字里行间：鱼叉式网络钓鱼电子邮件的内容不可知检测

Hugo Gascon[1]、Steffen Ullrich[2]、Benjamin Stritter[3]和 Konrad Rieck[1]

[1]布伦瑞克工业大学
[2]Genua 有限公司
[3]弗里德里希亚历山大大学埃尔朗根努恩贝格

抽象的。鱼叉式网络钓鱼是渗透公司和组织的有效攻击媒介。基于在线提供的大量个人信息，攻击者可以制作看似合法的电子邮件并诱使受害者打开恶意附件和链接。尽管存在反欺骗技术，但它们的采用仍然有限，需要替代的保护方法。在本文中，我们展示了发件人在电子邮件结构中留下了内容不可知的特征。基于这些特征，我们开发了一种方法，能够学习大量发件人的资料，并将欺骗性电子邮件识别为其偏差。我们对来自 16,000 名发件人的 700,000 多封电子邮件评估了我们的方法，并证明它可以区分数千名发件人，以 90% 的检测率识别欺骗性电子邮件，并且在 10,000 封电子邮件中误报不到 1 件。而且，我们表明，个人特征很难猜测，只有当发件人的全部电子邮件可供攻击者使用时，欺骗才会成功。

关键词：鱼叉式网络钓鱼 · 电子邮件欺骗 · 针对性攻击检测

1 介绍

电子邮件是渗透公司和组织的普遍攻击媒介。由于文档和链接在这些环境中和之间通过电子邮件定期交换，因此它们是将恶意有效负载传输给受害者的完美工具 [6, 20]。为了增加成功率，攻击者使用精心制作的电子邮件专门针对组织中的个别成员——这种技术被称为鱼叉式网络钓鱼。例如，攻击者可能会选择一个合适的主题，使用正确的措辞并欺骗一个知名的发件人，以使收件人相信电子邮件的真实性 [16]。这些有针对性的攻击比常规网络钓鱼或垃圾邮件活动更先进，因为它们会根据受害者的环境和行为进行单独调整。因此，不同的鱼叉式网络钓鱼攻击之间几乎没有相似之处，因此很难构建有效的防御措施。

尽管用户越来越意识到他们面临的风险，但他们不得不依赖电子邮件客户端提供的提示来检测欺骗性内容。在默认设置中，多个客户端，如 Microsoft Outlook 和 Mozilla Thunderbird，

仅显示用于识别发件人的少量信息，例如 From 和 Reply-To 字段。来自未知发件人的电子邮件可以被相应地标记和专门处理，但是这些和其他字段可以被伪造，这使得即使是熟练的用户也很难区分合法内容和精心设计的攻击 [5, 34]。虽然这些字段的不一致组合可以很容易地被检测到并用于通知用户潜在威胁，但如果所有字段都被对手正确调整，情况就会变得具有挑战性，这样电子邮件的内容和标题就显得完全合法.

发件人政策框架 [SPF, 24]、域密钥识别邮件 [DKIM, 7] 和最近的域消息身份验证报告和一致性 [DMARC, 25] 等常见反欺骗技术可以帮助验证电子邮件的发件人这个情况。同样，电子邮件的数字签名技术，例如 PGP [4] 和 S/MIME [29]，可以验证发件人。不幸的是，这些技术在实践中仍未得到广泛采用。虽然我们在评估数据中注意到几个带有 SPF 条目的电子邮件域，但在收集到的 700.000 封电子邮件中，只有不到 5% 包含相应的 DKIM 标头甚至数字签名。此外，所有这些技术都需要在发送方实施，如果不是所有通信方都采用该技术，就很难防止欺骗[13, 28]。因此，如果攻击者能够准确匹配已知发件人的地址， 用户无法检测到攻击，可能会被诱骗打开恶意文件或链接。

因此，需要替代方法来保护用户免受针对性很强的鱼叉式网络钓鱼电子邮件的侵害。在本文中，我们提出了一种方法，该方法能够在不依赖其内容的情况下验证与已知发件人地址完全匹配的电子邮件是否真正来自其合法来源。我们的方法建立在发件人在电子邮件结构中留下特征的观察之上，这些特征独立于文本内容并且经常随着时间的推移而持续存在。这些特征在发件人之间存在显着差异，反映了用户行为、电子邮件客户端和传递路径的特性，例如特定的标头组合、编码格式和附件类型。基于这一观察，我们开发了一种检测方法，该方法接收用户的邮箱作为输入，并应用机器学习技术为邮箱中的所有发件人生成配置文件，即使只有少数电子邮件可用。 这些配置文件提供了与发件人内容无关的视图，使我们能够发现欺骗性电子邮件与学习配置文件的偏差。

我们根据经验评估了我们对来自 12 个不同域的 92 个邮箱集合的方法，涵盖了来自 16,000 个发件人的 700,000 多封电子邮件。我们证明，我们的方法可以区分一个邮箱中的数千个发件人，并能够以 90% 的检测率识别欺骗性电子邮件，并且在 10,000 封电子邮件中误报率低于 1 起。此外，我们可以证明，在收件人端观察到的发件人的个人特征很难猜测，并且只有当对手知道发送给收件人的发件人的全部电子邮件时，欺骗尝试才会成功。尽管我们的方法通常不能排除由于电子邮件泄露而导致的欺骗，但它大大提高了针对性攻击的门槛

```
返回路径：<john@doe.com>
收到：来自［93.184.216.34］（ HELO example.com ）例
    如。 COM 与 ESMTP id 69815728;
    2017 年 5 月 16 日星期二 14:06:48 +0200
致：简●迪 <jane@example.com>
日期：2017 年 5 月 16 日星期二 14:00:02 +0200
消息 ID：<20170516133920.23212@doe.com> 主题：
安全会议
来自：约翰●多伊 <john@doe.com>
在回复中：<1405590537$56fe@example.com>
MIME 版本：1.0
内容类型：多部分/混合；边界=“边界”

– 边界
内容 – 类型：文本/纯文本

为了您的兴趣：https://tinyurl。 com / yao533fn

– 边界
内容类型：应用程序/八位字节流； name =
“x.exe” Content-Transfer-Encoding: base64

TVq BODYAAAAEAAA //8 AALg AAAAAAAAAQAAAAAAAAAKCkdy ZWV
aW5ncywgUmV2aWV3ZXIhCsKvXF8o44OEKV8vwq8KCg==
– 边界 –
```

图 1：作为运行示例的简化电子邮件。

并且——在没有广泛部署的服务器端解决方案的情况下——为鱼叉式网络钓鱼攻击的目标公司和组织提供有效保护。

总之，我们做出以下贡献：

- *典型的发件人资料：*我们识别特征，使我们能够在不依赖文本内容的情况下描述电子邮件发件人的特征。生成的配置文件具有足够的表现力来区分数千个发件人，同时考虑到单个电子邮件的多样性。
- 鱼叉式网络钓鱼电子邮件的检测：我们演示了如何使用学习到的发件人资料来识别欺骗性电子邮件，并在实践中没有更强大的服务器端解决方案的情况下帮助降低鱼叉式网络钓鱼攻击的风险。
- *评估和规避实验：*我们通过一系列越来越不利的场景来评估我们的方法的性能，在这些场景中，攻击者通过获取有关目标的更多信息并建立更好的欺骗发件人模型来变得更强大。

本文的其余部分组织如下：在第 2 节中，我们介绍了电子邮件结构中可观察到的特征，并在第 3 节中描述了如何使用这些特征来为发件人构建配置文件。我们在第 4 节中评估了由此产生的检测方法，并在第 5 节中讨论了它的影响和局限性。相关工作在第 6 节中进行了回顾，第 7 节总结了本文。

2 电子邮件结构中的特征

欺骗邮件的识别是网络安全的一个具有挑战性的问题。攻击者几乎可以任意操纵电子邮件的结构和内容，从简单的欺骗性 From 字段到精心制作的假 Received 标头序列［参见 30］。在实践中缺乏精确的检测技术，

例如 DKIM 和 DMARC，因此很难区分合法电子邮件和伪造电子邮件。

然而，可用于构建欺骗性电子邮件的自由也可能会反对攻击者并构成障碍。我们认为，在没有详细知识的情况下模仿来自特定发件人的电子邮件并非易事，并且电子邮件结构中的微小违规行为可能为识别鱼叉式网络钓鱼攻击提供有价值的线索。如果攻击者可以访问受害者已知的发件人的电子邮件，她可以简单地复制电子邮件结构，但如果此信息不完全可用，她需要做出很好的猜测，并希望伪造的结构能够很好地模仿原始通信.

为了揭露此类伪造行为，我们确定了可以表征电子邮件发件人的三组特征：首先，在撰写电子邮件时，发件人引入了反映个人偏好和特点的行为特征。其次，电子邮件客户端生成组合特征，识别特定客户端及其配置。第三，电子邮件的传递留下了捕获发送和接收基础设施细节的传输特性。在下文中，我们将更详细地描述这些特征组，并使用图 1 中的简化电子邮件作为贯穿本节的运行示例。

2.1 行为特征

当用户写一封电子邮件时，除了她的写作风格和习惯 [10, 33] 之外，她的一些个人偏好可以体现在电子邮件的结构中。例如，一些发件人经常使用 CC 标头包括收件人，而其他发件人则避免这种情况并且更喜欢直接使用 To 字段来处理所有收件人。同样，发件人在对话中附加到电子邮件的文件类型和数量也不同。虽然这些特征中的一些特征是易变的并且在不同的上下文之间变化，但其他特征可能会随着时间的推移而持续存在并为构建发送者的配置文件提供第一个基础。

对于我们的分析，我们确定了 13 种特征类型，这些特征类型描述了电子邮件结构中发件人的行为，包括

1. 附件的类型、数量和顺序，例如交换多个文档时，
2. 与其他电子邮件和收件人的关系，例如以参考资料的形式和 In-Reply-To 标头，
3. 附加到电子邮件的数字签名和证书以及相应的 PGP 和 S/MIME 字段，以及
4. 主要部分的文本量和电子邮件回复中引用的文本量。

附录的表 4 中提供了所有 13 个功能的完整列表。请注意，这些特征的基数不同，其中一些特征可能在一封电子邮件中出现多次，例如附件的类型，而其他特征只出现一次，例如 MIME 结构的深度。例如，图 1 中的电子邮件显示了可执行文件的附件（第 20 行）和对先前对话的引用（第 10 行）——这两个功能很少结合使用。

2.2 组成特点

电子邮件结构中特征的第二个来源是邮件用户代理（电子邮件客户端），它将提供的地址、文本和附件转换为适合传递的格式。由于电子邮件最初仅限于 ASCII 字符，因此存在大量用于将二进制数据转换为兼容的 ASCII 表示的编码方案 [例如，14、15、23]。这些方案由电子邮件客户端选择，并且在实施中通常略有不同，从而提供表征电子邮件组成的特征。例如，Base64 编码 [23] 不强制固定文本长度，因此客户端在相应文本块的格式上有所不同。类似地，在提供有关客户端及其配置的线索的多部分 MIME 消息的构造中存在一些微小的变化。

对于我们的分析，我们确定了 22 种捕获电子邮件客户端及其配置特性的特征类型，包括

1. 常见标头的类型、顺序和语法，例如 From、To、Subject 和 Message-Id 标头，
2. MIME 部分中标头的类型、顺序和语法，包括诸如内容类型和内容处置，
3. 地址字段的语法，例如姓名和电子邮件地址的格式和引用，
4. 主题字段、地址字段和文件名中的国际字符编码，
5. 文本内容的类型和位置，例如电子邮件中的 HTML 和纯文本部分，
6. 特定于客户端的行为，例如换行符的长度、缺失和多余的字符编码，
7. MIME 结构的个别细节，例如不同 MIME 部分的深度和顺序，以及
8. Message-Id 标头的结构和 MIME 边界的结构。

附录的表 5 中提供了 22 个组成特征的完整列表。虽然仅靠这些特征显然不足以识别攻击，但结合行为和传输特征，它们可以加强对发件人的观察，从而阻止电子邮件地址的欺骗。例如，图 1 中的电子邮件显示了发件人、收件人和主题字段（第 5-9 行）的唯一顺序，这表明一个罕见的电子邮件客户端。此外，Base64 编码的附件使用 60 个字符的行长度（第 23 行）进行格式化。

2.3 运输特点

第三组特征可归因于电子邮件的传递路径。当电子邮件从发送方移动到接收方时，邮件传输代理通常会经过多个跃点，因此结构中会添加不同的标头。这些标头以 Received 标头的形式描述各个邮件跃点，并提供有关可用传递功能的信息，例如传递协议、TLS 或时间

邮件服务器的区域。这些标头和功能再次生成一系列特征，有助于区分不同的发件人并发现交付过程中的违规行为。

尽管攻击者可以在发送电子邮件之前插入伪造的标头，但无法更改或删除通过传递路径上的跃点添加的标头。因此，攻击者只能通过直接连接到接收服务器或尝试在交付过程中尽早注入电子邮件来伪造这些标头——这在实践中是一项易于处理但并非易事的任务，因为它需要访问与攻击者试图欺骗的发件人相同的交付基础设施。

我们确定了 11 种传输特征，使我们能够重建电子邮件的传递路径，并发现与同一发件人过去的电子邮件的差异。这些功能包括

1. Received 标头的数量和顺序，其中每个跃点由其主机名的哈希值表示，
2. 交付过程中从第一跳到最后一跳的时区路径，
3. 某些 Received 标头中可用的传递协议和 TLS 功能，
4. 服务器添加的 DKIM 记录的有效性及其与声称的电子邮件发件人的关系，以及
5. 垃圾邮件过滤器或防病毒服务在电子邮件发送过程中添加的非标准标头。

附录中的表 6 提供了所有 11 项传输功能的列表。作为交付过程引入的特征示例，图 1 中的电子邮件包含详细的 Received 标头（第 2-4 行）。此标头定义邮件跃点、传递协议和传递时间。此信息可用于任何通过跃点的邮件，因此可能会泄露给攻击者。然而，我们在第 4 节中表明，仅了解传输特性不足以逃避我们的检测方法，并且攻击者需要访问发送给收件人的原始电子邮件才能成功欺骗发件人。

3 检测方法

配备了三组特征来表征电子邮件的发件人，我们准备使用机器学习技术开发相应的检测方法。学习方法的应用使我们免于为每个发件人手动构建检测规则，从而允许将我们的方法扩展到数千个发件人，正如我们在第 4 节中演示的那样。

3.1 特征提取和嵌入

拟议的特征组提供了有关收件人邮箱中每个发件人的电子邮件结构的详细信息。然而，为了从特征中学习一个概况，我们需要一个可以用于

结合常用的学习方法。作为一种补救措施，我们应用了词袋模型的概念——一种源自信息检索［32］和自然语言处理［21、22］的技术——并使其适应从电子邮件结构中提取的特征。

为此，我们将每个提取的特征表示为一个特征字符串，并构建一个联合集 F，其中包含来自三组特征的所有可观察字符串：

$$F := \text{F behavior} \cup \text{Fcomposition} \cup \text{Ftransport}。$$

利用这个集合 F，我们定义了一个 |F| 维向量空间，它在每个维度上取值 0 或 1。然后通过构建向量 ϕ(e) 将每个电子邮件 e 映射到该空间，这样对于从 e 中提取的每个特征 f，相应的维度设置为 1，而所有其他维度设置为 0。

形式上，这个映射可以为所有电子邮件 M 定义为

$$\phi : M \longrightarrow \mathbb{R}^{|F|}, \quad \phi(e) \longrightarrow (I_f(e))_{f \in F}$$

其中辅助函数 I 简单地表示特征 f 是否存在于 e 中，即

$$I(e)_f = \begin{cases} 1 & \text{如果电子邮件 e 包含特征 f} \\ 0 & \text{否则。} \end{cases}$$

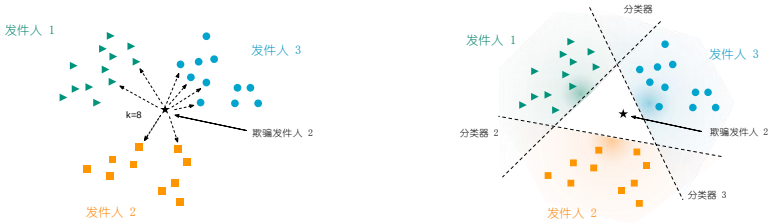
生成的二进制向量空间 $\mathbb{R}^{|F|}$ 允许我们将每封电子邮件表示为包含其发件人特征的向量。在下文中，我们将描述我们如何使用此表示来训练机器学习分类器，该分类器基于这些特征能够将每封电子邮件分配给其相应的发件人并指出可能是欺骗性的电子邮件。

3.2 模型学习和分类

可以应用多种学习方法对向量空间中的数据进行分类。然而，要在我们的环境中运行，学习方法需要满足额外的要求：首先，该方法必须能够在高维向量空间中运行，因为集合 F 可能涵盖数千种不同的特征。其次，该方法需要能够学习分类模型，即使只有很少的训练数据可用，例如只有几封电子邮件。

鉴于这些要求，我们为我们的检测方法选择了以下两种学习方法：（a）k-最近邻分类器（kNN），它可以用很少的训练数据产生良好的分类结果和（b）多类支持向量机器（SVM），以在高维向量空间中有效运行而闻名［见 9］。

K 最近邻分类器 kNN 算法是一种简单而有效的分类学习方法。它计算测试样本与训练集中所有现有样本之间的距离，并通过投票做出决定



(a) kNN 分类器 (b) SVM one-vs-all 分类器

图 2：检测示意图：当分类器的输出与原始发件人地址不匹配时，分类器用于将电子邮件识别为欺骗邮件。

应用权重函数后其 k 个最近样本的标签（参见图 2）。这种基于实例的学习算法不构建明确的学习模型，因此即使发件人只有一封电子邮件也可以应用。对于我们的方法，我们用原始发件人地址的地址标记每个特征向量。当收到一封新电子邮件时，我们计算该样本与所有现有电子邮件的特征向量之间的距离，如下所示

$$d(e_x, e_y) = \|\phi(e_x) - \phi(e_y)\|_1 = \sum_{f \in F} | I_f(e_x) - I_f(e_y) |,$$

其中 d 对应于曼哈顿或 L_1 距离。然后，我们的方法将传入发件人地址与分类器预测之间的不匹配标记为欺骗尝试。

然而，使用很少的训练数据进行预测的优势是有代价的。在做出决定之前需要计算每封新电子邮件与所有现有电子邮件之间的距离，这在大型邮箱上的计算量很大。幸运的是，这个问题可以通过两种方式解决：第一，可以使用特殊的数据结构来实现分类器，以减少距离计算的次数，例如球树和覆盖树 [2]。其次，如果训练实例的数量达到一定限度，可以简单地切换到另一种学习方法，例如支持向量机，或者在可能的情况下，根据保持分类器性能的分布对训练数据进行采样。

多类支持向量机作为第二种学习方法，我们采用线性多类支持向量机算法 [11]。该算法计算一系列最大间隔超平面，将来自一个发件人的电子邮件与所有其他发件人的电子邮件分开（见图 2b）。也就是说，给定 N 个不同的发送者，确定 N 个超平面，每个超平面由向量空间中的向量 $w \in \mathbb{R}^{|F|}$ 和标量 b 表示。

如果收到一封新邮件，我们只需确定所学超平面的位置并选择最匹配的发件人，即

$$h(e) = \langle \phi(e), w \rangle + b = \sum_{f \in F} I_f(e) \cdot w_f + b.$$

请注意，如果特征向量 $\phi(e)$ 是稀疏的，则可以有效地计算此函数，因为只有非零维度 $I_f(e)$ 对输出有贡献。因此，我们可以在从 e 中提取的特征 e 的数量的线性时间内计算 h(e)，分析电子邮件的总体运行时间为 $O(N_e)$。与 kNN 算法相反，线性 SVM 的预测运行时间与训练集的大小无关，因此如果有更多来自特定发件人的电子邮件可用，则这种学习方法是合适的［参见 11］。

4 评估

我们继续在真实世界电子邮件的大型数据集上评估我们的检测方法。特别是，我们有兴趣研究我们的方法根据电子邮件的结构来表征电子邮件发件人的能力，以及在对手的不同知识水平下识别欺骗性电子邮件的能力。在展示这些实验之前，我们首先介绍我们的数据集（第 4.1 节）并定义相应的攻击者模型（第 4.2 节）。

4.1 评估数据

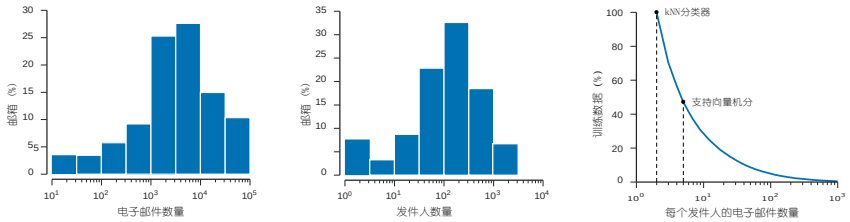
为了进行评估，我们收集了从 12 个不同域（包括企业和商业电子邮件服务）的 92 个邮箱中提取的匿名特征。为了评估我们的检测方法的有效性，我们至少需要一封电子邮件用于学习，一封用于测试-

表 1：评估数据统计。

基础统计			**全部的**邮箱 92 封
电子邮件			760,603 发件人
			17,381 个功能
			617,960
详细统计	**分钟**	**平均**	**最大值**
每个邮箱的电子	2	8,267	50,924
每封电子邮件的功	5	69	44,204
邮箱电子邮件	2	29	10,304

来自每个发件人，最后，只发送了一封电子邮件。我们的最终数据集总共包括所有电子[illegible]个发件人和来自 17,381 个发件人的 760,603 封电子邮件，其中每个发件人至少撰写了两封电子邮件。这些电子邮件由使用第 2 节中定义的特征提取的总共 617,960 个特征描述。表 1 概述了我们评估数据的统计数据。

图 3 更详细地描述了电子邮件和发件人如何在我们的数据集中分布。从图 3a 和 3b 我们可以看到，我们数据集中超过 50% 的邮箱包含 10^3 到 10^4 封电子邮件和 10^2 到 10^3 封不同的发件人。这个庞大的电子邮件语料库为评估我们的方法的性能提供了良好的基础。然而，根据应用的学习模型，我们要求每个发件人的电子邮件数量最少，因此并非所有发件人都可以接受培训。图 3c 显示了可用于学习方法的训练数据量，具体取决于每个发件人的最少电子邮件数量。虽然对于 kNN 分类器，所有发件人都可以用于评估，但对于 SVM 分类器，我们需要将实验限制在 46% 的数据，因为我们至少需要 5 封电子邮件进行训练。



(a) **(b)** **(c)**

图 3：评估数据概览：(a) 电子邮件分布和 (b) 92 个邮箱中的发件人分布；(c) 可用于学习的训练数据，每个发件人的电子邮件不同。

为了准备我们的实验，我们从评估数据中的所有电子邮件中提取特征向量。乍一看，这似乎是一项棘手的任务，因为生成的向量空间有超过 600,000 个维度。然而，这些维度中的大部分为零，每封电子邮件仅包含 5 到 183 个特征（见表 1）。因此，我们可以利用高效的数据结构来处理这些稀疏特征向量［参见 31］。

作为完整性检查我们的表示是否适合学习分类，我们首先研究邮箱中的发件人如何彼此不同，然后分析来自特定发件人的电子邮件如何随时间变化。为此，我们首先计算一个简单的统计数据：对于每个发件人，我们计算其特征向量的平均值，并测量每个邮箱中得到的 17,381 个平均向量之间的距离。我们利用曼哈顿距离（L_1距离）来比较均值向量。距离可以解释为发送者之间不同特征的平均数量，从而提供对提取特征质量的估计。

图 4 显示了每个邮箱中所有发件人之间的曼哈顿距离分布。可以观察到，大多数发件人之间的平均距离大于 40。这表明提取的几个特征是高度特定的，并且捕获了适合区分发件人的电子邮件结构的细微差别。多个来源可能会在发件人的电子邮件特征中引入可变性和噪音，例如软件更新、网络配置和不断变化的设备。因此，我们研究来自单个发件人的电子邮件如何随时间变化。特别是，我们想回答的问题是，与来自同一发件人的现有电子邮件相比，新电子邮件的功能有多少变化。为此，我们测量邮箱中某个时间点收到的每封电子邮件与之前从同一发件人收到的所有电子邮件之间的曼哈顿距离。 然后将不同特征的平均数量表示为特征空间维数的百分比。图 5 显示存在轻微的特征漂移。可以观察到，首先从发件人收到的初始电子邮件中，可变性是如何快速增长的。但是，当收到的电子邮件数量越来越多时，每个类别都会变得更加紧凑，并且新电子邮件中不同功能的平均百分比会降低。请注意，虽然配置文件随着时间的推移变得更加稳定，但它们也往往会有很大差异，如图 4 所示。

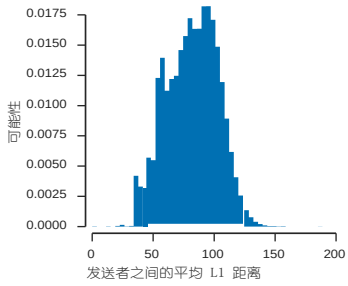


图 4：发送器之间的距离

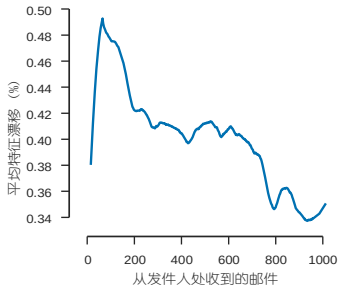


图 5：特征随时间的漂移

作为最后的准备步骤，我们使用相应的电子邮件客户端和传输功能确定 760,603 封电子邮件中是否存在反欺骗技术。表 2 显示了我们数据集中包含反欺骗技术的电子邮件的百分比，其中我们还报告了监控服务 BuiltWith [3] 中列出的前百万个 Web 域的统计数据。尽管目前 SPF [24] 的采用率已接近 40%，但在这两个数据源中，反欺骗技术的总体实施仍然很低。特别是，最近的技术，如 DKIM [7] 和 DMARC [25] 在不到 5% 的电子邮件中使用，从而强调了替代保护措施的必要性。

4.2 攻击者模型

在没有反欺骗技术的情况下，熟练的对手能够伪造电子邮件中包含的大部分数据。然而，我们认为，通过根据电子邮件结构的特征推断发件人资料，攻击者被迫模仿这种资料以有效地伪装成发件人。因此，这种欺骗的成功取决于有多少电子邮件结构的信息可供对手使用，以及攻击者是否可以访问发件人的传递基础设施。

表 2： 我们的评估数据和监控服务 BuiltWith 报告的反欺骗技术。

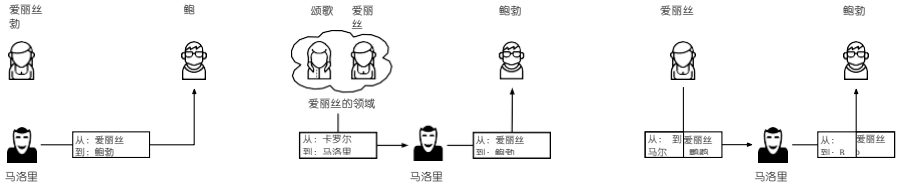
反欺骗技术	我们的数据	前 1M [3]
防晒指数	—	39.9%
金	4.3%	0.1%
DMARC(德国)	—	1.3%
PGP、S/MIME	0.88%	—

因此，我们通过在受控实验中测量攻击者如何通过欺骗发件人资料中越来越多的特征（即从邮箱中特定发件人收到的所有电子邮件中提取的所有特征）来影响检测性能来开始评估我们的方法)。为此，我们首先将邮箱中每个发件人的数据分成训练集和测试集，然后训练 kNN 和 SVM 分类器。为了进行测试，我们从其他邮箱中随机选择电子邮件，并将它们重新标记为目标邮箱的已知发件人，以模仿欺骗尝试。这意味着我们的测试集由 50% 的合法电子邮件和 50% 的欺骗电子邮件组成，其中目标发件人的正确特征的随机百分比。

请注意，要生成欺骗性电子邮件，我们不依赖其文本内容来进行特征提取。此外，我们调整了收件人 MTA 添加到收件人邮箱的传输功能。因此，我们测试集中的欺骗性电子邮件与攻击者发送的真实鱼叉式网络钓鱼电子邮件没有区别，因为没有考虑文本内容。

我们使用真阳性率 (TPR) 和假阳性率 (FPR) 来衡量分类器的检测性能。在我们的设置中，真正的肯定意味着已正确识别欺骗电子邮件，而误报对应于合法电子邮件被错误地标记为欺骗。此外，我们使用接受者操作特征 (ROC) 曲线来呈现两个评估指标，并计算 ROC 曲线下的面积 (AUC) 作为分类性能的数值聚合 [参见 12]。尽管容量不断增加的对手会影响分类器正确识别用户配置文件偏差的能力，但攻击者可用的信息受到现实中可能发生的威胁场景的限制。因此，在这项工作中，我们假设攻击者的知识范围可以从对欺骗发件人一无所知到拥有她的电子邮件的真实示例。

因此，我们通过一系列不断增加的对抗性设置对这些攻击者进行建模，并继续评估我们的方法在每个场景中的性能，如图 6 所示：



(a) 盲目欺骗 **(b)** 已知域 **(c)** 已知发件人

图 6：基于获得的有关欺骗发件人的知识来增强攻击者能力的威胁场景：(a) 攻击者没有关于发件人的信息，(b) 攻击者可以访问从发件人域接收的电子邮件，以及，(c) 攻击者可以访问来自真实发件人的一封或多封电子邮件。

(a) *盲目欺骗：*在这种情况下，攻击者（图 6 中的 Mallory）试图欺骗她没有任何信息的特定发件人。攻击者唯一可用的策略是简单地替换目标电子邮件的 From 和 Return-Path 标头，并尝试猜测行为、组成和传输特征。

(b) *已知域：*在这种情况下，攻击者已收到或有权访问由与欺骗发件人属于同一电子邮件域的发件人发送的一封或多封电子邮件。因此，攻击者可以预期他们的某些传输功能会出现在受害者从她想要欺骗的发件人那里收到的电子邮件中。

表 3：我们的方法在不同威胁场景中的检测性能。

威胁场景	盲目欺骗				已知域				已知发件人			
算法	kNN的		支持向量机		kNN的		支持向量机		kNN的		支持向量机	
公制	FPR	TPR	FPR	TPR	FPR	TPR	FPR	TPR	FPR	TPR	FPR	TPR
	0.01%	90.9%	0.01%	92.4%	0.01%	72.7%	0.01%	78.1%	0.01%	48.1%	0.01%	30.1%
	0.1%	90.9%	0.1%	92.4%	0.1%	72.7%	0.1%	78.2%	0.1%	48.2%	0.1%	30.2%
	1%	91.1%	1%	92.5%	1%	73.7%	1%	79.3%	1%	48.9%	1%	30.4%
	10%	91.9%	10%	92.9%	10%	78.4%	10%	84.1%	10%	53.2%	10%	33.9%

(c) *已知发件人：*在这种情况下，如图 6c 所示，攻击者已收到或有权访问由欺骗发件人发送的一封或多封电子邮件。因此，攻击者可以获得用于构建配置文件的几个特征，并且可以将其合并到她的欺骗性电子邮件中。

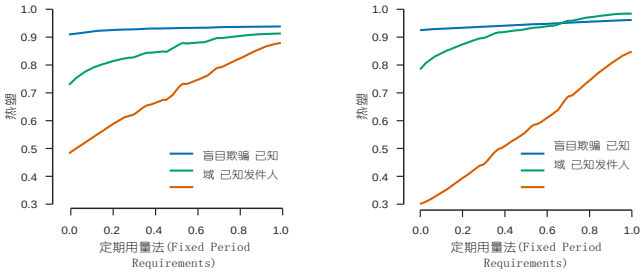
在下文中，我们将描述我们如何了解邮箱中每个发件人的个人资料并将受害者的角色分配给邮箱的所有者。然后，根据每个场景中描述的攻击策略并使用我们数据集中可用的电子邮件，我们为每个发件人构建相应的欺骗电子邮件集，并将它们与合法电子邮件结合起来以评估我们的方法。

4.3 欺骗性电子邮件检测

在下文中，我们评估了我们的方法在上一节中定义的威胁场景中的性能。为了了解每个发件人的个人资料，我们再次开始将所有可用的电子邮件分成训练和测试集。对于培训，我们考虑到某个时间点之前收到的所有电子邮件。在 kNN 分类器的情况下，来自训练集中发件人的一封电子邮件足以对来自该原始地址的传入电子邮件做出决定，而对于 SVM 分类器，我们需要至少 5 封来自发件人的电子邮件来包含此类训练。为了调整每个分类器的参数，我们将训练数据分成 5 个部分，并使用训练/验证分区，这样电子邮件的时间顺序就会被保留——类似于常规的交叉验证。这使我们能够使用过去的数据模拟训练并为尚未见过的数据生成预测。请注意，尽管邮箱或发件人可能没有提供足够的电子邮件进行训练，我们仍然使用这些样本来生成测试欺骗性电子邮件。

对于测试阶段，我们将合法电子邮件的测试集与根据第 4.2 节中描述的攻击者策略制作的一组电子邮件结合起来。在盲目欺骗攻击的情况下，我们选择一组随机的电子邮件发送给与受害者不同域的收件人，并将他们标记为欺骗发件人。同样，我们通过选择由不同发件人从欺骗发件人的域发送给其他收件人的电子邮件来评估已知域攻击。最后，我们选择欺骗发件人发送给不同收件人的电子邮件，在已知发件人攻击的评估中构建欺骗测试集。

在测试期间，我们希望分类器将合法电子邮件分配给其真实类别。相反，应将欺骗性电子邮件分配给任何

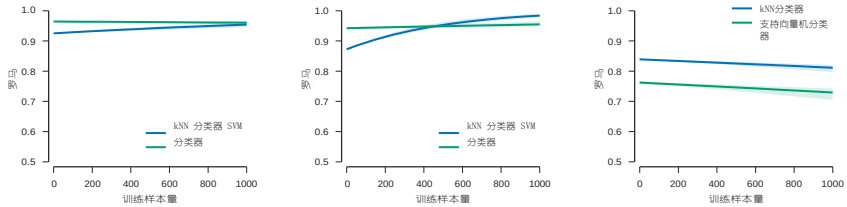


(a) kNN (k=10) **(b) 支持向量机**

图 7：合法电子邮件与具有不同知识水平的攻击者欺骗电子邮件的分类的 ROC 曲线。

其他类别，导致发送电子邮件的发件人地址与分类器的输出不匹配。因此，在检测到欺骗性电子邮件的概率与错误地将合法电子邮件突出显示为欺骗性电子邮件的概率之间存在权衡。图 7 中描绘的 ROC 曲线显示了两个分类器的误报率和误报率之间的权衡。

如果攻击者对欺骗性发件人缺乏任何了解，我们观察到 kNN 和 SVM 分类器可以以 0.01% 的低误报率分别以 90.9% 和 92.4% 的真阳性率识别欺骗性电子邮件。如果攻击者可以访问来自同一域的电子邮件，则性能会下降到 72.7% 和 78.1%，但分类器仍然能够以同样低的误报率有效运行。在最坏的情况下，攻击者有足够的信息来制作一封电子邮件，类似于被欺骗的发件人的学习资料，这会导致分类器的性能显着下降。表 3 以数字方式指定了在所有场景中两个分类器在 0.01%、0.1%、1% 和 10% 的误报率下实现的检测。



(a) 盲目欺骗 **(b)** 已知域 **(c)** 已知发件人

图 8：ROC 曲线下的面积与用于了解每个发件人个人资料的训练电子邮件数量的函数关系。

如上所述，我们为训练 SVM 分类器所需的最少电子邮件数量设置了一个较低的阈值。然而，如图 3 所示，对于许多发件人来说，可以收到大量高于此阈值的电子邮件。图 8 显示了在每个场景中用于训练分类器的来自发件人的电子邮件数量与所有邮箱和发件人的平均 AUC 之间的关系。

如第 4.1 节所述，随着电子邮件数量的增加，发件人资料往往更加紧凑。但是，这可能会根据攻击者可用的知识对性能产生不同的影响。例如，在威胁场景 a）和 b）中，电子邮件被分类为 AUC 超过 0.85，训练样本数量较少。欺骗性电子邮件位于此处，距离发件人配置文件足够远，从而在类别变得更多时导致性能稳定或提高。特别是，SVM 分类器在可用电子邮件数量较少时提供了更好的性能，而随着训练规模的增加，kNN 分类器超过了 SVM。

相反，在威胁场景 c）攻击者始终能够制作类似于欺骗发件人资料的电子邮件，而大量的训练样本会增加发件人资料的可变性。由于每封欺骗电子邮件都非常靠近目标类别或位于目标类别内，因此当样本量增加时，分类器将更难以正确地将合法电子邮件与欺骗尝试区分开来。一种可能的方法

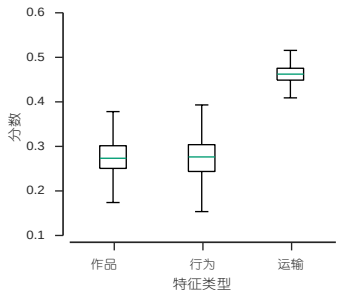


图 9：线性 SVM 分类器在训练期间学习到的每组特征的分数分布。

高风险场景，是在更高的 FPR 点操作分类器，并更频繁地在从最近收到的电子邮件的较小样本上重新训练模型每个发件人。最后，使用线性 SVM 进行分类使我们能够研究学习算法如何根据其对分类的重要性为每种类型的特征分配不同的权重。为此，我们确定归一化 SVM 权重的分布，并按特征类型对它们进行分组。在图 9 中，我们可以观察到，与行为和组合特征相比，传输相关特征对分类器的决策表现出更小的离散和更大的影响。因此，传输特征具有最大的辨别力，同时也是最难伪造的特征，因为即使是熟练的对手也无法在无法访问发送方的相同交付基础设施的情况下完全控制传输特征。

5 讨论与限制

上一节中的评估表明，如果攻击者对电子邮件结构的了解有限，我们的方法能够可靠地区分数千个发件人并识别欺骗性电子邮件。然而，由于在接收方检测欺骗的问题设置，我们的方法有一些固有的局限性，下面将讨论这些局限性。

高级伪造 虽然鱼叉式网络钓鱼和其他有针对性的电子邮件攻击如今侧重于伪造可见特征，例如发件人地址、电子邮件的主题和内容，以模仿可信赖的电子邮件 [18、26]，但我们可能不得不

在不久的将来应对更高级的攻击。如果当前的攻击由于像我们这样的用户意识和检测方法的提高而不再成功，攻击者将调整他们的技术。对于我们的方法，逃避的最佳策略是从原始发件人那里伪造尽可能多的特征。因此，几乎完美的伪造品是原始邮件的副本，包括收件人所观察到的真实传输特征，并添加了一些恶意内容。然而，攻击者需要注意我们的方法检查的几个特征，例如时间戳、接收到的标头中的 IP 地址和附件的特征。在最坏的情况下，攻击者能够伪造所有这些详细信息，因此欺骗性电子邮件的唯一迹象是 IP 地址和主机名之间的轻微不一致。我们的方法在这种情况下失败了，因为只有少数特征与发送者模型不同。尽管如此， 从发件人处获取电子邮件并获取对发件人交付基础设施的访问权限以控制传输功能，显然提高了进行鱼叉式网络钓鱼攻击的门槛。因此，在当前缺乏替代保护方法的情况下，我们的方法是对当前防御的有价值的扩展。

隐私和特征提取我们以隐私友好的方式实现了特征提取，因为发送者、传输者和接收者的所有敏感信息仅通过使用带有随机盐的散列以匿名形式存储。在模型的初始创建或重新训练中，只会保留和使用这些匿名特征。这使得可以在例如接收所有特征向量以供分析但不存储邮件的安全设备中实施该系统。然而，这也意味着不能简单地使用新功能扩展模型并使用旧数据重新训练模型，因为作为特征提取输入的原始邮件不再可用。因此，在每种情况下都在本地执行特征提取。尽管这限制了来自不同来源的匿名数据如何组合进行分析，但收件人的电子邮件信息永远不会离开本地机器，从而避免了隐私问题和可能的攻击媒介。

错误标记的数据训练数据包含欺骗性电子邮件的可能性不容忽视。然而，由于其本质，鱼叉式网络钓鱼电子邮件在发送给收件人的所有电子邮件中的流行率非常低。这个问题被称为标签噪声 [见 8]，这意味着训练样本可以被认为在训练期间受到加性噪声的影响，并且它们的标签有可能被翻转。然而，在我们的设置中，这种概率将非常低，并且在测试这种不常见示例的过程中产生的影响虽然存在，但可以忽略不计。

6 相关工作

检测不需要的和恶意的电子邮件是安全研究中一个公认的问题。在过去几年中设计了几种与我们的方法相关的方法，我们将在下面简要讨论。

例如，存在几种侧重于电子邮件内容及其编写风格的方法 [例如，10、17、33]。背后的假设

这些特征是一个发件人的写作风格与另一个发件人的写作风格有很大不同，并且攻击者很难以与她试图欺骗的发件人相同的风格写一封邮件。这种基于内容的特征的实现可以像使用 5 克分词器 [27] 一样简单，但也可以更复杂，包括字符分布、非典型词或更高级的文体特征 [10、17、33]。在许多情况下，这些文体特征与其他行为特征结合使用，例如写作时间。

虽然这些方法可能提供对欺骗性电子邮件的良好检测，但它们存在两个问题。首先，如果来自原始发件人的文本可从任何来源获得，则文体特征很容易伪造，其次，此类方法需要足够的数据来推断文体的微小差异，并且计算量大。因此，以前的工作通常使用小型数据集。例如，林等人。 [27] 由于缺乏可用数据，仅对 6 个发送者进行了评估。同样，杜曼等人。 [10] 在他们的实验中只区分了 215 个发送者。这些技术是否可以扩展到覆盖数千个发件人尚不清楚，因此用于鱼叉式网络钓鱼检测的应用程序样式特征仍然是一个悬而未决的问题。

Stringhini 和 Thonnard 解决了学习数据有限的问题 [33] 谁提出了一种检测方法，同时也依赖于电子邮件内容，能够分析更大的数据集。然而，他们的方法需要每个发件人至少 1,000 封电子邮件才能有效。此外，他们将防御定位在发件人的服务器上，并要求包括来自不同邮箱的电子邮件，以建立可靠的用户行为档案。这种方法与我们在收件人方面操作的方法是正交的，收件人只需要她自己的邮箱中包含的信息来建立有效的防御。此外，收件人相关的功能是基于这样的想法，即不同的收件人获得鱼叉式网络钓鱼邮件的风险不同。这些特征是由 Amin [1] 提出的，它决定了搜索引擎返回的关于收件人的信息量以及一个人过去收到恶意邮件的频率。毫不奇怪，后者被证明是一个主要特征，即 那些过去经常受到攻击的发件人将来可能也会受到很多攻击。

在我们的工作中，与基础设施相关的特征通常包括传输属性，如发送者 IP 地址或她的地理位置 [17, 27]。但使用过的邮件客户端的功能也属于此类，因为发件人通常只会使用一个或几个电子邮件客户端。与基础设施相关的功能对于同一域中的所有发件人来说通常是相似的，当只有来自特定发件人的几封邮件可用时，可以使用这些功能来提高模型的准确性。与文体特征相比，基础结构特征不模拟实际作者，而只模拟她的环境。因此，无法检测到具有这些功能的被黑帐户。另一方面，基础设施功能需要较少的训练数据来创建性能良好的模型。因此，结合这两种方法的优势可能会有用。基于结构的特征，而不是基于内容的特征是我们评估中的主要特征。 [1] 已经使用了这些功能。 与这项工作相反，我们的方法利用了来自邮件客户端及其传输和

基于这些特征来区分不同的发件人，而不是全局区分所有鱼叉式钓鱼邮件和所有良性邮件。

最后，Ho 等人最近提出的一种方法。［19］侧重于凭证网络钓鱼的识别，旨在识别来自看不见的发件人的攻击。我们的方法与这项工作正交，因为它解决了它的两个主要缺点：首先，Ho 等人。［19］由于 DKIM 和 DMARC 的可用性，认为地址欺骗问题无关紧要。然而，我们的实证分析表明，这两种技术在实践中并未广泛使用，因此需要替代方法。此外，DKIM 和 DMARC 需要在发送方实施，这使攻击者可以选择一个已知的发件人，但不支持此安全功能。其次，所提出的方法要求受害者通过单击链接与网络钓鱼电子邮件进行交互。这会带来严重的安全风险，并可能导致受害者的主机在实际检测到攻击之前就受到威胁。 我们的方法不需要交互，并且可以在网络钓鱼攻击到达受害者之前阻止它们，例如，通过删除电子邮件中的链接和附件。

7 结论

在本文中，我们展示了发件人在电子邮件的结构中留下了几个特征，这是由她的个人偏好、电子邮件客户端和基础设施造成的。基于这些特征，我们提出了一种检测方法，该方法能够学习发件人的配置文件并识别假冒电子邮件，而无需依赖其内容或服务器端实现。在对超过 17,000 名发件人进行的实证评估中，我们证明如果攻击者不知道发件人的资料，这种方法可以识别超过 90% 的欺骗电子邮件，并且在 10,000 封电子邮件中误报少于 1 次。如果攻击者可以访问来自与欺骗发件人相同域的电子邮件，我们的方法仍然可以达到 72% 的检测率，从而提高对手有效完成欺骗攻击的门槛。尽管我们的方法无法检测到拥有大量资源的对手的攻击， 它为无法从特定发件人获取原始电子邮件的攻击者提供了强大的保护。在实践中，我们的方法因此提供了一个有价值的工具来抵御鱼叉式网络钓鱼攻击，如果没有适当的反欺骗检测，这些攻击就会被忽视。

参考书目

[1] R.M.阿明。通过持续威胁和面向收件人的特征的监督分类检测有针对性的恶意电子邮件。博士论文，乔治华盛顿大学，华盛顿特区，美国，2010. AAI3428188.

[2] A. Beygelzimer、K. S. 和 J. Langford。为最近的邻居覆盖树木。在机器学习国际会议（ICML），第 97-104 页，2006 年。

[3] BuildWith 网站。使用技术查找构建。 https://builtwith.com，2017 年 11 月访问。

[4] J. Callas、L. Donnerhacke、H. Finney、D. Shaw 和 R. Thayer。 OpenPGP 消息格式。 RFC 4880（拟议标准），2007 年 11 月。ISSN 2070-1721。由 RFC 5581 更新。

[5] D. D. Caputo、S. L. Pfleeger、J. D. Freeman 和 M. E. Johnson。进行鱼叉式网络钓鱼：探索嵌入式培训和意识。 IEEE 安全与隐私，12(1):28 – 38，2014。

[6] P. Chen、L. Desmet 和 C. Huygens。一项关于高级持续性威胁的研究。 IFIP 国际通信和多媒体安全会议，第 63-72 页。施普林格，2014 年。

[7] D. Crocker、T. Hansen 和 M. Kucherawy。域名密钥识别邮件 (DKIM) 签名。 RFC 6376（互联网标准），2011 年 9 月。ISSN 2070-1721。

[8] N. D. Lawrence 和 B. Schölkopf。在存在标签噪声的情况下估计核 Fisher 判别式。在 ICML，第 1 卷，第 306-313 页，2001 年。

[9] R. Duda、P.E.Hart 和 D.G.Stork。模式分类。 John Wiley & Sons，第二版，2001 年。

[10] S. Duman、K. K. Cakmakci、M. Egele、W. Robertson 和 E. Kirda。EmailProfiler：具有电子邮件标题和文体特征的鱼叉式网络钓鱼过滤。在 COMPSAC，2016 年。

[11] 关于。范，K.-W。张，C.-J。谢，X.-R。王和 C.-J。林。 LIBLINEAR：大型线性分类库。 JMLR，9:1871 – 1874，2008。

[12] T. 福塞特。 ROC 分析简介。模式识别快报，27(8):861 – 874，2006。

[13] I. D. Foster、J. Larson、M. Masich、A. C. Snoeren、S. Savage 和 K. Levchenko。任何其他名称的安全性：关于基于提供商的电子邮件安全性的有效性。在第 22 届 ACM SIGSAC 计算机和通信安全会议记录中，CCS '15，第 450 – 464 页，美国纽约州纽约市，2015 年。 ACM。国际标准书号 978-1-4503-3832-5。 https://doi.org/10.1145/2810103.2813607。

[14] N. Freed 和 N. Borenstein。多用途 Internet 邮件扩展 (MIME) 第一部分：Internet 邮件正文的格式。 RFC 2045（标准草案），1996 年 11 月。ISSN 2070-1721。由 RFC 2184、2231、5335、6532 更新。

[15] N. Freed 和 K. Moore。 MIME 参数值和编码字扩展：字符集、语言和延续。 RFC 2231（拟议标准），1997 年 11 月。ISSN 2070-1721。

[16] S. Gupta、A. Singhal 和 A. Kapoor。关于社会工程攻击的文献调查：网络钓鱼攻击。在计算、通信和自动化 (ICCCA) 中，2016 年国际会议，第 537 – 540 页。 IEEE，2016 年。

[17] F. Han 和 Y. Shen。准确的鱼叉式网络钓鱼活动归因和早期检测。在 SAC，第 2079–2086 页，2016 年。

[18] S. Hardy、M. Crete-Nishihata、K. Kleemola、A. Senft、B. Sonne、G. Wiseman、P. Gill 和 R. J. Deibert。目标威胁指数：表征和量化出于政治动机的目标恶意软件。在 USENIX 安全性中，第 527 – 541 页，2014 年。

[19] G. Ho、U. C. Berkeley、A. Sharma、T. Lawrence、B. National、M. Javed、U. C. Berkeley、V. Paxson、U. C. Berkeley、D. Wagner、U. C. Berkeley、G. Ho 和 A. Sharma。在企业设置中检测凭据鱼叉式网络钓鱼攻击。在 USENIX 安全研讨会上，2017 年。ISBN 9781931971409。

[20] T. M. Inc. 鱼叉式网络钓鱼电子邮件：最受欢迎的 APT 攻击诱饵。技术报告，趋势科技公司，2012 年。

[21] T.约阿希姆斯。使用支持向量机进行文本分类：使用许多相关功能进行学习。技术报告 23，LS VIII，多特蒙德大学，1997 年。

[22] *T.约阿希姆斯。学习使用支持向量机对文本进行分类：方法、理论和算法。 Kluwer 学术出版社，2002 年。*

[23] S.约瑟夫森。 Base16、Base32 和 Base64 数据编码。 RFC 4648（拟议标准），2006 年 10 月。ISSN 2070-1721。

[24] S.基特曼。授权在电子邮件中使用域的发件人政策框架 (SPF)，版本 1。RFC 7208（拟议标准），2014 年 4 月。ISSN 2070-1721。由 RFC 7372 更新。

[25] M. Kucherawy 和 E. Zwicky。基于域的消息身份验证、报告和一致性 (DMARC)。RFC 7489（信息），2015 年 3 月。ISSN 2070-1721。

[26] S. Le Blond、A. Uritesc 和 C. Gilbert。从非政府组织的角度看有针对性的攻击。在 USENIX 安全性中，第 543 – 558 页，2014 年。

[27] E. Lin、J. Aycock 和 M. Mannan。用于检测电子邮件伪造的轻量级客户端方法，第 254-269 页。 Springer Berlin Heidelberg，柏林，海德堡，2012 年。ISBN 978-3-642-35416-8。 https://doi.org/10.1007/978-3_642-35416-8 18.

[28] T. Mori、K. Sato、Y. Takahashi 和 K. Ishibashi。如何使用和滥用电子邮件发件人身份验证？在第 8 届年度协作、电子消息、反滥用和垃圾邮件会议的记录中，CEAS ' 11，第 31-37 页，美国纽约州纽约市，2011 年。ACM。国际标准书号 978-1-4503-0788-8。https://doi.org/10.1145/2030376.2030380。

[29] B. Ramsdell 和 S. Turner。安全/多用途 Internet 邮件扩展 (S/MIME) 版本 3.2 消息规范。 RFC 5751（拟议标准），2010 年 1 月。ISSN 2070-1721。

[30] P.雷斯尼克。互联网消息格式。 RFC 5322（标准草案），2008 年 10 月。ISSN 2070-1721。由 RFC 6854 更新。

[31] K. Rieck、C. Wressnegger 和 A. Bikadorov。 Sally：在向量空间中嵌入字符串的工具。机器学习研究杂志（JMLR），13（十一月）：3247 – 3251，2012 年 11 月。

[32] G. Salton、A. Wong 和 C. Yang。用于自动索引的向量空间模型。 ACM 通讯，18(11):613 – 620，1975。

[33] G. Stringhini 和 O. Thonnard。那不是你：通过行为建模阻止鱼叉式网络钓鱼。在 DIMVA，2015 年。

[34] J. Wang、T. Herath、R. Chen、A. Vishwanath 和 H. R. Rao。研究文章网络钓鱼敏感性：对有针对性的鱼叉式网络钓鱼电子邮件处理的调查。 IEEE 专业交流汇刊，55(4):345 – 362，2012。

A 附录

表 4、5 和 6 分别概述了表征电子邮件的行为、组成和传输的不同特征。

表 4：行为特征列表。

标识符	基数说明		例子
附件类型	n	附件类型	附件类型（图片）
hdr-空	n	具有空值的标头	hdr-空（cc）
hdr-本地域	n	标头指示本地域	hdr-本地域（到：DO）
hdr 相关邮件	n	标题表明与其他电子邮件的关系	hdr-related-
mails(subject:re)	hdr-计数 n hdrcount(cc:1:2+)		标准标头的数量及其值
hdr-x	n	出现非标准标头	hdr-x(x-virus-
scanned) msgid	n	Message-Id头的结构描述	味精（<A.A@H>）
回复	n	Reply-To 标头中的散列发件人	回复(xxx)
反感	1	标头表示重新分配	反感(1)
返回路径	n	返回路径标头中的发件人	返回路径（完整：相同）文
本引用	1	主要部分引用总文本的比例	文本引用（0.3）
来自部分	n	2 克 From 字段	来自部分（xxx：yyy）
从	n	From 标头中的多个发件人	来自（完整：*）

表 5：成分特征列表。

标识符	基数说明		例子
基地64	n	Base64传输编码的特点	base64(linelen(72))
引用打印	n	Quoted-Printable 传输编码的特点 quoted-printable(unencoded-ctrl)	
7位	n	7位传输编码的特点	7位（7位包含-8位）
8位	n	8位传输编码的特点	8bit(长线)
附件扩展	n	附件的扩展	附件分机（doc）
依恋迷信	n	附件类型和扩展名不匹配	附件错误（doc|zip）
附件签名	1	如何指定附件的签名	附件信号（fTnT）
内联扩展	n	处置内联时附件的扩展	内联分机（jpeg）
结节性变性	n	如果没有给出处置，则附件的扩展	结节性扩展（JPEG）
边界	n	MIME边界的结构描述	边界（-= H-H-H）
hdr语法	n	标头的语法格式	hdr 语法（主题：q：ISO-8859-1）
hdr 对	n	标题的成对顺序	hdr 对（来自：日期）
部分HDR对	n	MIME 部分中标头的成对顺序	部分 hdr 对（内容类型：内容 ID）
ua	n	用户代理的简化名称	UA（展望16）
前言	n	MIME 序言摘要	序言（c928c8bf）
哑剧	n	MIME 使用的特点	mime(cd:内联+文件名)
深度	1	MIME 结构的深度	深度(2)
哑剧警告	n	MIME结构中的小问题	MIME 警告（无效内容类型）
哑剧错误	n	MIME结构中的主要问题	mime 错误（paramval 垃圾）
部分路径	n	MIME 部分的路径	部分路径（alt（R）。1：html）
零件尺寸	n	MIME 部分的大小	部分尺寸(html:10:1000)
零件类型	n	MIME 部分的类型	部分类型（图像：base64）

表 6：传输功能列表。

标识符	基数说明		例子
德金	n	DKIM 验证结果	dkim（1：有效），dkim（2：无效）
恢复光盘	1	接收到的标头数	化学气相沉积(13)
rcvd 对	n	先前和当前 Received 标头的哈希值	rcvd 对（xxx:yyy）
recvd-mta	n	给定标题位置的 MTA 功能散列	rcvd-mta(1:XXX)
rcvd源文件	n	给定标题位置的源特征哈希	rcvd-src(2:xxx)
rcvd-tls	n	给定标头位置的 TLS 功能哈希	rcvd-tls(3:xxx)
rcvd-tocc	n	接收标头中 To 字段的出现次数	rcvd-tocc（到：x1）
赫兹	1	来自 Received headers 的时区路径	hdrtz(-0200:+0800)
hdrz成本	1	基于时区变化的运输成本	hdrtz成本(6)
scrip-asn	1	客户端源 IP 地址的 ASN	srcip-asn(8881)
srcip-spf	1	客户端源 IP 地址的 SPF 结果	srcip-spf(spf:通过)