SenderBase是否在思科邮件安全设备(ESA)上另一个DNS RBL?

目录

问题

SenderBase是否在思科邮件安全设备(ESA)上另一个DNS实时黑洞列表(RBL)?

答案

SenderBase不是普通DNS RBL。在反垃圾邮件社区中，有许多基于DNS的阻止列表。基于DNS的阻止列表是多年来发展起来的一种技术，它提供了一种将标准化API（应用程序编程接口）添加到广泛分布的数据库的方法。由于网络设备（如邮件服务器）都内置有DNS客户端应用程序（有时称为“解析器”），因此使用DNS查找有关IP地址的信息对于大多数系统来说都是非常自然的操作。基于DNS的阻止列表的思想是为分布广泛的用户社区提供一种简便的方法，以便高效地查询面向IP的列表，而不必担心数据库复制、身份验证或更复杂的API。

大多数基于DNS的阻止列表的策略是说明阻止列表的某些描述（例如，“已知为开放中继的系统”），然后允许任何人查询该列表以查看该列表中是否有IP地址。如果地址出现，则列表所有者声称IP地址符合列表上的条件。换句话说，基于DNS的阻止列表是“是/否”答案 — 您是列表中的一员，或者您不是。

志愿者通常管理基于DNS的阻止列表（尽管很少有支付订用方式可用）。 它们的操作也往往非常特别。作为志愿者运营的项目，这些项目由对垃圾邮件问题有强烈感觉的个人或团体运营，并且通常倾向于在拦截合法邮件方面出错。选择使用基于DNS的阻止列表的企业发现这些列表对减少垃圾邮件的效果最低（例如，列表很难上且列表更新不及时），或者发现这些列表会生成非常高的误报率（即，列表太容易）。

创建SenderBase是为了减少基于DNS的阻止列表中的异常行为，并允许网络管理员自行决定使用列表的保守程度或力度。如果正确使用SenderBase，并结合ESA的限制功能，误报率将大大降低。同时，大部分垃圾邮件被排除在公司网络之外。

相关信息

- SenderBase如何工作？
- 技术支持和文档 - Cisco Systems