E-Mail Security

Francesco Palmieri
fpalmieri@unisa.it

Mail Spoofing

- Il protocollo SMTP è noto per essere inerentemente insicuro
- Tutte le funzioni di relay SMTP sono svolte da un daemon (Sendmail, Qmail, Postfix etc.) che aspetta connessioni sulla porta 25 per inviare la posta in uscita o ricevere posta in ingresso (tipiche funzioni MTA)
- Collegandosi tramite telnet in prova.it sulla porta 25 e digitando i comandi esatti, è possibile generare e-mail false
- Supponiamo che il nostro obiettivo è vittima@lamer.it a cui vogliamo recapitare una mail da parte di Bill_Gates@microsoft.com

```
$ telnet mail.unina.it 25
Trying 192.132.34.73...
Connected to mail.unina.it.
Escape character is '^]'.
220 smtp1.unina.it ESMTP Sendmail 8.14.4/8.14.4; Tue, 29 Sep 2015 09:44:14 +0200
```

Mail Spoofing

- Dopo esserci connessi a prova.it:25 dovremmo ottenere un messaggio del tipo:

```
220 prova.it ESMTP Sendmail 8.9.3/8.8.6; thu, 8 Jul 2006 11:46:01 +0000 (GMT)
```

- I comandi saranno:

```
HELO nomeprovider.it
```

- La risposta sarà:

```
250 prova.it Hello NOMEPROVIDER.IT, pleased to meet you
MAIL FROM: <Bill_Gates@microsoft.com>
RCPT TO: <vittima@lamer.it>
DATA
con il contenuto seguito da due righe vuote e da un punto


.
QUIT
221 2.0.0 prova.it closing connection
```

Mail Spoofing

Concettualmente è possibile seppellire la mail box di una potenziale vittima ponendo come mittente la vittima e destinatario un listserv

Un Listserv è un programma che invia programmi tramite e-mail nel caso non si riesca a prelevarlo via FTP.

Se ad esempio sappiamo che nella directory "mieifiles" del server pluto.it c'e` un file di 400 megabyte il cui nome è "enorme.gz" possiamo fare in modo che quei 400 MB vengano inviati sotto forma di testo nella e-mail della nostra vittima, ponendo nel campo SUBJECT quanto segue

```
REPLY vittima@lamer.it
CONNECT pluto.it anonymous indirizzo@falso.com
BINARY
GET mieifiles/enorme.gz
QUIT
```

Mail Spoofing: Analisi Headers

To: vern@ee.lbl.gov
Subject: RE: Russian spear phishing attack against .mil and .gov employees
From: jeffreyc@cia.gov
Date: Wed, 10 Feb 2010 19:51:47 +0100

Russian spear phishing attack against .mil and .gov employees

A "relatively large" number of U.S. government and military employees are being taken in by a spear phishing attack which delivers a variant of the Zeus trojan. The email address is spoofed to appear to be from the NSA or Intelink concerning a report by the National Intelligence Council named the "2020 Project". It's purpose is to collect passwords and obtain remote access to the infected hosts.

Security Update for Windows 2000/XP/Vista/7 (KB823988)

About this download: A security issue has been identified that could allow an attacker to remotely compromise a computer running Microsoft Windows and gain complete control over it. You can help protect your computer by installing this update from Microsoft. After you install this item, you may have to restart your computer.

Download:

http://mv.net.md/update/update.zip

“Headers” nel messaggio email

```
Delivery--Date: Wed Feb 10 10:51:55 2010
Received: from mailhost.icsi.berkeley.edu [192.150.186.11]
        by vpmini.icir.org with IMAP (fetchmail-6.3.11)
        for <vern@localhost> (single-drop); Wed, 10 Feb 2010 10:51:
Receiv                                                          .11) w
        for <vern@icsi.berkeley.edu>; Wed, 10 Feb 2010 10:51:50 -08
Received: from uw03.uniweb.no (uw03.uniweb.no [91.207.158.135])
        by ee.lbl.gov (8.14.4/8.14.4) with ESMTP id o1AIpmOf002895
        for <vern@ee.lbl.gov>; Wed, 10 Feb 2010 10:51:48 -0800 (PST
Authentication--Results: ee.lbl.gov; sender-id=softfail header.from=
Received: from w63697 by uw03.uniweb.no with local (Exim 4.66)
        (envelope--from <w63697@uw03.uniweb.no>)
        id 1NfHf9--0002n7--Md
        for vern@ee.lbl.gov; Wed, 10 Feb 2010 19:51:47 +0100
To: vern@ee.lbl.gov
Subject: RE: Russian spear phishing attack against .mil and .gov em
From: jeffreyc@cia.gov
Message--Id: <E1NfHf9--0002n7--Md@uw03.uniweb.no>
Date: Wed, 10 Feb 2010 19:51:47 +0100
Content--Length: 1116
```

Received: from mailhost.icsi.berkeley.edu [192.150.186.11]
by vpmini.icir.org with IMAP (fetchmail-6.3.11)
for <vern@localhost> (single-drop); Wed, 10 Feb 2010 10:51:
Received: from ee.lbl.gov (ee.lbl.gov [131.243.2.201])
by fruitcake.ICSI.Berkeley.EDU (8.12.11.20060614/8.12.11) w
for <vern@icsi.berkeley.edu>; Wed, 10 Feb 2010 10:51:50 -08
Received: from uw03.uniweb.no (uw03.uniweb.no [91.207.158.135]) by
ee.lbl.gov (8.14.4/8.14.4) with ESMTP id o1AIpmOf002895
for <vern@ee.lbl.gov>; Wed, 10 Feb 2010 10:51:48 -0800 (PST
Authenticati header.from=
Received: f 4.66)
(env
id
for +0100

I Tags To/Subject/From/etc. sono completamente sotto il controllo dell'attaccante

To: vern@ee.lbl.gov
Subject: RE: Russian spear phishing attack against .mil and .gov em
From: jeffreyc@cia.gov
Message--Id: <E1NfHf9--0002n7--Md@uw03.uniweb.no> Date:
Wed, 10 Feb 2010 19:51:47 +0100

X--Virus--Status: Clean
Content--Length: 1116

Received: from mailhost.icsi.berkeley.edu [192.150.186.11]
by vpmini.icir.org with IMAP (fetchmail-6.3.11)
for <vern@localhost> (single-drop); Wed, 10 Feb 2010 10:51:
Received: from ee.lbl.gov (ee.lbl.gov [131.243.2.201])
by fruitcake.ICSI.Berkeley.EDU (8.12.11.20060614/8.12.11) w
for <vern@icsi.berkeley.edu>; Wed, 10 Feb 2010 10:51:50 -08
Received: from uw03.uniweb.no (uw03.uniweb.no [91.207.158.135]) by
ee.lbl.gov (8.14.4/8.14.4) with ESMTP id o1AIpmOf002895
for <vern@ee.lbl.gov>; Wed, 10 Feb 2010 10:51:48 -0800 (PST
Authenticati header.from=
Received: f xim 4.66)
(env
id
for 7 +0100
To: vern@ee.lbl.gov
Subject: RE: Russian spear phishing attack against .mil and .gov em
From: jeffreyc@cia.gov
Message--Id: <E1NfHf9--0002n7--Md@uw03.uniweb.no> Date:
Wed, 10 Feb 2010 19:51:47 +0100
X--Virus--Status: Clean
Content--Length: 1116

Ogni header sotto di essi può anche essere sotto il controllo di chi attacca

```
Received: from mailhost.icsi.berkeley.edu [192.150.186.11]
        by vpmini.icir.org with IMAP (fetchmail-6.3.11)
        for <vern@localhost> (single-drop); Wed, 10 Feb 2010 10:51:
Received: from ee.lbl.gov (ee.lbl.gov [131.243.2.201])
                                                          2.11) w
                                                          :50 -08
Receive                                                   5])  by
                                                          895
                                                          00 (PST
Authenti                                                  from=
Received: from w63697 by uw03.uniweb.no with local (Exim 4.66)
        (envelope--from <w63697@uw03.uniweb.no>)
        id 1NfHf9--0002n7--Md
        for vern@ee.lbl.gov; Wed, 10 Feb 2010 19:51:47 +0100
To: vern@ee.lbl.gov
Subject: RE: Russian spear phishing attack against .mil and .gov em
From: jeffreyc@cia.gov
Message--Id: <E1NfHf9--0002n7--Md@uw03.uniweb.no> Date:
Wed, 10 Feb 2010 19:51:47 +0100
X--Virus--Status: Clean
Content--Length: 1116
```

Questo header ci informa circa il primo delivery “hop” nella catena dei relay.

Ipoteticamente fa riferimento a uw03.uniweb.no, ma non è certo…

Received: from mailhost.icsi.berkeley.edu [192.150.186.11]
by vpmini.icir.org with IMAP (fetchmail-6.3.11)
for <vern@localhost> (single-drop); Wed, 10 Feb 2010 10:51:
Received: from ee.lbl.gov (ee.lbl.gov [131.243.2.201])
by fruitcake.ICSI.Berkeley.EDU (8.12.11.20060614/8.12.11) w
for <vern@icsi.berkeley.edu>; Wed, 10 Feb 2010 10:51:50 -08
Received: from uw03.uniweb.no (uw03.uniweb.no [91.207.158.135]) by
ee.lbl.gov (8.14.4/8.14.4) with ESMTP id o1AIpmOf002895
for <vern@ee.lbl.gov>; Wed, 10 Feb 2010 10:51:48 -0800 (PST
Authentication-Results: ee.lbl.gov; sender-id=softfail header.from=

Gli headers per tutti gli hop successivi sono messi in testa

Received: from w63697 by uw03.uniweb.no with local (Exim 4.66)
(envelope-from <w63697@uw03.uniweb.no>)
id 1NfHf9-0002n7-Md
for vern@ee.lbl.gov; Wed, 10 Feb 2010 19:51:47 +0100
To: vern@ee.lbl.gov
Subject: RE: Russian spear phishing attack against .mil and .gov em
From: jeffreyc@cia.gov
Message-Id: <E1NfHf9-0002n7-Md@uw03.uniweb.no> Date:
Wed, 10 Feb 2010 19:51:47 +0100
X-Virus-Status: Clean
Content-Length: 1116

Delivery--Date: Wed Feb 10 10:51:55 2010
Received: from mailhost.icsi.berkeley.edu [192.150.186.11]
        by vpmini.icir.org with IMAP (fetchmail-6.3.11)
        for <vern@localhost> (single-drop); Wed, 10 Feb 2010 10:51:

        by fruitcake.ICSI.Berkeley.EDU (8.12.11.20060614/8.12.11) w
        for <vern@icsi.berkeley.edu>; Wed, 10 Feb 2010 10:51:50 -08

Questo header è l'host di partenza (vpmini.icir.org) indicante che il messaggio è stato ricevuto da mailhost.icsi.berkeley.edu.

Dato che mi fido del relay vpmini.icir.org, posso ragionevolmente credere che l'hop precedente sia stato realmente mailhost.icsi.berkeley.edu.

From: jeffreyc@cia.gov
Message--Id: <E1NfHf9--0002n7--Md@uw03.uniweb.no>
Date: Wed, 10 Feb 2010 19:51:47 +0100
X--Virus--Status: Clean
Content--Length: 1116

```
Delivery-Date: Wed Feb 10 10:51:55 2010
Received: from mailhost.icsi.berkeley.edu [192.150.186.11]
        by vpmini.icir.org with IMAP (fetchmail-6.3.11)
        for <vern@localhost> (single-drop); Wed, 10 Feb 2010 10:51:
Received: from ee.lbl.gov (ee.lbl.gov [131.243.2.201])
        by fruitcake.ICSI.Berkeley.EDU (8.12.11.20060614/8.12.11) w
        for <vern@icsi.berkeley.edu>; Wed, 10 Feb 2010 10:51:50 -08

        ee.lbl.gov (8.14.4/8.14.4) with ESMTP id o1AIpmOf002895
        for <vern@ee.lbl.gov>; Wed, 10 Feb 2010 10:51:48 -0800 (PST
Authentication-Results:  ee.lbl.gov;  sender-id=softfail  header.from=
R
To
Su                                                              em
Fr
Me
Da
X-
X-Virus-Status: Clean
Content-Length: 1116
```

mailhost.icsi.berkeley.edu è integrato con fruitcake.icsi.berkeley.edu (questo è il motivo per cui il nome differisce nell'header).

Potendo fidarmi di questo relay, mi fiderò anche dell'header Received che mi dice che il precedente hop è ee.lbl.gov (di cui posso fidarmi lo stesso).

```
Delivery--Date: Wed Feb 10 10:51:55 2010
Received: from mailhost.icsi.berkeley.edu [192.150.186.11]
        by vpmini.icir.org with IMAP (fetchmail-6.3.11)
        for <vern@localhost> (single-drop); Wed, 10 Feb 2010 10:51:
Received: from ee.lbl.gov (ee.lbl.gov [131.243.2.201])
        by fruitcake.ICSI.Berkeley.EDU (8.12.11.20060614/8.12.11) w
        for <vern@icsi.berkeley.edu>; Wed, 10 Feb 2010 10:51:50 -08
Received: from uw03.uniweb.no (uw03.uniweb.no [91.207.158.135])  by
        ee.lbl.gov (8.14.4/8.14.4) with ESMTP id o1AIpmOf002895
        for <vern@ee.lbl.gov>; Wed, 10 Feb 2010 10:51:48 -0800 (PST

Received: from w63697 by uw03.uniweb.no with local (Exim 4.66)
        (envelope--from <w63697@uw03.uniweb.no>)
To:
Subj                                                        .gov em
Fron
Mess
Date
X--V
X--Virus--Status: Clean
Content--Length: 1116
```

ee.lbl.gov dice che il messaggio proviene da uw03.uniweb.no.

Posso fidarmi di questa informazione, ma **non** di questo host. Conseguentemente qualsiasi informazione da questo punto in poi è inaffidabile.

Delivery--Date: Wed Feb 10 10:51:55 2010
Received: from mailhost.icsi.berkeley.edu [192.150.186.11]
by vpmini.icir.org with IMAP (fetchmail-6.3.11)
for <vern@localhost> (single-drop); Wed, 10 Feb 2010 10:51:
Received: from ee.lbl.gov (ee.lbl.gov [131.243.2.201])

In ogni caso ho imparato che il messaggio è stato inviato da una macchina in Norvegia, dove verosimilmente il destinatario non ha un mail server

Authentication--Results: ee.lbl.gov; sender-id=softfail header.from=
Received: from w63697 by uw03.uniweb.no with local (Exim 4.66)
(envelope--from <w63697@uw03.uniweb.no>)
id 1NfHf9--0002n7--Md
for vern@ee.lbl.gov; Wed, 10 Feb 2010 19:51:47 +0100
To: vern@ee.lbl.gov
Subject: RE: Russian spear phishing attack against .mil and .gov em
From: jeffreyc@cia.gov
Message--Id: <E1NfHf9--0002n7--Md@uw03.uniweb.no>
Date: Wed, 10 Feb 2010 19:51:47 +0100
X--Virus--Status: Clean
Content--Length: 1116

E-Mail Spamming

Spiced Pork Ham. Carne in scatola dei soldati americani nel dopo guerra

Monty Python

Le Origini

- Fino ai primi anni ‘90, la posta elettronica indesiderata consisteva nei messaggi delle cosiddette “catene di Sant’ Antonio”
  - In pratica non veniva fatto alcun tentativo per falsificare la provenienza dei messaggi, che venivano inviati ai destinatari direttamente dal server SMTP del loro mittente
- Secondo molti, la data d’ inizio dello spamming commerciale è il 1994, in cui avvenne la diffusione del famoso messaggio “Green-card laywers” degli avvocati Lawrence Canter e Martha Siegel, che più tardi divennero i primi esperti di Internet marketing
  - Il messaggio annunciava ai riceventi la fine della lotteria annuale per avere la Green Card, il permesso di soggiorno permanente negli Stati Uniti

Le Origini

- Tecnicamente, la novità del "Green-card laywers" stava nell'utilizzo di un programma per l'invio sistematico del messaggio a centinaia di gruppi Usenet e non nella dissimulazione del MTA mittente
  - Quest'ultimo obiettivo venne raggiunto l'anno successivo da Jeff Slaton, che divenne in breve il primo re dello spam, "**the Spam King**"
  - Nella sua più che decennale attività di spammer, Slaton ha affermato di poter raggiungere fino a 8 milioni di persone i cui indirizzi erano entrati in suo possesso grazie alla raccolta su Usenet

Definizioni

- **spam**: I mail che gli utenti non sono interessati a ricevere
- **UCE**: Unsolicited Commercial Email
- **UBE**: Unsolicited Bulk Email
- **ham**: I mail buoni (nel senso non spam)
- **Falsi Positivi**. Mail di tipo ham che vengono identificati come spam
- **Falsi Negativi**. Spam che non viene identificato dall'anti-spam e che quindi si mescola ai mail buoni.

Problema

- Tipico problema di separazione Segnale Rumore (S/N)
- Gli utenti sanno distinguere benissimo lo spam dall'ham
- Tuttavia questo task costa tempo e frustrazione agli utenti
- I programmi che trattano la posta devono aiutare gli utenti a gestire in modo automatico la maggior parte dello spam

Dimensioni problema

- La quantità di spam ricevuti dipende dalla anzianità di esposizione dell'indirizzo e-mailvittima su internet e dalla diffusione dello stesso (su siti web, su usenet news)
- Va considerate che a partire dal 2004 gli spam abbiano superato la posta legittima.
- Il trend è in continuo aumento
- Le grosse istituzioni sono le più colpite

Impatto dello spam

- Osterman Research inc.
  - Tempo speso dall'utente
    - Protetto 80 minuti ogni 1000 email (2.4 giorni/anno)
    - Non protetto 200 minuti/100 email (6.1 giorni/anno)
  - 46% di utenti hanno perso o non notato un mail buono a causa dello spam
  - 21% di utenti non sa se questo gli è successo
  - Gestione falsi positivi
  - Impatto sui sistemisti
    - 8.7 persone/ora ogni settimana per ogni mille mail per gestire lo spam oppure 1 FTE ogni 4600 utenti.
    - Da 0 ore/settimana in su, per chi non lo gestisce (e molte lamentele)

MUA o MTA?

- Lotta a livello di client

  + ottimi risultati

  + ogni utente ha un filtro personalizzato

  - non va bene quando l'utente usa client diversi

  - usano solo sistemi statistici o euristici

  - molti utenti chiedono semplicemente di non ricevere gli spam

Server side

- Lotta a livello di server
  + Si possono usare altri metodi
  + Una sola persona esperta combatte lo spam a vantaggio di tutti
  - Quello che sembra spam ad uno invece interessa ad un altro
  - Difficile da personalizzare

Open Relay

- Oltre a cercare di camuffare gli header attraverso sistemi mal configurati gli spammer molto spesso usano la tecnica indicata come ***3rd party relay***, cioè utilizzano il server di un terzo soggetto (che solitamente non ha alcun legame ne con il mittente ne con il destinatario), come relayer, ossia come propagatore di un messaggio SMTP.
- Un relay aperto viene individuato dagli spammer attraverso degli appositi programmi che in automatico cercano sulla rete: è solo questione di tempo e un server in quella condizione diventa ben presto una sorta di buco nero da cui può arrivare di tutto.
- Ecco perché quando ci si accorge che uno dei propri server è abilitato a fare da **relayer** lo si deve disconnettere dalla rete, fino a quando non si risolve il problema di configurazione.

.

Spam Botnets

- In mancanza di open relay, i bot agennts all'interno di una botnet possono essere usati per lanciare campagne di SPAM connettendosi direttamente alla porta 25 degli MX hosts di destinazione
- Per prevenire questo fenomeno è possibile agire a livello di controllo bloccando tutto il generico traffico uscente verso la porta 25 ed autorizzando solo in relay locale opportunamente configurato a far uscire tale traffico
- In questo modo l'unica alternativa possibile per inviare mail dall'interno di una rete è utilizzare il local relay che però sarà equipaggiato con opportuni controlli anti-spam per bloccare tale attività

Come gestire lo spam

- I server mail devono consegnare la posta elettronica quando l'hanno ricevuta (per correttezza verso il mittente ma ci dovrebbe anche essere un obbligo di legge)
- Non siamo obbligati ad accettare connessioni mail da siti "scorretti" che sono noti per generare spam
- Si possono modificare i mail aiutando gli utenti a capire se un mail contiene spam o virus ma il mail va comunque consegnato
- Gli utenti vanno aiutati nella preparazione di filtri per separare lo spam

Tecniche Antispam

- Black&white-listing, RBL
- Filtri di contenuti
- Sender Policy Framework
- DKIM
- Graylisting
- User training

Black&white-listing e RBL

- Sono controlli effettuati sul contenuto degli header dei messaggi, non sul body
- Il mail server ricevente consulta una lista di indirizzi o server mittenti validi (white) o vietati (black) e sulla base di questi match il chiude la comunicazione con il mittente
- Il database può essere anche online e gestito da un fornitore di servizi antispam; solitamente si chiama allora **Realtime Blocking List**
- Gli RBLs si consultano solitamente utilizzando il protocollo DNS (query e response)
- Le RBL sono aggirabili usando “open relays” oppure computer compromessi da virus o “trojan horse”
- Spesso queste fonti illecite sono usate solo per pochi minuti, prima che una RBL riesca a identificarle e bloccarle

Nuovi RBL

- SURBL
  - Spam URI Realtime BlockList: Nuovo tipo di RBL
  - SURBL: blocca (identifica) i messaggi basandosi sui nomi di dominio nel body (di solito siti web)
  - Quindi non blocca gli spam mail server come la maggior parte delle RBL ma permette di bloccare messaggi basandosi sui domini di spammer che sono nel body del mail
  - 40-60% identificazione con quasi zero falsi positivi
  - Viene spesso usato insieme ai RBL convenzionali (esempio liste di open relays)
  - Esiste un plugin per SpamAssassin 2.63 (SpamCopURI)

DNSBL

- Una DNS-based Blackhole List (anche DNSBL) è una RBL è un mezzo attraverso il quale è possibile pubblicare una lista di indirizzi IP, in un apposito formato facilmente "interrogabile" tramite DNS
- Le DNSBL sono principalmente utilizzate per la pubblicazione di indirizzi IP legati in qualche modo a spammer.
- Gran parte dei mail server possono essere configurati per rifiutare o contrassegnare messaggi inviati da IP presenti in una DNSBL
- Per operare una DNSBL è necessario disporre di un nome a dominio da utilizzare per la stessa, un name server per il dominio e una lista di indirizzi da pubblicare.
- È possibile gestire una DNSBL utilizzando il popolare server DNS BIND. Tuttavia, BIND è inefficiente per zone che contengono un notevole numero di indirizzi, in particolar modo per DNSBL che listano interi blocchi di IP.

DNSBL

- Quando un server di posta elettronica riceve una connessione da un client:
  1. ottiene l'indirizzo IP del client e ne inverte i byte - ad esempio l'indirizzo IP 192.168.1.254 diventa 254.1.168.192;
  2. appone il dominio della DNSBL all'indirizzo IP invertito appena ricavato: 254.1.168.192.spammers.example.net;
  3. esegue una query DNS per l'host name così ottenuto (di tipo "A", ovvero da nome host a indirizzo IP): se la risposta ricevuta è un indirizzo IP il client è listato, in caso contrario riceve una risposta "NXDOMAIN" ("No such domain", ovvero "Dominio non trovato");
  4. nel caso in cui il client sia presente nella lista, se appositamente configurato, esegue una query DNS di tipo "TXT" (testo) per lo stesso nome host. La risposta, eventuale, contiene ulteriori informazioni sul listing.
  5. Il nome host ottenuto (254.1.168.192.spammers.example.net) è simile al nome host associato al record DNS inverso (reverse) per l'indirizzo IP, che in questo caso sarebbe 254.1.168.192.in-addr.arpa. Il dominio speciale in-addr.arpa viene sostituito con il dominio della DNSBL e la query non è di tipo "PTR" ma di tipo "A".
- Viene utilizzato uno standard non ufficiale per gli indirizzi IP di risposta associati ai client listati.
  - La quasi totalità delle DNSBL risponde con un indirizzo IP nel range assegnato al network di loopback 127.0.0.0/8.
  - L'indirizzo 127.0.0.2 indica che il client è genericamente listato. Altri indirizzi vengono utilizzati per specifici listing, ad esempio per open relay o proxy.

Filtri di contenuti

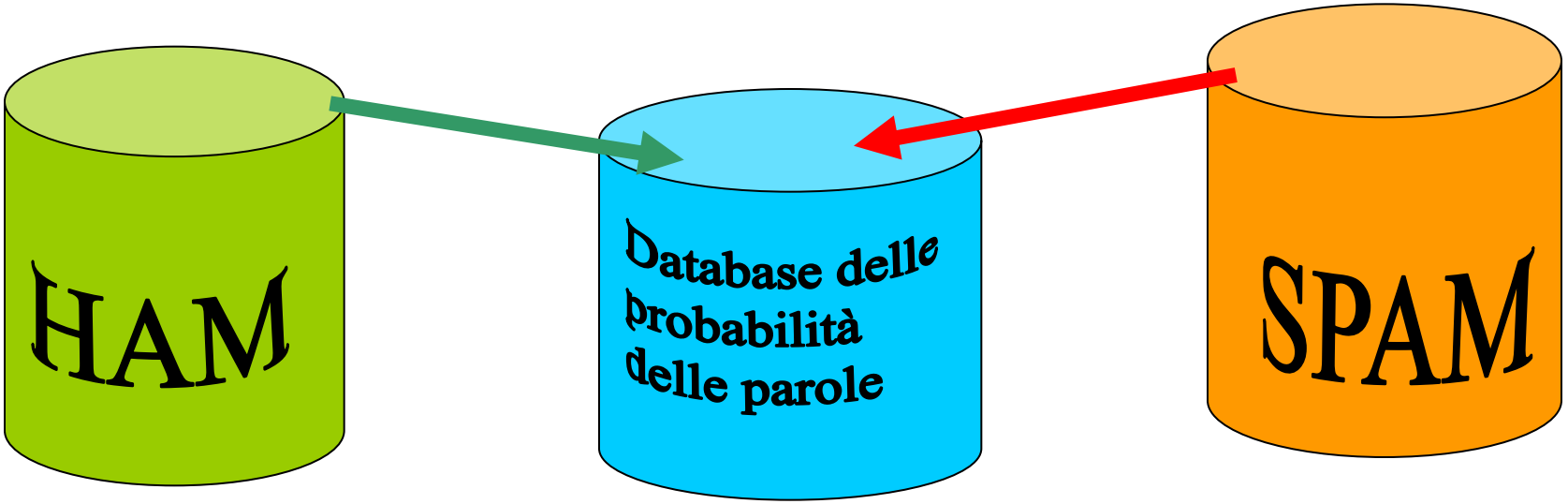
- Il sistema di posta, prima di consegnare la stessa agli utenti, applica vari algoritmi di analisi dei messaggi e misura, con varie metriche, un fattore di confidenza per classificare la email come *spam* o *ham*
- E' richiesto un training del sistema, che a volte deve essere effettuato dagli utenti stessi
- Attenzione agli aspetti legali: in Italia e in Germania per esempio non si può impedire agli utenti di ricevere lo spam in quanto tale azione verrebbe classificata come violazione della corrispondenza privata
- La mail classificata pertanto viene marcata come SPAM e il MUA la sposterà in una cartella speciale (es. SPAM o Quarantined) perché resti comunque a disposizione dell'utente

Filtri Bayesiani

- Teoria:
  - I filtri Bayesiani sono basati sul principio che molti eventi sono dipendenti e che la probabilità di un evento futuro si può dedurre dagli eventi passati
- Basi matematiche:
  - http://www-ccrma.stanford.edu/~jos/bayes/Bayesian_Parameter_Estimation.html
- Introduzione alle reti bayesiane:
  - http://www.niedermayer.ca/papers/bayesian/bayes.html
- Queste tecniche si possono usare per classificare lo spam. Se un pezzo di testo si trova spesso nello spam ma non in un ham, allora è ragionevole assumere che quel mail è spam

Come funziona?

- Dobbiamo crearci un Database con token (parole ma anche il simbolo $, indirizzi IP, domini etc…) raccolti da campioni di spam e ham



Calcolo *Probabilità di SPAM*

- Viene assegnato un valore di probabilità ad ogni token basato su calcoli che tengono conto di quanto spesso una parola si trova negli spam e negli ham.
- I token di entrambi gli insiemi sono analizzati per generare le probabilità che una parola sia spam
- Esempio:
  - "viagra" si trova 400 volte all'interno di 3000 mail di spam e 5 volte su 300 nei mail legittimi
  - La probabilità di spam è
  - 400/3000 diviso (5/300 + 400/3000) = 0,8889 → 89%

Formula

- T_S = numero dei mail di tipo SPAM
- N_S = numero di presenze di una parola tra gli SPAM
- T_H = numero dei mail di tipo HAM
- N_H = numero di presenza di una parola tra gli HAM
- P_S = probabilità che quella parola appaia in uno spam

$$P_S = (N_S/T_S) / (N_S/T_S + N_H/T_H)$$

- Se T_S e T_H sono uguali diventa

$$P_S = N_S / N_S+N_H$$

Creare il DB HAM

- Il database HAM deve replicare i mail buoni che desiderate ricevere. Una buona strategia potrebbe essere quella di usare come HAM i vostri mail in uscita (attenzione ai forward).
- Alcuni sw antispam arrivano con un db di HAM già pronto (Outlook, Exchange server) questo causa due problemi:
  1. Il database è pubblico e quindi gli spammer lo possono studiare e bypassare (vedi: www.mapilab.com/articles/outlook_spam_filter.html)
  2. Il DB di HAM è generale e non adattato al vostro solito traffico → è meno efficace e più esposto a falsi positivi.

Creare SPAM DB

- Deve includere un grande e variegato esempio di spam e deve essere costantemente aggiornato
- In questo modo il filtro è sempre a conoscenza degli ultimi trucchi degli spammer
- Usare un “troll address” o “spamtrap”

Come usiamo il DB

- Il fitro può essere usato sul DB delle probabilità
- Quando arriva un nuovo mail, questo viene “tokenizzato” e le parole più rilevanti (es le 15 con i valori più estremi) vengono scelte.
- Su questi token il filtro calcola la probabilità che il mail sia uno spam
- Si possono mettere soglie (es. Marca come spam se P almeno 90%)
- SpamAssassin invece assegna un punteggio ulteriore ad un mail secondo la probabilità

Euristici vs Bayesiani

- Tengono conto di tutto il messaggio
  - non vede solo le parole chiave tipiche dello spam ma anche quelle dei mail buoni. Considera solo le parole più interessanti che si discostano dalla media
- Si autoadatta
  - Si adatta nel tempo. Se lo spammer comincia a usare f.r.e.e. invece di free il filtro se ne accorge
  - Si adatta all'utente. (Es. Una facoltà di farmacia che studia il viagra)
  - Si adatta alla lingua: È intrinsicamente multi-lingua e internazionale mentre le liste di keyword sono spesse solo in inglese
- È difficile da imbrogliare.
  - Lo spammer deve usare meno parole utili (free, viagra, cash etc..) e più parole presenti nei mail validi (che sono però specifiche dell'utente).
  - Rompere le parole es. v-i-a-g-r-a è inutile perchè aumenta la probabilità che il messaggio venga identificato come spam dal momento che l'utente normale non userà mai quella forma.

Commenti

- I filtri bayesiani aiutano a separare il segnale dal rumore
- L'implementazione dentro è molto conservativa. Alcuni SPAM vengono visti con probabilita inferiore a 50% e quindi hanno punteggio aggiunto negativo
- I filtri invecchiano anche con l'autolearning: Es.
  - OK istruire il DB con gli spam con punteggio sopra il 10
  - Non OK istruire il DB con ham con score sotto 1
- Vogliamo trovare dei sistemi semi-automatici per continuare a istruirli
  - Per esempio Outgoing → HAM ; SpamTrap → SPAM?

Filtri ibridi: dspam

- http://www.nuclearelephant.com/projects/dspam/
  - I filtri antispam diventano sempre più complessi.
  - Gli spammer reagiscono con tecniche più sofisticate “obfuscation”, word list injection, sample flooding
  - Principio di base: Controllare la complessità e non aumentarla.
  - Altrimenti i filtri diventano troppo computing intensive, quindi non scalabili. Combattere lo spam costa più di gestirlo.

dspam

- Filtro Statistico Ibrido
  - Usa algoritmi per aumentare le capacità di identificazione concettuale dei filtri
  - Usa un insieme di feature ridotto (minori risorse)
  - Max 99.985% di identicazione (10 meglio di un umano)
  - Cerca di dare in pasto agli algoritmi attuali (Bayesiani, Chi quadro, etc) usando tecniche tipo: Chained Tokens, Inoculation Groups, Deobfuscation, Gruppi di classificazione e tecniche di riduzione rumore (Bayesian Noise Reduction)

DeObfuscation

Text Splitting:

Subject: Get your **F/R/E/E** 10 Day Supply **N/O/W!** Mime-Version: 1.0

Commenti HTML

Yes you he**<!lansing>**ard about th**<!crossbill>**ese weird **<!cottony>**little pil**<!domesday>** ls that are suppo**<!=anabel>**sed to make you bigger and of cou**<!chord>**rse you think they're b**<!soften>**ogus snake potion. Well, let's look

Diventa:

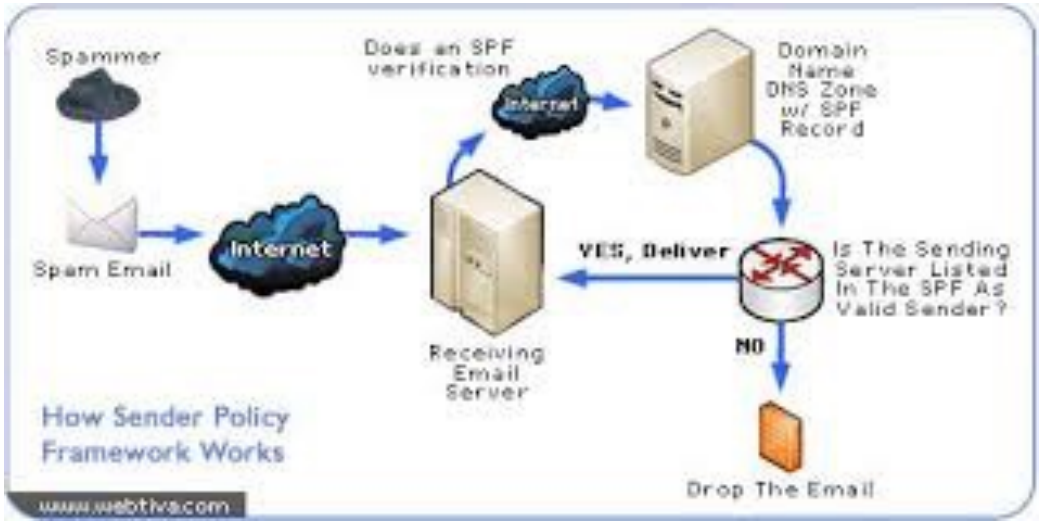
Yes you heard about these weird little pills that are supposed to make you bigger and of course you think they're bogus snake potion. Well, let's look

Sender Policy Framework (SPF)

- SMTP permette a chiunque di impersonare l'indirizzo email di chiunque altro.
- Molti spammer inventano indirizzi e-mail da usare esclusivamente per mandare spam. Alcuni mailer bloccano hotmail.com o aol.com a causa di questi indirizzi fasulli
- Sender Policy Framework (aka Sender Permitted From) cerca di impedire lo spam prima ancora che il messaggio venga spedito.
- SPF protegge dalle impersonificazioni. Come effetto collaterale ho meno spam, meno worm, meno virus. Obbliga gli spammer a mandare i mail dal loro dominio, in questo modo li possiamo identificare meglio
- SPF in pratica protegge il return-path. Quando un worm o virus cerca di cambiare l'indirizzo nello spam una vittima innocente si becca il messaggio di bounce

Sender Policy Framework (SPF)

- Nasce da una recente (2002) idea di Paul Vixie, evolutasi in seguito con contributi di Microsoft, in Sender ID e infine (2006) in Sender Policy Framework (SPF)
- L'idea alla base di SPF è pubblicare record DNS corrispondenti ai server che possono inviare posta per un particolare dominio; sono duali dei record MX
- Il ricevente può così controllare se il server mittente risulta pubblicato sul DNS secondo le regole di SPF, e diversamente decidere di non accettare la posta in entrata



Sender Policy Framework (SPF)

- Le specifiche definiscono per SPF l'uso di un record TXT contenente testo formattato, per velocizzare l'adozione di SPF:

```
example.org. IN TXT "v=spf1 mx ptr -all"
```

- Vi sono invece state proposte per la creazione di un record apposito (RR 99, assegnato da IANA), che richiede perciò il supporto dei sistemi DNS in circolazione
- Un grave problema è che SPF di fatto impedisce l'email forwarding, meccanismo che dovrà essere modificato p.es. in forme di "remailing" (dove il sender cambia, diversamente dal forwarding)
- I grandi Provider (es. Google, Hotmail e MSN), hanno di recente pubblicato i loro record SPF.
- Tuttavia finché questo meccanismo non sarà adottato da TUTTI i domini mittenti di posta elettronica nessuno si azzarderà a implementare lo switch-off (rifiutare la posta se proviene da un server non pubblicato tra i record SPF per quel dominio mittente)

SPF non è

- Una soluzione pensata per lo spam.
  - L'obiettivo è fermare l'impersonificazione non lo spam
  - Non è un prodotto. Vuole diventare uno standard open, una estensione di SMTP
  - Non pensato per identificare lo username. Identifica solo il nome del dominio (per il momento)

SPF è

- La controparte naturale del recod MX
- Standard aperto, estensioni di SMTP
- Supportato da SpamAssassin, Sophos, Symantec, etc
- Utile contro virus e worms
- Soluzione permanente, non richiede manutenzione o update di filtri.
- È progettato per proteggere il return-path. Con un pò di lavoro e complessità può proteggere anche il campo “From:”

Problemi di SPF

- SPF resolve un problema ma ne crea due nuovi:
  - forwarding e mail generate da web non funzionano più
- Ci sono contromisure per questo.
  - Trasparenti agli utenti e che riguardano solo gli amministratori.
- La soluzione di chiama SRS (Sender Rewriting Scheme)
- Anche chi usa “.forward” e “/etc/aliases” deve passare ad un MTA SRS-enabled
- Tema controverso tra gli esperti e in IETF

Esempio SPF

- Bob possiede il dominio example.net.
- Bob spesso invia mail attraverso il suo account GMail e contatta il support tecnico di GMail pre identificare il record SPF corretto per GMail.
- Dato che spesso gli ritornano indietro notifiche relative a messaggi che non ha mai inviato, decide di pubblicare un record SPF per prevenire abusi relative al suo dominio :

```
example.net  TXT  "v=spf1 mx
a:pluto.example.net
include:aspmx.googlemail.com -all"
```

Esempio SPF

example.net TXT "v=spf1 mx a:pluto.example.net include:aspmx.googlemail.com -all"

SPF record items	*explanation*
v=spf1	SPF version 1
mx	I server SMTP in ingresso (MXes) del doninio sono autorizzati a inviare mail anche per example.net
a:pluto.example.net	Amche l'host pluto.example.net è autorizzato
include:aspmx.googlemail.com	Qualsiasi cosa considetata legittima da gmail.com è legittima per example.net
-all	Qualunque altro host non è autorizzato

Controlli IP-dominio

- I mail servers (e.g. Gmail) contattati dai vari clients possono semplicemente verificare l'IP del client rispetto al dominio del sender: in mancanza di corrispondenza il messaggio è rigettato

```
<XXXX.YYYY@gmail.com>: host gmail-smtp-
in.l.google.com[173.194.78.26]
    said: 550-5.7.1 [aa.bb.cc.dd] The IP you're using to send mail
is not
    authorized to 550-5.7.1 send email directly to our servers.
Please use the
    SMTP relay at your 550-5.7.1 service provider instead. Learn
more at 550
    5.7.1
http://support.google.com/mail/bin/answer.py?answer=10336
    fl4si3665795wib.12 - gsmtp (in reply to end of DATA command)
```

DomainKeys Identified Mail (DKIM)

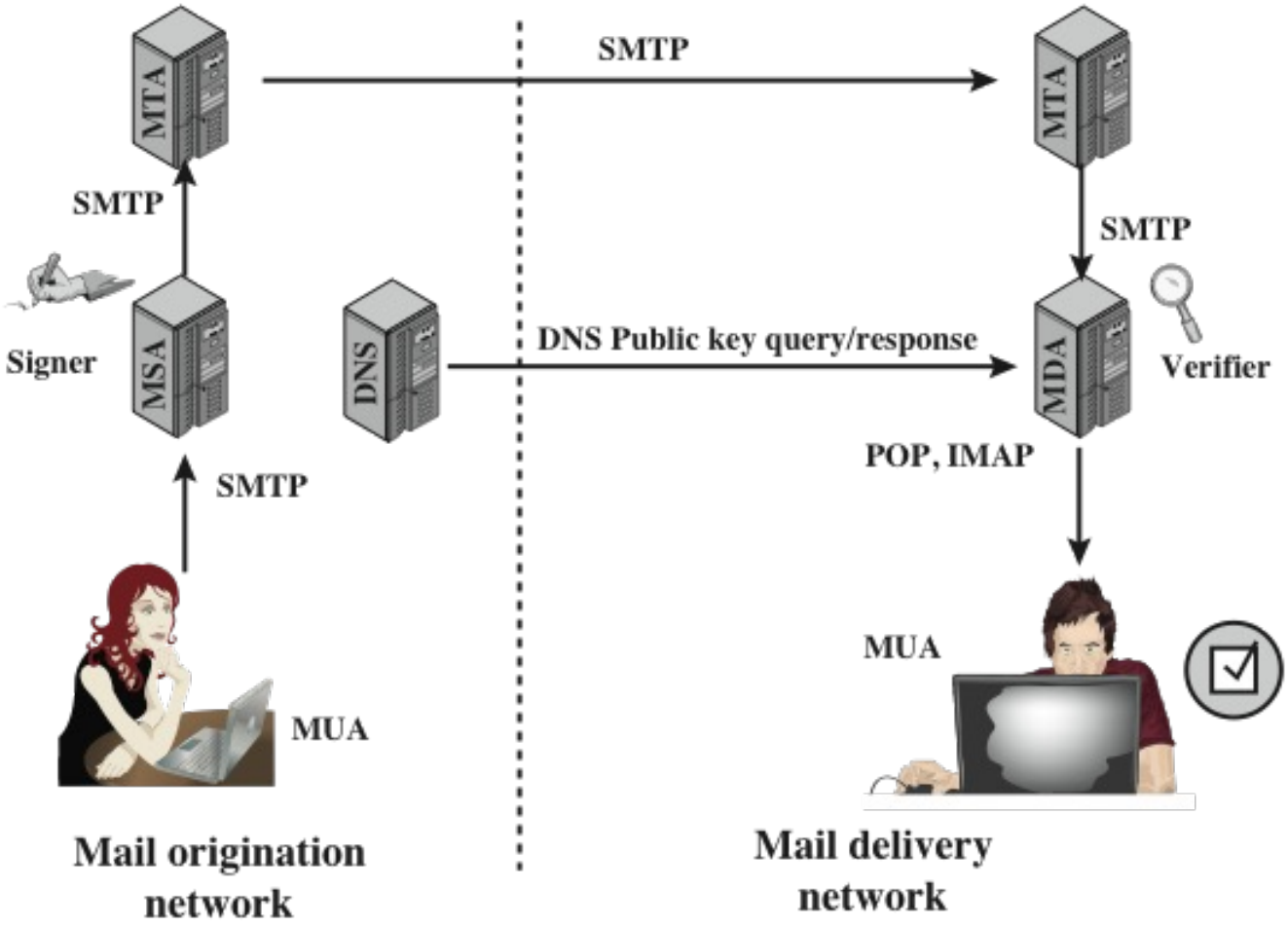
- DomainKeys Identified Mail (DKIM) è un metodo di autenticazione delle email, realizzato per prevenire lo spoofing.
  - Consente, a chi riceve un'email, di verificare la provenienza del messaggio, in modo da accertarsi dell'autenticità del mittente.
  - Il DKIM è utilizzato per contrastare il phishing e lo spamming

- In termini tecnici, il DKIM consente a un dominio di associare il proprio nome a un'email mediante l'apposizione di una firma digitale.
  - La verifica viene eseguita utilizzando la chiave pubblica del firmatario pubblicata nel DNS del dominio.
  - La firma garantisce che il messaggio non sia stato modificato dal momento in cui è stata apposta la firma
  - Di solito, le firme DKIM non sono visibili agli utenti poiché sono apposte nell'header e verificate dai service provider attraverso i mail server.
  - Per questo motivo, il DKIM differisce dalla crittografia end-to-end, la quale non prevede interazioni di terze parti.

DKIM

- I domini firmatari si attribuiscono la responsabilità per uno specifico messaggio.
- I soggetti riceventi (o gli agents che agiscono in loro vece) possono verificare la firma richiedendo direttamente al dominio del firmatario di ottenere l'opportuna chiave pubblica e quindi confermare che il messaggio è stato firmato da un soggetto in possesso di una chiave private associata al dominio firmatario
- DKIM è uno standard ufficialmente riconosciuto (RFC 4871: DomainKeys Identified Mail (DKIM) Signatures).
- DKIM è ampiamente utilizzato da fornitori di servizi e-mail, includendo agenize govarnative, grandi compagnie, gmail, yahoo, e molti Internet service providers (ISPs).

Scenario di uso DKIM



Trasformazione in forma canonica

- I server e-mail e i relay intermedi possono modificare la posta in transito, potenzialmente invalidando una firma
- Va garantito un formato standard
- Gli headers sono trasformati in forma canonica attraverso uno specifico algoritmo
  - relaxed (tollerante) or simple (stretto)
- Anche il corpo del messaggio è trasformato in forma canonica
  - Le scelte per header e corpo sono indipendenti (RFC 4871)

Selettori

- Per gestire multiple chiavi pubbliche concorrenti per dominio di firma si suddivide lo spazio delle chiavi usando I selettori
  - Per esempio un selettore può indicare i nomi di un ufficio, la data di firma o anche un singolo utente
- I selettiori permettono di implementare diversi scenari di uso:
  - Domini che vogliono delegare l'autorità di firma per un indirizzo specifico per un certo tempo a un determinate partner, ad esempio un provider o un organizzazione con funzioni di outsourcing
  - Domini che vogliono consentire a utenti che si spostano spesso di inviare messaggi localmente senza bosogno di connettersi a una particolare autorità di firma (MSA)
  - Domini con relazioni di "affinità" domains (e.g., associazioni di alumni) che consentono il forwarding della mail entrante ma che non supportano un servizio MSA per quella uscente

Esempio DKIM

a = Algoritmo di Hashing/firma

q = Algoritmo per ottenere la chiave pubblica

d = Dominio di firma

i = Identità del firmatario

s = Selettore

c = Algoritmo di trasformazione del messaggio in forma canonica

t = Data di firma (secondi da 1/1/1970)

x = Tempo di spirazione della validità

h = Lista di headers inclusi nella firma; implica l'uso di dkim-signature

b = La firma

bh = Hash del corpo del messaggio in forma canonica

```
Received: by mail-wg0-f44.google.com with SMTP id dr12so5400749wgb.35
        for <damore@dis.uniroma1.it>; Mon, 18 Mar 2013 14:17:04 -0700 (PDT)
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
        d=gmail.com; s=20120113;
        h=x-received:mime-version:in-reply-to:references:from:date:message-id
         :subject:to:content-type;
        bh=I7Gc1zNUyy13QDKdzeRoGrgVCJaaKCpVqUjIPSV24P8=;
        b=u1yT9znzpgvzRm4/hiXZKtrq77auuYbqT7HjzpKAL4siHsKKlCZNgElIiPXLHk6Y6l
         7daYBXnicBUiZLkU5jaoo/uK+IocGZNbCEJ0nC0A42mNxX4GkL84JiMNjXvdd4wMTvMF
         IUUgjQLk710OZYas9rCSMCkK48e8SeVbTFnAF42BhqF4rIXbHN/9PhlUy7AXuqnE1SSy
         BtRfS28eSlO7xjRR7Lkg+VHgsAIhMRn/SNVle1T09lXwWIJSXayjlPzQREb1DYQM8B6n
         xSuqSIwztkshtTd2BjC2JrORKXa+tUeTBZjA3vzDKiG7dMqEMJxMN9i2GN8VK2IiAR69
         Kkig==
```

Vouch by Reference

- VBR è un protocollo utilizzato nei sistemi di posta per la certificazione del mittente da parte di soggetti terzi.
- Certification providers indipendenti possono garantire per la reputazione dei mittenti verificando il nome del dominio che è associato con il relativo indirizzo
- Le informazioni VBR possono essere usate da un MTA, da un delivery agent o da un client di posta elettronica.
- Il protocollo è destinato a diventare uno standard per la certificazione e-mail del mittente descritto nella RFC 5518 .

Vouch by Reference

- Un utente di un servizio di certificazione e-mail VBR firma i suoi messaggi utilizzando DKIM e inserisce un campo *VBR-Info* nell'intestazione firmata.
- Il mittente può anche usare SPF per autenticare il proprio nome di dominio.
- L'header VBR-Info contiene:
  - il nome di dominio che sta certificando, tipicamente il dominio responsabile in una firma DKIM (d = tag),
  - il tipo di contenuto del messaggio,
  - un elenco di uno o più servizi di vouching, vale a dire i nomi di dominio dei providers che garantiscono sia per il mittente che per il tipo di contenuto:

```
VBR-Info: md=domain.name.example; mc=type;
mv=vouching.example:vouching2.example
```

Vouch by Reference

- Chi riceve una email può autenticare nome di dominio del messaggio utilizzando DKIM o SPF, individuando così i domini che sono responsabili per il messaggio.
- Successivamente ottiene il nome di un servizio vouching di cui si fida, sia tra il set fornito dal mittente o da un insieme configurato localmente di servizi vouching preferiti.
- Utilizzando il DNS, il ricevitore verifica se un servizio vouching garantisce per un dato dominio interrogando il DNS in cerca di un resource record di tipo TXT così composto:

```
domain.name.example._vouch.vouching.example
```

- Viene restituito, in caso positivo, un elenco SCII delimitato da spazi di tutti i tipi di garanzie che il servizio può fornire. Gli stessi devono devono corrispondere con quanto affermato nel messaggio.
  - I tipi definiti sono `transaction`, `list` e `all`.
- La verifica del messaggio permette di stabilire se il contenuto corrisponde.
- Il risultato della autenticazione può essere salvata in un nuovo campo di intestazione, secondo quanto previsto nella RFC 6212 , in questo modo:

```
Authentication-Results: receiver.example; vbr=pass
header.mv=vouching.example header.md=domain.name.example
```

Greylisting

- Nasce dal presupposto che la maggior parte del software creato per inviare spam non sia in grado di gestire i *deferrals* (errori SMTP 4xx)
- Per ogni incoming email viene composta la tripla:

  <sending IP, sender, recipient>

- Se questa risulta sconosciuta, viene aggiunta a una *graylist* e il mittente riceve un errore 4xx, con l'assunzione che questi riproverà l'invio più tardi
- Quando la stessa tripla si presenta successivamente, la email viene accettata e la tripla rimossa dalla *greylist* e inserita nella *whitelist*

Greylisting

- Al contrario dei filtri di contenuto questo meccanismo è molto leggero, perché rispondere con un errore 450 è immediato e non occupa risorse né di banda né di CPU
- Gli utenti non si accorgono di nulla tranne un certo delay nella ricezione del primo messaggio di un nuovo mittente, sia esso spam o posta legittima
- Mail server mittenti mal configurati possono comunque non gestire correttamente l'errore 450
- Prima o poi i software di spedizione dello spam implementeranno questo meccanismo, aggirandolo anche questa difesa

Greylisting

- http://projects.puremagic.com/greylisting/
  - Richiede che i mail da mittenti (numeri IP) non noti siano ritrasmessi dal client SMTP del loro ISP.
  - I mail da utenti noti sono passati aumaticamente
  - Molti SPAM arrivano via “open proxies” o altri meccanismi con MUA non standard.
  - Un MUA standard ritrasmette il mail dopo un rifiuto 4xx temporaneo (RFC2821 dice di ritrasmettere almeno 30 minuti dopo un failure
  - Gli SPAM attraverso open proxies e i worms non ritrasmettono
  - Richiede una versione modificata del server dcc
    - NB Il messaggio ritrasmesso deve essere identico all’originale per finire nella lista buona (oppure si usa “weak greylisting”)
    - Si può ignorare una parte dell’indirizzo IP del mittente per il greylisting per permettere ad utenti legittimi di cambiare client SMTP tra le ritrasmissioni

Greylisting - controindicazioni

- E’ compito del sistema mittente scegliere quando rimandare la posta, e può capitare che il ritardo sia eccessivo (molte ore)
  - ciò causa false segnalazioni di perdita di posta da parte degli utenti (es. se un mittente manda due messaggi arriva il secondo e dopo tempo arriva il primo)
- Se implementato, il graylisting deve quasi sempre operare come unico sistema antispam, e spesso non si può associare ad altri sistemi classificatori, se non perdendone parte delle funzionalità.
  - Questo è comunque un problema generale dei filtri di contenuti; per esempio, implementando un sistema antispam occorre rinunciare alla ridondanza sull’MX secondario
- Il greylisting usa le informazioni contenute negli header SMTP alla ricezione del messaggio:
  - questo momento dell’analisi non può che essere esclusivo
  - la decisione su che cosa fare di un messaggio in ingresso la può prendere un sistema solto e non ci possono essere 2 differenti “punti di ingresso” della posta

Tarpits

- Un mail server che risponde in modo patologicamente lento ad un client
  - Accetta i mail normalmente ma se pensa di essere contattato da uno spammer rallenta
  - Teergrube: Quando un server risponde intenzionalmente molto lento ai client. Postifix per esempio lo può fare (www.postifx.org/rate.html)
  - Oppure a livello TCP. Riduce la window size a zero ma continua a mandare l'ACK dei pacchetti, quindi tiene appeso il processo dello spammer a tempo indefinito. Usabile anche per assorbire attacchi di worms

Tarpit-Honeypot

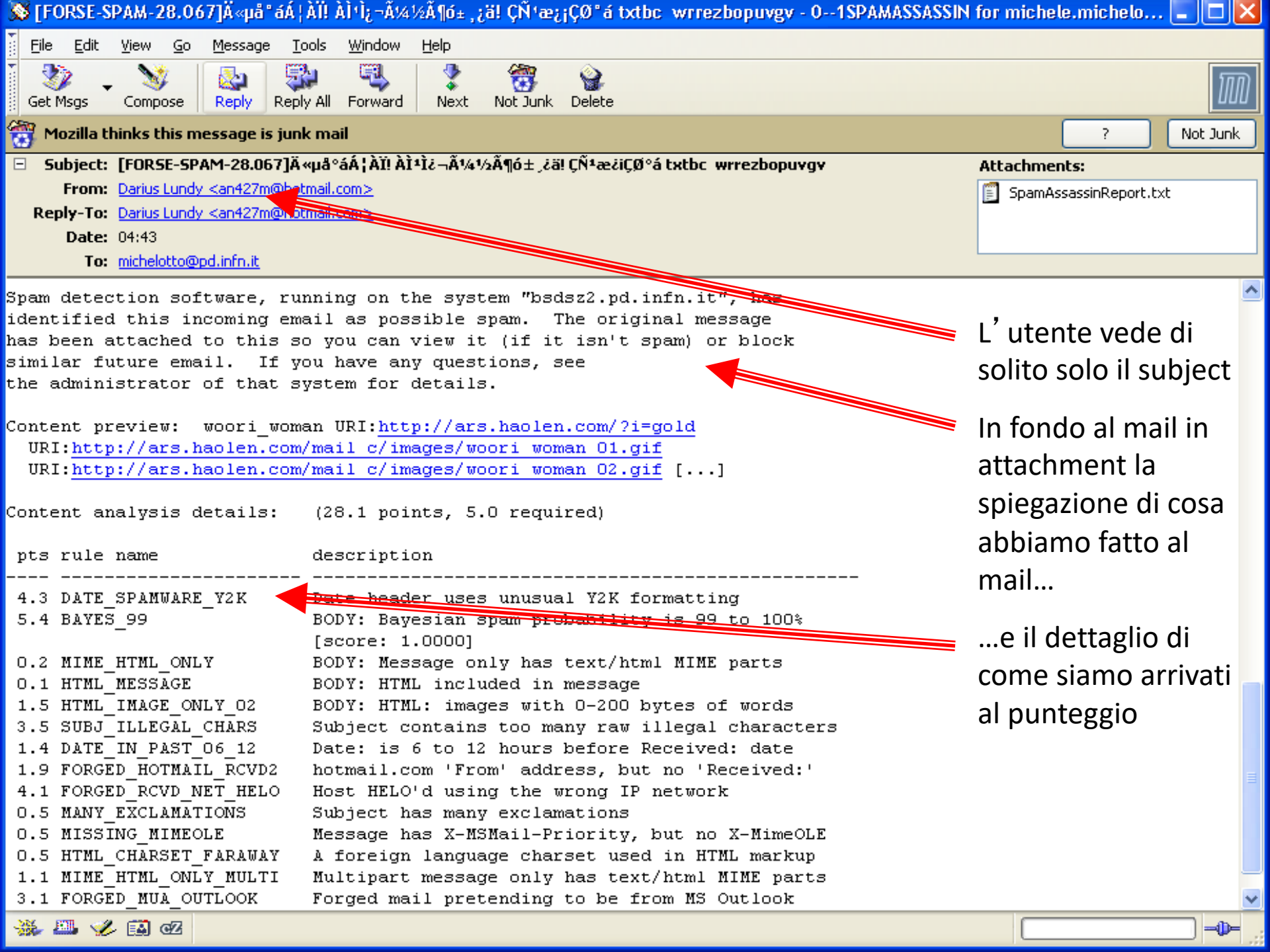
- Un altro tarpit imita un MTA con relay aperto.
  - Gli spammer che cercano sistemi con relay aperto cercano di mandare mail.
  - Il sistema semplicemente cancella questi tentativi di spam, oppure li sottomette a DNSBL (DNS Based Blackhole List) oppure li tiene per analizzarli.
  - Può anche lasciare passare qualche messaggio di tanto in tanto per simulare un vero relay

Challenge/Response

- Il mail server prima di consegnare il mail controlla se conosce il mittente
- Se ignoto chiede al mittente di passare alcuni test, se li passa il mittente viene “whitelistato”
  - Esempio. Leggere una parola nascosta in una immagine (magari un’immagine molto confusa)
  - Questi sistemi discriminano i non-vedenti o gli ipo-vedenti
  - Interagiscono molto male con le mailing list
  - Interagiscono molto male tra di loro (loop di C/R)
- Sistemi molto controversi

Spam Assassin

- Tool molto usato nel mondo open source
- Ogni mail viene confrontato con un insieme di regole e ogni regola aggiunge un punteggio di "*spam*" al mail
- Quando si raggiunge il punteggio di 5 il mail viene taggato come spam [FORSE-SPAM-N.mmm]
- Aggiungere nuove regole comporta il ribilanciamento del peso di quasi tutte le altre regole per evitare falsi positivi.
- Questo richiede un controllo di massa su un insieme enorme di mail e impedisce l'aggiornamento giornaliero delle signatures come nel caso degli antivirus (ci vogliono settimane)



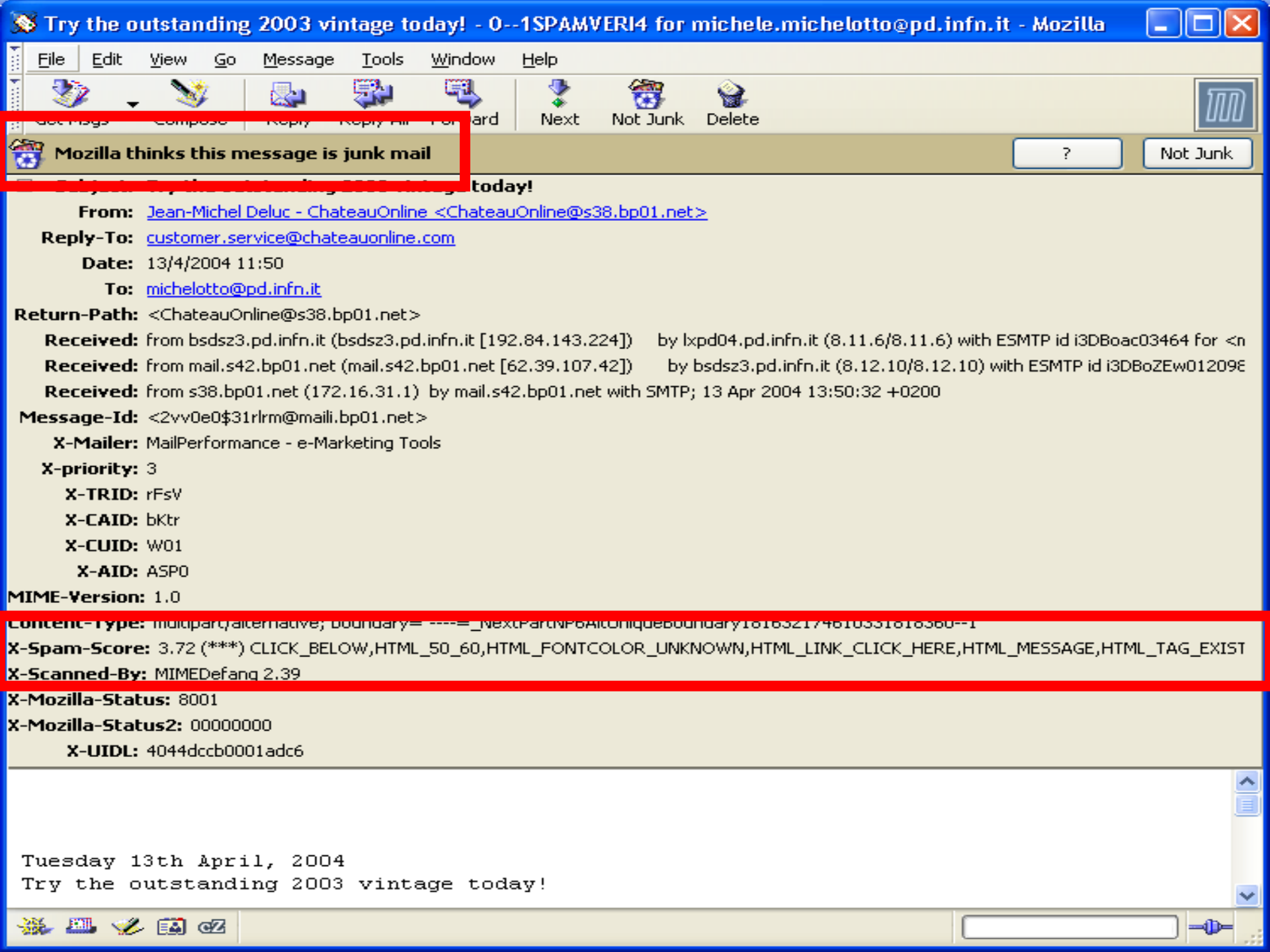
L'utente vede di solito solo il subject

In fondo al mail in attachment la spiegazione di cosa abbiamo fatto al mail…

…e il dettaglio di come siamo arrivati al punteggio

Campo X-Spam-Score

- Anche se il mail non supera la soglia viene inserito il punteggio nell'header nei campi opzionali
- Il campo X-Spam-Score viene usato da Mime-Defanger e di solito cancellato per mail sotto soglia.
- Lasciando questo campo si permette ad utenti evoluti di usare queste informazioni via procmail o con personalizzazioni dei filtri dei client
- Il campo risulta utile per capire per quale motivo lo spam non ha raggiunto il punteggio soglia:


Try the outstanding 2003 vintage today! - 0--1SPAMVERI4 for michele.michelotto@pd.infn.it - Mozilla
File Edit View Go Message Tools Window Help
Next Not Junk Delete
Mozilla thinks this message is junk mail
? Not Junk
today!
From: Jean-Michel Deluc - ChateauOnline <ChateauOnline@s38.bp01.net>
Reply-To: customer.service@chateauonline.com
Date: 13/4/2004 11:50
To: michelotto@pd.infn.it
Return-Path: <ChateauOnline@s38.bp01.net>
Received: from bsdsz3.pd.infn.it (bsdsz3.pd.infn.it [192.84.143.224]) by lxpd04.pd.infn.it (8.11.6/8.11.6) with ESMTP id i3DBoac03464 for <n
Received: from mail.s42.bp01.net (mail.s42.bp01.net [62.39.107.42]) by bsdsz3.pd.infn.it (8.12.10/8.12.10) with ESMTP id i3DBoZEw012098
Received: from s38.bp01.net (172.16.31.1) by mail.s42.bp01.net with SMTP; 13 Apr 2004 13:50:32 +0200
Message-Id: <2vv0e0$31rlrm@maili.bp01.net>
X-Mailer: MailPerformance - e-Marketing Tools
X-priority: 3
X-TRID: rFsV
X-CAID: bKtr
X-CUID: W01
X-AID: ASP0
MIME-Version: 1.0
X-Spam-Score: 3.72 (***) CLICK_BELOW,HTML_50_60,HTML_FONTCOLOR_UNKNOWN,HTML_LINK_CLICK_HERE,HTML_MESSAGE,HTML_TAG_EXIST
X-Scanned-By: MIMEDefang 2.39
X-Mozilla-Status: 8001
X-Mozilla-Status2: 00000000
X-UIDL: 4044dccb0001adc6
Tuesday 13th April, 2004
Try the outstanding 2003 vintage today!

Separare gli spam

- Una strategia utile:
  - Separare con i filtri i mail “borderline” con punteggio appena sopra il 5 (es fino a 7 oppure 8).
  - Cancellare con una rapida passata gli altri spam (es sopra 8)
  - Controllare per bene gli spam borderline per intercettare i falsi positivi

Spam difficili

- Le contromosse degli spammer
- Alcuni spam non sono UCE ma solo prove per vedere quali indirizzi sono buoni (quindi ricevono la posta) e quali fanno solo “bounce”
- Altro motivo per mandare spam senza senso potrebbe essere quello di “avvelenare” i filtri statistici

Gibberish

5.001 !!! Boderline spam

Contenuto utile per lo spammer

Contenuto “gibberish”: Tante parole (almeno 15) separate solo da uno spazio

Notare che altrimenti non sarebbe stato catturato dai bayesiani