ESA erlebt einen Bounce-Sturm (NDR)

Inhalt

Einführung

In diesem Dokument wird ein Problem beschrieben, bei dem Ihre E-Mail Security Appliance (ESA) einen Bounce-Sturm erfährt und eine Lösung für das Problem bietet.

Hintergrundinformationen

Ein Bounce-Sturm ist eine Nebenwirkung eines Joe-Jobs oder einer Rückstreuung von E-Mail-Spam.

Joe Job

Ein "Joe Job" ist ein Spam-Angriff, bei dem gefälschte Absenderdaten verwendet werden und der darauf abzielt, die Reputation des scheinbaren Absenders zu schädigen und/oder die Empfänger dazu zu bewegen, Maßnahmen gegen den scheinbaren Absender zu ergreifen.

Rückstreuung

Eine Rückstreuung ist eine Nebenwirkung von E-Mail-Spam, Viren und Würmern, bei der E-Mail-Server, die Spam und andere E-Mails empfangen, Bounce-Nachrichten an unschuldige Personen senden. Dies liegt daran, dass der ursprüngliche Umschlagabsender der Nachricht gefälscht ist, um die E-Mail-Adresse des Opfers enthalten zu können. Da diese Nachrichten nicht von den Empfängern angefordert wurden, einander im Wesentlichen ähneln und in großen Mengen zugestellt werden, gelten sie als unerwünschte Massenmail oder Spam. Daher können Systeme, die E-Mail-Rückstreuung generieren, in verschiedenen DNS-Listen (Domain Name System Blacklists) aufgeführt werden und gegen die Nutzungsbedingungen von Internetdienstanbietern verstoßen.

Problem

Ihre ESA erfährt einen Bounce-Sturm, bei dem eine Flut von Nachrichten in die ESA eingespeist wird. Während eines solchen Angriffs treten bei der Anzahl der eingehenden Verbindungen Spitzen auf. Die Appliance kann eine Workqueue-Sicherung entwickeln. Um zu überprüfen, ob die Appliance einem solchen Angriff ausgesetzt ist, überschreiben Sie die E-Mail-Protokolle für die **Von-**Adresse. Bounces (Non-Delivery Reports - NDRs) haben eine leere Umschlagmail **From-**Adresse.

```
ironport.com> grep -e "From:" mail_logs
Mon Oct 20 14:40:55 2008 Info: MID 10 ICID 19 From: <>
Mon Oct 20 14:40:55 2008 Info: MID 11 ICID 19 From: <>
Mon Oct 20 14:40:55 2008 Info: MID 12 ICID 19 From: <>
```

Bei einer Appliance, die einem Bounce-Sturm unterliegt, werden die meisten Nachrichten mit der Umschlagmail **Von-**Adresse **'<>'** angezeigt.

Lösung

Es gibt eine Reihe von Optionen, um einen Bounce-Sturm zu verwalten.

Bounce-Verifizierung

Zur Bekämpfung dieser fehlgeleiteten Bounce-Angriffe bietet AsyncOS die Cisco Bounce-Verifizierung. Wenn diese Funktion aktiviert ist, kennzeichnet diese Funktion die Umschlagabsenderadresse für Nachrichten, die über die ESA gesendet werden. Der Umschlagempfänger für Bounce-Nachrichten, die von der ESA empfangen werden, wird dann auf dieses Tag überprüft. Wenn legitime Bounce-Nachrichten empfangen werden, wird das Tag, das der Umschlagabsenderadresse hinzugefügt wurde, entfernt, und der Bounce wird an den Empfänger gesendet. Bounce-Nachrichten, die das Tag nicht enthalten, können separat behandelt werden.

AsyncOS betrachtet Bounces als E-Mail mit einer **From-**Adresse (**<>**). Nachrichten, die von Adressen wie mailer-daemon@example.com oder postmaster@example.com stammen, gelten nicht als Bounces durch das System und unterliegen nicht der Bounce-Verifizierung.

Adressmarkierungsschlüssel für die Bounce-Verifizierung konfigurieren

Die Liste mit Adressmarkierungsschlüsseln für die Bounce-Verifizierung zeigt Ihren aktuellen Schlüssel und alle zuvor verwendeten, nicht bereinigten Schlüssel an. Gehen Sie wie folgt vor, um einen neuen Schlüssel hinzuzufügen:

1. Im **Mail-Policys > Bounce-Verifizierung** auf **Neuer Schlüssel** klicken.
2. Geben Sie eine Zeichenfolge ein, und klicken Sie auf **Senden**.
3. Bestätigen Sie Ihre Änderungen.

Löschen von Schlüsseln

Sie können die alten Tasten für die Adressmarkierung löschen, wenn Sie im Dropdown-Menü eine Regel zum Löschen auswählen und auf **Entfernen** klicken.

Konfigurieren der Einstellungen für die Cisco Bounce-Verifizierung

Die Bounce-Verifizierungseinstellungen bestimmen, welche Aktion ausgeführt werden soll, wenn ein ungültiges Bounce empfangen wird.

- Auswählen **Mail-Policys** > **Bounce-Verifizierung**.
- Klicken **Einstellungen bearbeiten**.
- Wählen Sie aus, ob ungültige Bounces zurückgewiesen oder der Nachricht ein benutzerdefinierter Header hinzugefügt werden soll. Wenn Sie einen Header hinzufügen möchten, geben Sie den Headernamen und -wert ein.
- Aktivieren Sie optional intelligente Ausnahmen. Bei dieser Einstellung können eingehende E-Mail-Nachrichten und Bounce-Nachrichten, die von internen Mail-Servern generiert werden, automatisch von der Bounce-Verifizierung ausgenommen werden (auch wenn ein einzelner Listener sowohl für eingehende als auch für ausgehende E-Mails verwendet wird).
- Senden und bestätigen Sie Ihre Änderungen.

Konfigurieren der Cisco Bounce-Verifizierung mit der CLI

Sie können die Befehle **bvconfig** und **destconfig** in der CLI verwenden, um die Bounce-Verifizierung zu konfigurieren. Diese Befehle werden im Cisco AsyncOS CLI-Referenzhandbuch behandelt.

Cisco Bounce-Verifizierung und Cluster-Konfiguration

Die Bounce-Verifizierung funktioniert in einer Clusterkonfiguration, solange beide Cisco Appliances den gleichen "Bounce-Schlüssel" verwenden. Wenn Sie den gleichen Schlüssel verwenden, sollte jedes System in der Lage sein, ein legitimes Bounce-Back zu akzeptieren. Das geänderte Header-Tag/Schlüssel ist nicht für jede Cisco Appliance spezifisch.

Mail-Filter

Wenn Sie die Bounce-Verifizierung nicht verwenden können, weil Sie für Empfang und Zustellung separate Appliances verwenden, können Sie einen Nachrichtenfilter einrichten, um Nachrichten mit einer leeren **Von-**Adresse zu blockieren.

Mail-Block

Da diese Bounce-Nachrichten höchstwahrscheinlich über eine nicht vorhandene Umschlagempfängeradresse verfügen, können Sie ungültige Adressen mithilfe der LDAP-Empfängervalidierung (Lightweight Directory Access Protocol) blockieren, um die Auswirkungen solcher Nachrichten zu verringern.