ESA体验反弹(NDR)风暴

目录

简介

本文档描述您的邮件安全设备(ESA)遇到退回风暴时遇到的问题，并提供了解决该问题的解决方案。

背景信息

退回风暴是乔工作或电子邮件垃圾邮件后向散播的副作用。

乔·乔布

Joe作业是一种垃圾邮件攻击，它使用欺骗性发件人数据，旨在损害表观发件人的信誉和/或诱使收件人对表观发件人采取措施。

后向散射

后向散射是电子邮件垃圾邮件、病毒和蠕虫的副作用，接收垃圾邮件和其他邮件的电子邮件服务器向无辜的一方发送退回邮件。这是因为原始邮件信封发件人是伪造的，目的是包含受害者的电子邮件地址。由于这些邮件不是由收件人请求的，彼此大致相似，并且以批量形式发送，因此它们有资格成为未经请求的批量电子邮件或垃圾邮件。因此，生成电子邮件后向散点的系统可能会被列在各种域名系统黑名单(DNSBL)上，并违反互联网服务提供商的服务条款。

问题

您的ESA遇到退回风暴，在这种风暴中，大量邮件注入到ESA。此类攻击期间传入的连接计数峰值。设备可能会开发工作队列备份。要验证设备是否受到此类攻击，请为邮件发件人地址创建邮**件日**

志。退回（非传送报告 — NDR）的信封邮件地址为**空**的。

```
ironport.com> grep -e "From:" mail_logs
Mon Oct 20 14:40:55 2008 Info: MID 10 ICID 19 From: <>
Mon Oct 20 14:40:55 2008 Info: MID 11 ICID 19 From: <>
Mon Oct 20 14:40:55 2008 Info: MID 12 ICID 19 From: <>
```

受退回风暴影响的设备将包含大部分信封邮件发件人地址为“**<>**”**的邮件**。

解决方案

管理退回风暴有许多选项。

退回验证

为了抵御这些错误定向的退回攻击，AsyncOS包括思科退回验证。 启用后，此功能会为通过ESA发送的邮件标记信封发件人地址。然后，检查ESA收到的任何退回邮件的信封收件人是否存在此标记。收到合法退回邮件后，会删除添加到信封发件人地址的标记，并将退回邮件传送给收件人。不包含标记的退回邮件可以单独处理。

AsyncOS将退回视为具有空邮件发件人**地址**(**<>**)的邮件。 来自mailer-daemon@example.com或postmaster@example.com等地址的邮件不被系统视为退回，不受退回验证的约束。

配置退回验证地址标记密钥

“退回验证地址标记密钥”(Bounce Verification Address Tagging Keys)列表显示您当前的密钥和您过去使用的所有未清除的密钥。要添加新密钥，请完成以下步骤：

1. 在 **邮件策略 > 退回验证** ，单击“新**建密钥**”。
2. 输入文本字符串并点击 **提交**。
3. 提交更改。

清除密钥

如果从下拉菜单中选择要清除的规则并单击清除，则可以清除旧地址标记**键。**

配置思科退回验证设置

退回验证设置确定在收到无效退回时要采取的操作。

- 选择 **邮件策略 > 退回验证**。
- 单击 **编辑设置**。
- 选择是拒绝无效退回还是向邮件添加自定义信头。如果要添加信头，请输入信头名称和值。
- （可选）启用智能例外。此设置允许自动免除内部邮件服务器生成的传入邮件和退回邮件的退回验证处理（即使单个侦听程序同时用于传入和传出邮件）。

- 提交并提交更改。

使用CLI配置思科退回验证

您可以在CLI中使用**bvconfig**和**destconfig**命令来配置退回验证。这些命令在《Cisco AsyncOS CLI参考指南》中讨论。

思科退回验证和集群配置

只要两台思科设备使用相同的“退回密钥”，退回验证就可在集群配置中运行。 当您使用相同的密钥时，任何一个系统都应该能够接受合法退回。修改的报头标记/密钥不特定于每个思科设备。

邮件过滤器

如果由于使用单独的接收和传送设备而无法使用退回验证，则可以设置邮件过滤器以阻止邮件地址为空的**邮**件。

邮件阻止

由于这些退回邮件很可能具有不存在的信封收件人地址，因此您可以通过会话轻量级目录访问协议(LDAP)收件人验证阻止无效地址，以帮助降低此类邮件的影响。