

IRIS-CERT & Spanish National CSIRT

IRIS-CERT / INTECO

Meeting for CSIRT with National
Responsibility .CERT/CC .July 2006



Red IRIS

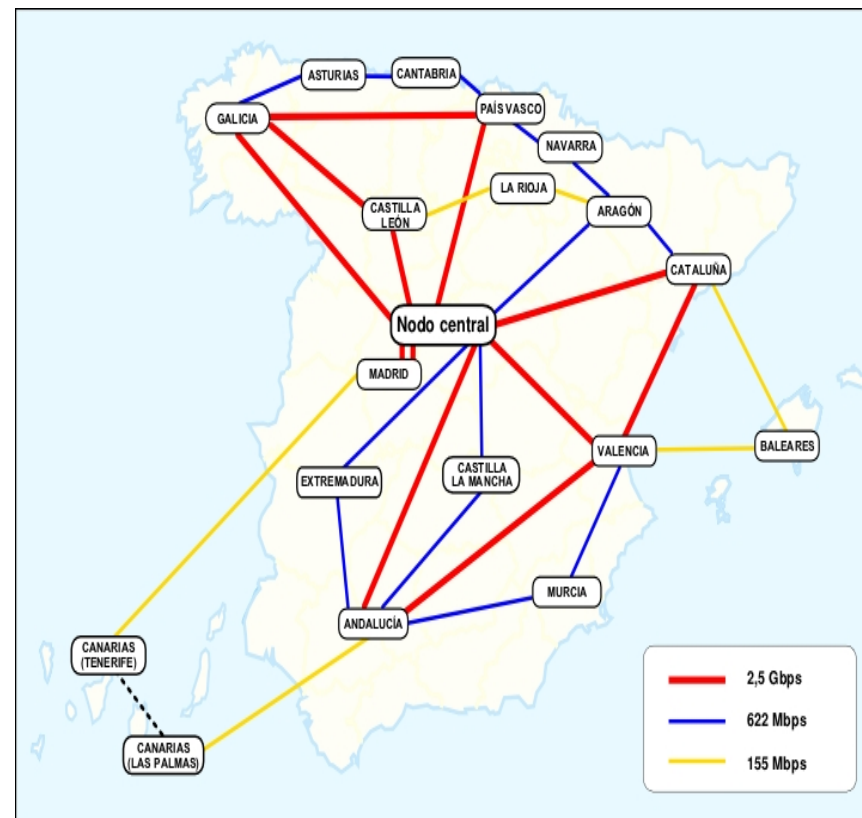


Introduction of RedIRIS/IRIS-CERT

Coordination and Network monitoring projects

IRIS-CERT: Security team for Spanish Academic and Research Network.

- ❑ About 250 directly connected Universities and Research centers.
- ❑ Coordination of incidents, with local staff in each University.
- ❑ Don't deal directly (at first steps) with the end user
- ❑ We don't support "in site" incident analysis, but provided limited reversing engineering of binaries and forensic analysis.



Formed in 1995,

FIRST member in 1997.

Incident and Response Team for:

❑ RedIRIS Network AS766

❑ Host under the “.es” TLD

➤ **In 1997 RedIRIS were also the register of “.es” domain**

➤ **Also coordination of NNTP services for “.es” hierarchy.**

❑ Until 2001 no other team Spanish team joined FIRST

In 2004 RedIRIS became part of Red.es (Spanish government funded company for Information Society)

❑ Started to help to form a government CSIRT in Spain

We received about 20 to 30 incidents every week about hosts not in our direct constituency:

- ❑ Compromised sites used to host Malware phishing pages
- ❑ Binaries stored in some free services in Spain.

The number is increasing since last year as many reported detected that we could contact with the right ISP

This has lead to us to try to coordinate abuse handling with the Spanish ISP.

Most used system for hosting malicious files in Spain

contacts in whois databases outdated.

Contacting with them was impossible:

- Wrong addresses***
- Corporate mail server don't allow some content encoding***
 - ***PGP signed mails were not received***
- Spam and antivirus system seems to drop all the mails to the abuse help desks.***

We succeeded to contact with the abuse team manager and sent him directly huge list of URL.

normal abuse reporting still and issue

Organization of abuse working group in Spain.

Most ISP treat us a neutral actor:

- We are government founded, but not work directly for the government .
- We are an ISP, but not a direct competitor

So it's more easy to work together with us:

Currently:

- Direct contact with the most important ISPs
- Directory of AUP of each ISP
- Working to build a white list for MX server and automatic reporting of network incidents.

European Coordination of Abuse Team , <http://www.e-coat.org>

- ❑ Forum for ISP in Europe
- ❑ Idea originated from some European ISP
- ❑ Focuses in the great abuse volume at ISP level
(SPAM, worm, copyright ...)

Goals:

- ❑ Coordination of Abuse teams in Europe
- ❑ Produce tools and procedures to allow better abuse management
 - Private irc server
 - Different mailing list for join projects

FIRST SIG group in Abuse to be created soon.

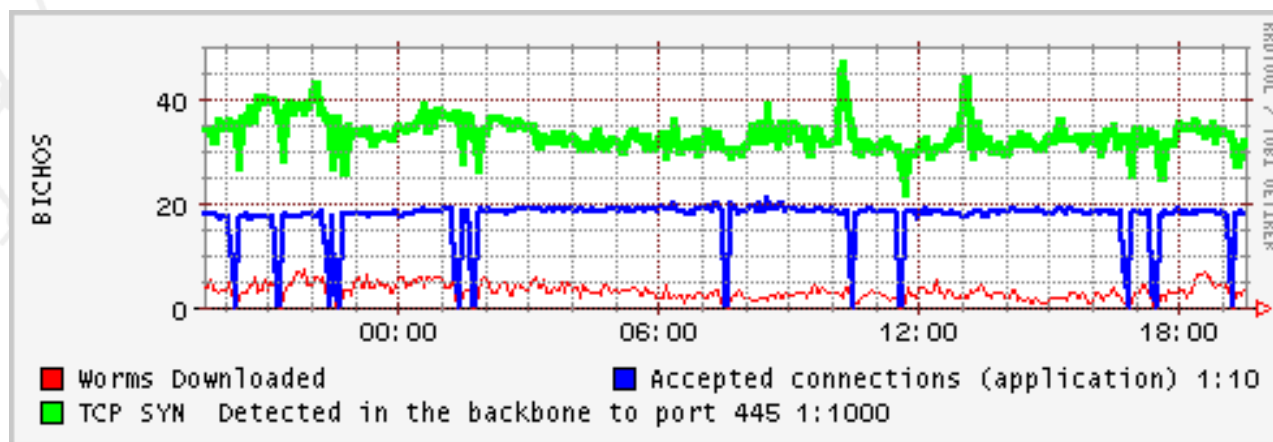
As an academic ISP we managed to block some malicious port in our backbone:

- Limit the impact of worms
- Avoid problem with small organization that have poor security

Capturing the worms:

- Instead of blocking the traffic redirect traffic to a central collector system
- Spoof the destination addresses and respond as the real machine
- Use malware collector (mwcollect, nepenthes) to recollect all the files

- ❑ Provide real (not vendor related) statistics of the worms attacking our network)
 - ❑ Combined with darknet space (for not monitored ports) allow to determine new treats.
 - ❑ Generate a updated clamav antivirus pattern with all the malware detected.
- **Problem: amount of traffic detected:**



Organized in collaboration with UNAM-CERT , Mexico

- We provide the image of the compromised system.
- Participants must send a technical and management report about a computer intrusion

Goals:

- Improve security awareness in our countries
- To promote the learning of Computer forensic using a “Practical case approach”

Help of of other CSIRT:

- Law enforcement agencies in Spain and Mexico
- ArCERT
- CAIS/RPN
- Security experts
- And companies Microsoft, Guidance , etc.

This year not use the typical honeypot / Opensource system compromised by a normal hacker:

- Image of a compromised windows machine***
- Compromised due to social engineering and WMF exploit***
- Steal of confidential information from a database server.***

The idea is to present a more realistic scenario

Results will be published soon.

Since 2004, RedIRIS it's in the same company as the “CATA” (Spanish Early warning system for email worms)

Soon we started to collaborate with them:

- Electronic Fraud working group
- Anti-spam working group

And this year the decision to form a national CSIRT was made:

.....