

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

Contenido

[Introducción](#)

[GUI](#)

[CLI](#)

[Información Relacionada](#)

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:

Mail Flow Limits	
Rate Limit for Hosts:	Max. Recipients Per Hour: <input checked="" type="radio"/> Unlimited <input type="radio"/> <input type="text"/>
	Max. Recipients Per Hour Code: <input type="text" value="452"/>
	Max. Recipients Per Hour Text: <input type="text" value="Too many recipients received this hour"/>
▶ Rate Limit for Envelope Senders: Settings to define maximum recipients for envelope sender, per time interval.	
Flow Control:	Use SenderBase for Flow Control: <input checked="" type="radio"/> On <input type="radio"/> Off
	Group by Similarity of IP Addresses: <i>This Feature can only be used if Senderbase Flow Control is off.</i>
	<input type="radio"/> Off <input type="radio"/> <input type="text"/> <i>(significant bits 0-32)</i>
Directory Harvest Attack Prevention (DHAP):	Max. Invalid Recipients Per Hour: <input type="radio"/> Unlimited <input checked="" type="radio"/> <input type="text" value="25"/>
	Drop Connection if DHAP threshold is Reached within an SMTP Conversation: <input checked="" type="radio"/> On <input type="radio"/> Off
	Max. Invalid Recipients Per Hour Code: <input type="text" value="550"/>
	Max. Invalid Recipients Per Hour Text: <input type="text" value="Too many invalid recipie"/>

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:

```
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**

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](#)