

DRAFT – For Public Comment

Managing Port 25 for Residential or Dynamic IP Space Benefits of Adoption and Risks of Inaction

Introduction

Spammers and other criminals are increasingly using viruses and “spyware” as vehicles to assume control over large numbers of computers. The continuing increase in computers with “always on” connections such as cable, DSL, or corporate networks provides even more targets and greater ability to wreak havoc. With a few technology changes, combined with user education which includes encouraging the use of anti-virus and firewall software, any email provider can gain greater control over potential malicious traffic emanating from their users’ systems. By managing the sending of email from personal computers, providers can reduce the costs of running their business, increase customer satisfaction, and reduce the level of Internet abuse associated with their service.

Email Transmission Threats and Abuse

Unabated transmission access (sending of email) from personal computers to email servers not managed or monitored by the email provider exposes both providers and their customers to a greater risk of victimization from rogue persons and software. Personal computers under the control of unauthorized and undetected third parties, popularly called “zombies,” provide a veil of anonymity for those who then use them to connect directly to mail exchange (MX) and unprotected SMTP relay servers and send yet more spam and viruses. As many as 80% of all spam messages pass through these “zombie” personal computers without the knowledge or authorization of their owners.

Risks of Inaction

The negative effects on the owners of the victimized computers are immediate and severe. The owners of the computers often experience extended periods of sluggish performance, particularly when attempting to use the Internet. Unbeknownst to them, a spammer may be saturating their upstream bandwidth and severely limiting their downstream bandwidth as well.

The provider to which the computer is connected may barely notice the extra bandwidth being used, but they are usually impacted negatively as well. The victimized customer may call in for technical support, which can cost the provider a month’s worth of revenue or more. Worse yet, the customer may simply decide the

provider's software, dial-up, or broadband services are performing poorly and cancel service altogether.

For however long as the user does stay connected in an infected state, the provider will amass complaints from those who are receiving the spam being pumped out through its infected customer. Complaints to customer support, abuse, and network operations departments can drive costs to painful heights with the presence of even a small number of "zombie" PCs. The provider may also soon find that its entire network is "blacklisted" or prohibited from sending email to popular destinations, based on the pattern of abuse originating from its network. Of course, every spam message sent is also one more received. Permitting this type of abuse to continue unchecked has a global, proportionate negative effect on *all* Internet users and access providers by decreasing consumer confidence, thereby reducing the consumers' willingness to utilize the Internet for communication, commerce, and fun.

Email Transmission Best Practices

Industry self-regulation is the most effective measure to address email transmission abuse, and the magnitude of the spam problem demands immediate action. The message has been received loud and clear from government agencies worldwide: absent immediate action and results, the industry faces increased scrutiny and regulation. Therefore, the MAAWG recommends the following set of Email Transmission Best Practices for Internet and Email Service Providers:

1. Provide Email Submission services on port 587, as described in RFC 2476.
2. Require authentication for Email Submission, as described in RFC 2554.
3. Abstain from interfering with outbound connectivity to port 587.
4. Configure email client software to use port 587 and authentication for Email Submission.
5. Block access **to** port 25 **from** all hosts on your network, other than those that you explicitly authorize to perform SMTP relay functions. Such hosts will certainly include your own Email Submission servers and may also include the legitimate Email Submission servers of your responsible customers.
6. Block incoming traffic to your network from port 25. This prevents potential abuse from spammers using asymmetric routing and spoofing IP addresses on your network.

These practices have been adopted by providers of all sizes, including many of the most popular service providers in the world and many MAAWG members, without any appreciable reduction in customer base.

Benefits of Adoption

Requiring authentication and aggregating email transmission traffic through SMTP relays provides an ISP with many valuable benefits. These measures enable the ISP to:

- Identify the party responsible for submitted messages.

- Filter out spam, viruses, and other abusive message payloads.
- Monitor and limit, per customer and/or in aggregate, transmission rates.
- Enforce acceptable use policies and terms of service for email submission.

Additionally, the ISP gains the following competitive advantages:

- Improved deliverability for legitimate email messages, because of a reduced risk of being blacklisted by receiving Internet and Email Service Providers.
- Reduced costs for abuse help desk, customer support, and network operations centers.
- Ability to offer premium tiers of service to customers who have a legitimate need to operate email servers with direct access to port 25.
- Reduced infrastructure costs due to reductions in port utilization and bandwidth consumption.
- Proportionate recipient's share in the global reduction of spam volumes.

Once these measures are in place, infected machines can no longer be vehicles of anonymity. Victimized computers can be rapidly identified and quarantined until the owner becomes aware of the problem and corrects it. In the process, customers are educated about security threats and are encouraged to better protect themselves. Each of these changes increases the safety and privacy for *all* end users.

Customer Education

The MAAWG cannot stress enough the importance of communicating with and educating customers about these threats, the measures being taken to address them, and the role that computer owners must play in this transition to a new method of email transmission. Internet and Email Service Providers must let their customers know what they are doing, why they are doing it, and why, to the vast majority of them, it will be transparent. All email carriers are strongly urged to adopt these technological practices as soon as possible, to regain control of port 25, and to provide ongoing education to their customers, keeping their service safe from abuse.

Related Reading

SMTP Service Extension for Authentication, J. Meyers, March 1999:

<http://www.ietf.org/rfc/rfc2554.txt>

Message Submission, R. Gellens and J. Klensin, December 1998:

<http://www.ietf.org/rfc/rfc2476.txt>

Operation Spam Zombies, Federal Trade Commission, May 2005:

<http://www.ftc.gov/bcp/online/edcams/spam/zombie/>

Anti Spam Technical Alliance Technology and Policy Proposal, Anti Spam Technical Alliance, June 11, 2004: [href="http://postmaster.info.aol.com/spf/details.html%20"](http://postmaster.info.aol.com/spf/details.html%20)

