Gauntlet Version 2.0

(For use with SmarterMail/IMail Only)

Pre-Tested Spam, by definition, the spammer pre-tests their campaigns against all available tests by sending samples to themselves on protected systems. When they have a version that gets past all of the tests deploy these messages in huge volumes with their bot-net. This tool is used to combat this technique.

Gauntlet Theory: http://www.lifeatwarp9.com/2012/06/gauntlet-a-solution-to-pre-tested-spam/

To Configure Gauntlet using Declude. ([PATH]= Please check actual directory locations for your server.)

1. Create a Directory called Gauntlet under your \Spool e.g. \Spool\ Gauntlet
2. Download the Gauntlet filter GAUNTLET.txt to you Declude\Filters Directory
3. Call the GAUNTLET.txt file from your global.cfg, ensure it is the last filter to be called.

   ```
   GAUNTLET   filter       [PATH]\Declude\Filters\GAUNTLET.txt   x   0   0
   ```

4. Add the following line to your $default$.junkmail file (or any per domain *.junkmail files you choose)

   ```
   GAUNTLET HOLD       [PATH]\Spool\Gauntlet
   ```

5. Download the DRGOutflow.exe utility and place in your C:\SmarterMail\Directory
6. Gauntlet uses the same service wrapper that Message Sniffer uses. Open the Windows Services area, stop the Message Sniffer service. Add these lines to your XYNTService.ini file typically located in the \Declude\SNF directory.

   ```
   [Process1]
   CommandLine = [PATH]\DRGOutflow.exe   i=[PATH]\Spool\Gauntlet   o=[PATH]\\spool\proc d=60
   PauseStart= 100
   PauseEnd= 100
   UserInterface = No
   Restart = Yes
   ```

7. The above will example will hold messages in the Gauntlet for 1 hours (d=60).
8. Re-Start the Message Sniffer service.
9. Gauntlet is now running.

Notes

The purpose of the gauntlet is to delay *suspect messages long enough for other Spam tests to be updated with the new information in order to catch the pre-tested spam.

As Message Sniffer updates it's rule-base every 30 min we suggest a minimum time period of 45 minutes for the Gauntlet. We have been running the Gauntlet successfully on two servers with over 1000 domains with only a handful of complaints of delay in the beginning which we have resolved.

*Suspect Messages

- Any Messages that are Whitelisted by SmarterMail/IMail or Declude will never be held by the Gauntlet.
- The Gauntlet filter is specifically designed to target messages that look like pre-tested spam, to reduce delaying good email.

If you need further assistance, questions or help setting this up please do not hesitate to contact us.

Mail's Best Friend
support@mailsbestfriend.com
www.mailsbestfriend.com
1. 866.919.2075

mail's best friend
If you work with eMail, you need Mail's Best Friend