白皮书

有针对性的网络钓鱼

邮件是大多数组织的主要通信媒介。遗憾的是，大部分传入邮件并非组织所需邮件，甚至是恶意邮件。如今，现代垃圾邮件拦截设备几乎可以完全清除绝大多数简单的垃圾邮件活动，因而最终用户的收件箱只会装满合法邮件。然而，根据反信息滥用工作组的调查，事实上超过 85% 的传入邮件中包含垃圾邮件或“滥用邮件”。

为了避开高级反垃圾邮件技术，网络不法分子正在变得更加危险和复杂。除了诱使垃圾邮件收件人购买可疑产品外，利润更加丰厚的“网络钓鱼”攻击还试图搜集用户的个人信息，例如，姓名和地址，甚至个人银行的登录信息。尽管所发送的此类网络钓鱼邮件数量相对来说仍然较少，但数量在不断增加，并且目标受害者面临的危险也很高。随着互联网用户开始越来越熟练地检测出对个人信息进行网络钓鱼的不当尝试，垃圾邮件发送者有选择性地使用专门吸引各个组的内容来缩小其进行网络钓鱼的目标人群。这种社会工程邮件目标性极强，被称为“有针对性的网络钓鱼”或“鱼叉式网络钓鱼”，甚至可以欺骗最精明的互联网用户。

趋势和解决方案

自 20 世纪 90 年代末以来，“网络钓鱼”邮件（旨在欺骗收件人移交登录名和密码等个人信息的邮件）已经大规模发送到邮件收件箱中。“网络钓鱼者”是一群网络不法分子，他们模拟知名在线服务或合法公司的邮件创建邮件，通常一次性发送数百万封邮件，目的是窃取哪怕只是几个收件人的网上银行或其他登录名和密码等信息。

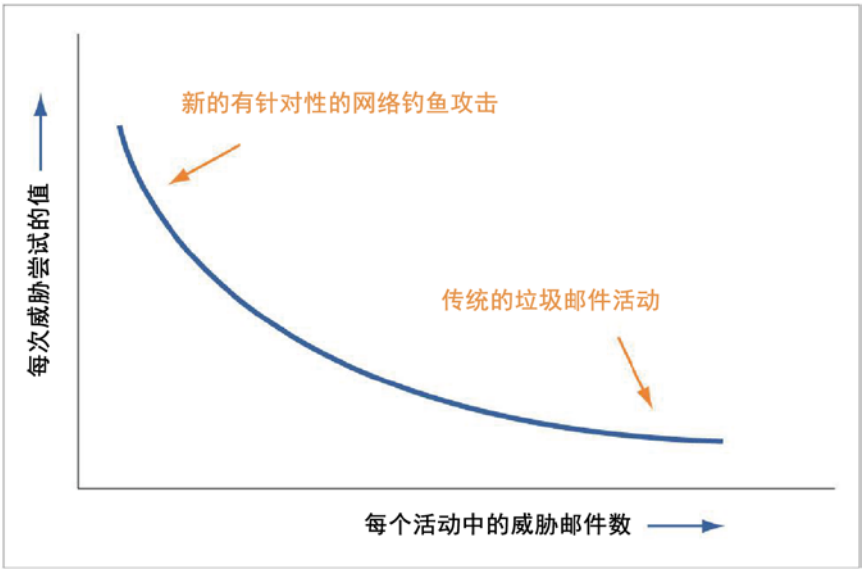
有针对性的网络钓鱼的发展和回报

有针对性的网络钓鱼攻击属于百分比不断增长的邮件传播的攻击，该种攻击以特定组织或一群人为目标。目标对象会收到精心设计的网络钓鱼邮件，旨在索取更深层次的个人数据，例如，有权访问含有敏感信息的公司网络或数据库的登录名和密码信息。除了索取登录信息外，有针对性的网络钓鱼邮件还可以提供恶意软件，例如，用于跟踪受害者键入的所有信息的按键记录程序。

与传统网络钓鱼活动相比，有针对性的网络钓鱼需要网络不法分子投入更多的时间和资金。不法分子需要租用或窃取目标组织或群体的有效邮件地址列表，然后创建可能会诱使收件人提供个人数据的貌似可信的邮件。但是，有针对性的网络钓鱼成功后，不法分子可能会赢得较为丰厚的回报，因而值得他们进行投资。

目前，有针对性的网络钓鱼邮件约占所有网络钓鱼活动的 1%。然而，由于有针对性的网络钓鱼往往仅以组织中的高管为攻击目标，可能会对财务、数据安全和客户关系造成极大的损害。此外，有针对性的网络钓鱼方法具有个性化，因此加大了通过标准反钓鱼技术清除这些邮件的难度，从而导致组织容易受到攻击。

图 1. 传统垃圾邮件活动大批量发送邮件，预计点击率和销售转化率较低。而有针对性的新攻击本质上更为危险，它依赖于少量邮件通过传统垃圾邮件过滤器。



有针对性的网络钓鱼为何有效

促使受害者点击钓鱼网站的技术日益复杂，受害者要么会无意间向不法分子提交敏感信息，要么会在自己的计算机上下载恶意软件。目前，大多数垃圾邮件都包含将收件人定向到恶意网站的 URL。如今，受害者被定向到的欺骗性网站的外观通常与合法站点极为相似。

根据加州大学伯克利分校的研究，从长远来看，常见的互联网用户有时会受到恶意网站的欺骗。为了避免进入网络钓鱼网站，用户必须采用某种策略来持续检查内容的合法性等级、地址栏及其安全设置、浏览器框中的挂锁图像，以及他们被定向到的所有网站的安全证书。

如今，旨在广泛分发列表的网络钓鱼邮件依赖于社会工程技术，例如，需要收件人采取操作的内容，以及跳转到看似合法的网站（如欺骗性的在线银行站点）的内容。但是，这些类型的邮件很少使用邮件中的任何个人数据。

同时，有针对性的网络钓鱼邮件使社会工程达到了一个新水平。通过按名称找到收件人并直接向其邮件地址发送邮件，不法分子逐渐提升恶意邮件以及受害者定向到的虚假网站的可信度。

在以下示例中，企业高管收到了声称来自美国国税局的网络钓鱼邮件，该邮件称正在对其公司进行涉嫌税收欺诈的调查。该邮件发送到了特定人员，并在邮件主体中引用了公司名称。

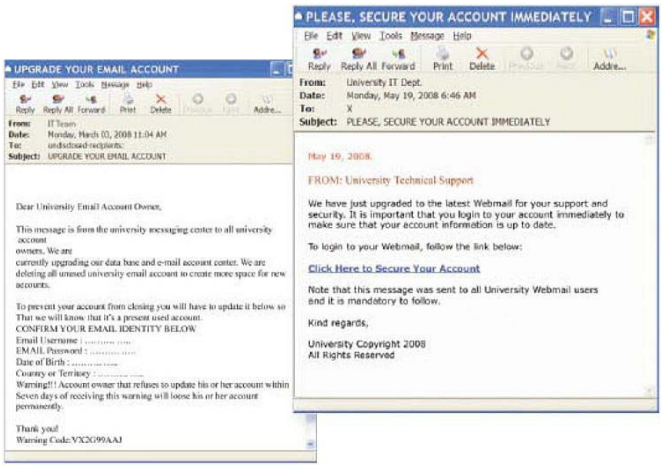
邮件中的 URL 启动了特洛伊木马的可执行文件，这会窃取从收件人邮件浏览器发送的所有交互式数据，并且将访问经过 SSL 加密之前的表单数据。另一封发送给高管的有针对性的网络钓鱼邮件模仿的是 来自美国地方法院的邮件，表面上是传唤收件人出庭一个民事诉讼案例。

图 2. 有针对性的网络钓鱼攻击要求不法分子有效地构建适当的资源并欺骗受害者暴露重要的私有信息。

成功的社会工程

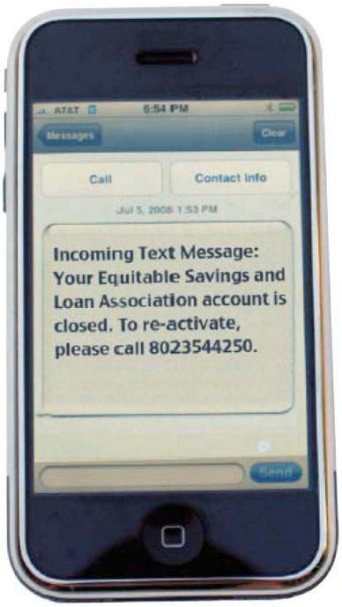
有针对性的网络钓鱼攻击不仅仅针对企业高管。最近许多网络钓鱼活动的邮件据称是从本地银行发送到其客户，要求客户更新其在线帐户或者登录其帐户阅读特定邮件。其他有针对性的攻击看似来自大学 IT 部门，指导邮件用户答复其网页邮件凭据，目的是保留其大学邮件帐户或者利用安全升级。这些不安全的帐户之后可能经常用来发送大规模垃圾邮件活动。

图 3. 有针对性的网络钓鱼邮件示例，据称来自大学 IT 部门，目的是获取邮件凭据。



发送有针对性的网络钓鱼活动的不法分子继续优化其策略，诱使受害者转到欺骗性网站或不安全网站。网络不法分子向手机发送文本邮件甚至已经成了公开的事实。例如，此类攻击针对本地银行所在区域的手机号码，通知客户其帐户因进行可疑活动而被终止，然后指导其拨打某个电话号码重新激活帐户。呼入号码由不法分子设置用来收集帐号和登录凭据。

图 4. 不法分子还设置了自动化系统来收集不知情客户的银行登录信息。



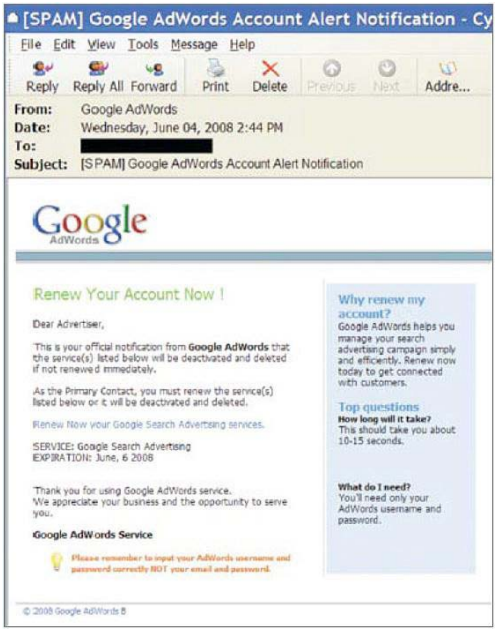
无论有针对性的网络钓鱼攻击如何实施犯罪活动，其目的都是为了收集个人数据，从而让网络不法分子窃取金钱或信息。2007 年，一项有针对性的网络钓鱼活动的发件人几乎成功从一家小型连锁超市 Supervalu Inc. 骗取一千万美元。

在 Supervalu 的案例中，网络不法分子以欺骗手段从两家小型连锁超市供应商 American Greetings 和 Frito-Lay 获取电汇说明。不法分子（装扮成供应商的员工）然后将含有“更新”电汇说明的邮件发送给 Supervalu 员工，指示他们在几天内向不法分子的银行帐户转账一千万美元。

对于 Supervalu 来说，幸运的是，American Greetings 和 Frito-Lay 的员工较为警惕，他们意识到并未收到付款并与 Supervalu 取得了联系。同时，他们可以通知执法机构，将欺骗性的帐户进行冻结。

其他最近的网络钓鱼活动也展示了与这些邮件相关的威胁，事实上，不法分子寻求窃取的数据不只是银行信息。有一项网络钓鱼活动将邮件发送到了美国航空公司的频飞乘客，让这些乘客填写在线调查并为其奖励 50 美元，该调查对收件人保密，目的是获取个人信息。美国航空公司必须向其所有客户发送邮件，提醒他们警惕网络钓鱼邮件。另一项网络钓鱼活动是要求 Google AdWords 客户确认其帐户。如果这些客户这样做，其 Google AdWords 帐户信息（包括金融数据）不仅会被不法分子窃取，而且受害者的 AdWords 流量也会重定向到不法分子的网站。

图 5. 看似与 Google AdWords 帐户相关的邮件欺骗受害者提供登录信息。



即使收件人未对网络钓鱼邮件做出响应因而未受骗，有针对性的网络钓鱼攻击也会对公司及其与客户的关系造成不利影响。

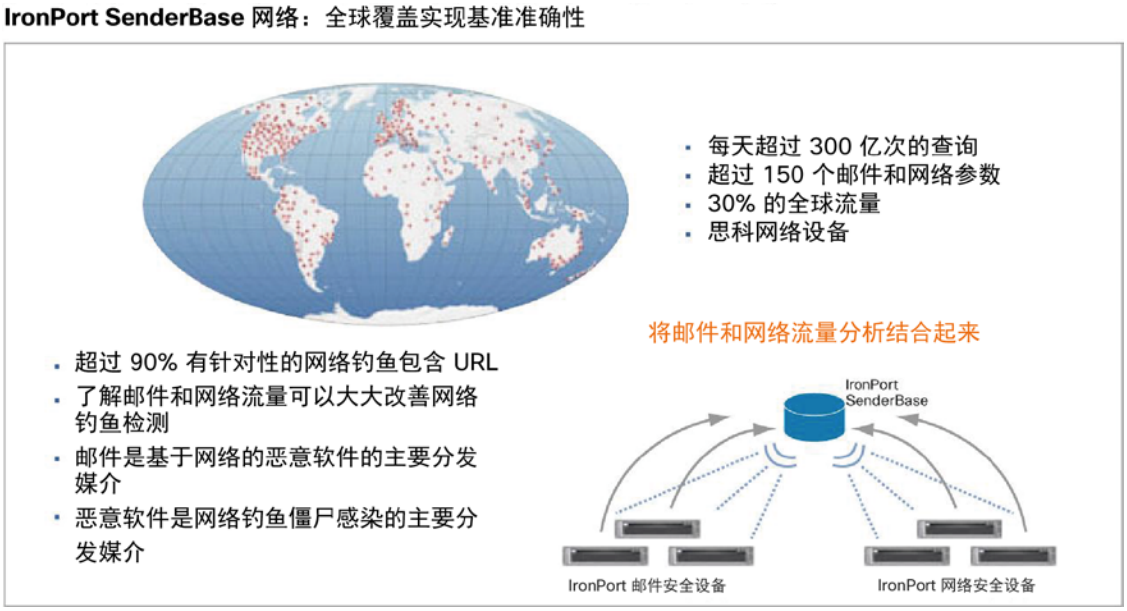
根据 Forrester Research 的调查，收到有针对性的网络钓鱼邮件的高管会对邮件失去信心。在其“Phishing Concerns Impact Consumer Online Financial Behavior”（网络钓鱼问题会影响消费者在线金融行为）报告中，Forrester 发现，26% 的美国消费者将不使用在线金融产品，20% 的消费者将不接收其金融提供商发送的邮件或者不注册在线银行或账单支付，归根结底是因为他们害怕成为网络钓鱼攻击的受害者。

IronPort 如何阻止有针对性的网络钓鱼

IronPort 现在是思科的一部分，其提供了一组不断扩展的复杂技术，可确保最终用户不必担心所查看的邮件是否会非法获取其帐户信息。借助 IronPort® 解决方案，客户可以安全使用邮件和网络，并且免受新型攻击，例如，有针对性的网络钓鱼。IronPort 支持一种多层方法，可以监控全球邮件和网络流量，并使用复杂的 Web 声誉过滤器和高级邮件身份验证技术。

SenderBase：IronPort 的 SenderBase® 网络持续监控超过 30% 的全球邮件和网络流量。SenderBase 使用 IP 地址信息跟踪超过 150 个参数，例如，邮件发送和网站流量、投诉等级、“垃圾邮件陷阱”帐户、DNS 解析、原产地以及是否有黑名单。之后，系统使用收集的数据创建声誉分数，从而指示进入组织的各封邮件邮件的威胁等级，以及每封邮件中包含的 URL。由于 90% 的恶意邮件包含 URL，SenderBase 同时监控网络和邮件流量的独特能力是 IronPort 能有效识别和阻止有针对性的网络钓鱼攻击的关键组件。

图 6. 超过 100,000 个组织参与 SenderBase，形成了世界上最大的邮件和网络流量监控系统。



IronPort 网络声誉过滤器：IronPort 网络声誉过滤器根据每封邮件中每个 URL 包含恶意内容的可能性，将网络声誉分数分配到这些 URL。随后，IronPort 邮件和网络安全设备允许根据这些声誉分数来标记或阻止某些发件人的邮件以及某些网站的流量。

声誉分数基于 SenderBase 数据以及对难以欺骗的 IP 地址数据的额外分析，例如，域名的注册时间、托管站点的国家/地区和/或更改频率，以及声称由财富 500 强公司托管的域实际上是否由该公司托管。

Cisco IronPort 的 SenderBase 网络和声誉过滤器可同时阻止 99% 的网络钓鱼邮件，这主要取决于对 IP 地址及其周围活动的详细了解程度。

SPF 和 DKIM 邮件验证：高级邮件身份验证技术支持将声明的发件人身份与实际发件人身份进行匹配。发件人策略框架（SPF）和域名密钥识别邮件（DKIM）是两种常用的互补式邮件身份验证方法，可以检测欺骗性邮件。这些身份验证技术目前受到业界团队、邮件提供商和企业更广泛的认可，由于其应用范围更加广泛，因而可增强在防御网络钓鱼邮件方面的效能。SPF 和 DKIM 可以分别处理特定的问题，并且可以结合使用来提供分层的安全方法。

SPF 是一种发件人路径身份验证方法，可帮助收件人识别特定域经过授权的邮件服务器，并且确认其收到的邮件实际上来自这些经过授权的来源。使用此技术的邮件发件人（例如 ISP 和公司）发布 SPF 记录，其中指定了允许使用相应名称的主机。SPF 兼容的邮件收件人使用发布的 SPF 记录在邮件事务期间测试发送邮件传输代理的身份是否得到授权。	**DKIM** 是一种基于密码的身份验证方式，可帮助验证并确定来自给定域的邮件的授权。DKIM 提供多邮件标头字段和邮件正文的“密码签名”（或“密钥”）。在 DNS 记录中，DKIM 保护的网络域发布与其自己生成的私有签名密钥相对应的公共密钥（或“域密钥”）。邮件收件人可以使用该密钥来验证邮件标头和正文与发送域的身份是否匹配，从而帮助他们确定邮件是否有可能是网络钓鱼或其他恶意邮件。

SPF 和 DKIM 专门结合使用，在检测有针对性的网络钓鱼邮件时非常有效。根据身份验证和在线信任联盟（AOTA），目前全球范围内所有合法邮件中大约有半数经过身份验证。这种接受级别意味着接收大量垃圾邮件和网络钓鱼邮件的知名高管可能会从基于邮件身份验证失败的其他邮件过滤和阻止工具中受益。

HTML 清理：HTML 清理（也称为 HTML 转换）可对满足预先确定条件的邮件提供额外的保护，例如，当 SPF 和 DKIM 无法验证邮件时。启用 HTML 清理时，URL 将无法供用户点击并且会转换为纯文本，从而向收件人显示隐藏的潜在恶意内容。然而，这在收件人想要查看邮件中引用的合法 URL 时会给其增添一定的负担，因为他们必须将纯文本链接复制并粘贴到其浏览器中才能访问该网站。但是，对于成为不法分子攻击目标的个人，这样便能另外提供出色的保护层，因为它能让这些人员看到其尝试访问的网站。

IronPort S 系列网络安全产品：对于想要深度防御有针对性的网络钓鱼和其他恶意软件攻击的组织，IronPort S 系列可以提供一个易于管理且分层的集成网络安全平台。该设备可处理各种网络流量，通过使用功能强大的声誉筛选器和反恶意软件防御技术来保护已知站点和未知站点。

小结

网络钓鱼中的新威胁 - 有针对性的网络钓鱼正在成为危险的问题。这些邮件使用高级社会工程技术（如按名称找到收件人（并识别其公司））说服精心挑选的受害者无意间向网络不法分子传送敏感数据或资金。

由于创建有针对性的网络钓鱼邮件需要采用较多的资源，因此，它们目前仅危及全球范围内一小部分网络钓鱼邮件。但是，这些邮件的回报非常大，这意味着其数量毫无疑问会增加。

为了帮助组织避免成为有针对性的网络钓鱼活动和其他恶意软件攻击的受害者，Cisco IronPort 提供了一种分层的邮件和网络安全集成方法，即将互联网流量监控、声誉过滤器和身份验证技术组合在一起。

联系人

Cisco IronPort 销售代表、渠道合作伙伴和支持工程师随时可以帮助您评估 IronPort 产品如何能使您的邮件基础设施变得安全可靠，且更易于管理。如果您认为您的组织可以从 Cisco IronPort 的行业领先产品中获益，请致电 650-989-6530 或访问我们的网络，网址为：http://www.ironport.com/try。

美洲总部
Cisco Systems, Inc.
加州圣何西

亚太地区总部
Cisco Systems (USA) Pte.Ltd.
新加坡

欧洲总部
Cisco Systems International BV
荷兰阿姆斯特丹

思科在全球设有 200 多个办事处。 地址、电话号码和传真号码均列在思科网站 www.cisco.com/go/offices 中。

美国印刷 C11-701843-00 02/12