"Potential Directory Harvest Attack detected" 경고 메시지는 무엇을 의미합니까?

목차

소개

이 문서에서는 Cisco ESA(Email Security Appliance)에서 수신한 "잠재적 디렉토리 수집 공격(Potential Directory Harvest Attack)" 오류 메시지에 대해 설명합니다.

"Potential Directory Harvest Attack detected" 경고 메시지는 무엇을 의미합니까?

ESA의 관리자는 다음 DHAP(Directory Harvest Attack Prevention) 경고 메시지를 받았습니다.

```
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
```

이러한 알림은 정보 제공으로 간주되므로 어떤 조치도 취할 필요가 없습니다.외부 메일 서버에서 잘못된 수신자를 너무 많이 시도하여 DHAP(Directory Harvest Attack Prevention) 알림을 트리거했습니다.ESA는 메일 정책 컨피그레이션에 따라 구성된 대로 작동합니다.

리스너가 원격 호스트로부터 받을 시간당 최대 잘못된 수신자 수입니다.이 임계값은 총 RAT 거부 및 SMTP call-ahead 서버 거부 수와 SMTP 대화에서 삭제되거나 작업 대기열에서 반송된 잘못된 LDAP 수신자에 대한 총 메시지 수를 나타냅니다(관련 리스너의 LDAP 수락 설정에서 구성됨). LDAP 수락 쿼리를 위한 DHAP 구성에 대한 자세한 내용은 Email Security User Guide의 "LDAP Queries" 장을 참조하십시오.

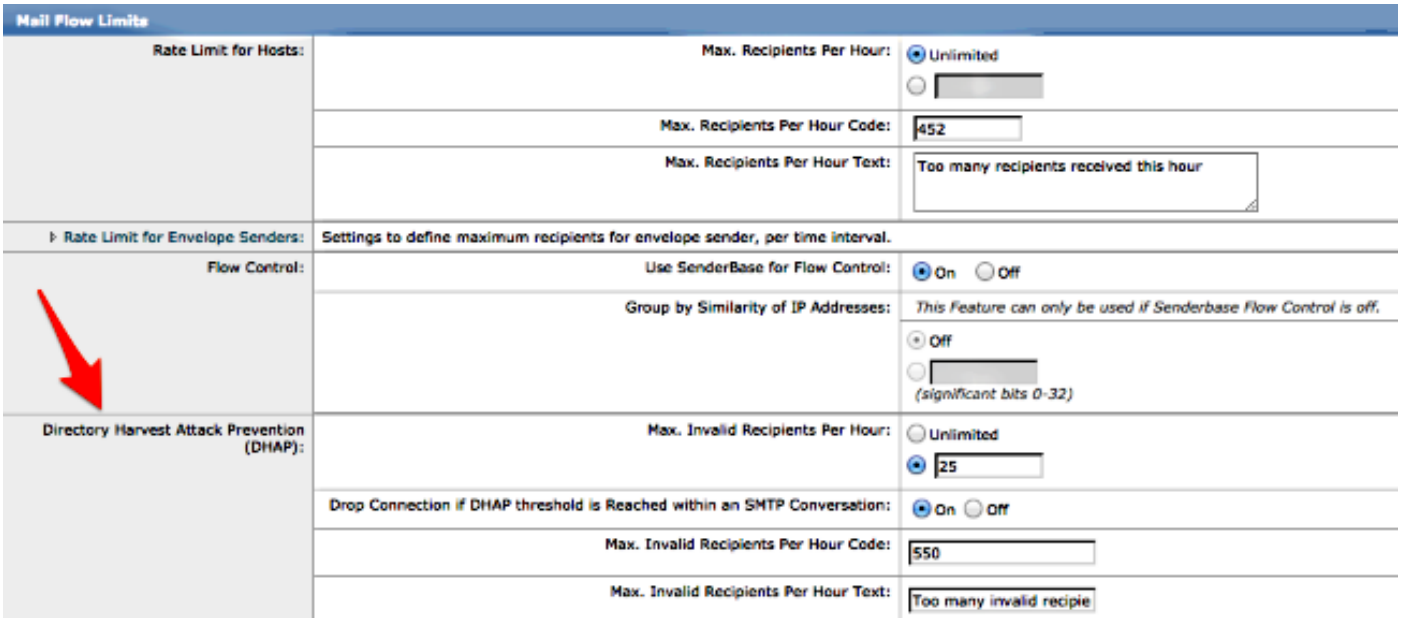
경고 프로필을 alertconfig로 조정하여 다음 알림을 받지 않으려면 이러한 알림을 필터링할 수 있습니다.

```
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
```

또는 GUI **System Administration(GUI 시스템 관리) > Alerts(알림) > Recipient *Address(수신자 주소)***에서 수신한 심각도를 수정하거나 전체 심각도를 수정합니다.

GUI

GUI에서 DHAP 컨피그레이션 매개변수를 보려면 **Mail Policies(메일 정책) > Mail Flow Policies(메일 플로우 정책) > *Policy Name(수정할* 정책 이름)*을*** 클릭하거나 **Default Policy Parameters(기본 정책 매개변수) >**를 클릭하고 필요에 따라 **Mail Flow Limits/Directory Harvest Attprevention (DHAP)** 섹션을 변경합니다.



GUI에 변경 사항을 제출하고 커밋합니다.

CLI

CLI에서 DHAP 컨피그레이션 매개변수를 보려면 listenerconfig **> edit**(*편집할 리스너 번호 선택*)*> hostaccess > default를 사용하여 DHAP* 설정을 편집합니다.

```
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]>
```

업데이트나 변경 사항이 있는 경우 기본 CLI 프롬프트로 돌아가 모든 변경 사항을 커밋합니다.

관련 정보

- Cisco Email Security Appliance – 엔드 유저 가이드
- 기술 지원 및 문서 – Cisco Systems