maps

Application Note:

Guidelines for reporting email abuse

1737 North First Street
San Jose, CA 95112
www.mail-abuse.com

Table of Contents

What to Report

There are several elements in any spam that can and should be reported to the appropriate abuse desks, these include:

- Spam Source (i.e., Dial-up or source host)
- Legitimate relay servers
- Open Relay servers
- Spamvertised Websites
- Drop Boxes

The following should also be reported, where applicable and time permitting:

- Click-through pages
- Mailto: addresses
- Merchant Accounts (credit card services, etc.)
- How to Report

Abuse desks exist to protect their network. When they address an abuse report sent in by a third party, the action taken by the abuse staff is taken to protect their equipment and their resources. The fact that it also serves to protect the third party's equipment and resources is an added benefit.

It is our experience, and the opinion of the abuse personnel that we have corresponded with, that spam reports should be professional and concise. While traceroutes, registry look-ups, etc., are necessary in the preparation of the spam report, it is not necessary or desirable to "show your work" in the actual spam report. In general, this creates needless clutter and slows the progress of the abuse staff member. Exceptions to this rule would be the inclusion of source code from a spamvertised website which shows the click through, mailto: address or the merchant account; data needed to support a less than obvious connection; data needed to demonstrate an inaccuracy of a registry record; or, other similar and unusual information.

The spam reports must contain the full headers and complete content of the spam. There may be occasional rare exceptions to including large binary attachments. If the complete content of such a binary file is omitted, the report should state this fact and the binary should be retained and available should the abuse staff request it. In addition, the report should briefly explain why each provider is receiving that report. This can be as simple as:

```
Source host - This UCE originated on your system.
Webhost - You host the advertised domain www.example.com.
```

```
Please handle your users in accordance with your TOS/AUP
Thank you
-----BEGIN HEADERS----
<spam and complete headers>
```

All spam reports and related "attachments" should be sent in-line. It is not reasonable to ask an abuse desk to take the risk of opening an attachment from an unknown source, and many will not accept them as a matter of policy. In the case of a known virus, state in the subject that the post has a live virus attached.

Where to Report

Spam reports should be directed to the appropriate reporting address(es) for that domain. The easiest place to find these is the abuse.net index (www.abuse.net). If no address is registered at abuse.net, the proper reporting address can often be determined by visiting the website and attempting to locate the information in the contact pages or in the TOS/AUP of the provider; an SMTP verify of abuse@domain; or checking various other website compilations of abuse address listings. When no official abuse reporting address can be located, the default address should be postmaster@domain. Registry (i.e. ARIN, RIPE, *NIC) contacts should generally not be used for the reporting of loose spam.

"Shotgunning" spam reports to an excessive number of addresses at a single provider, or to an excessive number or providers is considered abusive and should never be done.

Spam Source

Spam sources can be dial-ups; static or dynamic DSL, cable and ISDN connections; or hosts on other dedicated connections.

An attempt should be made to determine the nature of the source IP. The reasoning behind this is that MAPS Dynamic User List (DUL®) only accepts listings of dial-ups, not any other type of static or dynamic connection. Additionally, some very badly configured mail servers will relay mail without adding a received line and can appear to be the spam injection point.

If the spam source is a dial-up, check to see if that IP address is listed on the DUL, by using the MAPS IP Address Lookup tool (http://www.mail-abuse.com/support/support_lookup.html). If the source is not listed and is a dial-up, it can be submitted to the DUL for inclusion.

Relays

There are several varieties of mail relays that appear in the loose spam: legitimate relay, closed relay, and open (third party) relay. All of these may be single hop or multi-hop.

Legitimate relays are mailservers that have transmitted mail from an authorized user of their system. It is important to watch the source vs. mailserver relationship as many ISPs have multiple netblocks or lease POPs from third parties. Spam passing through a legitimate relay should be reported to the owner of that mailserver, stating that the person sending the spam appears to be a customer. Legitimately relayed mail should not be submitted to the RSS, despite the fact that the relay may also be open.

Closed relays are mailservers that relay mail for only those sources or users that have a valid account on that system or can authenticate with that server in some manner. Most ISP's mailservers will relay only for their own IP addresses. Spam passing through a closed relay should also be reported to the owner of that mailserver, stating that the person sending the spam appears to be a customer.

Open relays are mailservers that will relay for any source without authentication requirements. In order to determine whether or not a server a server is open, the server can be tested via abuse.net, Sam Spade or telnet. If the server tests open, check to see if it is listed on the MAPS Relay Spam Stopper (RSS®) list by using the IP Address Lookup tool. The relay owner should be notified of the open relay and pointed toward the Application Note: How to secure your mail system against third-party relay for assistance in closing the relay.

Single Hop relays are mailservers that have the same input and output IP address. In most cases there will be a simple chain from source through the single hop server to the receiving server. In some rare cases, the server may insert a daemon line or internal hop between the input and the output. If the IP of the input and the IP of the output are the same, it is considered a single hop relay. In addition to sending the Notice, any single hop open relay that is not listed on the MAPS RSS should be submitted in accordance with the established submission policies for the RSS list at http://www.mail-abuse.com/support/support_nominats_rss.html.

Multi-Hop relays are mailservers that have an input IP address that is different from the output IP address. There may or may not be intermediate received lines showing daemons, internal IP addresses or external IP addresses. In multi-hop relays, the output side of the multi-hop is generally functioning as the smart host for the input host. In most cases the smart hosts

are set up to collect and send mail for multiple input hosts; conversely, many input hosts use a series of smart hosts. This can make it difficult to get a relay test header to match the spam header exactly. The fact that smart hosts often serve multiple input hosts makes the potential for collateral damage caused by the listing of a smart host very high. Multi-hop relays are therefore not listed in the MAPS RSS. These should be sent a Notice of Intent to Nominate and eventually be nominated directly to the MAPS Realtime Blackhole List (RBL®) should they remain open.

Spamvertised Websites

When a loose spam advertises a URL, check to see if the webpage is still active. If it is, report the offending URL to the web host. If it appears that the URL is under the control of the spammer, the URL should be reported to the block owner.

If there is no response from the host, or the host fails to take appropriate action on the website, send a Notice of Intent to Nominate (see section below) to the webhost. Please note that failure to terminate a site, in and of itself, does not constitute inappropriate action.

When reporting spam, take care not to complain about innocent sites that may be listed in a spam. An example of this would be a legitimate stock market index site being shown in an unrelated stock spam. At most, these should be sent to the site owner as a heads-up that their site is being used in a stock scam.

There are a variety of tools available to help with decoding obfuscated URLs and java script. Often, a traceroute or ping of the obfuscated URL will yield the decoded URL. Also popular for decoding URLs:

NetDemon http://www.netdemon.net/tools.html

For java script, the following are some of the tools available. Please note that you may have to try several sites to obtained the decoded java:

InterDEcryptor http://www.swishweb.com/dec.shtml - for decrypting pages encrypted with Intercryptor DePsyralizer - for decrypting pages encrypted with Psyral Phobia version 1, 3, or 4

Hesketh http://hesketh.com/schampeo/spam-l/decode_haywyre.html - will decode Haywyre

NetDemon http://www.netdemon.net/haywyre/ - also Haywyre

Dropboxes

Dropboxes are email addresses that the spammer uses to collect responses to his UBE. These are normally found within the body of the email. Occasionally the spammer will use a valid Reply to: but these are the exceptions rather than the rule. An attempt can be made to confirm that the Dropbox exists via an SMTP VRFY, EXPN or RCPT TO: test, prior to reporting them to the provider.

"Tickling" Dropboxes (i.e., replying to the Dropbox to ask for additional information) can lead to some issues of entrapment and must be handled carefully. Any mail subsequent to tickling the Dropbox is *solicited* and should not be reported as spam. The spam reports must be based around the initial unsolicited contact.

Click-Throughs

Click-throughs are secondary websites that are reached by a redirect from the spamvertised website, or via a button on the spamvertised website. This is often done in order to protect the "real" website by hiding it behind an easily replaced "throwaway" website.

Identifying click-throughs requires analyzing the source code of the page(s) in front of the "real" website. In this code can be found the redirect links or the click links. In some cases the code is in obfuscated java. There are a variety of tools that can decode the java, see the references above in the *Spamvertised Websites* section.

When reporting click-throughs, always attach a copy of the source code from the spamvertised site. These sites are typically removed quickly, and without the source code the abuse staff at the click-through host will have no proof of complicity.

Mailto: Addresses

Mailto: links are found in the source code of a website, much like click-throughs. They are usually located on the webform provided on the site for responses; however, in many cases the page uses a "hidden form value" and the mailto: may not be obvious.

Once the Mailto: is found, the address can be treated much the same as a Dropbox, with the added requirement that the source code from the webpage should be attached to the report.

Notice of Intent to Nominate

Before a nomination can be submitted, the parties that would be impacted by a listing need to be notified that a nomination to a MAPS list is being prepared. Please check to make sure that the IP address in question is not already listed on the intended list prior to sending notice or submitting a nomination.

The notice explains what is going to be nominated, why it is going to be nominated and how to avoid the nomination.

The receipt of the notice is critical and every effort should be made to ensure that the notification is delivered to a valid address.

In all cases the range of the IP addresses notified should only include addresses for which a credible and viable nomination can be presented to the MAPS Team. Please note that it is highly unusual for blocks larger than individual /32s to be listed outside of an escalation of an existing listing.

It is important to clearly outline the reasons why the Notice is being sent. The most common things reasons for notices on are:

- **Open Relays** - To be eligible for nomination to the MAPS RSS, relays merely need to be proven that they are open and that spam has been transmitted through them. When notifying an open relay, state that the person being notified has an open relay or an open multi-hop relay that is being used in the transmission of spam. Bear in mind that the relay "owner" may not be aware of that fact, may not have the technical knowledge to understand open relaying, or, may not be in physical possession of the relay server.
- **Spam Source** - Persistent unaddressed spam sources are eligible for listing on the RBL. Notify the source host that there has been a pattern of both complaints and a lack of response to those complaints. State pertinent information regarding the complaints and responses (or lack thereof) should be included.
- **Open Mailing Lists** - Open Mailing lists are those lists that do not follow a policy of closed loop opt-in, these are eligible for inclusion in the MAPS Nonconfirming Mailing List (NML[SM]). The list manager should be informed of the fact that they are sending unsolicited mail via an unconfirmed mailing list. Use of the word "spam" or "spamming" is discouraged. In *most* cases, the list owner and the sender are sending unsolicited mail out of ignorance of proper list procedures.
- **Spamvertised Websites** - Spamvertised websites that are not being adequately addressed by the web host are also eligible for inclusion in

the RBL. Notify the web host that there has been a pattern of both complaints and a lack of response to those complaints. State pertinent information regarding the complaints and responses (or lack thereof) should be included.

The notices should contain direction on what the provider can do to rectify the situation that is bringing about the notification. In most cases, this can be done by including a link to the Remove page on the Support section of the MAPS website.

The owner of the implicated IP address should be the party that is notified of an impending nomination. This is normally found by determining the rDNS of the IP address or the owner of the block. The following should be notified of the intent to nominate for all IP addresses to be nominated:

- The owner of the FQDN (Fully qualified Domain Name) shown in the rDNS
- The owner of any additional FQDNs aliased to that IP address
- The owner of the netblock or the immediate upstream

Notifications on larger blocks require notification of the block owner and their immediate upstream only.

The preferred contacts are the registered abuse.net contacts. If there are no addresses registered with abuse.net, the default is the appropriate required role account, such as postmaster@domain or hostmaster@domain. It is recommended that every effort be made to verify that the address that the notice is sent to is a valid one. Should a notification bounce, it is incumbent on the nominator to find a good reporting address to resend the notification to before that IP address is nominated. Postmaster@[IP] or postmaster@IP should only be used as a last resort for the notification.

Nominating an IP to a MAPS List

MAPS considers any listing to be a failure on our part to educate the offender. It is for this reason that Nominations are to be undertaken only as a last resort, when all attempts to convert parties involved have failed. Nominations should never be undertaken as long as the offending party is willing to work to resolve the issue that brought about the Notice of Intent to Nominate.

The time period between notifying the owner of an impending nomination and actual submittal of a Nomination should be viewed as the last chance to reach the offender and education should be actively pursued.

Response After a Notice

In most cases, the Notice will produce a response from the notified party. For relays, this is either the closure of the relay or a response stating that the administrator is working to close the relay. In other types of notifications, the response may be an explanation of what action was taken, a request for more information, etc.

If the response states that the problem situation is in the process of being rectified, a reasonable time period for the corrective activity should be established. The offending party should not be given an open-ended chance to correct the issue. The definition of a "reasonable time period" can vary depending on the contractual and technological issues that must be resolved.

Phone Calls

Nominators are expected to make every effort to contact the offending domain prior to submitting any Nominations, up to and including making a phone call to the domain when necessary. Please note that no one is expected to make international phone calls. The purpose of this phone call is to ensure that the correct parties at the domain in question are aware of the issue, understand the reasons for the impending nomination, understand the consequences of a continued failure to act and have been given every opportunity to amend the behavior. A phone call is not a threat of a listing; it is a last chance attempt at education.

Bear in mind that often the person you are speaking to does not have the technological answer to his problem either. It is often extremely helpful to suggest some possible answers to the problem or point the way to other resources that will enable a resolution. Always remember that you are calling to effect a correction, not because it is required prior to a nomination.

All phone conversations should be documented as to date, time, person or people involved and the gist of the conversation. This should be done with notes during the conversation and in more depth immediately following the conversation. This is necessary to provide documentation of agreements reached during the conversation, or, if education fails, to provide documentation for the evidence file.

What to Nominate

MAPS' purpose is simply to stop the spam. When this cannot be done by education, MAPS must take action to protect its subscribers. This action takes the form of a listing on the appropriate list. When compiling any nomination, nominate the smallest possible amount of netspace that will effectively stop the spam. In most instances this is one or more individual IP addresses (/32s). Larger blocks are most often listed as a result of escalations of existing

listings. If a nominator is escalating an existing listing, the nomination should clearly state that.

Writing the Nomination

The first sentence of the nomination should tell the MAPS Team what is being Nominated and why. (i.e.. “This is an RSS Nomination for the Open Relay at xxx.xxx.xxx.xxx”, or “This is an RBL Nomination for xxx.xxx.xxx.xxx (FQDN) for spam support”)

The next paragraph should outline the history of what brought about the nomination. This should provide enough detail for an uninvolved third party to understand all the issues, but should not merely restate what is contained in the evidence to be attached.

Include in-line, all related phone conversation transcripts, the spam, the abuse report, the response or auto-ack and any other correspondence. Additional information should include further documentation of the spam problem, webpage source code, or other necessary information.

Submitting the Nomination

Before submitting a nomination, it is good to review the submission guidelines at http://www.mail-abuse.com/support/support_nominats.html. for specific instructions for each list. When the nomination is complete, it should be emailed to the appropriate list management team.

RBL Nominations: rbl@mail-abuse.com

DUL Nominations: dul@mail-abuse.com

RSS Nominations: relays@mail-abuse.com

OPS Nominations: proxies@mail-abuse.com

NML Nominations: nml@mail-abuse.com