Was ist das UNIX-mbox-Format (Mailbox)?

Inhalt

Einführung

Dieses Dokument beschreibt das Unix-Mailbox-Format (mbox) und seine Beziehung zur Verwendung auf der Cisco E-Mail Security Appliance (ESA).

Was ist das UNIX-mbox-Format (Mailbox)?

Das UNIX-mbox-Format wird von AsyncOS verwendet, wenn Nachrichten archiviert und in der Aktion log() des Nachrichtenfilters angemeldet werden. "Archive Message" ist eine zusätzliche Konfigurationsoption für IronPort Anti-Spam (IPAS), Anti-Virus (Sophos und McAfee), Advanced Malware Protection (AMP) und Graymail auf der ESA.

Das Mbox-Format ist ein ASCII-formatiertes (d. h. nicht binäres) Dateiformat, das 0 (null) oder mehr E-Mail-Nachrichten enthalten kann. Nachrichten werden in der mbox-Datei verkettet und können abhängig von bestimmten Zeichenfolgen in der Datei getrennt werden. Dieses Format ist identisch mit der Nachricht, da sie zwischen RFC 2821-kompatiblen Mail-Gateways übertragen wird.

Jede Nachricht im mbox-Format beginnt mit einer Zeile, die mit der Zeichenfolge "From" (ASCII-Zeichen F, r, o, m und Leerzeichen) beginnt. Auf "Von"-Zeilen folgen mehrere weitere Felder: Umschlagabsender, Datum und (optional) weitere Daten.

Das erste Feld nach der Zeichenfolge "From" ist der Umschlagabsender der Nachricht. Je nachdem, von welcher Anwendung die mbox-Datei erstellt wird, kann der Umschlagsender als echte Mailbox vorhanden sein, oder es kann sich um ein anderes Zeichen oder eine Zeichenfolge handeln. In der Regel wird der Umschlagabsender durch ein "-" (Single Character Dash) ersetzt, wenn der eigentliche Umschlagabsender nicht verfügbar oder nicht bekannt ist. Das von der ESA eingeführte Datumsfeld hat das UNIX-asctime()-Standardformat und ist immer 24 Zeichen lang. In einigen mbox-Dateien, die von Nicht-AsyncOS-Implementierungen geschrieben wurden, folgen weitere Informationen dem Datumstempel. Diese drei Felder sind durch ein einzelnes Leerzeichen getrennt.

Im Folgenden sehen Sie ein Beispiel für eine mbox-Datei mit einer einzelnen Meldung:

```
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--
```

Wenn mbox-formatierte Dateien analysiert werden, ist es wünschenswert, nicht zu viel Semantik in die "From"-Zeile zu lesen, in der Nachrichten getrennt werden. Da viele verschiedene Dienstprogramme mbox-Dateien schreiben, gibt es erhebliche Abweichungen in diesen Zeilen. Die Zeile "From" kann jedoch immer als Trennlinie für Nachrichten verwendet werden, um zuverlässig anzuzeigen, dass eine neue Nachricht in der mbox-Datei gestartet wurde. Insgesamt gibt es ca. 20 bekannte Formate für die Zeichenfolgen nach dem "From"-Meldungs-Trennzeichen, was es in der Regel sehr schwierig macht, sie zu analysieren.

Nach der Zeile "From" (Von) wird eine E-Mail im RFC 2822-Format mit einer Reihe von Nachrichtentext-Headern gefolgt von einer leeren Zeile gefolgt von einem zusätzlichen Nachrichtentext angezeigt.

Um sicherzustellen, dass Nachrichten ordnungsgemäß getrennt werden, werden Zeilen, die mit der Zeichenfolge "From" beginnen, immer mit einem einzigen ">" vorangestellt. Verschiedene Varianten von mbox-Dateien behandeln Zeilen, die mit ">From" beginnen. In früheren Implementierungen von Anwendungen, die mbox-Dateien geschrieben hatten, wurden diese Zeilen selbst nicht zitiert. AsyncOS-Protokolldateien stellen Zeilen, die mit einem oder mehreren ">"-Zeichen beginnen, gefolgt von "From", immer ein ">" voran.

Hier ein Beispiel für eine mbox-Datei, die eine Meldung enthält, die Zeilen enthält, die die Startzeichenfolgen "From", ">From" und ">>>From" enthalten:

```
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
```

Das Ende einer Nachricht in einer mbox-Format-Datei wird normalerweise durch eine leere Zeile signalisiert. Dies ist jedoch nicht immer vorhanden (obwohl AsyncOS es dort ablegt). Wenn eine mbox-formatierte Datei analysiert wird, sollten Sie das Ende einer Nachricht entweder durch den Beginn einer neuen Nachricht (löschen Sie die leere Zeile, wenn eine vorhanden ist) oder durch das Ende der Datei signalisieren.

Eine weitere Variante im mbox-Format forderte die Signalisierung der Länge der Nachricht in einem Feld "Content-Length" im Nachrichtenheader. In diesem Format wurde keine "From"-Posten-Angebotserstellung verwendet. AsyncOS verwendet dieses Format nicht und fügt kein Feld für die Länge von Inhalten ein.