Subject: Open Mail Relay
Posted by KDCnetgroup on Wed, 01 Sep 2004 13:36:18 GMT

We are having e-mails come into our system with our domain name ghosted. Does NoSpamToday block this or is this a feature enhancement? We have another firewall on the otherside but it also is not blocking for some reason and we are trying to get this to stop.

Subject: Re: Open Mail Relay
Posted by support on Wed, 01 Sep 2004 13:45:04 GMT

> We are having e-mails come into our system with our domain
> name ghosted. Does NoSpamToday block this or is this a feature
> enhancement? We have another firewall on the otherside but it
> also is not blocking for some reason and we are trying to get
> this to stop.

You can try using the "HostRejectList" feature to block these mails.
Put the IP address of the offending mail hosts onto your host reject list, by adding a line like this to your nospamtoday.cf file:

HostRejectList=11.22.33.44

After restarting the NoSpamToday! service, every time someone from this address tries to send an email will receive an error response. Note that the HostRejectList option also supports wild cards: Use HostRejectList=11.22.33.* or similar to reject IP address ranges.

If you use a firewall with network address translation (NAT), NoSpamToday! will no longer be able to see the real host address of the incoming connection, instead all incoming connections are forwarded from the firewall. The incoming host addresses in this case will be something like 10.x.x.x or 192.168.x.x.
In this case, the HostRejectList settings cannot be used.
Instead, you can use the HeloRejectList. With this configuration setting, NoSpamToday! looks at the name the incoming mail transfer agent (MTA) supplies with the SMTP HELO/EHLO command to find out where a connection originates. In all other aspects the HeloRejectList setting is similar to the HostRejectList setting.