¿Qué el mensaje de advertencia detectado “ataque de recopilación de direcciones potencial” significa?

Contenido

Introducción

Este documento describe el mensaje de error del “ataque de recopilación de direcciones potencial” según lo recibido en el dispositivo de seguridad del correo electrónico de Cisco (ESA).

¿Qué el mensaje de advertencia detectado “ataque de recopilación de direcciones potencial” significa?

Los administradores para el ESA han recibido el mensaje de advertencia siguiente de la prevención del ataque de recopilación de direcciones (DHAP):

```
The Warning message is:

Potential Directory Harvest Attack detected. See the system mail logs for more
information about this attack.

Version: 8.0.1-023
Serial Number: XXBAD1112DYY-008X011
Timestamp: 22 Sep 2014 21:21:32 -0600
```

Estas alertas se consideran informativas y usted no debe necesitar tomar ningunas medidas. Un mail server exterior intentó a demasiados beneficiarios inválidos y accionó la alerta DHAP (prevención del ataque de recopilación de direcciones). El ESA está actuando como configurado sobre la base de la configuración de la política del correo.

Éste es el número máximo de beneficiarios inválidos por la hora que el módulo de escucha recibirá de un host remoto. Este umbral representa el número total de rechazos del servidor de los rechazos RAT y de la llamada-a continuación S TP combinados con el número total de mensajes a los beneficiarios inválidos LDAP caídos en la conversación SMTP o despedidos en la cola de trabajo (como está configurado en el LDAP valide las configuraciones en el módulo de escucha

asociado). Para más información sobre configurar DHAP para el LDAP valide las interrogaciones, ven que el “LDAP pregunta” el capítulo del guía del usuario de la Seguridad del correo electrónico.

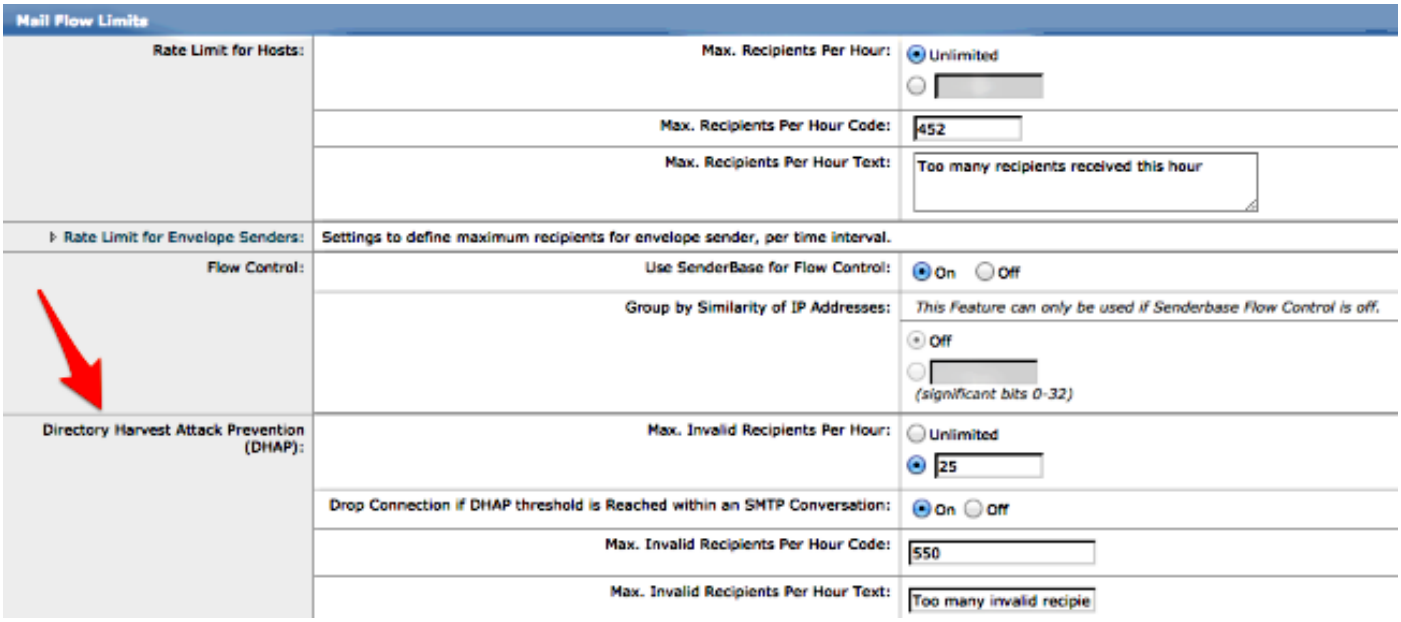
Usted puede ajustar su perfil alerta con el **alertconfig** para filtrar éstos hacia fuera si usted no desea recibir estas alertas:

```
myesa.local> alertconfig

Sending alerts to:
robert@domain.com
Class: All - Severities: All

Initial number of seconds to wait before sending a duplicate alert: 300
Maximum number of seconds to wait before sending a duplicate alert: 3600
Maximum number of alerts stored in the system are: 50

Alerts will be sent using the system-default From Address.

Cisco IronPort AutoSupport: Enabled
You will receive a copy of the weekly AutoSupport reports.

Choose the operation you want to perform:
- NEW - Add a new email address to send alerts.
- EDIT - Modify alert subscription for an email address.
- DELETE - Remove an email address.
- CLEAR - Remove all email addresses (disable alerts).
- SETUP - Configure alert settings.
- FROM - Configure the From Address of alert emails.
[]> edit

Please select the email address to edit.
1. robert@domain.com (all)
[]> 1

Choose the Alert Class to modify for "robert@domain.com".
Press Enter to return to alertconfig.
1. All - Severities: All
2. System - Severities: All
3. Hardware - Severities: All
4. Updater - Severities: All
5. Outbreak Filters - Severities: All
6. Anti-Virus - Severities: All
7. Anti-Spam - Severities: All
8. Directory Harvest Attack Prevention - Severities: All
```

O de la **administración del sistema** GUI **> alerta >** ***direccionamiento receptor*** y modifica la gravedad recibida, o la alerta en su totalidad.

GUI

Para ver sus parámetros de la configuración DHAP del GUI, el tecleo con las **directivas del correo > directivas >** ***tecleo del*** **flujo de correo el nombre de la directiva** ***a editar, o*** **parámetros de la política predeterminada >** y para realizar los cambios a los **límites/a la prevención del ataque de recopilación de direcciones (DHAP) del flujo de correo** seccionar según las necesidades:



Someta y **confíe** sus cambios al GUI.

CLI

Para ver sus parámetros de la configuración DHAP del CLI, el **listenerconfig del** uso **> edita** (*eligiendo el número del módulo de escucha para editar*) **> los hostaccess > valor por defecto** para editar las configuraciones DHAP:

```
Default Policy Parameters
==========================
Maximum Message Size: 10M
Maximum Number Of Concurrent Connections From A Single IP: 10
Maximum Number Of Messages Per Connection: 10
Maximum Number Of Recipients Per Message: 50
Directory Harvest Attack Prevention: Enabled
Maximum Number Of Invalid Recipients Per Hour: 25
Maximum Number Of Recipients Per Hour: Disabled
Maximum Number of Recipients per Envelope Sender: Disabled
Use SenderBase for Flow Control: Yes
Spam Detection Enabled: Yes
Virus Detection Enabled: Yes
Allow TLS Connections: No
Allow SMTP Authentication: No
Require TLS To Offer SMTP authentication: No
DKIM/DomainKeys Signing Enabled: No
DKIM Verification Enabled: No
SPF/SIDF Verification Enabled: No
DMARC Verification Enabled: No
Envelope Sender DNS Verification Enabled: No
Domain Exception Table Enabled: No
Accept untagged bounces: No

There are currently 5 policies defined.
There are currently 8 sender groups.

Choose the operation you want to perform:
- NEW - Create a new entry.
```

```
- EDIT - Modify an entry.
- DELETE - Remove an entry.
- MOVE - Move an entry.
- DEFAULT - Set the defaults.
- PRINT - Display the table.
- IMPORT - Import a table from a file.
- EXPORT - Export the table to a file.
- RESET - Remove senders and set policies to system default.
[]> default

Enter the default maximum message size. Add a trailing k for kilobytes, M for
megabytes, or no letter for bytes.
[10M]>

Enter the maximum number of concurrent connections allowed from a single
IP address.
[10]>

Enter the maximum number of messages per connection.
[10]>

Enter the maximum number of recipients per message.
[50]>

Do you want to override the hostname in the SMTP banner? [N]>

Would you like to specify a custom SMTP acceptance response? [N]>

Would you like to specify a custom SMTP rejection response? [N]>

Do you want to enable rate limiting per host? [N]>

Do you want to enable rate limiting per envelope sender? [N]>

Do you want to enable Directory Harvest Attack Prevention per host? [Y]>

Enter the maximum number of invalid recipients per hour from a remote host.
[25]>

Select an action to apply when a recipient is rejected due to DHAP:
1. Drop
2. Code
[1]>

Would you like to specify a custom SMTP DHAP response? [Y]>

Enter the SMTP code to use in the response. 550 is the standard code.
[550]>

Enter your custom SMTP response. Press Enter on a blank line to finish.

Would you like to use SenderBase for flow control by default? [Y]>

Would you like to enable anti-spam scanning? [Y]>

Would you like to enable anti-virus scanning? [Y]>

Do you want to allow encrypted TLS connections?
1. No
2. Preferred
3. Required
4. Preferred - Verify
5. Required - Verify
[1]>
```

```
Would you like to enable DKIM/DomainKeys signing? [N]>

Would you like to enable DKIM verification? [N]>

Would you like to change SPF/SIDF settings? [N]>

Would you like to enable DMARC verification? [N]>

Would you like to enable envelope sender verification? [N]>

Would you like to enable use of the domain exception table? [N]>

Do you wish to accept untagged bounces? [N]>
```

Si usted hace cualesquiera actualizaciones o cambia, vuelva al prompt principal CLI y **confíe** todos los cambios.

Información Relacionada

- Dispositivo de seguridad del correo electrónico de Cisco - Guías del usuario final
- Soporte Técnico y Documentación - Cisco Systems