Spam ? No Grazie!

Claudio Allocchio

III Incontro di GARR-B

Firenze, 24 e 25 Gennaio 2001

Sommario

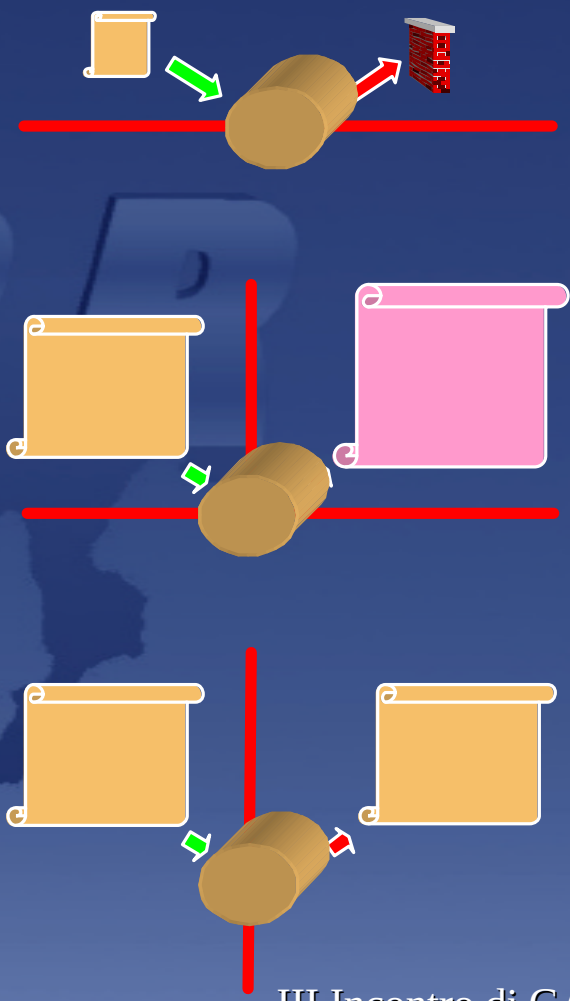
- Rissunto delle puntate precedenti...
- ...non c'e' un solo tipo di Spam!
- Come raccogliere le informazioni
- Header e "logs": l'impronta digitale del "delitto"
- Come si leggono le prove?
- Dove sono i colpevoli?
- Cosa fare quando li scopriamo?
- E per difendersi meglio?

Riassunto: cosa e' lo SPAM?

- Invio di migliaia di messaggi a "spese altrui": MTA e risorse di rete (banda)
- Utilizzo di account gratuiti (AOL, Compuserve, msn, hotmail, tin, libero, tiscali,...)
- Utilizzo di software "per spamming"
- Spamming "ingenuo"
- La legge e lo SPAM: DL 185/99

Riassunto: Tipologie di SPAM

- Classico:
  - "unauthorized mail relaying"
- Delitto Perfetto:
  - "doppio non delivery"
- Attacco Diretto:
  - "forged e-mail address"



Classico: Protezione proprio MTA

- http://www.cert.garr.it/documenti/sendmail
- http://www.cert.garr.it/incontri/na/mail.html
- http://www.orbs.org/otherresources.html
- ...

Doppio non delivery

- ... poca difesa (ma anche poco usato)
- leggere gli headers del messaggio
- il proprio MTA e' innocente!

Attacco Diretto

- ... i colpevoli sono “gli altri”
- leggere gli headers del messaggio
- il proprio MTA e’ innocente!
- come segnalare o bloccare gli MTA colpevoli

SPAM “ingenuo”

- Mittente “vero” !!
- Destinatario “vero” (la vittima)
- Il vostro MTA e’ innocente !
- Messaggio “Unsolicited Commercial E-mail” (UCE)
- Messaggio “Chain Letter” (catena di S. Antonio)
- Segnalare l’attacco al CERT ed alla Naming Authority Italiana abuse@na.nic.it

La Legge e lo SPAM

- TUTTO lo SPAM e' vietato dalla Netiquette, obbligatoria per i domini del ccTLD "it"
- Le UCE sono vietate dalla legge: DL 185/99, articolo 10, con sanzione amministrativa da 1 a 10 Milioni di Lire

Raccolta Informazioni

- un e-mail e' composto da:
  - Envelope Esterna (SMTP)
  - Header Interno (RFC822)
  - Contenuto (eventualmente "multipart")
- ognuna contiene informazioni utili!
  - Header Interno
    - Envelope Esterna
      - parti del Contenuto

Dove trovo le parti?

- Envelope Esterna:
  - Log file del proprio MTA
- Header Interno:
  - dentro il messaggio !
  - richiedere sempre Headers COMPLETI !!
- Contenuto
  - dentro il messaggio !
  - richiedere informazioni tipo:
    - numero di telefono, fax,...
    - indirizzi, caselle postali, ...

Esempi di Header “inutili”

From: Tullio Regge <regge@POLITO.IT>
Reply-To: Segnalazione Spam <ABUSE@NA.NIC.IT>
Subject: Fwd: |||| Must Be 21 Yrs |||| -- Get The Ultimate "Herbal"

>Date: Thu, 02 Nov 2000 21:23:18 -0400
>From: qhsia@mail.region.durham.on.ca
>Subject: |||| Must Be 21 Yrs |||| -- Get The Ultimate "Herbal”
>To: njxxk@mail.region.durham.on.ca
>Original-recipient: rfc822;regge@polito.it

Cosa devo Cercare?

- Che tipo di SPAM e'?
  - Classico?
  - Doppio non Delivery?
  - Diretto?
  - Ingenuo?
- Dove distinguo?
  - dall'Header:
    - mittente
    - destinatario

Header SPAM Classico

```
Return-Path: <free_credit_card@gnl.cplaza.ne.jp>
Received: from inetsrv.dsgroup.it ([212.17.198.157])
        by mtiwgwc24.worldnet.att.net
        (InterMail vM.4.01.03.10 201-229-121-110) with ESMTP
        id <XAQE11671.mtiwgwc24.worldnet.att.net@inetsrv.dsgroup.it>;
        Fri, 27 Oct 2000 16:37:55 +0000
Received: from come.to (pppa66-resalenashville2-4r7232.saturn.bbn.com
      [4.54.209.159]) by inetsrv.dsgroup.it with SMTP (Microsoft Exchange
      Internet Mail Service Version 5.5.2650.21)
      id 4YPABXTW; Fri, 27 Oct 2000 18:40:03 +0200
Message-ID: <DtQaZ.+7f.I3s.RwzaE0J0ses-FL@come.to>
From: free_credit_card@gnl.cplaza.ne.jp <free_credit_card@gnl.cplaza.ne.jp>
To: free@india23.com <pinebeetle@att.net>
Subject: FREE Visa Gold Card (73487)
Date: Fri, 27 Oct 2000 11:35:48 -0400 (EDT)
MIME-Version: 1.0
Content-Type: TEXT/PLAIN; charset="US-ASCII"
Content-Transfer-Encoding: 7bit
X-Mozilla-Status2: 00000000
```

Header SPAM Classico (2)

From: free_credit_card@gnl.cplaza.ne.jp
<free_credit_card@gnl.cplaza.ne.jp>

To: free@india23.com
<pinebeetle@att.net>

- ... ma io cosa c'entro con questi due domini?
- ... perche' protestano con me?

Header SPAM
“doppio non delivery”

Received: from inetsrv.dsgroup.it ([212.17.198.157])
by mtiwgwc24.worldnet.att.net
Fri, 27 Oct 2000 16:37:55 +0000
From: postmaster <postmaster@inetserv.dsgroup.it>
To: free@india23.com <pinebeetle@att.net>
Subject: your message could not be delivered
Date: Fri, 27 Oct 2000 11:35:48 -0400 (EDT)

550 No such user <123dshl@inetserv.dsgroup.it>

---------- returned mail message ----------

Received: from come.to (pppa66-resalenashville2-4r7232.saturn.bbn.com
by inetsrv.dsgroup.it with SMTP; Fri, 27 Oct 2000 18:40:03 +0200
Message-ID: <DtQaZ.+7f.l3s.RwzaE0J0ses-FL@come.to>
From: free@india23.com <pinebeetle@att.net>
To: <123dshl@inetserv.dsgroup.it>
Subject: Get VIAGRA Now !

Header SPAM Diretto

Received: from 212.239.17.90 [212.239.17.91] by posta.alinet.it
(SMTPD32-5.05) id AA2C19F200E6; Mon, 30 Oct 2000 19:13:00 +0100
Date: Mon, 30 Oct 2000 12:10:00
From: yoyrserver@it.buongiorno.com
To: bowling@posta.alinet.it
Subject: N.6: Arriva la newsletter del Nobel Dario Fo
Message-Id: <200010301913768.SM00179@212.239.17.90>
X-RCPT-TO: <bowling@posta.alinet.it>
X-UIDL: 631
Status: U

... e' quello per cui i PROPRI utenti protestano!
... il destinatario e' un nostro utente VERO!
... il mittente e' invece solitamente uno user FALSO
... il dominio del mittente puo' essere vero o falso

Header SPAM Ingenuo

Received: from 212.239.17.90 [212.239.17.91] by posta.alinet.it
(SMTPD32-5.05) id AA2C19F200E6; Mon, 30 Oct 2000 19:13:00 +0100
Date: Mon, 30 Oct 2000 12:10:00
From: katia5@it.buongiorno.com
To: bowling@posta.alinet.it
Subject: il mio nuovo WEB online !
Message-Id: <200010301913768.SM00179@212.239.17.90>
X-RCPT-TO: <bowling@posta.alinet.it>
X-UIDL: 631
Status: U

e' tutto vero! MITTENTE e DESTINATARIO
e' come lo SPAM Diretto, ma con il MITTENTE VERO !

Come si legge un Header?

```
Received: from 212.239.17.90 [212.239.17.91] by posta.alinet.it
  (SMTPD32-5.05) id AA2C19F200E6; Mon, 30 Oct 2000 19:13:00 +0100
Date: Mon, 30 Oct 2000 12:10:00
From: katia5@it.buongiorno.com
To: bowling@posta.alinet.it
Subject: il mio nuovo WEB online !
Message-Id: <200010301913768.SM00179@212.239.17.90>
X-RCPT-TO: <bowling@posta.alinet.it>
X-UIDL: 631
Status: U
```

- dal BASSO verso l'ALTO!
- le righe Received sono la traccia degli MTA usati
- la riga Date e' inserita dal Client Mittente (inaffidabile)
- attenzione ai Fusi Orari

I campi Importanti

- From:
- To:
- Message-ID:
- Received:

Message-ID:

Message-ID: <guhvVnJ47q+V9.S85V6aLT4xltaB@come.to>

Message-Id: <200010301913768.SM00179@212.239.17.90>

Message-Id: <000801c082c2$9a1afc60$83c06397@it>

- La parte interessante e' dopo la @
- Solitamente e' il dominio o il numer IP del primo mailer
- Non e' SEMPRE vero!

Received:

Received: from alfliglibero (pool0-131.cisea.it [151.99.192.131])
by dns.cisea.it (8.9.3/8.9.3) with SMTP id LAA10789
for <hostmaster@PANIX.COM>; Sat, 20 Jan 2001 11:22:30 +0100

Data,

Ora,

Fuso Orario

- GMT +/- differenza
- MET, PST, CST-DST, A-Z (Military), ...

Received:

Received: from alfliglibero (pool0-131.cisea.it [151.99.192.131])
by dns.cisea.it (8.9.3/8.9.3) with SMTP id LAA10789
for <hostmaster@PANIX.COM>; Sat, 20 Jan 2001 11:22:30 +0100

from (MTA Mittente)
- nome “dichiarato” dall’MTA Mittente
- nome ricavato dal DNS (PTR reverse lookup)
- indirizzo IP (dalla socket di connessione)

Received:

Received: from alfliglibero (pool0-131.cisea.it [151.99.192.131])
by dns.cisea.it (8.9.3/8.9.3) with SMTP id LAA10789
for <hostmaster@PANIX.COM>; Sat, 20 Jan 2001 11:22:30 +0100

by (MTA che ha scritto la riga)
nome del MTA che ha scritto la riga
software di MTA (in questo caso Sendmail)
protocollo usato per la transazione
ID sulle code del MTA (da usare per i LOG)

SPAM Ingenuo: cosa faccio?

- tecnicamente e' un mail "normale"
- controllo il percorso tramite i "Received"
- cerco con un WHOIS il responsabile dominio
  - whois -h whois.nic.it (.it) *host/dominio*
  - whois -h whois.ripe.net (europei) *host/dominio*
  - whois -h whois.internic.net (gTLD) *host/dominio*
- se lo trovo, lo informo che il suo utente fa SPAM

SPAM Diretto: cosa faccio?

- tecnicamente e' un mail diretto a noi
- il mittente (user e/o dominio) e' spesso falso
- controllo il percorso tramite i "Received"
- solitamente e' implicato un Open Mail Relay
- identificare l'Open Mail Relay
- segnalarlo al CERT e/o ORBS

SPAM Diretto: caccia al Relay!

Return-Path: <free_credit_card@gnl.cplaza.ne.jp>
Received: from inetsrv.dsgroup.it ([212.17.198.157])
by mtiwgwc24.worldnet.att.net
(InterMail vM.4.01.03.10 201-229-121-110) with ESMTP
id <XAQE11671.mtiwgwc24.worldnet.att.net@inetsrv.dsgroup.it>;
Fri, 27 Oct 2000 16:37:55 +0000
Received: from come.to (pppa66-resalenashville2-4r7232.saturn.bbn.com
[4.54.209.159]) by inetsrv.dsgroup.it with SMTP (Microsoft Exchange
Internet Mail Service Version 5.5.2650.21)
id 4YPABXTW; Fri, 27 Oct 2000 18:40:03 +0200
Message-ID: <DtQaZ.+7f.l3s.RwzaE0J0ses-FL@come.to>
From: free_credit_card@gnl.cplaza.ne.jp <free_credit_card@gnl.cplaza.ne.jp>
To: free@india23.com <pinebeetle@att.net>
Subject: FREE Visa Gold Card (73487)
Date: Fri, 27 Oct 2000 11:35:48 -0400 (EDT)

SPAM Diretto: caccia al Relay!

Received: from inetsrv.dsgroup.it ([212.17.198.157])
by mtiwgwc24.worldnet.att.net
(InterMail vM.4.01.03.10 201-229-121-110) with ESMTP
id <XAQE1167.worldnet.att.net@inetsrv.dsgroup.it>;
Fri, 27 Oct 2000 16:37:55 +0000
Received: from come.to (pppa66-resalenashville2-4r7232.saturn.bbn.com [4.54.209.159]) by inetsrv.dsgroup.it with SMTP (Microsoft Exchange Internet Mail Service Version 5.5.2650.21)
id 4YPABXTW; Fri, 27 Oct 2000 18:40:03 +0200
Message-ID: <DtQaZ.+7f.I3s.RwzaE0J0ses-FL@come.to>

2 Received, esaminare il primo!

Il Relay e' nel campo "by"

L'origine e' nel campo "from"

... e se il Relay e' il mio MTA?

- siete sicuri che la configurazione e' OK?
- prima di tutto, vediamo se e' davvero passato di qui...
- identificare dal Received l'ID del MTA
- identificare il mailer dichiarato, e' il mio?
- cercare nel log MTA traccia del messaggio

Received: from come.to (pppa66-resalenashville2-4r7232.saturn.bbn.com [4.54.209.159]) by inetsrv.dsgroup.it with SMTP (Microsoft Exchange Internet Mail Service Version 5.5.2650.21) id 4YPABXTW; Fri, 27 Oct 2000 18:40:03 +0200

Come si legge un Log?

- dipende dal formato del mailer (RTFM)
- vediamo sendmail...

grep 4YPABXTW /var/log/syslog

Fri, 27 Oct 2000 18:40:03 +0200 myhost sendmail[9897]: 4YPABXTW : from=<free_credit_card@gnl.cplaza.ne.jp>, size=2610, class=0, pri=32610, nrcpts=1, msgid=< DtQaZ.+7f.I3s.RwzaE0J0ses-FL@come.to > bodytype=8BITMIME, proto=ESMTP, relay=smtp2.libero.it [193.70.192.52]

Ma non c’e’ nel Log!

- siete probabilmente innocenti...
- eravate un Open Relay nel passato?
- cerchiamo il vero Open Relay
- e’ il SECONDO Received ...
- ... e esiste almeno un TERZO Received!
- Ricostruire il path degli MTA
- ... e confrontalo con il “mail routing” da DNS !

Dove sono i colpevoli?

```
Return-Path: <free_credit_card@gnl.cplaza.ne.jp>
Received: from mail1.bbn.net ([218.18.12.167])
        by mtiwgwc24.worldnet.att.net
        (InterMail vM.4.01.03.10 201-229-121-110) with ESMTP
        id <XAQE11671.mtiwgwc24.worldnet.att.net@mail1.bbn.net>;
        Fri, 27 Oct 2000 16:37:55 +0000
Received: from inetsrv.dsgroup.it with ([4.54.209.159]) by mail1.bbn.net with
      SMTP id 3AS2XTW;  Fri, 27 Oct 2000 12:40:18 -0600
Received: from come.to (pppa66-resalenashville2-4r7232.saturn.bbn.com
      [4.54.209.159]) by inetsrv.dsgroup.it with SMTP id 4YPABXTW;
      Fri, 27 Oct 2000 18:40:03 +0200
Message-ID: <DtQaZ.+7f.I3s.RwzaE0J0ses-FL@come.to>
From: free_credit_card@gnl.cplaza.ne.jp <free_credit_card@gnl.cplaza.ne.jp>
To: free@india23.com <pinebeetle@att.net>
Subject: FREE Visa Gold Card (73487)
Date: Fri, 27 Oct 2000 11:35:48 -0400 (EDT)
```

Dove sono i colpevoli?

Received: from inetsrv.dsgroup.it with ([4.54.209.159]) by
mail1.bbn.net with SMTP id 3AS2XTW;
Fri, 27 Oct 2000 12:40:18 -0600

- dice che sono io (nome), ma l'IP NO!
- ma io non nessuna traccia nel log...
- ma che "routing" ha fatto il mail ??
- inetserv.dsgroup.it --> mail1.bbn.net --> att.net ?
- ... e... se fosse colpa di mail1.bbn.net ?!

Dove sono i colpevoli?

- inetserv.dsgroup.it --> mail1.bbn.net --> att.net ?
- il DNS (RR MX) e' impazzito?
- nslookup
  - set q=MX
  - att.net
- ma bbn.net non c'e' nelle risposte!
- ... ma E' IL COLPEVOLE !!

Faccio SPAM? Impossibile!

- ho il mio MTA configurato bene!
- tutti gli altri MTA sono ben configurati, o invisibili
- ed invece mi segnalano che messaggi passano dal mio MTA e sono SPAM
- sara' un "finto" Received !
- ... ma... ho il messaggio nel Log ...
- ... che succede ??

Faccio SPAM? Impossibile!

Return-Path: <free_credit_card@gnl.cplaza.ne.jp>
Received: from inetsrv.dsgroup.it ([212.17.198.157])
by mtiwgwc24.worldnet.att.net
(InterMail vM.4.01.03.10 201-229-121-110) with ESMTP
id <XAQE11671.mtiwgwc24.worldnet.att.net@inetsrv.dsgroup.it>;
Fri, 27 Oct 2000 16:37:55 +0000
Received: from rs23.dsgroup.it ([4.54.209.159]) by inetsrv.dsgroup.it with SMTP
(Microsoft Exchange Internet Mail Service Version 5.5.2650.21)
id 4YPABXTW; Fri, 27 Oct 2000 18:40:03 +0200
Message-ID: <DtQaZ.+7f.I3s.RwzaE0J0ses-FL@dsgroup.it>
From: free_credit_card@gnl.cplaza.ne.jp <free_credit_card@gnl.cplaza.ne.jp>
To: free@india23.com <pinebeetle@att.net>
Subject: FREE Visa Gold Card (73487)
Date: Fri, 27 Oct 2000 11:35:48 -0400 (EDT)

... mai pensato che hai uno spammer “in casa”?

Per proteggersi meglio

- MTA di frontiera configurati !
- MTA interni sorvegliati o filtrati!
- scansioni interne per identificare gli MTA !
- per difendersi dallo SPAM diretto, filtri (ORBS, black list, procmail, ...)
- educare gli utenti (Catene S. Antonio)

Conclusione

- e’ la maggior fonte di incidenti !!
- non sottovalutatelo!
- segnalare gli spammer “nazionali” se identificati (ma il CERT vi aiuta!) funziona !
- e’ la maggior causa di “tagli” da parte del CERT... pensateci!
- GRAZIE !