

## Re: A flood of spams – another virus on the way?

**Source:** <http://unix.derkeiler.com/Newsgroups/comp.os.vms/2003-09/1754.html>

---

**From:** Don Sykes (*anonymous\_at\_pacbell.net*)

**Date:** 09/20/03

Date: Sat, 20 Sep 2003 19:32:50 GMT

As I've been complaining about recently, I can't even get the HP SMTP service to check incoming messages for a valid user during the initial connection, which IIRC could be done in the 2nd step of the connection process!

This most recent onslaught of crap is just another example of what the problem REALLY is – i.e. no check points along the email path. In the current SMTP model the only one who even has an opportunity to block spam & assc viruses is the end recipient. This means that even if you have a "good filter" on your email reader and don't ever "see" the bad emails, an enormous amount of bandwidth is taken up on the internet, because each piece of crap sent out gets the same treatment all along the way to the destination user. Only then do we get a chance to ignore it. So who's at fault? Our own industry for embracing tcpip/smtp as the holly grail in its original form – i.e. no forced checkpoints. As I see it any ISP that is authorized to hand out an IP address s/b responsible for its misuse. They should at minimum be required to check the source of all email to be sure it's valid and has not been spoofed. Further each of the ISP's customers should have to register an approximate number of emails they will be sending out in any one day. Then if they grossly exceeded that, the initial ISP router should reject further emails and immediately inform their customer of the action. Any ISP failing to do this should have their IP addresses revoked or put on a lookaside list of all legit routers and not route emails from them.

Granted this is a half-baked idea at this point, but if WE, as a community, are ever going to stop this madness, we're going to have to come up with a technical solution at a fundamental, routing level; not just add more and different filters for the end user to implement.

--

Have VMS, Will Travel  
Wire paladin, San Francisco  
(paladinATalphaseDOTcom)  
Paul Sture wrote:

>

> More spams. Is this another virus / worm on the loose?

>

> Since 13:44 CET yesterday I have received some 114 spam messages (oops, another

## comp.os.vms: Re: A flood of spams – another virus on the way?

```
> one just came in) in this account.
>
> Normally I just get 3 or 4 per day. Spam filters are in place and the last
> time they were adjusted was for the last round of email attacks - SoBig.F
>
> I don't have time to analyze the contents of any at the moment, but here's
> a summary for the rest of you:
>
> $ mail
>
> You have 112 new messages.
>
> MAIL> dir
>
>
> # From Date Subject NEWMAIL
>
> 1 MX%"rcfgam-svmrgrq@n 18-SEP-2003 new microsoft patch
> 2 MX%"amailprogram@roc 18-SEP-2003 Returned Message
> 3 MX%"eknlmalraq_57934 18-SEP-2003 Network Security Pack.
> 4 MX%"rob@mirr.demon.n 18-SEP-2003 Newest Microsoft Critical Patch
> 5 MX%"qmailengine@amer 18-SEP-2003 failure message
> 6 MX%"smtpautomat@yahoo 18-SEP-2003 Failure Announcement
> 7 MX%"kuraokmiignvzm@n 18-SEP-2003 New Internet Critical Patch
> 8 MX%"checkme2003@yahoo 18-SEP-2003 Absolutely FREE!!! Time:12:38:55 PM
> 9 MX%"tixqspiniqtek_fm 18-SEP-2003 Latest Internet Upgrade
> 10 MX%"tlgthochrtra-nzb 18-SEP-2003
> 11 MX%"cmailprogram@yah 18-SEP-2003 Failure Letter
> 12 MX%"kmailengine@aol. 18-SEP-2003 Abort Advice
> 13 MX%"yqhmxezrgggdvci@ 18-SEP-2003 new microsoft critical patch
> 14 MX%"conch49@bellsout 18-SEP-2003 Latest Update
> 15 MX%"mailerrobot@free 18-SEP-2003 abort advice
> 16 MX%"mailroutine@bigf 18-SEP-2003 Undelivered Message User unknown
> 17 MX%"MAILER-DAEMON@bo 18-SEP-2003 Virus warning
> Press RETURN for more...
>
> MAIL>
>
> # From Date Subject NEWMAIL
>
> 18 MX%"MAILER-DAEMON@bo 18-SEP-2003 Virus warning
> 19 MX%"srwmuivjriglae@f 18-SEP-2003 Net Critical Update
> 20 MX%"emailbot@aol.com 18-SEP-2003 Message
> 21 MX%"xnfirkakou@newsl 18-SEP-2003 newest net patch
> 22 MX%"gbivjcjvmebyoz-o 18-SEP-2003 Current Security Patch
> 23 MX%"masterdaemon@fre 18-SEP-2003 Mail: Returned To Sender
> 24 MX%"jfdpecdd-zqoklwg 18-SEP-2003 Newest Internet Security Upgrade
> 25 *** valid message here ***
> 26 MX%"postservice@micr 18-SEP-2003 Failure Announcement
> 27 MX%"mcbroom5@teluspl 19-SEP-2003 Abort Message
> 28 MX%"spdytmvqwdcrkx@ 19-SEP-2003 New Security Upgrade
> 29 MX%"quceoievmhfnm-l 19-SEP-2003 Latest Net Patch
> 30 MX%"mimi-6@comcast.n 19-SEP-2003 Internet Update
> 31 MX%"emailprogram@roc 19-SEP-2003 Bug Notice
> 32 MX%"Antivirus-Daemon 19-SEP-2003 Recipient Virus-alert (sender: wibi@sybe
> 33 MX%"tpbjvsxt-psvzeyw 19-SEP-2003 Latest Network Upgrade
> 34 MX%"mailerservice@ro 19-SEP-2003 Undeliverable Message: Returned To Maile
> Press RETURN for more...
>
> MAIL>
>
> # From Date Subject NEWMAIL
```

comp.os.vms: Re: A flood of spams – another virus on the way?

> 35 MX%"vzzaampltzt@tech 19-SEP-2003 Newest Internet Update  
> 36 MX%"sjolmws\_mmsfa@yy 19-SEP-2003 Current Internet Security Update  
> 37 MX%"aeskfojazs@advis 19-SEP-2003 Latest Internet Patch  
> 38 MX%"amaildaemon@amer 19-SEP-2003 Report  
> 39 MX%"fgaxksowjxe\_cxri 19-SEP-2003 New Security Pack  
> 40 MX%"dennisonk@adalp 19-SEP-2003 advice  
> 41 MX%"vrcxctaxxskau@co 19-SEP-2003 Last Security Update  
> 42 MX%"jsjssekkggesmh@up 19-SEP-2003 Newest Microsoft Critical Pack  
> 43 MX%"masterbot@yahoo. 19-SEP-2003 Undelivered Message: Returned To Mailer  
> 44 MX%"webroutine@rocke 19-SEP-2003 Undeliverable Mail: Returned To Sender  
> 45 MX%"zmailautomat@mic 19-SEP-2003 Announcement  
> 46 MX%"fdjiybui@bulleti 19-SEP-2003 New Internet Critical Patch  
> 47 MX%"postdaemon@micro 19-SEP-2003 Undelivered Mail: Returned To Sender  
> 48 MX%"vfdujxlayoougai\_ 19-SEP-2003 Last Internet Critical Pack  
> 49 MX%"tmdyvsf@newslett 19-SEP-2003 last microsoft critical pack  
> 50 MX%"mailerform@purem 19-SEP-2003 Returned Message User unknown  
> 51 MX%"noinjbqxfomyiz\_h 19-SEP-2003 Last Internet Security Upgrade

> Press RETURN for more...

>

> MAIL>

> NEWMAIL

#	From	Date	Subject
52	MX%"emailprogram@aol	19-SEP-2003	Bug Notice
53	MX%"ccumfrmlhsvezne_	19-SEP-2003	Net Security Update
54	MX%"xvhehc@newslette	19-SEP-2003	Internet Critical Upgrade
55	MX%"webform@yahoo.co	19-SEP-2003	Bug Notice
56	MX%"lnlhqdqvk-nncvtq	19-SEP-2003	Latest Microsoft Critical Upgrade
57	MX%"pvlqyz@confidenc	19-SEP-2003	Latest Network Update
58	MX%"emailautomat@roc	19-SEP-2003	
59	MX%"ktztcmnppffjyh@	19-SEP-2003	Newest Internet Critical Pack
60	MX%"postdaemon@purem	19-SEP-2003	message
61	MX%"vjjnawljmkk-avqm	19-SEP-2003	Latest Network Security Update
62	MX%"mailservice@rock	19-SEP-2003	notice
63	MX%"MAILER-DAEMON@cn	19-SEP-2003	message
64	MX%"hqjgmna@updates	19-SEP-2003	Last Microsoft Security Upgrade
65	MX%"webautomat@ameri	19-SEP-2003	Message: User unknown
66	MX%"jfzaopfimsuj-qfl	19-SEP-2003	New Net Critical Update
67	MX%"azncwoj_osqtv@u	19-SEP-2003	Latest Network Security Update
68	MX%"zmmcc1kfkqvande-	19-SEP-2003	Latest Internet Upgrade

> Press RETURN for more...

>

> MAIL>

> NEWMAIL

#	From	Date	Subject
69	MX%"mailprogram@bigf	19-SEP-2003	Failure Notice
70	MX%"vkckdghoseko@new	19-SEP-2003	Internet Critical Pack
71	MX%"smtpautomat@netm	19-SEP-2003	
72	MX%"twestzrshxsl_qbb	19-SEP-2003	Latest Internet Critical Update
73	MX%"eagabohf_wvopm@n	19-SEP-2003	New Update
74	MX%"emailform@netmai	19-SEP-2003	Undelivered Message: Returned To Sender
75	MX%"fdwetxnrikiatn_z	19-SEP-2003	Last Upgrade
76	MX%"webprogram@freem	19-SEP-2003	error message
77	MX%"owypdvkvddffd_hp	19-SEP-2003	Latest Critical Update
78	MX%"mailerengine@aol	19-SEP-2003	Error Message
79	MX%"shposik@wpube.co	19-SEP-2003	latest microsoft critical update
80	MX%"gdadlhc_lhvwztr	19-SEP-2003	Latest Internet Pack
81	MX%"masterrobot@free	19-SEP-2003	failure advice
82	MX%"mailerdaemon@aol	19-SEP-2003	Notice
83	MX%"vyqltjy@newsle	19-SEP-2003	
84	MX%"vapxjfszdo@suppo	19-SEP-2003	Latest Patch

## comp.os.vms: Re: A flood of spams – another virus on the way?

```
> 85 MX%"mwoxbkemhk@updat 19-SEP-2003 Newest Microsoft Critical Pack
> Press RETURN for more...
>
> MAIL>
>
> # From Date Subject NEWMAIL
>
> 86 MX%"postdaemon@ameri 19-SEP-2003 returned message
> 87 MX%"postrobot@rocket 19-SEP-2003 Error Letter
> 88 MX%"qfhorntdlsqfku@t 19-SEP-2003 Network Upgrade
> 89 MX%"bjugiww@bulletin 19-SEP-2003 Pack
> 90 MX%"haashk@netvigato 19-SEP-2003 Undelivered Mail: User unknown
> 91 MX%"mcnjbhpc-oafi@bu 19-SEP-2003 Current Security Patch
> 92 MX%"webbot@america.c 19-SEP-2003
> 93 MX%"qdgono-rgrb@new 19-SEP-2003 New Microsoft Patch
> 94 MX%"cpuguqqidnjvg_or 19-SEP-2003 New Internet Security Update
> 95 MX%"fnzusou_cvnhcso@ 19-SEP-2003 New Net Security Patch
> 96 MX%"postdaemon@yahoo 19-SEP-2003 bug message
> 97 MX%"bmailrobot@ameri 19-SEP-2003 Bug Report
> 98 MX%"pxrjnr_lgmzyg@bu 19-SEP-2003 Last Microsoft Update
> 99 MX%"reoyqoj_gcrutohu 19-SEP-2003 Security Patch
> 100 MX%"webautomat@rocke 19-SEP-2003 Bug Advice
> 101 MX%"xovfjaqjm_opjtif 19-SEP-2003 Latest Net Security Patch
> 102 MX%"mailerengine@fre 19-SEP-2003 Announcement
> Press RETURN for more...
>
> MAIL>
>
> # From Date Subject NEWMAIL
>
> 103 MX%"mplrco-tmmppz@co 19-SEP-2003 Current Microsoft Critical Patch
> 104 MX%"mailerprogram@am 19-SEP-2003 Notice
> 105 MX%"eqokxhwcarcj@new 19-SEP-2003 New Network Security Update
> 106 MX%"mailbot@yahoo.co 19-SEP-2003 Undelivered Message: Returned To Sender
> 107 MX%"imdupgds_bbsvdrl 19-SEP-2003 Latest Net Patch
> 108 MX%"mailservice@yaho 19-SEP-2003 Mail: Returned To Sender
> 109 MX%"ekjlwjephctmtx_h 19-SEP-2003 new net critical update
> 110 MX%"szjdrqhozxy-lhc 19-SEP-2003 last internet critical pack
> 111 MX%"smtprobot@freema 19-SEP-2003 error notice
> 112 MX%"maildaemon@netma 19-SEP-2003 Undeliverable Message: User unknown
>
> MAIL>
>
> And another just arrived.
>
> Now, these appear to be junk addresses, but allegedly coming from valid
> domains - msn.com, msn.net, yahoo.com, microsoft.com, support.com and other
> well known ones.
>
> 99% seem to be coming from .net and .com addresses, so I also wonder
> whether this could be a side effect of the VeriSign change -
> reverse lookups and RBLs not functioning properly anymore ??
>
> Meanwhile on checking another email account, I see my spam filter there
> caught one entitled "PayPal Account Security Measures". This one is
> inviting me to verify my account details. Nope. Not going there...
>
> And they are still rolling in by the minute. Definitely not a good day
> for email.
```