Cos'è il formato mbox (mailbox) di UNIX?

Sommario

[Introduzione](#)
[Cos'è il formato mbox (mailbox) di UNIX?](#)

Introduzione

In questo documento viene illustrato il formato mbox (mailbox) di Unix e come utilizzarlo sull'appliance di sicurezza Cisco Email Security Appliance (ESA).

Cos'è il formato mbox (mailbox) di UNIX?

Il formato mbox UNIX viene utilizzato da AsyncOS quando i messaggi vengono archiviati e registrati nell'azione log() del filtro messaggi. "Archive Message" è un'opzione di configurazione aggiuntiva per Ironport Anit-spam (IPAS), Anti-virus (Sophos e McAfee), Advanced Malware Protection (AMP) e Graymail sull'ESA.

Il formato Mbox è un formato di file in formato ASCII (non binario) che può contenere zero o più messaggi di posta elettronica. I messaggi vengono concatenati nel file mbox e possono essere suddivisi in base a specifiche stringhe nel file. Questo formato è identico al messaggio in quanto vengono trasferiti tra gateway di posta conformi alla RFC 2821.

Ogni messaggio in formato mbox inizia con una riga che inizia con la stringa "From" (caratteri ASCII F, r, o, m e spazio). Le righe "Da" sono seguite da altri campi: busta-mittente, data e (facoltativamente) altri dati.

Il primo campo dopo la stringa "Da" è il mittente della busta del messaggio. A seconda dell'applicazione che crea il file mbox, il mittente della busta potrebbe essere presente come cassetta postale reale oppure potrebbe essere un altro carattere o una stringa. Nella maggior parte dei casi, si noterà che un "-" (trattino a carattere singolo) sostituisce il mittente della busta se il mittente effettivo non è disponibile o non è noto. Il campo data inserito dall'ESA è in formato standard UNIX asctime() ed è sempre lungo 24 caratteri. In alcuni file mbox scritti da implementazioni non AsyncOS, il timbro data è seguito da ulteriori informazioni. Questi tre campi sono separati da uno spazio.

Di seguito è riportato un esempio di file mbox con un singolo messaggio:

```
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
```

```
--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--
```

Quando si analizzano file in formato mbox, è consigliabile non leggere troppa semantica nella riga "Da" che separa i messaggi. Poiché molte utilità diverse scrivono file mbox, c'è una notevole variazione in queste righe. Tuttavia, la riga "Da " può sempre essere utilizzata come riga di separazione dei messaggi per indicare in modo affidabile l'inizio di un nuovo messaggio nel file mbox. In tutto, ci sono circa 20 formati noti per le stringhe dopo il separatore di messaggio "Da", che in genere rende molto difficile analizzarle.

Dopo la riga "Da" viene visualizzato un messaggio e-mail in formato RFC 2822, con una serie di intestazioni del corpo del messaggio seguite da una riga vuota seguita da contenuto aggiuntivo del corpo del messaggio.

Per garantire la corretta separazione dei messaggi, le righe che iniziano con la stringa "From" vengono sempre anteposte da un singolo carattere "**>**". Diverse varianti di file mbox gestiscono in modo diverso le linee che iniziano con "**>**Da". Nelle prime implementazioni di applicazioni che scrivevano file mbox, queste righe non erano citate. I file di registro AsyncOS anteporranno sempre "**>**" alle righe che iniziano con uno o più caratteri "**>**" seguiti da "From".

Di seguito è riportato un esempio di file mbox contenente un messaggio con righe contenenti le stringhe iniziali "From", "**>**From" e "**>>>**From":

```
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
```

In genere, la fine di un messaggio in un file in formato MBOX viene segnalata da una riga vuota. Tuttavia, questa condizione non è sempre presente (anche se viene inserita da AsyncOS). Quando si analizza un file in formato mbox, è necessario segnalare la fine di un messaggio sia all'inizio di un nuovo messaggio (eliminare la riga vuota se presente), sia alla fine del file.

Un'altra variante nel formato mbox richiedeva che la lunghezza del messaggio fosse segnalata in un campo "Content-Length" all'interno dell'intestazione del messaggio. Tale formato non utilizzava le virgolette di inizio riga. AsyncOS non utilizza questo formato e non inserisce un campo Content-Length.