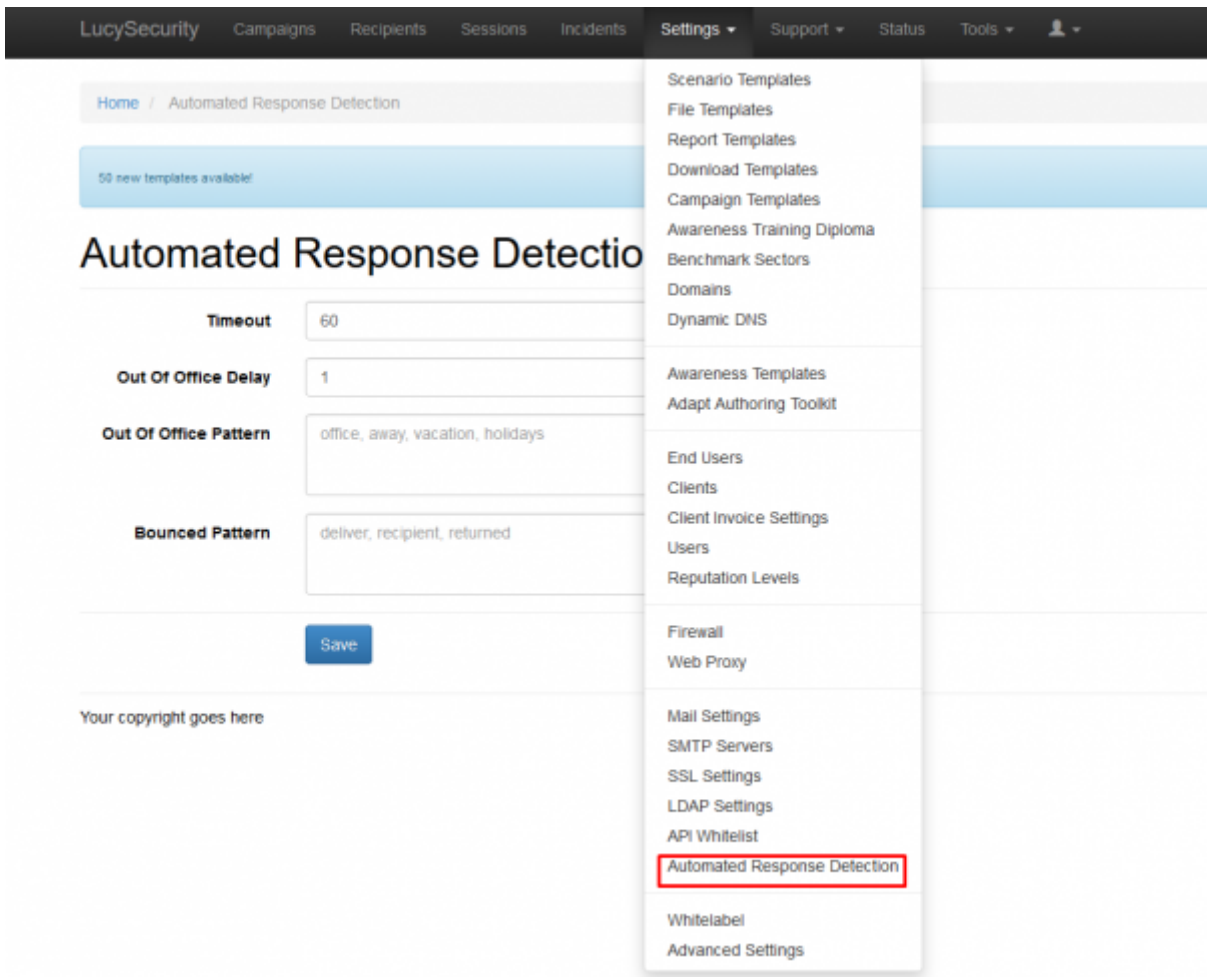# Response Detection

For accurate statistics, Lucy has the functionality to work with emails that came in response to a phishing email. Thus, you can determine which of the recipients did not actually receive the e-mail or do not include the auto-responses in the statistics.

You could change settings of Automated Response Detection here:

There are 4 main types of track responses settings:

Automated Response Detection

1 **Timeout**   60

2 **Out Of Office Delay**   1

3 **Out Of Office Pattern**   office,away,vacation,holidays

4 **Bounced Pattern**   error 450, not found

Save

1. Emails returned immediately after sending a phishing emails are most likely an auto-reply. If an email will arrive within the given period (in seconds) after submitting an attack email, the incoming email will be treated as an automated response.
2. The best way to coverage all recipients in a campaign is to resend phishing email to victims who for some reason set up an automated response. Since most likely the victim is not in the workplace or he does not read the email, it is best to resend the message in a few days. In this field, specify number of days to wait until sending a reminder for the victim that is out of office.
3. Patterns to find in replies to mark them as 'out of office' responses. For example its can be patterns related with holidays or business trip. A repeated email will arrive in the number of days specified in "Out Of Office Delay"
4. Each mail server has its own template of bounced emails. In this field, you can specify pattern to find in replies to mark them as 'bounced' responses or some errors from mail server.

From:
https://wiki.lucysecurity.com/ - **LUCY**

Permanent link:
https://wiki.lucysecurity.com/doku.php?id=response_detection&rev=1548769524

Last update: **2019/07/25 12:50**