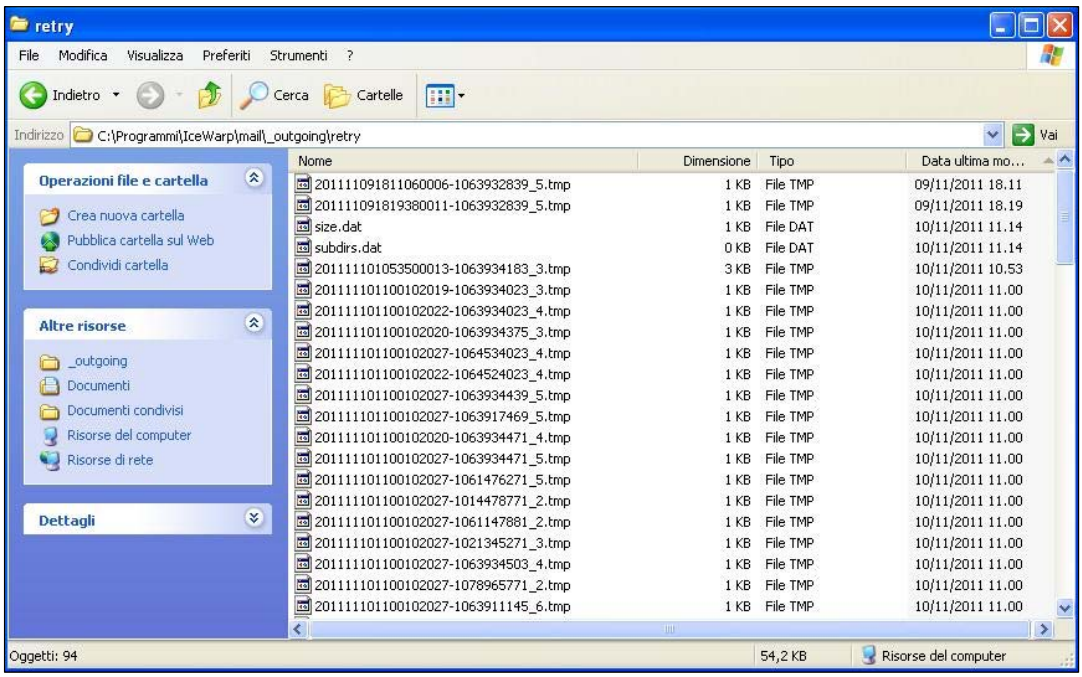
Tecniche di messa in sicurezza di un Server violato

Le sessioni SMTP del tuo server sembrano moltiplicarsi a vista d'occhio?
La coda dei messaggi in uscita cresce a dismisura?
Gli utenti segnalano un consistente numero di messaggi indesiderati provenienti da account locali e “fidati” o da improbabili mittenti che avrebbero dovuto essere filtrati dal sistema Antispam?
Questi sono i sintomi tipici di un sistema vittima di una violazione.

Dinamiche tipiche di una violazione

Un programma di individuazione di credenziali agisce tipicamente tramite un algoritmo a forza bruta che tenta tutte le possibili combinazioni fino ad individuare una coppia valida di nome utente e password. Sempre più spesso, inoltre, le credenziali di autenticazione possono essere state carpite da virus e trojan che hanno infettato la macchina client.
Una volta in possesso di tali credenziali lo *spammer* le utilizza per effettuare invii di messaggi indesiderati verso un elevatissimo numero di indirizzi, molti dei quali composti casualmente e di conseguenza inesistenti. Per questo motivo uno dei primi sintomi di una violazione è la presenza nelle directory “_outgoing” e “_outgoing\retry” di un elevato numero di messaggi diretti a improbabili destinatari e tipicamente di dimensioni molto ridotte.



FAST*flow* S.r.l. – IceWarp Italia
Via A. Manzoni, 25 – 22040 Lurago d'Erba (CO)
Tel. 031-697457, Fax: 031-697458
e-mail: info@icewarp.it
Web: www.icewarp.it

L'operazione di pulizia della coda di retry è generalmente ostica sia per via del filtraggio che è necessario applicare per distinguere i messaggi correlati ad attività di spamming da quelli genuini sia per il numero tipicamente molto elevato dei messaggi da cancellare i quali rappresentano un ostacolo "fisico" tutt'altro che trascurabile (selezionare ed eliminare migliaia di messaggi non è semplicissimo).
Per questo motivo risulta spesso indispensabile affidarsi a strumenti come batch di cancellazione di cui vi riportiamo un esempio:

File cleanqueue.bat

```
@echo off
cls
if "%1" == "" goto error
grep -rl "%*" <IceWarp_path>\mail\_outgoing\*.*|xargs --no-run-if-empty -i{} rm \"{}\"
pause
exit
:error
echo Nessuna stringa di ricerca specificata.
echo .
echo Sintassi: cleanqueue STRINGA
echo Esempio: cleanqueue pippo@gmail.com
```

Un file .bat come questo permette di eliminare tutti i messaggi contenenti la stringa indicata (nell'esempio: pippo@gmail.com). Dopo averlo salvato sarà sufficiente lanciarlo dal prompt dei comandi postponendo la stringa di ricerca al nome del file.
Tipicamente tutti i messagi provenienti da uno stesso flusso di spamming contengono una o più informazioni comuni (fantomatici mittenti e/o destinatari, URL, nomi di prodotti, ecc.) e sarà appunto un'informazione di questo tipo la stringa di ricerca designata.
Affinché il batch funzioni correttamente è necessario specificare all'interno del suo codice il percorso della cartella *_outgoing*.
I comandi grep, xargs e rm utilizzati nel suddetto batch sono reperibili sul sito http://unxutils.sourceforge.net oppure su http://www.icewarp.it/download/support/cleanqueue.zip.

FAST*flow* S.r.l. – IceWarp Italia
Via A. Manzoni, 25 – 22040 Lurago d'Erba (CO)
Tel. 031-697457, Fax: 031-697458
e-mail: info@icewarp.it
Web: www.icewarp.it

Individuazione dell'account violato

Prelevando uno dei messaggi sopra descritti dalla coda di retry e analizzandolo è possibile risalire all'account oggetto della violazione.

```
MsgID: TUQ42143
LocalSender: user@icewarpdemo.com
From: <lucas_johnson@wegotit.ru>
To: <julie_charles@notforsale.com>
Received: from 12-dgfj-it ([192.168.26.20])
        by localhost (IceWarp 10.3.4) with ASMTP id TUQ42143
        for <julie_charles@notforsale.com>; Thu, 10 Nov 2011 10:58:43 +0100
Date: Wed, 10 Nov 2011 10:59:11 +0100
From: Lucas <lucas_johnson@wegotit.ru>
Organization: External
To: "Julie" <julie_charles@notforsale.com>
Subject: We know what you need
Message-ID: <d587ae35e4d92a2d735b568696b4f201@wegotit.ru>

Buy 1 get One free
http://ert.hump.com
```

L'header *LocalSender* contiene l'informazione relativa all'account le cui credenziali sono state utilizzate per effettuare autenticazione SMTP. L'header *From* indica invece l'indirizzo che è stato dichiarato come mittente nella medesima sessione.
Anche l'informazione *MsgID* è molto utile in quanto ci permette di risalire agevolmente alla sessione Server.

```
192.168.26.20   [0D38] 10:57:43 Connected, local IP=192.168.26.20
192.168.26.20   [0D38] 10:57:43 >>> 220 localhost ESMTP IceWarp 10.3.4; Thu, 10 Nov 2011 10:57:43 +0100
192.168.26.20   [0D38] 10:57:49 <<< ehlo 12-dgfj-it
192.168.26.20   [0D38] 10:57:49 >>> 250-localhost Hello 12-dgfj-it [192.168.26.20], pleased to meet you.
192.168.26.20   [0D38] 10:57:57 <<< auth login
192.168.26.20   [0D38] 10:57:57 >>> 334 VXNlcm5hbWU6
192.168.26.20   [0D38] 10:58:04 <<< dXN1cg==
192.168.26.20   [0D38] 10:58:04 >>> 334 UGFzc3dvcmQ6
192.168.26.20   [0D38] 10:58:06 <<< dXN1cg==
192.168.26.20   [0D38] 10:58:06 >>> 235 2.0.0 Authentication successful
192.168.26.20   [0D38] 10:58:21 <<< mail from:<lucas_johnson@wegotit.ru>
192.168.26.20   [0D38] 10:58:21 >>> 250 2.1.0 <lucas_johnson@wegotit.ru>... Sender ok
192.168.26.20   [0D38] 10:58:38 <<< rcpt to:<julie_charles@notforsale.com>
192.168.26.20   [0D38] 10:58:38 >>> 250 2.1.5 <julie_charles@notforsale.com>... Recipient ok; will forward
192.168.26.20   [0D38] 10:58:43 <<< data
192.168.26.20   [0D38] 10:58:43 >>> 354 Enter mail, end with "." on a line by itself
192.168.26.20   [0D38] 10:59:43 <<< 192 bytes (overall data transfer speed=3 B/s)
192.168.26.20   [0D38] 11:00:10 <<< 225 bytes (overall data transfer speed=3 B/s)
192.168.26.20   [0D38] 11:00:10 Start of mail processing
192.168.26.20   [0D38] 11:00:10 *** <lucas_johnson@wegotit.ru> <julie_charles@notforsale.com> 1 220 00:01:27 OK TUQ42143
192.168.26.20   [0D38] 11:00:10 >>> 250 2.6.0 220 bytes received in 00:01:27; Message id TUQ42143 accepted for delivery
192.168.26.20   [0D38] 11:00:12 <<< quit
192.168.26.20   [0D38] 11:00:12 >>> 221 2.0.0 localhost closing connection
192.168.26.20   [0D38] 11:00:12 Disconnected
```

Nella sessione sono chiaramente individuabili le credenziali utilizzate per effettuare l'autenticazione, codificate in base64 (la seconda e la quarta riga dopo il comando “AUTH LOGIN”). Utilizzando un qualsiasi decodificatore base64, ad esempio presente anche nell'Analizzatore di Log IceWarp, è possibile risalire all'account.
Nel caso riportato nell'esempio, decodificando la stringa '**dXNlcg==**' fornita sia come nome utente che come password, otteniamo 'user'.
Prendiamo ora in esame la sessione Client che ha fatto seguito alla sessione Server sopra riportata.

```
1  SYSTEM          [1474] 18:13:21 Client session Message id TUQ42143 item 201111101100102022-1063944618_7.tm$
2  SYSTEM          [1474] 18:13:21 Client session DNS query 'notforsale.com' 0 (0) [OK - 1]
3  SYSTEM          [1474] 18:13:21 Client session Connecting to 'notforsale.com'
4  SYSTEM          [1474] 18:13:22 Client session Could not connect to 'notforsale.com(174.137.125.47)'
5  SYSTEM          [1474] 18:13:22 Client session *** <lucas_johnson@wegotit.ru> <julie_charles@notforsale.com> 1 463 00:00:00 INCOMPLETE-SESSION TUQ42143
6  SYSTEM          [1474] 18:13:22 Client session Disconnected
```

Come si può facilmente notare la sessione non si è correttamente conclusa per via dell'impossibilità di connettersi al server remoto. Evidentemente la query DNS non ha restituito alcun record MX e ciò significa che l'indirizzo di destinazione, come spesso succede per i sistemi di invii massivi di messaggi indesiderati, non esiste ed è stato probabilmente composto automaticamente.

Azioni da intraprendere

Una volta riconosciuta la violazione ed individuato l'account veicolo dell'invio di messaggi indesiderati è necessario “chiudere la falla” e procedere con la messa in sicurezza del sistema.
Prima di tutto è ovviamente necessario cambiare le credenziali dell'account violato ed eliminare tutti i messaggi indesiderati nella coda di retry.
Tramite il *tool* di IceWarp Server è poi necessario individuare tutti gli account che presentano credenziali deboli, le quali ben si prestano ad essere individuate e utilizzate degli spammer. E' senz'altro bene individuare gli account che presentano alias e password uguali:

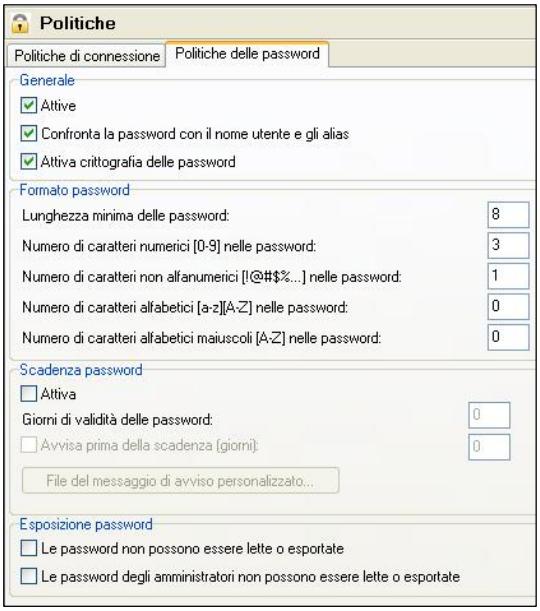
```
C:\Programmi\IceWarp>tool -filter="u_alias = u_password" display account "*@*" u
_alias u_password
admin@icewarpdemo.com
u_alias: admin
u_password: admin

user@icewarpdemo.com
u_alias: user
u_password: user

user1@icewarpdemo.com
u_alias: user1
u_password: user1
```

FAST*flow* S.r.l. – IceWarp Italia
Via A. Manzoni, 25 – 22040 Lurago d'Erba (CO)
Tel. 031-697457, Fax: 031-697458
e-mail: info@icewarp.it
Web: www.icewarp.it

e anche quelli che presentano nome utente e password uguali:

```
C:\Programmi\IceWarp>tool -filter="u_name = u_password" display account "*@*" u_
name u_password
admin@icewarpdemo.com
u_name: Admin
u_password: admin
```

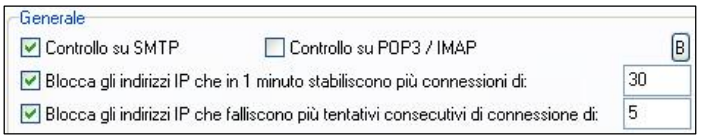
Dopo aver effettuato questi primi controlli e avere individuato gli account che rappresentano un grande rischio per il sistema è consigliabile definire delle politiche di robustezza delle password nella sezione *[Domini e account > Politiche > Politiche delle password]*.



E' fortemente consigliato attivare le funzionalità di controllo della password con i nomi utenti e gli alias affinché non sia più possibile definire account che presentino una forte vulnerabilità.
E' poi possibile, secondo le proprie preferenze, definire delle regole di formato delle password mirate a renderle più complesse e quindi più difficilmente individuabili da algoritmi di individuazione a forza bruta.
Una volta ridefinite le politiche è possibile individuare gli account ad esse non conformi, sempre per mezzo del *tool*.

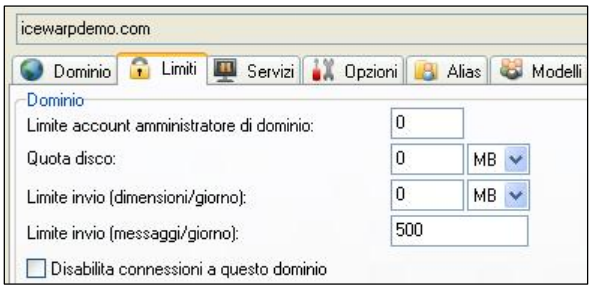
```
C:\Programmi\IceWarp>tool check account "*@*" passpolicy
admin@icewarpdemo.com

user@icewarpdemo.com

user1@icewarpdemo.com

user2@icewarpdemo.com

user3@icewarpdemo.com

icewarp@icewarpdemo.com

user4@icewarpdemo.com

user5@icewarpdemo.com

mario@icewarpdemo.com

user6@icewarpdemo.com

pippo@backup.it
```

Si può poi eventualmente passare alla revisione della sezione *[Posta > Sicurezza]* nel caso in cui la violazione del sistema sia stata facilitata da qualche impostazione poco stringente a livello di sicurezza e autorizzazione.
La sezione *Prevenzione intrusioni* e le sue impostazioni sono molto importanti al fine di evitare queste situazioni, si presti particolare attenzione ai valori dati alle funzionalità che stabiliscono il blocco degli IP, specialmente le prime due per le quali potrebbe essere opportuno assegnare valori stringenti.



Nel caso del nostro esempio inoltre, la mancanza della funzionalità *"Respingi se SMTP AUTH non corrisponde al mittente"* ha fatto sì che fosse eseguita autenticazione con le credenziali di un account salvo poi dichiarare un mittente completamente diverso in sessione.
Attivando tale funzionalità ci si assicura che chiunque effettui autenticazione debba poi dichiarare lo stesso indirizzo come mittente del messaggio.
Questo vincolo apre nuove possibilità in quanto permette di utilizzare i limiti degli account e dei domini onde evitare gli invii massivi di qualsiasi genere.

FAST*flow* S.r.l. – IceWarp Italia
Via A. Manzoni, 25 – 22040 Lurago d'Erba (CO)
Tel. 031-697457, Fax: 031-697458
e-mail: info@icewarp.it
Web: www.icewarp.it



Per utilizzare i limiti è necessario abilitare la relativa funzionalità all'indirizzo *[Domini e account > Impostazioni globali > Utilizza limiti dominio/utente]*.
E' bene tenere presente che gli invii a destinatari locali non concorrono al raggiungimento dei limiti stabiliti.

Questi accorgimenti dovrebbero contribuire a rendere il sistema difficilmente violabile.
In base alle esigenze dell'utenza e dell'amministrazione del server è possibile personalizzare la sicurezza restringendo i controlli e ponendo più ostacoli sulla strada degli spammer (es: scadenza periodica delle password, greylisting) cercando allo stesso tempo di non incidere eccessivamente sull'usabilità e sulle prestazioni del sistema.

FAST*flow* S.r.l. – IceWarp Italia
Via A. Manzoni, 25 – 22040 Lurago d'Erba (CO)
Tel. 031-697457, Fax: 031-697458
e-mail: info@icewarp.it
Web: www.icewarp.it