ESA伪装了邮件筛选

文档ID117796

已更新：钧窑11， 2014

贡献用Nasir Shakour， Cisco TAC工程师。

相关产品

- 思科电子邮件安全工具

目录

简介

本文描述在思科电子邮件安全工具的问题(ESA)遇到，当垃圾邮件和欺骗电子邮件加入到网络时。对此问题的可能的解决方案也描述。

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下列硬件和软件版本：

- 思科ESA所有版本
- AsyncOS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。

问题

欺骗尝试扮演电子邮件。当电子邮件人格化(主旨从)时您的公司员工的成员，可以是特别欺骗的并且有可能性导致混乱。为解决看上去产生从公司的此问题，电子邮件管理员也许尝试阻塞入站邮件(*被伪装的*邮件)的内部。

也许似乎逻辑，如果阻塞从有公司回复地址在域名的互联网的入站邮件，它解决问题。不幸地，当您这样时阻塞邮件，它能同时也阻塞合法电子邮件。参见这些示例：

- 透明地重定向所有简单邮件传输协议(SMTP)流量到ISP邮件服务器的员工传播并且使用旅馆互联网服务提供商。当邮件被发送时，也许看起来流经直接地企业SMTP服务器，但是通过一个第三方SMTP服务器实际上发送，在传送对企业前。

- 员工订阅对电子邮件讨论目录。当信息传送对电子邮件列表时，他们返回给所有用户，表面上从创建人。

- 外部系统用于为了监控外部可见的设备的性能或可接通性。当警报发生时，电子邮件有公司域名在回复地址。第三方服务提供商，例如WebEx，相当频繁地执行此。

- 由于临时网络配置错误，从里边邮件公司通过入站监听程序被发送，而不是出站监听程序。

- 某人在公司外面收到他们转发回到与邮件用户代理的消息(MUA)的公司该用途新建的报头行而不是原始报头。

- 一基于互联网的应用程序，例如**发运页**或Yahoo**电子邮件的**联邦快递公司**此条款**页，创建与回复地址的合法邮件该点回到公司。 邮件合法并且从里边有源地址公司，但是从里边不产生。

这些示例显示，如果阻塞根据域信息的入站邮件，能导致错误肯定。

解决方案

此部分描述您应该进行为了解决此问题的推荐的操作。

应用过滤器

为了避免合法电子邮件消息损耗，请勿阻塞根据域信息的入站邮件。反而，您能标记这些消息类型标题栏，当他们进入网络，表明到收件人消息潜在被伪造。 这可以完成用消息过滤器或用内容过滤器。

这些过滤器的基本策略是检查向后针对性的正文报头行(**从**数据是最重要)，以及RFC 821信封发送方。这些报头行通常在MUA显示并且是很可能由一个欺骗人伪造的那个。

在下一个示例的消息过滤器显示您如何能标记潜在人格化的消息。此过滤器进行数次行动：

- 如果标题栏已经有**“{可能伪造}”**在它，则另一复制没有由过滤器添加。这是重要，当回复在消息流时包括，并且标题栏也许通过邮件网关移动几次，在消息线索完成前。
- 此过滤器搜索信封发送方或**从**有该一个的地址末端在域名**@yourdomain.com的**报头**。**请注意发件人搜索自动地不区分大小写，但是从-报头搜索不是。如果域名在任何一个位置被找到，过滤器插入“{**可能伪造}”在**标题栏尽头。

这是过滤器的示例：

```
MarkPossiblySpoofedEmail:

   if ( (recv-listener == "InboundMail")       AND
        (subject != "\\{Possibly Forged\\}$") )
   {
       if (mail-from == "@yourdomain\\.com$") OR
          (header("From") == "(?i)@yourdomain\\.com$")
       {
           strip-header("Subject");
           insert-header("Subject", "$Subject {Possibly Forged}");
       }
   }
```

另外的测量

由于没有简单方法识别从合法邮件的被伪装的邮件，没有办法完全地消除问题。所以，思科建议您启用IronPort反垃圾邮件扫描仪(集成与AsyncOS)，有效识别欺骗邮件(网络钓鱼)或垃圾邮件并且确实地阻塞它。使用此反垃圾邮件扫描仪，当耦合用在前面部分描述的过滤器，提供最好的结果，不用合法电子邮件损耗。

如果必须识别进入您的网络的欺骗电子邮件，则请考虑使用域密钥识别的邮件(DKIM)技术;它要求更多设置，但是它是一次好测量网络钓鱼和欺骗电子邮件。AsyncOS版本5.5和以上充分地支持DKIM技术。

> **注意**：关于消息过滤器的更多信息，参考在IronPort系统支持页面的**AsyncOS用户指南**。

相关的思科支持社区讨论

思科支持社区是提出和解答问题、分享建议以及与同行协作的论坛。

有关本文档中所用的规则信息，请参阅 Cisco Technical Tips Conventions 。

已更新：钧窑11， 2014
文档ID117796