Il servizio GARR-CERT

VI Incontro del GARR
Roma, 16-18 Novembre 2005

GARR-CERT

- Lo CSIRT della rete GARR:
  - attivo dal Giugno 1999;
  - opera in stretta collaborazione con il Network Operation Center (NOC).
- Risorse umane:
  - nucleo operativo (sede a Firenze): 4 (3 full-time);
  - esperti e “ufficiali di collegamento”: 5;
  - contatti locali (APM): ≈ 350.
- “Trusted Inroducer” Level 2 Team (http://www.ti.terena.nl/)

Interfaccia esterna

- Web server: http://www.cert.garr.it/
- FTP server (a richiesta)
- Mailing list:
  - **cert@garr.it**: segnalazioni incidenti;
    - gli iscritti sono i membri di GARR-CERT.
  - **sicurezza@garr.it**: security alert

Attività preventive

- Partecipazione a incontri tecnici
- Consulenze
- Scansioni alla ricerca di vulnerabilità (su richiesta dell' APA/APM)
- Verifiche periodiche sullo stato dei nodi già coinvolti in incidenti
- **SENTINEL**: Sistema di allarme per attacchi DoS in corso (in collaborazione con Bruno Melideo)

Incidenti: apertura

- Un “incidente”
  - coinvolge almeno un nodo GARR;
  - è causato dalla violazione di una qualche “regola” (leggi, AUP, *netiquette*).
- Quando:
  - ogni segnalazione ricevuta che rispetta la definizione di sopra e non sia palesemente falsa;
  - analisi di log (p.e. password nel log di uno *sniffer*);
  - controlli preventivi.
- E-mail inviati a tutte le parti coinvolte.

Incidenti: chiusura

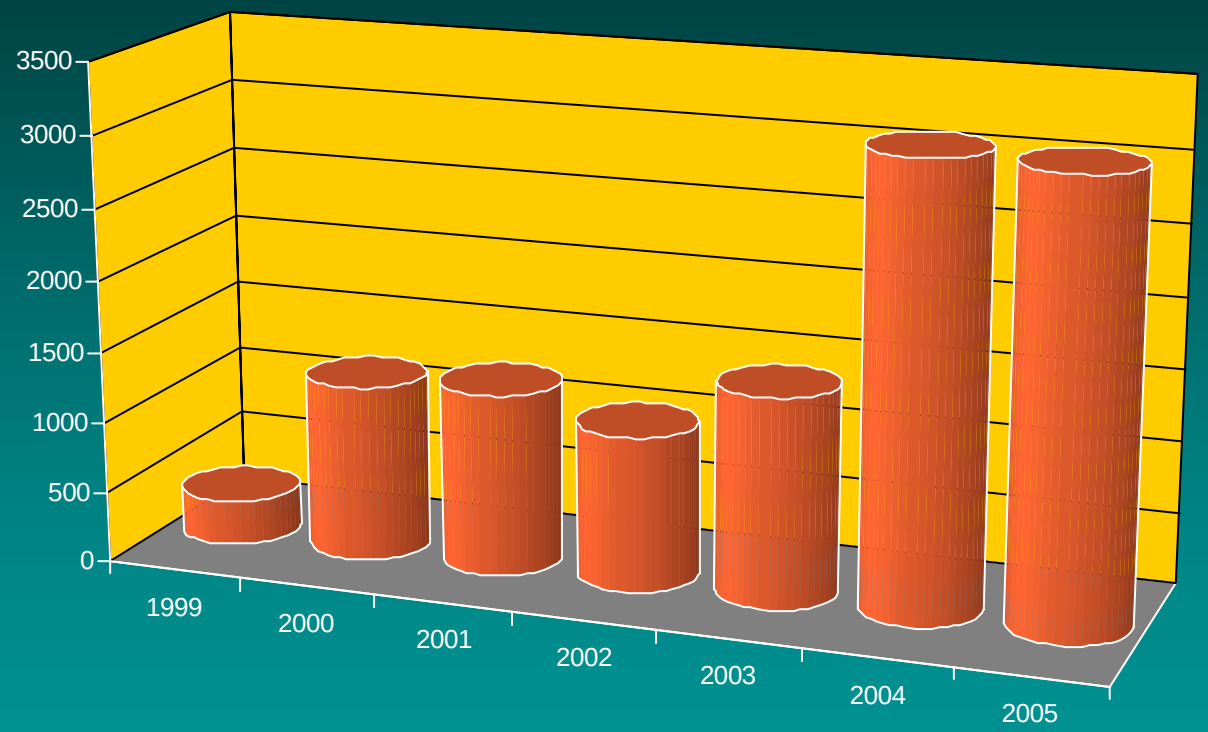
- Gli incidenti che hanno origine da nodi GARR **devono** essere risolti (almeno temporaneamente) in un tempo massimo predefinito.
- In caso contrario GARR-CERT chiede all'APM di filtrare il nodo sul router di accesso.
- Se l'APM non interviene tempestivamente, GARR-CERT chiede l'intervento del NOC.
- E-mail con dettagli sulle azioni intraprese inviati a tutte le parti coinvolte.

La rete GARR

- Estremamente eterogenea
- Struttura globale di AA inesistente
- Grande abbondanza di banda
  - ideale per attacchi DoS
- Molte sedi con personale insufficiente
- Difese perimetrali spesso poco efficaci
- Molti utenti roaming
- Attività di tipo “grid”

Numero totale incidenti

(dal 1999 ad oggi)



	1999	2000	2001	2002	2003	2004	2005
#	312	1229	1281	1086	1461	3132	3100

Evoluzione delle minacce 1/2

- Spam
  - ormai pochi open relay
  - cambiano le tecniche: open proxy, WebDAV, spamming trojan
- Warez
  - in aumento le segnalazioni di distribuzione via p2p di materiali coperti da copyright
- Scansioni
  - principalmente virus

Evoluzione delle minacce 2/2

- Worm & virus
  - ormai scritti da professionisti
  - diffusione
    - servizi (80, 135, 137, 445, 1433, …), mail, p2p, irc, instant messenger, social engineering
  - conseguenze
    - (D)Dos
    - zombie (botnets)
- Phishing

Attività future

- Educazione dell'utenza
- Realizzazione delle norme minime di sicurezza
- Miglioramento del coordinamento con gli altri csirt
- Sistema di "early warning"
- Architettura di AA