如何捕获并且阻塞有可执行软件的嵌入式超链接？

目录

问题

如何捕获并且阻塞有可执行软件的嵌入式超链接？

答案

您能使用消息过滤器扫描正文和所有HTML附件。通常，这些电子邮件通过HTML电子邮件进来。 为了扫描引擎能检测它，您必须使用正文包含情况。如果只处理出站邮件，则您能使用‘只正文包含’情况。

下列信息过滤器将寻找该所有长度的超链接与可执行的末端。一旦情况符合，两操作将激活。第一操作将是通知本地管理员通过发送电子邮件对admin@example.com。

第二将是丢弃电子邮件最后的行动。电子邮件不需要是丢弃，反而可以被检疫。 删除下面操作‘drop(); ’能用‘替换(‘’操作); ’

必须定义检疫，否则过滤器引擎不会允许过滤器。您能或者使用默认策略检疫，或者请创建您自己的检疫(请参考的检疫创建或删除检疫的指南)。

```
Block_exe_urls: if body-contains("://\\S*\\.exe(\\s|\\b|$)")
{
notify ("admin@example.com");
drop();
}
```

您能也使用删除坏URL从正文和替换他们用删除的URL的此版本。

```
remove_exe_urls: if body-contains("://\\S*\\.exe(\\s|\\b|$)")
{
edit-body-text("://\\S*\\.exe(\\s|\\b|$)", "URL REMOVED");
}
```

关于关于如何的详细信息说明输入消息过滤器，请查看[我如何添加一个新的消息过滤器到我的思科](#)

IronPort设备？

请参考电子邮件安全工具部分呼叫的策略执行的思科ESA AsyncOS高级用户指南能查看消息过滤器。