CERT-FI Autoreporter

2011-12-14
Mini MetriCon 5.5

Jussi Eronen
Information Security Adviser
CERT-FI
Finnish Communications
Regulatory Authority

Finnish Communications Regulatory Authority

Agenda

Background

The Autoreporter Project


CERT/CC
CERT.BR
UNIRAS
SITIC/NORCERT
CERT-FI
cert-fi
1 (LOWEST)
2 (MEDIUM)
Condition Green
1 (LOW)
GUARDED
Risque Bas
ELEVATED
MEDIUM
N. AMERICA
84
Loss: 9%
INTERNET TRAFFIC REPORT
EUROPE
70
Loss: 11%
S.AMERICA
42
Loss: - %
BE
DE
IT
ES
UK
DK
DE
IT
SE
UK
FO
IT
NL
SE
UK

Background

Mostly harmless?

CERT-FI – Finnish national CSIRT authority

The duties of the Finnish Communications Regulatory Authority are:

1) to supervise compliance with this Act and any provisions issued under it, unless otherwise provided in section 32;

*2) to **collect information on violations of and threats to information security** in respect of network services, communications services and value added services, and on significant faults and disruptions in such services;*

*3) to **investigate violations of and threats to information security** in respect of network services, communications services and value added services, and significant faults and disruptions in such services; and*

*4) **publicize information security matters**.*

Act on the Protection of Privacy in Electronic Communications (516/2004) section 31

Finnish Communications Regulatory Authority

Finnish Networks and Other Assets

- By Finnish networks we mean:
  - Autonomous Systems in Finnish soil, operated or owned by Finnish organisations or otherwise important to Finnish interests.
  - Domains under .FI and .AX DNS root
  - Public telephone networks with +358 prefix
  - Other networks operated or owned by Finnish organisations
- By Finnish network services we mean:
  - Services located in Finnish networks
  - Services operated or owned by Finnish organisations
- Other assets we consider Finnish
  - Finnish Credit Card Prefixes
  - Bank Account Numbers
  - Finnish Brand Names

```
; File automatically created at 20100723073745
;
; This is a list of Autonomous System Numbers rel
; Finnish organisations. As a national CSIRT for
; act as a proxy in case some of these organisati
; contacted in timely and/or confidential manner
;

375     | EU | TIETOTIE-AS Finnish State Computer
544     | EU | SONERA-FUNET-TRANSIT Sonera Corpora
565     | EU | Technical Research Centre of Finlan
719     | FI | ELISA-AS Elisa Oyj
761     | EU | TIETORAITTI-AS Seinajoen Tietoraitt
764     | EU | FI-PMO-AS Prime Minister_s Office
790     | EU | EUNETFI EUnet Finland
1234    | EU | FORTUM-AS Fortum
1248    | EU | NOKIA Nokia Internet
1253    | EU | VEROAUTOSYS-AS The National Board o
1342    | EU | Fujitsu Invia Finland IP-network
1732    | EU | MIKROK-AS Mikrokonsultit Oy
1738    | EU | OKOBANK-AS OP-Pohjola Group Central
1739    | EU | TUTNET TUT Autonomous system
1741    | EU | FUNETAS FUNET autonomous system
1748    | EU | FINNAIR-AS FINNAIR
1759    | FI | TSF-IP-CORE TeliaSonera Finland IP
1780    | EU | VALNET Valmet Corporation
1854    | EU | NOVOGROUP Novo Group Oyj
1923    | EU | Tampere Telelphone Company
1926    | EU | UTANET-AS University of Tampere
2016    | EU | OTANET Otaniemi Science Park
2017    | EU | KRPNET National Bureau of Investiga
2026    | EU | HELSINKI City of Helsinki
2045    | EU | FACILITIES ICL Data Oy
2112    | EU | VALIODATA ValioData Oy
2862    | EU | MOL autonymous system
3222    | FI | CORENETFI Corenet Oy
3238    | EU | ALCOM Alands Datakommunikation Ab
3246    | EU | TDCSONG TDC Finland
3274    | EU | CYGATE Cygate Oy
3290    | EU | TVS- Tekniikka
3292    | EU | TDC TDC Data Networks
3336    | FI | ELISA-AS Elisa Oyj
4457    | EU | NESTE-NET NESTE Corporation
4458    | EU | CCNET CarelComp Oy
4588    | EU | FINNPAP-MRS FinnPap
4878    | US | NRC-RDI - Nokia Research Center
5411    | EU | CC-NET-AS
5420    | EU | KEMNET KemNet Autonomous system
5469    | EU | AGNET A. Ahlstrom Corporate Global
```

cert-fi

Special about the Finnish model..

Applies to Telecommunications Operators only:

Mandatory reporting of Information Security Incidents as well as Major Faults:

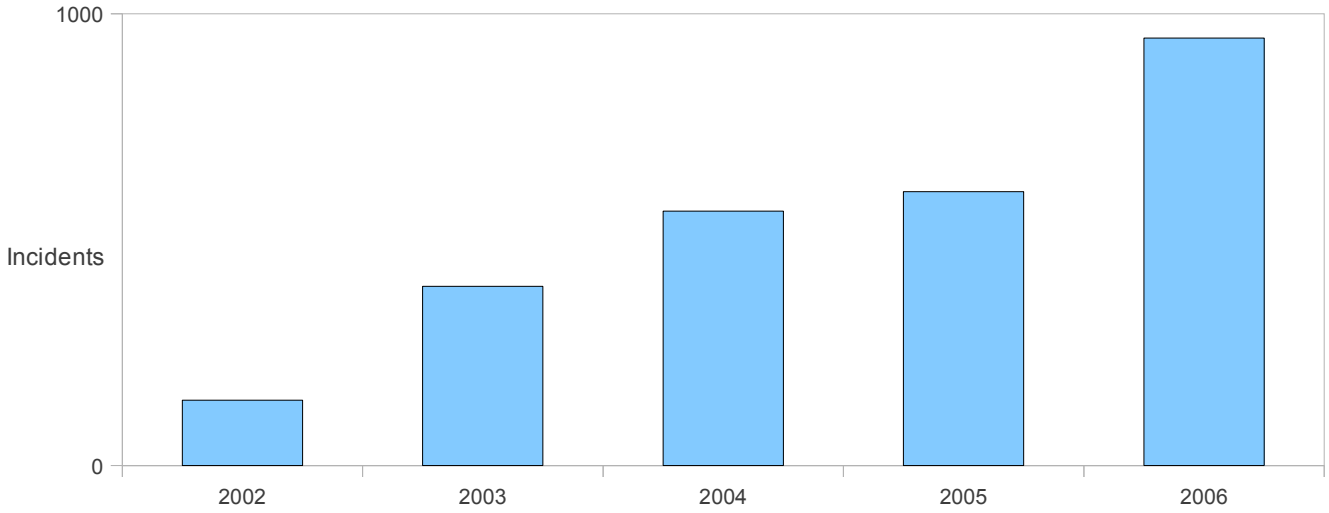
- affecting the networks
- affecting users of the networks
- affecting service provider's ability to operate it's networks

Some Actions by FICORA

- Regulation for service providers
  - Basic security of facilities and processes
  - Mandating BCP:s
  - Block outgoing spam
- Mandatory reporting for ISP:s
- Establishing CERT-FI
  - Key point in establishment was lower the reporting threshold

Problems

- Regulation for service providers - problem: now we're being the good neighbor, but still get attacked
- Mandatory reporting - problem: Most incidents out of scope
- Establishing CERT-FI - problem: No ownership/visibility of networks, incident statistics reflect available workforce and goodness of abuse handling script framework

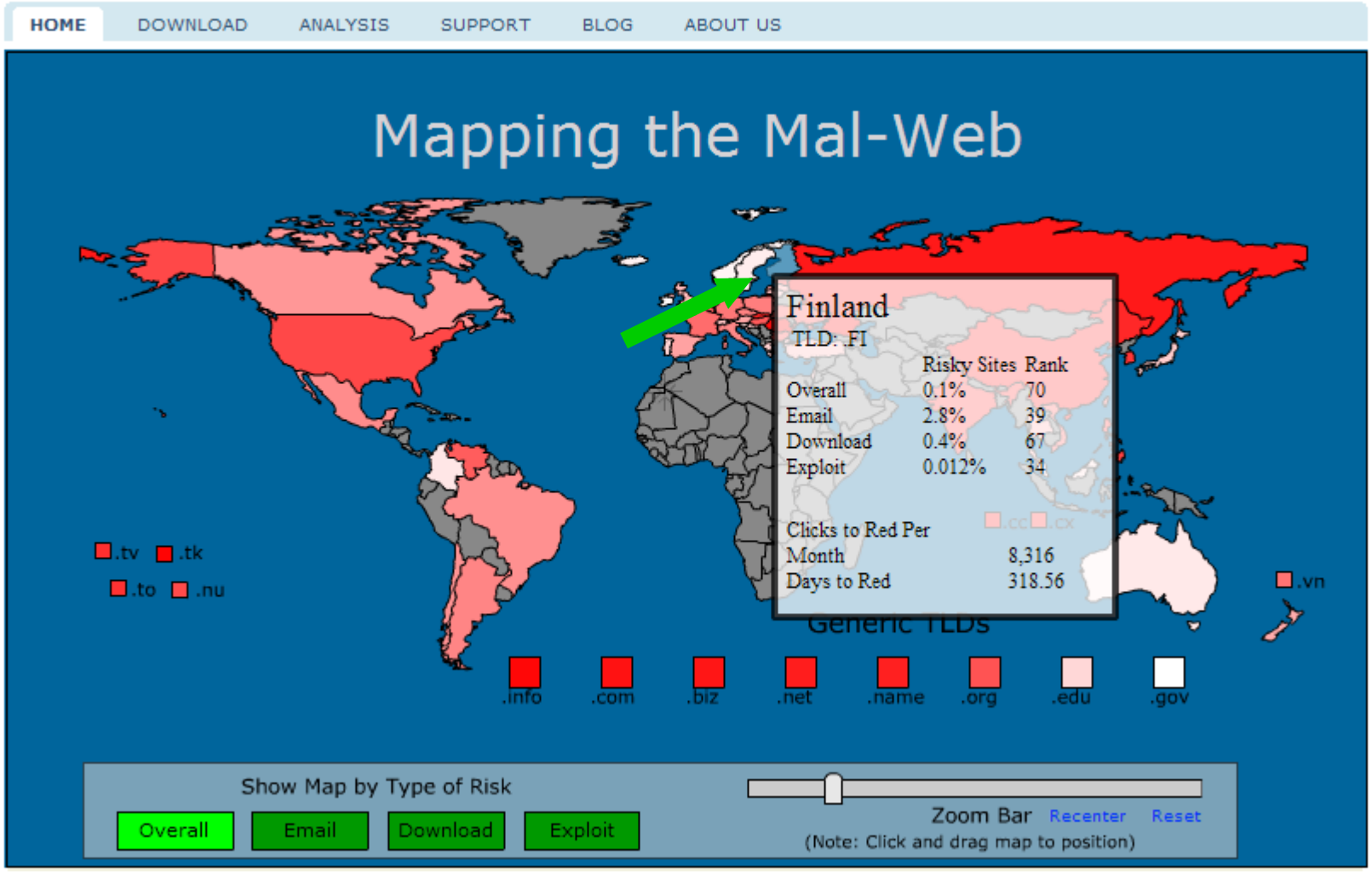


Some Open Questions

- How many incidents affect Finnish networks?
- Is “x incidents per year” good or bad?
  - Or: How do we compare to our neighbors?
- Are we doing the right things?
- Are things better or worse than last year?

How do we compare to our neighbors?

McAfee SiteAdvisor™



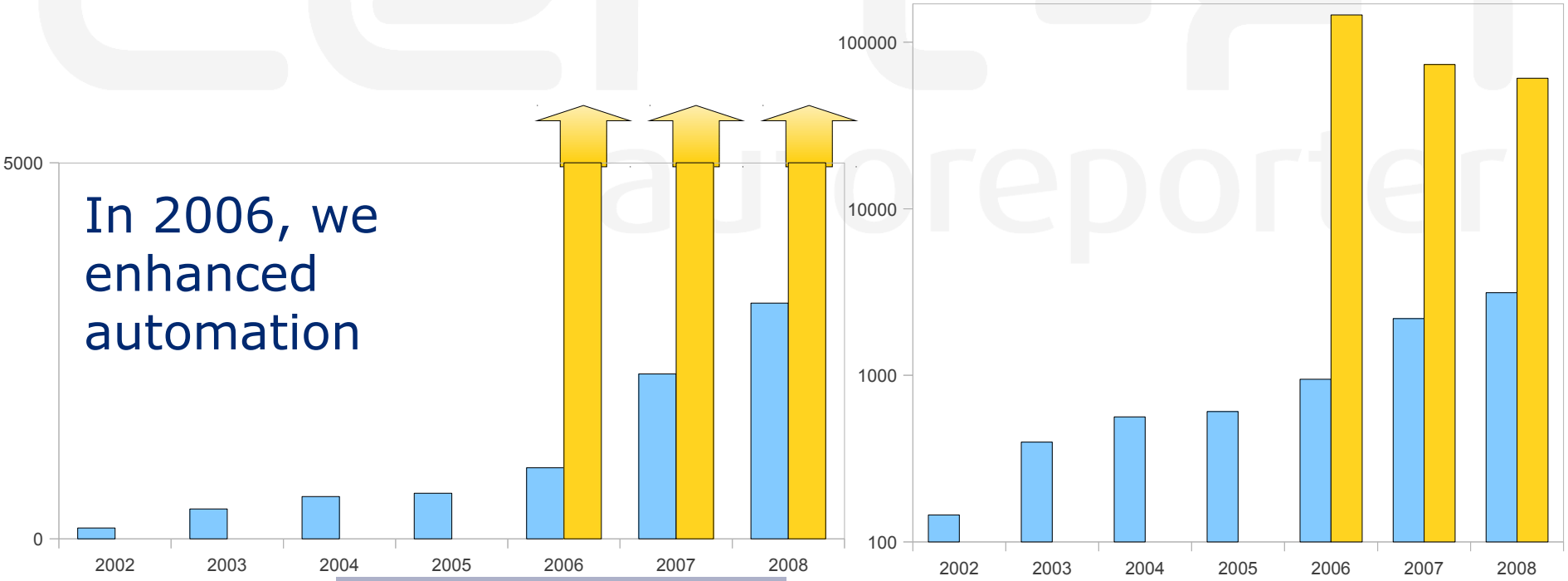
Finnish Communications Regulatory Authority

The Autoreporter Project

cert-fi

How many incidents are there?

- Since 2006, CERT-FI adopted an automated system to systematically collect Incident Reports (mostly malware infections) from various monitoring projects around the world
- **That opened our eyes!!**
- We probably still only see the tip of the iceberg..



Autoreporter

Daily reports

The daily reports are sent as emails with predefined and agreed-upon subjects

All reports are signed

The reported incidents are listed in the body of the email

- The same information is also included as an attached XML-file (IODEF-format)

```
From: cert-fi-autoreporter
Subject: [FICORA #123456] Daily abuse report for your network

CERT-FI has received information regarding systems on your
network which may have security problems. All timestamps are
according to UTC. The format is as follows:

ASN | IP | TIMESTAMP (UTC) | PTR/DNAME | CC | TYPE | INFO

Here CC refers to the country code, TYPE to the type of the secu
problem, CASE to the CERT-FI tracking code for the case, and the
column is reserved for any additional information.

If more information is needed, please contact CERT-FI.

90000 | 1.2.3.4 | 2008-10-01 19:00:00 | 1-2-3-4.adsl.fi | FI | Bo
90000 | 2.3.4.5 | 2008-10-01 06:00:00 |  | FI | Ddos | 123456 | C
90000 | 3.4.5.6 | 2008-10-01 09:00:00 | 3-4-5-6.adsl.fi | FI | Bo
```

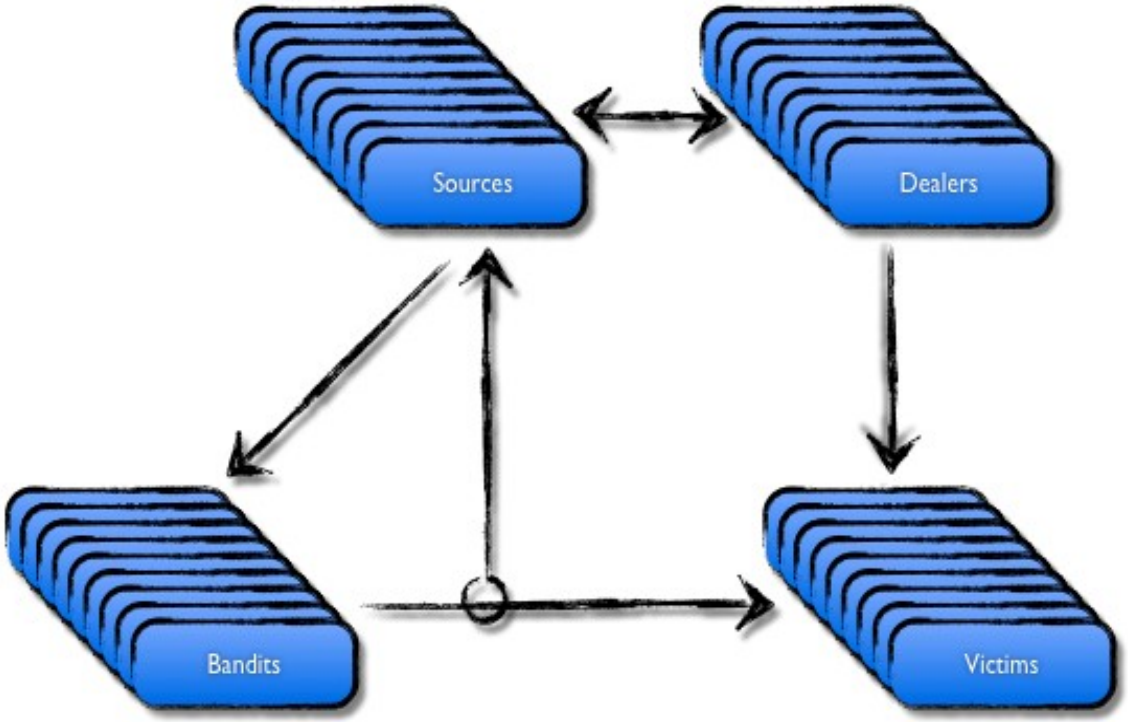

```
<?xml version="1.0" ?>
- <IODEF-Document lang="en" version="1.00" xmlns="urn:ietf:params:xml:ns:iodef-
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="https://www.cert.fi/autoreporter/IODEF-Document.xs
  - <Incident purpose="mitigation">
    <IncidentID name="www.cert.fi">123456</IncidentID>
    <ReportTime>2008-10-01T19:00:00+00:00</ReportTime>
    - <Assessment>
      <Impact lang="en" type="admin" />
    </Assessment>
    - <Contact role="creator" type="organization">
      <ContactName>CERT-FI</ContactName>
      <Email>cert@ficora.fi</Email>
      <Telephone>+35896966510</Telephone>
    </Contact>
    - <EventData>
      <Description>Bot</Description>
```

Abuse Handling Process

- Detecting Abuse
- Receiving reports (email, phone, fax..)
- Stalking badness through data mining
  - Scraping feeds
  - Normalizing data
  - Correlating data
- Dealing with badness
  - Mapping events to address space/netblocks
  - Finding right contacts and their contact preferences
  - Customer expectation management
- Reporting
  - Statistics, trends, chronic cases
- Responding

Autoreporter: Sources (in practice)

- We receive the most useful abuse information from trusted 3rd parties, not-for profit "internet superheroes" that perform
  - Honeypots/nets
  - Sinkholing
  - Malware analysis
  - Spamtraps
  - Malicious URL/ phishing/ defacement tracking
  - Investigations
  - ...



OSINT

Feeds – abusehelper Collab

22nd An... | AusCER... | ToBeNa... | Feeds – ... | Lessons ... | The Lon...

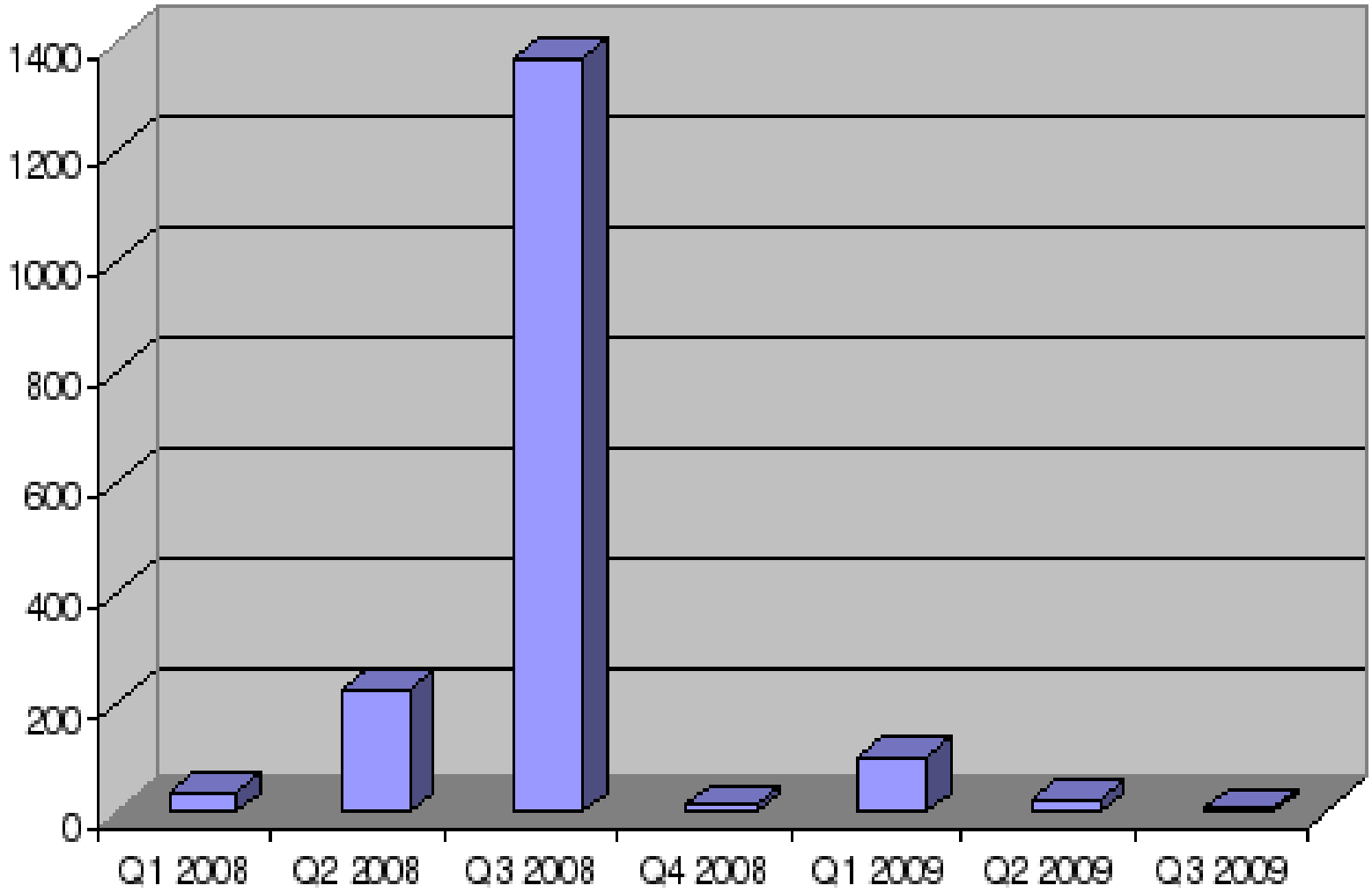
Web site vuln, attack or incident feeds

- Good list: http://www.okamalo.com/2009/11/malicious-ips-and-url-free-databases.html
- Defacements: http://zone-h.org/archive/special=1
- XSS incidents: http://www.xssed.com/archive/special=1
- Some wepawet JS deobfuscation analyses contain CVE:s http://wepawet.cs.ucsb.edu/static/torpig-twitter.html
- Various attack data: http://barometer.interoute.com/barom_stat_alerts.php
- IP blacklists: http://whatismyipaddress.com/staticpages/index.php/is-my-ip-address-blacklisted
- sources of malicious IPs.
  - abusechff http://dnsbl.abuse.ch/fastfluxtracker.php
  - abusechweb http://dnsbl.abuse.ch/webabusetracker.php
  - arbor http://atlas-public.ec2.arbor.net/public/ssh_attackers
  - autoshun http://www.autoshun.org/files/shunlist.csv
  - badguys http://www.t-arend.de/linux/badguys.txt
  - blacklisted http://www.infiltrated.net/blacklisted
  - brawg http://www.brawg.com/hosts.deny
  - cleanmxv http://support.clean-mx.de/clean-mx/xmlviruses?response=alive&format=csv&fields=url,ip,domain&domain=
  - cleanmxp http://support.clean-mx.de/clean-mx/xmlphishing?response=alive&format=csv&fields=url,ip,domain&domain=

Working with Data

- Incoming feeds wide and varied in format, formalism and transports
- Availability (downtime, missed reports, etc)
- Integrity of the information
- Bugs
- Update frequency: near-real-time, hourly, daily..
- Report de-duplication (overlapping refreshes)
- Timespan: last n days, specific date
- Provided details
- Terminology
- Formatting (csv, xml, etc)
- Transports (HTTP, SMTP, IRC, etc)

Finnish Victims to Data Breach Incidents

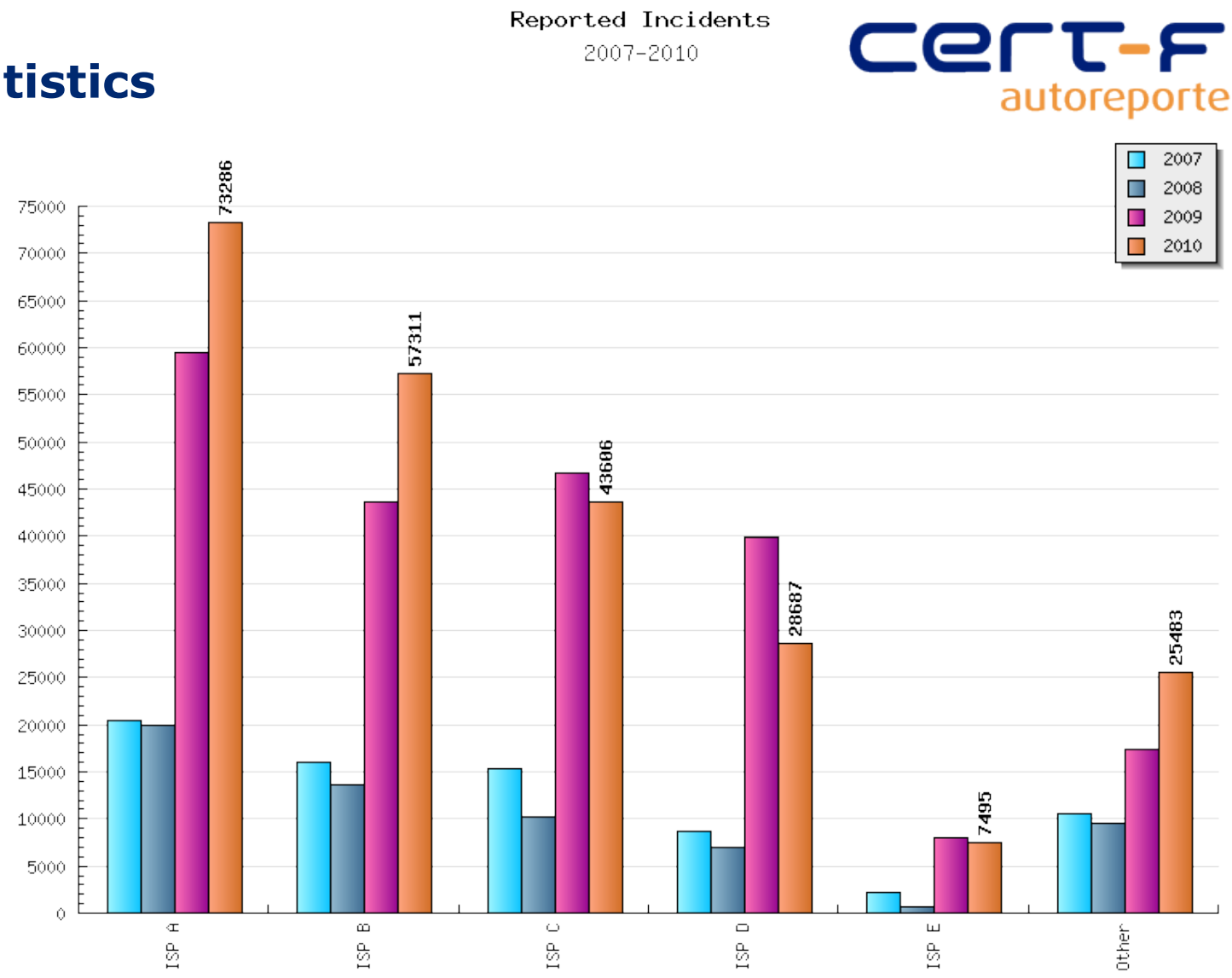


Open Questions Revisited

- What are we not seeing?
- What should I prepare for?
- Am I targeted or just collateral damage?
- Can I trust the data?

Autoreporter Statistics

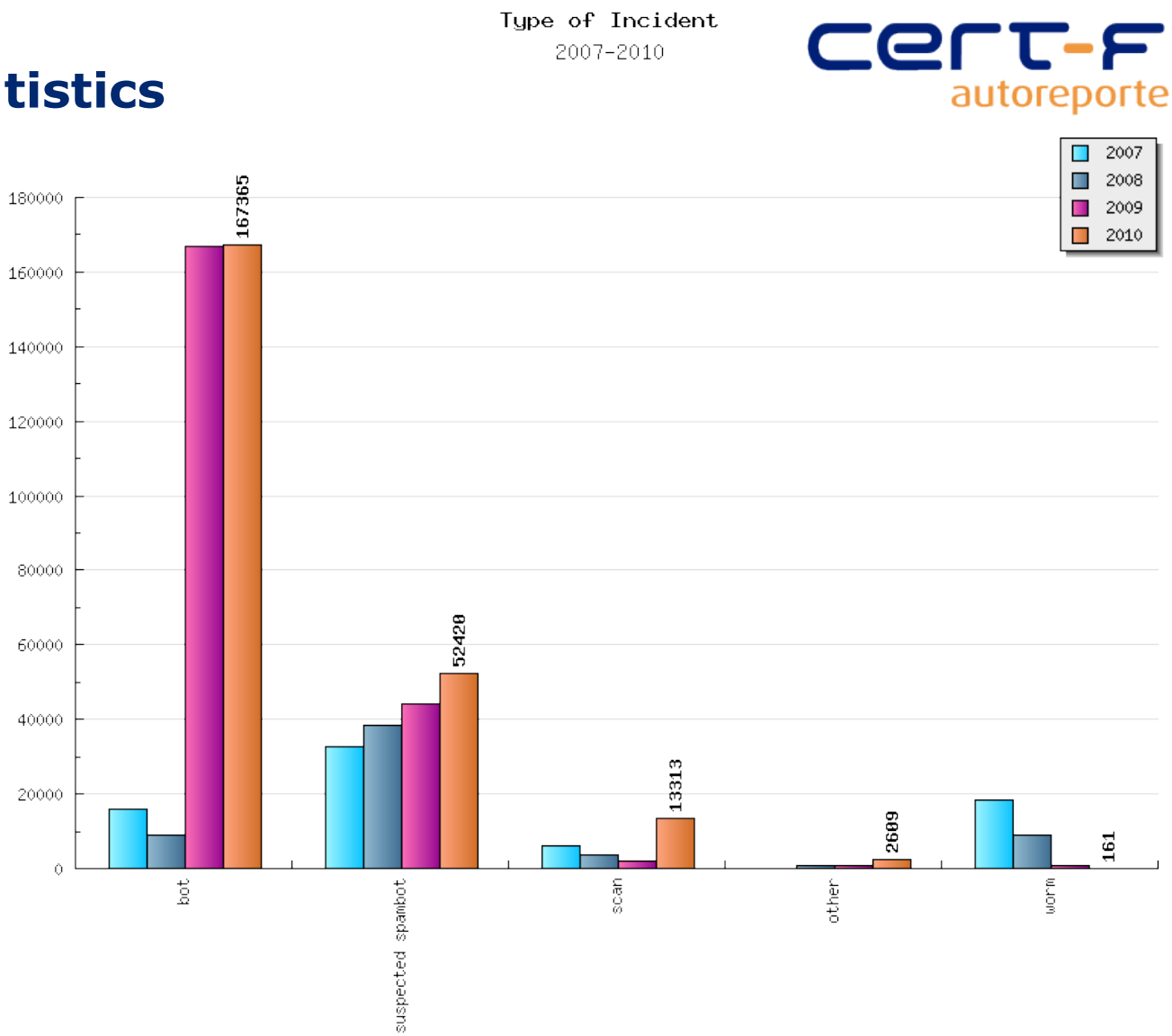
Statistics



Finnish Communications Regulatory Authority

Autoreporter Statistics

Statistics

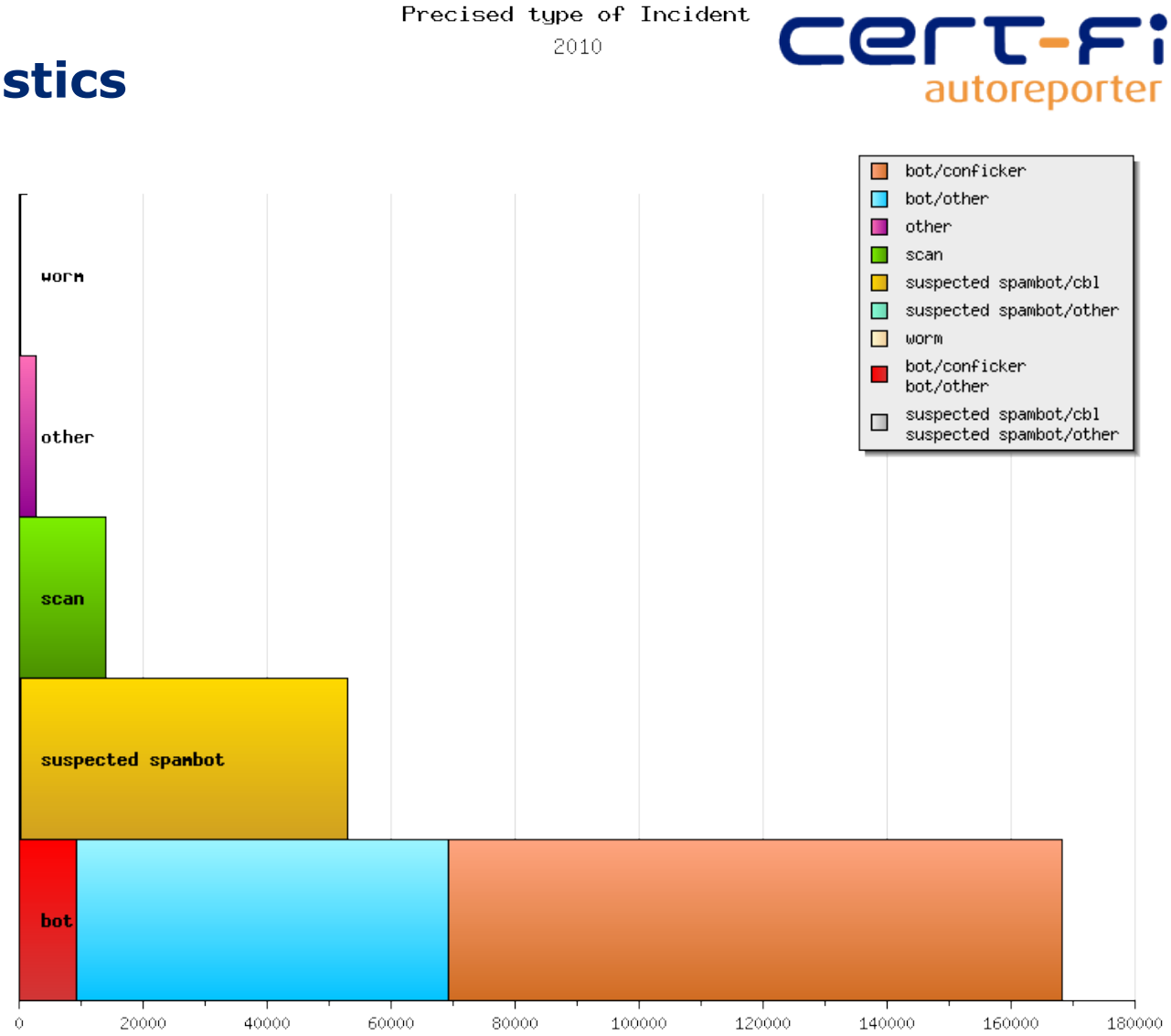


cert-fi autoreporter

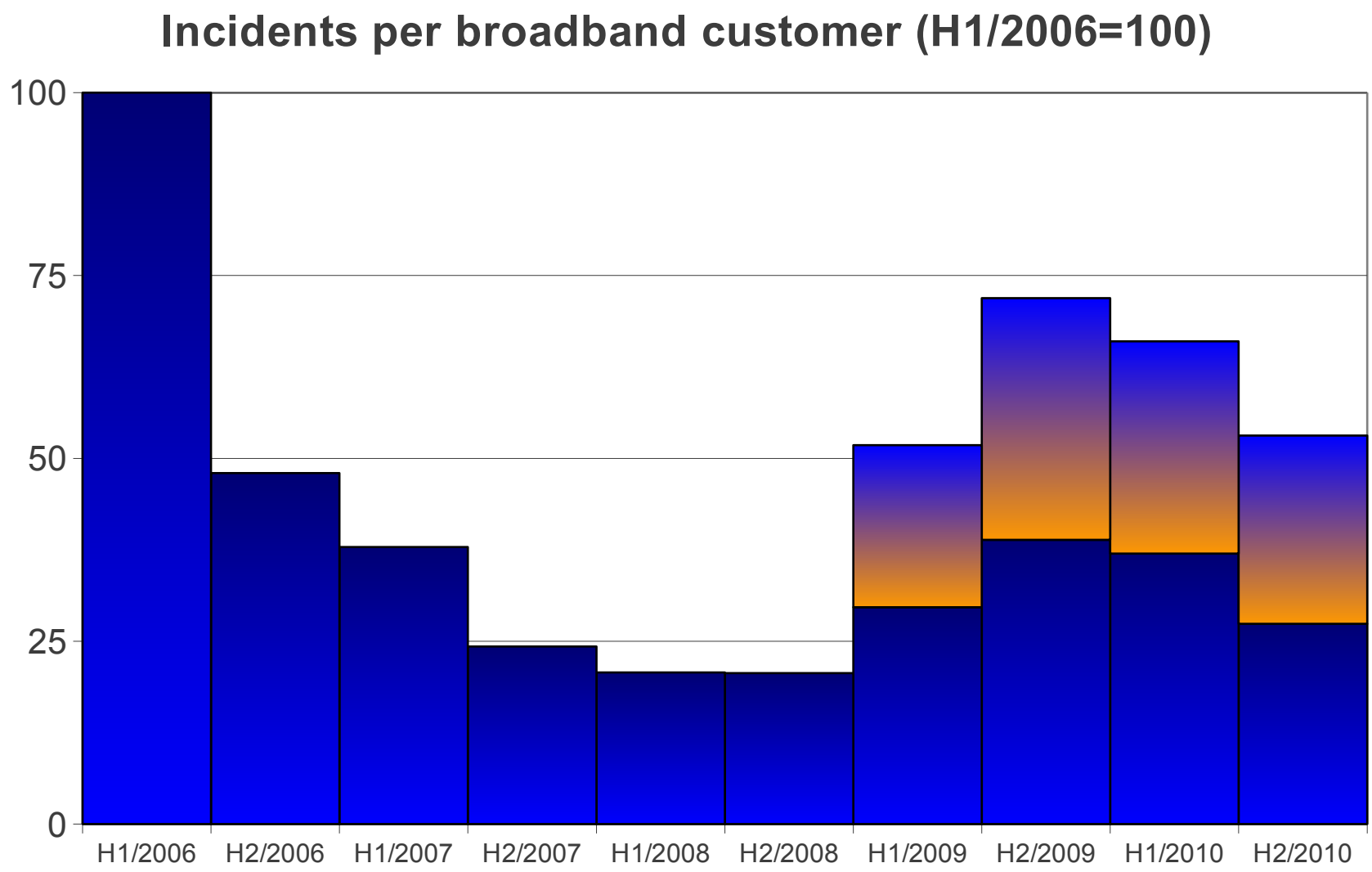
Finnish Communications Regulatory Authority

Autoreporter Statistics

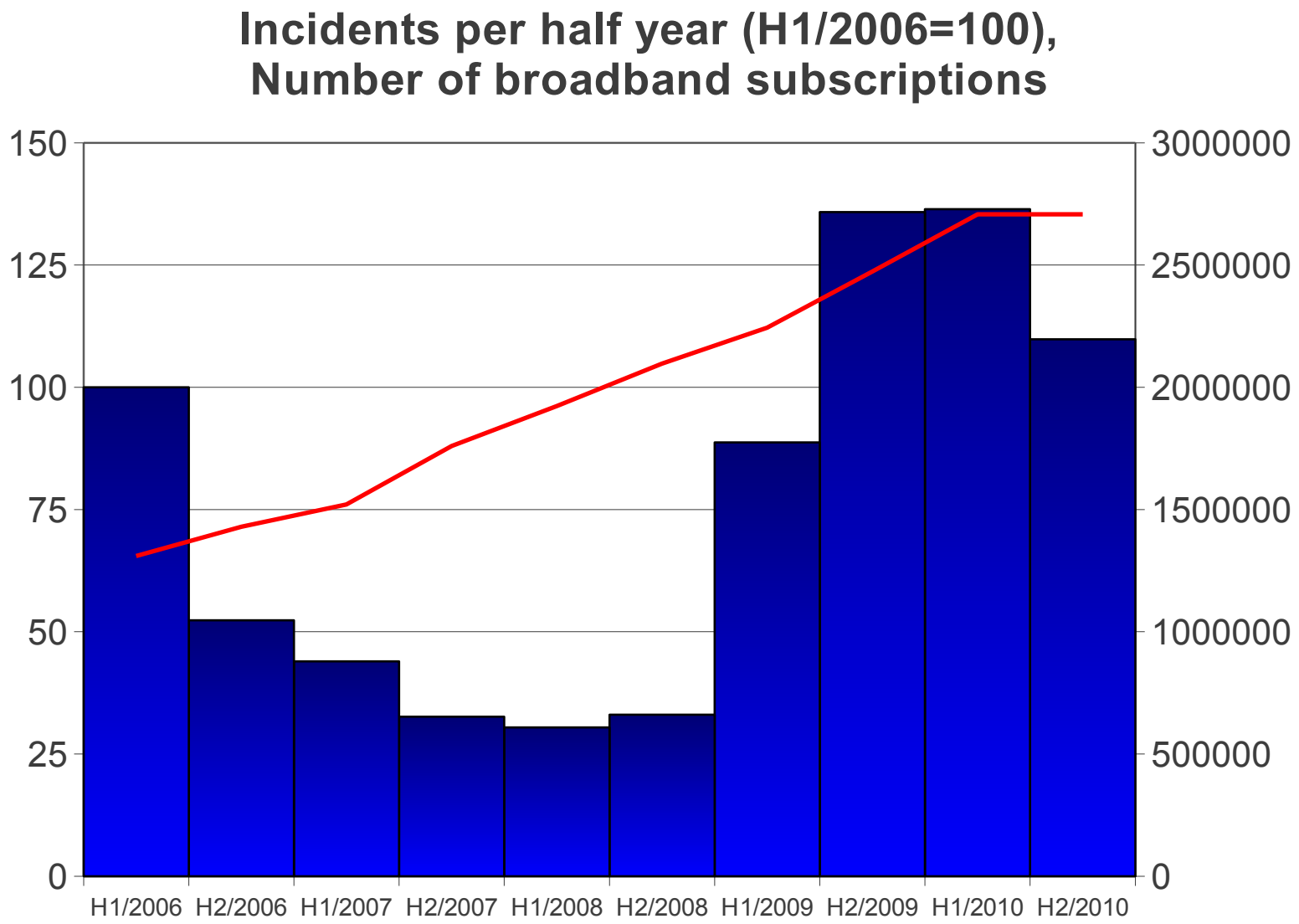
Statistics



Autoreporter Statistics



Autoreporter Statistics

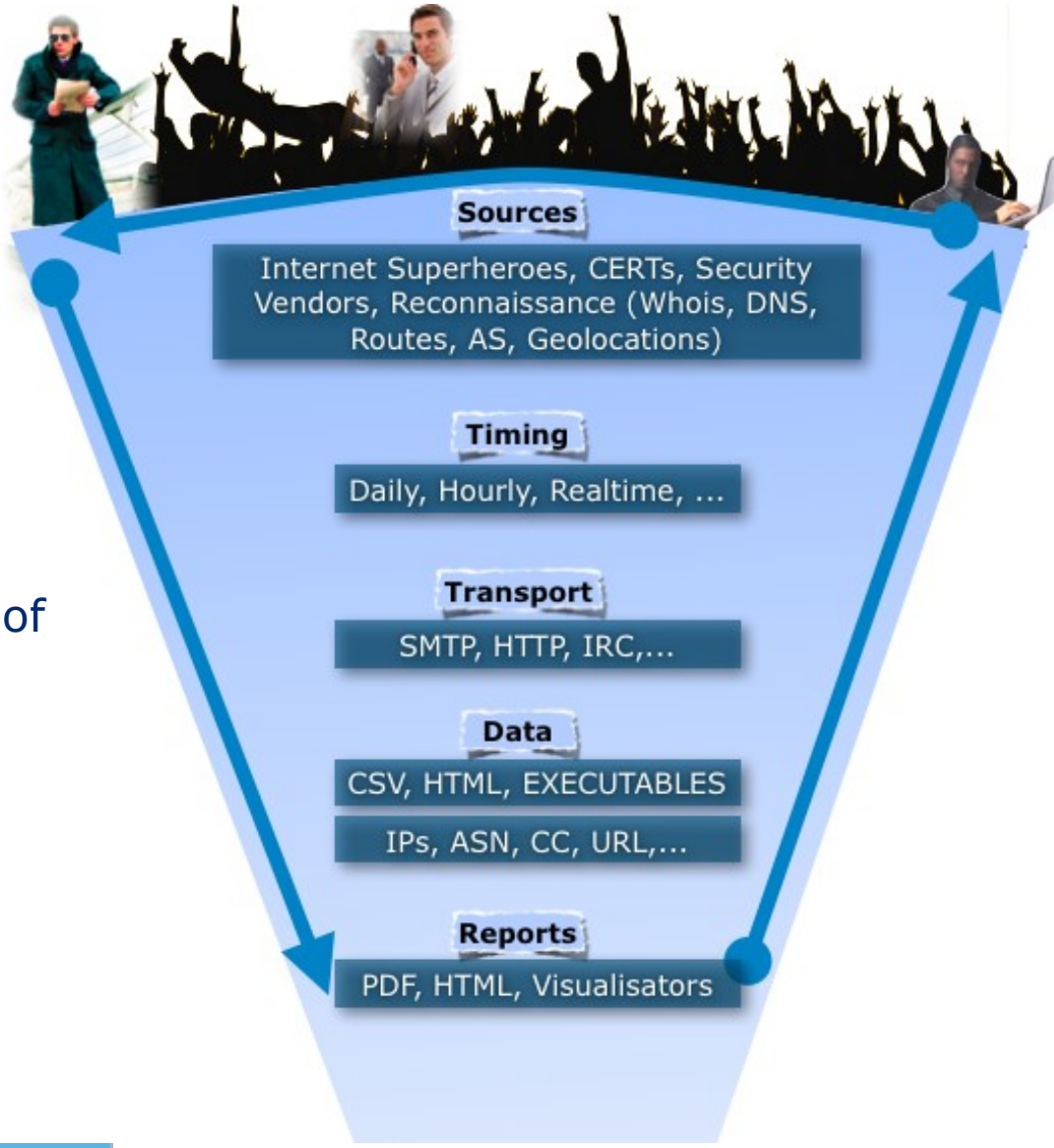


Autoreporter: Challenges

- 5 generations of CERT-FI Autoreporter and 2 generations of CERT-EE Abuse Killer
- Common challenges
  - Works for me, my sources, my processes, my tools
  - Integration with other “worksforme” processes and tools
  - Customer requirements, processes, involvement, commitment
- Progressing from this point might require more of a community effort → enter Abusehelper

https://code.google.com/p/abusehelper

- The goal of the Abusehelper project is to provide common understanding, framework and tools for handling abuse
  - To bring further focus to somewhat scattered Internet Abuse handling scene: documenting and unifying abuse related terminology, documenting assumptions, taking into account different needs, enabling the creation of processes and workflows
  - To take the next step in maturity, from works-for-me information systems to modular, scalable (with regards to performance and usability), commonly developed, and shared one.

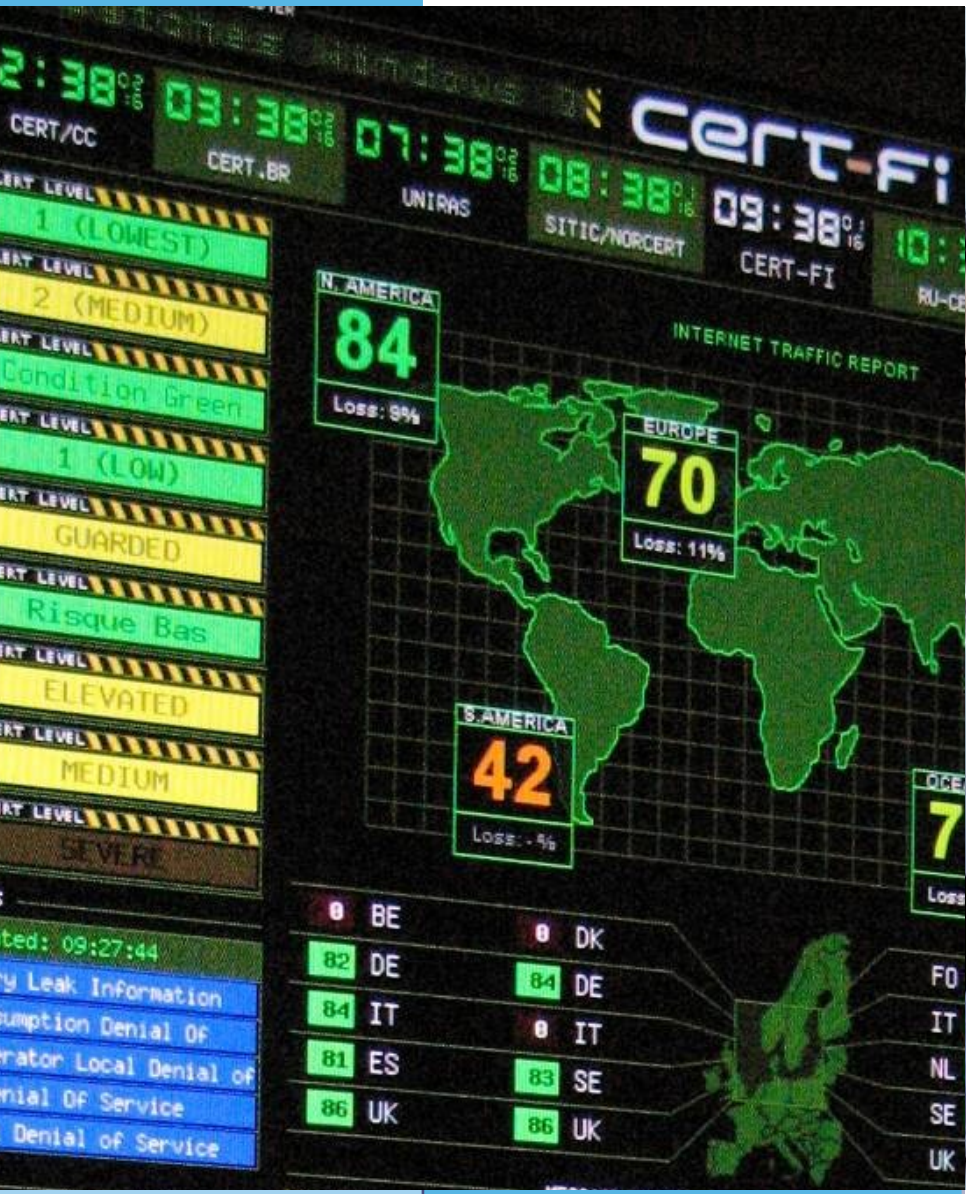


Some Closing Remarks

1. Many (if not most) incidents are detected by outside parties
   - Any Infrastructure/OSINT monitoring will help in finding badness in your network. The more data you grab, the more incidents you will find

1. Working with incident data is difficult
2. Finding working incident reporting contacts is challenging
3. Collaborative use of automation not fully exploited in incident reporting
4. Customers want reports on how they are doing compared to their peers
5. Incident response process maturity
   - All by hand
   - Ad hoc (in-house) scripts
   - Hands on automata (abuse specific ticketing system)
   - Hands off automata

Finnish Communications Regulatory Authority



In collaboration with:

National EMERGENCY SUPPLY Agency

Co-operation for the protection of critical systems

Telephone: +358 9 6966 510

E-mail: cert@ficora.fi

WWW: www.cert.fi

CERT-FI alerts and advisories are available in Finnish via:

- E-mail
- SMS (subscription fees apply)
- web pages
- RSS feed
- TELETEXT page 848 (YLE)

cert-fi