FILE BASED ATTACKS (INSIDE OUT)

Introduction

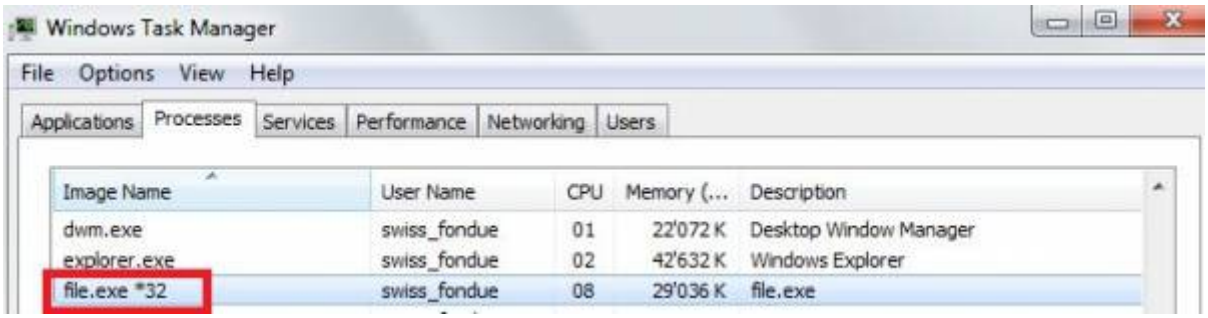
Inside-Out attacks try to initiate network connections from the trusted (corporate) to the untrusted (Internet) network. These attacks require that an “insider” execute code. This is usually because the person that executes the code is unaware of security issues and doesn’t realize that an application can do anything to their system within the limits of the access that is granted to that user. The inside out attack consists of three steps:

- STEP 1 Getting the backdoor in the network (delivery)
- STEP 2 Executing the backdoor by the user (execution)
- STEP 3 Sending the data out (output delivery)

LUCY's approach

With LUCY's file-based attack you are able to perform the following steps:

- **STEP 0 Trojan compilation**: Via the Web GUI you will be able to define the settings of the trojan simulation (e.g. what the file should look like & do upon execution). The trojan simulation can be either an executable (which gets compiled during the campaign), some payload which you upload to LUCY yourself or some Office file that contains a Macro.
- **STEP 1 Delivery**: The trojan simulation can be integrated into a landing page on LUCY so it may be downloaded from the clients or it can be attached in the mail.
- **STEP 2 Execution**: By using a phishing mail which can be edited on LUCY you can try to lure the recipient into opening the Trojan simulation. Once the Malware Simulation is executed on a Windows Client, you can see the file in the Task Manager as "file.exe". LUCY has some command restrictions to prevent LUCY administrators from damaging the client's system, therefore not all shell commands are allowed.

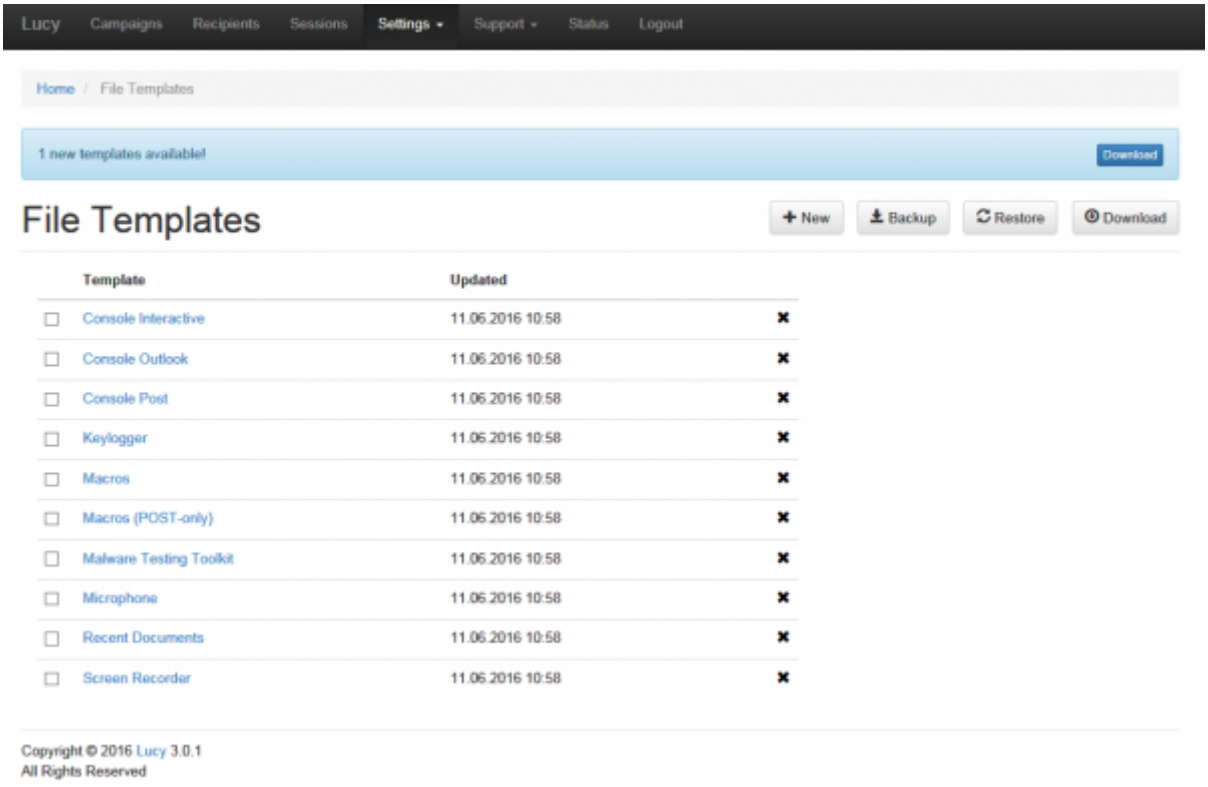


- **STEP 3 Output Delivery**: The files compiled by LUCY communicate back to your server using HTTP/HTTPS. Therefore LUCY needs to be reachable via those protocols to make the scenarios work.

Note: The files are non-intrusive, run only in the memory and have no effect on the System (no changes are made). In the current edition, the executable runs only on Windows (Windows 7/8).

File based attack simulation templates

LUCY can compile different custom Malware Simulations:

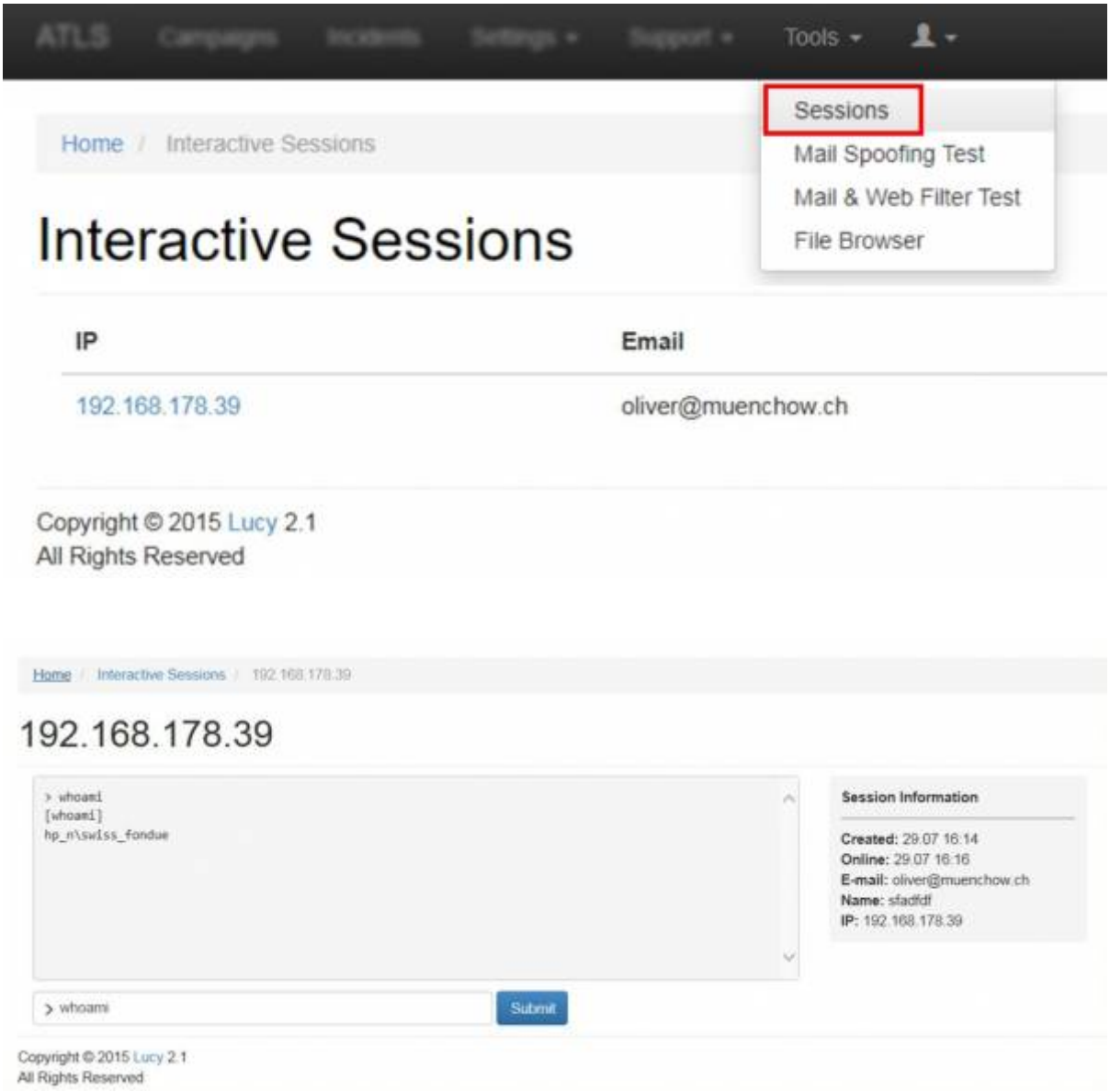


Each file type can be modified (layout, filetype, name) before using it in a campaign. Currently, LUCY comes with the following file types:

- **Consolepost**: Execute your commands within the Windows shell and send back the output to LUCY. This tool allows you to use a limited set of commands. Some commands in Windows are not executable. They are built into the command line (Example of command with executable: whoami). If you need to use a command which is a built-in command line, then you should call cmd directly (example for requesting the directory content: "cmd /c dir"). Here a list of possible commands.
- **Recentdocs**: Send back a predefined number of documents listed in the recent doc cache to LUCY.
- **ConsoleOutlook**: Execute commands and send the output back via Outlook (access Outlook hidden via MAPI) to a predefined email address. It also has the ability as a PoC to send back the subject line from last received email in Outlook.
- **Keylogger**: Record keys pressed on a keyboard for a short time period. Display GUI option may have a value of 0 to 4: 0 - no GUI, 1 - Progress Bar, 2 - Decryptor Window, 3 or 4 - Error Message Window.
- **Microphone**: Get audio recording from a microphone for a short period. Display GUI option may have a value of 0 to 4: 0 - no GUI, 1 - Progress Bar, 2 - Decryptor Window, 3 or 4 - Error Message Window.
- **WebRecorder**: Records screenshots and tries to access the webcam to record a few seconds as a PoC.
- **Ransomware Screenlocker**: Will lock the PC screen and ask the user to enter a password that

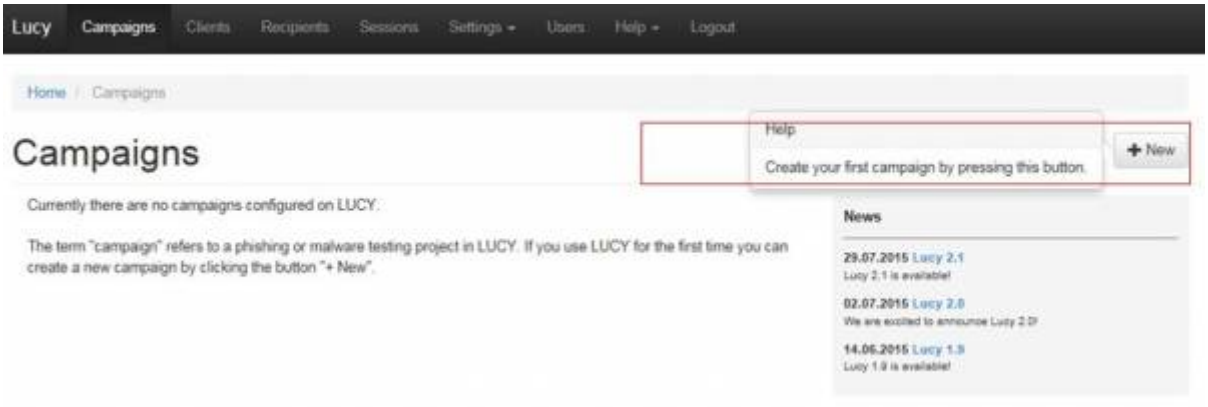
can be set in the backend. The idea is to have the user call some helpdesk to ask for the password to have a better learning effect.

- **ConsoleInteractive**: This tool allows you to establish a reverse HTTP/HTTPS channel to LUCY. Once the file has been executed, you can see the session in “Sessions”. The tool only runs in the memory (called “file” in Process View). After the termination, the session can no longer be established. You can click on the IP and start executing commands within the Windows shell. The output should appear after a few seconds automatically. This Tool only works with Windows 7/8 in combination with IE and Firefox. More background info can be found here.

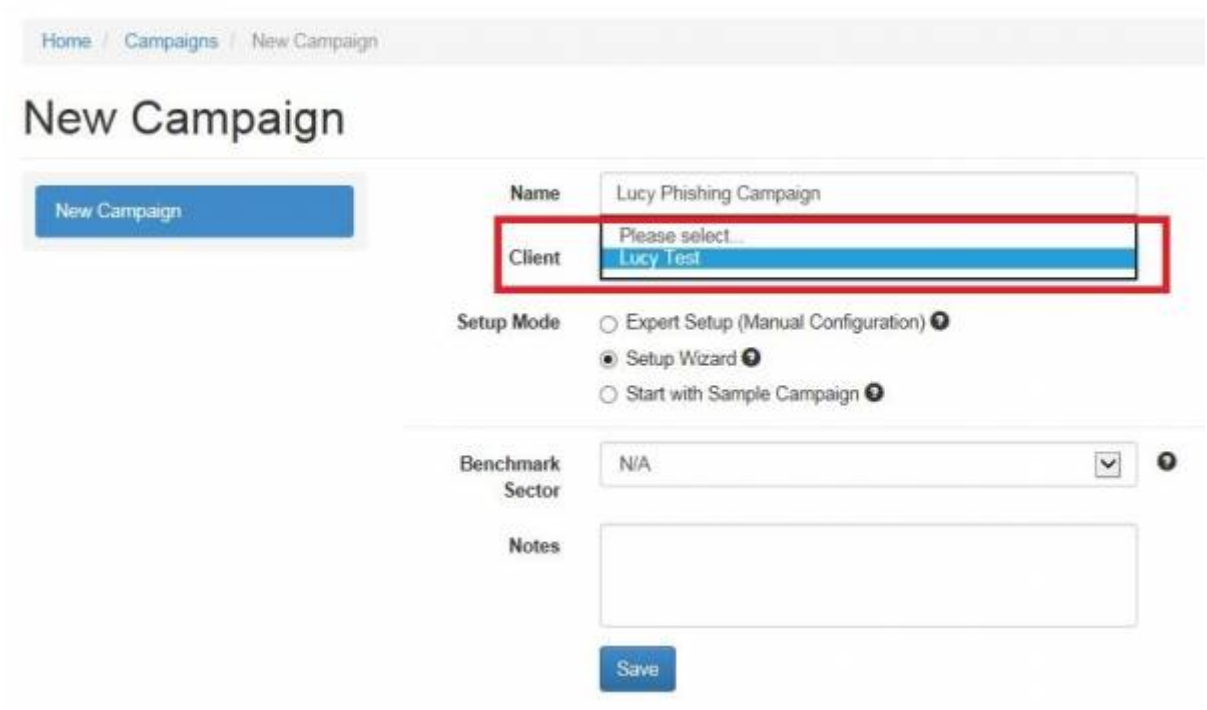


File based attack simulation configuration

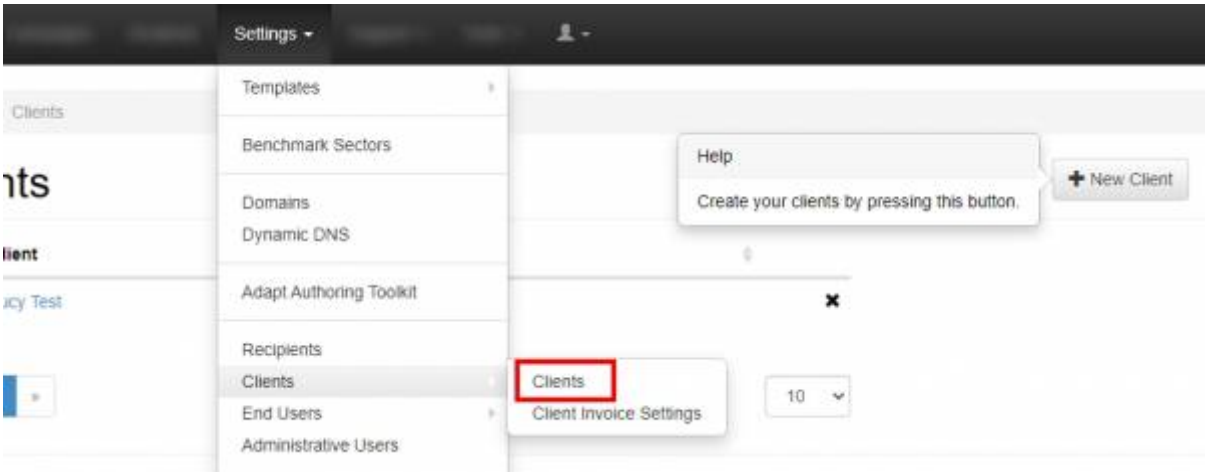
STEP 1 - Create a New Campaign After the login, you can create your first Phishing Campaign by pressing the button “**New**”.



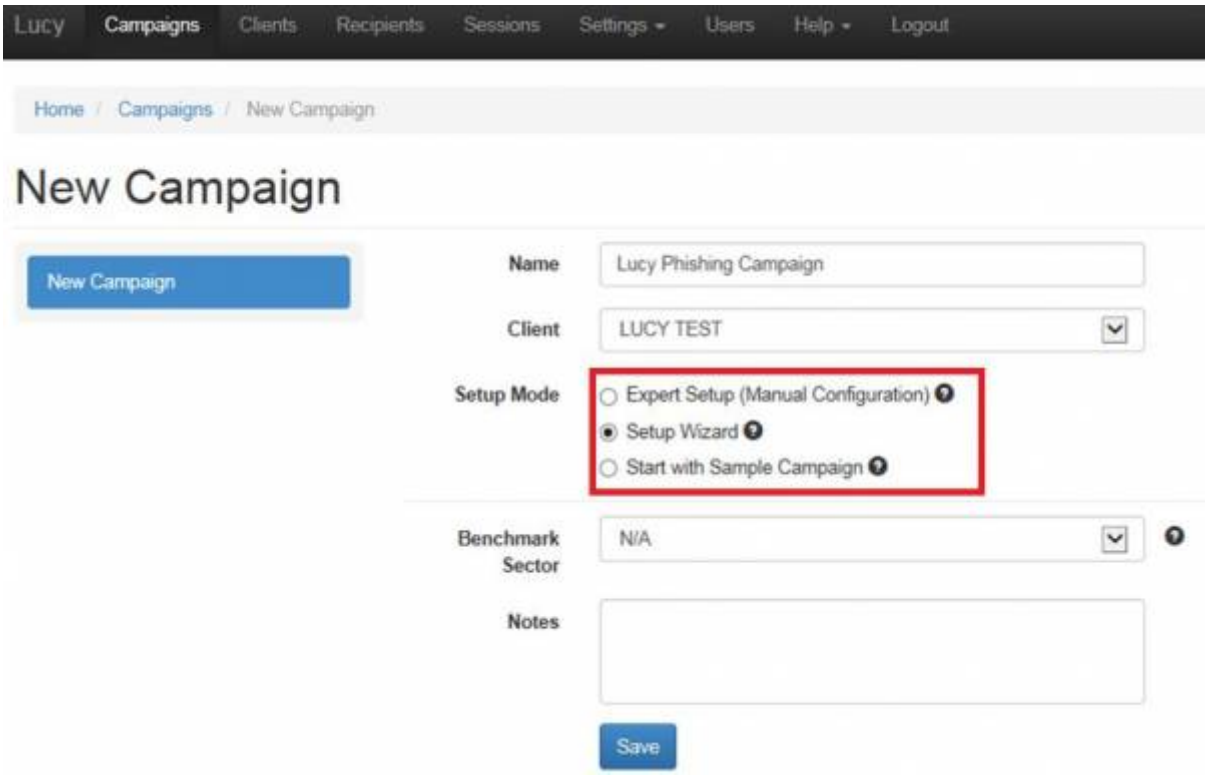
STEP 2 - Select or Create a Client: Create a client or choose the built-in client (a client can be your own organization or the company who asked you to perform a phishing test). This is important because you can also create view only accounts which are associated with those clients.



New clients can be created under "clients". In LUCY v. 2.5 and higher this is created under settings/clients.



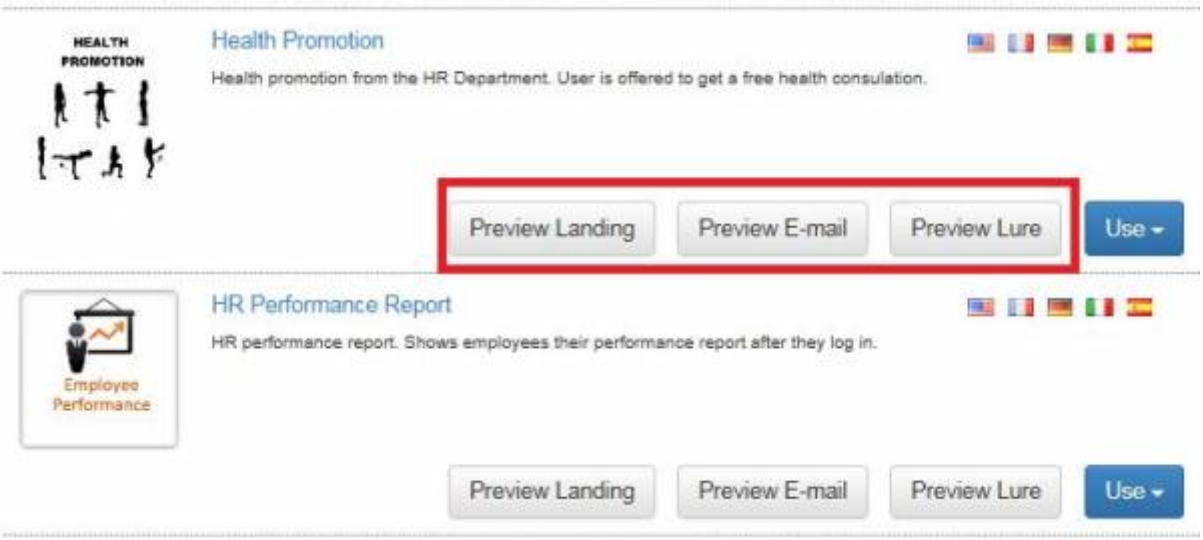
STEP 3 - Choose Your Configuration Mode: You may either continue with the **Expert Setup** or the **Setup Wizard**. We recommend using the Setup Wizard when used for the first time.



STEP 4 - Select your Phishing Scenario: Now you need to select one or multiple phishing scenarios. Since you are going to do a file based attack you need to pick a scenario either from the "file based templates" or the "mixed templates"

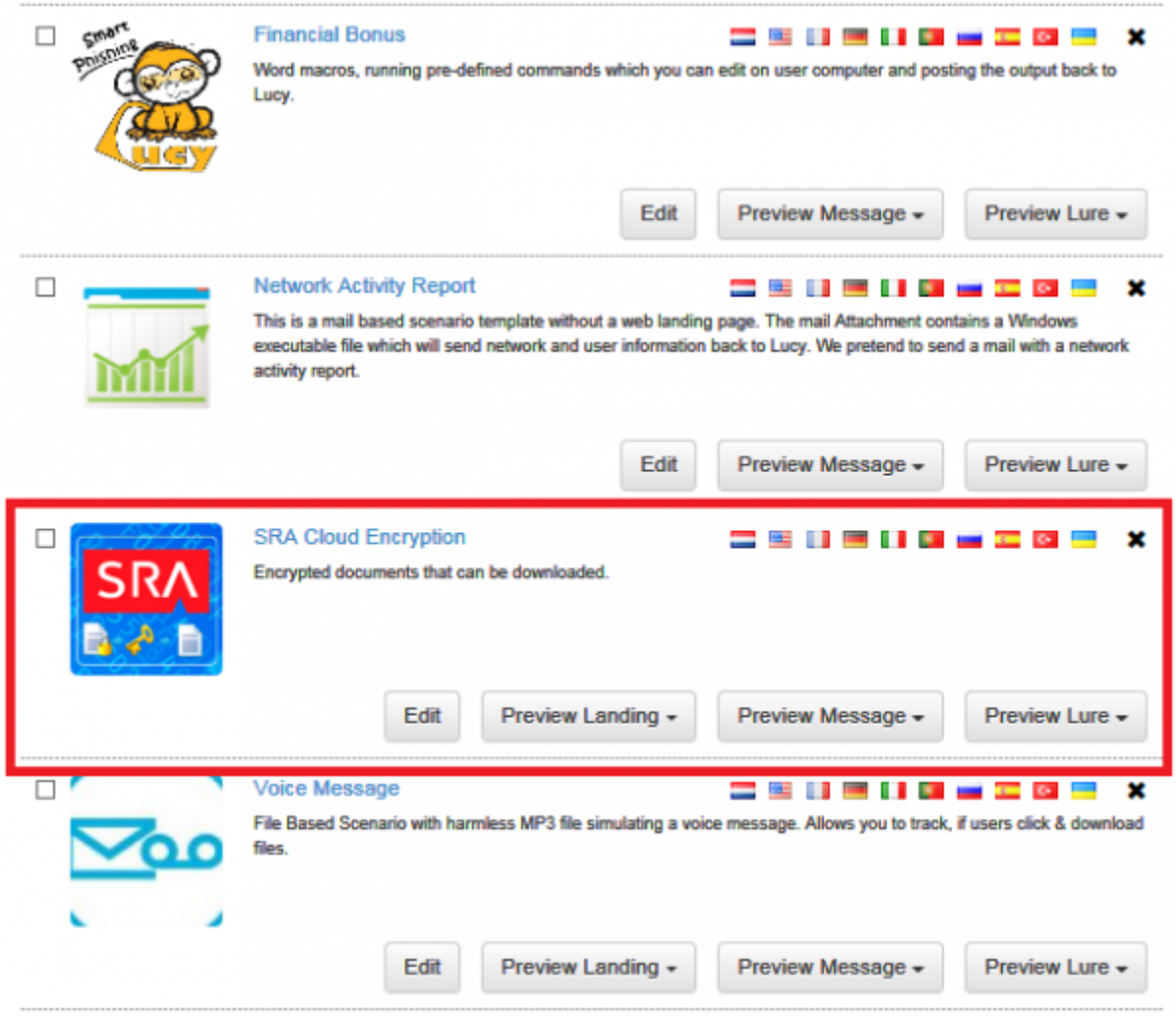


You are able to preview every template before selecting it. In the **Preview Mode** you can test the site using all the features (just enter some random login to get to the next page).

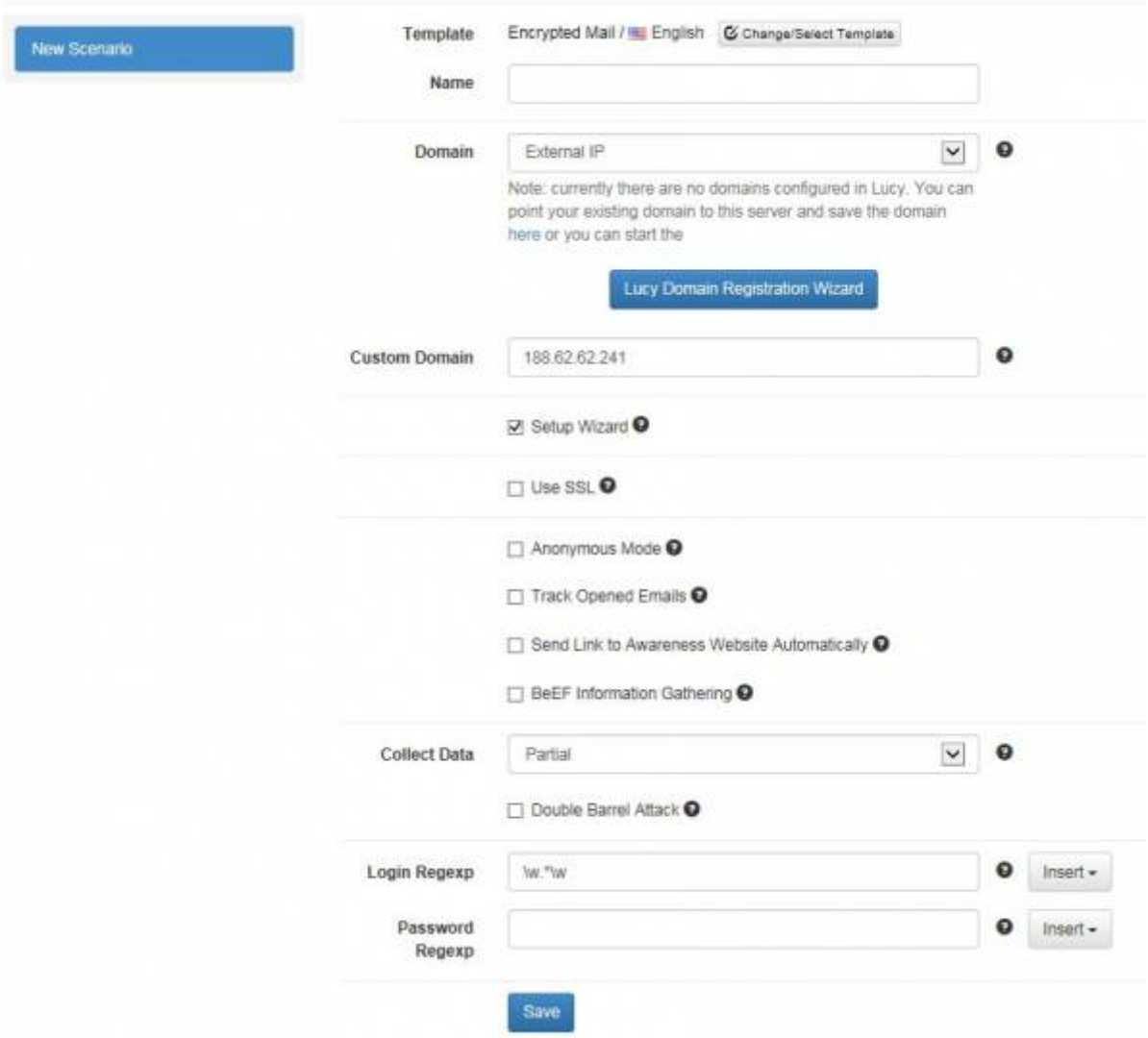


Note: **You can allocate multiple scenarios within one campaign** and they can all be started simultaneously! Example: A company might want to split the employees into 2 or 3 groups. One group could get a phishing mail with a landing page that contains many obvious errors and should be easily detectable while the other scenario is almost perfect. This way the client can identify the variables that drive the awareness in one single campaign.

STEP 5: For this tutorial, as an example, we select the “cloud encryption template”, where the user will be asked to download some encrypted file.

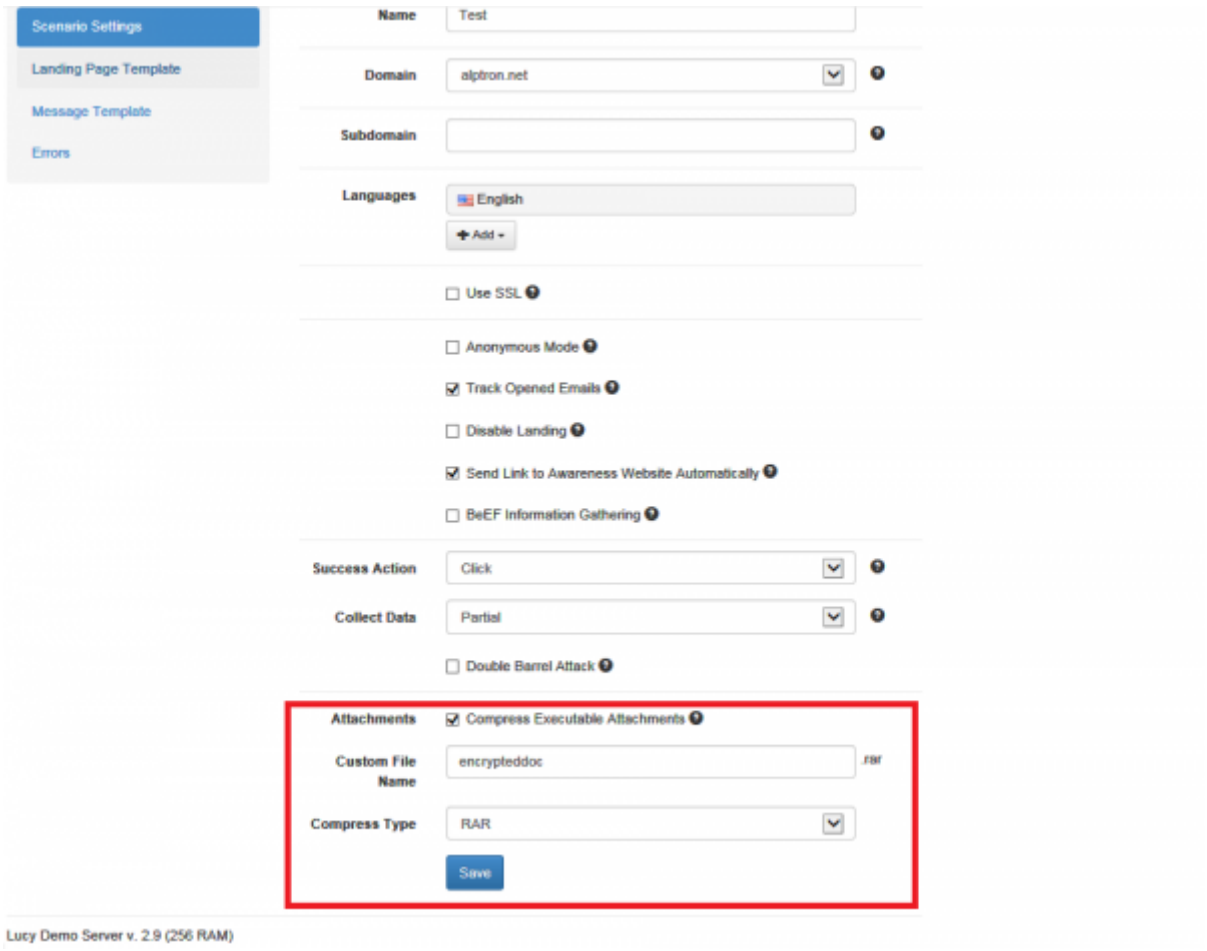


STEP 6 - Configure the Base Settings of Your Campaign Once you have selected the scenario, you need to configure the **Base Settings** of the campaign. First, give your campaign a name and then choose how your recipients will be able to access LUCY by defining the Domain. Finding the appropriate domain name is a very important step for the success and it depends very much on your campaign scenario. If you plan to create a fake web mail login you might try to reserve a domain like "webmail-server365.com" and point it to LUCY.



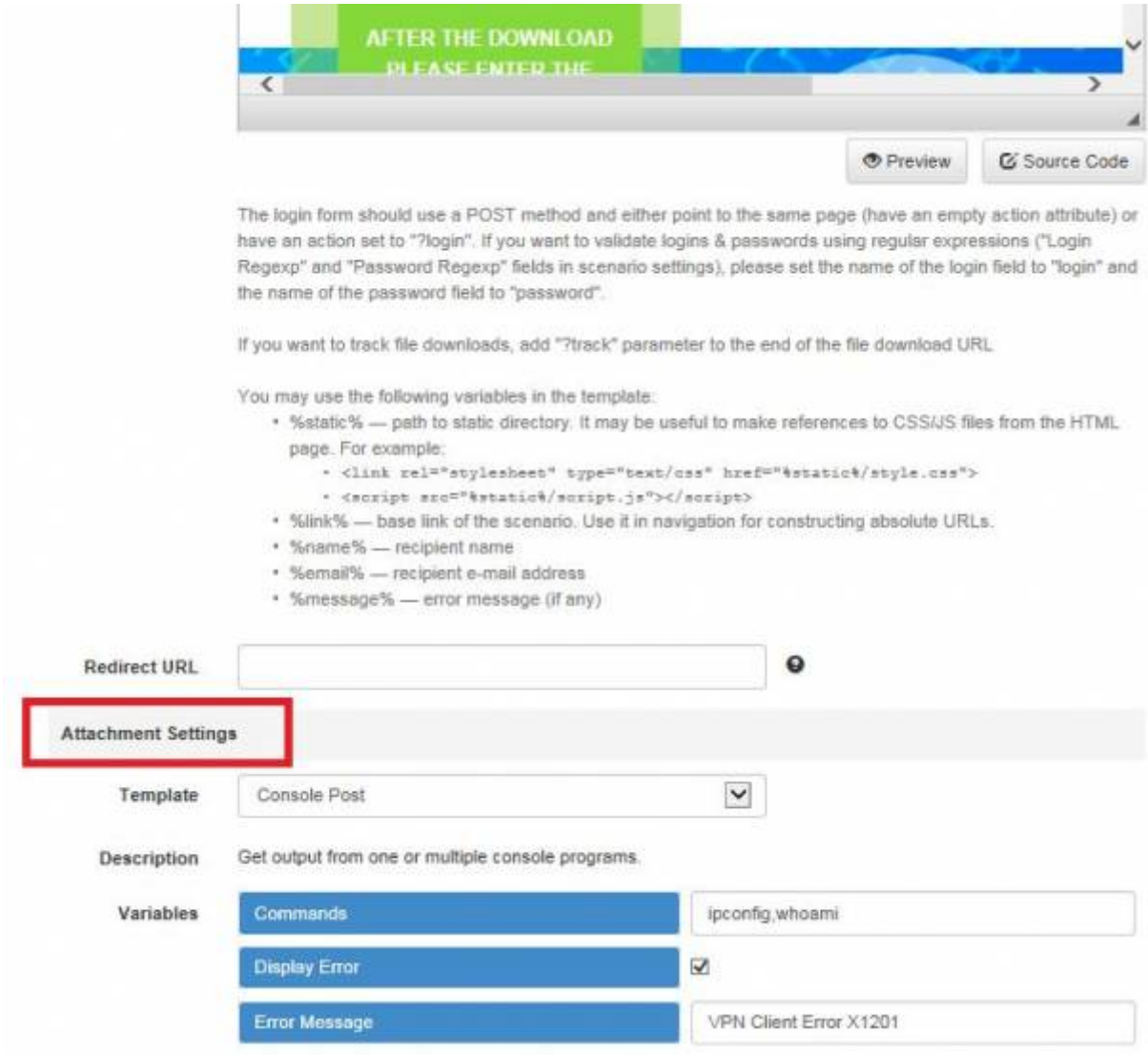
STEP 7 - Fine Tune the Basic Settings (each scenario has its own base settings): There a few **Optional Settings** that you can apply within the Base Settings. For the file based scenario you can adjust those settings within the "scenario settings":

- Attachments - Compress Executable Attachments: instead of sending the attachment as a plain file (e.g. file.exe) or providing it as an executable file to download you can set the compression option (this is recommended). Like this the file will be archived.
- Custom file name: you can give the archive a custom name (e.g. "encrypteddoc.zip")
- Compress Type: you can choose which compression type you want (the common type which is supported by all windows clients is .zip; other compression types will need additional client software)

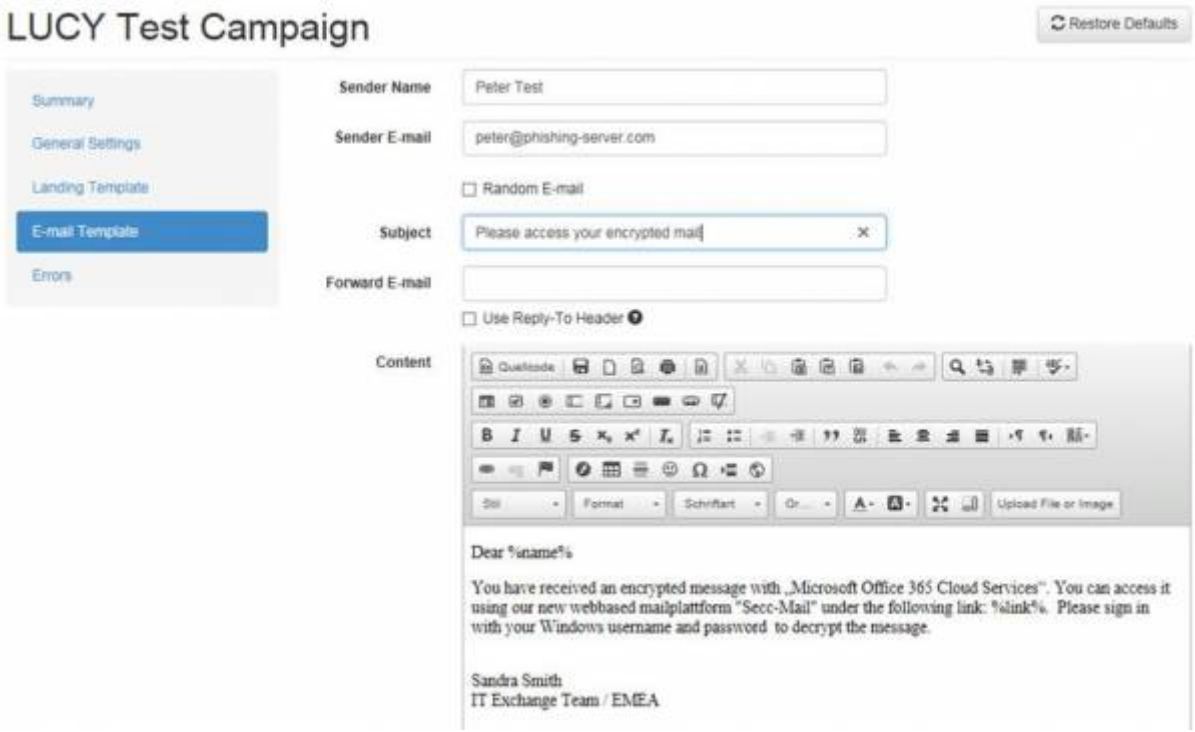


STEP 8 - Edit your Landing Web Page within Your Campaign: After saving the Base Settings, you can now Edit the Landing Page, Upload Your Own Webpage or simply copy any website on the internet. The Landing Page is the webpage that the users will see when they click on the link in the email they receive. First, select the drop-down menu at the top the page where you want to edit. Please note that the same landing page may be available in different languages. So make sure you edit the correct language. When you choose a file based attack scenario you will see some additional configuration options appearing at the bottom of the page. Those settings define what file is provided within the download button for the recipient and what the executable should do upon opening. We recommend starting with a "harmless", non-intrusive trojan simulation that doesn't violate the recipients data privacy. A harmless simulation is, for example, the ConsolePost" Trojan, which will stealthily execute a few pre-defined commands (like "whoami") in the users shell and send the output back to LUCY. You have a few additional options:

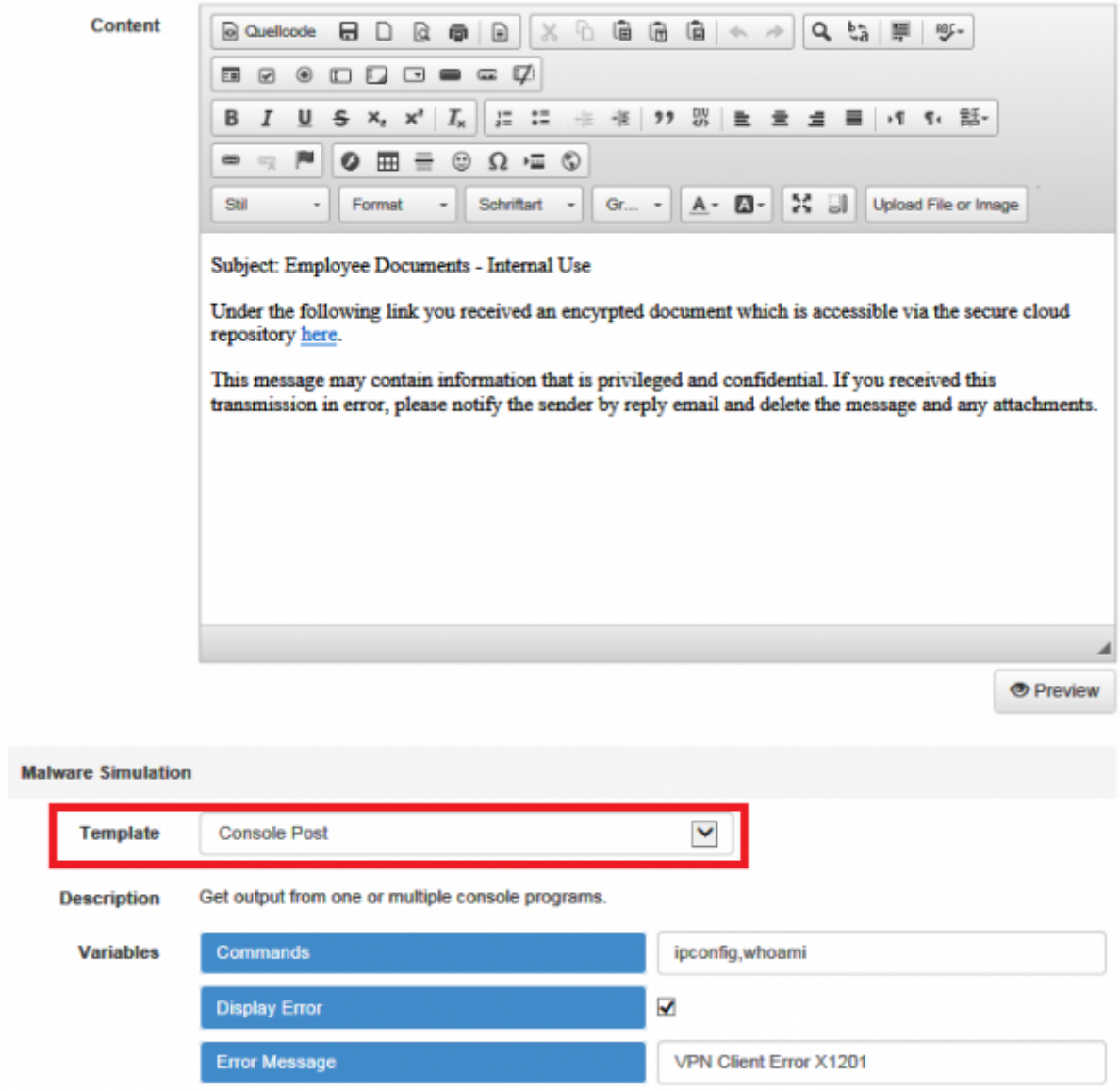
- Decide if the user should see some fake GUI upon execution or not
- Specify a specific error message that will appear upon execution
- Specify the Trojan settings (e.g. enable/disable specific Trojan features or define custom commands)



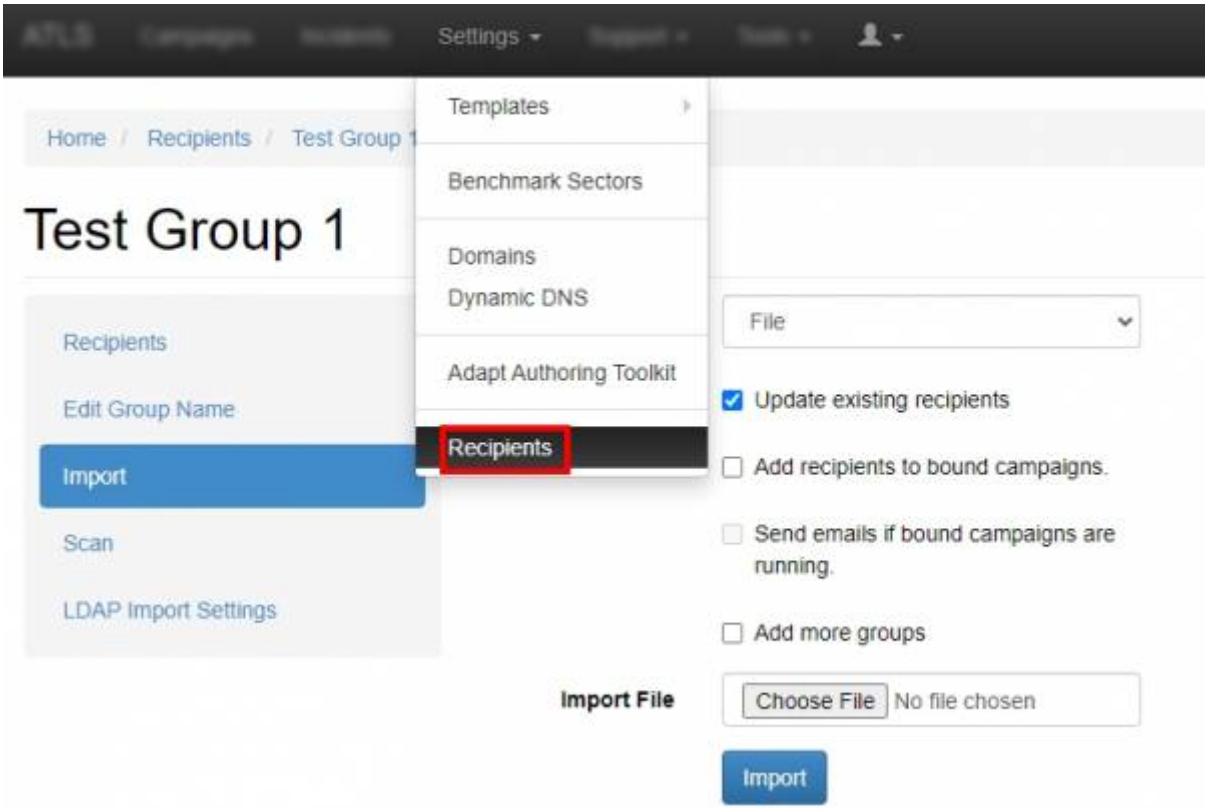
STEP 9 - Configure Message Settings (Email): It's time to setup email communication (if you want you can also use SMS as an alternative). Choose your sender's name, email address, and subject. Please also choose the language for each group. If you configured an English landing page, then select English also within that recipient group. If you have different groups with different languages within your company you can simply create a group and select a language for each recipient. LUCY then will direct each user to an individual landing page that matches that language. Please read the Mail Settings Chapter for more configuration options.



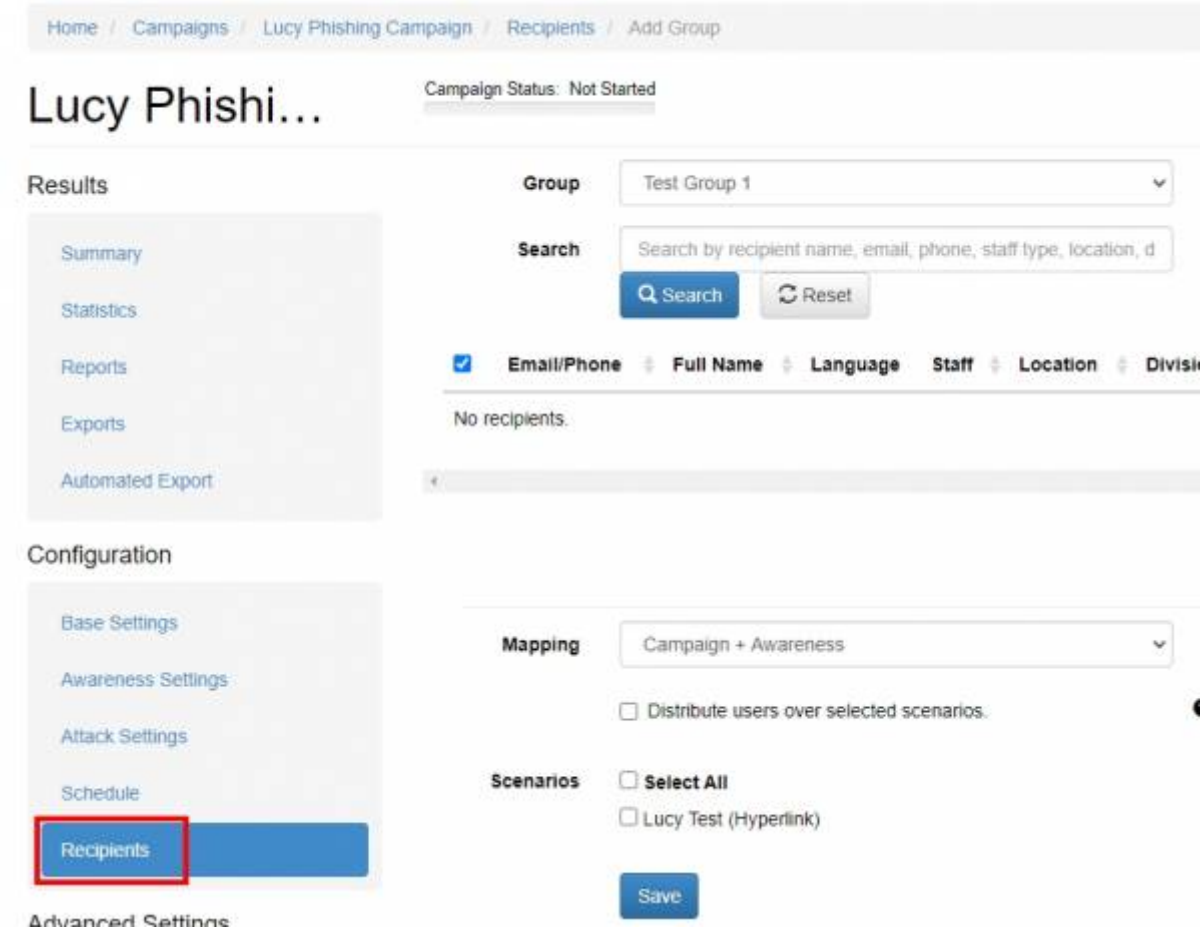
When choosing a file based scenario LUCY will offer you additionally to send the Trojan simulation via mail. If you already have chosen a landing page where the Trojan simulation can be downloaded it is not necessary to attach it via mail as well. Therefore if you don't want LUCY to send the file via mail choose "NA" within the malware simulation template dropdown menu:



STEP 10 - Add Recipients to Your Campaign: You need to create the Recipients List in the Menu item "Recipients".



This is the list of users that will get the phishing emails. You can add them manually, import a file with all your recipients or even search them on the internet. Once you have created that group, you can select it in your campaign and map them to a specific scenario. You can also define if they should be used only for the Landing Page link, the Awareness site link (e-learning) or both.



Please read the Recipients Settings Chapter for more configuration options.

STEP 11 - Add Scheduling Options to Your Campaign: If you want, you can create a schedule to run the campaign using a delay or customized time delays between campaign phases. If you are new to the system, we'd recommend that you go with the Default Timing Settings and skip this step. Please read the Schedule Settings Chapter for more configuration options.

Step 12 - Add E-learning Content to Your Campaign There is the option to have LUCY automatically send some e-learning content to all users or only users who have failed the phishing test. This configuration setting is part of an Separate Chapter (E-learning).

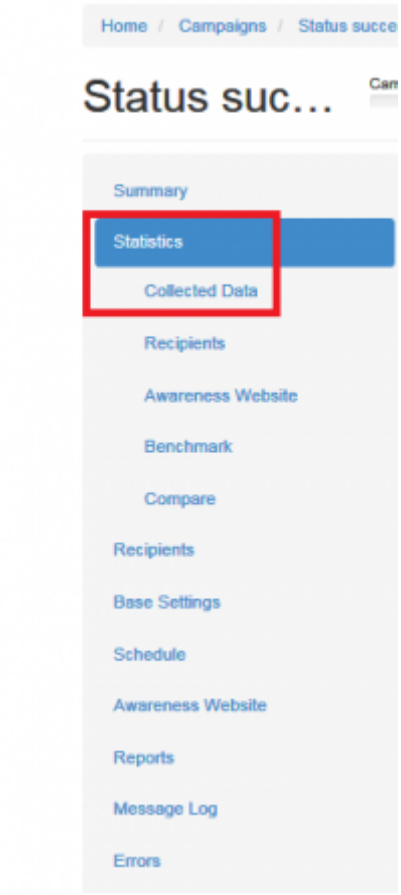
Step 13 - Start Your Campaign: Now you are ready to start. Although we recommend performing a test run with a single recipient before you start attacking all users, additionally it is a good idea to use the LUCY SPAM Checker. Just click “Real Attack” and LUCY will test your settings before starting the campaign. If you want to skip the checks, press "Skip Checks". Your first recipients should receive the emails within seconds. Please read the Start Campaign Settings Page for more configuration options. If you experience any problems with starting/running your campaign, please Consult the Troubleshoot Section first.



Step 14 - Monitor Your Campaign: The progress of the campaign can always be monitored in Real-Time. Click "Statistics" within your campaign. Please read the Statistics Chapter for more configuration options.



The output from each Trojan execution can be found under "statistics/collected data":

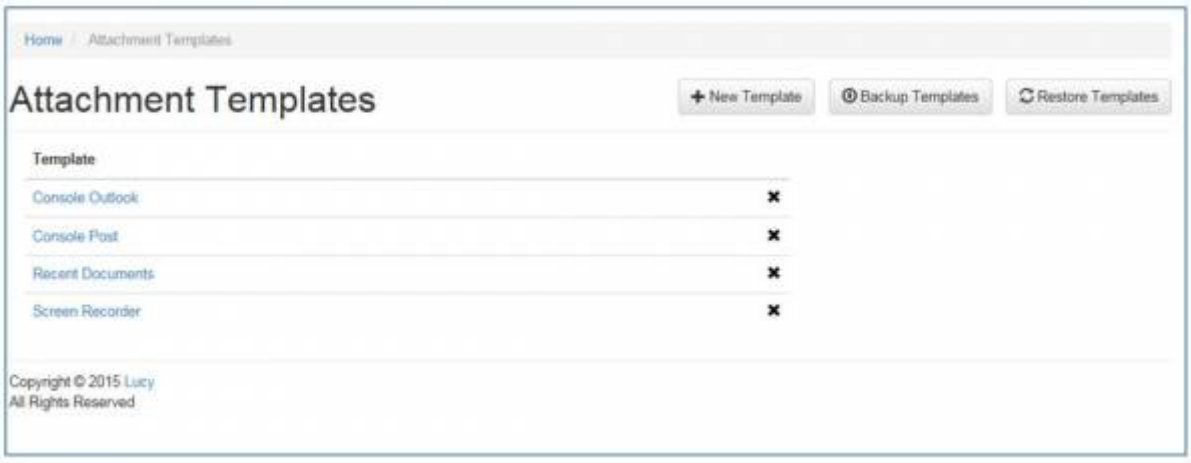


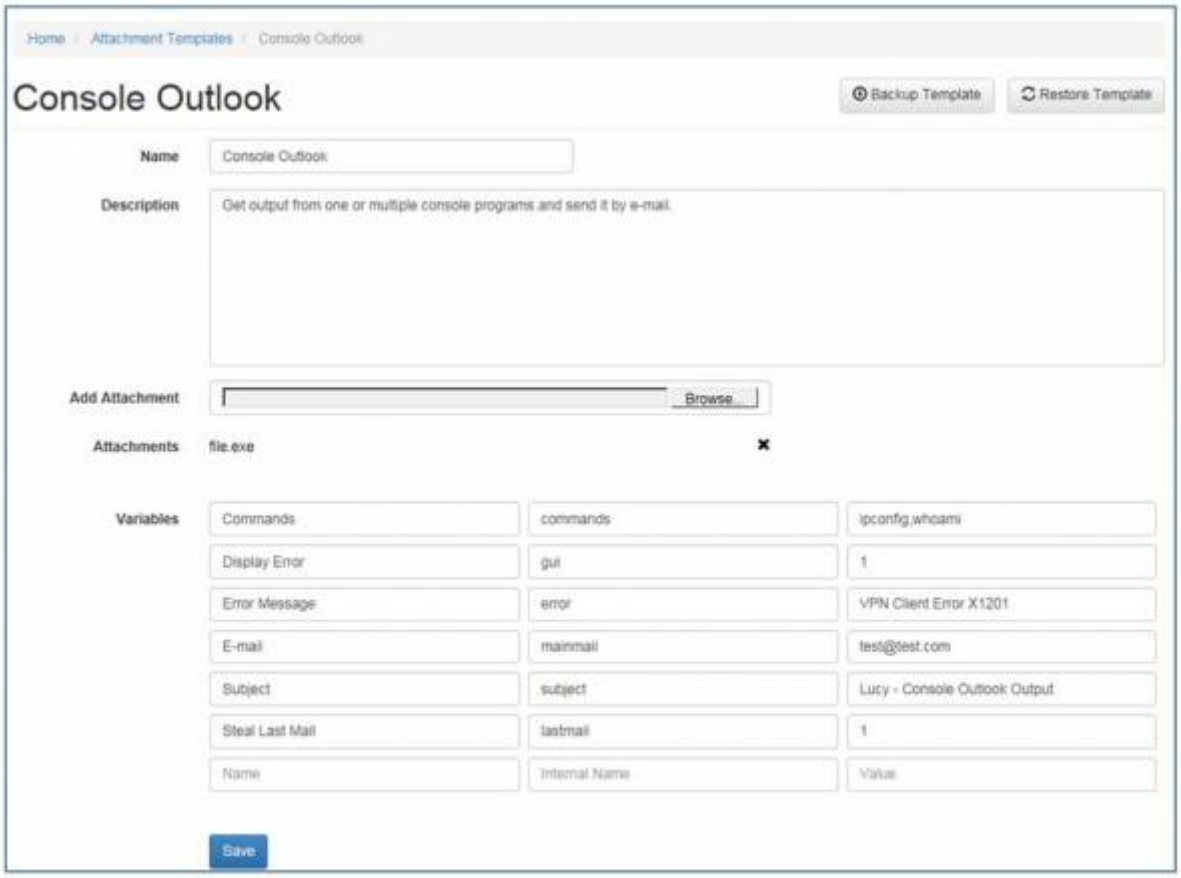
Step 15 - Create Reports: Once you have finished the campaign, you may create different types of reports (PDF, HTML or raw export). Please read the Creating Reports Chapter for more configuration options.



Edit File based templates

All attachments can be edited within LUCY. The Attachments Settings can be stored as Default templates under Settings/Attachment templates.





You can rename the file templates from file.exe to any filename. In LUCY < 3.2 you can do that by downloading the file.exe, renaming it & then uploading it back to the generic file template.

Technical Details about the data delivery

Upon execution, this tool will execute the predefined commands or access documents. It will open the built-in Internet Explorer or another default browser (in hidden mode) or access Outlook and send out the collected data to LUCY via HTTP or HTTPS or via SMPT (it will automatically choose HTTPS if you run your campaign via SSL). This tool will also work in environments where the Internet is accessed with Proxy servers - only allowing access for authorized Windows users. The file can then be downloaded as a plain exe or as a zipped archive.

Note: The current edition of LUCY will include tools that access files on shares and upload them to the campaign or access the email client via MAPI. These features have restricted configuration options in the community edition (like maximum number of files that can be uploaded, etc.) the same goes for the number of screenshots or length of videos. Only the Commercial Editions have no limitations. You can upload your own custom payload. But keep in mind that reverse channels to LUCY won't work; only attachments from LUCY are compiled in Real Time with certain settings (IP, Domain Name, URL etc.).

Delivery Challenges

Executable files usually cannot be delivered to a user via e-mail attachment. These are blocked by

most email programs.

In order to deliver a malware simulation to the user, the attachment should not be provided via email, but via download on a website. There you have the possibility to download the file:

- Inside an archve (zip, jar, rar etc.)
- Inside an encrypted file (e.g. zip with a password)
- Inside a PDF
- Tunneled through an aplet
- Download as a plain exe

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

Permanent link:
https://wiki.lucysecurity.com/doku.php?id=create_a_phishing_campaign_with_malware_simulations&rev=1568098723

Last update: **2019/09/10 08:58**