Understanding SPAM headers

Environment

Netmail Secure 5.4.x and later releases

Synopsis

With the release of Netmail Secure 5.4, Netmail simplified the information presented in the headers regarding items deemed to be SPAM.

The tag X-MplusSpamScore: has been made obsolete by the X-MplusEngineMask.

Details

SPAM3:

Level	Definition
0	Not Spam
1	Never Seen
2	Unused
3	Bulk
4	Spam

SPAM4:

Category	Definition
1	Sender Spammy Reputation
2	URL Spammy Reputation
3	HTML Formatting
4	Spam Tricks: Obfuscation
5	HTML Image Spam
6	URL formatting hosting service domain
7	Spammy keyword Stocks
8	Spammy keyword Porn
9	Spammy keyword Drugs
10	Spammy keyword Loans
11	Spammy keyword Degrees
12	Spammy keyword Software
13	Spammy keyword Dating
14	Spammy keyword Free stuff
15	Spammy keyword Advance Fee Fraud
16	Spammy keyword Marketing

17	Spammy keyword Lottery
18	Spammy keyword Internet Business
19	Email header inconsistency
20	Virus
21	Phish
22	Replica
23	Generic spam indicator
24	Ham indicator
25	Other

SPAM5:

Level	Definition
1	SPAM
2	Virus
3	Bounces
10	Mainstream Newsletters
11	Miscellaneous Newsletters
12	Bad Newsletters
13	Social Media

X-MplusEngineMask Values:

Bits	Value	Meaning
0000 0000	0	None
0000 0001	1	SPAM5
0000 0010	2	DBL/URIBL/etc (SURBL Agent)
0000 0100	4	SPAM3
0000 1000	8	SPAM4
0001 0000	16	AntiMasking / Anti Spoofing
0010 0000	32	ZetaScan

Bits	Value	Meaning
0000 0011	3	SPAM5 + URIBL
0000 0101	5	SPAM5 + SPAM3
0000 0110	6	URIBL + SPAM3
0000 0111	7	SPAM5 + URIBL + SPAM3
0000 1001	9	SPAM5 + SPAM4

0000 1010	10	URIBL + SPAM4
0000 1011	11	SPAM5 + URIBL + SPAM4
0000 1100	12	SPAM3 + SPAM4
0000 1101	13	SPAM5 + SPAM3 + SPAM4
0000 1110	14	URIBL + SPAM3 + SPAM4
0000 1111	15	SPAM5 + URIBL + SPAM3 + SPAM4
0001 0001	17	SPAM5 + AntiSpoof
0001 0010	18	URIBL + AntiSpoof
0001 0011	19	SPAM5 + URIBL + AntiSpoof
0001 0100	20	SPAM3 + AntiSpoof
0001 0101	21	SPAM5 + SPAM3 + AntiSpoof
0001 0110	22	URIBL + SPAM3 + AntiSpoof
0001 0111	23	SPAM5 + URIBL + SPAM3 + AntiSpoof
0001 1000	24	SPAM4 + AntiSpoof
0001 1001	25	SPAM5 + SPAM4 + AntiSpoof
0001 1010	26	URIBL + SPAM4 + AntiSpoof
0001 1011	27	SPAM5 + URIBL + SPAM4 + AntiSpoof
0001 1100	28	SPAM3 + SPAM4 + AntiSpoof
0001 1101	29	SPAM5 + SPAM3 + SPAM4 + AntiSpoof
0001 1110	30	URIBL + SPAM3 + SPAM4 + AntiSpoof
0001 1111	31	SPAM5 + URIBL + SPAM3 + SPAM4 + AntiSpoof
0010 000	32	ZetaScan

Spam Header Example 1:

X-Mplus-Spam-Scanned: mplusversion: 5.4.5.26-debug; timestamp: Fri, 05 Feb 2016 15:27:25 -0500
engine: XCFSPAM3 Engine; version: 8.00.0106; level: 1
ref: str=0001.0A020201.56B505D6.024A,ss=1,re=0.000,recu=0.000,reip=0.000,cl=1,cld=1,fgs=0
status: success;error: none
engine: XCFSPAM4 Engine; version: 8.0.2/2016.02.05.10.19.59/2005.02.11.04.44.13/; level: 99
ref: 1 22, 4 30, 19 48
status: success;error: none
X-MPlusSpamScore: 3
X-MPlusEngineMask: 4 **(Value 4 is 0100, so only SPAM engine 4 caught this as spam)**

Spam Header Example 2:

X-Mplus-Spam-Scanned: mplusversion: 5.4.5.26-debug; timestamp: Fri, 05 Feb 2016 15:57:31 -0500
engine: XCFSPAM3 Engine; version: 8.00.0106; level: 4
ref: str=0001.0A020206.56B50CDC.0132,ss=1,re=0.000,recu=0.000,reip=0.000,pt=F_4810712,cl=4,cld=1,fgs=0
status: success;error: none
X-MPlusSpamScore: 5
X-MPlusEngineMask: 8 **(Value 8 is 1000, so only SPAM engine 3 caught this as spam)**

Spam Header Example 3:

X-Mplus-Spam-Scanned: mplusversion: 6.0.0.1438630642-debug; timestamp: Fri, 29 Jan 2016 11:25:56 -0500
engine: XCFSPAM4 Engine; version: 8.0.2/2016.01.29.08.41.51/2005.02.11.04.44.13/; level: 99
ref: 1 100

status: success;error: none
engine: XCFSPAM3 Engine; version: 8.00.0106; level: 4
ref: str=0001.0A090205.56AB9215.001D,ss=4,sh,re=0.000,recu=0.000,reip=0.000,cl=4,cld=1,fgs=8
status: success;error: none
engine: XCFSPAM5 Engine; version: Vade Retro 01.387.06#88 (01.386.00) AS+AV+AP+RT Profile: NETMAIL,VRUnsubscribe; Bailout: 300; level: 1
ref:
gggruggvucftvghtrhhoucdtuddrfeekjedrtdeigdekkeculddtuddrfeekiedrtddtmdcutefuodetggdotefrodftvfcurfhrohhfihhlvgemucfpgffvofetkffnpdggtfgfnh
hsuhgsshgtrhhisggvnecuuegrihhlohhuthemuceftddtnecujfgurhcuheduuddtucdlvddttddmnedhkfhnvhhishhisghlvgcufihorhgushculdehtddmnegfrhhlu
cfvnfffucdlqdehmdenoggfufdqpfefjeelqdegieculdeftddtmdenucfjughrpefvkffhufhrgggtffesrgdttdfotddtvdenucfhrhhomhepofeutecuuggvghhrvggvuch
ophhtihhonhhsuceoufgrrhgrhhesfihgihhhohhtvghlrdgtohhmqeenucffohhmrghinhepfihgihhhohhtvghlrdgtohhmpdgslhhsrdhgohhvpdgvugdrghhovhe
nucfrrghrrghmpehhvghlohepughurhgrnhhothhitgguohhorhdrfihgihhhohhtvghlrdgtohhmpdhinhgvthepudeivddrvddugedrvddurdejjedpmhgrihhlfhhroh
hmpeeolfgvrhgvmhhirghhofhilhhlshesughurhgrnhhothhitgguohhorhdrfihgihhhohhtvghlrdgtohhmqecuuefqffgjpeekuefkvffokffogfdprhgtphhtthhopee
ouggrnhesghifthhoohhlshdrtghomheq/545/Unsub=http://rex.wgihotel.com##To=<dan@gwtools.com##ReplyTo=<Sarah@wgihotel.com##From=MBA degree options <Sarah@wgihotel.com##
status: success;error: none
X-MPlusSpamScore: 9
X-MPlusEngineMask: 13 **(Value 13 is 1101, so SPAM engines 3,4,5 caught this as spam)**