Fehlerbehebung bei unerwünschten ausgehenden E-Mails auf der ESA von kompromittierten Konten

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie Sie die Warteschlangen auf der E-Mail Security Appliance (ESA) beheben und korrigieren können, wenn ein internes Benutzerkonto kompromittiert und weltweit ungesicherte E-Mails versendet wurde.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf AsyncOS 7.6 und höher für die ESA.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Fehlerbehebung

Es empfiehlt sich, das Konto zu sperren, das den Spam sendet, wenn es bekannt ist, andernfalls sperren Sie das Konto, sobald durch die Untersuchung auf der ESA entdeckt wurde.

Workqueue-Checks

Wenn der Arbeitswarteschlangen-Zähler eine große Anzahl von E-Mails enthält und die Anzahl der im System eingehenden E-Mails die Geschwindigkeit, mit der das System verlassen wird, bei Weitem übersteigt, deutet dies darauf hin, dass die Workqueue beeinträchtigt wird. Sie können den Befehl workqueue verwenden, um die Prüfung durchzuführen.

```
C370.lab> workqueue status

Status as of:  Thu Feb 06 12:48:02 2014 GMT
Status:        Operational
Messages:      48654

C370.lab> workqueue rate 5

Type Ctrl-C to return to the main prompt.

Time      Pending    In   Out
12:48:04    48654    48     2
12:48:09    48700    31     0
```

Absender oder Betreff der E-Mails in der Warteschlange ist bekannt

Um die E-Mails zu entfernen, die sich auf die Workqueue auswirken, wird die Verwendung eines Nachrichtenfilters empfohlen. Durch die Verwendung eines Nachrichtenfilters kann die ESA diese E-Mails am Anfang der Warteschlange und nicht am Ende bearbeiten, um beim Entfernen der E-Mails in einem effizienteren Intervall behilflich zu sein.

Dieser Filter kann verwendet werden, um Folgendes zu erreichen:

```
C370.lab> filters


Choose the operation you want to perform:
- NEW - Create a new filter.
- DELETE - Remove a filter.
- IMPORT - Import a filter script from a file.
- EXPORT - Export filters to a file
- MOVE - Move a filter to a different position.
- SET - Set a filter attribute.
- LIST - List the filters.
- DETAIL - Get detailed information on the filters.
- LOGCONFIG - Configure log subscriptions used by filters.
- ROLLOVERNOW - Roll over a filter log file.
[]> new

Enter filter script.  Enter '.' on its own line to end.

FilterName:
if (mail-from == 'abc@abc1.com')
{
drop();
}
.

OR

FilterName:
```

```
if (subject == "^SUBJECT NAME$")
{
drop();
}
.
```

Prüfung der Lieferwarteschlange

Der Befehl **tophosts** zeigt die aktuell betroffenen Hosts an. In einer Live-Umgebung wird der Host des Empfängers (aktuelle aktive Warteschlange) bei einer großen Anzahl aktiver Empfänger beeinträchtigt. Für diese Ausgabe ist das Beispiel **impactedhost.queue**.

```
C370.lab> tophosts

Sort results by:

1. Active Recipients
2. Connections Out
3. Delivered Recipients
4. Hard Bounced Recipients
5. Soft Bounced Events
[1]>  1

Status as of:                   Thu Feb 06 12:52:17 2014 GMT
Hosts marked with '*' were down as of the last delivery attempt.

                                Active  Conn.     Deliv.       Soft       Hard
#   Recipient Host              Recip.    Out     Recip.    Bounced    Bounced

1   impactedhost.queue          321550     50        440      75568       8984
2   the.euq.queue                    0      0          0          0          0
3   the.euq.release.queue            0      0          0          0          0
```

Wenn es sich bei dem betroffenen Host um eine unbekannte Empfängerdomäne handelt, in der vor dem Entfernen aller E-Mails weitere Informationen erforderlich sind, können die Befehle **Empfänger**, **Showmessage** und **Delecipients** verwendet werden. Der Befehl **showReceients** zeigt die Nachrichten-ID (MID), Nachrichtengröße, Zustellversuche, Umschlagabsender, Umschlagempfänger und den Betreff der E-Mail an.

```
C370.lab> showrecipients

Please select how you would like to show messages:
1. By recipient host.
2. By Envelope From address.
3. All.
[1]> 1

Please enter the hostname for the messages you wish to show.
> impactedhost.queue
```

Wenn die vermutete MID in der Zustellwarteschlange legitim aussieht, können Sie den Befehl **showmessage** verwenden, um die Nachrichtenquelle anzuzeigen, bevor Sie Maßnahmen ergreifen.

```
C370.lab> showmessage

Enter the MID to show.
```

```
[]>
```

Wenn Sie diese E-Mails als Spam bestätigt haben, entfernen Sie sie, und verwenden Sie den Befehl des **Empfängers**. Der Befehl bietet drei Optionen zum Löschen von E-Mails aus der Lieferwarteschlange. Nach Umschlagabsender, Empfänger-Host oder Alle E-Mails in der Zustellwarteschlange.

```
C370.lab> deleterecipients

Please select how you would like to delete messages:
1. By recipient host.
2. By Envelope From address.
3. All.
[1]> 2

Please enter the Envelope From address for the messages you wish to delete.
[]>
```

Proaktive Überwachung und Aktion

In Version 9.0+ AsyncOS auf der ESA ist eine neue Nachrichtenfilterbedingung mit dem Namen Header Repeats Rule (Regel für wiederholte Kopfzeilen) verfügbar.

Header wiederholt Regel

Die Header Repeats-Regel wird als true ausgewertet, wenn zu einem bestimmten Zeitpunkt eine angegebene Anzahl von Nachrichten vorhanden ist:

- Mit dem gleichen Betreff werden in der letzten Stunde erkannt.
- Von demselben Umschlag-Absender werden in der letzten Stunde erkannt.
- header-Repeats(<target>, <threshold> [, <direction>])

Weitere Informationen zu diesem Zustand finden Sie im Online-Hilfe-Handbuch Ihres Geräts.

Melden Sie sich bei der CLI an, und stellen Sie den Filter bereit, um diese Prüfung und die gewünschte Aktion auszuführen. Ein Beispielfilter, um E-Mails zu verwerfen oder einen Administrator zu benachrichtigen, wenn ein Schwellenwert erreicht ist.

```
C370.lab> filters


Choose the operation you want to perform:
- NEW - Create a new filter.
- DELETE - Remove a filter.
- IMPORT - Import a filter script from a file.
- EXPORT - Export filters to a file
- MOVE - Move a filter to a different position.
- SET - Set a filter attribute.
- LIST - List the filters.
- DETAIL - Get detailed information on the filters.
- LOGCONFIG - Configure log subscriptions used by filters.
- ROLLOVERNOW - Roll over a filter log file.
[]> new

Enter filter script.  Enter '.' on its own line to end.
```

```
FilterName:
if header-repeats('mail-from',1000,'outgoing')
{
drop();
}
.
```

OR

```
FilterName:
if header-repeats('subject',1000,'outgoing')
{
notify('admin@xyz.com');
}
.
```

Zugehörige Informationen

- Häufig gestellte Fragen zur ESA: Wie lösche ich Empfänger manuell aus der E-Mail-Warteschlange?
- Technischer Support und Dokumentation - Cisco Systems