This translation is a joint initiative of MAAWG (www.maawg.org) and ITU (www.itu.int/ITU-D/cyb/cybersecurity).

MAAWG（反滥发信息工作组）建议书

《为住宅或动态 IP 空间管理端口 25》采纳的好处和不作为的风险

引言

垃圾邮件传播者和其它犯罪分子正在更多地利用病毒和“间谍软件”等传播手段，将大量计算机置于自己的控制之下。配备 DSL、有线或公司网络等“永远在线”连接的计算机越来越多，使他们更易于捕捉目标，施展其破坏力。通过对技术稍加改革，并辅以包括鼓励使用反病毒和防火墙软件的用户宣教工作，所有电子邮件提供商都可以提高对其用户系统发出的潜在恶意邮件的控制能力。通过对来自个人计算机的电子邮件加以管理，提供商可以削减其业务运行成本、提高用户满意度，并降低涉及其业务的互联网滥用程度。

对电子邮件传输的威胁和滥用

个人计算机对未经电子邮件提供商管理或监测的电子邮件服务器的传输访问（发送电子邮件）有增无减，使提供商及其客户面临不轨人员和流氓软件肆虐的更大危险。受未经授权和检测的第三方控制的个人计算机，即俗称的“僵尸”（zombies）或“僵尸网络”（botnets），为利用计算机直接与邮件交换机（MX）和无防护的 SMTP 中继服务器连接的人隐形其后、进一步传播垃圾邮件和病毒提供了掩护。高达 80%的垃圾邮件信息是在所有者不知情或未授权的情况下，通过这些“僵尸”个人计算机传播的。

不做为的风险

这给受害计算机的所有者带来的消极影响是直接和严重的。这些计算机的所有者通常会长时间地感到计算机运行缓慢，这种情况在试图上网时尤为突出。垃圾邮件发送者可以在神不知鬼不觉地用尽其上游带宽的同时，使下游带宽也严重受限。

连接这台计算机的提供商可能注意不到被占用的额外带宽，但他们通常也会受到消极影响。受害客户可能会通过电话联系技术支持，而这样做可能耗费掉提供商一个月或更多的收入；也许客户会简单地认定提供商的软件、拨号入网或宽带业务效率低下，干脆撤消服务。

只要受感染的用户还在网上，提供商面前就会堆满用户投诉，因为用户收到了受感染用户的计算机生成的大量垃圾邮件。即使少数几个“僵尸”个人计算机引发的向客户支持、防止滥用和网络运行部门的投

诉，也会使成本上升，令人难以承受。提供商也许会突然发现，他的整个网络上了“黑名单”，甚至会根据其网络发出滥用邮件的形式，被禁止向颇具人气的目的地发送电子邮件。当然，每发出一条垃圾邮件信息都意味着会有接收的下家。 允许这类滥用活动畅行无阻，会降低客户的信任度，而所有互联网用户和接入提供商都会因为这种失信而在不同程度上受到全球性的消极影响，从而打击了客户利用互联网进行交流、经商和娱乐的积极性。

电子邮件传输的最佳做法

行业自律是解决电子邮件传输滥用的最有效手段，而且必须刻不容缓地就严重的垃圾邮件问题采取行动。世界各国政府机构都在大声疾呼：如不马上采取行动、立竿见影，行业将面临更严格的检查与监管。MAAWG 因此向互联网和电子邮件服务提供商推荐以下这套电子邮件传输的最佳做法：

1. 根据 RFC 2476 的介绍，在端口 587 提供电子邮件提交服务。
2. 按照 RFC 2554 所述，要求对电子邮件的提交进行认证。
3. 避免对与端口 587 的连接进行干预。
4. 对电子邮件客户机软件进行配置，以便使用端口 587 和进行电子邮件提交认证。
5. 除您明确授权执行 SMTP 中继功能的主机之外，阻断您网络上的所有主机对端口 25 的访问。这类端口当然包括您自己的电子邮件提交服务器，并也可能包括您所负责的客户的合法电子邮件提交服务器。
6. 阻断自端口 25 进入您的网络的入局业务流，以防垃圾邮件发送者利用您网络上的非对称路由和欺骗性 IP 地址从事可能的滥用活动。

各种规模的提供商，包括许多世界上最著名的业务提供商和众多 MAAWG 成员，都采用了这些做法，而且用户基数未见明显下降。

采纳的好处

通过 SMTP 中继请求验证和综合电子邮件传输流，可使 ISP 受益匪浅。这些措施使 ISP 能够：

- 确定信息的提交方。
- 滤掉垃圾邮件、病毒和其它滥用信息负载。
- 对客户个人和/或整体的传输速率进行监测和限制。
- 对电子邮件的提交执行可接受的服务使用策略和条件。

ISP 还能获得以下竞争优势：

- 减少被接收方互联网和电子邮件业务提供商列入黑名单的风险，从而提高合法电子邮件信息的发送率。
- 降低滥用情况问讯台、客户支持和网络运行中心的成本。
- 具备向需要运行直接连接端口 25 的电子邮件服务器的客户提供高档服务的能力。
- 因减少端口的使用和带宽的消耗而降低基础设施成本。
- 按全球垃圾邮件量的下降比例享受减少接收这类邮件的实惠。

一旦这些措施得到实施，受感染的机器就不再是隐姓埋名的工具。受害的计算机可以被迅速发现和隔离，直至所有者发现问题并采取纠正措施。客户在这一过程中受到应对安全威胁的训练和提高自我保护的鞭策。这其中的每一项改革都会使所有最终用户的安全性和隐密性得到增强。

客户宣教工作

MAAWG 认为，就上述威胁、其应对措施以及计算机所有者在向更安全的电子邮件传输方式过渡过程中的应有作用进行客户交流和宣教，是一项无比重要的工作。互联网和电子邮件提供商必须使其客户了解他们正在从事的工作，为什么这样做，以及为什么这项工作对于他们之中的绝大多数人将是透明的。一股强大的力量正在推动所有电子邮件运营商尽快采用这些技术性做法，恢复对端口 25 的控制，不断向客户进行宣传教育，保证其业务安全、免遭滥用。

相关读物

《用于验证的 SMTP 业务扩展》，J. Meyers 著，1999 年 3 月：http://www.ietf.org/rfc/rfc2554.txt

《信息提交》，R. Gellens 和 J. Klensin 著，1998 年 12 月：http://www.ietf.org/rfc/rfc2476.txt

《垃圾邮件僵尸终结行动》，联邦贸易委员会，2005 年 5 月：
http://www.ftc.gov/bcp/conline/edcams/spam/zombie/

《反垃圾邮件技术联盟的技术与策略建议》，反垃圾邮件技术联盟，2004 年 6 月 11 日：
http://www.postmaster.aol.com/asta/proposal_html.html

《终止垃圾邮件 – 建设一个强大安全的互联网》，加拿大工业部，2005 年 4 月：
http://e-com.ic.gc.ca/epic/internet/inecic-ceac.nsf/en/gv00329e.html