根据安全邮件中的TLD阻止邮件中的URL

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景信息](#)

[步骤1.创建过滤器](#)

[步骤2.使用正则表达式](#)

[步骤3.在监控模式下测试](#)

[性能注意事项](#)

[结论](#)

简介

本文档介绍如何根据特定顶级域(TLD)阻止思科安全邮件中的URL。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息基于Cisco Secure Email。

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。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

根据特定TLD阻止URL是保护您的电子邮件系统免受潜在威胁的有效方法。思科邮件安全网关(CES/ESA)会分析URL的信誉，并根据各种标准执行这些信誉。

但是，如果您的公司策略要求阻止某些TLD，此过程将说明如何使用邮件系统中的过滤器和词典来实现此功能。

步骤1.创建过滤器

要阻止整个TLD，您首先需要在邮件系统中创建内容过滤器。此过滤器标识并阻止包含您要限制的

TLD的URL。您可以使用词典管理TLD列表并合并相关正则表达式，从而增强此过程。通过将正则表达式添加到词典，您可以有效地管理和应用过滤条件。

步骤2.使用正则表达式

正则表达式(regex)是识别URL中特定模式的强大工具。

为了有效阻止基于TLD的URL，您可以将这些正则表达式添加到词典。此方法可实现轻松管理和更新您的过滤条件：

1.用于阻止以HTTP或HTTPS开头的URL的正则表达式，包括对Punycode域的支持：

```
(?i)https?:\\\/((xn--\w+\.)|(\w+\.))+(\zip|mov)
```

2.使用电子邮件格式阻止URL的正则表达式，也支持Punycode:

```
(?i)https?:\\\/.*@((xn--\w+\.)|(\w+\.))+(\zip|mov)
```

通过这些正则表达式添加到词典，您可以简化过滤URL的过程，确保您的电子邮件系统有效地阻止指定的TLD。

Dictionary Properties

Name:	<input type="text" value="URL_TLD"/>
Advanced Matching:	☐ Match whole words ☐ Case Sensitive
Smart Identifiers: ?	Match specific patterns such as social security numbers and credit card numbers.

Dictionary

Number of terms: 2

Add Terms:

Separate multiple entries with line breaks.

Weight: ?

Displaying 1 - 2 of 2 items
Page 1 of 1

<< Previous 1 Next >>

Term	Weight	Delete
https?:\\\/((xn--\w+\.) (\w+\.))+(\zip mov)	1	<input type="button" value="Delete"/>
https?:\\\/.*@((xn--\w+\.) (\w+\.))+(\zip mov)	1	<input type="button" value="Delete"/>

注意：如果需要考虑Unicode字符，例如U+2215(/)和U+2044(/)，可能需要对正则表达式进行其他调整。

步骤3.在监控模式下测试

在生产环境中实施这些过滤器之前，建议在监控模式下使用它们。此方法允许您评估过滤器的有效性，而无需立即阻止电子邮件，从而避免您的电子邮件系统遭受任何意外中断。

在监控模式下，系统会记录URL与指定条件匹配的实例，使您能够观察结果并进行必要的调整。为了便于操作，您可以配置日志条目操作，以捕获有关匹配URL的相关信息。例如，您可以使用此日志条目操作：

```
log-entry("URL TLD: $MatchedContent")
```

此操作会记录与您的过滤条件匹配的特定内容，从而提供在过滤器处于活动状态时将阻止的URL的有价值见解。通过查看这些日志，您可以微调正则表达式和字典条目，以确保它们准确捕获预期的URL，而不会影响合法电子邮件。

此外，通过监控一段时间的日志，您可以评估过滤器的性能影响并根据需要进行优化。一旦您确信过滤器按预期运行，就可以从监控模式转换为主动阻止模式：

Content Filter Settings

Name:	<input type="text" value="URL_TLD_Control"/>
Currently Used by Policies:	No policies currently use this rule.
Editable by (Roles):	Cloud Operator, Delegate1, fullaccess
Description:	<input type="text"/>
Order:	<input type="text" value="1"/> (of 124)

Conditions

Order	Condition	Rule	Delete
1	Message Body	body-dictionary-match("URL_TLD", 1)	<input type="button" value="Delete"/>

Actions

Order	Action	Rule	Delete
1	Add Log Entry	log-entry("URL TLD: \$MatchedContent")	<input type="button" value="Delete"/>

性能注意事项

对正则表达式的广泛使用可能会影响电子邮件系统的性能。因此，必须根据需要进行测试和优化。

结论

根据特定TLD阻止URL可以增强邮件系统的安全性。值得注意的是，Google引入的新TLD(例如.zip和.mov)因其与流行的文件扩展名相似而引起了安全担忧。仔细测试您的过滤器，并考虑其对性能的影响，有助于维护一个高效安全的系统。

Google Registry宣布了8个新的TLD:.dad、.phd、.prof、.esq、.foo、.zip、.mov和.nexus。但是，.zip和.mov特别受到关注，因为它们与广泛使用的文件扩展名相似，因此必须在您的安全措施中解决这些问题。

有关.zip TLD安全影响的更多见解，请参阅Talos情报博客文章：[ZIP TLD信息泄漏](#)。该资源进一步说明了与这些TLD相关的潜在风险，并强调了实施适当过滤战略的重要性。

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）。