То, что "Потенциальный Каталог Получает Атаку, обнаружило" среднее значение предупреждающего сообщения?

Содержание

Введение

Этот документ описывает "Потенциальное сообщение об ошибках" Атаки Урожая Каталога, как получено на Cisco Email Security Appliance (ESA).

То, что "Потенциальный Каталог Получает Атаку, обнаружило" среднее значение предупреждающего сообщения?

Администраторы для ESA получили следующее предупреждающее сообщение Предотвращения атаки урожая каталога (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
```

Эти предупреждения считают информационными, и вы не должны должны быть принимать любые меры. Внешний почтовый сервер делал попытку слишком многих недопустимых получателей и инициировал DHAP (Предотвращение Атаки Урожая Каталога) предупреждение. ESA действует согласно конфигурации на основе почтовой конфигурации политики.

Это - максимальное число недопустимых получателей в час , который слушатель получит от удаленного хоста. Этот порог представляет общее число отклонений RAT, и отклонения сервера вызова вперед SMTP, объединенные с общим числом сообщений недопустимым получателям LDAP, заглядывали диалогу SMTP или возвратились в рабочем списке

(согласно конфигурации в LDAP, принимают параметры настройки на связанном слушателе). Для получения дополнительной информации о настройке DHAP для LDAP примите запросы, см. "главу" Запросов LDAP Руководства пользователя Безопасности электронной почты.

Если вы не хотите получать эти предупреждения, можно отрегулировать аварийный профиль с **alertconfig** для фильтрования их:

```
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
```

Или от **Администрирования системы** GUI**> Предупреждения>** ***Адрес Получателя*** и модифицирует степени серьезности ошибки , получил, или предупреждение полностью.

GUI

Для просмотра параметров конфигурации DHAP от GUI нажмите через **Почтовую Политику>, Почтовая Политика Потока>** ***Нажимает*** **Policy Name*****, чтобы отредактировать, или*** **Параметры Политики по умолчанию>** и внести изменения в **Почтовое Предотвращение Атаки Урожая Пределов/Каталога Потока (DHAP)** раздел по мере необходимости:

Отправьте и **Передайте** свои изменения GUI.

CLI

Для просмотра параметров конфигурации DHAP от CLI используйте **listenerconfig>, редактируют** (*выбор количества слушателя для редактирования*)**> hostaccess> по умолчанию** для редактирования параметров настройки 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]>
```

При создании каких-либо обновлений или изменений возвратитесь к основному CLI, вызывают и **передают** все изменения.

Дополнительные сведения

- [Устройство безопасности электронной почты Cisco - руководства пользователя]

- Cisco Systems – техническая поддержка и документация