# Script di prevenzione invii massivi

Vi siete mai trovati a dover fronteggiare una **violazione** con **invio massivo di SPAM** da uno dei vostri account locali?
L'individuazione dell'account bucato e la successiva messa in sicurezza hanno richiesto **tempo e fatica**?

L'invio massivo di messaggi indesiderati è una delle situazioni che in maniera più rapida possono influire negativamente sul funzionamento di un server, andando a sporcarne la reputazione. Le **DNSBL** (Blackhole List basate sui DNS) e le **RBL** (Real-Time Blackhole List) si occupano infatti di mantenere un elenco di IP di host e reti da cui sono state generate comunicazioni di tipo SPAM e la maggior parte dei mail server è configurata per respingere o contrassegnare i messaggi provenienti da questi indirizzi.

Perché allora non fare qualcosa per fermare queste situazioni **prima che dilaghino**?

In questa guida è illustrato l'utilizzo di uno script che si occupa di analizzare le statistiche degli account, negando l'invio a quelli che hanno superato un limite di messaggi inviati all'esterno in un determinato arco temporale. In caso di disabilitazione di uno o più account lo strumento si occupa anche di mandare una mail di notifica ad un indirizzo scelto dall'utente, generalmente un amministratore del Server, segnalando gli account in questione.

FASTflow 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

**Installazione dello script e impostazione parametri**

Affinché lo script funzioni, è **essenziale** che i log statistici degli account siano attivi. Si verifichi quindi da console di amministrazione l'impostazione di [Stato > Statistiche account > Attiva i log statistici degli account] oppure la variabile API *c_accounts_global_accounts_userstat*.

Lo script si installa estraendo la cartella compressa *floodblocker.zip* nella root del Web Server di IceWarp ( *<IceWarp_path>\html* ) e andando ad impostare alcuni parametri in modo da adattare l'esecuzione dello script alle proprie preferenze. In particolare sarà necessario prestare attenzione ai *Parametri di esecuzione:*

`$from` data di inizio del periodo considerato (per default impostata alla data del giorno);
`$to` data di fine del periodo considerato (per default impostata alla data del giorno);
`$limite` limite di messaggi oltre il quale l'account viene disabilitato.

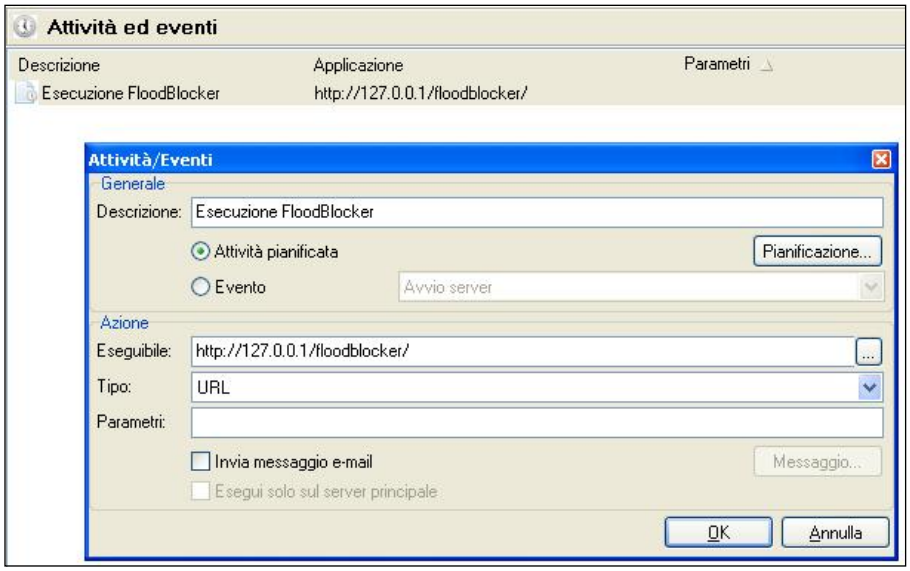
Modificando il valore della variabile `$from`, avvalendosi delle funzioni di PHP, è possibile aumentare o diminuire il range temporale al quale applicare il controllo. Ad esempio se volessimo considerare gli ultimi tre giorni potremmo usare queste funzioni:

```
date("Y/n/j", mktime(0, 0, 0, date("m"), date("d")-2, date("Y")));
```

Vi è inoltre una sezione *Parametri per mail di notifica* che consente di personalizzare la comunicazione da generare in occasione del blocco dell'invio di uno o più account:

| | |
|---|---|
| `$com1->RemoteHost` | Server tramite il quale inviare il messaggio (per default localhost); |
| `$com1->Helo` | Hostname dichiarato nel comando HELO della sessione; |
| `$com1->MailFrom` | Indirizzo email del mittente; |
| `$rcpt_name` | Nome del destinatario; |
| `$rcpt_address` | Indirizzo email del destinatario; |
| `$com1->IsHTML` | Formato del messaggio (per default HTML supportato); |
| `$com1->FromName` | Nome del mittente negli Header; |
| `$com1->FromAddress` | Indirizzo email del mittente negli Header; |
| `$com1->Subject` | Oggetto del messaggio; |
| `$msg_body` | Corpo del messaggio. |

Conclusa la fase di definizione dei parametri sarà necessario creare un'attività pianificata tramite [Sistema > Strumenti > Attività ed eventi].




Per l'attività può essere definita qualsiasi ricorrenza. Ogni esecuzione dello script sarà registrata nel file di log apposito, creato all'interno della cartella di installazione.

```
### Script eseguito il 26/3/2013 alle 17:12:14 ###
Data di inizio: 2013/3/26
Data di fine: 2013/3/26
Limite messaggi: 100

====================
Dominio: demo.com


---
Alias: admin
Percorso casella: C:\Programmi\IceWarp\mail\demo.com\admin\
L'utente ha inviato 3 messaggi all'esterno nel periodo definito
---
Alias: user;mario;m.rossi
Percorso casella: C:\Programmi\IceWarp\mail\demo.com\user\
L'utente ha inviato 21 messaggi all'esterno nel periodo definito
---
```

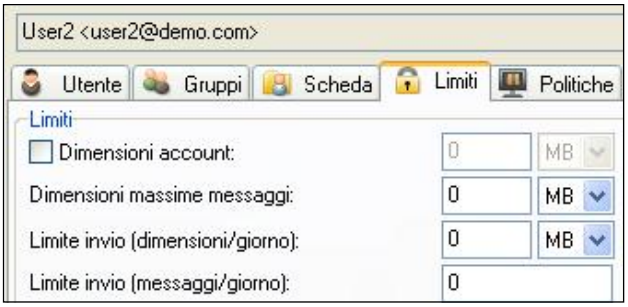
All'inizio del codice vi è una variabile `$log_level` che controlla il livello di questo log

0: Disabilitato;
1: Sintetico (Predefinita), registra solo gli account che hanno superato i limiti;
2: Completo, registra il dato statistico di invio di ciascun account.

**Attenzione**: nei casi di esecuzioni pianificate frequentemente, e registrate in maniera dettagliata, il file di log potrebbe raggiungere rapidamente elevate dimensioni e sarebbe pertanto opportuno archiviarlo o cancellarlo periodicamente per consentire la creazione di un nuovo file.

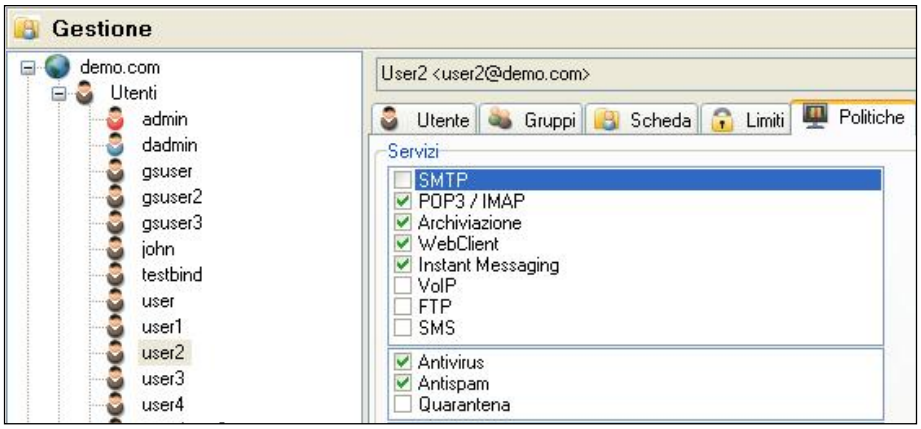
**Differenza con i Limiti dell'account**

Ciascun account ha una sezione Limiti nella quale è possibile impostare un limite massimo di invii al giorno (sempre intesi come messaggi inviati a destinatari remoti).




L'utilizzo di questo limite non è però alternativo allo script, in quanto i due sistemi di controllo hanno differenze sostanziali.
Per mezzo del limite dell'account ulteriori invii all'esterno vengono impediti ma gli invii locali restano comunque sempre possibili. Lo script in oggetto si occupa invece di disabilitare il supporto SMTP per l'account rendendo pertanto impossibili anche gli invii locali. Questa particolarità è utile in quanto, se l'account bloccato è stato effettivamente oggetto di violazione, la diffusione di SPAM viene totalmente impedita.

Lo script, a differenza del limite, permette anche di inviare una mail di notifica che segnala l'avvenuta disabilitazione dell'invio per uno o più account, allertando quindi l'amministratore di una situazione anomala che è opportuno analizzare. Nel caso in cui l'account bloccato sia legittimato a superare il limite di invii, l'amministratore potrà prontamente provvedere a ristabilirgli il servizio SMTP.




Il consiglio è quindi quello di avvalersi del Limite dell'account nei casi in cui, per accordi contrattuali tra il fornitore del servizio ed il cliente o per politiche amministrative del Server, non sia consentito inviare all'esterno più di un certo numero di messaggi al giorno, e di affidarsi invece allo script nei casi in cui il fine ultimo non sia imporre un limite di invii ma piuttosto tenere monitorate situazioni potenzialmente anomale, bloccandole per poterle analizzare.