ماذا تعني الرسالة التحذيرية "هجوم حصاد الدليل المحتمل"؟

المحتويات

المقدمة

يصف هذا المستند رسالة الخطأ "هجوم حصاد الدليل المحتمل" كما تم تلقيها على جهاز أمان البريد الإلكتروني (ESA) من Cisco.

ماذا تعني الرسالة التحذيرية "هجوم حصاد الدليل المحتمل"؟

تلقى المسؤولون في وكالة الفضاء الأوروبية الرسالة التحذيرية التالية الخاصة بمنع هجوم حصاد الدليل (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
```

تعتبر هذه التنبيهات إعلامية ويجب ألا تحتاج إلى إتخاذ أي إجراء. حاول خادم بريد خارجي إجراء عدد كبير جدا من المستلمين غير الصحيحين وقام بتشغيل تنبيه DHAP (منع هجوم حصاد الدليل). يعمل ESA كمكون استنادا إلى تكوين نهج البريد.

هذا هو الحد الأقصى لعدد المستلمين غير الصحيحين في الساعة التي سيتلقاها المصغي من مضيف بعيد. يمثل هذا الحد العدد الإجمالي لرفض RAT ورفض خادم إستدعاء SMTP بالإضافة إلى العدد الإجمالي للرسائل إلى مستلمي LDAP غير صالحة التي تم إسقاطها في محادثة SMTP أو تم إرجاعها في قائمة انتظار العمل (كما تم تكوينها في إعدادات قبول LDAP على المصغي المقترن). لمزيد من المعلومات حول تكوين DHP ل LDAP قبول الاستعلامات، راجع الفصل "استعلامات LDAP" من دليل مستخدم أمان البريد الإلكتروني.

يمكنك ضبط ملف تعريف التنبيه باستخدام **AlertConfig** لتصفية هذه التنبيهات إذا كنت لا ترغب في تلقي هذه التنبيهات:

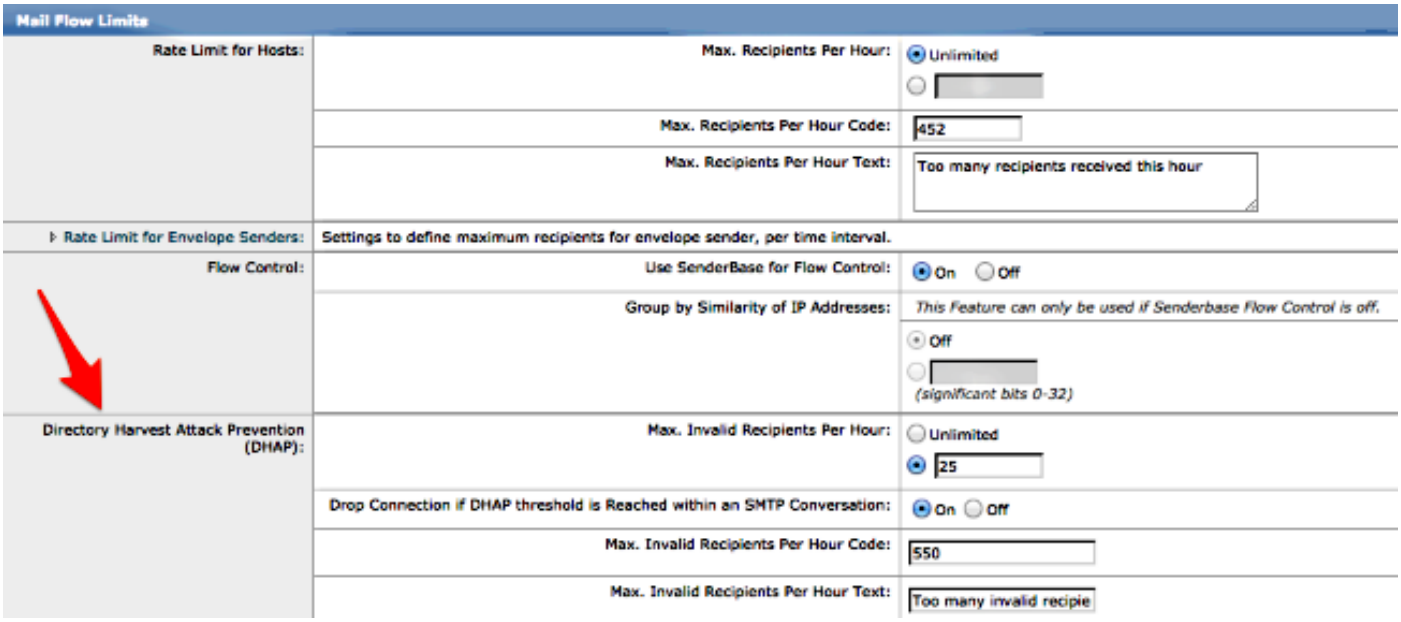
```
myesa.local> alertconfig
```

```
: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
(robert@domain.com (all .1
1 <[]

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

أو من **إدارة نظام** واجهة المستخدم الرسومية (GUI) **> التنبيهات >** ***عنوان المستلم*** وتعديل مستوى الخطورة الذي تم إستلامه، أو التنبيه بأكمله.

واجهة المستخدم الرسومية

لعرض معلمات تكوين DHP الخاصة بك من واجهة المستخدم الرسومية، انقر فوق **سياسات البريد > سياسات تدفق البريد >** ***انقر فوق*** **اسم السياسة** للتحرير، ***أو معلمات السياسة الافتراضية >*** وقم بإجراء تغييرات على قسم **حدود تدفق البريد/منع هجوم الدليل (DHAP)** حسب الحاجة:



قدم التغييرات **التي** أجريتها على واجهة المستخدم الرسومية (GUI) وقم بإلتزامها.

CLI

لعرض معلمات تكوين DHP الخاصة بك من واجهة سطر الأوامر، أستخدم **listEnergyConfig** > **تحرير** (*إختيار رقم المصغي الذي تريد تحريره*) > **hostaccess** > **الإعداد الافتراضي** لتحرير إعدادات DHP:

```
                                    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
Drop .1
Code .2
<[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
No .1
Preferred .2
Required .3
Preferred - Verify .4
Required - Verify .5
<[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
```

إذا قمت بإجراء أي تحديثات أو تغييرات، فارجع إلى مطالبة واجهة سطر الأوامر الرئيسية وقم **بتنفيذ** كافة التغييرات.

معلومات ذات صلة

- جهاز أمان البريد الإلكتروني من Cisco - أدلة المستخدم النهائي
- الدعم التقني والمستندات - Cisco Systems

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).