M3AAWG
MESSAGING MALWARE MOBILE

Messaging, Malware and Mobile Anti-Abuse Working Group

Help – I'm on a Blocklist

Updated February 2018, Version 1.0.1 (June 2014)
Shortened URL to this document: www.m3aawg.org/BlocklistHelp

Table of Contents

Updated in this Version

Minor changes have been made in the February 2018 version to improve the clarity and update the text.

Executive Summary

Nearly all email systems have delivery issues at some point because their sending IPs or domains are included on a blocklist. This includes Email Service Providers and network operators. Depending on where mail is blocked, these listings can trigger widespread panic within the blocked company. Knowing how to triage and respond to the block can ensure a timely resolution. This document specifically addresses delivery failures due to active blocks placed against a sender's IP address or domain.

A number of steps need to be taken to remediate an IP or domain that has been included on a blocklist:

1. Verifying that you are on a blocklist.
    a. Identify why mail is failing and if it is due to a listing.
    b. Identify the underlying organization responsible for the listing.
    c. Identify the steps needed for delisting.
2. Assess the impact of the listing.
    a. Identify how much mail is undelivered as a result of the listing.
    b. Quantify the costs of remediation.
    c. Determine if the costs outweigh the impact.
3. Take action.
    a. Implement a remediation plan or
    b. Decide to take no action.
4. Communicate the actions that were taken (if any).
    a. Contact the owner of the blocklist.
    b. Inform the blocklist owner of the remediation steps taken.
    c. Request delisting from the blocklist.

Through early detection, an established triage procedure, implementing a disaster response plan, and effective internal and external communications, organizations can minimize the impact of a block to their business. Undertaking these actions can quickly address the problem and move toward delisting. This document describes the most common features of blocklists, how IPs or domains become listed and methods by which the owners can remediate the problem and restore their ability to deliver email.

Introduction

At one point or another, almost every organization that sends email or provides SMTP service will be unable to deliver mail because they are on a blocklist. For an organization reliant on sending email, such as an ESP or network operator, a listing on a blocklist can be an emergency that precludes rational discussion of workable long-term solutions. This document helps an organization plan for these circumstances by describing how to detect a listing and outlines the steps for remediation.

Many organizations do not realize they have options when experiencing an email block. They are so focused on restoring their mail delivery that they often fail to consider the most appropriate steps needed to resolve the issue. The correct course of action will depend on the business impact of the listing and the difficulty posed by meeting the blocklist requirements. Understanding the basics of blocklists makes the decisions and resolution paths clearer, even under the duress of an active listing. Knowing the available options and forming a plan ahead of a crisis makes resolving the issue and communicating about it much more effective.

There are numerous reasons that email may be blocked; having an IP address or domain name(s) on a blocklist is only one. This document focuses on general processes for identifying blocked email specifically caused by inclusion on a blocklist, determining the listing's impact, investigating the relevant blocklist operators' removal processes, and getting delisted where and when appropriate.

What is a Blocklist?

In general, a blocklist, in its simplest form, is a list of IP addresses or domain names that are suspected of emitting some form of malicious traffic, including spam, emails containing viruses or malware, unwanted SSH connections, etc. Blocklists can be used as access controls to prevent malicious or undesirable traffic from reaching the intended recipient and may be based on IP addresses, IP ranges, domain names, URLs, or other characteristics found in undesirable traffic. While lists can contain different types of information (IP

addresses, domain names, ASNs, etc.), this document refers to "IP address" in the discussion below to simplify the terminology. When dealing with a list that contains domain names, URLs or some other information, the reader should mentally substitute that information type for the term "IP address."

In the context of email, a blocklist is a collection of identifying data used by receiving mail systems to help prevent spam, viruses, or phishing emails from reaching end users. The protection is accomplished by rejecting inbound email connections from listed IP addresses or domain names. In some cases, lists block email containing links to problem content or domains.

Because of the diversity of lists, listing policies and delisting requirements, we are unable to detail the specifics of different blocklist policies. There is no "typical" listing. This document focuses on general processes for identifying email stoppages caused by a blocklist, investigating the cause, identifying the necessary removal procedures and getting delisted.

There are two primary varieties of blocklists: internal (private) and external (third-party) blocklists:

- An **internal** blocklist is a list maintained directly by the group or mailbox provider who receives the mail. To resolve a block from an internal list, listees[1] must communicate directly with the entity blocking their mail. Internal list maintainers are responsible for protecting their own networks and they seek to satisfy their employers and end users.
- An **external** list is maintained by a third party. Delisting requires communicating with the entity compiling the list rather than the mailbox provider who is using the list. There are a number of different operator and management styles for external blocklists. Some are commercial with paid staff members while others are staffed by volunteers or perhaps even a single volunteer/hobbyist. Some lists use both paid staffers and volunteers. External list maintainers seek to satisfy the mailbox providers using their lists. Most of the widely used external blocklists have been around long enough to have a proven track record of success. They also have publicly available policy pages and many of them provide some method for delisting an IP address.

There is one special kind of list that is not related to sending practices. These "informational" lists are not used to block "bad" senders; instead, they are used to enforce local policies that are not based on sender behavior. Informational lists include location-based lists, lists of "dynamic" or "residential class" IP addresses, lists of domain names that do not have properly-configured RFC-2142[2] role accounts, or ASN[3] routing lists. In the case of informational lists, delisting is rarely an option. The only time delisting occurs is when an entity on the list is incorrectly classified.

Blocklist Policies

Each blocklist has its own criteria for adding or removing IP addresses. Many lists describe their listing criteria on their websites. Overall, however, listees cannot rely on the people running the blocklist to tell them exactly why they are listed. Listees are expected to troubleshoot their listing using generally available information without relying on the list's personnel for specific information. The lack of support from list operators makes understanding the how and why behind a listing critical for troubleshooting.

---

[1] The term "listee" refers to the person or entity that has administrative control over the IP or other entry that is on a blocklist.

[2] IETF RFC 2142, Mailbox Names for Common Services, Roles and Functions, https://www.rfc-editor.org/rfc/rfc2142.txt

[3] ASN (Autonomous system), https://en.wikipedia.org/wiki/Autonomous_system_(Internet)

Many blocklists rely on passive detection techniques. These blocklists do not actively scan networks looking for IP addresses to list. Rather, listings are the result of email sender behavior as seen by receiving networks; i.e., incoming IP addresses or domains controlled by the listed entity that seem to fall within the receiving network's policy of prohibited behavior. For internal lists, any traffic sent to that organization can be used as criteria for updating its blocklist. In the case of external lists, the information is gathered from the blocklist's own networks and from shared information provided from their users' networks. Passive detection techniques usually rely on mail sent to recipients who did not request the mail. Often these "recipients" are actually automated spam traps. In some cases, however, mail sent directly to individuals who did not ask for the mail can trigger a listing.

There are a few blocklists that rely on active detection methods for finding IPs to list. These techniques include open relay and open proxy scanning, user nominations and ASN monitoring looking for newly spun up IPs. Other types of lists monitor newly registered domain names and reports on new domains. Lists that are location or characteristic based typically rely on active techniques for detection. For instance, lists that target dynamically-assigned IP addresses may list all IP space that contains a particular word or style of reverse DNS. It should be noted that a list can be pre-built or determined and populated on the fly. The effect on the sender's operations does not usually depend on how the list was constructed.

It is critical for a listee to understand that simply because an IP shows up on a publicly available list it does not mean any specific email failure is related to that list. There are very few public lists that are used on a global scale.

Most of the widely used lists tend to have good, consistently applied policies and clear delisting criteria. The lists that do not have reasonable policies, or explain them poorly, tend to be less frequently used and are therefore typically considered as less relevant to a listee. Some questionable lists might be employed on a regional basis due to local "popularity" or inclusion in a mail appliance that is related in some manner to the list owner or maintainer. Weighing the severity of a listing is detailed below in Step 2: Block Impact Assessment.

Internal lists implement policies of the specific receiver. Sometimes, these policies may seem excessive and overly burdensome on senders. Receiving systems are in a position to decide the rules for sending to them, e.g., no receiving domain can be forced to accept email that they do not wish to accept. It should be assumed that the list is providing value to the receiver, although senders may not understand the underlying logic.

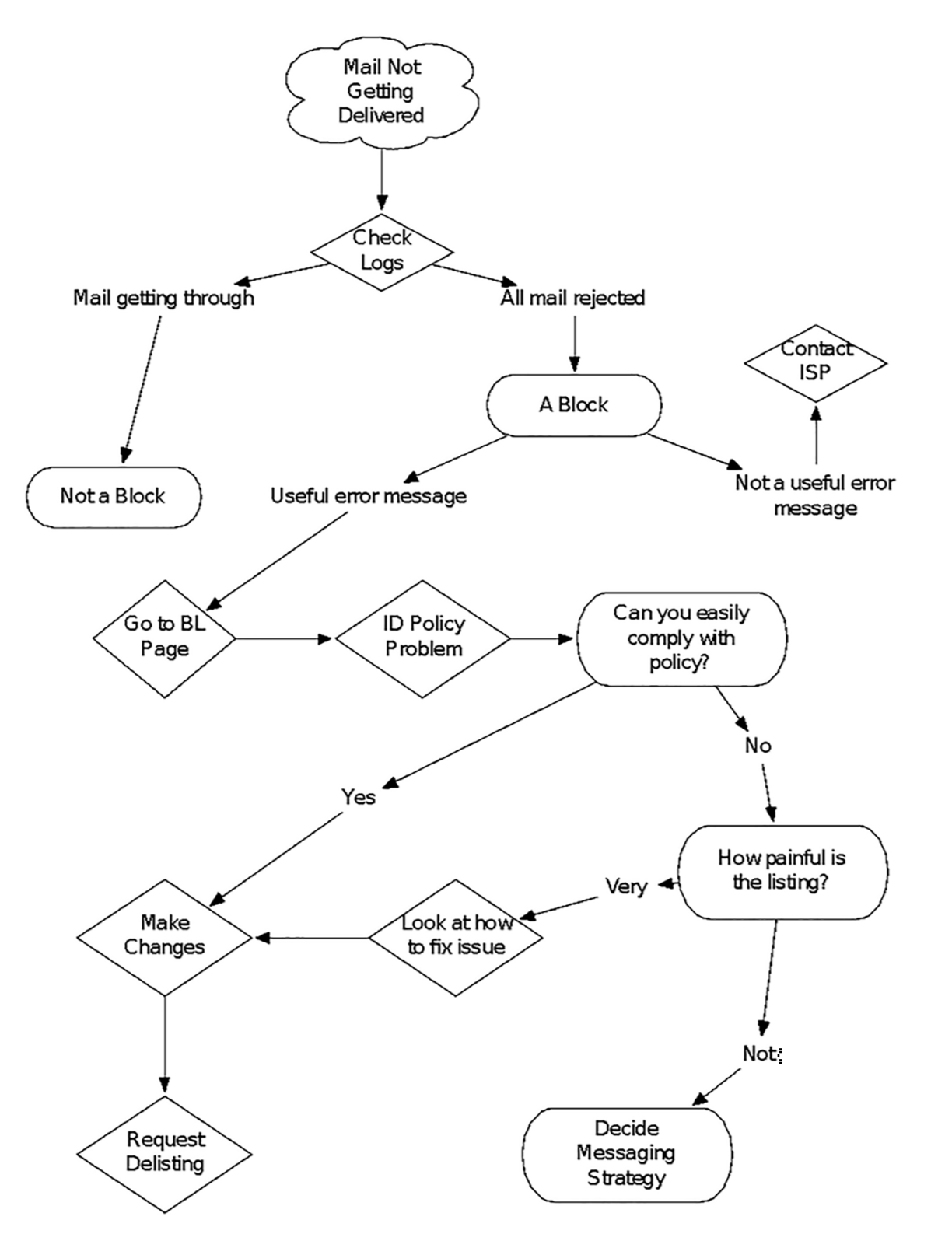
While each blocklist's policies are unique, the most common blocklist policies are listed in Appendix A - Common Blocklist Listing Policies.

Responding to a Listing

This section describes the discovery of a listing and how to respond to, and communicate about, the listing.

1. Discovery
2. Block Impact Assessment
3. Take Action (or Choose to Take No Action)
4. Communicate Actions Taken or Resolution

The following diagram illustrates the blocklist discovery, response and remediation process.



Step 1: Discovery

There are many ways to discover and identify the inclusion of your sending IPs or domains on a blocklist—these include both proactive detection mechanisms and reactive methods. Early detection monitors alert senders about blocks before they can cause significant delivery problems. In some cases, a sender can address the issue before customers notice their email is not being delivered.

Early warning methods include monitoring mail logs for terms common to blocklists, including "blocked by," "spam," and other identifying terminology. Another way to preemptively identify inclusion on a blocklist is to monitor the list directly. This works well with external lists but can be impossible or unsupported for internal lists that are seldom exposed outside of an organization or domain.

Most lists do not provide any email notice or other warning before a listing occurs. Thus, it is important to have effective monitoring in place to determine if a blocklist has identified a network problem. Depending on what type of internet access an organization provides, effective monitoring needs to be in place. For instance, ISPs that provide network services often do not have access to SMTP queues and logs but can still find their IP space on an external blocklist. Other ISPs provide SMTP service and can monitor queues and mail logs, but do not have access to click and inbox placement data.

Whether you are an ESP or a Mailbox Provider, it is recommended there be some periodic checks against public blocklists and mechanisms for internal log monitoring specifically to identify blocking and mail delivery problems. These checks can include any of the following:

- Complaints from customers about sent mail bouncing
- Notifications from scripts monitoring external lists
- Complaints from customers/end users about not receiving mail
- The percentage/number of emails undelivered
- Mail queues filling up and not draining
- Other aggregate checks (open/click/conversion rate)
- Low inbox placement rates
- Specific details found in mail delivery logs detailing the reason for failed or deferred deliveries
- Spam reports through Feedback loops

Even the best early warning monitors can miss some listings. In these cases, a listing may not be discovered until there is a significant email deliverability impact.

Different websites offer the ability to check an IP address across many different blocklists. These sites often value quantity of checks over the quality of the lists they check. Not all listings cause significant delivery problems. ISPs and network owners should look at the reputation of the public list before making a decision about how to handle the customer responsible for a listing. ESPs should look at their log files to determine if a specific list is responsible for mail failures.

Some deliverability or brand monitoring companies may offer commercial services for monitoring an organization's IPs and domains against known blocklists. Some of the blocklists may offer direct notification services for trusted users. Expect this to vary by list, organization and user.

Subscribing to important blocklist data feeds is another way to check for inclusion. This generally requires loading the list into a database and then comparing it to your network space(s), both DNS and IP. Usually this process can be scheduled to run automatically on a daily or hourly basis. Before investing in a strategy like this, you should be sure to identify which list(s) are actually important for the delivery of your mail traffic.

Step 2: Block Impact Assessment

Inclusion on a blocklist does not necessarily explain network or delivery failures. In the case of networks, IP based blocks may not affect its broader customer base, so the network owner may decide to let the individual customer(s) deal with it. On the other hand, some network blocks result in widespread routing failures affecting multiple customers. In these cases, network owners may have to address the block, possibly disconnecting the problem customer due to the severity of the impact.

For ESPs, block impact is measured differently. Blocking is all about how much it is affecting email delivery. Just because an IP is listed on a blocklist does not mean that all the delivery failures are due to that blocklist. There is significant overlap between some blocklist listings and some internally maintained lists. The best way to determine if a listing is impacting your delivery is to examine the bounce messages you receive and the logs collected by the sending server; they will contain the most information about any relevant listings. Some bounces will say which blocklist caused the bounce, but this is not always entirely accurate.

Some common questions ISPs and network operators should ask in order to determine the importance of a listing are:

- Where is my network listed?
- Is this listing affecting one customer or multiple customers?
- Does this listing indicate I have network abusers that have been disconnected from other networks?
- Does this listing indicate something on my network is infected with a bot or a Trojan?
- Does this listing indicate something on my network is providing command and control (C&C) services for a botnet?

Given the prevalence of infections and Trojans, and their significant impact on users and the broader internet, listings that indicate an infection or C&C presence on a network should be investigated and mitigated in every case.

Some common questions ESPs should ask in order to determine the importance of a listing are:

- Is this listing blocking mail to a substantial percentage of your recipients?
- Is it a small domain but with a strong relationship between sender and receiver, so that even a block that affects only one email address is important enough to resolve?
- Is resolution even possible?

Occasionally, bounces may cite blocklists or other sources to check for information about the refusal to accept mail, but no information will be present by the time someone investigates. Other bounces may not indicate which blocklist is involved. Because of this, it is important to know how to research a block. The lifetime of a particular entry on a list can vary, so blocks can go away just by time passing and may not require active intervention. It is prudent to verify that the listing is still active at each stage of the investigation.

Analysis of bounce data to assess the impact of a listing can be accomplished in multiple ways:

1. Examine if a particular blocklist is cited more than any other in a given data set, where the data set consists of all bounces received within a given timeframe, regardless of the receiving domain.
2. Restrict the dataset to only the domains that are of interest.
3. Restrict the dataset to those citing a particular listing, to determine the breadth and impact.

There are numerous other ways to determine the scope of the problem; some are more relevant to the systems sending mail and an organization's specific architecture.

When bounce data analysis implicates a blocklist as a possible cause of delivery failure, but no particular blocklist is cited, it may be possible to look for other bounces within the same time period(s) that do reference blocklists and determine if those cited may be the same as the undisclosed causes. However, a mere correlation between one bounce type citing a blocklist and another bounce type where the blocklist remains undisclosed does not necessarily mean both bounce types are due to the same listing.

Many times, a given blocklist will provide data that the listee can use to identify the problem. There are numerous means to obtain this data. Below are just a few examples:

- Certain blocklists have formal notification procedures in place that will automatically notify an affected listee. This may take the form of an email to the contact information available in WHOIS, through previously established channels or to the abuse address at the IP owner. Sometimes this notification will include information pertaining to the reason for a listing. Often times, this information is actionable. [Also, see below regarding postmaster and abuse contacts in "Step 3: Take Action (or Choose to Take No Action).]
- Many blocklists make this data available directly on their website. Network providers and ESPs can use this information to identify problem customers.
- The listed party may need to request listing data from the blocklist directly, using a Web form on their site or via email if the blocklist operator provides a contact email address. When communicating with a blocklist operator, it is important to be clear and as concise as possible with respect to what is being requested. It is possible to request actionable data prior to asking for a delisting, but many blocklists do not provide actionable data.
- Sometimes, depending on the blocklist in question, it is not possible to engage directly with personnel running the blocklist and all interaction with the blocklist is done via automated means. In these cases, it is important to thoroughly review the blocklist's Web information in an effort to understand their listing criteria. In some instances, this data is enough to get the listed party moving in the right direction toward addressing a listing issue.

For an ESP's impact assessment, it is vital to look at the amount of mail blocked that mentions the blocklist specifically. There are cases where blocked mail may not be related to a blocklist that is listing a specific IP address. Removing the IP address from that blocklist is not going to fix the underlying email delivery problem. Additionally, there are lists that may not be widely used except at a specific recipient site critical to an organization's email delivery.

Many widely used blocklists have reasonable policies. However, in a situation where a list is not in wide use, but is significantly impacting delivery, the listee has several options. The first is to conform to the listing criteria, no matter how difficult, and get delisted. The other is to talk directly to the organization using the list, explaining the reasons these policies seem unreasonable and why the sender cannot comply with them.

When mail is wanted or useful to the receiving organization, most receivers can make exceptions to the blocklist. However, some receivers will not be willing to consider any exceptions to their standard policies.

Overall, assessing the impact of any specific listing requires analyzing the number of delivery failures and determining how those delivery failures are impacting an organization's business. There is no one decision that will be correct for every organization or in every situation; just as there is no such thing as a blocklist that will be a problem universally or a blocklist that will never be an issue.

Step 3: Take Action (or Choose to Take No Action)

Once listees are aware of the cause or nature of the listing, there are numerous actions they can take to stop the abusive traffic. Some are far more aggressive than others, but the bottom line is that the listee in question needs to weigh the overall impact, financial ramifications and reputational impact of the listing(s) versus the effect of taking little to no action.

Delisting and resolution procedures vary from blocklist to blocklist; the list below is a set of common practices used to resolve inclusion on a blocklist. (**Note**: some of these procedures require knowing exactly what caused the issue and if there was, in fact, an isolated incident that spawned it). If one does not know the exact cause, achieving a resolution can become much more difficult.

When contacting an administrator, a polite, professional tone is extremely helpful. Messages should include the sending IP address, time and date (including the relevant time zone), any information from the delivery logs or undeliverable mail notifications, and a request for any information they can provide to help determine what behavior they found objectionable.

One highly ineffective approach for getting delisted from spam trap-based blocklists is to ask for the spam trap address "in order to remove it from our mailing lists." Most blocklists treat spam traps as a symptom of an underlying list problem. The presence of a spam trap address on a list indicates there are other addresses on that list that did not opt in to receive mail from the sender. Simply removing the trap address does not stop mail to the other non-opted in recipient addresses. Requesting a spam trap address may actually prolong the listing because it demonstrates to the operator a reluctance to resolve the underlying list problem and lack of understanding in how the blocklist operates. A better approach would be to periodically review those lists for click-opens and other engagement metrics. Spam traps do not open messages.

Network providers like ESPs and ISPs can often deal with a listing simply by terminating the problem customer and preventing them from further use of their mailing infrastructure. This situation may be more common for ESPs who tend to troubleshoot such issues on behalf of their customers. The clear conveyance of this action to a blocklist operator lets them know that the listed party was concerned about the problem and took swift action to resolve the situation. If a network provider does not choose to simply terminate the customer, for whatever reason, there are a number of things they can require of the customer before restoring the customer's ability to send email.

One of the most common solutions is to have the customer confirm all or part of their database. Full reconfirmation means that an email is sent to every member of the database asking if the recipient wants to continue receiving email from the sender. If the recipient responds affirmatively, the address is retained in the database as suitable to send future emails. If the recipient does not respond affirmatively, the address should not be mailed to again. With partial reconfirmation, senders can exempt segments from the reconfirmation process. These segments should be limited to recipients that have recent, demonstrated engagement with an email from that sender. So, for instance, a recipient that clicked through a message and

made a purchase within a short period of time (60 – 90 days is common) can be exempted from reconfirmation.

Another strategy for resolving a listing is removing a particular segment of a mailing list. This is usually implemented in cases where a sender has a history of clean mail but has imported a set of addresses from a particular source. If the blocklisting can be tracked to that segment, removing that segment completely may solve the issue.

For listings due to virus or malware infestation, the proper way to resolve the issue is to actually repair the infected machine. If the listed IP is a NAT (Network address translation), this may be a significant undertaking in scanning multiple machines using a single external IP address. It is possible to configure a NAT to only allow authorized machines to send through SMTP, through port 25, or through alternate mail ports, which can potentially resolve a listing problem. However, this does not fix the underlying security issue of infected machines inside a corporate or home firewall.

In some cases, listees may decide to take no action for a listing. There are a number of reasons to decide this. One is that the list itself is an informational list and the IP address or domain name meets the criteria for listing. Another reason organizations decide not to resolve listings is that the listing itself is not causing any serious delivery problems because the list is not widely used. Finally, some organizations decide that the blocklists' conditions for delisting are too onerous or problematic to comply with.

Step 4: Communicate Actions Taken/Resolution

Once the cause of the listing is identified and solved, the resolution should be reported back to the blocklist in question. It is important to be honest and forthright when communicating these actions to blocklist operators. The listed party must keep in mind that if action is communicated, yet never actually taken, a transient blocklisting may turn into a permanent one.

Each blocklist has its own preferred method of communication for delisting. Check the blocklist website and follow the directions. Failure to follow directions specifically may delay delisting; misdirected delisting requests may be thrown away or not acted on by the blocklist.

One of the common methods by which blocklists accept delisting requests is for the affected party to send an email to a specific address at the blocklist. Most of the major blocklists, both internal and external, have email addresses staffed by individuals trained to interact with listees. These emails should be brief while containing sufficient relevant information. Relevant information includes:

- The IP address or domain name listed
- A summary of actions taken to resolve the problem
- A timeline of when changes will be finished (if they are not yet complete)

Some blocklists provide a Web form instead of an email address. In this case, fill out all of the information requested. Again, it is extremely important to include the IP address or domain name that is listed. While most groups using Web forms carefully construct them to reject delisting requests that do not contain the IP address, some may accept a submission lacking this critical piece of information.

Certain blocklists do not accept delisting requests. It is unlikely that these lists are going to have much of an impact on a sender, but senders should be aware of their existence. In some cases, these blocklists have

auto-expiration policies; IP addresses or domain names that cease the behavior that caused the listing will be automatically removed after a certain period of time. Other lists never delist and the operators believe that there can be no fix. Again, these lists are likely not used in a way that is going to have a considerable impact to delivery.

There are also blocklists that expect payment for delisting. M[3]AAWG strongly discourages the practice of blocklist operators charging delisting fees in any form; we acknowledge that under some exigent situations, listed entities may choose to pay such fees. For example, paying a delisting fee may be a viable option for senders who are able to quickly identify the underlying problem, solve it, and have no issue paying such fees. However, failure to identify and solve the problem sets the sender up for future listings and, thus, future delisting fees. Furthermore, a payment does not preclude future listings for repeated problems or different issues.

Conclusion

Knowing how to identify a listing and understanding the methods to resolve it are vital to managing the situation effectively. The urgency of the issue is determined by the impact to the affected business and its flexibility in complying with the necessary requirements. The business impact can vary from blocklist to blocklist.

Blocklists with reasonable policies that are applied consistently tend to be the most widely used. Often, these listing entities will publish their listing criteria and may provide information about the listing trigger that can assist in the internal investigation and response plan.

Listings can be triggered for a number of reasons: Spam traffic, malware traffic, open proxy/open mail relays or, more subjectively, unprofessional sending behavior. Spam traffic is measured both with recipient complaints (mail delivered to addresses that never asked to receive the mail) and invalid addresses. Unprofessional sending behavior can include sending patterns indicative of abuse, like changing IPs or spreading mail across many IPs in different ranges, or even outright threats to a blocklist provider.

Having a business procedure in place for responding to a blocklisting allows for the reasonable management of the stresses associated with having mail go undelivered. Inclusion on a blocklist for an organization whose business it is to send email constitutes an emergency. Following a predefined method of discovery, analysis, and course of action provides for rational discussions and workable long-term solutions.

Appendix A - Common Blocklist Listing Policies

Spam Traffic

Most often, an IP address, server, or ISP is listed as a result of passing spam from their IP space to an endpoint observed by the blocklist provider. Most widely used blocklists use the definition of unsolicited commercial or unsolicited bulk email (UCE or UBE). Some ISPs also block based on their determination of how much their users want mail of a particular type or from a specific source. These blocks are usually dynamic and are outside the scope of this document.

Blocklist providers use different methods to detect spam traffic. Many of these techniques rely on receiving email at an address that never asked to receive the mail (often referred to as spam traps or honey pots). Some blocklists also use data from their subscribers, including complaints and individual block data, to determine which addresses should be added to the list.

Malware Traffic

IP addresses can be listed as a result of sending viruses to a blocklist's detectors or through analysis of captive spyware protocol activity. In addition, blocklists leverage data that is delivered to blocklist-operated firewalls.

Generally, these include virus-infected users who are unknowingly being used as spam servers, also known as Zombies, and listing can be performed whenever a host is suspected of being hacked or abused. This can occur when an infected host contacts a test server belonging to a blocklist and attempts to exploit known worm code. In this way, a single infected machine sending spam through a network utilizing NAT can result in blocked email from the entire LAN. If malware is dispatched with regularity, the listing can be escalated.

Listings can also occur based on the perceived probability that URLs or other distinctive strings are appearing as part of a spam or virus attack. In other words, recipient systems may parse various tokens seen in mail messages and adjust the blocklist based on what has been seen in previous traffic.

Open Proxy/Open Mail Relay

Some blocklists list open proxies or open mail relays. These machines provide anonymizing connections to senders. In many cases, open relays and open proxies are actually virus infected machines. There are a number of ways open relays or proxies are detected. Generally, open relay and open proxy lists will test the machine before listing it as an open relay or open proxy.

Organizational/ROKSO[4] Listings

The listing of IP addresses and host names based on the traffic coming directly from or leading directly to that machine have resulted in a few cases where systems under the control of specific organizations are listed. These listings require a history of malicious traffic from systems under the control of the organization and a documented failure to take lasting and effective steps to stop malicious traffic. In addition to organizational listings, some blocklists have focused on calling out and listing individuals suspected of long term, abusive

[4] Register of Known Spam Operations. http://www.spamhaus.org/rokso. "The Register of Known Spam Operations (ROKSO) is a register of spam senders and spam services that have been thrown off Internet Service Providers 3 times or more in connection with spamming or providing spam services, and are therefore repeat offenders. . . The ROKSO database collates information and evidence on each spam operation to assist ISP Abuse Desks and Law Enforcement Agencies," per Spamhaus website.

sending that borders on abject fraud. These listings are akin to the FBI's "most wanted" in the mail world and are not subject to remediation.

Organizational listings can affect IP ranges and host names completely separate from the source of malicious traffic. One type of organizational listing is the escalated listing. Blocklists that employ escalated listings may list additional IPs, such as corporate mail servers, in an effort to bring the listing to the attention of the listee. Escalated listings may follow an organization from provider to provider.

There are a number of factors that contribute to an organizational listing, including:

- Repeated spam after listing occurs
- Absence of proper responses to abuse complaints (or bounces in reply to complaints)
- Knowingly harboring spammers after being alerted to the problem. For example:
    - Providing support services to the activities of a spammer
    - A provider who moves their user from one IP range to another to evade listings
    - A provider who ignores severe abuse for long periods or actively expresses their intention to assist the customer in avoiding the listing
    - When spam is sent from excessive numbers of IPs within a range (usually a /24 or larger)
    - When the listing of a single IP address seems to have no effect

As with all documents that we publish, please check the M[3]AAWG website (www.m3aawg.org) for updates to this document.