Open Mail Relays in Janet

Open relays allow any combination of origin and destination address, and are frequently abused by advertisers and others to distribute UBE. This will usually overload an organisation's mail server, affecting its ability to handle legitimate mail, and often leaves the organisation with a flood of complaints and error messages to deal with. Sites that are frequently abused as relays may be added to blacklists used by many network operators and ISPs to reject all e-mail and other traffic. Advice on preventing relaying is available from the MAPS website:

http://www.mail-abuse.com [1].

Another term used in this context is UCE, but for most purposes the 'bulk' aspect of the problem is more important than the 'commercial'.

There are now a number of bodies that seek to make UBE unworkable and one of their most effective activities is the maintenance of public blacklists of systems or networks that are in some way sources of UBE, particularly open relays. Of the well-known services, Janet uses certain services from the MAPS RBL™, a subscription system for creating intentional network outages ('blackholes') for the purpose of limiting the transport of known-to-be-unwanted mass e-mail. The policies and methods of some other lists are more controversial.

Janet has subscribed to some MAPSSM services on behalf of all Janet customer organisations and they are encouraged to use the RBLSM. Guidance notes on how to use these services are available to assist managers or administrators of mail services within Janet-connected organisations from https://community.ja.net/library/janet-services-documentation/dns-block-... [2]

The Janet Tester

Janet-connected organisations MUST NOT allow any computers on their networks to be used to relay UBE. Janet therefore provides facilities for checking that e-mail systems are secure against unauthorised relaying.

The Janet mail relay team operate the E-mail Advice and Testing System (formerly STAN - Spam-relay Tester And Notification) that attempts to connect to an organisation's mailer and relay a series of individual messages through it, just as bulk mailers do in preparation for a UBE run. A report of any vulnerabilities found is then sent to the organisation.

The tests involve SMTP sessions in which certain sequences of commands are sent to the system concerned and various forms of address are used in attempted message transfers. They include some sequences and addresses that do not conform to the relevant standards, described in RFC 2821 Simple Mail Transfer Protocol and RFC 2822 Internet Message Format.

Details of the E-mail Advice and Testing System can be found at https://community.ja.net/library/janet-services-documentation/spam-relay... [3].

This site includes instructions on:

- Requesting tests
- When to run tests
- Conditions of use
- Responses
- Tests that time out
- Tests you didn't ask for (i.e. unscheduled tests)
- Active testing by Janet
- Repairing Open Mail Relays

If a Janet-connected organisation is relaying messages without authorisation, the manager of the e-mail system should take appropriate action to repair the open relay. Instructions outlining what action they should take are available at https://community.ja.net/library/janet-services-documentation/spam-relay... [3].

This also includes advice on getting off blacklists and mending fences.

E-mail and Security Issues

E-mail is one of the most widely used services on the Internet but there are far more hosts offering mail services than are required or desirable. A host only needs to run a mail service if it is used to store delivery mailboxes. Since most workstations only process mail under the direct control of a user, for example when moving messages from an inbox to local folders, they do not need to run mail server software.

Unfortunately, most UNIX® systems are delivered with the sendmail server installed and running. All too often this will be an old version with known security or configuration problems. The first task in securing an e-mail system is therefore to disable all these unnecessary services and install extra protection at the network level, to help avoid problems that will undoubtedly spring up in future. For those hosts that do need to provide a mail service there are less powerful alternatives to sendmail available, which may be sufficient for many situations while also being easier, and therefore less error-prone, to set up. Further information about security issues may be found on the Janet CSIRT web pages.

All the usual network level threats and consequent countermeasures apply to computer and networking equipment associated with e-mail provision. As with other application services, there are also issues specific to the nature of mail and the way it is used and abused on the Internet.

General Countermeasures

Ensure that an intruder cannot take control of mail systems by:

- limiting connections with packet filters at firewalls and routers
- disabling unnecessary services on servers and workstations
- configuring servers to accept connections only as authorised
- installing patches and updates promptly for operating systems, mail and other applications and anti-virus software.

Specific Threats and Countermeasures

Monitor the service to establish what is a normal level of activity, and to recognise signs of overload before they cause difficulty. Document actions that might need to be taken if a problem occurs which requires disconnecting the mail server.

Unsolicited Bulk E-mail for their Own Users

Consider configuring the mail server to consult one or more DNS Block Lists about the source IP address before accepting each connection. The Janet mirror of the MAPS RBL+™ is one

such list conveniently available for organisations connected to Janet.

Consider central filtering of incoming messages by pattern matching, or support so that the users can filter their own mail.

Relaying Through the Mail or Proxy Servers by Bulk Mailers

This can lead to overload, damage to reputation and blocking of mail to other places. Consider restricting access to TCP port 25 (SMTP) so that e-mail traffic can only travel by the intended route through the network. Similar considerations apply to TCP port 587, which RFC 2476 assigns for message submission.

For other issues surrounding e-mail relays, see the separate Janet documentation at https://community.ja.net/library/janet-services-documentation/janet-csirt [4]

Open proxies are systems not primarily for mail use that accept some sort of inward connection and allow it to set up an ongoing connection that may be a mail transfer. Typically the incoming connection is web or HTTP on TCP port 80, and it is intended that client computers within the network can send all their web requests through it. SOCKS on port 1080 is another proxy protocol. Other ports are sometimes used, and an incorrectly configured web server can show the same behaviour.

Elimination of open proxies follows much the same pattern as elimination of open relays: examination of possible paths through one or more systems in the network and careful configuration and checking of firewalls, servers and client computers.

Introduction of Viruses and Other Malicious Software Through E-mail

If possible, use anti-virus software to scan incoming messages both at the mail server and on client computers; keep it up to date and regularly scan all the computers as viruses may arrive by routes other than e-mail.

Trojan Software Performing Bulk Mail Abuse

Software introduced into servers or client computers as a worm or virus by user indiscretion or by some intrusion may act as a proxy or may originate bulk mail on its own. Such rogue software installed through a system compromise can be very hard to detect on the machine affected, but routine monitoring of patterns of network traffic can alert the administrator to an incident and the headers of any mail sent will normally give some pointers to the source. It will often be necessary to rebuild a machine after such damage, and then try to find how the intrusion occurred to reduce the likelihood that it will happen again.

Further information on the use of e-mail, for both organisations and individuals can be found in Appendix 12.

Source URL: https://community.jisc.ac.uk/library/janet-services-documentation/open-mail-relays-janet

Links
[1] http://www.mail-abuse.com
[2] https://community.ja.net/library/janet-services-documentation/dns-block-lists
[3] https://community.ja.net/library/janet-services-documentation/spam-relay-tester-and-notification-system
[4] https://community.ja.net/library/janet-services-documentation/janet-csirt