警告メッセージ「Potential Directory Harvest Attack detected」は何を意味しますか。

目次

概要

この資料は Cisco E メール セキュリティ アプライアンス (ESA) で受け取られるように「潜在的なディレクトリ収穫攻撃」エラーメッセージを記述したものです。

警告メッセージ「Potential Directory Harvest Attack detected」は何を意味しますか。

ESA のための管理者は次のディレクトリ収穫攻撃防止 (DHAP) 警告メッセージを受け取りました:

```
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
```

これらのアラートは情報と考慮され、処置をとる必要があるべきではありません。 外部メール サーバは余りにも多くの無効 な受信者を試み、DHAP （ディレクトリ収穫攻撃防止) アラートを引き起こしました。 ESA はメール ポリシー 設定に基づいて設定されるように機能しています。

これはリスナーがリモートホストから受け取る 1 時間あたりの無効 な受信者の最大数です。 このしきい値は SMTP メッセージ交換で廃棄されるか、または作業待ち行列で跳ねられる無効 な LDAP 受信者にメッセージの総数によって結合される RATS 拒絶および SMTP コール前方サーバ拒絶の総数を表します (LDAP の設定によって関連するリスナーの設定を受け入れて下さい) 。 LDAP のための DHAP の設定に関する詳細については「LDAP が」E メール セキュリティ ユーザガイドの章を問い合わせることをクエリを、見ます受け入れて下さい。

これらのアラートを受け取りたくない場合これらをフィルタ· アウトするために alertconfig とのアラート プロファイルを調節できます:

```
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
```

または GUI **システム 管理**から **> > *受信者のアドレス* 警告 し**、受け取った重大度を修正するかまたは完全に警告 します。

GUI

GUI からの DHAP コンフィギュレーションパラメータを表示することは、**かデフォルトポリシーパラメータを > *編集し*、メール フロー制限/ディレクトリ**への変更に必要に応じて**攻撃防止（ DHAP ）**セクションを**収穫させます**、**メール ポリシー > メール フロー ポリシー**によってクリックするために **> ポリシー名 *クリックします***:

GUI への変更を**入れ、保存して下さい。**

CLI

CLI からの DHAP コンフィギュレーションパラメータを表示するために、**listenerconfig > Edit を**（ *編集するためにリスナーの数を選択する* ）**>** DHAP 設定を編集する **hostaccess > デフォルト**使用して下さい:

```
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]>
```

更新を行うか、または変更する場合、主要な CLI プロンプトに戻し、すべての変更を**保存して下さい**。

関連情報

- Cisco 電子メール セキュリティ アプライアンス - エンド ユーザ ガイド
- テクニカルサポートとドキュメント - Cisco Systems