

Qual è il significato del messaggio di avvertenza "Potential Directory Harvest Attack detected"?

Sommario

[Introduzione](#)

[GUI](#)

[CLI](#)

[Informazioni correlate](#)

Introduzione

Questo documento descrive il messaggio di errore "Potential Directory Harvest Attack" ricevuto su Cisco Email Security Appliance (ESA).

Qual è il significato del messaggio di avvertenza "Potential Directory Harvest Attack detected"?

Gli amministratori dell'ESA hanno ricevuto il seguente messaggio di avviso per la prevenzione degli attacchi di tipo con annidamento del raccolto (DAP):

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
```

Questi avvisi sono considerati di carattere informativo e non è necessario intraprendere alcuna azione. Un server di posta esterno ha tentato di inviare troppi destinatari non validi e ha attivato l'avviso DHCP (Directory Harvest Attack Prevention). L'ESA funziona come configurato in base alla configurazione dei criteri di posta.

Numero massimo di destinatari non validi all'ora che il listener riceverà da un host remoto. Questa soglia rappresenta il numero totale di rifiuti RAT e di rifiuti del server di call-ahead SMTP combinati con il numero totale di messaggi inviati a destinatari LDAP non validi eliminati nella conversazione SMTP o rimbalzati nella coda di lavoro (come configurato nelle impostazioni di accettazione LDAP sul listener associato). Per ulteriori informazioni sulla configurazione di DHCP per le query di accettazione LDAP, vedere il capitolo "LDAP Queries" della [Email Security User Guide](#).

È possibile regolare il profilo di avviso con **alertconfig** per filtrare questi avvisi se non si desidera riceverli:

```
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**

Oppure dalla GUI **Amministrazione di sistema > Alert > Indirizzo destinatario** e modificare la severità ricevuta o l>alert nella sua interezza.

GUI

Per visualizzare i parametri di configurazione DHCP dalla GUI, fare clic su **Mail Policies > Mail Flow Policies > Fare clic sul nome del criterio da modificare o su Default Policy Parameters >** e apportare le modifiche desiderate alla sezione **Mail Flow Limits/Directory Harvest Attack Prevention (DHAP)**:

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 checked="" type="radio"/> Off <input type="radio"/> <input type="text"/> <small>(significant bits 0-32)</small>
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"/>

Inviare e confermare le modifiche alla GUI.

CLI

Per visualizzare i parametri di configurazione DHCP dalla CLI, usare `listener config > edit` (scegliendo il numero del listener da modificare) > `hostaccess > default` per modificare le impostazioni DHCP:

```

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]>

Se si apportano aggiornamenti o modifiche, tornare al prompt della CLI principale ed eseguire il **commit** di tutte le modifiche.

Informazioni correlate

- [Cisco Email Security Appliance - Guide per l'utente](#)
- [Documentazione e supporto tecnico – Cisco Systems](#)