ESA DHAP功能支持

目录

简介

本文档介绍如何在思科邮件安全设备(ESA)上启用目录搜集攻击防御(DHAP)功能以防止目录搜集攻击(DHA)。

先决条件

要求

Cisco 建议您了解以下主题：

- 思科ESA
- AsyncOS

使用的组件

本文档中的信息基于AsyncOS的所有版本。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

背景信息

DHA是垃圾邮件发送者用来查找有效电子邮件地址的一种技术。有两种主要技术用于生成DHA的目标地址：

- 垃圾邮件发送者会创建字母和数字的所有可能组合的列表，然后附加域名。

- 垃圾邮件发送者使用标准的字典攻击，并创建一个包含常用名字、姓氏和首字母的列表。

DHAP是思科内容安全设备上受支持的功能，当使用轻量级目录访问协议(LDAP)接受验证时可以启用该功能。DHAP功能跟踪来自给定发件人的无效收件人地址的数量。

一旦发件人超过管理员定义的阈值，该发件人将被视为不受信任，并且来自该发件人的邮件将被阻止，而不会产生网络设计要求(NDR)或错误代码。您可以根据发件人的信誉配置阈值。例如，不可信或可疑的发件人可以具有低DHAP阈值，而可信或可信的发件人可以具有高DHAP阈值。

启用DHAP

要启用DHAP功能，请从内容安全设备GUI导航到**邮件策略 > 主机访问表(HAT)**，然后选择**邮件流策略**。从**Policy Name**（策略名称）列中选择要**编辑的**策略。

HAT具有四个基本访问规则，用于对来自远程主机的连接执行操作：

- **接受**:连接被接受，邮件接受进一步受侦听程序设置的限制。这包括收件人访问表（用于公共侦听程序）。
- **拒绝**:最初接受连接，但尝试连接的客户端收到4XX或5XX问候语。不接受电子邮件。
- **TCPREFUSE**:在TCP级别拒绝连接。
- **中继**:连接被接受。允许接收任何收件人，且不受收件人访问表的限制。域密钥签名仅适用于中继邮件流策略。

在选定策略的**邮件流限制**部分中，通过设置最大值查找并设置**目录搜集攻击防御(DHAP)配置。**每小时无效的收件人数。您还可以选择自定义Max。每小时无效收件人数码和最大值。如果需要，每小时的收件人文本无效。

您必须重复此部分才能为其他策略配置DHAP。

确保在GUI中提交和提交所有更改。

> **注意**：Cisco建议您使用介于5和10之间的最大数**量，作为远程主机设置中每小时无效收件人的最**大数。

> **注意**：有关详细信息，请参阅思科支持门户上的**AsyncOS用户指南**。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。