“潜在的目录收获攻击检测的”警告消息是什么意思？

目录

简介

本文在思科电子邮件安全工具(ESA)描述“潜在的目录收获攻击”错误消息如接收。

“潜在的目录收获攻击检测的”警告消息是什么意思？

ESA的管理员接收以下目录收获攻击预防(DHAP)警告消息：

```
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
```

这些警报被认为信息性，并且您不应该需要采取任何行动。外部邮件服务器尝试了许多无效收件人并且触发了DHAP (目录收获攻击预防)警报。ESA作为已配置的根据邮件策略配置。

这是无效收件人最大每个监听程序从远程主机将接收的小时。此阈值代表RATS拒绝和SMTP呼叫向前与消息总数一起的服务器拒绝总数到在工作队列丢弃在SMTP会话或重新启动的无效LDAP收件人(如LDAP所配置的一样请接受在相关的监听程序的设置)。关于配置LDAP的DHAP的更多信息请接受查询，参见“LDAP查询”电子邮件安全用户指南的章节。

如果不希望收到这些警报，您能调节您与**alertconfig的**提醒的配置文件过滤掉这些：

```
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
```

或者从GUI**系统管理>警告>*接收地址***并且修改接收的严重性的或者警告全文。

GUI

要查看您的从GUI的DHAP配置参数，通过**邮件策略>邮件流量策略**单击**>*点击*策略名称*编辑或者*默认策略参数>**和做对**邮件流量限额/目录的**变动**收获攻击预防(DHAP)**部分当必要时：

提交并且**确认**您的对GUI的更改。

CLI

要查看您的从CLI的DHAP配置参数，请使用**listenerconfig > Edit** (*选择监听程序的编号编辑*) **>**编辑DHAP设置的**hostaccess >默认**：

```
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
```

如果做任何更新或更改，请回到主CLI提示符并且**确认**所有更改。

相关信息

- 思科电子邮件安全工具-最终用户指南
- 技术支持和文档 - Cisco Systems