cert-fi

Co-operation against cybercrime CSIRTs – LE – private sector

Octopus Interface 2010

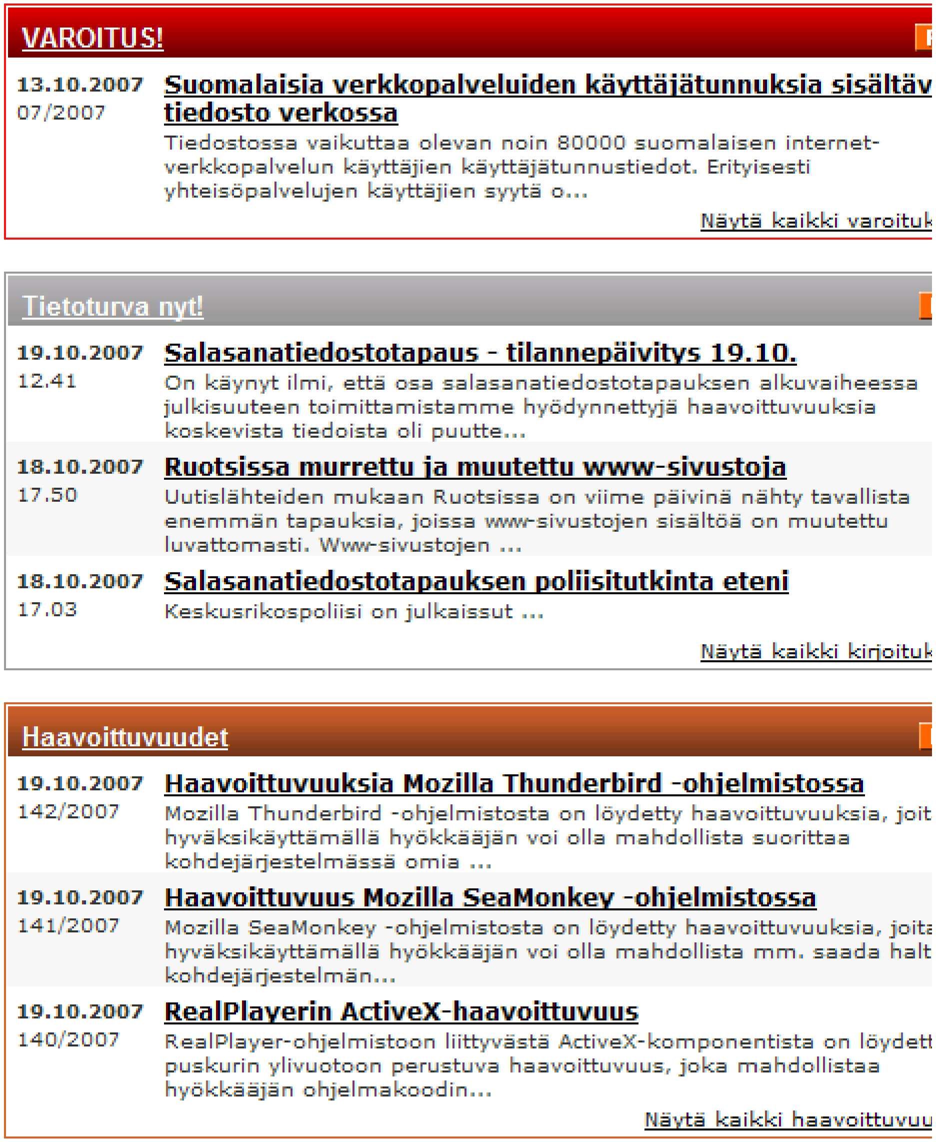
Kauto Huopio
Sr. Infosec Advisor
Finnish Communications
Regulatory Authority

CERT-FI – Finnish national CSIRT authority

- National Point of Contact for incident reports
- Incident Handling

- National Information Security Situation Awareness Service
- Vulnerability Coordination

On duty 24/7/365



VAROITUS!

13.10.2007
07/2007
Suomalaisia verkkopalveluiden käyttäjätunnuksia sisältäv tiedosto verkossa
Tiedostossa vaikuttaa olevan noin 80000 suomalaisen internet-verkkopalvelun käyttäjien käyttäjätunnustiedot. Erityisesti yhteisöpalvelujen käyttäjien syytä o...

Näytä kaikki varoituk

Tietoturva nyt!

19.10.2007
12.41
Salasanatiedostotapaus - tilannepäivitys 19.10.
On käynyt ilmi, että osa salasanatiedostotapauksen alkuvaiheessa julkisuuteen toimittamistamme hyödynnettyjä haavoittuvuuksia koskevista tiedoista oli puutte...

18.10.2007
17.50
Ruotsissa murrettu ja muutettu www-sivustoja
Uutislähteiden mukaan Ruotsissa on viime päivinä nähty tavallista enemmän tapauksia, joissa www-sivustojen sisältöä on muutettu luvattomasti. Www-sivustojen ...

18.10.2007
17.03
Salasanatiedostotapauksen poliisitutkinta eteni
Keskusrikospoliisi on julkaissut ...

Näytä kaikki kirjoituk

Haavoittuvuudet

19.10.2007
142/2007
Haavoittuvuuksia Mozilla Thunderbird -ohjelmistossa
Mozilla Thunderbird -ohjelmistosta on löydetty haavoittuvuuksia, joit hyväksikäyttämällä hyökkääjän voi olla mahdollista suorittaa kohdejärjestelmässä omia ...

19.10.2007
141/2007
Haavoittuvuus Mozilla SeaMonkey -ohjelmistossa
Mozilla SeaMonkey -ohjelmistosta on löydetty haavoittuvuuksia, joita hyväksikäyttämällä hyökkääjän voi olla mahdollista mm. saada halt kohdejärjestelmän...

19.10.2007
140/2007
RealPlayerin ActiveX-haavoittuvuus
RealPlayer-ohjelmistoon liittyvästä ActiveX-komponentista on löydett puskurin ylivuotoon perustuva haavoittuvuus, joka mahdollistaa hyökkääjän ohjelmakoodin...

Näytä kaikki haavoittuvuu

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

VAROITUS!

13.10.2007
07/2007
Suomalaisia verkkop
tiedosto verkossa
Tiedostossa vaikuttaa o
verkkopalvelun käyttäjie
yhteisöpalvelujen käyttä

Tietoturva nyt!

19.10.2007
12.41
Salasanatiedostotap
On käynyt ilmi, että osa
julkisuuteen toimittamis
koskevista tiedoista oli

18.10.2007
17.50
Ruotsissa murrettu j
Uutislähteiden mukaan
enemmän tapauksia, jo
luvattomasti. Www-sivus

18.10.2007
17.03
Salasanatiedostotap
Keskusrikospoliisi on jul

Haavoittuvuudet

19.10.2007
142/2007
Haavoittuvuuksia Mo
Mozilla Thunderbird -ohj
hyväksikäyttämällä hyök
kohdejärjestelmässä om

19.10.2007
141/2007
Haavoittuvuus Mozil
Mozilla SeaMonkey -ohje
hyväksikäyttämällä hyök
kohdejärjestelmän...

19.10.2007
140/2007
RealPlayerin ActiveX
RealPlayer-ohjelmistoon
puskurin ylivuotoon peru
hyökkääjän ohjelmakoo

Special about the Finnish model..

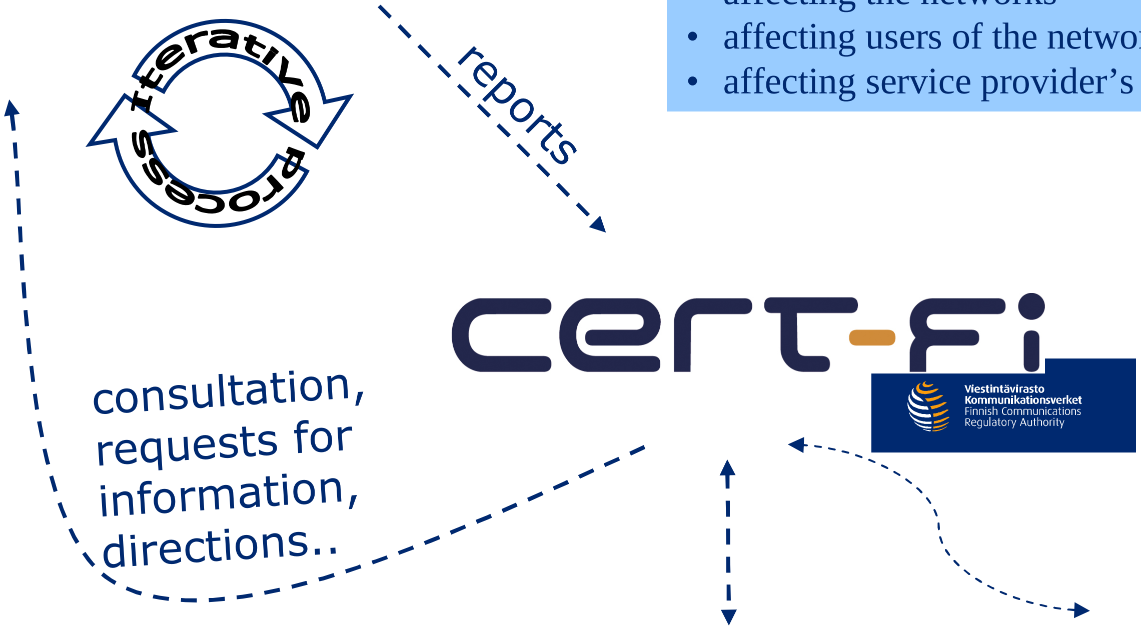
etc.. (>300 TelCos)

Telecommunications operators

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


Iterative process
reports
consultation, requests for information, directions..
cert-fi
Viestintävirasto
Kommunikationsverket
Finnish Communications Regulatory Authority

General Public
(& Central Government)

Critical Infrastrucure

- Energy
- Finance
- Logistics
- Basic Industry

Role of a national CSIRT

- **CERT-FI is the national point of contact for incident & abuse reports related to information security incidents**
  - Major ISPs have their own teams
  - CERT-FI is _not_ the law enforcement PoC
- Due to the very networked nature of CSIRT activity, CERT-FI is often the first government authority in Finland to receive information about an information security incident or ICT crime in progress
- Fast and appropriate redelivery of this information is critical on limiting the adverse effects of the incident in question

Roles of CERT-FI and LE in Finland

- CERT-FI has the mandate to investigate violations of and threats to information security. This means in practice giving assistance in following areas to the affected parties:
  - Verifying that the incident is a valid case
  - Identifying the breadth and seriousness of the incident
  - Incident information delivery to all affected parties
    - anonymisation if necessary
  - Coordination of the case with other authorities
  - Directing the actions needed to limit the adverse effects of the information security incident
  - Securing the affected ICT infrastructure

CERT-FI and LE in Finland

- **Any further investigative work is within the area of the pre-trial investigation powers of the law enforcement authorities**
- CERT-FI has good working relationship with the whole LE structure in Finland, NBI IT investigation in particular
  - Victims are actively informed on LE contacts and adviced on the possibility to report a crime
  - Victims are assisted to find the most relevant police unit capable to take the case
  - Victims are assisted and reminded on securing the evidence
  - Many positive customer experiences – easing the concerns regarding reporting a crime to law enforcement

CERT-FI and law enforcement experiences

- CSIRT teams are often in a position to introduce case-related LE authorities to each other
  - The incident related to Finland can be a part of a major case widely known in the CSIRT community – and already under LE investigation known to CSIRTs
- CERT-FI providing assistance on specialist technical analysis, especially related to malware
- Background information on global level incidents

Joint report on infomation stealing malware

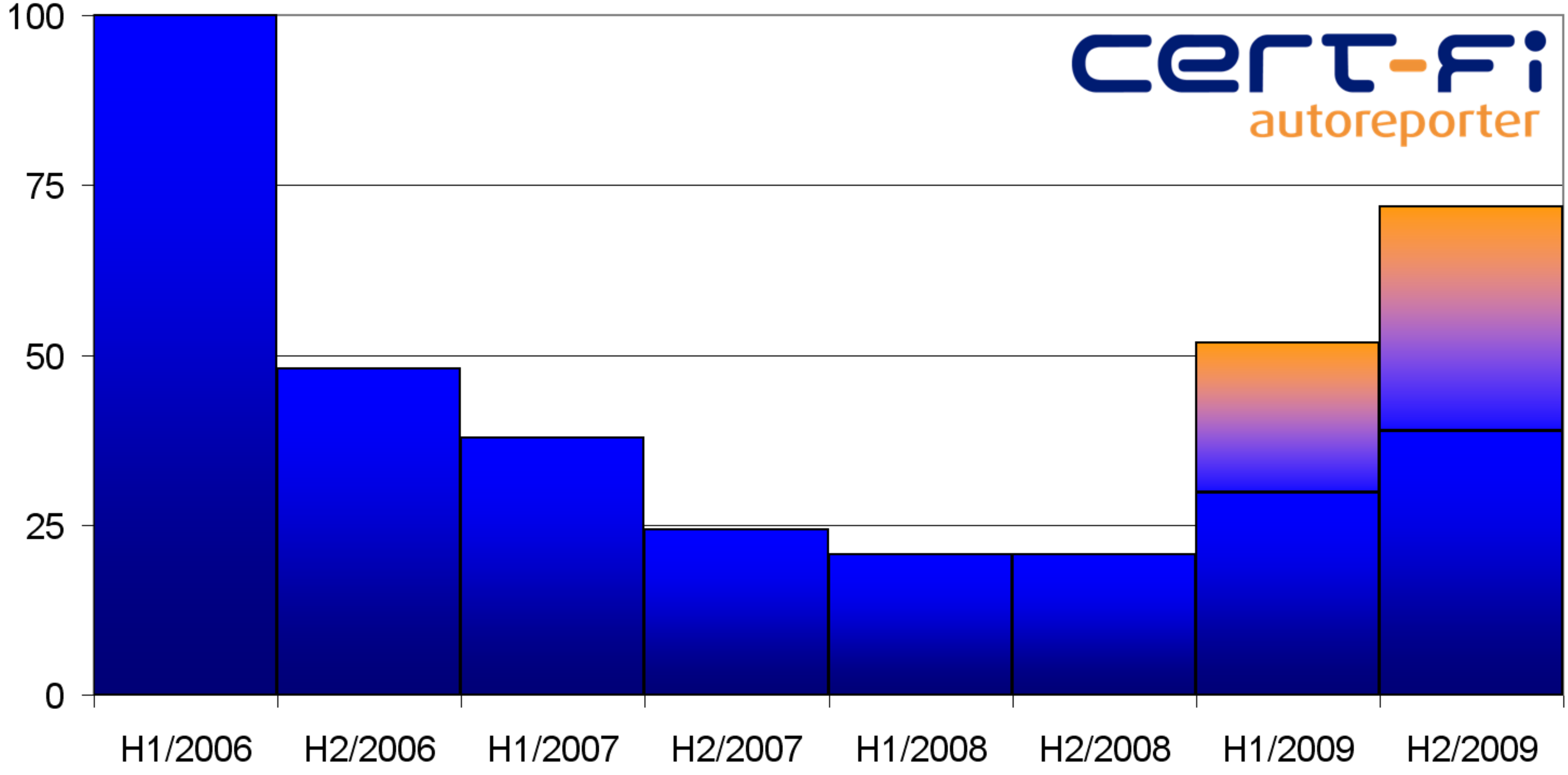
- **CERT-FI, National Bureau of Investigation Finland (NBI) and the Finnish Data Protection Ombudsman have jointly developed a report on data stealing malware**
  - Description of the threat landscape
  - Description of the government authorities and other parties involved in information exchange
  - Description of the legal enviroment and paths/limitations on information sharing
- Report to be available soon available in English at CERT-FI website:
  http://www.cert.fi

CERT-FI Autoreporter

- Autoreporter is a service to collect malware and information security incidents related to Finnish networks from worldwide resources
- Incidents are automatically reported to relevant network maintainers (ISP NOCs or abuse teams)
- Service has been in operation since 2006 and covers all network areas in Finland
- Many ISP:s have automated their receiving processing of these reports
- Autoreporter has clearly caused **a positive effect on the cleanliness of Finnish IP space**
- Further service development with CERT-EE: Abuse Helper
- Current statistics show challenges with Conficker worm

Statistics

Incidents per broadband customer (H1/2006=100)



Observations on recent developments

- Criminal operatives have enhanced their practices on gaining access to network resources
  - IP address space
  - Network capacity with ISP level routing capability
  - Computer hosting facilities
- These capabilities are not stolen, but “purchased”
- With these properly arranged, technically the criminal enterprise on the network looks exactly the same as a regular internet service provider (ISP)
- There are indications of increased activity on this area, related to operation of several common malware operating infrastructures

Observations

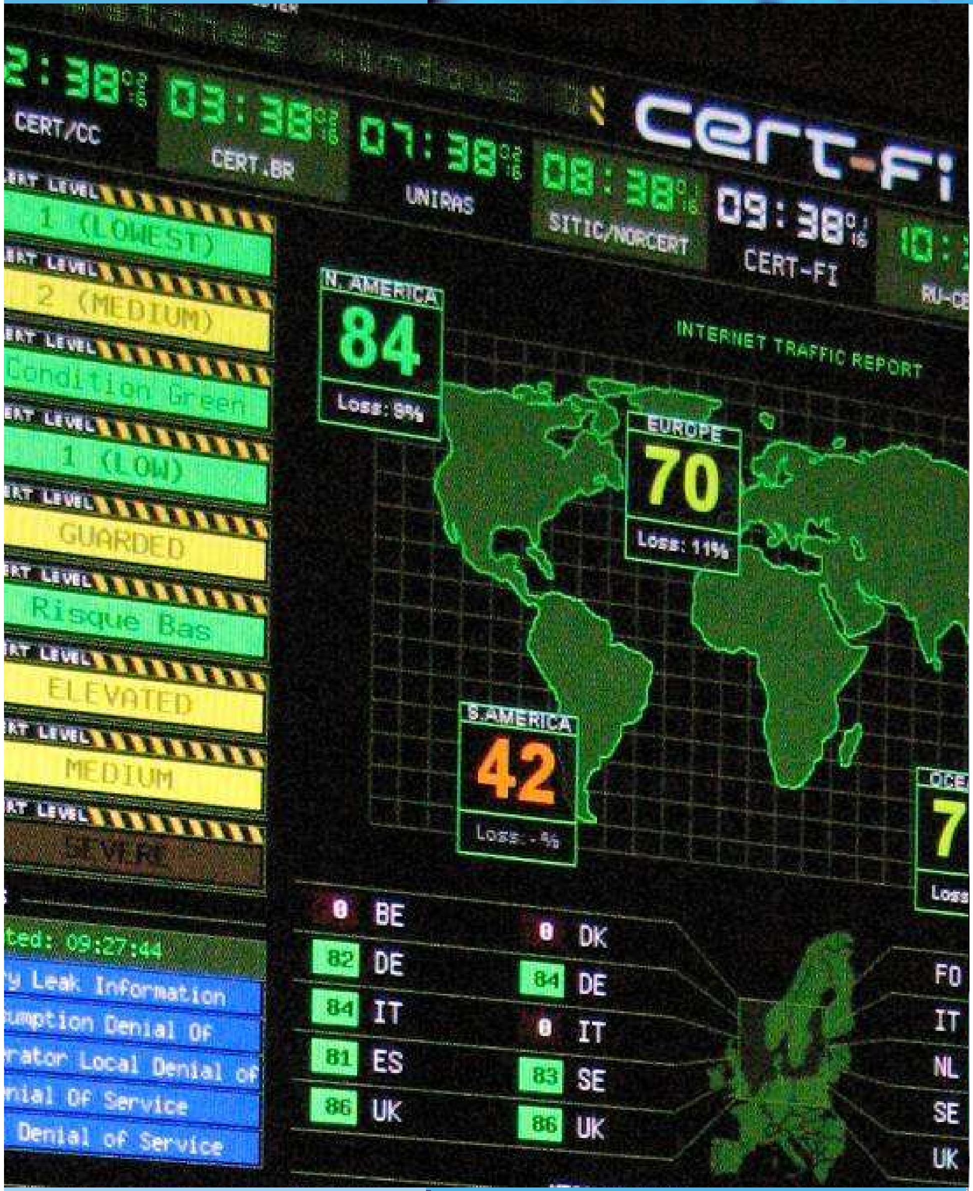
- The task of RIRs (Regional Internet Registries) in processing applications for address space and AS (autonomous system) resources is a challenging one
  - registration document and data verification
  - Need for active coordination with CSIRT and LE communities
- Similar, even more challenging situation with the domain registries and registrars
  - *Operating a "clean" country code top level domain is possible*
- ISPs need education on signs of a potentially malicious customers
  - Issues mostly (but not always) related to small providers in a financially challenged situation and without a properly resourced security department

Observations II

- The criminal actors are very well aware of the challenges related to cyber crime case investigations
  - Initiation of a LE investigation takes a lot of time – at least from a Internet time perspective
  - Criminals try clearly to maximise on unenforceability
- The networks of CSIRTs, responsible ISP security teams and security researchers are used to act in a very short timeframe
  - These networks are based not on international agreements but on a trust developed on day-to-day incident handling
  - Operational security community is capable of working together and self organising
  - The community’s focus is usually short-term, but effective

Observations III

- Networking of CSIRTs, global security community at large and LE resources – can create very positive results
  - The community is very willing to assist LE
  - There is a need for longer-term attention span and proper ”broad picture” –analysis
  - There is a lot of background information and data available
  - The membership in the communities is ad-hoc, trying to grow as fast as possible while maintaining the very high level of trust involved
  - Appropriate legal limitations, information “firewalls” must be applied and understood by all participating parties
  - Support and network with your national and sector-spesific CSIRT teams!



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)