Hijack Manual

Overview

Declude Hijack allows your users to send out Email easily while preventing spammers from relaying much mail through your mail server. This can be done without restricting users to specific IP addresses or requiring users to use SMTP authentication. The concept is simple: it works by only letting users send out a specific amount of mail in a given time period.

You will set 2 thresholds (which consist of a time period, and the amount of Email allowed within that time period). For example, the first threshold may be 20 Emails with 10 minutes, and the second threshold 100 Emails within 30 minutes.

Normally, all of a users' Email will go out when they sent it. However, if they reaches the first threshold (20 Emails within 10 minutes in this example), all subsequent Email is quarantined by Declude Hijack. If the second threshold is not reached (in this case, 30 minutes goes by without 100 Emails being sent), then the mail will be sent. However, if they reach the second threshold, the mail will be moved to a permanent holding directory and will not be sent out.

By default, Declude Hijack will log (to \spool\hi####.log) every Email that it scans. It will report whether the Email was incoming or outgoing, as well as whether it was quarantined temporarily or held permanently.

Basic Configuration

Declude Hijack comes with a default configuration that you don't have to change. The main configuration consists of RELAYTHRESHOLD1 and RELAYTHRESHOLD2. These define the two thresholds (when a user reaches the first, the mail is held temporarily; when the user reaches the second, the mail is held permanently). Both RELAYTHRESHOLD1 and RELAYTHRESHOLD2 have the same format: RELAYTHRESHOLD1 or RELAYTHRESHOLD2 followed by the time period, followed by the number Emails allowed in that time period. For example, to have Declude Hijack allow 20 Emails in 10 minutes as the first threshold, you would use "RELAYTHRESHOLD1 10 20".

If you need to allow Email from a specific IP address, you can add a line "ALLOWIP 127.0.0.1" to the \Declude\hijack.cfg file (replacing 127.0.0.1 with the IP address you wish to allow). The ALLOWIP will allow that IP address to send unlimited Email.

Example
Let's assume that your first threshold is 20 Emails within 10 minutes, and that your second threshold is 100 Emails within 30 minutes

User	What he sends	How Declude Hijack handles it
Low volume user	1:03PM: Sends 1 Email.	Declude Hijack sees the 1 Email at 1:03PM, and sends it (since he hasn't sent more than 20 Emails within 10 minutes yet).
		At 1:13PM, Declude Hijack sees that the user has only sent 1 Email during the 10 minute threshold, so it re-sets the settings for that user.
	3:35PM: Sends 1 Email.	At 3:35PM, Declude Hijack sees the 1 Email, and sends it (since he hasn't sent more than 10 Emails with 10 minutes yet).
RESULT: All of the low volume users' Emails go out.		

User	What he sends	How Declude Hijack handles it
High volume user	1:03PM: Sends 1 Email to 6 recipients.	Declude Hijack sees the 6 Emails at 1:03PM, and sends them (since he hasn't sent more than 20 Emails within 10 minutes yet).
	1:05PM: Sends 5 Emails, each to 1 recipient.	Declude Hijack sees that the user has only sent 11 Emails during the 10 minute threshold, so it sends these 5 Emails.
	1:07PM: Sends 1 Email to 15 recipients.	Declude Hijack sees that the user has sent 26 Emails in the past 4 minutes, so it does NOT send this Email. Instead, it holds it in \spool\spam\hold1.
	1:10PM: Sends 2 Emails each to 1 recipient.	These 2 Emails are held in \spool\spam\hold1, since the user has already reached the first threshold (they have sent out more than 20 Emails in the past 10 minutes).
		At 1:13, 10 minutes have passed, but Declude does nothing at this point, since it has already started quarantining the Email from this user.
	1:15PM: Sends 2 Emails each to 1 recipient.	These 2 Emails are held in \spool\spam\hold1, since the user has already reached the first threshold (they have sent out more than 20 Emails in the past 10 minutes).

		At 1:33, 30 minutes have passed, and since the user hasn't sent out 100 Emails yet, Declude sends out the Email that it had been quarantining and re-sets the settings for this user.
	1:35PM: Sends 2 Emails each to 1 recipient.	Declude Hijack sees the 2 Emails at 1:35PM, and sends them (since he hasn't sent more than 20 Emails within 10 minutes yet, since his information was reset at 1:33PM).
RESULT: All of the high volume users' Emails go out.		

User	What he sends	How Declude Hijack handles it
Spammer 1	1:03:20PM: Sends 1 Email to 15 recipients.	Declude Hijack sees the 15 Emails at 1:03PM, and sends them (since he hasn't sent more than 20 Emails within 10 minutes yet).
	1:03:25PM: Sends 1 Email to 15 recipients.	Declude Hijack sees that the user has sent 30 Emails in the past 5 seconds (more than 20 in 10 minutes), so it does NOT send these Emails. Instead, it holds them in \spool\spam\hold1.
	1:03:30PM: Sends 1 Email to 15 recipients.	Declude Hijack sees that the user has sent more than 20 Emails in the past 10 minutes, so it does NOT send these Emails. Instead, it holds them in \spool\spam\hold1.
	1:03:35PM: Sends 1 Email to 15 recipients.	Declude Hijack sees that the user has sent more than 20 Emails in the past 10 minutes, so it does NOT send these Emails. Instead, it holds them in \spool\spam\hold1.
	1:03:40PM: Sends 1 Email to 15 recipients.	Declude Hijack sees that the user has sent more than 20 Emails in the past 10 minutes, so it does NOT send these Emails. Instead, it holds them in \spool\spam\hold1.
	1:03:45PM: Sends 1 Email to 15 recipients.	Declude Hijack sees that the user has sent more than 20 Emails in the past 10 minutes, so it does NOT send these Emails. Instead, it holds them in \spool\spam\hold1.
	1:03:50PM: Sends 1 Email to 15 recipients.	At this point, the spammer has sent 105 Emails in under a minute. That's more than the 2nd threshold of 100 Emails in 30 minutes, so Declude Hijack permanently holds this and all following Emails in \spool\spam\hold2. It also takes the Email that was being quarantined in \spool\spam\hold1 and holds it permanently in \spool\spam\hold2.
	1:03:55PM: Sends 1 Email to 15 recipients.	Since the spammer has passed the 2nd threshold, he is banned, and all his Email gets held permanently in \spool\spam\hold2. He will only be able to send mail again if the Declude Console is closed... in which case he will get banned again as soon as he passed the 2nd threshold again.
RESULT: Only 15 of the spammer's Emails go out.		

User	What he sends	How Declude Hijack handles it
Spammer 2	1:03:20PM: Sends 1 Email to 50 recipients.	Declude Hijack sees that the user has sent 50 Emails just now, which is move than 20 in 10 minutes, so it does NOT send these Emails. Instead, it holds them in \spool\spam\hold1.
	1:03:25PM: Sends 1 Email to 50 recipients.	Declude Hijack sees that the user has sent 100 Emails in the past 5 seconds (more than 100 in 30 minutes), so the second threshold has been reached. It holds this Email peranently in \spool\spam\hold2, and moves the Email from \spool\spam\hold1 into \spool\spam\hold2 permanently.
	1:03:30PM: Sends 1 Email to 15 recipients.	Since the spammer has passed the 2nd threshold, he is banned, and all his Email gets held permanently in \spool\spam\hold2. He will only be able to send mail again if the Declude Console is closed... in which case he will get banned again as soon as he passed the 2nd threshold again.
	1:03:35PM: Sends 1 Email to 15 recipients.	Since the spammer has passed the 2nd threshold, he is banned, and all his Email gets held permanently in \spool\spam\hold2. He will only be able to send mail again if the Declude Console is closed... in which case he will get banned again as soon as he passed the 2nd threshold again.
	1:03:40PM: Sends 1 Email to 15 recipients.	Since the spammer has passed the 2nd threshold, he is banned, and all his Email gets held permanently in \spool\spam\hold2. He will only be able to send mail again if the Declude Console is closed... in which case he will get banned again as soon as he passed the 2nd threshold again.
	1:03:45PM: Sends 1 Email to 15 recipients.	Since the spammer has passed the 2nd threshold, he is banned, and all his Email gets held permanently in \spool\spam\hold2. He will only be able to send mail again if the Declude Console is closed... in which case he will get banned again as soon as he passed the 2nd threshold again.
	1:03:50PM: Sends 1 Email to 15 recipients.	Since the spammer has passed the 2nd threshold, he is banned, and all his Email gets held permanently in \spool\spam\hold2. He will only be able to send mail again if the Declude Console is closed... in which case he will get banned again as soon as he passed the 2nd threshold again.

	1:03:55PM: Sends 1 Email to 15 recipients.	Since the spammer has passed the 2nd threshold, he is banned, and all his Email gets held permanently in \spool\spam\hold2. He will only be able to send mail again if the Declude Console is closed... in which case he will get banned again as soon as he passed the 2nd threshold again.
RESULT: None of the spammer's Emails go out!		

Theory

Declude intercept all Email between the point at which it is received, and the point at which your mail server delivers it. This way, Declude catches all Email that goes through the mail server -- incoming and outgoing.

Oops, my customer's Email was held permanently!
Don't worry about this. It is easy to fix. If you already have spam in the \spool\spam\hold2 directory, you will need to find (in the log file) the IP address that the legitimate user was sending mail from. In the Declude\Tools\ folder there is a command line tool to help redeliver these messages.

Manual process Imail

Go to the \spool\spam\hold2 directory. Rename all the files (or, if there is spam in there from before, all files beginning with that IP address you just looked up) so that they start with a "Q" or "D" (for example, rename "127.0.0.1.IPQ1234567.SMD" to "Q1234567.SMD"). Then, copy them to the \spool directory, and IMail will send them out on the next queue run (typically 20-30 minutes).

Manual process Smartermail

Go to the \spool\spam\hold2 directory. Rename all the files (or, if there is spam in there from before, all files beginning with that IP address you just looked up) removing the IP address. Then, copy them to the \spool directory, and Smartermail will send them out on the next queue run.

Release Notes

You can view the release notes here