Manomissione del serverone

Leandro Noferini
lnoferin@cybervalley.org

Firenze Linux User Group

EPrivacy 2006 - 19 maggio 2006 - Firenze

Sommario

Perché questo intervento

il Firenze Linux User Group e il serverone
- Serverone

Breve storia dell'housing
- Firenze
- Milano
- Ritorno a Firenze e scoperta della manomissione

Manomissione
- Scoperta
- Conseguenze

Perché questo intervento

Il serverone ha ospitato e ospita tutt'ora

- servizi per l'anonimato (remailer, server tor)
- la comunità che si ritrova intorno al Progetto Winston Smith

Similitudini con la vicenda del server degli autistici il quale ospitava servizi simili a quelli del serverone

Cos'è il FLUG

Il Firenze Linux User Group (Flug) è uno dei GNU/Linux User Group esistenti a Firenze
Fondato con un'assemblea pubblica nel marzo 1998 non si è mai costituito come associazione regolarmente riconosciuta di conseguenza non ha alcun tipo di rappresentanza con valore legale

- nessuno può stipulare un contratto a nome del Flug
- nessuno può presentare una denuncia a nome del Flug

Scopi e nascita del serverone

Il serverone è un computer gestito dal Flug per offrire ospitalità e servizi alla comunità del software libero
Il nomignolo deriva dal fatto che nella sua prima incarnazione il computer era un piccolo 486 con otto mega di ram
Attualmente il suo hardware è il seguente:

- Processore Pentium 4 a 2.40 Ghz
- 512 mega di ram
- 2 dischi uguali da 200 giga
- case da 1 unità

Servizi disponibili sul serverone

Al momento della scoperta della manomissione questi erano i servizi disponibili sul serverone

- server web
- liste posta elettronica
- alias di posta elettronica
- remailer di tipo II *antani*
- remailer di tipo III
- login diretto sul computer (esclusivamente per i gestori del computer)

Successivamente è stato attivato anche il server tor *tortuga*

Gruppi ospitati sul serverone

- GNU/Linux user group di Firenze, Empoli e Perugia
- gruppo di traduttori italiani di Gnome
- Progetto Winston Smith

Housing a Firenze

DADA (http://www.dada.net) è un noto provider internet italiano nato a Firenze
Rapporto con Dada iniziato nel 1999
Prima installazione nel CED di via Pandolfini (nel centro della città di Firenze)
Primo spostamento nel nuovo CED di viale Giovine Italia (sempre nel centro della città)

Trasferimento a Milano

Spostamento a Milano all'interno dello spazio riservato espressamente a Dada nello stabile del provider *Inet*
Spostamento avvenuto nel febbraio 2003 e curato direttamente dei tecnici di DADA
Successivamente il Flug acquistò l'hardware attualmente in uso, installato in due giorni 14 e 15 gennaio 2004
Da quella data il serverone è rimasto acceso ininterrottamente così come abbiamo verificato direttamente dall'uso nonché dalla registrazione dell'uptime fino al giorno dello spostamento all'interno del CED di Dada

Spostamento all'interno del CED

DADA ci comunicò che il 23 marzo 2005 il serverone, insieme a molti altri server, sarebbe stato spostato da una stanza ad un'altra
Lo spostamento è stato curato esclusivamente dai tecnici di Dada
Il server fu spento dagli amministratori del Flug da remoto
Fu riacceso dai tecnici di Dada circa tre ore dopo
Da quel giorno il serverone rimase ancora acceso initerrottamente fino al giorno della scoperta della manomissione
Lo spostamento è stato verificato successivamente (il giorno della scoperta della manomissione) personalmente dagli incaricati del Flug che lo avevano installato la prima volta

Offerta da parte di Playnet

Durante i primi mesi del 2005 la ditta Playnet (del gruppo EsseDi) ha fatto al Flug un'offerta di sponsorizzazione
Sponsorizzazione da concretizzarsi anche con l'offerta di housing gratuito presso il loro CED di Firenze

- housing gratuito
- avvicinamento a *casa*
- inizio di un rapporto con Playnet

Scoperta

Il 27 giugno 2005 due amministratori del serverone hanno verificato la manomissione del serverone in presenza di un tecnico di Inet
Dopo la contestazione il server è stato staccato e portato a Firenze
Appena arrivati a Firenze sono stati convocati i membri del Flug più direttamente coinvolti nella gestione del server e dei vari servizi
Sono stati verificati i danni subiti
È stato deciso di considerare compromesso il server
È stato redatto il comunicato da diffondere per spiegare perché il server non sarebbe stato reso disponibile

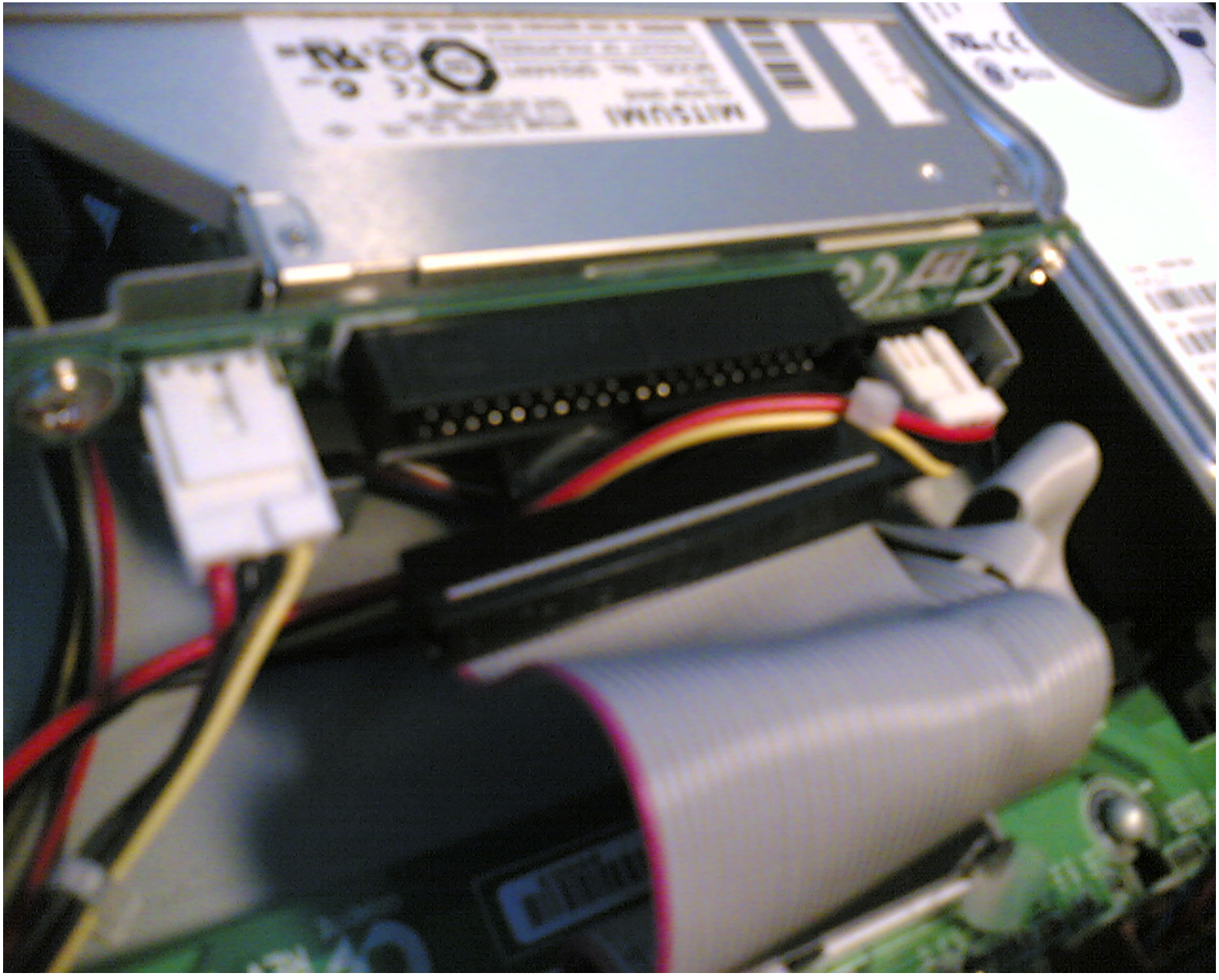
Danni accertati

- all'esterno il case era in evidenza chiuso male
- all'esterno risultavano mancanti alcune viti di fissaggio del case
- all'interno il cavo di collegamento IDE del cdrom era completamente staccato
- all'interno risultavano mancanti le viti di fissaggio delle slitte degli harddisk

Case chiuso male 1/2

Case chiuso male 2/2

Cavo ide del cdrom



Vite degli hard disk

Viti esterne

Etichetta di Dada

Passi tecnici

- sospensione di tutti i servizi
- cambio degli harddisk
- reinstallazione di tutto il software
- cambio delle chiavi del remailer

Passi legali

È stata presentata denuncia per i reati del Codice Penale

- 635 (danneggiamento)
- 635 bis (danneggiamento di sistemi informatici)

Presentata da un gruppo di persone *scelte* come rappresentanti delle varie anime del serverone: amministratore, responsabile legale, amministratore del remailer e rappresentate del gruppo
Presentata il 20 settembre 2005 a Firenze
Attualmente non abbiamo ricevuto alcuna comunicazione da parte degli inquirenti

Passi politici

Il senatore *Fiorello Cortiana* ha presentato il 28 luglio 2005 un'interrogazione parlamentare ai ministri delle *Comunicazioni* e della *Innovazione e Tecnologia*
Su sollecitazione degli amministratori di Antani
L'interrogazione non ha ancora ricevuto alcuna risposta