Many Asterisk servers will have Postfix installed to accommodate the mail function (FreePBX, Elastix, A2Billing etc.). Any server open to the web with Postfix is especially interesting for lamers and injecting spambots.

If your server has been infected, finding a particular spambot script is easy.

Step 1: Temporarily stop Postfix

service postfix stop ~*or*~ pkill -9 postfix

Step 2: Show entire Postfix queue and select a random spambot-generated email:

postqueue -p

Step 3: Locate the script generating the spam email by tracing the email ID. Example:

postcat -q EMAILIDHERE 37D

Step 4: Clean or remove the infected script completely and start the Postfix service