Que “o mensagem de advertência detectado da colheita do diretório ataque potencial” significa?

Índice

Introdução

Este documento descreve “o Mensagem de Erro do ataque potencial da colheita do diretório” como recebido na ferramenta de segurança do email de Cisco (ESA).

Que “o mensagem de advertência detectado da colheita do diretório ataque potencial” significa?

Os administradores para o ESA receberam o seguinte mensagem de advertência da prevenção do ataque da colheita do diretório (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
```

Estes alertas são considerados informativos e você não deve precisar de tomar nenhuma ação. Um mail server exterior tentou receptores inválidos demais e provocou o alerta DHAP (prevenção do ataque da colheita do diretório). O ESA está atuando como configurado com base na configuração das normas do correio.

Este é o número máximo de receptores inválidos pela hora onde o ouvinte receberá de um host remoto. Este ponto inicial representa o número total de rejeções do server das rejeções do RATO e do atendimento-adiante S TP combinadas com o número total de mensagens aos receptores inválidos LDAP deixados cair na conversação SMTP ou saltados na fila de trabalho (como configurado no LDAP aceite ajustes no ouvinte associado). Para obter mais informações sobre de configurar DHAP para o LDAP aceite perguntas, veem que o “LDAP pergunta” o capítulo do Guia do Usuário da Segurança do email.

Você pode ajustar seu perfil alerta com **alertconfig** para filtrar para fora estes se você não deseja receber estes alertas:

```
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
```

Ou da **administração do sistema** GUI **> alerta >** ***endereço destinatário*** e alteram a severidade recebida, ou alertam-na em sua totalidade.

GUI

Para ver seus parâmetros de configuração DHAP do GUI, clique com as **políticas do correio > políticas >** ***clique do*** **fluxo de correio o nome da política** ***a editar, ou*** **parâmetros da política padrão >** e para fazer mudanças aos **limites do fluxo de correio/diretório colher a** seção da **prevenção do ataque (DHAP)** como necessária:

Submeta e **comprometa** suas mudanças ao GUI.

CLI

Para ver seus parâmetros de configuração DHAP do CLI, o **listenerconfig do** uso **> edita** (*escolhendo o número do ouvinte editar*) **> hostaccess > padrão** para editar os ajustes DHAP:

```
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 você faz quaisquer atualizações ou as muda, retorne à alerta principal CLI e **comprometa** todas as mudanças.

Informações Relacionadas

- Cisco envia por correio eletrónico a ferramenta de segurança - Guias do utilizador final
- Suporte Técnico e Documentação - Cisco Systems