「檢測到的潛在目錄收集攻擊」警告消息表示什麼意思？

目錄

簡介

本檔案介紹在思科電子郵件安全裝置(ESA)上收到的「可能的目錄收集攻擊」錯誤訊息。

「檢測到的潛在目錄收集攻擊」警告消息表示什麼意思？

ESA管理員收到以下目錄收集攻擊預防(DHAP)警告消息：

```
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
```

這些警報被視為資訊性警報，您無需採取任何措施。外部郵件伺服器嘗試了太多無效收件人，並觸發了DHAP（目錄收集攻擊防禦）警報。ESA按照基於郵件策略配置的配置運行。

這是監聽程式每小時從遠端主機接收的最大無效收件人數。此閾值表示RAT拒絕和SMTP Call-Ahead伺服器拒絕的總數，以及被丟棄在SMTP會話中或退回到工作隊列中的無效LDAP收件人的郵件總數（在相關偵聽程式的LDAP接受設定中配置）。 有關為LDAP接受查詢配置DHAP的詳細資訊，請參閱郵件安全使用手冊的「LDAP查詢」一章。

如果不想接收這些警報，可以使用**alertconfig**調整警報配置檔案，以過濾這些警報：

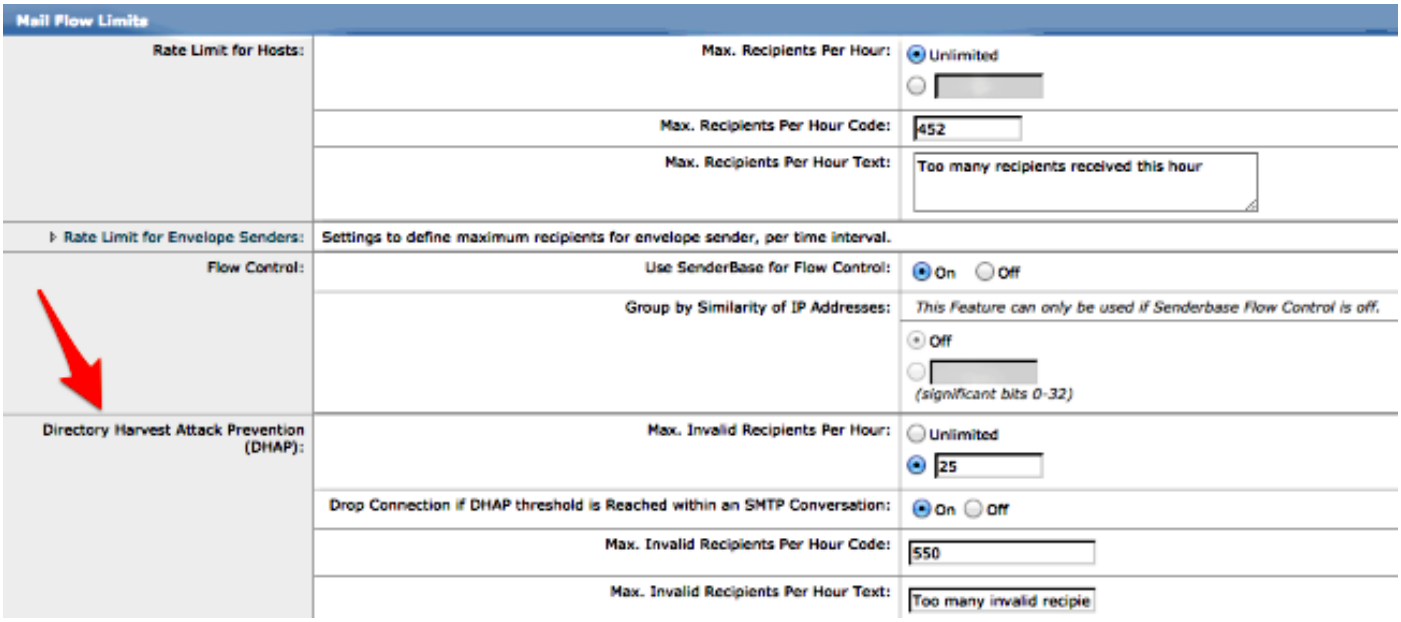
```
myesa.local> alertconfig

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
```

或者從GUI **System Administration > Alerts > *Recipient Address***中，修改嚴重性已接收，或者完整修改警報。

GUI

要從GUI檢視DHAP配置引數，請點選**Mail Policies > Mail Flow Policies > *Click the* Policy Name** to edit，或**Default Policy Parameters >** ，並根據需要更改**Mail Flow Limits/Directory Harvest Attack Prevention(DHAP)**部分：



提交並**提**交對GUI所做的更改。

CLI

要從CLI檢視DHAP配置參數，請使用**listenerconfig > edit**(選擇要編輯的監聽程式的編號)> hostaccess > default編輯DHAP設定：

```
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]>
```

如果您進行任何更新或更改，請返回主CLI提示符並提交所有更改。

相關資訊

- Cisco Email Security Appliance — 最終使用手冊
- 技術支援與文件 - Cisco Systems