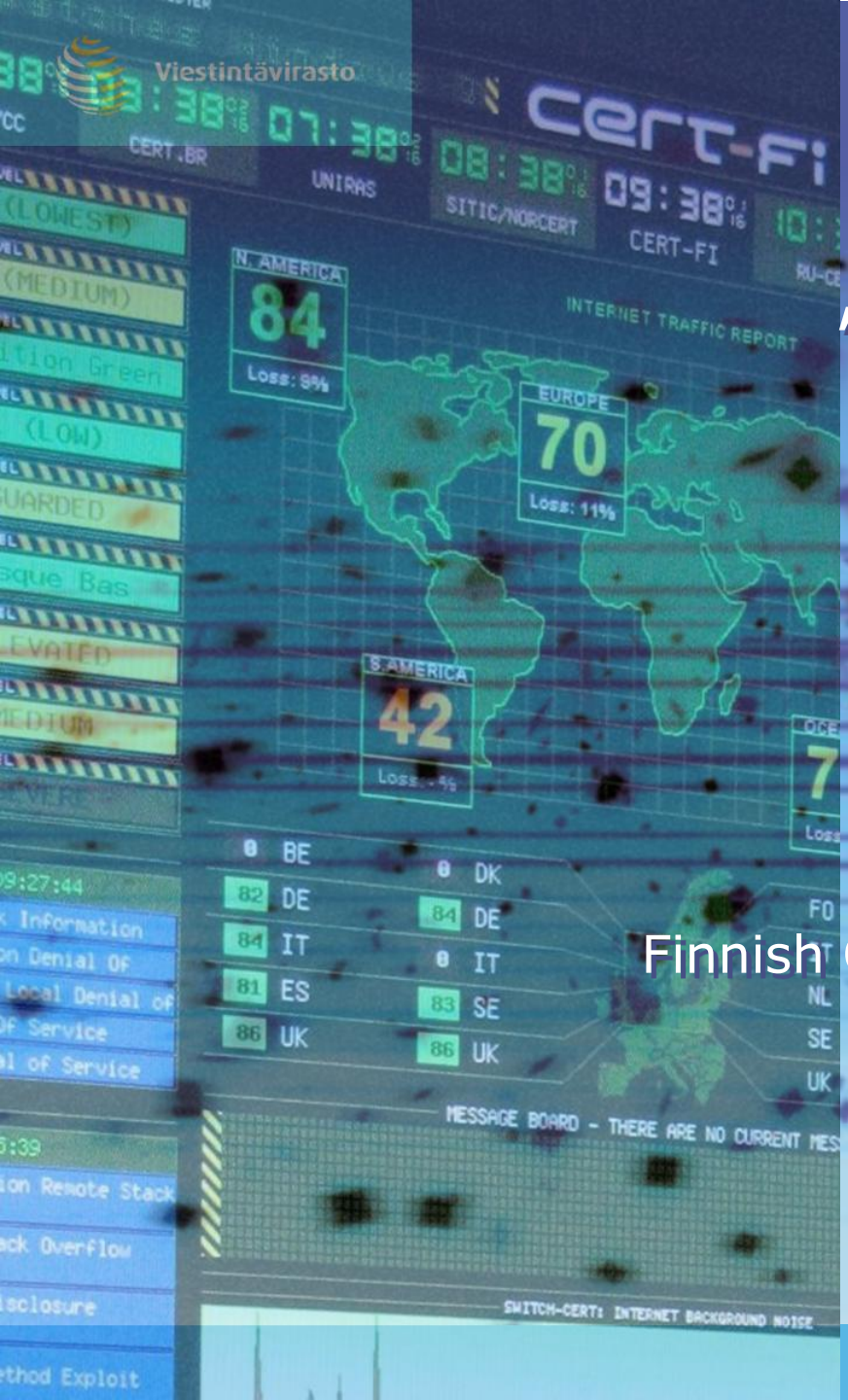


cert-fi

"CERT-FI Autoreporter"

Enisa Resilience Workshop

Brussels

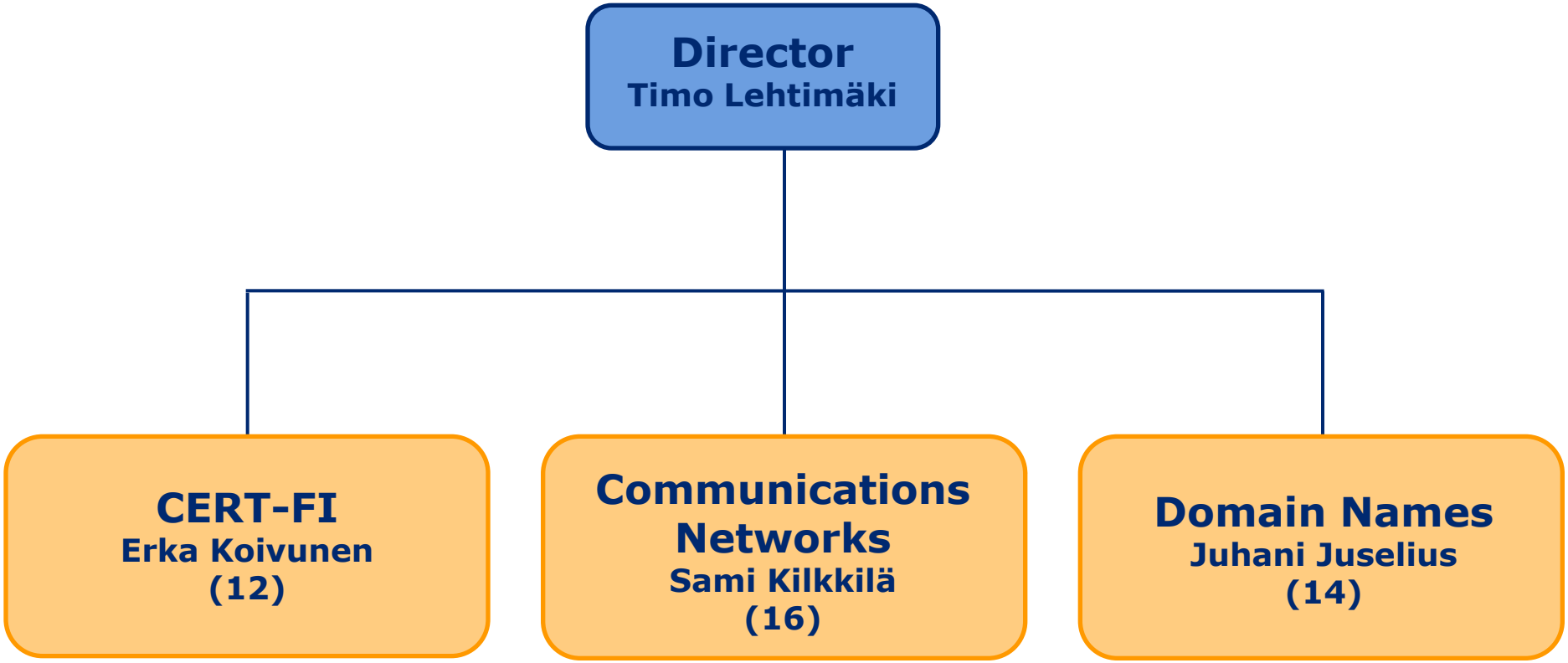
12.-13.11.2008

Sami Kilkkilä
Head of Communication Networks
Finnish Communications Regulatory Authority

Presentation material produced by:
Thomas Grenman
Information Security Adviser
CERT-FI

Networks and Security Division

Organisation



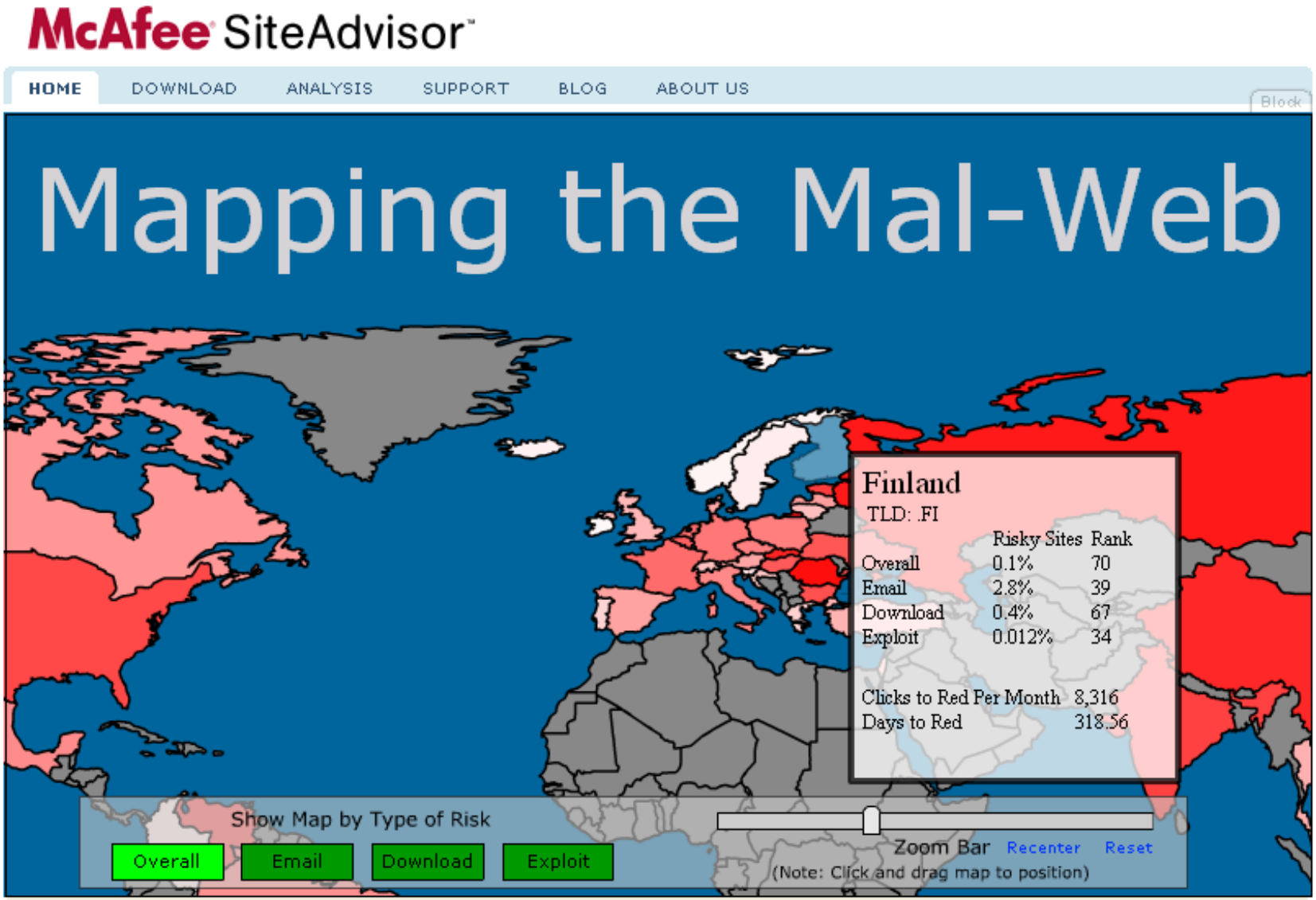
Number of employees in brackets

Autoreporter

What?

- Autoreporter is a service, which automatically collects data on malware and information security incidents related to Finnish networks
- The data is constantly collected from various sources
- The incidents are categorised and daily reports are compiled and sent to the network operators
- Autoreporter is integrated with CERT-FI's ticketing system
- The granularity of the reporting is currently based on AS-numbers (IP-blocks under consideration)
- The service has been in use since late 2005 and it covers roughly 160 AS-numbers

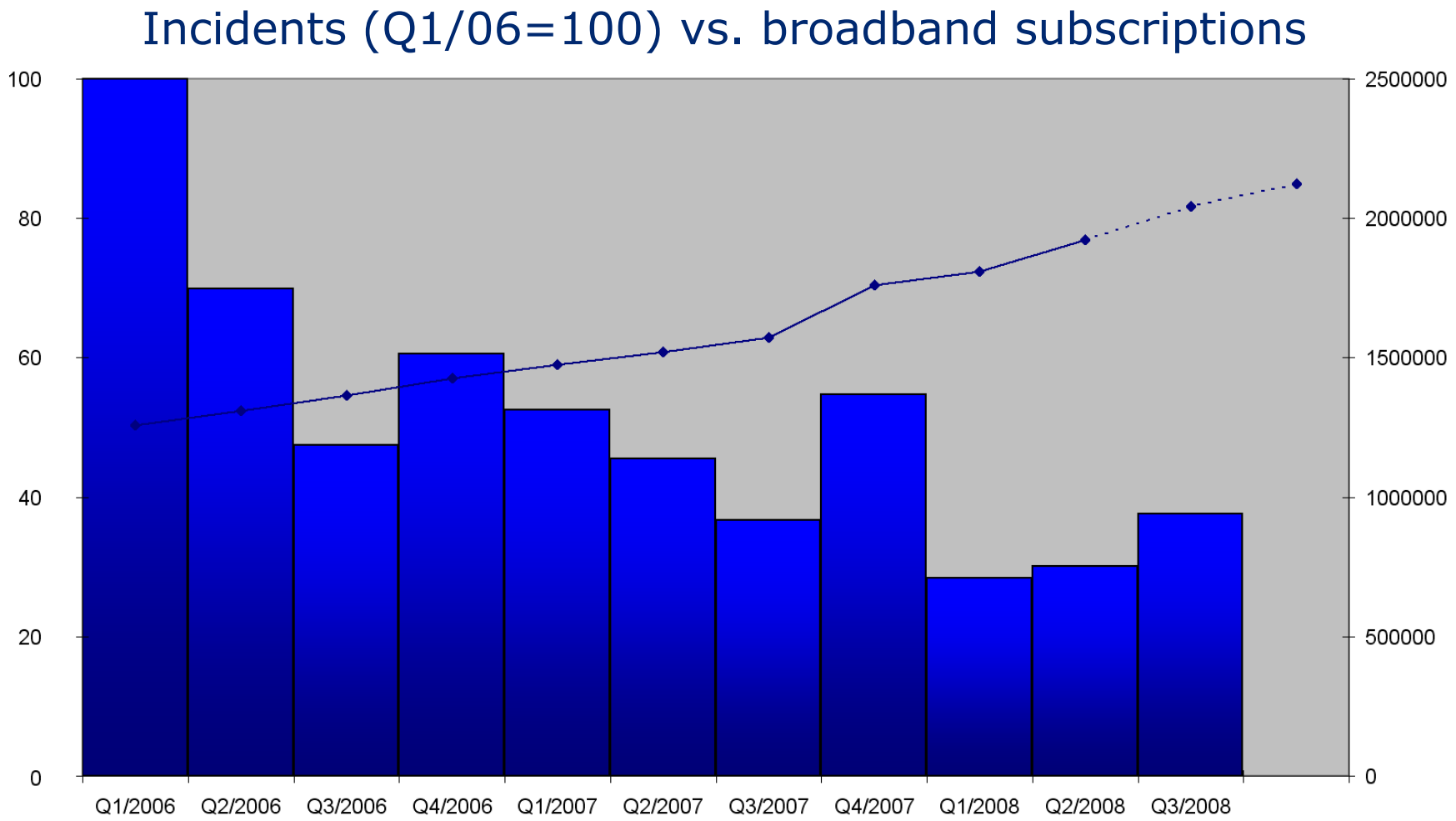
Autoreporter



Sources of information

- We use a threefold category of the processed sources
  - *"primary"* sensor networks and intrusion detection systems operated by CERT-FI
  - *"secondary"* telecommunications operators, corporate or association subscribers, news agencies, governmental bodies, local law enforcement, AV vendor, ...
  - *"tertiary"* third-party operated dark- and/or honeynets, trustworthy blogs, RSS-feeds, Zone-H.org, XSSed.com, ...
- We have started at the bottom, working our way up (this is mostly an issue with results vs. costs)

Statistics


Incidents (Q1/06=100) vs. broadband subscriptions
100
80
60
40
20
0
2500000
2000000
1500000
1000000
500000
0
Q1/2006
Q2/2006
Q3/2006
Q4/2006
Q1/2007
Q2/2007
Q3/2007
Q4/2007
Q1/2008
Q2/2008
Q3/2008

Autoreporter

Challenges...

- Keeping our database with contact information and AS-numbers up to date (e.g., moving from 16 to 32 bits)
- Keeping the codebase clean and maintainable

...and future improvements

- The information processing is made more generic (i.e., built upon a common framework with specific plug-ins for the different sources of data)
- The categorisation of incidents and the daily reports are strictly formatted (e.g., using IODEF/RFC 5070) making it easier for the recipients to process
- Constantly looking for new sources of information

Autoreporter

- **Daily reports**
- The daily reports are sent as emails with predefined and agreed-upon subjects
- 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
problem, CASE to the CERT-FI tracking code for the case, and
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 | Ddos | 1234
90000 | 2.3.4.5 | 2008-10-01 06:00:00 | FI | Ddos | 1234
90000 | 3.4.5.6 | 2008-10-01 09:00:00 | 3-4-5-6.adsl.fi | FI | Ddos | 1234

Regards,

CERT-FI autoreporter

CERT-FI duty desk: +358 9 6966 510
E-mail: cert@ficora.fi
```


```
<?xml version="1.0" ?>
- <IODEF-Document lang="en" version="1.00" xmlns="urn:ietf:params
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="https://www.cert.fi/autoreporter/IODEF-
  - <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>+35869660510</Telephone>
    </Contact>
    - <EventData>
      <Description>Body</Description>
      <Expectation action="investigate" />
      - <EventData>
        - <Flow>
          - <System category="source">
            - <Node>
              <NodeName>1-2-3-4.adsl.fi</NodeName>
              <Address category="ipv4-addr">1.2.3.4</Address>
              <Address category="asn">90000</Address>
            </Node>
          </System>
        </Flow>
      </EventData>
    </EventData>
  </Incident>
  - <Incident purpose="mitigation">
    <IncidentID name="www.cert.fi">123456</IncidentID>
    <ReportTime>2008-10-01T06:00:00+00:00</ReportTime>
    - <Assessment>
      <Impact lang="en" type="dos">C&C at 4.5.6.7:6667, AS 7000
```

telephone: +358 9 6966 510
e-mail: cert@ficora.fi
www: www.cert.fi

Public alerts and advisories (in Finnish):

- E-mail alert service
- SMS alert service (pay-per-subscription)
- CERT-FI www-pages
- RSS newsfeed
- YLE teletext page 848

National EMERGENCY SUPPLY Agency
Co-operation for the protection of critical systems