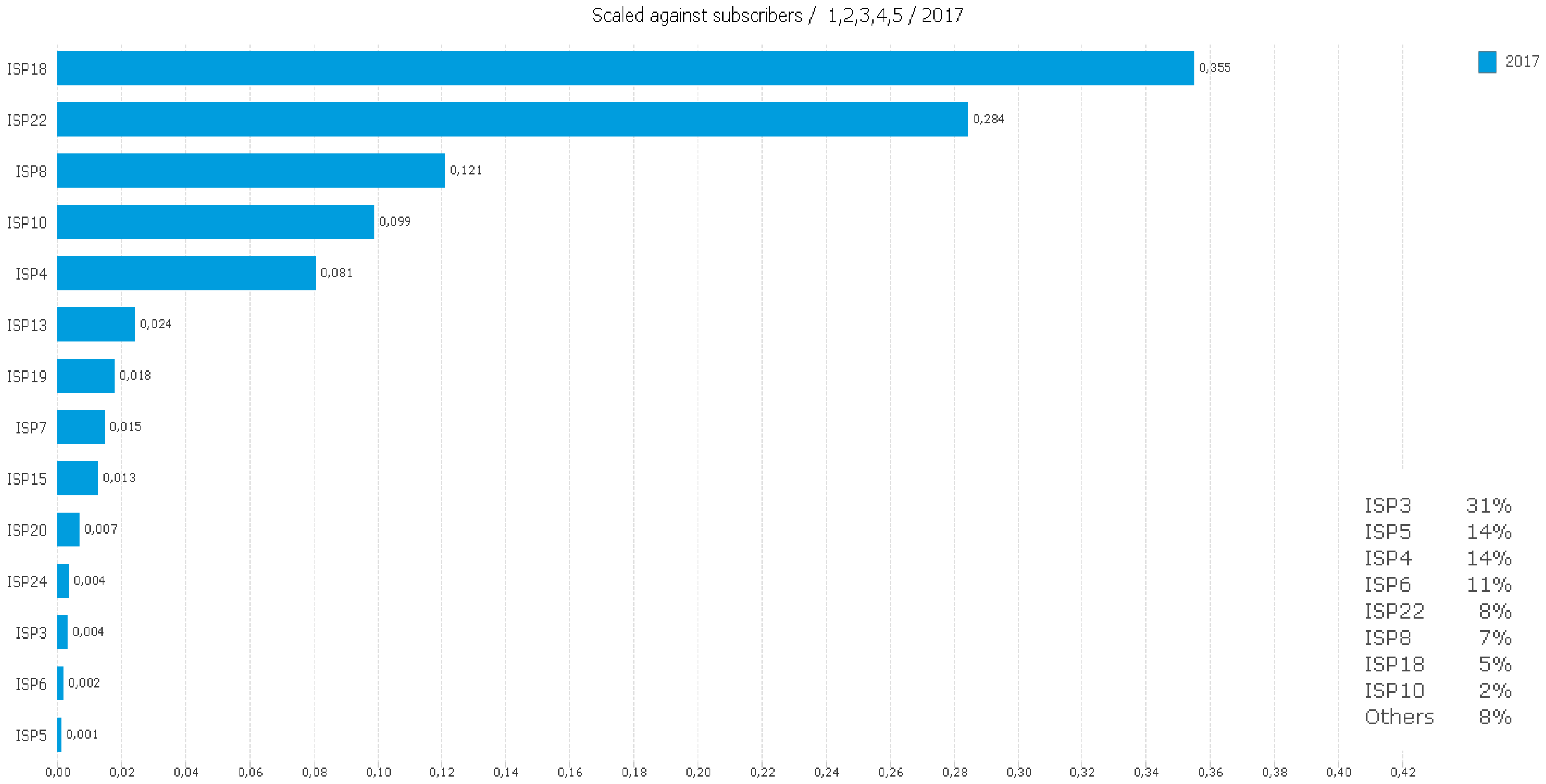

Percent of computers encountering malware, 2Q16
40% +
30% to 40%
20% to 30%
10% to 20%
> 0 to 10%
Insufficient data
Worldwide: 21.2%
Microsoft Security Intelligence Report
http://www.microsoft.com/sir

Secrets behind our success

We need you

- Finnish networks are so clean because of the efforts by Finnish ISP:s
- Please keep up the good work

Havainnot tilaajaa kohden



ISP3	31%
ISP5	14%
ISP4	14%
ISP6	11%
ISP22	8%
ISP8	7%
ISP18	5%
ISP10	2%
Others	8%

What next

Possible future developments

- We have **a lot** data on vulnerable services in Finnish networks
- Streamlining customer notification?
- More proactive actions: scanning, malware followup, ?
- Your wish here

Finnish Communications Regulatory Authority

National Cyber Security Centre

www.ncsc.fi
www.ficora.fi