

GARR

The Italian Academic & Research Network



www.garr.it

GARR-CERT

Update

Simona Venuti

TF-CSIRT, Rome, 30.01.2012



OLD GARR-CERT Presentation

... I do not know who was the first to present GARR-CERT

... And I do not have that presentation, nor any presentation at all

Since my duty is to make an *«update»*

... I added a general (but detailed) description of GARR-CERT (next 14 slides), but I'm not going to explain them in this speech

Read it if interested!

(Or go to page 17)

GARR Presentation (before update)

GARR (whose acronym means "Gestione Ampliamento Rete Ricerca" - "Research Network Widening Management") is composed by all subjects representing the Italian **Academic and Scientific Research Community**. GARR activities are ruled by **Consortium GARR** and operationally by **Consortium GARR Management**.

The main institutional tasks of GARR towards its own Community is:

to implement and to manage the networking interconnection service and the interconnection service to the other **european** and **worldwide** Research networks and to Internet in general;

to supply **operational and application** networking services;

to support the coordination and collaboration among the Research activities (national and international level) via telematic services, including the **research and development in telematics** itself;

to support the dissemination, the information update and the exchange of knowledge in telematics, also organising **Workshops and Courses**.

Mission Statement:

- to assist the users of the **GARR Network** in implementing proactive measures to reduce the risk of computer security incidents;
- to assist the users of the GARR network in responding to such incidents when they occur.

GARR-CERT Presentation

- **Constituency:** The GARR-CERT constituency is the community of the users of the GARR Network, the Italian Academic and Research Network.
- **Sponsorship:** GARR-CERT is an operative service of the GARR Network.
- **Authority:** GARR-CERT operates under the auspices of the GARR members and the supervision of the GARR management.
- In case of missing support from the local APM, it has authority to obtain from GARR NOC the filtering of the involved node(s) on the GARR network border routers.

Foudation:

- The GARR-CERT was formally founded in 1st of March 1999
- GARR-CERT is a Level 2 Team of Trusted Introducer since 1st if January 2001

GARR-CERT Policies 1/2

Types of Incidents and Level of Support

www.garr.it

GARR-CERT is authorized to address all types of computer security incidents that occur at nodes connected to the GARR network.

The level of support given by GARR-CERT will vary according to the severity of the incident and the GARR-CERT's resources at the time. Every effort will be done to give some response within one working day. No direct support will be given to end-users, as they are expected to contact their system administrators.

GARR-CERT expects that the APM of the sites involved in security incidents will cooperate in the resolution of the problem.

The incident handling procedure, which, in extreme cases, will lead to filtering the compromised node(s) on the GARR network border routers -- as approved by the OTS GARR -- can be found at (in Italian):
<http://www.cert.garr.it/incidenti.php3>

GARR-CERT is committed to keeping its constituency informed of potential vulnerabilities, possibly before they are actively exploited.

7

GARR-CERT Policies 2/2

Co-operation, Interaction and Disclosure of Information:

GARR-CERT, unless explicitly authorized, will not divulge the identity of nodes victims of computer security incidents.

Communication and Authentication:

Telephone and unencrypted e-mail are considered sufficient for the transmission of low-sensitivity data. If it is necessary to send high sensitivity data by e-mail, PGP will be used.

Network file transfers will be considered similar to e-mail for these purposes

GARR-CERT WorkFlow 1/3

1- When GARR-CERT receives a report about an incident, it verifies that at least one of involved entities belongs to its own constituency. If this is not the case, then GARR-CERT tries to forward the message to the appropriate external CSIRT.

2- GARR-CERT assigns an unique id number to the incident, and sends a report to the local Access Point Manager (APM), the manager of the router connecting the involved site to the GARR Network. The APM is also asked to forward the information to the local people involved. In this communication GARR-CERT specifies the maximum time allowed to solve the problem.

GARR-CERT then replies to the entity that signalled the incident, sending a first report which includes the assigned id.

In case of particularly severe issues, e.g. those with penal relevance, the communication sent to the local APM will also includes a formal invitation to filter out the involved node without further confirmation request, in case the problem cannot be solved within the time limit specified. A copy of this message will be also be sent to GARR-NOC (the Network Operations Centre). In this case we proceed to step 5.

GARR-CERT WorkFlow 2/3

3- If the incident is solved within the requested time frame, we proceed to step 9.

4- If the incident is not solved within the requested time frame, GARR-CERT asks the local APM to filter the involved network/computer/service on his/her local router. In this notification GARR-CERT indicates the maximum time allowed to the APM for the action.

5- If the APM acts within the time limit, we continue with step 8

6- If the local APM does not act within the requested time, GARR-CERT sends to GARR-NOC the request to filter the involved network/computer/service.

If the deadline for the filtering action was outside GARR-CERT working hours, GARR-NOC will proceed without the GARR-CERT formal request.

7- GARR-NOC install the filters as requested and notifies GARR-CERT

GARR-CERT WorkFlow 3/3

8- GARR-CERT verifies that the network/computer/service causing the problem is filtered and sends a report of "neutralized problem" to all the involved parties.

9- When the local people communicate that the problem is solved, GARR-CERT, after a successful verification, sends a request to remove the applied filters to the local APM or GARR-NOC. Then GARR-CERT sends a communication of "problem solved" to all the involved parties and it closes the incident.

The maximum allowed time for solving the problems are as follows:

- * open mail relay: 3 days;
- * Nodes that are source of hostile actions (port scan, attacks, etc.): 1 day;
- * Nodes used for DoS attacks: 5 hours.
- * Incidents with penal relevance: 4 hours.

GARR-CERT Services 1/3

Incident Response:

GARR-CERT will help system administrators of nodes connected to the GARR network in handling computer security incidents. In particular:

- * investigating the nature and extent of the incident;
- * determining the initial cause (e.g. Vulnerability exploited);
- * keeping contacts with other sites involved;
- * reporting to other CSIRTs;
- * helping in removing the vulnerability.

GARR-CERT Services 2/3

Proactive Activities:

GARR-CERT coordinates and maintains the following services to the extent possible depending on its resources:

- * mailing lists.
- * auditing services;
- * dissemination of information about vulnerabilities and recommended security measures;
- * testing and developing security tools.

Certification Authority:

GARR-CERT coordinates and maintains the GARR Certification Authority and SCS Registration Authority to provide:

- * GARR-CA Personal Certificates;
- * GARR-CA Server Certificates;
- * TERENA Server and e-Science Server Certificates (TCS)
- * TERENA Personal and e-Science Personal Certificates

GARR-CERT People

Leader:

Roberto Cecchini

Operational (4FTE):

Barbara Monticini (CA and AAA)

Andrea Pinzani (Incident Response)

Maria Sole Scollo (Incident Response)

Simona Venuti (NetFlow & Research)

How to reach GARR-CERT

Web Server:

<http://www.cert.garr.it>

- Names of members and list of public pgp keys
- Telephone numbers and snail mail address
- Historical Security Alerts
- Web form to report an incident

Mailing lists:

cert@garr.it

to report incidents

sicurezza@garr.it

to inform about security alert

Information/Update

- Established on the 1st of March 1999
- TI Accreditation: 1 January 2001
- Constituency:
Italian Academic and Research Network
- AS: 137

Staff

- The BoSS
 - Roberto Cecchini



- 2 FTE
 - Maria Sole Scollo – Incident Response
 - Andrea Pinzani – Incident Response



- 2 FTE
 - Barbara Monticini – CA, AAI
 - Simona Venuti – NetFlow & Research



GARR Network Evolution

From **GARR-G** (GARR GigaBit):

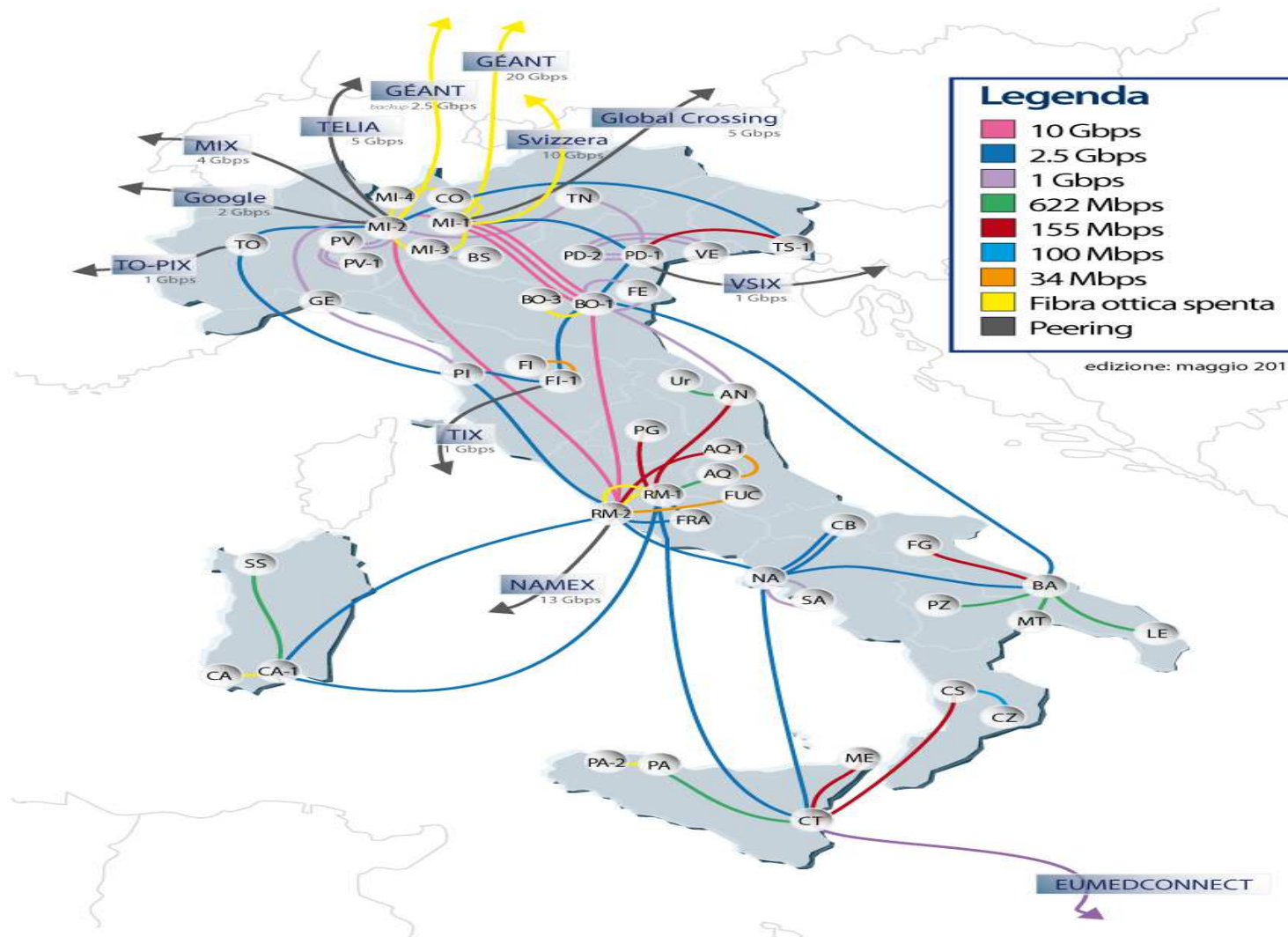
- GigaBit Ethernet for the whole backbone (up to 10Gb)
- GigaBit Ethernet for almost every leaf

to **GARR-X** (2012)

- We are buying our own dark fiber
- We are going to completely own our routers
- We are not sharing the net anymore with private ISPs

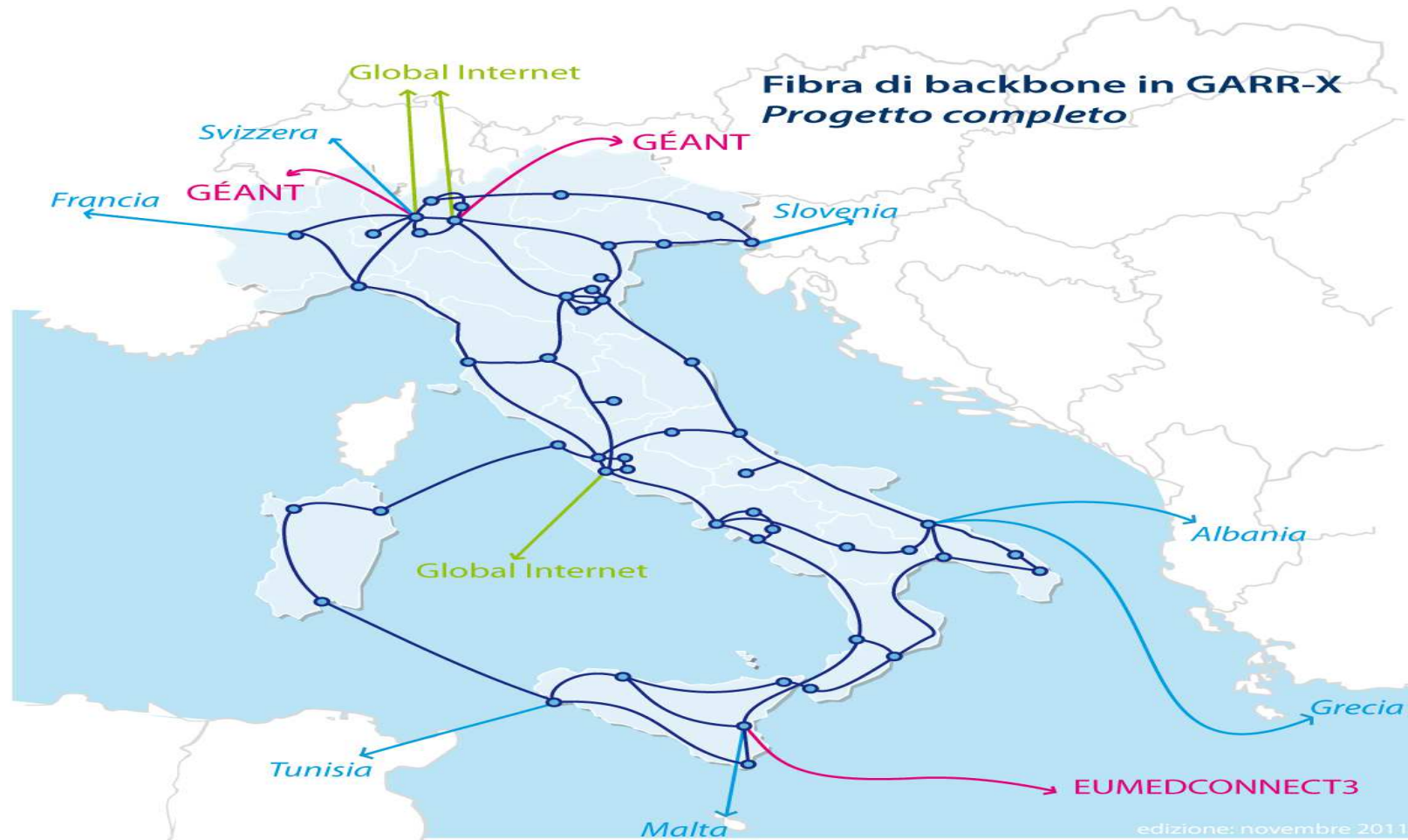
GARR-G

Topologia di backbone di GARR-G



GARR-X

www.garr.it



- collegamenti di backbone nazionale previsti dal progetto GARR-X
- collegamenti transfrontalieri (Cross Border Fibers)
- collegamenti alle reti GÉANT e EUMEDCONNECT3
- punti di peering con il Global Internet

Functions



Reaction

■ Alerts and Warnings

GARR-CERT Security Alerts (per data)

In questa pagina vengono raccolti i Security Alerts ritenuti più interessanti per gli utenti GARR.

[Indice per soggetto](#)

- 24/01/12 [Alert GCSA-12006 - Vulnerabilita' in Google Chrome](#)
- 20/01/12 [Alert GCSA-12005 - Oracle Critical Patch Update Advisory \(January 2012\)](#)
- 12/01/12 [Alert GCSA-12004 - Vulnerabilita' in Google Chrome](#)
- 11/01/12 [Alert GCSA-12003 - Vulnerabilita' in OpenSSL](#)
- 11/01/12 [Alert GCSA-12002 - APSP12-01 Vulnerabilita' in Adobe Reader e Acrobat](#)
- 11/01/12 [Alert GCSA-12001 - Microsoft Security Bulletin January 2012](#)
- 30/12/11 [Alert GCSA-11087 - Aggiornamento integrativo Microsoft Security Bulletin December 2011](#)
- 29/12/11 [IMPORTANT: Remote root vulnerability in telnet daemons \(CVE-2011-4862\)](#)
- 21/12/11 [Alert GCSA-11086 - Vulnerabilita' nei prodotti Mozilla](#)
- 19/12/11 [Alert GCSA-11085 - APSP11-30 Vulnerabilita' in Adobe Reader/Acrobat](#)
- 14/12/11 [Alert GCSA-11084 - Microsoft Security Bulletin December 2011](#)
- 18/11/11 [Alert GCSA-11083 - Vulnerabilita' in ISC BIND 9.x](#)
- 11/11/11 [Alert GCSA-11082 - Vulnerabilita' in Google Chrome](#)
- 11/11/11 [Alert GCSA-11081 - Vulnerabilita' in Adobe Flash Player](#)
- 09/11/11 [Alert GCSA-11080 - Apple Mac OS X aggiornamento per Java](#)
- 09/11/11 [Alert GCSA-11078 - Microsoft Security Bulletin November 2011](#)
- 09/11/11 [Alert GCSA-11079 - Vulnerabilita' in Mozilla Firefox e Thunderbird](#)
- 04/11/11 [Alert GCSA-11077 - Vulnerabilita' 0-day in Microsoft Windows](#)
- 21/10/11 [Alert GCSA-11076 - Vulnerabilita' in MIT Kerberos](#)
- 19/10/11 [Alert GCSA-11074 - Oracle Critical Patch Update Advisory \(October 2011\)](#)
- 19/10/11 [Alert GCSA-11075 - Oracle Java SE Critical Patch Update Advisory \(October 2011\)](#)
- 17/10/11 [Alert GCSA-11073 - Vulnerabilita' in Apple Safari](#)
- 17/10/11 [Alert GCSA-11072 - Apple OS X Lion v10.7.2 and Security Update 2011-006](#)
- 14/10/11 [Alert GCSA-11071 Microsoft Security Bulletin October 2011](#)
- 05/10/11 [Alert GCSA-11070 Vulnerabilita' in Google Chrome](#)
- 30/09/11 [Alert GCSA-11069 - Vulnerabilita' multiple nei prodotti Mozilla](#)
- 23/09/11 [Alert GCSA-11068 - Vulnerabilita' in Google Chrome](#)
- 23/09/11 [Alert GCSA-11067 - APSP11-26 Vulnerabilita' in Adobe Flash Player](#)
- 19/09/11 [Alert GCSA-11066 - Vulnerabilita' multiple in Adobe Reader / Acrobat](#)
- 14/09/11 [Alert GCSA-11065 - Vulnerabilita' in Microsoft Office \(MS11-072 MS11-073 MS11-074\)](#)

Reaction

- Incident Response

+ OpenPGP Firma autentica per Andrea Pinzani <Andrea.Pinzani@fi.infn.it>

da GARR-CERT <cert@garr.it>☆
oggetto **GARR-CERT-13A2403 Spam from ██████████**
a apm@████████☆
cc cert@garr.it☆

Incident Number: GARR-CERT-13A2403
#####

Salve,

sono un membro del GARR-CERT (www.cert.garr.it), il Computer Security Incident Response Team della rete GARR (www.garr.it), la rete Accademica e della Ricerca in Italia.

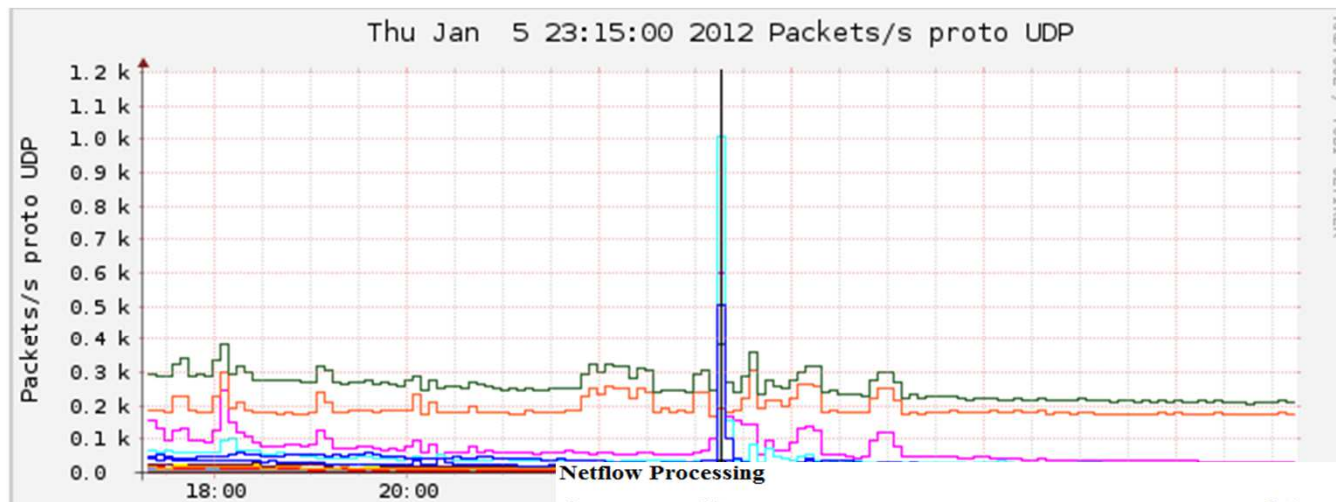
Abbiamo ricevuto alcune segnalazioni, simili a quella inoltrata di seguito, secondo le quali il nodo mfe1 ██████████. (131 ██████████) e' apparentemente origine di email spam.

Vi chiediamo di indagare e di informarci sugli esiti.

Cordiali saluti,
GARR-CERT staff

Reaction

- Incident Investigation



Source: rc1sa rc1tn rcmt rcmi5 rcur rcpal All Sources

Filter: proto udp and ip [redacted]

Options:

- List Flows Stat TopN
- Limit to: 10000 Flows
- Aggregate:
 - proto
 - srcPort srcIP
 - dstPort dstIP
 - start time of flows
- Sort: [dropdown]
- Output: long / IPv6 long

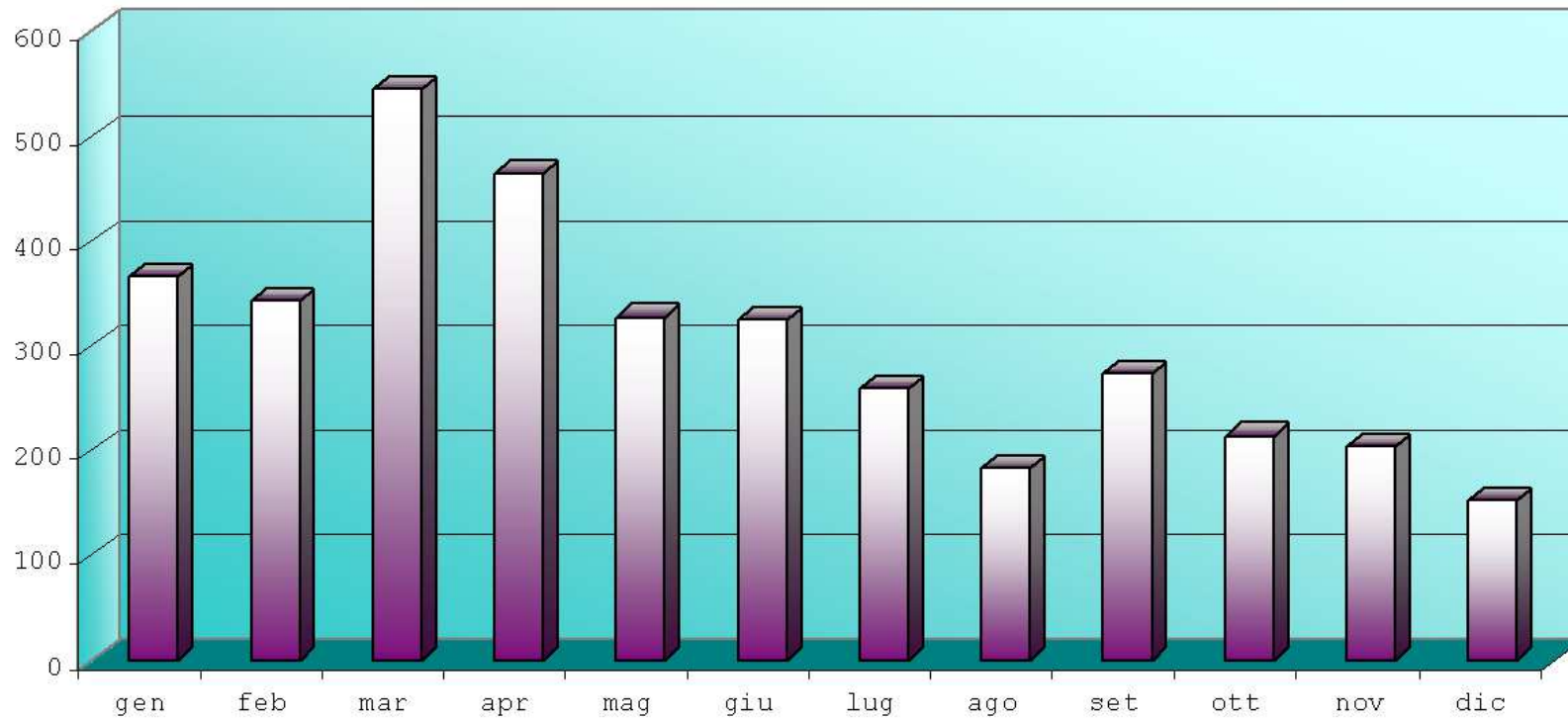
Buttons: Clear Form process

```

** nfdump -M /data/nfsen/profiles-data/live/rc1sa:rc1tn:rcmt:rcmi5:rcur:rcpal:rcan:rcal:rcpv:rtbal:rtmi2:rt1mi1:rtmi3:rtfil
nfdump filter:
proto udp and ip [redacted]
stat() error '/data/nfsen/profiles-data/live/rc1sa/2012/01/05/nfcapd.201201052315': File not found!
stat() error '/data/nfsen/profiles-data/live/rcmi5/2012/01/05/nfcapd.201201052315': File not found!
Date flow start      Duration Proto      Src IP Addr:Port      Dst IP Addr:Port      Flags Tos      Packets      Bytes      Flows
2012-01-05 23:15:42.260  31.716 UDP      [redacted]:59229 -> [redacted]:53      ..... 0      4421      190103      1
2012-01-05 23:15:42.745  31.231 UDP      [redacted]:32983 -> [redacted]:53      ..... 0      4521      194403      1
2012-01-05 23:15:42.777  31.199 UDP      [redacted]:51140 -> [redacted]:53      ..... 0      1958      84194      1
2012-01-05 23:15:42.297  31.675 UDP      [redacted]:43047 -> [redacted]:53      ..... 0      17435     749705      1
2012-01-05 23:15:42.256  31.716 UDP      [redacted]:47406 -> [redacted]:53      ..... 0      4577      196811      1
2012-01-05 23:16:14.010  26.958 UDP      [redacted]:59229 -> [redacted]:53      ..... 0      3752      161336      1
    
```

Statistics 1/2

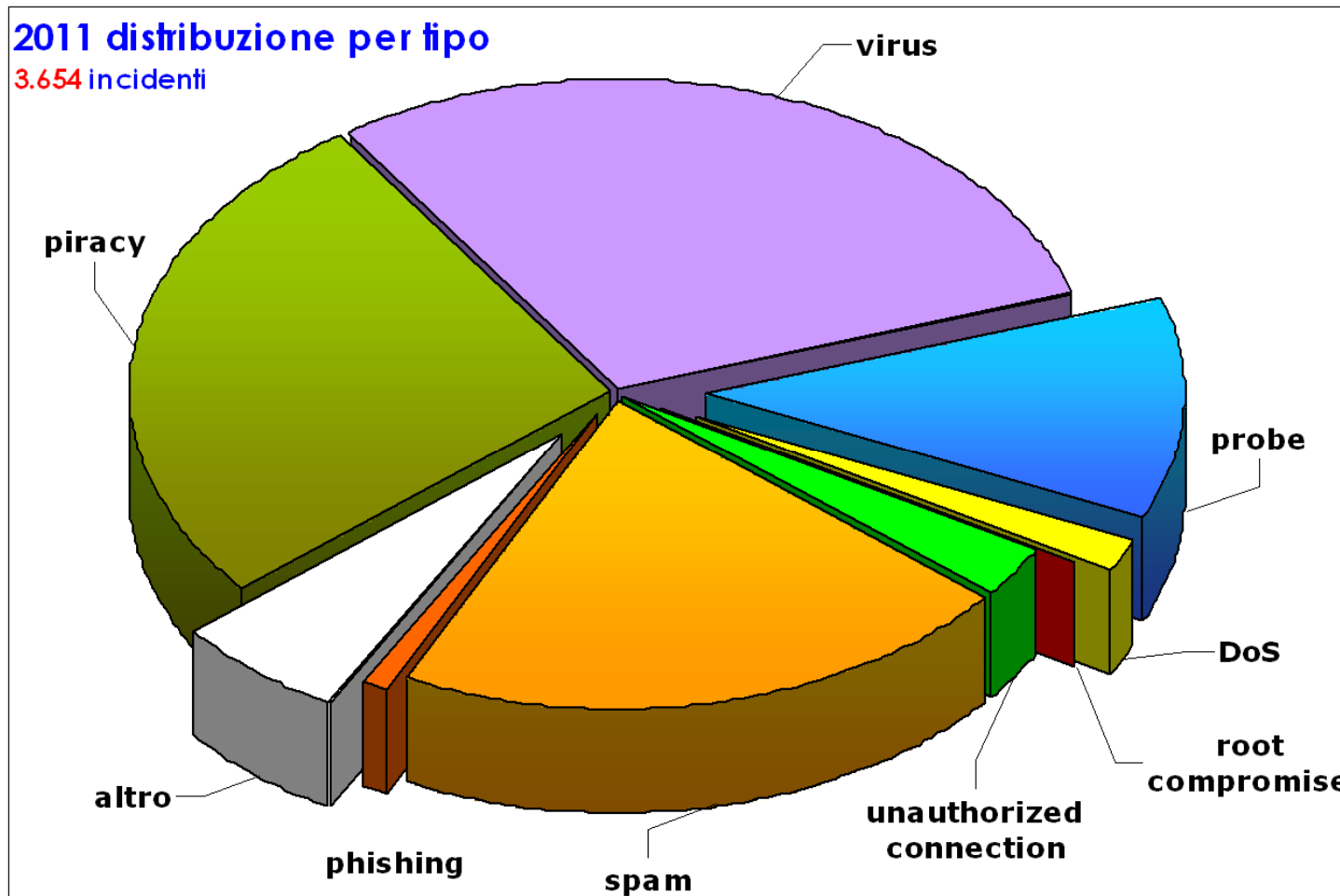
- Number of incidents in 2011



Total 3654 incidents

Statistics 2/2

- Distribution of types of incidents in 2011



Prevention

■ Security FAQ



alert	documenti	statistiche	FAQ
mailing list	membri	PGP	



FAQ

In questa pagina sono pubblicate alcune domande frequenti

- [Ho scoperto che esistono nomi di dominio molto simili al mio: e' un illecito? Come posso procedere?](#)
- [Abbiamo ricevuto una email nella quale veniamo avvisati che nomi a dominio di nostro interesse, sotto meno noti TLD \(tipo .asia\), stanno per essere registrati da altri. Ci viene quindi proposto di procedere noi per primi alla registrazione dietro pagamento. Come suggerite di agire?](#)
- [Ho notato numerosi tentativi illeciti di connessioni ssh sui miei sistemi, quali difese posso attuare?](#)
- [Come posso individuare sistemi infetti dal virus Conficker situati dietro server NAT, senza avere informazioni complete circa le connessioni sospette?](#)

Prevention

- Security Guides



alert	documenti	statistiche	FAQ
mailing list	membri	PGP	



Documenti

- [Informazioni su alcuni tipi di malware](#)
- [Francesco Palmieri, *Advanced Network Security* \(pdf, 4MB\).](#)
- [Luca Fini, *Virus inviati per posta elettronica*.](#)
- [Luca dell'Agnello, *Configurazione sicura di un mail server*.](#)
- [Luca dell'Agnello, *Guida alla configurazione sicura del router*.](#)

Prevention

- SCARR (<http://scarr.garr.it>)

Remote Vulnerability Scanning on Demand

www.garr.it

SCARR - Scansioni Ripetute a Richiesta *Beta!*

Navigator

- Home
- Scansioni
 - Scansione Immediata
 - Pianifica Scansione**
- Reports
 - Report Scansioni
 - iReports
- GarrSSO
 - Gestisci i tuoi permessi di scansione
- Amministra
 - Richiedi scansione a nome di altri
 - Gestisci Profili Nessus
 - Collabora

Home / Dashboard Scansioni / Pianifica Scansione x Reports x Reports / Report Scansioni x Scansioni / Pianifica Scansione x

Target della scansione:

Tipo scansione:

Quando: Ripeti ogni:

Profilo:

Metti qualcuno in cc:

30

Cooperation

- Trusted Introducer

- TERENA TF-CSIRT Task Force

- Geant collaboration
 - GN3 – SA2 – T4 (Security Services)
 - GN3 – JRA2 – T4 (Security Research)

Research

- Research on unknown vulnerabilities with a HoneyPot system
- Research on bad traffic characteristics by monitoring the traffic towards 2 class C darknets
- Research and collaboration with external security groups

How to reach GARR-CERT (again)

Web Server:

<http://www.cert.garr.it>

- Names of members and list of public pgp keys
- Telephone numbers and snail mail address
- Historical Security Alerts
- Web form to report an incident

Mailing lists:

cert@garr.it

to report incidents

sicurezza@garr.it

to inform about security alert

Thank you!

If you have any question
feel free to ask

simona.venuti@garr.it