Messaging, Malware and Mobile Anti-Abuse Working Group

M³AAWG Best Common Practices for Managing Port 25 for IP Networks

Original recommendation published 2005

Updated August 2023

The reference URL for this document is https://www.m3aawg.org/Port25_IPNetworks

Introduction

Spammers and other abusers often use viruses and spyware as vehicles to assume control over large numbers of computers. The ever-increasing number of computers with "always on" connections such as fiber, cable, corporate, and hosting provider networks provides more targets and greater ability to wreak havoc. However, connectivity providers can gain greater control over potentially malicious traffic emanating from their users' systems with a few technology changes, user education, and operational assistance that includes the use of anti-virus and firewall software. By managing the sending of email from devices on their network, 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

Transmission of email from computers not intended to be email servers exposes both providers and their customers to an increased risk of victimization by bad actors and malicious software. Computers under the control of unauthorized and undetected third parties, popularly called "zombies" or "botnets," provide a veil of anonymity for those who then use them to connect directly to SMTP receipt hosts (mail exchange [MX]) and unprotected SMTP relay servers in order to send spam and malware. Despite improved network management in recent years, many spam messages pass through these "zombie" computers without the knowledge or authorization of their owners.

Risks of Inaction

Owners of these computers often experience immediate and severe negative effects, such as extended periods of sluggish performance, particularly when doing network-intensive tasks such as gaming or video streaming. Without their knowledge, a spammer may be saturating their upstream bandwidth and even 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 also usually affected negatively. The victimized customer may call in for technical support. A single customer support call can cost the provider a month's worth of the customer's revenue or more, or the customer may simply decide the provider's software or network services are performing poorly and cancel service altogether. Third parties that notice abusive traffic may also generate support costs through abuse reports.

As long as the computer stays connected in an infected state, the provider will continue to receive complaints from recipients of the spam 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" devices. The provider may also soon find that its entire network is "blocklisted," 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. Allowing this abuse has a global, proportionately negative effect on all internet users and access providers by decreasing consumer confidence and burning through valuable time and resources.

Email Transmission Best Practices

Industry self-regulation has been the most effective measure to address email transmission abuse, and the magnitude of the spam problem continues to demand diligent action. The message has been received loud and clear from government agencies worldwide: absent the action and results reflected by the original publication in 2005 of these Best Practices, the industry would have faced increased scrutiny and regulation. Therefore, M[3]AAWG continues to recommend the following set of Email Transmission Best Practices for internet and Email Service Providers:

1. Provide email submission services on ports 465 and 587 as described in RFC 6409 and the updates in RFC 8314.
2. Require authentication for email submission as described in RFC 4954.
3. Allow customer hosts to connect to port 465 and 587 submission servers on your network and on other networks.
4. Configure email client software to use port 465 or 587 and authentication for email submission.
5. Block access to port 25 from all hosts on your network other than those that you explicitly permit to operate as SMTP relays. 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 other than to authorized SMTP relay hosts. This prevents potential abuse from spammers using asymmetric routing and spoofing of IP addresses on your network.
7. Ensure that all hosts send traffic only with their own source IP address in order to prevent abusive asymmetric routing as advocated by the MANRS project.

These practices have been adopted by providers of all sizes, including many of the world's most popular service providers, and by many M[3]AAWG members, leading to an effective reduction in the use of their networks to send spam 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 blocked by receiving mail systems.
- 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.
- Improved reputation due to less spam from the ISP seen at other networks.

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 safety and privacy for all end users.

Customer Education

A key part of this process is communicating with and educating customers about these threats, the measures being taken to address them, and the role that computer owners must play in maintaining a safer 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 since neither user mail programs such as Outlook nor webmail uses port 25. 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.

References and Related Reading

SMTP Service Extension for Authentication, R. Siemborski and A. Melnikov, July 2007: https://www.rfc-editor.org/info/rfc4954

Message Submission, R. Gellens and J. Klensin, November 2011: https://www.rfc-editor.org/info/rfc6409

Cleartext Considered Obsolete: Use of Transport Layer Security (TLS) for Email Submission and Access, K. Moore and C. Newman, January 2018: https://www.rfc-editor.org/info/rfc8314

Operation Spam Zombies, Federal Trade Commission, May 2005: https://www.ftc.gov/news-events/news/press-releases/2005/05/ftc-partners-launch-campaign-against-spam-zombies

Anti-Spam Technical Alliance Technology and Policy Proposal, Anti-Spam Technical Alliance, June 11, 2004: https://www.uceprotect.net/downloads/asta.pdf

Stopping Spam - Creating a Stronger, Safer Internet, Industry Canada, April 2005: https://publications.gc.ca/site/eng/9.687489/publication.html

Mutually Agreed Norms for Routing Security (MANRS), https://www.manrs.org/ (and see Network Operator Actions, https://www.manrs.org/netops/network-operator-actions/)

As with all documents that we publish, please check the M3AAWG website (www.m3aawg.org) for updates.