JRES 2003

Filtrage de mail sur serveur de messagerie

Joe's j- chkmail

Jose- Marcio.Martins@ensmp.fr

Gladys.Huberman@ensmp.fr

Ecole des Mines de Paris

Plan

- Virus et Spam
- Les objetifs de notre filtre de messagerie
- Comment ajouter un filtre sur un serveur de messagerie
- Filtrage des vers de messagerie
- Filtrage de SPAM
- Résultats
- Sécurité
- Conclusions

Virus (vers de messagerie) et SPAM

Pourquoi filtrer les mails

- **Serveur de messagerie – passage obligé pour les messages *« indésirables »***

  - ✔ **Virus – vers de messagerie**
    - **ensmp.fr – 200/300 virus par jour – pics de 3000 lors de Blaster**
  - ✔ **SPAM**
    - **En semaine, environ entre un tiers et la moitié du trafic est constitué de SPAM et autres indésirables – jusqu'à trois quarts pendant le week- end**

- **Ma boîte aux lettres personnelle – 40 à 50 SPAMs par jour**

Objetifs du filtre

Objectifs du filtre

- Privilégier l'utilisation des fonctionnalités du serveur SMTP
- Rapidité du traitement
  - ✔ Capacité de traiter trafic important
  - ✔ Décision rapide – le plus tôt possible dans la connexion
  - ✔ Charge du filtre marginale par rapport aux autres fonctions du serveur
  - ✔ Meilleure résistance aux attaques
- Robustesse et résistance aux pannes
  - ✔ Filtre «increvable» - daemon de surveillance
  - ✔ Contrôle de charge – refus si le niveau des ressources est trop bas
- Observabilité
  - ✔ Logs riches, interrogation en ligne, statistiques, suivi graphique en temps réel, …
- Extensibilité
  - ✔ Ajout aisé de nouveaux modules.

Exemples de consultation de l'état du filtre

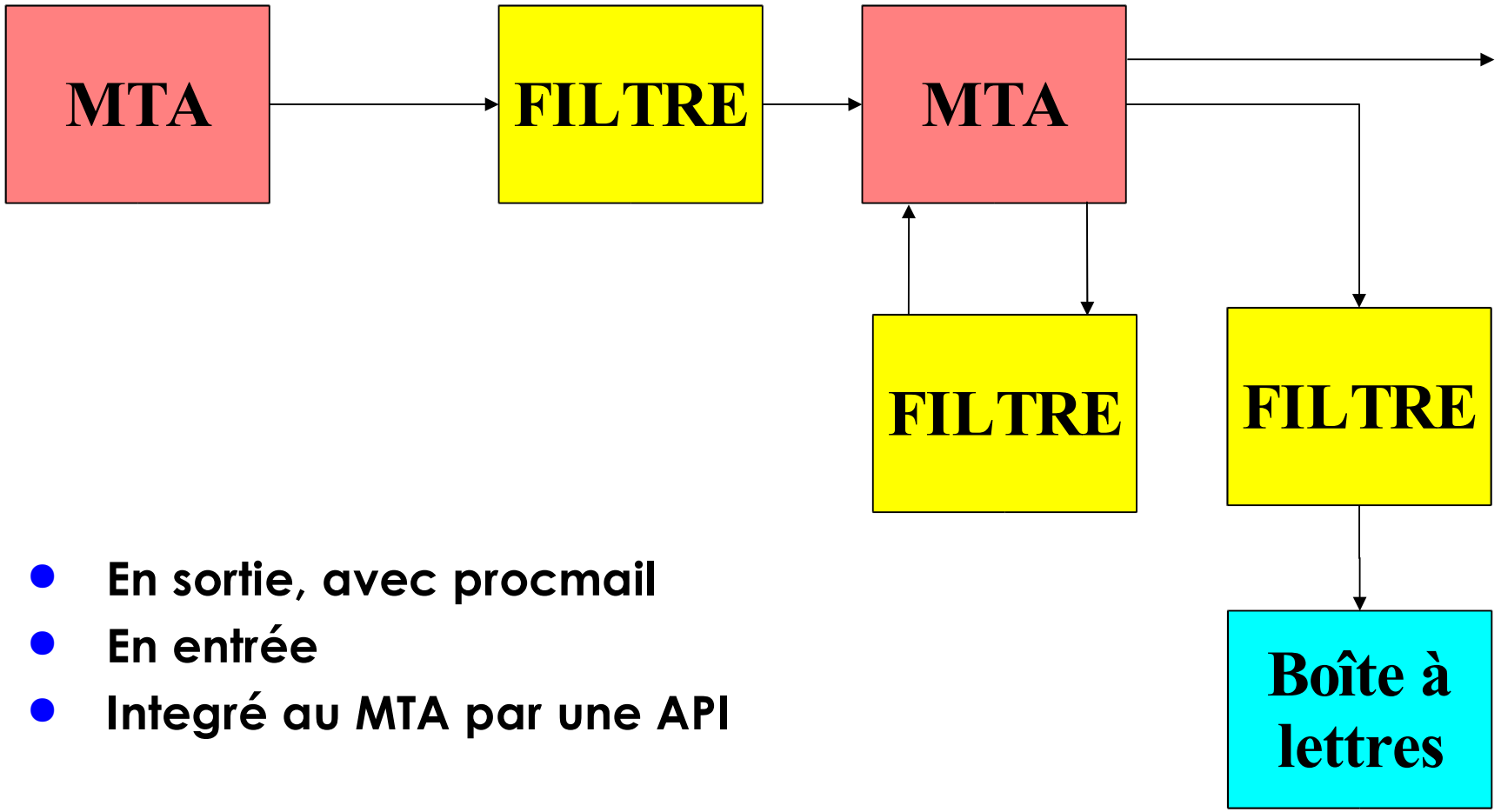
```
paris{root}: j-printstats -q -l 1d
*** TOTAL
 First Connection  : Thu Nov  6 10:52:13 2003
 Last Connection   : Fri Nov  7 10:52:11 2003
 Connections       :   24750
 Gateways          :    8945
 Throttle Max      :     374 / 10 min (for the server)
 Throttle Max      :     185 / 10 min (for a single gateway)
 Duration (sec)    :   0.020  15.494 7740.433 167.863 (min mean max std-dev)
 Work (sec)        :   0.000   0.027    1.906   0.069 (min mean max std-dev)
 Mean Throuput     :   1.879 KBytes/sec
Counts
 Messages          :   17314
 Empty Connections :       6
 Reject            :    3184
 Volume            :  737644 KBytes
 Mean Volume       :   41.61 KBytes/msg
 Recipients        :   24367
 Bad Recipients    :    4877
 Yield             :    0.70 msgs/connection
 Yield             :    0.98 rcpt/connection
 Files             :    2766
 X-Files           :     215
Reject
 DNS resolve       :     104
   FAIL            :      96
   FORGED          :       8
 Connection Rate   :     122
 Open Connections  :       8
 Empty Connections :       0
 Bad Recipients    :     401
 Content reject    :    2559
 Oracle reject     :    9483
 Rcpt reject       :       2
 Intranet User     :      26
```


```
martins@paris:~> j-printstats -q -l 1d -m c
Version                         : Joe's j-chkmail v1.4-031027

*** Connections flagged by content checking

. IP ADDRESS     : CONNECT    MSGS CONTENT  ORACLE : HOSTNAME
. 12.110.97.3    :       1       1       1       1 : exchange.splis.com
. 12.129.95.196  :       3       2       0       2 :
. 12.129.205.47  :       1       1       1       1 : mail3047.flowgo.com
. 12.129.205.55  :       1       1       1       1 : mail3055.flowgo.com
. 12.129.205.58  :       1       1       1       1 : mail3058.flowgo.com
. 12.129.205.60  :       3       2       1       2 : mail3060.flowgo.com
. 12.129.205.61  :       1       1       0       1 : mail3061.flowgo.com
. 12.129.205.62  :       1       1       1       1 : mail3062.flowgo.com
. 12.129.205.80  :       1       1       1       1 : mail3080.flowgo.com
. 12.147.201.3   :       1       1       0       1 :
. 12.167.170.95  :       1       1       1       1 : jpi-minn-170-95.dmisinetworks.com
. 12.175.224.231 :       1       1       1       1 : 12-175-224-231.dsl-cust.gwtc.net
. 12.203.220.106 :       1       1       1       1 : 12-203-220-106.client.attbi.com
. 12.203.244.229 :       1       1       1       1 : 12-203-244-229.client.attbi.com
. 12.206.81.219  :       2       1       1       1 : 12-206-81-219.client.attbi.com
. 12.206.221.74  :       1       1       0       1 : 12-206-221-74.client.attbi.com
. 12.207.18.229  :       1       1       0       1 : 12-207-18-229.client.attbi.com
. 12.207.232.246 :       1       1       1       1 : 12-207-232-246.client.attbi.com
. 12.208.216.54  :       1       1       1       1 : 12-208-216-54.client.attbi.com
. 12.209.161.165 :       1       1       1       1 : 12-209-161-165.client.attbi.com
. 12.210.160.68  :       1       1       1       1 : 12-210-160-68.client.attbi.com
. 12.210.175.137 :       1       1       1       1 : 12-210-175-137.client.attbi.com
. 12.211.245.22  :       1       1       0       1 : 12-211-245-22.client.attbi.com
...
martins@paris:~>
```

```
martins@paris:~> j-printstats -q -l 1d -m rb | head -40
Version                          : Joe's j-chkmail v1.4-031027

*** Rejected connections (clients harvesting addresses)

. IP ADDRESS      | CONNECT | BADRCPT |    REJETS   | HOSTNAME
. 12.217.68.110   |       3 |       7 |          2  | 12-217-68-110.client.mchsi.com
. 12.221.208.72   |       1 |       7 |          1  | 12-221-208-72.client.insightBB.com
. 12.240.129.219  |       2 |       7 |          2  | 12-240-129-219.client.attbi.com
. 12.252.103.25   |       3 |       7 |          2  | 12-252-103-25.client.attbi.com
. 24.0.33.63      |       1 |       5 |          1  | c-24-0-33-63.client.comcast.net
. 24.3.97.244     |       1 |       7 |          1  | c-24-3-97-244.client.comcast.net
. 24.27.100.30    |       2 |       3 |          2  | cs2427100-30.houston.rr.com
. 24.30.179.31    |       3 |       7 |          1  | cpe-24-30-179-31.socal.rr.com
. 24.34.3.78      |       1 |       8 |          1  | h0010b5534432.ne.client2.attbi.com
. 24.34.134.85    |       1 |       7 |          1  | h000c4122d164.ne.client2.attbi.com
. 24.62.133.187   |       2 |       8 |          1  | h00045a6c4aaf.ne.client2.attbi.com
. 24.88.5.19      |       4 |      15 |          3  | cae88-5-019.sc.rr.com
. 24.92.223.100   |       2 |       8 |          1  |
. 24.95.87.160    |       3 |       8 |          1  | dhcp9587160.columbus.rr.com
. 24.112.147.66   |       4 |       5 |          2  | R2Z3H3.cpe.net.cable.rogers.com
. 24.136.183.137  |       2 |      12 |          1  | user-0c8hds9.cable.mindspring.com
. 24.144.54.87    |       1 |       4 |          1  | dhcp54-87.cable.conwaycorp.net
. 24.147.41.178   |       3 |      13 |          1  | h0008a121a382.ne.client2.attbi.com
. 24.161.134.9    |       2 |      11 |          1  | cpe-24-161-134-9.hawaii.rr.com
. 24.168.254.191  |       2 |       7 |          1  | cae168-254-191.sc.rr.com
. 24.175.186.212  |       1 |       7 |          1  | cpe-24-175-186-212.stx.rr.com
. 24.184.97.55    |       7 |      17 |          5  | ool-18b86137.dyn.optonline.net
. 24.186.232.4    |       1 |       7 |          1  | ool-18bae804.dyn.optonline.net
. 24.189.4.30     |       1 |       9 |          1  | ool-18bd041e.dyn.optonline.net
. 24.194.189.227  |       4 |      13 |          2  | alb-24-194-189-227.nycap.rr.com
. 24.194.238.213  |       2 |      11 |          1  | alb-24-194-238-213.nycap.rr.com
...
```

```
martins@paris:~> j-printstats -q -l 1d -m x
Version                         : Joe's j-chkmail v1.4-031027

*** Gateways sending X-Files

. IP ADDRESS     : CONNECT  XFILES : HOSTNAME
. 12.234.86.73   :      18      17 : 12-234-86-73.client.attbi.com
. 24.239.153.83  :       1       1 : user-0cev6aj.cable.mindspring.com
. 62.26.116.129  :       6       4 : relay1.tiscali.de
. 62.62.156.27   :       7       2 : ioskeha.hittite.isp.9tel.net
. 62.62.156.28   :       4       1 : huva.hittite.isp.9tel.net
. 62.81.186.19   :       1       1 : smtp09.iddeo.es
. 62.106.58.121  :       1       1 :
. 62.106.65.34   :       2       1 : msg3.net-up.com
. 62.106.65.253  :       2       1 : ns2.net-up.com
. 62.147.58.106  :       7       1 : bordeaux-1-a7-62-147-58-106.dial.proxad.net
. 64.7.192.136   :       1       1 : smtp-01-003.root-mail.com
. 68.72.215.29   :       1       1 : adsl-68-72-215-29.dsl.akrnoh.ameritech.net
. 68.72.220.34   :       1       1 : adsl-68-72-220-34.dsl.akrnoh.ameritech.net
. 68.115.120.164 :       6       1 : cpe-68-115-120-164.bft.sc.charter.com
. 80.9.65.253    :       1       1 : Mix-Dijon-117-2-253.w80-9.abo.wanadoo.fr
. 80.15.146.116  :       1       1 : AMontsouris-108-1-17-116.w80-15.abo.wanadoo.fr
. 80.201.174.126 :       2       2 : 126.174-201-80.adsl.skynet.be
. 81.49.199.10   :       2       1 : AFontenayssB-110-1-5-10.w81-49.abo.wanadoo.fr
. 81.64.252.35   :       1       1 : m35.net81-64-252.noos.fr
. 81.248.105.15  :       1       1 : AMarseille-107-1-26-15.w81-248.abo.wanadoo.fr
. 129.104.30.64  :      24       2 : x-mailer.polytechnique.fr
. 130.37.64.40   :      22       1 : sheba.geo.vu.nl
. 144.135.24.153 :       1       1 : mta05bw.bigpond.com
...
```

Comment ajouter un filtre sur un serveur de messagerie



- En sortie, avec procmail
- En entrée
- Integré au MTA par une API

Un “dialogue” SMTP

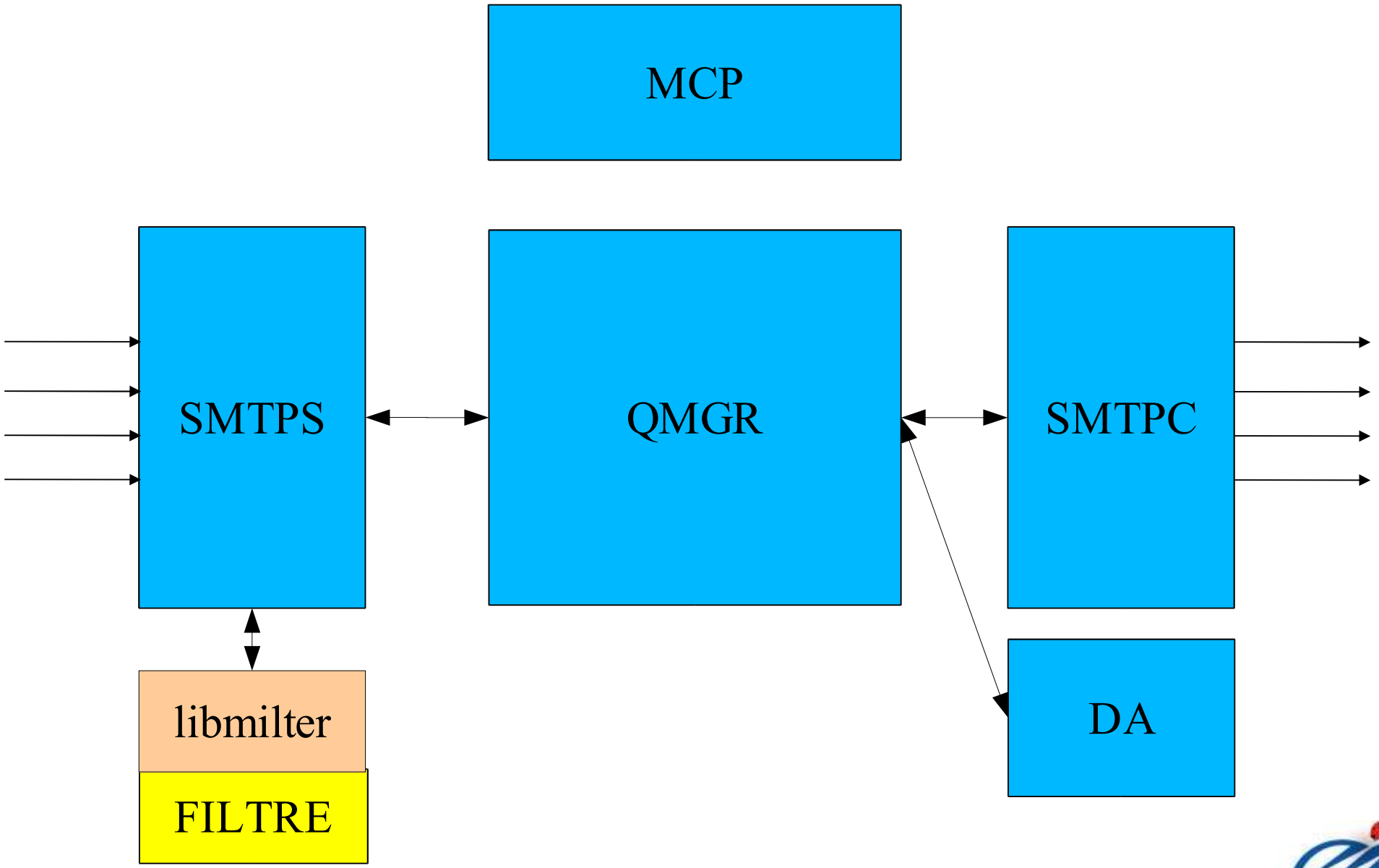
```
    martins@calloway:~> telnet paris smtp
     Trying 194.214.158.200...
     Connected to paris.
     Escape character is '^]'.
<-   220 paris.ensmp.fr ESMTP Sendmail 8.12.8/8.12.7/JMMC
->   helo calloway
<-   250 paris.ensmp.fr Hello calloway [194.214.158.171], pleased to meet you
->   mail from:joe@ensmp.fr
<-   250 2.1.0 joe@ensmp.fr... Sender ok
->   rcpt to:martins
<-   250 2.1.5 martins... Recipient ok
->   rcpt to:tartonpion
<-   550 5.1.1 tartonpion... User unknown
```

Enveloppe

```
->   data
<-   354 Enter mail, end with "." on a line by itself
->   From: Antoine
->   To: Joe
->   Subject: test telnet
->
->   C'est un test, je dis !
->   .
<-   250 2.0.0 h2QBmFBx017626 Message accepted for delivery
->   quit
<-   221 2.0.0 paris.ensmp.fr closing connection
     Connection to paris closed by foreign host.
    martins@calloway:~>
```

Corps

Sendmail 9



"Parenthèse" – Sendmail 9

- **Sendmail 8 – 10 ans de vie déjà...**
  - ✔ **Version 8.13 - dernière version avec des nouvelles fonctionnalités**
  - ✔ **Phase de maintenance jusqu'à la sortie de sendmail 9**

- **Sendmail 9 prendra la relève ...**
  - ✔ **Durée de vie souhaitée – 10 ans**
  - ✔ **Sécurité accrue**
  - ✔ **Fiabilité, robustesse**
  - ✔ **Modularité**
  - ✔ **Performance – 1000 connexions par seconde**

Le filtrage anti- viral

Principe

- **Détection des messages ayant des fichiers attachés pouvant contenir du code exécutable – « Unsafe Files »**

  http://support.microsoft.com/default.aspx?scid=kb;EN- US;q262631
  http://www.cknow.com/vtutor/vtextensions.htm

ade	adp	bas	bat	bin	btm	chm	cmd	com	cpl
crt	dll	drv	exe	hlp	hta	inf	ini	ins	isp
je	js	jse	lnk	mdb	mde	msc	msi	msp	mst
pcd	pif	reg	scr	sct	shb	shs	sys	url	vb
vbe	vbs	vxd	wsc	wsf	wsh				

Virus en circulation - Statistiques

1	W32/Sobig.F@mm	-	75,8 %
2	W32/Swen.A@mm	1	6,6 %
3	W32/Ganda.A@mm	2	3,3 %
4	W32/Bugbear.b@mm	1	1,5 %
5	Backdoor.Agobot.3.f	-	1,1 %
6	W32/Klez.h@mm	2	1,1 %
7	W32/Parite.B	-	1,0 %
8	W32/Bugbear.dam@mm	-	0,9 %
9	W32/MSBlast.A	1	0,8 %
10	W32/Lentin.F@mm	-	0,8 %
11	W32/Dumaru.A@mm	-	0,7 %
12	W32/Mimail.a@mm	2	0,6 %
13	W32/Sobig.B@mm	-	0,4 %
14	W32/Sobig.E@mm	2	0,4 %
15	W32/Sircam.worm@mm	-	0,4 %
16	W32/Nimda.E@mm	-	0,3 %
17	W32/Sobig.C@mm	-	0,2 %
18	W32/BugBear.A@mm	2	0,2 %
19	W32/Welchia	-	0,2 %
20	Backdoor.IRCBot.gen	-	0,2 %
21	BAT/Looper.F	-	0,2 %
22	W32/Sobig.A@mm	2	0,1 %
23	Trojan.JS.NoClose.e	-	0,1 %
24	W32/Elkern.C	-	0,1 %
25	W32/Lentin.H@mm	-	0,1 %
26	TrojanDownloader.Win32.Checkin.b	-	0,1 %
27	Worm.Randex.g	-	0,1 %
28	W32/FunLove.4070	-	0,1 %
29	TrojanDownloader.Win32.Swizzor.c	-	0,1 %
30	W32/Lirva.C@mm	-	0,1 %

Source :
http://www.f-secure.com

Le 30 Octobre2003

Résultats – Mai 2002

- Messages 420 000
- Messages avec des fichiers attachés 105 000
- Messages avec des «Unsafe Files» 4 233
  - exe 1431
  - bat 821
  - js 9
  - pif 995
  - com 54
  - scr 918
  - lnk 45
- 8 messages bloqués par erreur, dont 3 avec des « exe » et les autres 5 avec des « js » (cartes de voeux et programmes), soit 0,2 %

Une semaine avec Sobig

	02/09	03/09	04/09	05/09	06/09	07/09	08/09	TOTAL
* .bat	13	11	14	13	7	2	11	71
* .exe	51	62	43	29	19	30	47	281
* .mdb	0	0	0	1	0	2	0	3
* .pif	1277	1587	2812	2003	1284	1903	2420	13286
* .scr	187	245	346	264	154	227	341	1764
* .url	1	1	3	0	1	0	2	8
* .zip	21	16	16	17	7	6	24	107
TOTAL	1550	1922	3234	2327	1472	2170	2845	15520

Virus en quarantaine...

- W32/Sobig.f@MM 2844
- W32/Klez.eml 56
- W32/Sobig.dam 39
- W32/Dumaru.a@MM 30
- W32/Mimail@MM 24
- Exploit-MIME.gen.exe 9
- W32/Bugbear.b.dam 5
- W32/Bugbear.b@MM 4
- W32/Dumaru.h@MM 3
- W32/Hybris.gen@MM 3
- W32/Yaha.g@MM 1
- W32/Pate.b 1
- W32/Bugbear@MM 1

Avantages et Inconvénients

- Avantages
  - ✔ Rapidité du traitement – jusqu' à 200 fois plus rapide qu'un vrai antivirus
  - ✔ Pas besoin de fichiers de signatures
    - Pas de mises à jour
    - Nouveaux virus sont détectés tout de suite (Blaster, Sobig..)
  - ✔ Cas spécifiques : par exemple : RFC 2046
    - Fichiers découpés
    - Transmission de fichiers par référence

```
Content-Type: message/external-body; name=install.exe;
              site=hacker.com; mode=image;
              access-type=ANON-FTP; directory=pub
```

- Inconvénients
  - ✔ Transmission de fichiers exécutables – solution : modification de l' extension ou compression
  - ✔ Pas de détection des virus macro
  - ✔ Pas de détection des virus Macintosh
  - ✔ Pas d' identification immédiate des virus bloqués

Le filtrage de SPAM

Les méthodes anti- spam

- **Aujourd'hui**
  - ✔ RBL – Real- time Blacklist – liste de relais ouverts et adresses source de SPAM
  - ✔ Filtrage de contenu (pattern matching - URLs)
  - ✔ Empirique
    - Spam Assassin – environ 950 critères (+/- significatifs) pondérés
  - ✔ Statistique - Probabilité d'appartenance des mots à une classe SPAM/HAM
    - Bogofilter
    - SpamOracle (Inria – Xavier Leroy)
  - ✔ Autres méthodes...

- **Les méthodes de demain ???**
  - ✔ ASRG/IRTF (Internet Research Task Force)
    - Consent Framework – l'utilisateur défini ce qu'il veut bien recevoir
    - RMX – Reverse MX – Rendra plus difficile l'anonymat des messages

Problèmes des méthodes pondérés

- **Apprentissage**
  - ✔ **Répresentativité de l'échantillon SPAM/HAM**
    - **Répartition - 50/50, 20/80 ou 80/20 ???**
    - **Contenu – dépend de la population**
  - ✔ **Répresentativité spatiale**
    - **Population hétérogène**
  - ✔ **Répresentativité temporelle**
    - **Le spam change à chaque jour (avec plusieurs cycles - courts et longs)**
- **Tests *blanchisseurs* : PGP, mots savants parfois invisibles...**
- **Les spammeurs arrivent à contourner certains outils, grâce à la connaissance des méthodes employées**

Le filtrage de SPAM par j- chkmail

Buts recherchés

- **Efficacité**
  - ✔ **Le but à rechercher est plutôt qualitatif (confort des utilisateurs) que quantitatif**
- **Performance**
  - ✔ **Traitement rapide**
- **Sécurité**
  - ✔ **Le serveur de mail est une cible potentiel**

Filtrage pendant «enveloppe SMTP»

- **Mesure de cadence de connexion**
  - ✔ Trafic poissonien versus rafales
  - ✔ Mesure du nombre de connexions (par adresse IP) sur une fenêtre temporelle glissante de taille 10 minutes
  - ✔ Erreur 4xx (temporaire) en cas de dépassement
  - ✔ Attribution d'un quota, selon la confiance attribuée au client SMTP (local, ami, inconnu)
  - ✔ Actuellement plus utile pour protéger le serveur que pour éviter le SPAM

- **Résolution DNS de la passerelle**
  - ✔ Vérification de :
    - Existence de résolution DNS inverse
    - Cohérence des résolutions directe et inverse
  - ✔ Pb : un certain nombre de serveurs legitimes sans déclaration DNS correcte -> Solution : quota de connexions par jour ou liste blanche
  - ✔ Remarque : les solutions du type RMX, en cours d'étude à l'IRTF, ne seront utilisables que si avoir des déclarations DNS correctes devient une obligation pour les serveurs de mail.

Filtrage pendant «enveloppe SMTP»

- **Détection de collecte d'adresses (*harvest*)**
  - ✔ **Limitation du nombre d'erreurs d'adressage (*User Unknown*) sur une fenêtre temporelle glissante**

- **Historique des connexions – en cours**
  - ✔ **Blackliste dynamique en fonction des résultats précédents**
  - ✔ **Arrêter très tôt les connexions en provenance de clients ayant un historique d'envoi de spam**

Filtrage après réception message

- **Recherche d'expressions regulières**
  - ✔ **Exemple :**

```
BODY   50   http://[^ /]*targetincest.net
BODY   50   http://[^ /]*4you.(com|net|org|biz)
BODY   50   http://[^ /]*/host/default.asp\?id=
BODY    5   http://[^ /]*@
BODY   30   http://[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}
```

  - ✔ **Inconvénients**
    - **Trop long si beaucoup d'expressions régulières**
    - **Exige maintenance minimale – mais moins qu'on peut le penser**

- **"Oracle"**
  - ✔ **Une série de critères empiriques – actuellement 21**
    - **Entropie, partie texte codée en base 64...**
  - ✔ **Rechercher des critères objectifs représentatifs des SPAMs**
  - ✔ **Pas de critères «blanchisseurs» de spam**
  - ✔ **Détecte trois fois plus que la recherche d'expressions régulières**

- **Actions possibles : rejet, suppression, marquage par en- tête**

Résultats - performance

Performance - résultats

- Serveur ensmp.fr
  - ✔ Sun E280R – Solaris 9 – bi- processeur 2 x 900 Mhz
    - MX domaine ensmp.fr
    - DNS domaine ensmp.fr
  - ✔ Entre 30000 et 40000 connexions par jour
  - ✔ 1 Go transferé par jour
  - ✔ 1100 comptes locaux + redirection domaine
  - ✔ Charge CPU habituelle du filtre : < 1 %
  - ✔ Place mémoire occupée par le filtre : ~ 12 Mo
  - ✔ Temps moyen de traitement par connexion : ~ 50 ms

```
martins@paris:~> j-printstats -t
*** THROTTLE TABLE (units each 10 minutes) at Mon Nov  3 20:50:05 2003
*** CONNECTIONS :    210 / 10 min (3408 entries)

martins@paris:~> /bin/ps -p `pgrep -d, j-chkmail` -o pid,pcpu,pmem,vsz,...
  PID %CPU %MEM  VSZ  RSS    SZ   CLS NLWP PSR S COMMAND
20521  0.1  0.3 12880 12128 1610   TS   15   - S /usr/sbin/j-chkmail
20520  0.0  0.1  7648  1672  956   TS    1   - S /usr/sbin/j-chkmail
martins@paris:~>
```

```
paris{root}: j-printstats -q -l 1d
*** TOTAL
 First Connection  : Thu Nov  6 10:52:13 2003
 Last Connection   : Fri Nov  7 10:52:11 2003
 Connections       :   24750
 Gateways          :    8945
 Throttle Max      :     374 / 10 min (for the server)
 Throttle Max      :     185 / 10 min (for a single gateway)
 Duration (sec)    :   0.020  15.494 7740.433 167.863 (min mean max std-dev)
 Work (sec)        :   0.000   0.027    1.906   0.069 (min mean max std-dev)
 Mean Throuput     :   1.879 KBytes/sec
Counts
 Messages          :   17314
 Empty Connections :       6
 Reject            :    3184
 Volume            :  737644 KBytes
 Mean Volume       :   41.61 KBytes/msg
 Recipients        :   24367
 Bad Recipients    :    4877
 Yield             :    0.70 msgs/connection
 Yield             :    0.98 rcpt/connection
 Files             :    2766
 X-Files           :     215
Reject
 DNS resolve       :     104
   FAIL            :      96
   FORGED          :       8
 Connection Rate   :     122
 Open Connections  :       8
 Empty Connections :       0
 Bad Recipients    :     401
 Content reject    :    2559
 Oracle reject     :    9483
 Rcpt reject       :       2
 Intranet User     :      26
```


Sécurité – Protection du serveur

- Limitation de la cadence de connexions par client SMTP
- Limitation du nombre de connexions ouvertes en même temps par client SMTP
- Contrôle de charge et des ressources disponibles
  - ✔ Ressources = charge CPU, descripteurs de fichier disponibles, ...
    - Si niveau < N1, refus connexions venant de clients inconnus
    - Si niveau < N2 (N2 < N1), refus connexions
  - ✔ Implementation partielle
- Evaluation de la contribution de chaque client à la charge globale du serveur – en cours

Attaque – nombre de connexions ouvertes

tant que *vrai*

- démarre connexion &
- démarre connexion &
- Sleep 1

fin tant que

- Le filtre terminera lorsque tous les descripteurs de fichier seront occupés (16 erreurs consécutives).
- Sendmail refuse nouvelles connexions lorsque *MaxDaemonChildren* seront déjà actives

```
TELNET victim 25
WAIT OK
SEND HELO
WAIT OK
SEND MAIL FROM
WAIT OK
SEND RCPT TO
WAIT OK
SEND DATA
WAIT OK
tant que vrai
   SEND DUMMY LINE
   SLEEP some time
fin tant que
```

Attaque sur serveur ensmp.fr – avril 2003

- 10536 connexions en 8 minutes
- 238 clients du réseau 66.216.119.0/24 (rapiddealsbyemail.com)
- Connexions par client : [28 – 67]
- Pic : 86 connexions dans la même seconde (21:48:29)
- 15 messages refusés par le contenu, dans les 3 premières minutes

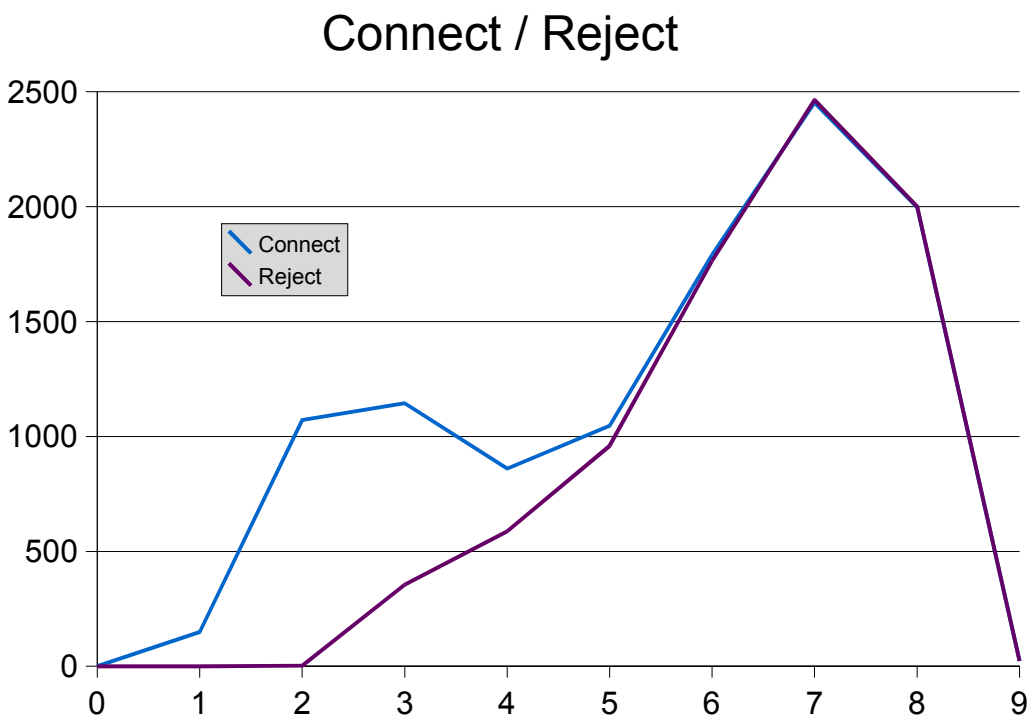
```
http://[^ /]*greatedeals.com
```

- 8156 connexions refusées par la mesure de cadence de connexion
- Les autres concernant des destinataires inconnus
- Aucun message légitime perdu pendant l'attaque !

Connexions/rejets en provenance de 66.216.119.0/24

(valeurs mesurées par le filter)

21h	Connexions	Rejets
40	0	0
41	149	0
42	1072	3
43	1145	355
44	860	587
45	1047	959
46	1790	1764
47	2452	2464
48	1998	2001
49	23	23



Conclusions

Conclusions

- **Outil de filtrage de mail performant**
- **En production sur quelques sites de taille importante (250000 messages par jour)**
- **Outil français, *open- source* mis à la disposition, en priorité, de la communauté enseignement/recherche, mais plus d'utilisateurs étrangers que français.**
- **En cours d'évolution – des nouvelles méthodes anti- spam à experimenter**