

GARR-CERT

Roberto Cecchini

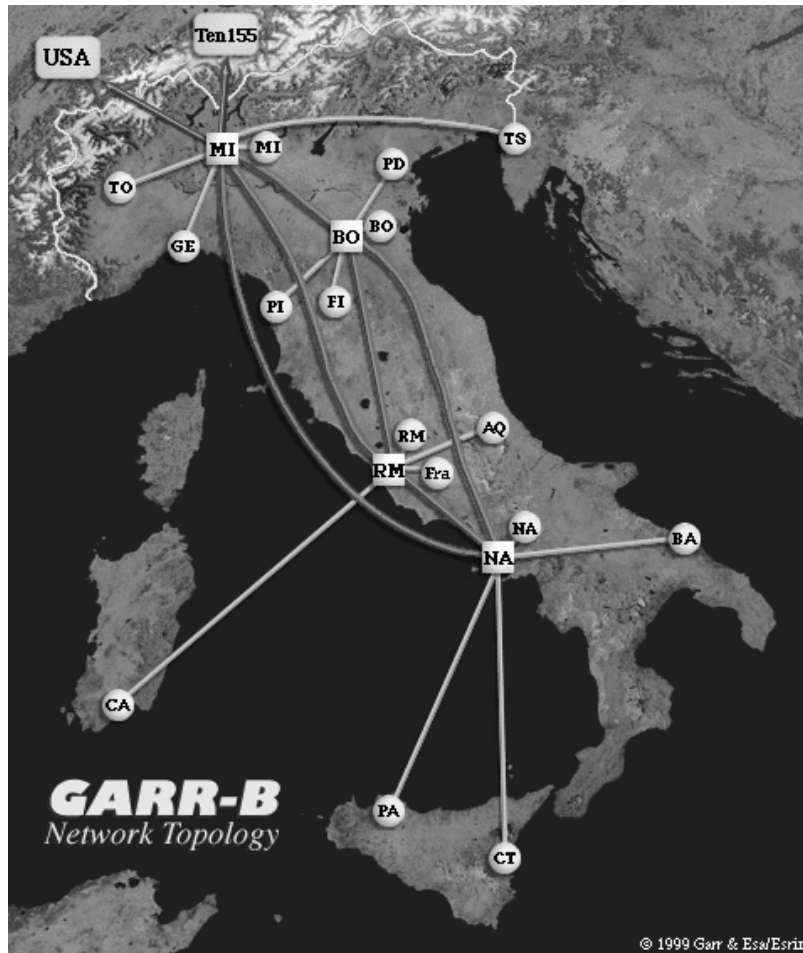
TF-CSIRT Meeting
Barcelona, 18-19 January 2001

GARR-CERT

- The CSIRT of the GARR Network
 - active since June 1999;
 - a GARR service temporarily managed by the *Istituto Nazionale di Fisica Nucleare* (INFN).
- Constituency
 - all the Italian Academic and public Research Institutions connected to the GARR Network.
- Formal description (RFC2350) in **<http://www.cert.garr.it/GARR-CERT-descr-rfc.html>**
- TI “Level 2” team.



The GARR Network



- International Links (155 and 622 Mbps):
 - Milan-Frankfurt (Ten-155): 155 Mbps;
 - Milan-Geneva (Ten-155): 155 Mbps;
 - Milan-New York: 622 Mbps.
- Backbone (155 Mbps):
 - fully meshed between the 4 transport nodes:
 - Milan, Bologna, Rome and Naples.
- Other links (2÷155 Mbps):
 - from local access points (≈ 300) to the transport nodes.
- Peering with private ISPs:
 - Milan (MIX);
 - Rome (RIX).
- 10915 C Classes.

Mission Statement

- To assist constituency in:
 - implementing proactive measures to reduce the risk of computer security incidents;
 - responding to such incidents when they occur.
- To diffuse information on common vulnerabilities, trends, etc..
- To raise awareness of security problems.

Proactive Activities

- Organization of technical meetings;
- scans (on demand):
 - port and vulnerability (**nmap**, **nessus**, **SARA**, etc.);
- checks (weekly):
 - incidents temporarily closed (filtered nodes);
 - ex open mail relay;
- ORBS database (monthly).

Human Resources

- Members
 - operative kernel: 4 (2 full time, 1 for alerts);
 - “Liaison officers” and experts: 4.
- Site security contacts (≈ 250)
 - Access Point Managers (APMs);
 - main interlocutors: they receive all the mails sent to the site;
 - enormous differences between them in competence.
- Hours of activity:
 - Mon-Fri, 8:00-17:00

External Interface

- Web server (<http://www.cert.garr.it/>)
 - documents;
 - alerts;
 - incident reporting form;
 - laws.
- FTP Server (on demand)
 - only for uploads of incident-related data (logs, programs, etc.);
 - files are immediately moved to “internal” machines.
- Mailing lists:
 - **cert@garr.it** (**abuse@garr.it**)
 - GARR-CERT members are the subscribers;
 - **apm@garr.it**
 - the site security contacts are the subscribers;
 - **sicurezza@garr.it**
 - security alerts and communications of general interest;
 - open to everyone (not only constituency).
- All mails sent are (PGP-)signed with the personal key of the sender;
 - the team key is used to sign pages on the web server and for incoming encrypted mail.

Internal Interface

- Access restricted to the machines of the operative kernel.
- Incidents Database (**MySQL**)
 - dates, nodes, status, priority, e-mails, logs;
 - statistical data:
 - type (primary & secondary), hardware, OS, exploit (**CVE** when available), damages, tools.
- Internal web server (**Apache + mod_ssl + php**)
 - incident management;
 - list of contacts, templates, etc..
- Repository of incident-related data:
 - online until analysis is complete and incident closed;
 - on CD-ROM afterwards.
- Home-made procedures (60% php, 39% perl, 1% C).

Incident Opening

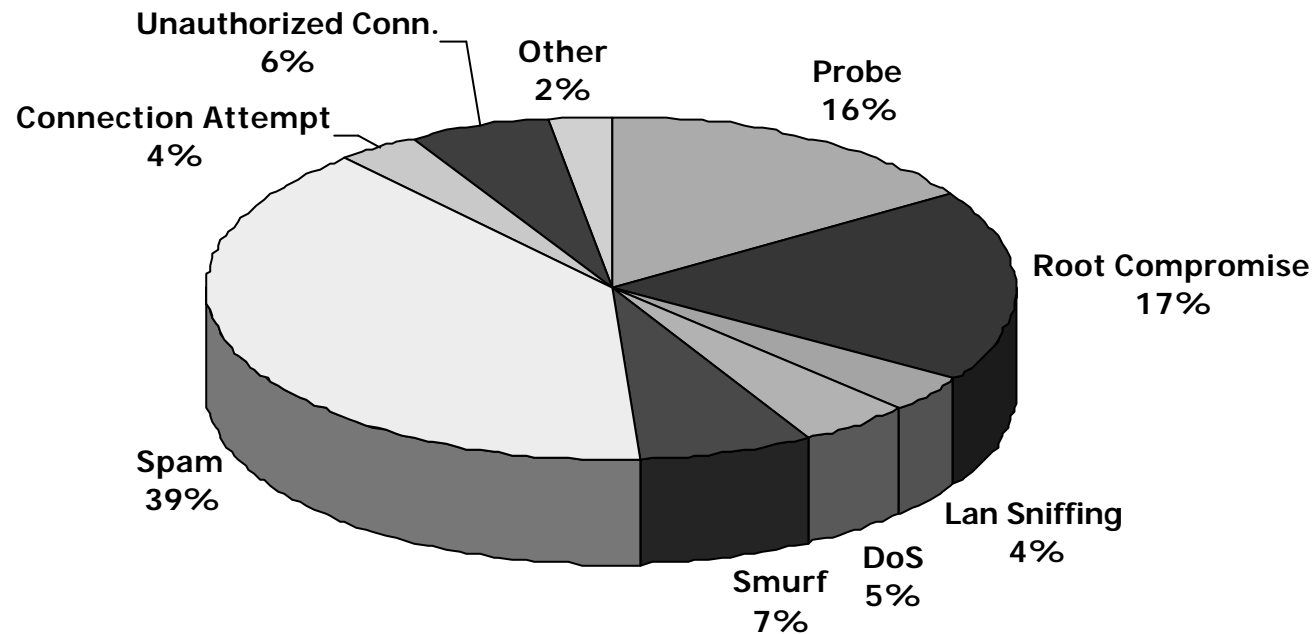
- An incident
 - involves a GARR node;
 - implies a violation of some “rule” (laws, AUPs, netiquette);
- When:
 - each report received if obeys the rules above and not blatantly false (e.g. a GARR node found in a faked spam mail header): the report is kept in every case;
 - log analysis (e.g. passwords in a sniffer log);
 - proactive checks (old incidents, ORBS).
- Incidents are stored in the database, classified and prioritized (RFC2350):
 - one unique code (date + progressive number) for each couple victim–attacker (node or network).
- E-mails are sent to all the involved parties
 - except automatic mail from *SpamCop* and similar.

Incidents Closure

- Incidents originating from GARR nodes:
 - must be solved (at least temporarily) in predefined maximum times (according as severity);
 - if it doesn't happen, GARR-CERT asks the local APM to filter the node on the access router;
 - if the APM doesn't intervene, GARR-CERT asks the NOC to filter the node on the border router.
 - During year 2000:
 - requests to APMs: ≈ 70 ;
 - requests to NOC: ≈ 30 .
- Incidents originating from non-GARR nodes which don't answer our mails are usually closed after a predefined time.
- Mails with some details about the actions taken are sent to all involved parties.

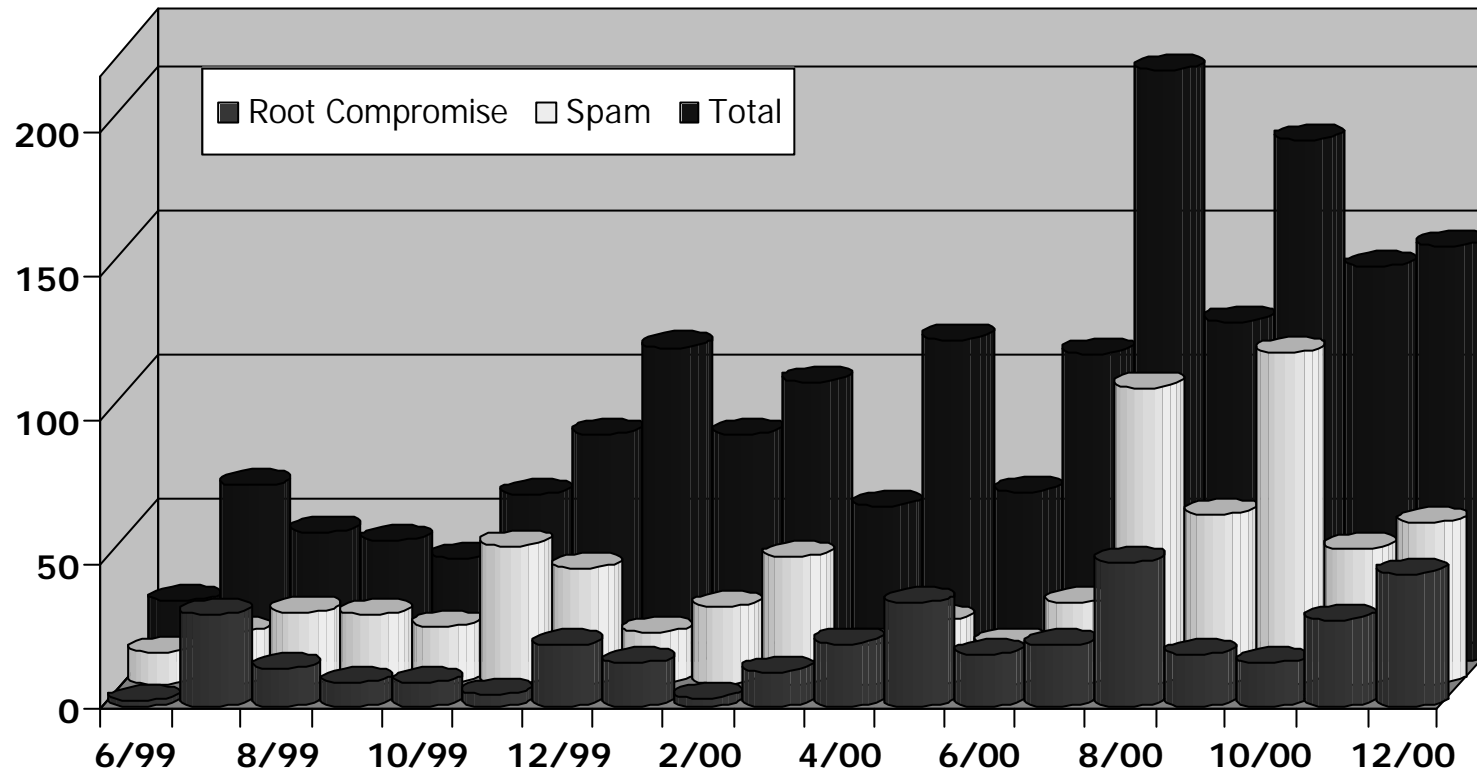
Incidents (by type)

From 1/1/2000 to 31/12/2000



Total: 1381
(e-mails handled: 10130)

Incidents (by month)



Root Compromise includes Lan Sniffing and DoS