Subscription Bomb aka List Bomb

This article applies to:

Definition:

Subscription bombing or List Bombing as it is commonly referred to is when spambots (automated computer programs) submit fraudulent information through lead collection forms on websites. This may also be referred to as form abuse or mail bombing.

The intentions of subscription bombing can be but not limited to:

- Harassing the address owners by overwhelming their inbox with emails sent from every form the address was submitted to.
- Affect the sender reputation of the website owner and/or the email service provider that sends the email.
- Hide or distract the address owner from seeing legit account alerts like password resets or questionable login attempt emails.
- Harassing the company or ESP to trigger a denial-of-service (DoS) event

Why is this bad:

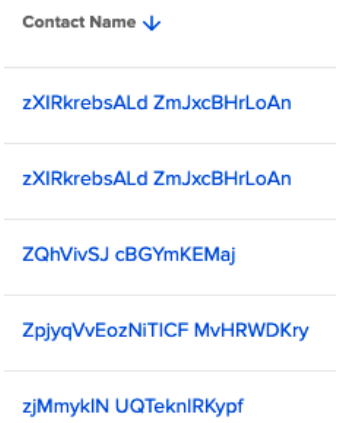
There are many problems associated with Subscription bombing. Examples are, fraudulent signups will trigger the sending of unsolicited email. This then causes increases in spam complaints, Hard Bounces, Unsubscribes and worst of all spam trap hits against the users and the ESP that sent the mail. These bad sign ups then force the sending of mail to fraudulent addresses.

This is a big issue, as sending too much mail in a short time frame—in these situations, potentially thousands or more at a time within a short time span—can result in your sending network (IP pool, domains, etc..) being blocked by the Internet service providers (ISPs: Gmail or Yahoo) or 3rd party email monitoring services The results can be devastating to the senders network as mail can be blocked from entire ISPs networks

What to do when this happens:

In the event this has happens to a user they should do the following:

- Pause/stop all automation that has any Lead capture attached to it.
- Secure any and all forms by adding some sort of security like reCaptcha
- Perform a list cleanup looking for fraudulent signups or patterns:
    - volume spikes in signups that are not common for the form
    - URLs in the First/Last name fields
    - Random Set of Letters, numbers or combinations including difference case for letters similar to this:



- Consider using a list cleaning service like klean13 (https://www.klean13.com/)
- Use other types of security services on your lead collection forms like List Cleaner and Spamkill
- Make sure any 3rd party site like Word press or Drupal that you have lead capture forms on is up to date and secure.

How to protect against this:

There are several tools that can be used to help prevent this.

- Use confirmed opt-in during the lead collection process also called double opt-in
- Add and use reCaptcha on lead capture forms
- Add a hidden field (also called honey pot) to you forms that only a bot could see/fill out and then tag those that have data in the field.
- Monitor lead collection stats for abnormalities looking for suspicious activity. They can be seen in odd names or domain info. In some cases, they might do things like the same value for first and last name or use random patterns of letters and numbers.
- Use other types of security services on your lead collection forms like List Cleaner and Spamkill