CERT.PT
Serviço de Resposta a Incidentes de Segurança Informática

Update on CERT.PT

TF-CSIRT, León 2009

Lino Santos

Presentation objectives

- Get to know FCCN
- Get to know cert.pt activities
- Get to know cert.pt national and international cooperation

Agenda

- What does FCCN do?
- CERT.PT
- National cooperation
- International cooperation
- Other security activities
- Future development

What does FCCN do?

Private non-profit organization

- National Foundation for Scientific Computing
  - Foundation for Science and Technology
  - University Dean Council
  - National Laboratory of Civil Engineering

- Board
  - Pedro Veiga (Head)
  - Lusitana Fonseca
  - Pedro Guedes Oliveira
  - Gaspar Barreira
  - Maria Alzira Santos

- Staff: ~75

What does FCCN do?

The network

- FCCN manages the Portuguese NREN, TLD .pt and Portuguese IXP;
- More than 100 Higher Education and Research institutions
- More than 8.000 public schools
- More than 200 disability associations
- Own fiber between Valença - Braga - Lisbon - Elvas
- 10Gbps to London, 2.5 Gbps to Madrid

What does FCCN do?

Government initiatives

Portuguese Key Initiatives:

1. RCTS
2. Connecting Schools over Broadband
3. e-U - Virtual Campus
4. b-On - Online Knowledge Library

New Development Domains

a) Grid Computing

b) VOIP

Agenda

- What does FCCN do?
- CERT.PT
  - Short description
  - Statistics
  - Resources and funding
- National cooperation
- International cooperation
- Other security activities
- Future development

Mission

- Offering technical support to computer users in resolving security incidents, advising on best-practices, analyzing artifacts, and coordinating actions with the parties involved.
- Gather and disseminate a set of information about vulnerabilities and recommendations, pertaining to potential security risks and ongoing malicious activities
- Gather from accredited sources information related to security vulnerabilities, and act on the community with the goal of minimizing impact at the National level
- Promote the creation of new CERT/CSIRTs in Portugal, and raise awareness of security issues on computer users

Constituency

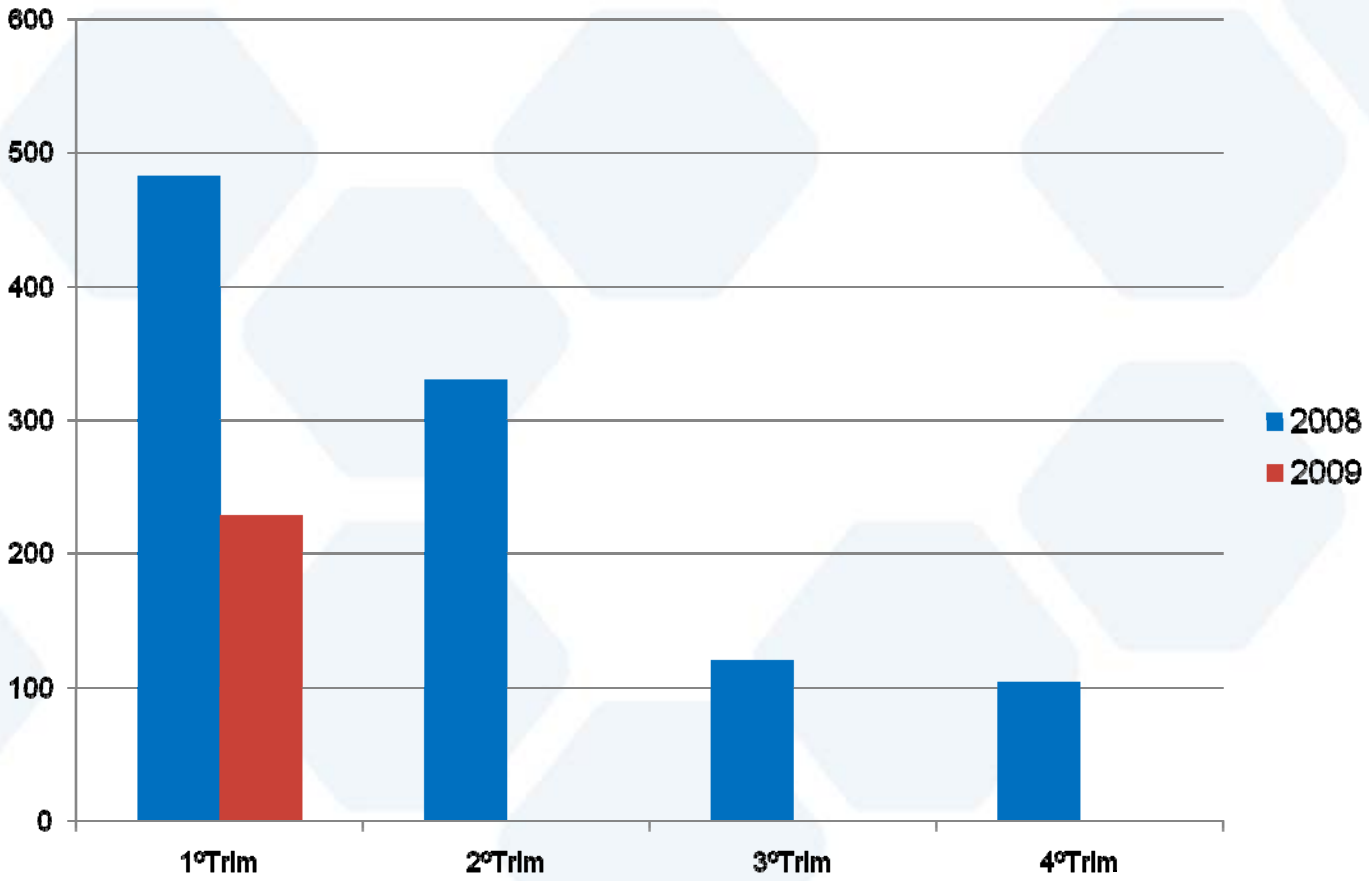
- IPv4 e IPv6 IP address blocks assigned by RIPE
- NREN
- School network
- NOCs
- FCCN Corporate network

- Incident coordination within Portugal

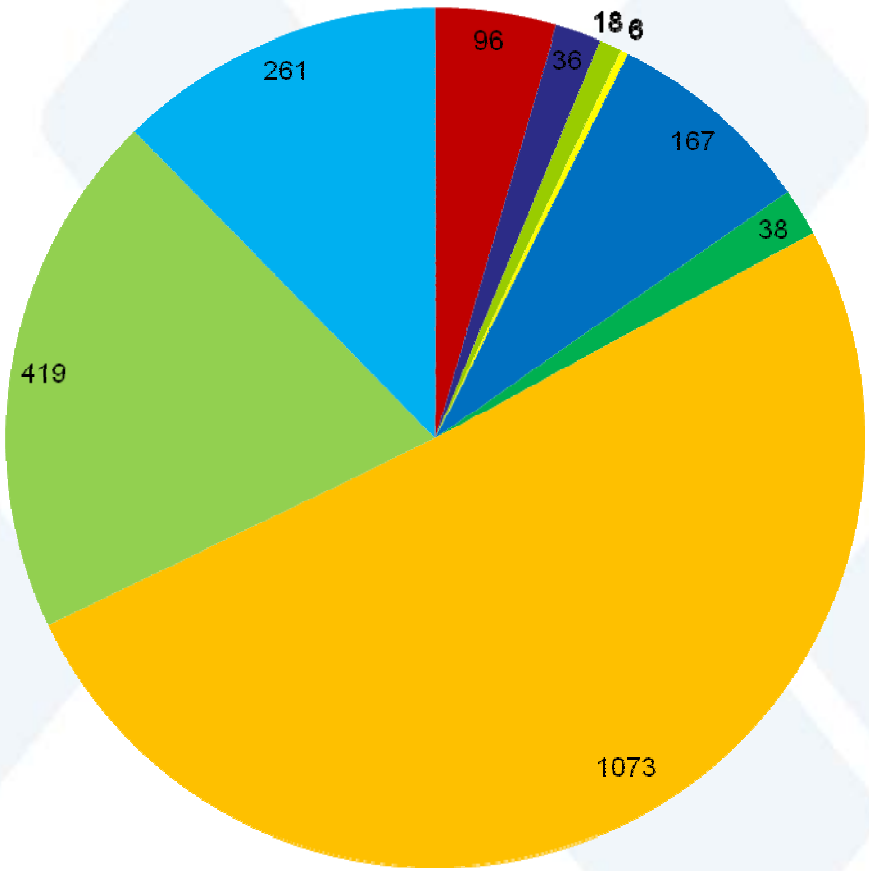
Service portfolio

- Incident handling
- Incident coordination
- Alert and best practice dissemination
- Training
  - Establishment of new CSIRTs
  - Prosecutors and law enforcement
- Vulnerability testing

CERT.PT
Statistics

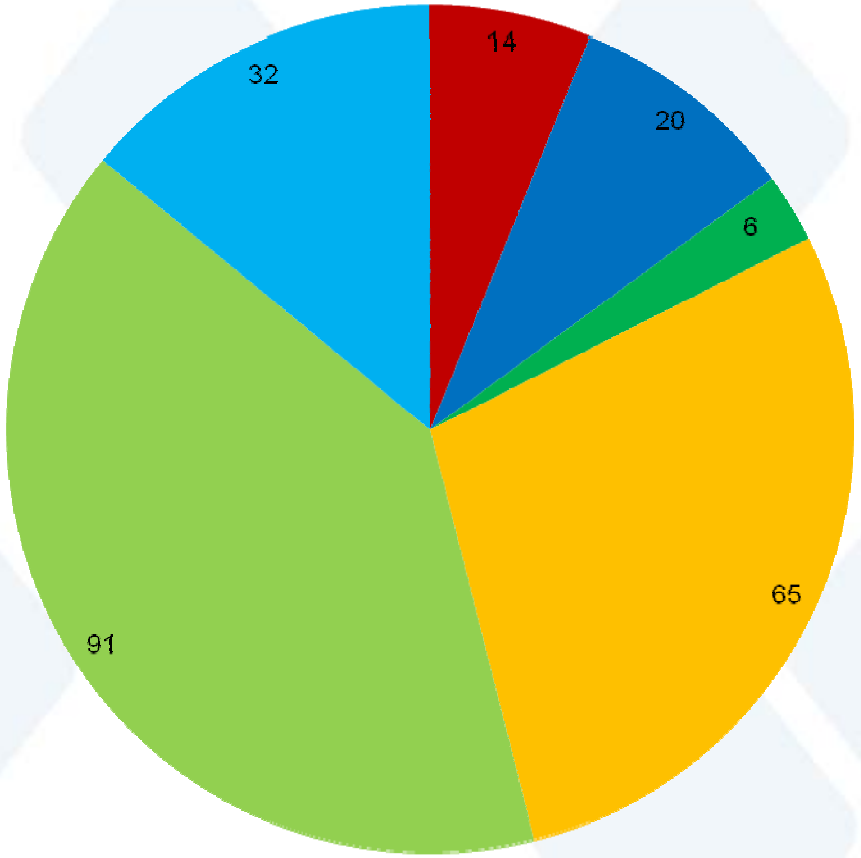


CERT.PT
Statistics 2008



- Port scanning
- Malicious code
- Denial of Service
- Root compromise
- Intrusion atempt
- Unauthorized access
- SPAM
- Copyright violation
- Fraud

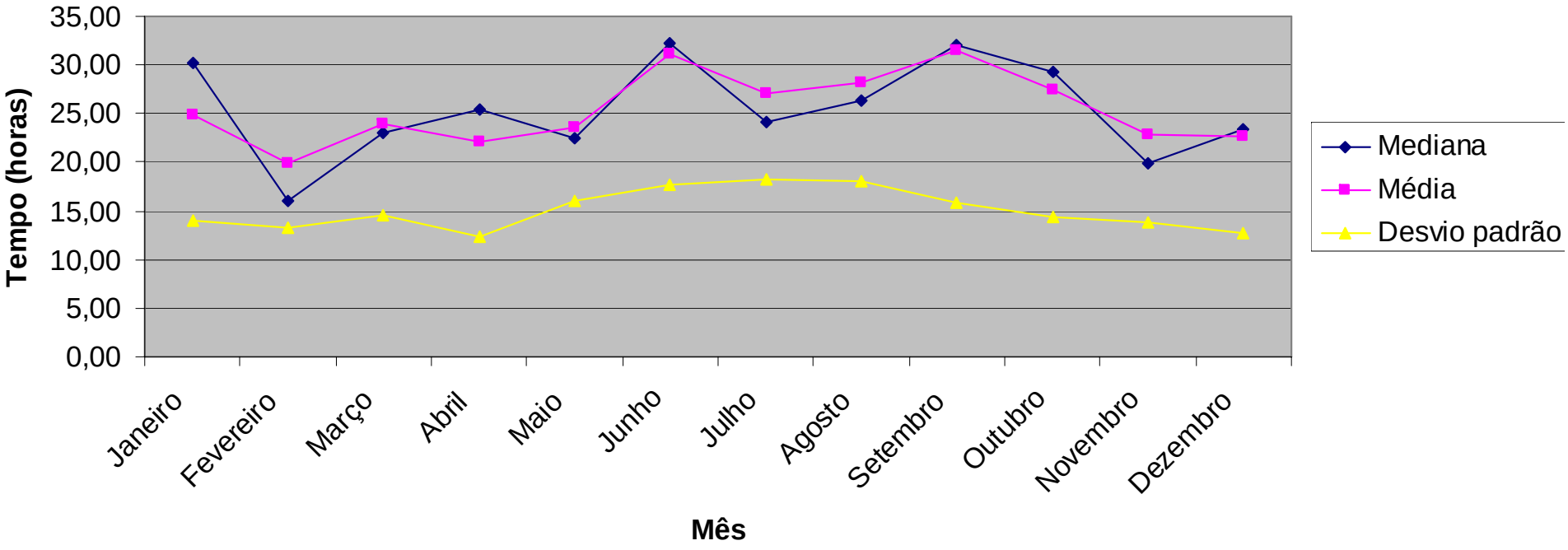
CERT.PT
Statistics 2009



- Port scanning
- Malicious code
- Denial of Service
- Root compromise
- Intrusion atempt
- Unauthorized access
- SPAM
- Copyright violation
- Fraud

CERT.PT
Statistics

First response time

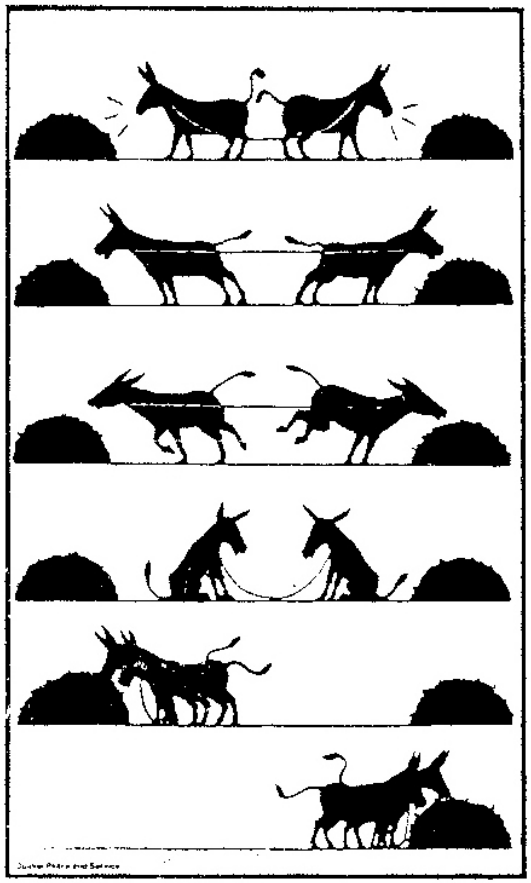


The Team

Resources and funding

- Funding
  - OE-UMIC: Incident handling and awareness activities
  - POSC: Training and other development projects
- Human resources
  - Lino Santos, Gustavo Neves, Luís Morais, Filipa Macieira, on-going recruitment

Agenda



- What does FCCN do?
- CERT.PT
- National cooperation
  - Training
  - National CSIRT network
  - Law enforcement
- International cooperation
- Other security activities
- Future development

National cooperation

Training

Sector	Participants	
Industry	25	BPN, Microsoft, Novabase, Siemens, Unysis, SINFIC, CGD
Telecom	8	Zon, Portugal Telecom, SonaeCom
Public administration	15	LNEC, CM Alpiarça, CEGER, GNS, IGF, CNPCE, MoI
Higher education	22	IPB, U.Aberta, UTL, UP, UTAD, UBI, UAL, UNL, …
Military	18	Army, Navy and Air forces

National cooperation

National CSIRT network

- National directory of security contacts
- Formal agreement:
  - Mandatory incident handling capability
  - Points of contact
  - Common Taxonomy and policies
  - Statistical gathering
- Target entities
  - ISPs
  - Banking
  - Universities
- Technical Forum

National cooperation

Law enforcement

- Formal agreement with criminal investigation body
- Informal agreements with other security agencies
- Formal agreement with armed forces

- Specific training to security agencies and judicial authorities

Agenda

- What does FCCN?
- CERT.PT
- National cooperation
- International cooperation
  - TF-CSIRT
  - ENISA
  - Microsoft
- Other security activities
- Future development

Internacional cooperation

TF-CSIRT

- Attendance since 2002
- Accredited team since 2004
- Member of RTIR WG
- Co-organized the Lisboa meeting in 2006
- TRANSITS training course in Carcavelos

Internacional cooperation

ENISA

- National Liaison Officer
- Head of FCCN is member of the board

Internacional cooperation

Microsoft SCP

- Portuguese version of microsoft bulletins
- Exchange of statistics
- Technical support

Agenda

- What does FCCN?
- CERT.PT
- National cooperation
- International cooperation
- Other security activities
  - Safer Internet Project
  - Critical infrastructures Protection Program
- Future development

Other security activities

Safer internet project

- Linha Alerta hotline operation
- Content production
- Awareness activities

UMIC

FCCN Fundação para a Computação Científica Nacional

Other security activities

- Critical Infrastructure Protection Program
  - Within the Portuguese emergency preparedness council (CNPCE)
  - GIS of CI
  - Establishing the cyberspace committee
  - Starting a project on risk analysis on CI
  - CIWIN support officer

Agenda

- What does FCCN do?
- CER.PT
- National cooperation
- International cooperation
- Other security activities
- Future Development

Other security activities

Netflow analysis

- Real time traffic monitoring
- QoS analysis and BW management
- Abnormal traffic detection
- Malaware detection and analysis
- Security policies violation
- Tool identified: Nfsen

Other security activities

IDS network

- Major pilar for proactive activities
  - Ongoing malicious activity
- Centralized managment
  - Signature managment
  - Database
  - Pattern detection
  - Statistical information
- Trial with 4 Universities

Future Development

National CSIRT network

- Build a CSIRT and security contact directory
- Agree on
  - Taxonomy
  - Toolset
  - Code of practice
  - Accreditation procedure

CERT.PT
Serviço de Resposta a Incidentes de Segurança Informática

Thanks!

UMIC
Agência para a Sociedade do Conhecimento

FCCN
Fundação para a Computação Científica Nacional