Analisi dei risultati di utilizzo di Antispam LIVE

IceWarp Server offre un servizio Antispam che si compone di diverse tecnologie e risulta altamente modellabile, consentendo ad ogni amministratore la ricerca di una situazione il quanto più possibile conforme alle necessità della propria installazione.
SpamAssassin, filtro Bayesiano, RBL, Greylisting, Razor2, SURBL, SPF, DKIM e filtri sul contenuto sono le principali funzionalità di cui si compone il servizio.
In questo articolo rendiamo pubblici i dati raccolti in occasione di un'analisi dell'utilizzo di Antispam con opzione LIVE su due differenti sistemi.

Prima di introdurre i risultati vorremmo però fornire qualche dettaglio sulle tecnologie prese in esame.

Antispam

Greylisting: questa funzionalità si occupa di rimandare l'accettazione di una sessione per un determinato periodo di tempo, sfruttando la scarsa pazienza della maggior parte dei sistemi di spamming automatizzati, che rinunciano all'invio nel caso in cui la sessione non venga immediatamente autorizzata.

RBL: le *Realtime Blackhole Lists* sono elenchi di indirizzi IP noti per essere l'origine di un certo quantitativo di spam o per effettuare attività sgradite o sospette. Il sistema si basa sul semplice principio che bloccare gli indirizzi di provenienza degli spammer sia il miglior modo per contrastarne l'attività.

SpamAssassin: si tratta di un progetto open source dedicato al contrasto dello spam che fa uso di un insieme di regole per decretare il livello di genuinità di un messaggio. SpamAssassin è molto efficace specialmente nell'individuazione di messaggi di "phishing" volti a ottenere le credenziali dei servizi finanziari degli utenti. IceWarp Server utilizza il set di regole di SpamAssassin ma ha un proprio motore interno per processare i messaggi.

FAST*flow* S.r.l. – IceWarp Italia
Via A. Manzoni, 25 – 22040 Lurago d'Erba (CO)
Tel. 031-697457 - Fax: 031-2280459
e-mail: info@icewarp.it - web: www.icewarp.it
C.F. e P.I. 02340830138 - Registro Imprese di Como - REA 255581 - Capitale sociale 10.400 euro i.v.

Antispam LIVE

La tecnologia Antispam LIVE è basata su RPD (*Recurring Pattern Detection – Rilevazione di schemi ricorrenti*) e consiste nell'analisi statistica di varie componenti del messaggio con i dati rilevati dai centri di monitoraggio del traffico, i quali esaminano grandi quantitativi di messaggi di posta elettronica, identificando nuove tipologie di attacchi spam, virus e phishing poco dopo la loro immissione sulla Rete.
Lo scopo di Antispam LIVE non è quello di dare un giudizio finale su di un messaggio quanto piuttosto di integrare il punteggio spam assegnato tramite le altre tecnologie. Per questo motivo Antispam LIVE entra in funzione solo quando il punteggio è inferiore a quello necessario per classificare un messaggio come indesiderato.

FAST*flow* S.r.l. – IceWarp Italia
Via A. Manzoni, 25 – 22040 Lurago d'Erba (CO)
Tel. 031-697457 - Fax: 031-2280459
e-mail: info@icewarp.it - web: www.icewarp.it
C.F. e P.I. 02340830138 - Registro Imprese di Como - REA 255581 - Capitale sociale 10.400 euro i.v.

Analisi

Le impostazioni del sistema Antispam sono quelle predefinite, a parte i parametri del sistema LIVE, che sono stati impostati sui seguenti valori:

- punteggio messaggi genuini: -1
- punteggio messaggi virus e mailing di massa: +7
- punteggio messaggi spam: +10

I valori rendono chiaro il concetto che il sistema LIVE è molto utile per riconoscere i messaggi indesiderati mentre contribuisce in misura molto minore a giudicare i messaggi genuini.
Nell'analisi non vengono considerati i messaggi per i quali la classificazione è stata ottenuta da una lista bianca o nera.
Le impostazioni dei sistemi utilizzati per l'analisi sono:

1) RBL (Spamhaus) + SpamAssassin + LIVE; rappresenta quella che potrebbe essere definita una soluzione pronta all'uso senza nessuna impostazione particolare da parte dell'amministratore.
2) Greylisting + RBL (Spamhaus) + SpamAssassin + LIVE; è una soluzione altamente personalizzata e ottimizzata secondo le esigenze degli utenti.

In entrambi i casi presi in esame le impostazioni e i sistemi sono gestiti direttamente dal nostro personale tecnico.

1) RBL + SpamAssassin + LIVE

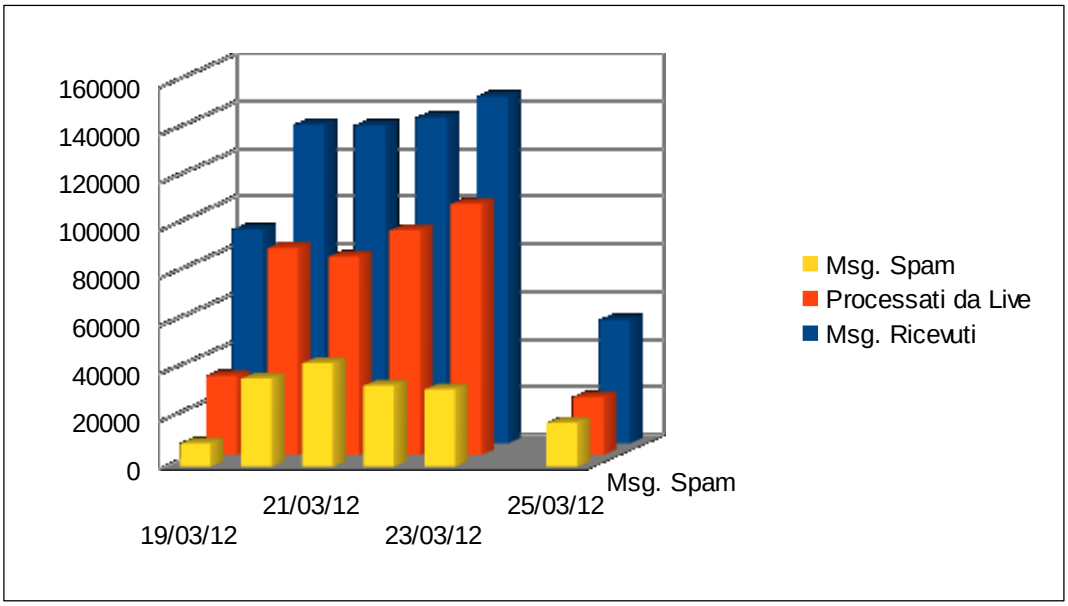
Data	Msg	Marcati	Rifiutati	Accettati	Spam	%
19/03/12	89735	7176	2700	79859	9876	11,0
20/03/12	133560	29364	7668	96528	37032	27,7
21/03/12	133215	32625	10669	89921	43294	32,5
22/03/12	136549	24776	9133	102640	33909	24,8
23/03/12	145443	22474	9821	113148	32295	22,2
25/03/12	51786	11392	6992	33402	18384	35,5
Totale	690288	127807	46983	515498	174790	25,3

Circa il 25% dei messaggi accettati dal server viene marcato come spam.

Data	Msg	Live	Spam->Msg	% S2M	Msg->Spam	% M2S
19/03/12	89735	33140	3657	4,1	3111	3,5
20/03/12	133560	86841	13292	10,0	16888	12,6
21/03/12	133215	83334	11122	8,3	19277	14,5
22/03/12	136549	94239	18946	13,9	20275	14,8
23/03/12	145443	105339	35056	24,1	17828	12,3
25/03/12	51786	24147	775	1,5	9166	17,7
Totale	690288	427040	82848	12,0	86545	12,5

Msg: Numero totale di messaggi analizzati dal sistema Antispam
Live: Numero di messaggi per i quali è intervenuto l'Antispam LIVE
Spam->Msg: Numero di messaggi per i quali l'Antispam LIVE ha eliminato la marcatura
Msg->Spam: Numero di messaggi per i quali l'Antispam LIVE ha prodotto la marcatura

L'Antispam LIVE contribuisce quindi alla corretta identificazione di oltre il 20% dei messaggi. Considerando il totale dei messaggi marcati, 174.790, l'Antispam LIVE è direttamente responsabile per circa il 50% di essi.



FAST*flow* S.r.l. – IceWarp Italia
Via A. Manzoni, 25 – 22040 Lurago d'Erba (CO)
Tel. 031-697457 - Fax: 031-2280459
e-mail: info@icewarp.it - web: www.icewarp.it
C.F. e P.I. 02340830138 - Registro Imprese di Como - REA 255581 - Capitale sociale 10.400 euro i.v.

2) Greylisting + RBL (spamhaus) + SpamAssassin + LIVE

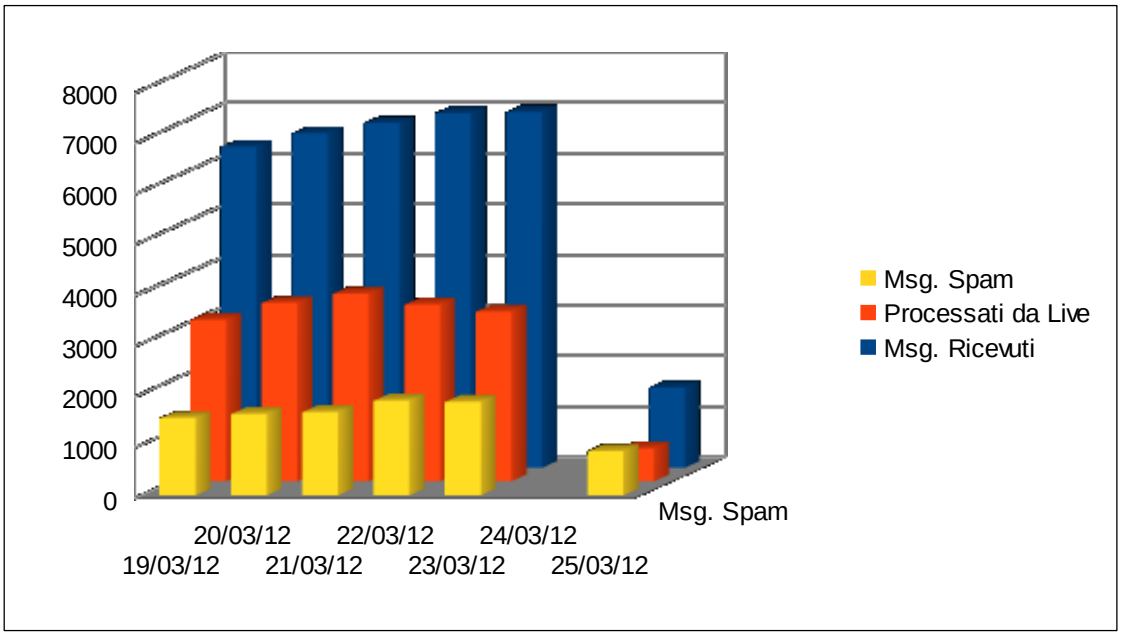
Data	Msg	Marcati	Rifiutati	Accettati	Spam	%
19/03/12	6329	547	970	4812	1517	24,0
20/03/12	6595	633	971	4991	1604	24,3
21/03/12	6796	636	1000	5160	1636	24,1
22/03/12	6995	656	1205	5134	1861	26,6
23/03/12	7022	542	1299	5181	1841	26,2
25/03/12	1575	195	676	704	871	55,3
Totale	35312	3209	6121	25982	9330	26,4

Come nel caso precedente circa il 25% dei messaggi accettati dal server viene marcato come spam.

Data	Msg	Live	Spam->Msg	% S2M	Msg->Spam	% M2S
19/03/12	6329	3188	20	0,3	440	7,0
20/03/12	6595	3519	29	0,4	466	7,1
21/03/12	6796	3703	39	0,6	540	7,9
22/03/12	6995	3490	22	0,3	448	6,4
23/03/12	7022	3353	30	0,4	395	5,6
25/03/12	1575	645	3	0,2	122	7,7
Totale	35312	17898	143	2,261815	2411	6,8

Msg: Numero totale di messaggi analizzati dal sistema Antispam
Live: Numero di messaggi per i quali è intervenuto l'Antispam LIVE
Spam->Msg: Numero di messaggi per i quali l'Antispam LIVE ha eliminato la marcatura
Msg->Spam: Numero di messaggi per i quali l'Antispam LIVE ha prodotto la marcatura

Rispetto al caso precedente, come auspicabile, la marcatura dell'Antispam LIVE è molto meno significativa soprattutto ai fini della classificazione di messaggi genuini.
Il sistema LIVE è responsabile della marcatura di circa il 25% dei messaggi spam, 2411 su 9330.



Conclusioni

In entrambi i casi il sistema LIVE si è dimostrato uno strumento efficace per l'analisi e l'identificazione del traffico sia indesiderato che non. Inoltre, data la modalità di funzionamento, Antispam LIVE è particolarmente indicato nelle situazioni in cui si vuole avere uno strumento che funzioni in maniera semplice, senza dover spendere troppo tempo nella configurazione.

FAST*flow* S.r.l. – IceWarp Italia
Via A. Manzoni, 25 – 22040 Lurago d'Erba (CO)
Tel. 031-697457 - Fax: 031-2280459
e-mail: info@icewarp.it - web: www.icewarp.it
C.F. e P.I. 02340830138 - Registro Imprese di Como - REA 255581 - Capitale sociale 10.400 euro i.v.

Note

Le interrogazioni utilizzate nell'analizzatore di log per ricavare i dati delle tabelle sono le seguenti:

```
SELECT as_Date,COUNT(*), SUM(IF(as_RSSpamLive!='',1,0)) Live,
       SUM(IF( (as_RSSpamAssassin>=3) AND (AS_RSSpamLive='N')
          AND (as_Action='NONE'), 1,0 ) ) Spam2N,
       SUM(IF( (as_RSSpamAssassin<3) AND
               (AS_RSSpamLive IN('H','Y')) AND
               (as_Action!='NONE'), 1,0 ) ) Ham2Spam
FROM antispam

WHERE as_RSBW='N'
GROUP BY as_Date
```

```
SELECT as_Date, COUNT(*), SUM(IF(as_action='SPAM',1,0)) Spam,
     SUM(IF(as_action IN('REJECT','DELETE'),1,0)) Rej,
     SUM(IF(as_action='NONE',1,0)) Ham
FROM antispam GROUP BY as_Date
```

FAST*flow* S.r.l. – IceWarp Italia
Via A. Manzoni, 25 – 22040 Lurago d'Erba (CO)
Tel. 031-697457 - Fax: 031-2280459
e-mail: info@icewarp.it - web: www.icewarp.it
C.F. e P.I. 02340830138 - Registro Imprese di Como - REA 255581 - Capitale sociale 10.400 euro i.v.