

Why are there false positives in the campaign?

Sometimes, it happens that campaign statistics do not correspond to the real number of clicks. For example, a campaign has just been stopped, the report has been generated and sent to the client. And the client responds that some of the recipients shown as clicked or successfully attacked did not actually click on the phishing link (or input data/download file). In 100% of cases, statistics discrepancy is produced by automated security measures and services.

Why this happened?

Most probably, Lucy IP address or domains used in the campaign has not been properly whitelisted on the recipient's side. Most of the mail servers and clients utilize global and built-in security measures that study the content of incoming email before delivering them to the recipient. In the case of Lucy emails, phishing links get clicked by such services in order to gather information about the source. Thus, Lucy web-server receives requests to unique URLs and considers those as clicks from real users. Some of the mail security tools before showing to the recipient put incoming email into the sandbox and proceed to all links and even download attachments or files from the landing page. Which may as well produce incorrect statistics from [Tracked opened emails tool](#).

How to avoid such issues in future campaigns?

Whitelisting Kindly contact the mail admins and security team in order to verify that tLucy IP address and/or domain names are properly whitelisted within the infrastructure. Though even arriving at the recipient's inbox, emails can produce incorrect statistics because the link has been already clicked by the bot.

Firewall Protection Interval The following [feature](#) provides a short interval at the beginning of the campaign (after email is sent) during which every click would be considered as automatically produced by security policies on the recipients end.

Filters Functionality that allows defining IP addresses from which Lucy will ignore any requests (clicks).

Testing The only way to find out if there are any security policies that may produce false positives mid-campaign is only to run several test campaigns to a small group of the recipients. During tests, one can find out IP addresses and policies prevent possible incorrect statistics.

From:
<https://wiki.lucysecurity.com/> - LUCY

Permanent link:
https://wiki.lucysecurity.com/doku.php?id=false_positives_in_campaign_statistics

Last update: **2021/06/28 15:02**

