

Re: TCPIP Services for OpenVMS V5.4 ECO1 anti spam feature

Source: <http://unix.derkeiler.com/Newsgroups/comp.os.vms/2004-05/2173.html>

From: John E. Malmberg (*wb8tyw_at_ql.network*)

Date: 05/29/04

Date: Sat, 29 May 2004 00:12:23 -0400

Jonathan Boswell wrote:

>

> *Oh rats. That explains why it's not working. So by "client", HP really means "last relay". This is useless in my present circumstance since I have never seen the outblaze.com spammers use the same relay twice.*

Outblaze is known for prompt nuking of spammers or blocking of any spam sources, but they are a very large ISP for their geographical area.

From every anti-spam forum on the Internet that I monitor, Outblaze is well known to terminate spammers on their networks as fast as possible.

Much faster than many other ISPs.

You can not trust the I.P. address that a relay that delivers spam to you claims it got it from, unless you control the relay.

Spammers routinely inject spam through a compromised machine with fake headers to make it look like it came from another network.

Essentially they are expecting that if the mail server accepted the spam, then the any user content filter would then check the fake headers that the spammer inserted, and send the abuse report there.

If you get a spamcop.net account (free and paid versions available) you can use the parser showing technical details to see where the parser is detecting the spam coming from. This is good for a postmortem to improve your spam defenses.

[Care is needed when reporting spam through spamcop.net. while usually accurate, it can by mistake allow you to report your own mailserver as the source of the spam]

As a mail message passes through each relay, a line is added by each to indicate the path.

The spamcop.net parser checks each line from the mail servers from the last one to see if every thing matches, and also checks several public reports to see if the alleged mail server is listed as a DHCP host, open proxy, or open relay.

If the spamcop.net parser finds a mis-match in what the relay claims to be it's name and the names that it's DNS servers give for it, or if it finds that an open relay, open proxy, or apparent DHCP address, it stops the parse and does not trust it further.

It is a more sophisticated test than most spam filters, and while not perfect, it is pretty accurate. It does make the occasional error, either due to software bugs, misconfigured DNS servers, or general internet errors that can give incorrect DNS information.

-John
wb8tyw@qsl.network
Personal Opinion Only