GARR-CERT

Roberto Cecchini

INFN Firenze

III Incontro di GARR-B

Firenze, 24-25 Gennaio 2001

GARR-CERT

- Il servizio
  - istituito nel Marzo 1999, pienamente operativo da Giugno 1999;
  - 7 unità: 1 a tempo pieno e 6 a tempo parziale, sede centrale a Firenze.
- Gli utenti sono tutte le istituzioni afferenti alla rete GARR:
  - gli APM gli interlocutori principali.
- Descrizione formale (RFC2350):
  www.cert.garr.it/GARR-CERT-descr-rfc.html
- Coordinamento con gli altri CSIRT Europei
  - "Trusted Inroducer" Level 2 Team (**www.ti.terena.nl**)

I compiti

- Rispondere alle segnalazioni di incidenti, avvertire ed assistere gli utenti coinvolti e seguirne gli sviluppi.
- Diffondere informazioni sulle vulnerabilità più comuni e sugli strumenti da adottare.
- Aumentare il livello di sensibilità dell'utenza verso i problemi della sicurezza.
- Svolgere attività preventive per ridurre la probabilità di incidenti.
- Provare strumenti esistenti e svilupparne di nuovi per esigenze specifiche.

Chi siamo

- Membri
  - Roberto Cecchini <roberto.cecchini@fi.infn.it>
  - Claudio Allocchio <claudio.allocchio@elettra.trieste.it>
  - Paolo Amendola <paolo.amendola@ba.infn.it>
  - Luca dell'Agnello <luca.dellagnello@cnaf.infn.it>
  - Francesco Gennai <francesco.gennai@iat.cnr.it>
  - Francesco Palmieri <fpalmier@unina.it>
  - Andrea Pinzani <andrea.pinzani@fi.infn.it>
- Tutti i nostri e-mail sono firmati (PGP) con la chiave personale del mittente (reperibili su **www.cert.garr.it/PGP/**).
- È disponibile anche una chiave PGP di GARR-CERT con cui vengono firmate alcune pagine sul server web e utilizzabile per inviare informazioni in forma riservata.

I servizi

- Server web: **www.cert.garr.it**
  - documenti sui problemi più comuni;
  - raccolta alert (e riepilogo);
  - mini collezione di leggi.
- Server FTP
  - a richiesta e solo per scarico dati relativi ad incidenti (ad es. logfile).
- Mailing list
  - **cert@garr.it** (**abuse@garr.it**)
    - gli iscritti sono tutti i membri di GARR-CERT;
    - posting libero;
    - chiunque può (e dovrebbe) usarla per segnalare incidenti.
  - **sicurezza@garr.it**
    - iscrizione aperta a tutti, posting ristretto;
    - diffusione di allarmi di sicurezza e comunicazioni di interesse generale;
    - per iscriversi inviare un mail a **majordomo@garr.it**, con nel testo **`subscribe`**

Attività preventive

- Scansioni (su richiesta dell'APM):
  - porte e/o vulnerabilità.
- Controllo nodi ex open mail relay (settimanale).
- Controllo nodi nei database pubblici di open mail relay (mensile).
- Organizzazione e partecipazione a incontri su problemi di sicurezza.
- Whishlist
  - Controllo configurazione dei router:
    - *smurf*, *ingress* e *egress filtering*, diritti di accesso.
  - Sistema di allarme (semi-)automatico per attacchi DoS (insieme al NOC).

Apertura incidente

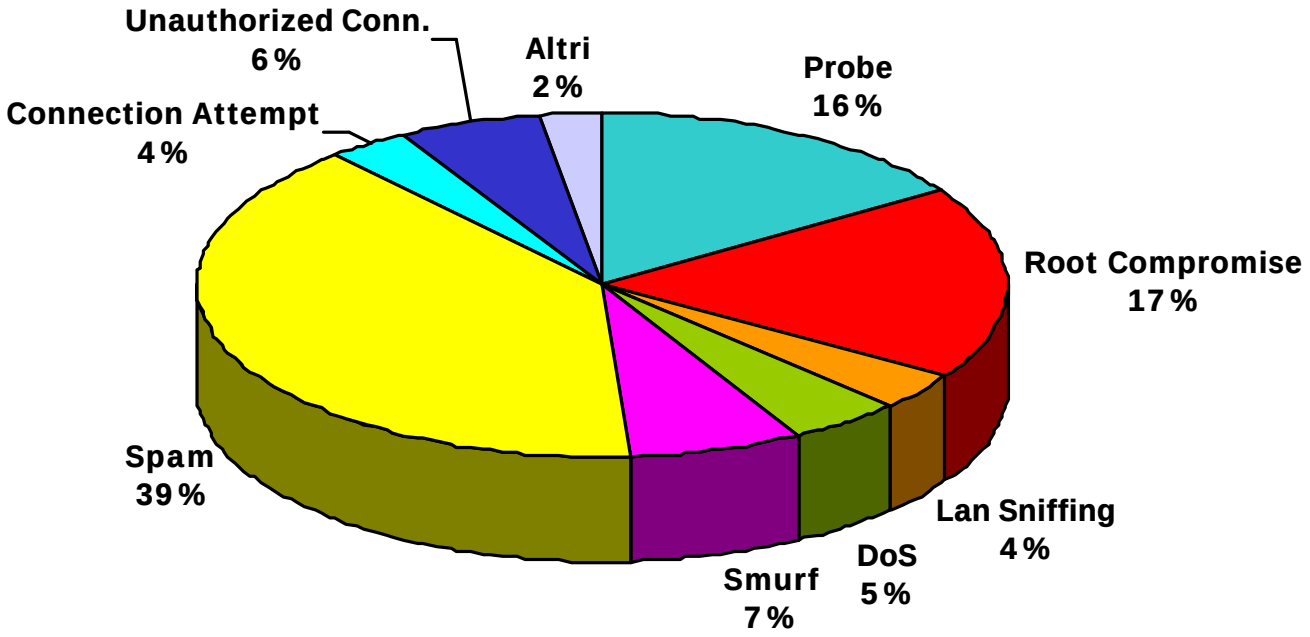
- Un incidente:
  - coinvolge un nodo della rete GARR;
  - implica la violazione di una qualche “regola” (leggi, AUP, netiquette);
- Quando:
  - ogni segnalazione ricevuta che obbedisca alle regole di sopra e non sia palesemente errata (ad es. un indirizzo GARR in un header di mail falsificato): in ogni caso viene conservata;
  - analisi di file di log (ad es.: password in un log di sniffer);
  - attività preventive (ad es.: vecchi incidenti, ORBS).
- Gli incidenti vengono memorizzati nel nostro database e classificati:
  - un codice univoco (data + numero progressivo) per ogni coppia vittima-attaccante (nodo o rete), eccetto gli spam (un solo codice).
- E-mail vengono inviati a tutte le parti coinvolte:
  - ad esclusione dei messaggi automatici da *SpamCop* e simili.

Chiusura incidente

- Incidenti che originano da nodi GARR **devono** essere risolti (almeno temporaneamente) in tempi massimi predefiniti.
  - Procedura approvata dall'OTS GARR il 20/12/99: (**www.cert.garr.it/incidenti.php3**)
    - **GARR-CERT invia una comunicazione di apertura incidente ai responsabili locali coinvolti e all'APM;**
    - **se il problema non viene risolto nei tempi previsti, GARR-CERT invia all'APM la richiesta di filtraggio sul router di connessione alla rete GARR;**
    - **se l'APM non interviene, GARR-CERT invia al GARR-NOC la richiesta di filtraggio sul router di accesso al GARR.**
  - Nel 2000: ≈ 70 richieste agli APM e ≈ 30 al NOC.
- Incidenti causati da nodi non GARR che non rispondono alle nostre segnalazioni vengono, di solito, chiusi d'ufficio dopo un tempo predefinito.
- E-mail con qualche dettaglio sulle azioni intraprese vengono inviati a tutte le parti coinvolte.

Incidenti (per tipo)

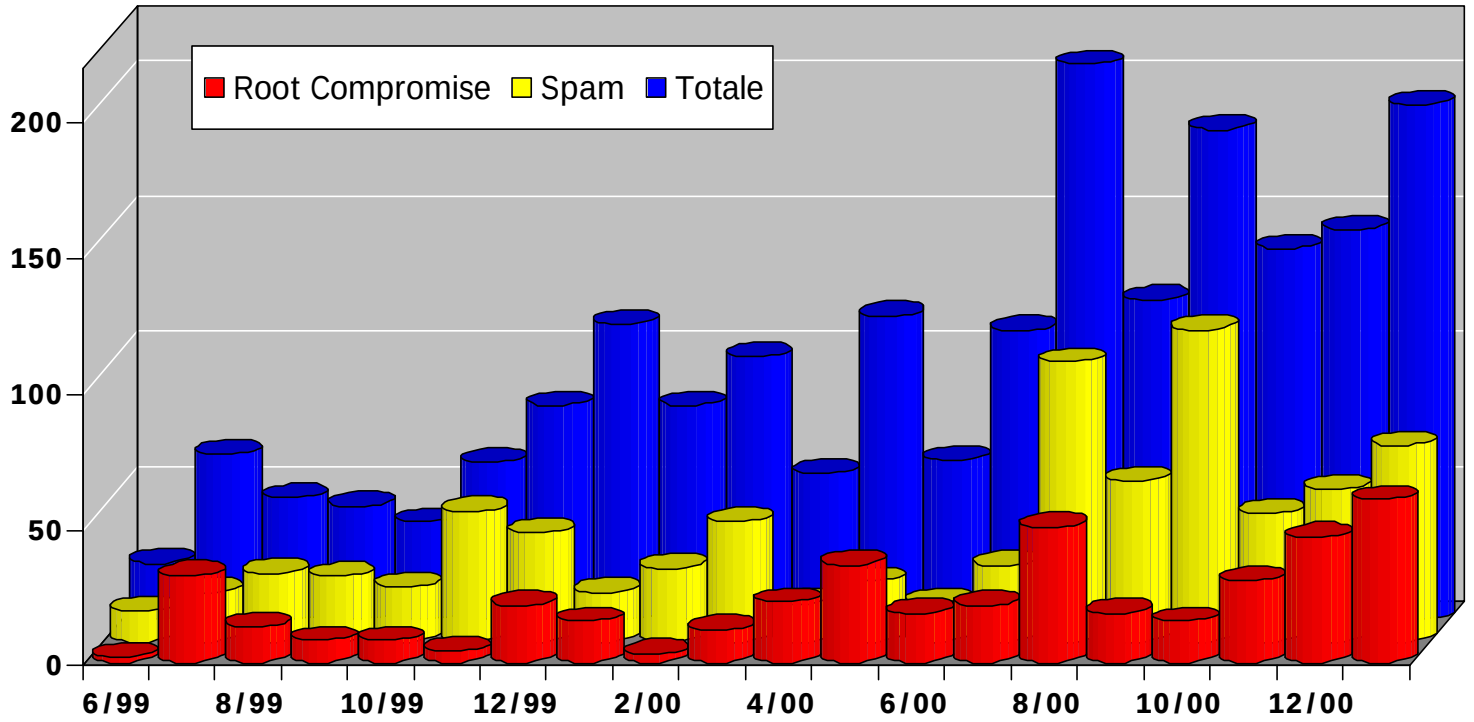
Dal 1/1/2000 al 31/12/2000



Totale: 1381

messaggi di e-mail: 10300

Incidenti segnalati



Root Compromise include *Lan Sniffing* e *DoS* (dati per 01/01 estrapolati)

Che percentuale del totale?

Perché segnalare un incidente?

- Possiamo cercare di aiutarvi:
  - assistenza tecnica;
  - gestione incidente.
- Le vostre segnalazioni ci permettono di avere un quadro più chiaro di cosa sta succedendo sulla rete:
  - possiamo aiutare meglio gli altri dando informazioni più precise.
- Informare i responsabili dei siti da cui è giunto l'attacco è quasi sempre fare loro un favore.
- È una delle regole di convivenza civile su internet:

> The Internet is a cooperative venture. The culture and practice in the Internet is to render assistance in security matters to other sites and networks. Each site is expected to notify other sites if it detects a penetration in progress at the other sites, and all sites are expected to help one another respond to security violations.
>
> *Guidelines for the Secure Operation of the Internet* (RFC1281)

Come segnalare un incidente (1/2)

- Inviate un mail a **cert@garr.it** (o riempite il modulo online) con:
  - data e ora (con la precisione del vostro clock);
  - descrizione dell'incidente;
  - come essere contattati;
  - estratti dai log e eventuali altri file lasciati dall'intruso:
    - **se oltre 500k non li spedite, limitatevi a dire che li avete: verrete richiamati per stabilire le modalità del trasferimento;**
  - permesso (o diniego) di diffondere la vostra identità:
    - la vostra identità viene **sempre** mascherata, viene fornita **solo** su esplicita richiesta della controparte e **solo se avete esplicitamente concesso l'autorizzazione**.

Come segnalare un incidente (2/2)

- Riceverete un mail di conferma apertura incidente e verrete tenuti aggiornati sugli sviluppi fino alla chiusura:
  - vi verrà comunicato un codice identificativo dell'incidente (**GARR-CERT-xxxxxx**), che vi preghiamo di citare in tutta la corrispondenza successiva.