Risk Assessment

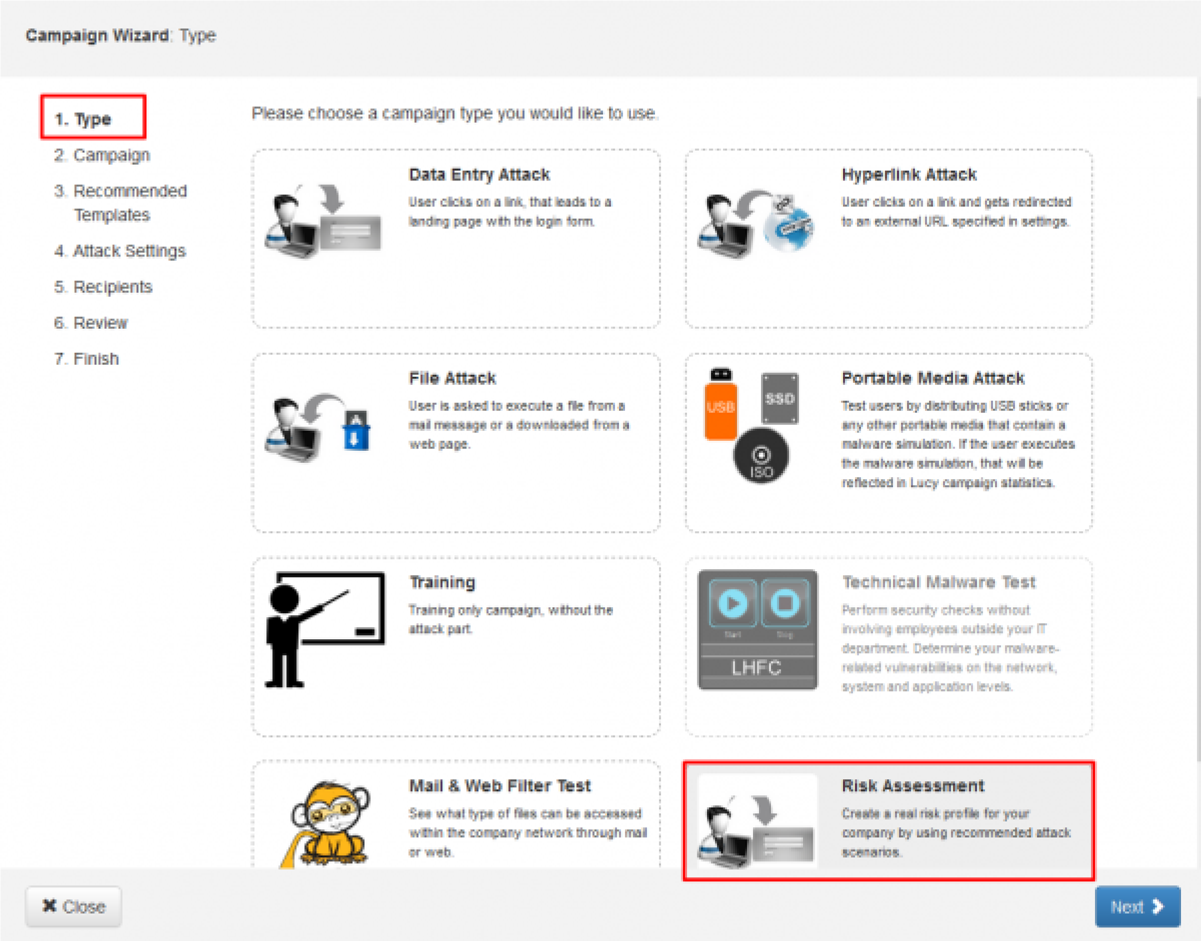
Instead of showing only raw data about how many users have been successfully phished, we can additionally provide a risk assessment methodology in LUCY, that shows the exposure to certain threats. We can classify different types of threats/Likelihoods such as

- Technical threats (e.g. unsecured windows PC, unsecure browser, etc.),
- Internal threat (e.g. uneducated user who clicks on certain content) and
- Externals threats through hackers (latest trends in attacks, e.g. exploiting a specific browser vulnerability).

In LUCY we implemented only a part of the 2nd analysis step and in the coming releases, this feature will be improved.

Using the risk assessment in LUCY

Select the campaign type "risk assessment" in campaign wizard:



Campaign Wizard: Type

Please choose a campaign type you would like to use.

Data Entry Attack
User clicks on a link, that leads to a landing page with the login form.

Hyperlink Attack
User clicks on a link and gets redirected to an external URL specified in settings.

File Attack
User is asked to execute a file from a mail message or a downloaded from a web page.

Portable Media Attack
Test users by distributing USB sticks or any other portable media that contain a malware simulation. If the user executes the malware simulation, that will be reflected in Lucy campaign statistics.

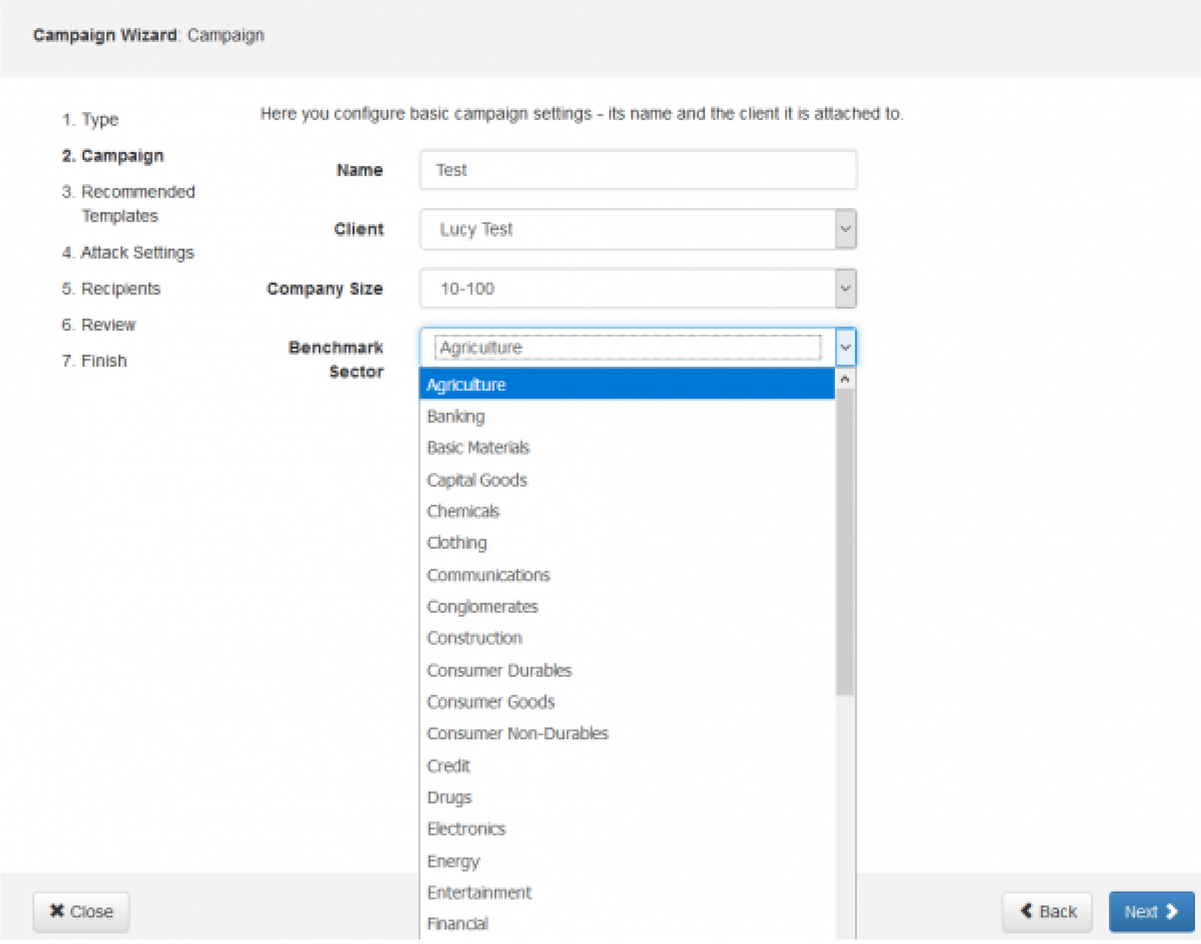
Training
Training only campaign, without the attack part.

Technical Malware Test
Perform security checks without involving employees outside your IT department. Determine your malware-related vulnerabilities on the network, system and application levels.

Mail & Web Filter Test
See what type of files can be accessed within the company network through mail or web.

Risk Assessment
Create a real risk profile for your company by using recommended attack scenarios.

Select your company size and industry type. Then you will be presented a recommended set of attack templates:



Campaign Wizard: Campaign

1. Type
2. **Campaign**
3. Recommended Templates
4. Attack Settings
5. Recipients
6. Review
7. Finish

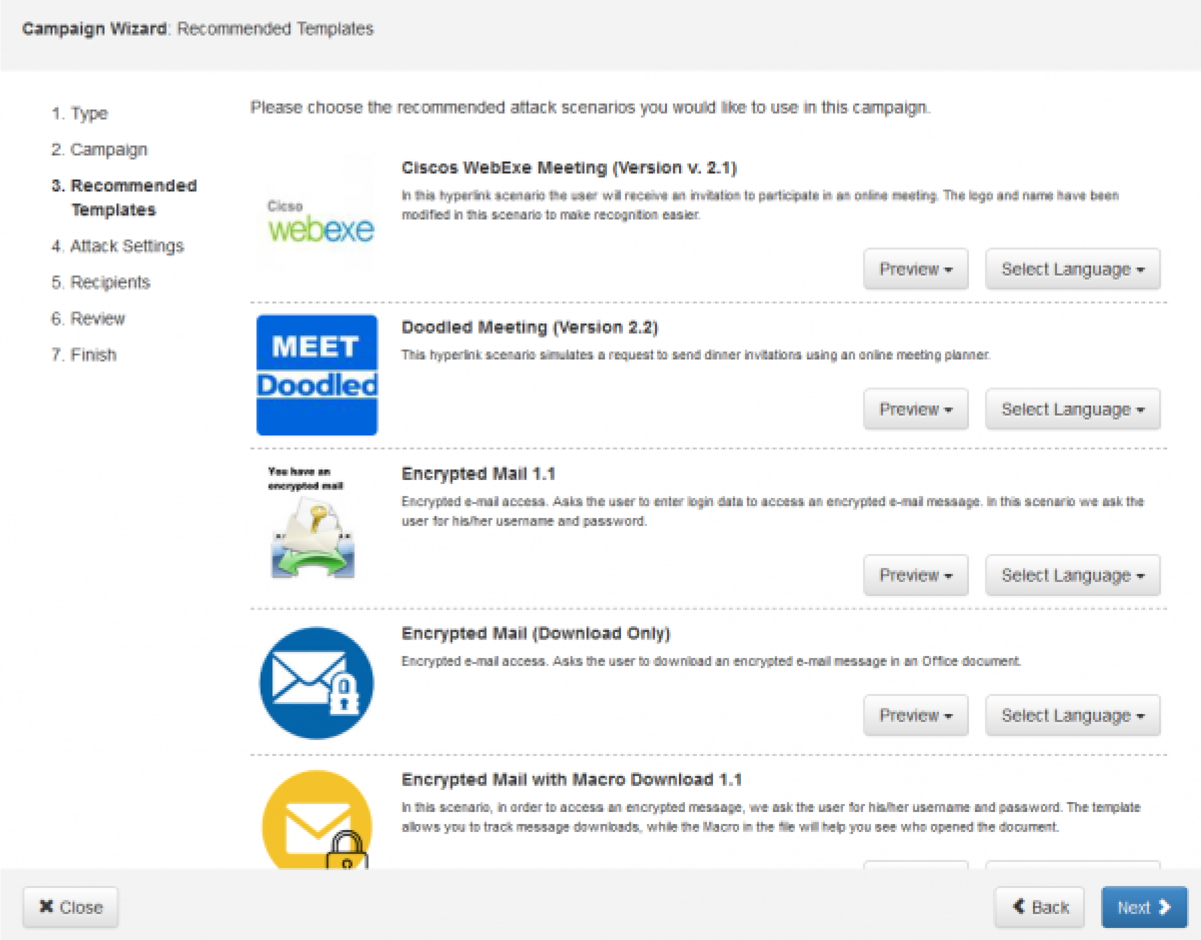
Here you configure basic campaign settings - its name and the client it is attached to.

Name Test

Client Lucy Test

Company Size 10-100

Benchmark Sector Agriculture



Campaign Wizard: Recommended Templates

1. Type
2. Campaign
3. **Recommended Templates**
4. Attack Settings
5. Recipients
6. Review
7. Finish

Please choose the recommended attack scenarios you would like to use in this campaign.

Ciscos WebExe Meeting (Version v. 2.1)
In this hyperlink scenario the user will receive an invitation to participate in an online meeting. The logo and name have been modified in this scenario to make recognition easier.

Doodled Meeting (Version 2.2)
This hyperlink scenario simulates a request to send dinner invitations using an online meeting planner.

Encrypted Mail 1.1
Encrypted e-mail access. Asks the user to enter login data to access an encrypted e-mail message. In this scenario we ask the user for his/her username and password.

Encrypted Mail (Download Only)
Encrypted e-mail access. Asks the user to download an encrypted e-mail message in an Office document.

Encrypted Mail with Macro Download 1.1
In this scenario, in order to access an encrypted message, we ask the user for his/her username and password. The template allows you to track message downloads, while the Macro in the file will help you see who opened the document.

Please try to use a variation of different attack types (hyperlink, web-based & file based) to get a better understanding, how your employees react to different threats. You will find the risk specific threats within the campaign statistics under "risk assessment".

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

Permanent link:
https://wiki.lucysecurity.com/doku.php?id=risk_assessment&rev=1561725216

Last update: **2019/07/25 12:52**