Quel est format de mbox UNIX (boîte aux lettres) ?

Contenu

Introduction

Ce document décrit le format de boîte aux lettres d'Unix (mbox) et comment il associe pour l'utiliser sur l'appliance de sécurité du courrier électronique de Cisco (ESA).

Quel est format de mbox UNIX (boîte aux lettres) ?

Le format de mbox UNIX est utilisé par AsyncOS quand des messages sont archivés et a ouvert une session l'action de log() de filtre de message. Le « message d'archives » est une option de configuration supplémentaire pour l'Anit-Spam d'Ironport (IPAS), l'antivirus (Sophos et McAfee), la protection avancée de malware (AMP), et le Graymail sur l'ESA.

Le format de Mbox est (c'est-à-dire,) un format de fichier non binaire ASCII-formaté qui peut contenir zéro messages ou plus. Des messages sont concaténés dans le fichier de mbox et peuvent être soulevés à part ont basé sur les chaînes spécifiques dans le fichier. Ce format est identique au message car ils sont transférés entre les passerelles conformes de messagerie RFC 2821.

Chaque message dans le format de mbox commence par une ligne « à partir » de la laquelle commence avec la chaîne (caractères ASCII F, r, o, m, et espace). « » Des lignes sont suivis par plusieurs plus de champs : enveloppe-expéditeur, date, et (sur option) plus de données.

Le premier champ après « » de la chaîne est l'enveloppe-expéditeur du message. La personne à charge sur laquelle l'application crée le fichier de mbox, l'enveloppe-expéditeur pourrait être présent pendant qu'une vraie boîte aux lettres ou ce pourrait être un caractère ou une chaîne différent. Le plus généralement, vous constaterez que « - » (tiret de caractère unique) remplace l'enveloppe-expéditeur si l'enveloppe-expéditeur réel n'est pas disponible ou non connu. Le champ de date inséré par l'ESA est dans le format standard d'asctime() UNIX et est toujours 24 caractères de longueur. Dans des quelques fichiers de mbox écrits par des réalisations de non-AsyncOS, les informations supplémentaires suivent le tampon-date. Ces trois champs sont séparés par un espace simple.

Voici un exemple d'un fichier de mbox avec un message simple dans lui :

```
From Adam@Outside.COM Sun Oct 17 12:03:20 2004
Received: from mail.outside.com (192.35.195.200)
by smtp.alpha.com with ESMTP; 17 Oct 2004 12:03:20 -0700
X-IronPort-AV: i="3.85,147,1094454000";
v="EICAR-AV-Test'0'v";
d="scan'208"; a="86:adNrHT37924848"
```

```
X-IronPort-RCPT-TO: alan@mail.example.com
From: Adam@Outside.COM
To: Alan Alpha <Alan@mail.example.COM>
Subject: Exercise 7a Anti-Virus Scanning
Reply-To: Adam Alpha <adam@outside.com>
Date: Sun, 17 Oct 2004 12:02:39 -0700
MIME-version: 1.0
Content-type: multipart/mixed; boundary="IronPort"

--IronPort
Content-type: text/plain; format=flowed; charset=us-ascii
Content-transfer-encoding: 7bit

Blah blah blah blah blah
Blah blah blah blah blah
Blah blah blah blah blah
...
--IronPort
Content-type: text/plain
Content-transfer-encoding: 7bit
Content-disposition: inline

X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-
FILE!$H+H*">X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*

--IronPort--
```

Quand des fichiers mbox-formatés sont analysés, il est desirable de ne pas lire trop de sémantique dans « » de la ligne qui sépare des messages. Puisque beaucoup de différents utilitaires écrivent des fichiers de mbox, il y a variation considérable de ces lignes. Cependant, « » de la ligne peut toujours être utilisé comme ligne de séparateur de message afin d'indiquer sûrement qu'un nouveau message a commencé dans le fichier de mbox. En tout, il y a environ 20 formats connus pour les chaînes après « » du séparateur de message, qui le rend généralement très difficile de les analyser.

Après que « » de la ligne soit un message électronique dans le format RFC 2822, avec une gamme d'en-têtes de corps du message suivies d'une ligne vide suivie du contenu supplémentaire de corps du message.

Afin de s'assurer que des messages sont correctement séparés, des lignes dont commencez par la chaîne « » sont toujours ajoutées au début par un simple « **>** ». Diverses différentes variantes des lignes de traitement de fichiers de mbox qui commencent par le « >From » différemment. Dans des réalisations tôt des applications qui ont écrit des fichiers de mbox, ces lignes elles-mêmes n'ont pas été citées. Les fichiers journal d'AsyncOS ajouteront toujours au début « **>** » aux lignes des lesquelles commencez par un ou plusieurs « **>** » des caractères suivis « de ».

Voici un exemple d'un fichier de mbox qui contient un message qui a eu les lignes dont contenez commencer ficelle « », « >From » et « **>>>>**From » dans lui :

```
From jtrumbo@example1.com Sun Dec 12 12:27:33 2004
X-IronPort-RCPT-TO: trumbo@example1.com
From: jtrumbo@example1.com
To: trumbo@example2.com
Subject: Quote this, if you dare
Date: Sun, 12 Dec 2004 12:28:00 -0700

The following line is just From
>From A From Line
```

```
The following line has quoted >From
>>From A >From Line

The following line has many >>>>From
>>>>>From This line has 4 > characters before From

And this is the last line
```

L'extrémité d'un message dans un fichier de format de mbox est traditionnellement signalée par une ligne vide. Cependant, ce n'est pas toujours présent (bien qu'AsyncOS le place là). Quand un fichier de mbox-format est analysé, vous devriez signaler l'extrémité d'un message par le début d'un nouveau message (supprimez la ligne vide si on est présent) ou vers la fin du fichier.

Une autre variante dans le format de mbox nécessité la longueur du message à signaler dans un domaine de « content-length » dans l'en-tête de message. Ce format ne l'a pas utilisé « » de la ligne citation. AsyncOS n'utilise pas ce format et n'insère pas un champ de content-length.