Cosa bolle nella pentola di GARR-CERT

Roberto Cecchini
coordinatore di GARR-CERT

IV Incontro di GARR-B
Bologna, 25 Giugno 2002

GARR-CERT
servizio sicurezza GARR

GARR-CERT

- Lo CSIRT della rete GARR:
  - in attività dal Giugno 1999;
  - opera in stretta collaborazione con il Network Operation Center (NOC).
- Risorse umane:
  - nucleo operativo (sede a Firenze): 4 (2 full-time);
  - esperti e "ufficiali di collegamento": 4;
  - contatti locali (APM): ≈ 280.
- "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** (**abuse@garr.it, abuse@cnr.it, abuse@infn.it**): segnalazioni incidenti;
    - gli iscritti sono i membri di GARR-CERT.
  - **sicurezza@garr.it**: security alert;
    - iscrizione libera.

Attività preventive

- Partecipazione a incontri tecnici;
- Scansioni alla ricerca di vulnerabilità (su richiesta dell' APA/APM)
  - ≈ 60 nel 2001.
- 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.
- Ad ogni incidente viene assegnato un numero univoco per ogni coppia vittima-attaccante.
- E-mail sono 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.
  - Nel 2001 ≈ 70 richieste agli APM (il 40% scalato al NOC).
- E-mail con dettagli sulle azioni intraprese sono inviati a tutte le parti coinvolte.

eCSIRT: obiettivi

- Progetto europeo.
- Obiettivi:
  - definizione di un linguaggio comune per lo scambio di dati tra CSIRT;
  - scambio di informazioni su incidenti, come normale prassi operativa tra CSIRT;
  - meccanismo di raccolta di statistiche *non ambigue* di incidenti;
  - raccolta di dati relativi ad incidenti al fine di fornire agli CSIRT informazioni di "early warning" da distribuire all'utenza.

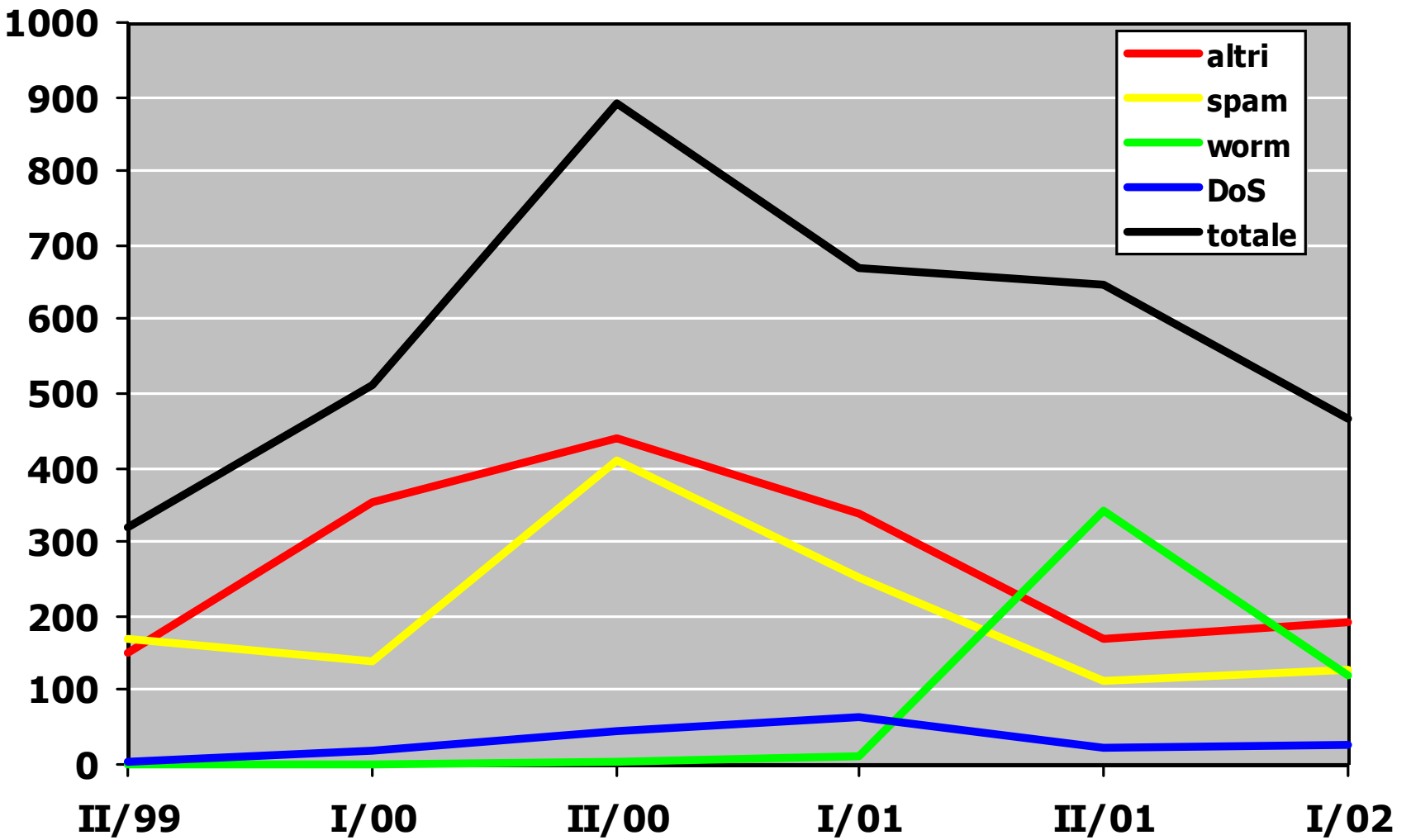
eCSIRT

- Durata 15 mesi.
- Partecipanti
  - M&I/Stelvio b.v. (NL)
  - PRESECURE Consulting GmbH (D)
  - GARR-CERT (I)
  - Le CERT Renater (F)
  - JANET-CERT (UK)
  - DFN-CERT GmbH (D)
  - CERT-Polska (PL)
  - DK-CERT (DK)
  - IRIS-CERT (E)

Nuovo uso **security@garr.it**

- Brevi segnalazioni dei principali alert pubblicati (a cura di Massimo Ianigro).
- Pubblicazione di note d'uso, esperienze, tutorial, how-to, ecc. ecc.
  - i vostri contributi sono indispensabili!
    - spediteli a **cert-staff@garr.it**;
    - verranno valutati da un mini comitato editoriale e, se ritenuti di interesse generale, inviati a **security@garr.it** e pubblicate sul server web di GARR-CERT.

Incidenti segnalati a GARR-CERT



Honeypot

- Esperimento al San Diego Supercomputer Center (SDSC):
  - **23/12/99**: installazione completa di RedHat 5.2 su di una macchina inutilizzata e tenuta sotto osservazione;
  - **14/1/00**: probe per Solaris RPC;
  - **14-18/1/00**: prova di 20 exploits (POP, IMAP, telnet, RPC, mountd ...) falliti perchè per RedHat 6;
  - **xx/2/00**: compromissione via vulnerabilità POP e installazione di rootkit e sniffer;
  - **18/2/00**: altra compromissione, server web defacing, diffusione notizia su IRC e segnalazione di attrition.org.
- Lo stesso esperimento ripetuto nel 2001:
  - prima scansione dopo **30 secondi**;
  - primo tentativo di compromissione dopo **1 ora**;
  - compromissione completa dopo **12 ore**.

Attività dopo la compromissione

- Riproduzione (worm);
- Bot IRC;
- Attacchi (D)DoS (smurf, *trinoo*, *tfn, tfn2k, stacheldraht*, ...);
- Warez;
- Sniffer;
- Scansioni;
- Attacchi ad altri nodi (in special modo sulla stessa LAN).

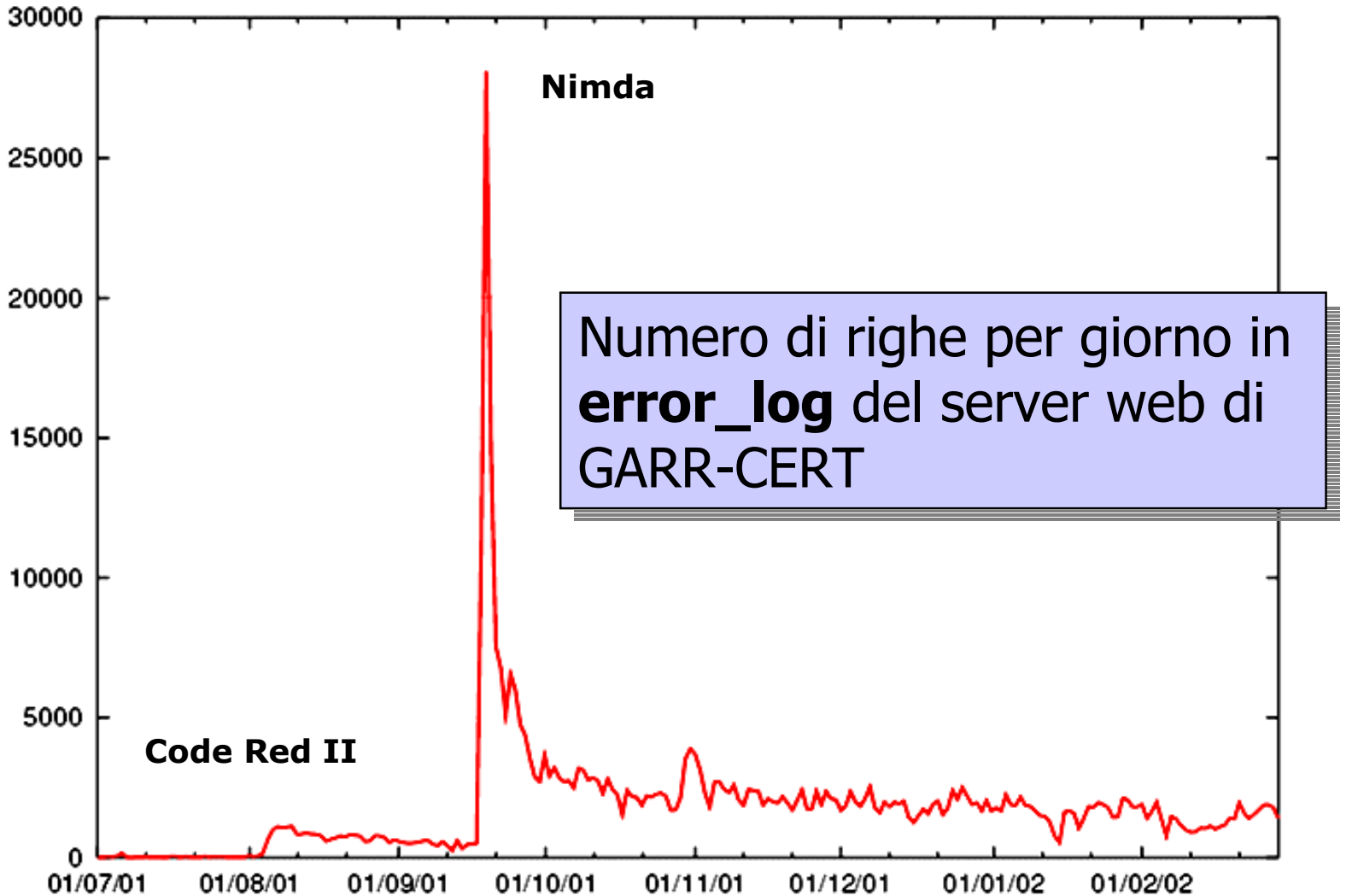
I worm 1/2

- Un worm è del codice ostile in grado di autopropagarsi da solo, senza necessità di intervento dell'utente, a differenza dei virus.
- La combinazione di un meccanismo di propagazione veloce con una grande diffusione della vulnerabilità sfruttata produce velocità di diffusione impressionanti.
- Spesso l'effetto più importante è il denial of service provocato dalle scansioni alla ricerca di nuovi sistemi da compromettere.

I worm 2/2

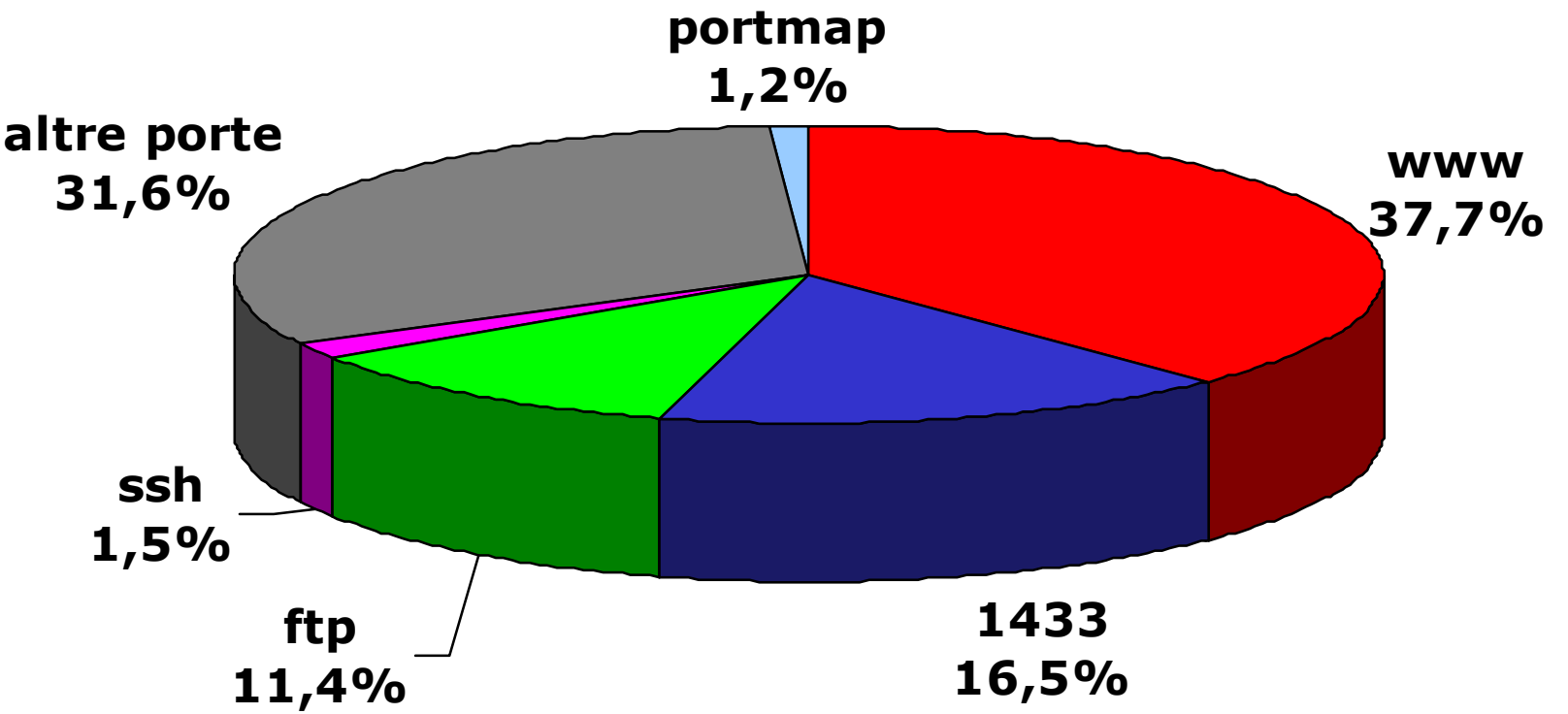
- Social Engineering
  - W32/Sircam
- Specifiche vulnerabilità
  - sadmind/IIS worm
  - Code Red, Code Red II
  - Nimda
  - Spida/SQLsnake/Digispid
- Le principali vittime sono utenti windows
  - meno sofisticati tecnicamente
  - meno protetti
  - meno attenti ai security alert

Propagazione dei worm



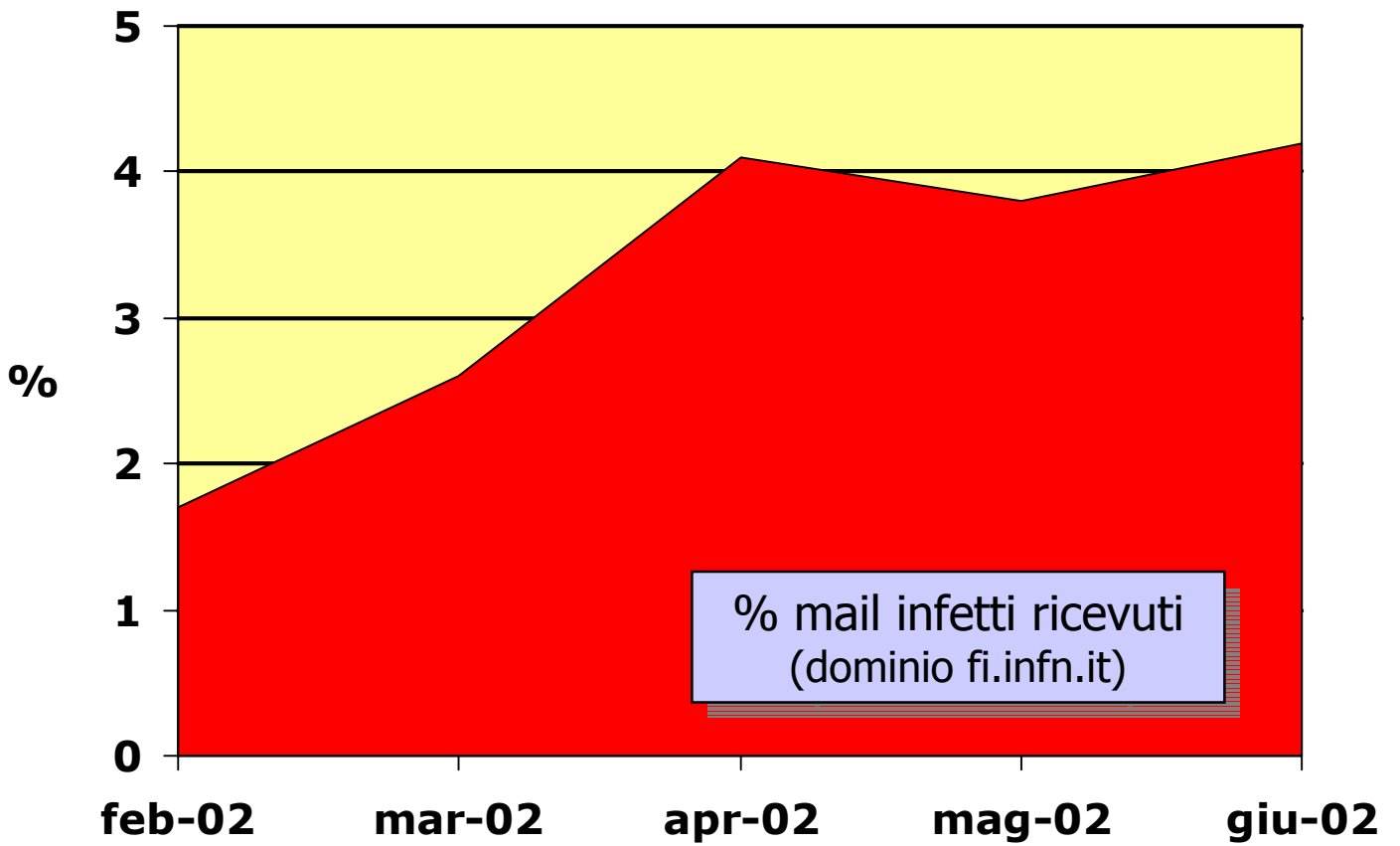
Numero di righe per giorno in **error_log** del server web di GARR-CERT

Scansioni nel periodo 10-17/6/02



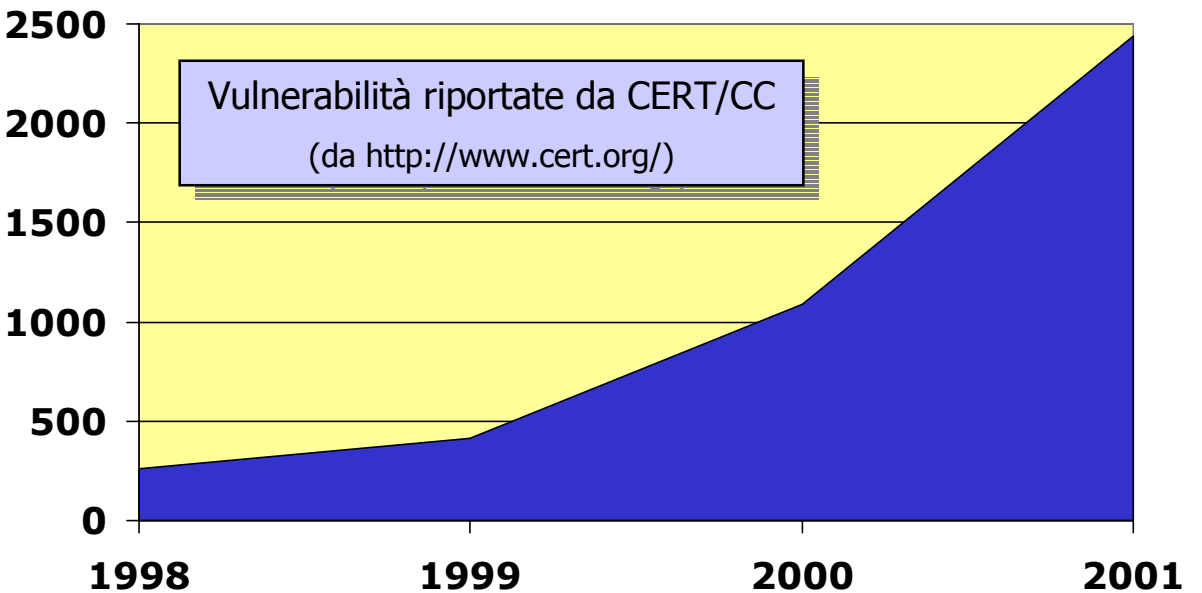
da http://www.incidents.org/

Virus via mail



Il futuro 1/2

- La qualità del software prodotto non sembra migliorare:
  - il ciclo sviluppo-prova-rilascio software è in continua diminuzione;
  - continua a essere rilasciato software con vulnerabilità di tipo ormai ben noto (ad es. *buffer overflow*).



Il futuro 2/2

- Prevedibile una nuova generazione di worm e virus più virulenti.
- I nodi GARR, con l'aumento della banda a disposizione, sono molto appetibili come strumenti per attacchi (D)DoS.
- Nuove tecnologie pongono nuovi problemi di sicurezza
  - "griglie" di calcolo (ad es. DataGRID);
  - nuovi protocolli "firewall-friendly";
  - P2P;
  - wireless;
  - ...

Che fare? 1/2

- Stabilire (e far rispettare!) serie politiche di sicurezza a livello di Ateneo e Istituti di ricerca (compresa la creazione di nuovi CSIRT).
  - Direttiva della Presidenza del Consiglio dei Ministri (Dipartimento per l'Innovazione e le Tecnologie), *Sicurezza informatica e delle telecomunicazioni nelle pubbliche amministrazioni* (16 Gennaio 2002):
    - autodiagnosi del livello di adeguatezza della sicurezza informatica e delle telecomunicazioni (ICT);
    - attivazione delle necessarie iniziative per posizionarsi sulla "base minima di sicurezza", che consenta di costruire con un approccio unitario e condiviso, le fondamenta della sicurezza della pubblica amministrazione;
    - promuovere la creazione e la successiva attivazione di un modello organizzativo nazionale di sicurezza ICT che comprenda tutti gli organi istituzionali, scientifici ed accademici deputati, ciascuno per il proprio ruolo, ad assicurare organicità e completezza al tema sicurezza.

Che fare? 2/2

- Aumentare la consapevolezza dell'utenza e migliorare la tempestività dell'informazione
- Aumentare (in quantità e qualità) le interazioni tra gli CSIRT (in particolare con quelli degli ISP).
  - eEurope ActionPlan: "*Stimulating public/private cooperation on dependability of information infrastructures (including the development of early warning systems) and improving cooperation amongst national computer emergency response teams*".

Servizi da bloccare o controllare

- Da raccomandazioni di CERT/CC
  - Login: 21/T, 22/T, 23/T, 139/T, 512-514/T
  - RPC & NFS: 111/TU, 2049/TU, 4045/TU
  - NetBIOS: 135/TU, 137-138/U, 445/TU
  - X Windows: 6000-6255/T
  - Naming: 53/TU, 389/TU
  - Mail: 25/T, 109-110/T, 143/T
  - Web: 80/T, 443/T
  - Small Services: <20/TU, 37/TU
  - Vari: 69/U, 79/T, 119/T, 123/T, 161-162/TU, 179/T, 514/U, 515/T, 1080/T
  - ICMP: ...
- Molto meglio bloccare tutto e aprire caso per caso!